Avaya one-X® Attendant 4.02

connected to

Avaya Communication Manager

Installation and Administration Manual

16-603459-EN
Release 4.02
Version 1
December 2012

Service and Installation Manual

one-X® Attendant connected to Avaya Communication Manager

Version: 12/2012

All technical data, information and properties of the product described in this document have been compiled to the best of our knowledge at the time of printing.

Subject to modification and improvements to the product in the course of technical developments.

Avaya GmbH & Co. KG Documentation

About this document

Who is this manual for?

This manual is for technical staff who install and configure Avaya one-X   Attendant applications.

Use this manual as you wish for reference purposes regarding individual topics or to learn how to install and configure the applications.

What information is available in the manual?

This manual contains information on how to install and configure the one-X Attendant and how to upgrade from a former version.

What information is not in the manual?

This manual does not contain any information on how to use the one-X Attendant.

How is this manual structured?

The structure of this manual provides a step–by–step introduction. Usually, an introduction to the topic is provided first. Prerequisites or necessary skills are often described next. Instructions follow the prerequisites or necessary skills. An illustration or example further clarifies the topic.

Where can you find additional information?

Further information on one-X Attendant and the installation of various components can be found in the documents specified in the references .

Avaya one-X Attendant Overview

Please familiarize yourself with these components

List of components

Whether you serve as a switchboard for many users or connect calls on a smaller scale, the **one-X Attendant** operator position provides just the tools and functions you need to expertly forward calls to the correct party.

Before you can use a one-X Attendant operator position, various components must be installed and operational.

Below is a list of all components. The following descriptions explain the functions of each of the components.

- one-X Attendant application
- One–X Attendant server (Database/JOnAS/Tomcat)
- SCAPI, iClarity
- SVA Manager (network–wide busy display)
- Presence Server (Absence and Busy Display)
- WebLM
- WebAccess
- Absence Info Server
- TTrace

Component: one-X Attendant application

The **one-X Attendant** application is a client application you can use to access different servers and databases.

Component: Database/JOnAS

In order to run the **one-X Attendant** application you need a database. The database contains the configuration and phone book data. A database management system, **Sybase SQL Anywhere 11.0.1**, (ASA) and an application server, **JOnAS**, are used for the database.

JOnAS and **ASA** cannot be separated. Both servers must be installed on the same computer.

Component: SCAPI, iClarity

After you start one-X Attendant, it loads Softconsole API (SCAPI) and starts iClarity. These processes are used for communication between OS-TAPI and Avaya Communication Manager (ACM).

In Road Warrior-mode iClarity is used for VoIP-voice communications between one-X Attendant (e.g. using a headset) and ACM. iClarity is a component of Avaya Softconsole. It is installed automatically and does **not** have a separate setup.

Components: QTAPI Framework, TSAPI Client

QTAPI Framework and TSAPI Client together form the interface between AES-Server and the SVA Manager. Both components are installed together with SVA Manager.

A new program group **Avaya AE Services** > **TSAPI Client** will be created for TSAPI.

Component: MasterDirectory

MasterDirectory is an application for the management of databases. Master directory consolidates and synchronizes the managed databases. CM-data can be easily imported using MasterDirectory.

The MasterDirectory is integrated into one-X Attendant just like every other database.

Component: SVA Manager

SVA Manager is an independent server. Its purpose is to provide the network–wide busy display.

It uses the QTAPI framework and is connected with the one-X Attendant using a TCP/IP-interface.

SVA Manager runs as a service on the PC and has no windows. It is started every time the PC is booted up, independently of one-X Attendant.

SVA Manager only needs to be installed once in the network. At least it can be installed on the client, on the server , or on another PC in the Network.

Program outputs can be viewed using the TTrace Monitor.

Component: Presence Server

The Presence Server is a discrete Server for the transmission of absence and busy states. The one-X Attendant is connected via a ppresence SDK with the Presence Server. This „local Presence Server“ is started with the start of the Absence Info Pusher. The Presence Server has no window and is administered via SMGR.

Component: Web server

A web server is needed for the out–of–office notice. One-X Attendant uses the Tomcat web server which is integrated in the JOnAS. You cannot use another web server (such as Apache Web Server) for one-X Attendant

Component: WebAccess

WebAccess contains the HTML and Java Server pages for the Web server to configure the out–of–office notice using AIS (see below) or a browser. Installing the one-X Attendant Server(JOnAS) installs the following components.

- HTML pages
- Java Server Pages
- Web server activation

Component: WebAccess admin tool

This tool is used for resetting the user password for WebAccess.

Component: Absence Info Server (AIS)

AIS lets the **one-X Attendant** application detect and use an out–of–office notice set in Microsoft Exchange Server. AIS is installed on a central PC in the network and uses MAPI to access the Exchange Server.

Component: WebLM License Manager

WebLM License Manager must be available on the network. It manages licenses for one-X Attendant and its components.

Component: Calendar information

You can use Outlook or Lotus Notes to query calendar information. However, you can only use one of these at a time. You need an appropriate active client on the one-X Attendant client PC (and the AVAYA one–X Attendant Presence License).

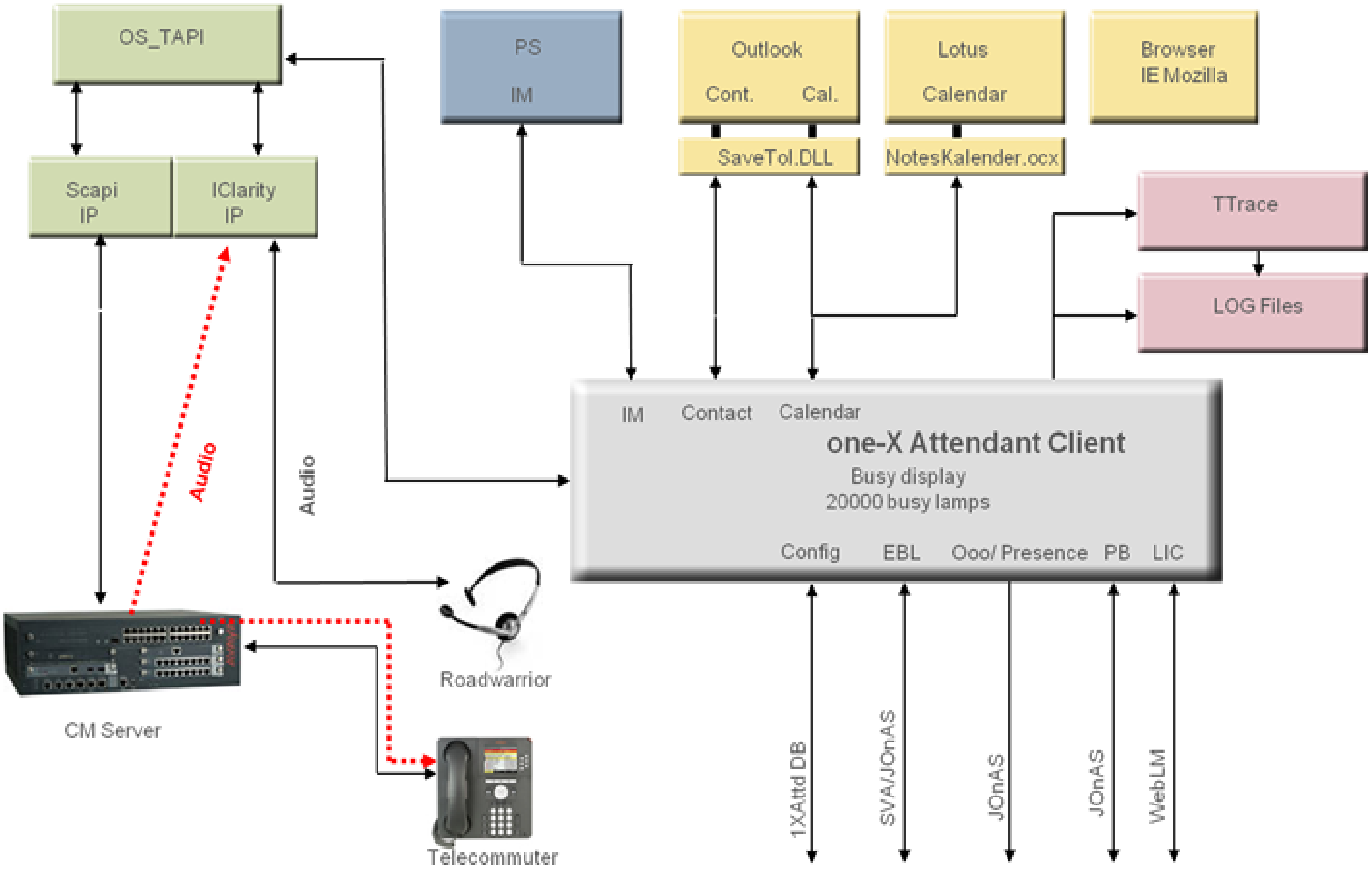
Valid component versions

For one-X Attendant to work with all the other components, you must have the correct version of the components. Installing the components from the installation CD will of course install the correct versions. Always consult your system specialist before installing any other versions, even newer versions! You will find some information in the chapters Systemrequirements for Avaya one–X Attendant or System Requirements for ACM or Absence Infor Server (AIS).

Block diagram of one-X Attendant in conjunction with all additional components

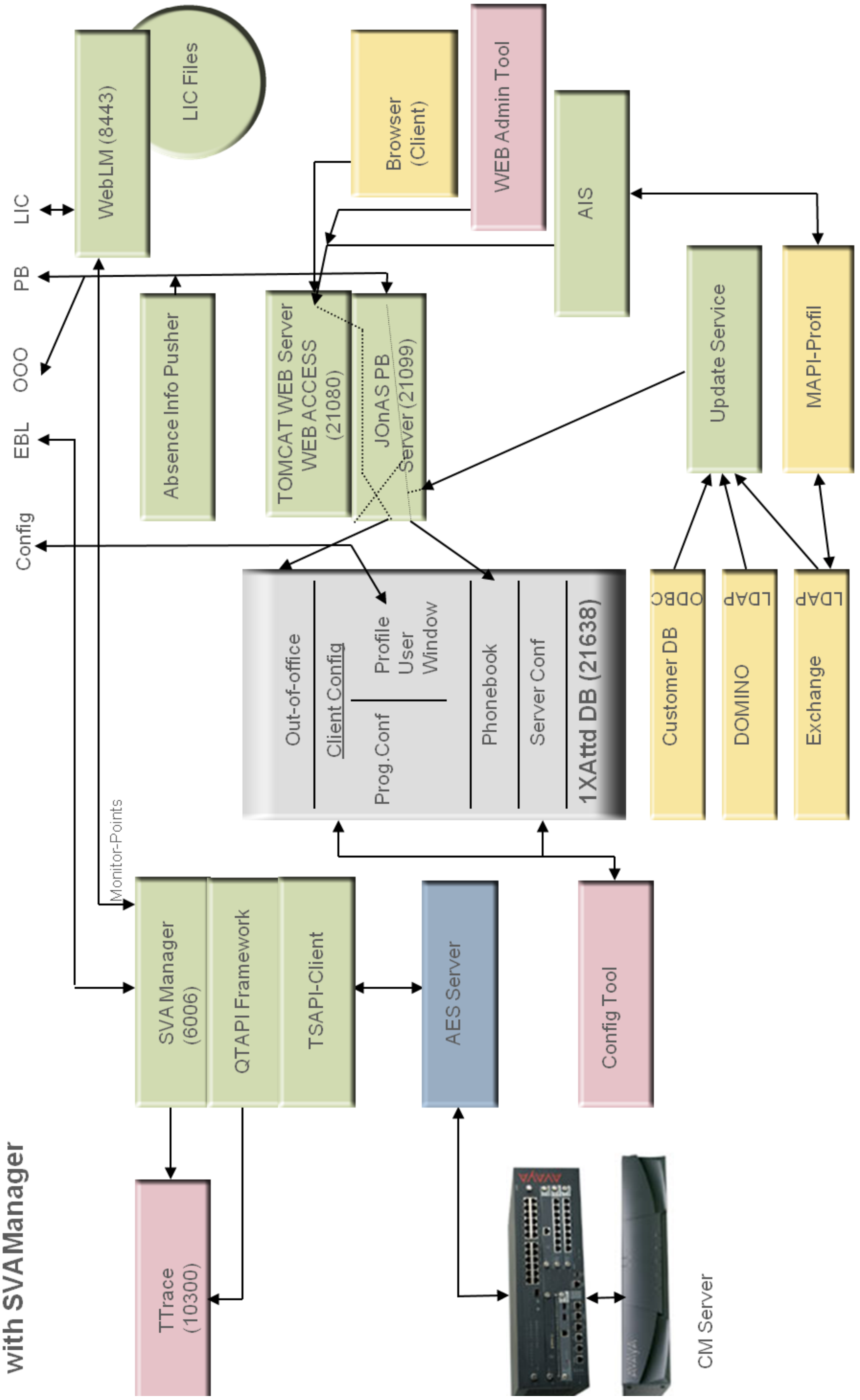
The following block diagrams of one-X Attendant Client and one-X Attendant Server show how all the application components work together.

Block diagram one-X Attendant Client (ACM)



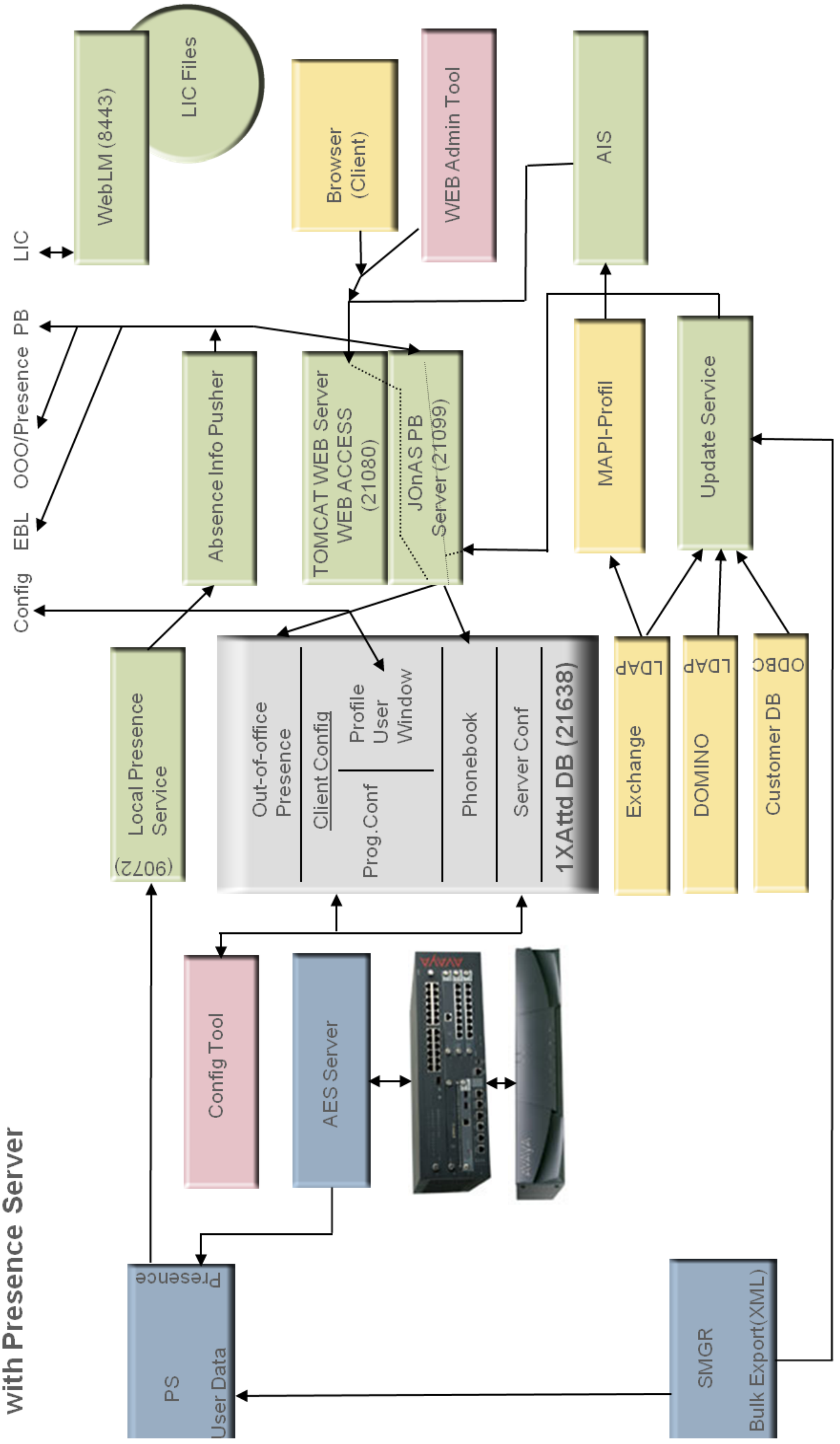
Block diagram one-X Attendant Server (CM)

with SVAManager



Block diagram one-X Attendant Server (CM)

with Presence Server



Connecting to Avaya Communication Manager

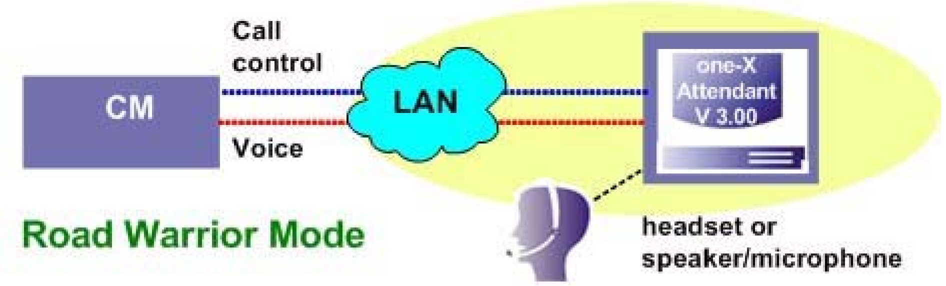
Avaya one-X Attendant can be connected with the ACM in two ways –
in Road Warrior mode or in Telecommuter mode.

Road Warrior mode:

In the Road Warrior configuration there is only one IP connection between PC and ACM. Control software and audio software must be installed on the PC.

In this case, the control software is the one–X Attendant application, which performs all call signaling and control tasks.
VoIP communication is processed using iClarity IP Audio (an H.323-V2- compatible audio application). Avaya iClarity IP Audio runs in the background. This program is launched automatically as soon as you launch up Avaya one–X Attendant.
You need one of the following for communication:

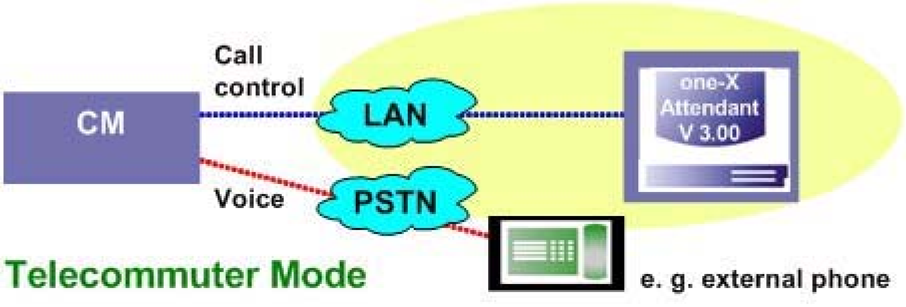
- a headset connected to the PC,
- a combination of PC speakers and a microphone, or
- a USB phone. A USB phone converts the analog audio data into digital signals itself, thus relieving the PC of the task. We recommend a USB–phone for this reason.



Telecommuter mode.:

In Telecommuter (dual connection) mode, the PC on which one-X Attendant is running and a telephone are connected separately to ACM.

The PC is connected to ACM over an IP network (LAN). All calls are signaled and controlled via this connection.
Voice communication takes place using any telephone connected anywhere to your PBX (ISDN, analog, VoIP). The actual conversations can therefore be made with the usual quality and convenience to which you are accustomed.



Hint:
see Tips&Tricks “One-X Attendant in Telecommuter Mode” on page 144

Installing the software

Avaya one-X Attendant system requirements

System requirements: Server

The PC running the server components must meet the following minimum requirements:

The latest service pack has to be installed in all cases.

Only one-X Attendant server:

- Quad Core CPU with 3 GHz (Server-Hardware or comparable powerful Virtual Machine)
- 3 GBytes RAM (Recommended 6 GBytes for 64Bit)
- 1 GBytes available disk space (depending on data)
- 100 Mbit/s Ethernet IP connection
- Operating systems 32 Bit: Windows Server 2008 SP2 Standard/Enterprise (recommended), Windows 7 Professional/Ultimate
- Operating systems 64 Bit: Windows Server 2008 R2 Standard/Enterprise (recommended), Windows Server 2008 SP2 Standard/Enterprise, Win 7 Professional/Ultimate, 2008 R2 (Enterprise/Standard), Windows 7 (Professional/Ultimate).
- The latest service pack has to be ionstalled in all cases.

one-X Attendant Server with other server components (i.e. Exchange, Lotus Domino etc..) :

- Quad Core CPU with 3 GHz (Server-Hardware or comparable powerful Virtual Machine)
- 4 GBytes RAM (recommended 6 GBytes)
- 2 GBytes available disk space (depending on data)
- 100 Mbit/s Ethernet IP connection
- Operating systems 64 Bit: Windows Server 2008 R2 Standard/Enterprise (recommended).
- Operating systems 32 Bit: Windows Server 2008 SP2 Standard/Enterprise (recommended)
- The latest service pack has to be installed in all cases.

One-X Attendant Server on a virtual Machine:

- VMWare ESXi, 4.0.0,208167
- Per VM 1vCPU, 1GB RAM
- 100 Mbit/s Ethernet IP connection
- Operating system: Windows 7 Professional 64 Bit, Windows 7 Ultimate 32 Bit, Windows 7 Ultimate 64 Bit, Windows Server 2008 SP2 32 Bit, Windows Server 2008 SP2 64 Bit.
- One-X Attendant Client on a separat PC, system requirements see. below

Or

- HyperV Manager
- Per VM 1vCPU, 1GB RAM
- 100 Mbit/s Ethernet IP connection
- Operating system: Windows 7 Professional 64 Bit, Windows 7 Ultimate 32 Bit, Windows 7 Ultimate 64 Bit, Windows Server 2008 SP 32 Bit, Windows Server 2008 SP2 64 Bit.

- One-X Attendant Client on a separat PC, system requirements see below

System requirements: Client

The PC running the **one-X Attendant** application must meet the following minimum requirements:

- PC with 2 GHz
- 1 GBytes RAM, (2 GB for 64 Bit OS and in case of 3rd party products e.g. MS Office, …)
- 700 MBytes available disk space (depending on data)
- 100 Mbit/s Ethernet IP connection
- 19"-monitor with 1280x1024 pixels.(or a 21" monitor for visually impaired users)
- 1 free COM interface if a Braille module is connected.
- Printer with graphics capability for printing charges and statistical data.
- *In Road Warrior mode:* Only USB Headsets with DSP or USB phone.
- *In Telecommuter mode:* Any telephone that can be reached from theACM.
- Operating system 32 Bit: Windows 7 Professional/Ultimate (recommended), Windows XP Professional, Windows Server 2008 SP2 Enterprise/Standard .
- *Operating system 64 Bit:* Windows 7 Professional/Ultimate (recommended), Windows Server 2008 R2 Enterprise/Standard
- R2 (Enterprise/Standard), Windows 7 (Professional/Ultimate).
- The latest service pack has to be installed in every case.
- Running Softconsole and one-X Attendant in parallel
- Softconsole and one-X Attendant cannot be run in parallel on the same PC. However, parallel running on the same ACM on different PCs is possible.

System requirements: Single-user

A PC with a single–user solution must meet the following hardware and software requirements.

- PC with 2 GHz
- 3 GBytes RAM (recommended 5 GBytes),depending on the configuration and installation of other components (for example MS-Outlook, MS-Word)
- Operating system 32 Bit: Windows 7 Professional/Ultimate (recommended), Windows XP Professional, Windows Server 2008 SP2 Enterprise/Standard .
- Operating systems 64 Bit: Windows 7 Professional/Ultimate (recommended), Windows Server 2008 R2 Enterprise/Standard).
- The latest service pack has to be installed in every case!
- 800 MBytes available disk space (depending on data)
- 100 Mbit/s Ethernet IP connection
- 19"-TFT-monitor with 1280x1024 pixels (for visually impaired users a 21"-TFT-monitor)
- 1 free COM interface if a Braille module is connected.
- *In Road Warrior mode:* USB Headsets with DSP or USB phone.
- *In Telecommuter mode:* any telephone connected to your PBX.
- You will need a printer with graphics capability to output charges data and statistical data.
- Running Softconsole and one-X Attendant in parallel
  Softconsole and one-X Attendant cannot be run in parallel on the same PC. However, parallel running on the same ACM on different PCs is possible

Client–server LAN connection

Client and server must be connected via a LAN offering sufficient bandwidth.

Avaya Communication Manager system requirements

Version

The ACM with which the one-X Attendant is connected must be version 3.1 or higher.
If you want to use the network–wide busy display, you must also connect an
AES version 4.2.1 or higher.

Licenses

The **ACM** must have the following licenses installed (material code 174.066):

“Value_IP_ATTD_CO” (IP Attendant Consoles),
“VALUE_PORT” (Maximum Ports),
“REGISTRATION” (IP Endpoint Registration) and
“FEAT_IP_ATTN” (IP Attendant Consoles).

The licenses are supplied together with the one-X Attendant licenses. One-X Attendant does not run without these licenses.

If you want to use **AES**, the following licenses must be available for every TSAPI link (material code 217.340)::

“VALUE_TSAPI_USERS_T1” (TSAPI Simultaneous User).

Configuration

The ACM must have an “attendant” configured there so that the one-X Attendant can run with it. Some of these settings affect the

one-X Attendant directly. These settings will be loaded every time the one-X Attendant logs on to the ACM.

Note:

Any changes to these settings within one-X Attendant do not affect the settings of the ACM.

Example configurations for ACM can be found in the appendix.

If one-X Attendant client is in conversation status (it has an active call) no other call
shall be delivered to this client. In paticular CM Huntgroups could be configured
by the parameter "Multiple Call Handling" to deliver more than one call simultaneously. Don't use this option.

Installations (setups)

Possible installations

This chapter describes the first installation of a One–X Attendant on a machine. To use all the **one-X Attendant** functions, you must perform the following installations (setups). There is one installation file for each installation.

1. Avaya WebLM server
   Installing WebLM installs the Avaya license management program for one-X Attendant. The server is an absolute requirement and must be installed before one-X Attendant
2. one-X Attendant
   There are four different types of setup. For a detailed description, see below.
3. Absence Info Server (AIS)
   The AIS evaluates the out–of–office information from Exchange. You need special licenses for the AIS The AIS can be installed after the one-X Attendant .

Migrating from previous OSPC versions

It is possible to migrate from OSPC version 2.5x. Direct upgrades are not supported .

General setup information

You must have administrator rights to install all one-X Attendant components.

- The setup user interface language is the language of your operating system. If a language other than German or English is set there, the setup language is English.
- All settings are preconfigured with default values.
- Following installation, all Services are started automatically.

Install WebLM License Manager

One-X Attendant is licensed using the Avaya **WebLM** license manager.

Installations

First, you need to install the WebLM server.

It is recommended that you install it from the one-X Attendant CD, even if there is another WebLM server running on the network already. It is possible that the license manager cannot serve one-X Attendant and other applications simultaneously.

More detailed information on installation and configuration can be found in references /1/ and /9/ .

1. Insert the one-X Attendant installation CD in your CD drive.
   The Overview start page opens in your standard browser.
2. Click Avaya WebLM Server.
3. .Follow the directions given by the installation wizard.

Request license

The licenses for the one-X Attendant are tied to the PC hardware of the WebLM server (MAC address). If the WebLM is installed on a new PC, a new license must be requested.

Import licenses

In order to import the licenses for the one-X Attendant, enter the following address in your browser:

https://hostname:8443/WebLM

(hostname = PC name/IP-address of WebLM server)

A logon window opens. You are automatically guided through the necessary steps.

Grace Period 1XA Client

30 days grace period: If WebLM is not installed or not reachable or !XA basis license in not existing or exoired, there is a 30 days test period while !XA Client can fully be used without license. Begin and end date of the grace period are shown after 1XA client start in system config window for license.

Grace Period SVAManager

30 days grace period: If WebLM is not installed or not reachable or 1XA busy lamp license is not existing or expired, there is a 30 days test period while SVA Manager can fully be used without license. Begin and end date of the grace period are shown in TTrace log of the SVAManager (category SVA Info).

Licenses overview

The table below shows which one-X Attendant licenses you need for using the different features.

Material	Name of license	Name of license in *.lic	Effects on one-X Attendant
228.500	ONE–X ATTENDANT CLIENT NEW USER LIC	VALUE_1XATTD_CLIENT	Basic license for new customers, this is pre–requisite for the one-X Attendant client to start *Value range*: integer ≥ 1
228.501	ONE–X ATTENDANT CLIENT UPG USER LIC	VALUE_1XATTD_CLIENT	Basic license for a Softconsole upgrade, this is pre–requisite for the one-X Attendant client to start *Value range*: integer ≥ 1
228.502	ONE–X ATTENDANT EXTL DATABASE LIC	FEAT_1XATTD_EXTERNAL_DB	Required for connecting external data sources. Only one license is required per system.
228.503	ONE–X ATTENDANT PRESENCE LIC	FEAT_1XATTD_PRESENCE	Required for the functions: - Absence from calendar, - Absence from Outlook or Notes - Web Server (basis for AIS and WebBrowser). - Presence Server connection (for busy and presence status). Only one license is required
228.504	ONE–X ATTENDANT EXTENDED BUSY LAMP LIC	FEAT_1XATTD_EXTENDED_ BUSY_LAMP	For all ways of signaling the network–wide busy states. One license per system will be needed, which monitors up to 20,000 extensions.

Installing one-X Attendant

Setup types

The following setup types are available for installation of one-X Attendant.

You must use the correct setup type based on the application.

Client

Installs one-X Attendant without database. Use this setup type for a client–server solution. Before you can install the one-X Attendant client, you must install the one-X Attendant server (database) on a suitable PC. For the one-X Attendant client you need the host name or

TCP/IP address of the one-X Attendant server as well as the name of the one-X Attendant database.

The following components are installed:

- All Client components
- JRE (Java Runtime Engine)
- iClarity IP Audio Server

Server

Use this setup type for a client–server solution. The one-X Attendant

Server must be installed before the clients.

The following components are installed:

- Database (Sybase ASA 11)
- Phone book server (JOnAS)
- MasterDirectory
- Update service
- JDK (Java Development Kit)
- WebAccess (JOnAs)
- Absence Info Pusher

Full (single–user)

Installs one-X Attendant with a local database. Use this setup type for a single–user solution, which means client and server are on the same PC.

Customized

This setup-type is only for advanced users. You can select the desired components. You must select this type if you want to install **SVA Manager** (Network–wide busy display) but do not have a single–user solution.

Prepare for installation

Close any other Windows programs (such as MS Word). **Make sure that no Adaptive Server Anywhere (ASA) database is running.** If an ASA (service) is running, close it. If you use a screen saver in Windows, deactivate it before installing **one-X Attendant**. Once the installation is complete, you can use the screen saver as you normally would.

Starting the installation

To start the installation, follow these steps.

1. Insert the one-X Attendant installation CD in your CD drive. The Overview start page opens in your standard browser.
2. Click **one-X Attendant**. An InstallShield Wizard starts up. The InstallShield Wizard dialogs are in the same language as your operating system.The **Welcome** dialog opens.
3. Click **Next**. The **License Agreement** dialog opens. Read and comply with the copyrights.
4. You must agree to the license terms to install the program. Select the correct option and click **Next**. The **Setup type** dialog opens.
5. Select the required setup-type and click **Next**. Follow the instructions on screen to continue.

Custom install

You have begun the installation with step 1 (above) and selected Custom as the setup type.

The **Select Features** dialog opens. Select the desired components.

Note:

The following procedure describes how to install all components.

2. Click **Next**. The **Edit data** dialog requests the URL for the WebLM server (license server). The address is entered by default if is set up on your PC. Use the default setting.
3. Click **Next**. The **Choose destination path** dialog opens. You can select the folder into which the corresponding client data will be copied. Only if WebLM resides on the PC you are installing the server on. Use the default setting.
4. Click **Next**. The second **Choose destination path** dialog opens. You can select the folder into which the data of the different server components will be copied. se the default setting. (The path must **not** contain any spaces.)
5. Click **Next**. The **Edit data** dialog opens. You must specify the following information for the phone book server.
   Host
   Shows the host name of the phone book server, or TCP/IP number if no DNS server is installed on the network. The default setting is the name of this computer.
   If the TCP/IP number is used be sure that the number is also used for the host in the following file of the server: <ServerDirectory>\JONAS\conf\joramAdmin.xml (3 entries)
   Port
   Indicates the port for database access to the phone book server (JOnAS). Accept the default.

6. Click **Next**. A new **Edit data** dialog opens**.** This dialog lets you set up the database connection.
   Server name
   Shows the name of the database (engine name in the ODBC settings). Accept the default. The name of the database must be unique within the network.
   Port
   Shows the port for the database-server. Accept the default.
7. Click **Next**. The **Password** dialog opens**.** The password is used to access the database. If you change the password, you must enter it twice to confirm it.
8. Click **Next**. . The choice appears if you want to connect one-X Attendant with a Presence Server or a SVA Manager.
   Choice SVA - Manager
   The **Edit data** dialog for **SVA Manager** opens. If you want to use a network–wide busy display, you must specify the following information:

Host

Enter the host name of the PC running SVA Manager.

Port

Enter the port for accessing SVA Manager.

Choice Avaya AURA Presence Server

Enter host names of Presence Server and SMGR as well as user and password of SMGR

9. Click **Next**. The **Edit data** dialog for the Web server port opens.
   Port
   Enter the port used to access the web server.
10. Click **Next**. The **Select additional languages** dialog opens. The default setting is to install all languages currently offered by one-X Attendant. Here you can select the languages which you do not wish to install. You do this by unchecking the relevant checkboxes.
11. Click Next. The Ready to install the program dialog opens.
12. Click **Install**. The installation starts. This process takes several minutes. The **Setup status** dialog indicates the progress of the installation.
13. If you wish to install an SVA Manager, the setup for the **Avaya AE Services TSAPI Client** now starts
14. After prompting for the save location, the **TCP/IP Name Server**
    Configuration dialog opens.
    Host name or IP Address:
    If you wish to display the busy states of a ACM which is located in your network, enter the name or the IP address of the AES server.
    Port:
    Enter the AES server port through which it communicates with the TSAPI client.
15. Click on the button **Add to list**.
    The application checks whether you can access the AES server.
16. Repeat steps 14 and 15 if necessary and add further existing AES
    servers to the list.
17. End the installation of the **TSAPI Client** with **Finish**.
18. After the end of the installation, SVA Manager configuration is carried out. The **QConfig tool** is launched automaticly by the setup, only the password has to be inserted by the user**.** In the log on dialog, enter the password “Recall”.
19. Click **Next**. QConfig opens the configuration user interface for the file
    SVA_Manager.xml.
    All the input and option fields which are needed for configuration of the SVA Manager are described in the section **SVA Manager Configuration**
20. Click **Save**. You will be asked if you want to restart SVA Manager.
    Click **No** as it will be started later anyway.
21. Click **Exit**. The SVA Manager installation is complete.
    Next, the InstallShield Wizard starts the following services: Avaya Phonebook Server,
    Avaya Phonebook Server – Absence Info Pusher, Avaya Phonebook Server – Update Service, .
22. The one-X Attendant Configuration Tool Collection then starts.
    Log on as the default user “Avaya” with the password “000000”. Save your values for the address parser here and test them
    All settings are described in the one-X Attendant Configuration Tool
    Collection section
23. Close the application. The last installation dialog, **InstallShield Wizard Complete**, opens. To end the installation, click **Finish**.

Installing the one-X Attendant Client setup-type

You have begun the installation and selected “Client” as the setup type.

1. Click **Next**. The **Edit data** dialog requests the URL for the WebLM server (license server). The address is entered by default if it was set up on your PC with standard paths.
2. Click **Next**. The **Choose destination path** dialog opens. You can select the folder into which the corresponding client data will be copied. Use the default setting.
3. Click **Next**. The **Edit data** dialog opens. You must specify the following information for the phone book server.
   Host
   Shows the host name of the phone book server. In this case, the host is the name or TCP/IP number if no DNS server is installed on the network. The default setting is the name of this computer.
   If the TCP/IP number is used be sure that the number is also used for the host in the following file of the server: <ServerDirectory>\JONAS\conf\joramAdmin.xml (3 entries)

   Port
   Indicates the port for database access to the phone book server (JOnAS). Accept the default.
4. Click **Next**. A new **Edit data** dialog opens**.** This dialog lets you set up the database connection.
   Server name
   Shows the name of the database (engine name in the ODBC settings). Accept the default. The name of the database must be unique within the network.
   Port
   Shows the port for the database-server. Accept the default.
5. Click **Next**. The **Password** dialog opens. Enter the password for accessing the one-X Attendant database which you set when you installed the server.
6. Click **Next**. The **Setup type** dialog opens. If you want to use the network–wide busy display, you must establish a connection to an SVA Manager. To do this, select the “Yes” option.
7. Click **Next**. The choice appears whether you want to connect one-X Attendant with a Presence Server or a SVA Manager.
   Choice SVA Manager
   The **Edit data** dialog for **SVA Manager** opens if you selected “Yes” in the previous dialog. You must make the following settings:
   Host
   Enter the host name of the computer on which the SVA Manager is running.
   Port
   Enter the port for accessing SVA Manager.
   Choice Avaya AURA Presence Server
   The parameters for the presence sever connection are only necessary during the installation of the server components.
8. Click **Next**. The **Select additional languages** dialog opens. The default setting is to install all languages currently offered by one-X Attendant. Here you can select the languages which you do not wish to install. You do this by unchecking the relevant checkboxes.
9. Click Next. The Ready to install the program dialog opens.
10. Click **Install**. The installation starts. This process takes several minutes. The **Setup status** dialog indicates the progress of the installation.
11. The last installation dialog, **InstallShield Wizard Complete**, opens. To end the installation, click **Finish**.

Note

If the client installation finds Lotus Notes (various versions) on the PC, the database name is checked on the server where the calendar function is set up. The Lotus Notes COM interface is registered as well.

Installing single–user type setup

You have begun the installation and selected single–user as the setup type. The installation is identical to the User–defined installation in which all components were selected.

Installing one-X Attendant server setup type

You have begun the installation and selected “Server” as the setup type. This installs all the server components.

1. Click **Next**. The **Edit data** dialog requests the URL for the WebLM server (license server). The address is entered by default if it was set up on your PC with standard paths. Use the default setting.
2. Click **Next**. The **Choose destination path** dialog opens. You can select the folder into which the data for the different server components will be copied. Use the default setting. (The path must **not** contain any spaces.
3. Click **Next**. The **Edit data** dialog opens. You must specify the following information for the phone book server.
   Port
   Indicates the port for database access to the phone book server (JOnAS). Accept the default. (JOnAS). Accept the default.
4. Click **Next**. A new **Edit data** dialog opens**.** This dialog lets you set up the database connection.
   Server name
   Shows the name of the database (engine name in the **ODBC settings**). Accept the default. The name of the database must be unique within the network.
   Port
   Shows the port for the database-server. Accept the default.
5. Click **Next**. The **Password** dialog opens**.** The password is used to access the database. If you change the password, you must enter it twice to confirm it.
6. Click **Next**. The **Setup type** dialog opens. If you want to use the network–wide busy display, you must install an SVA Manager. To do this, select the ”Yes” option.
7. Click **Next.** The choice appears wether you want to connect the one-X Attendant to a Presence Server or a SVA Manager.
   Choice SVA Manager
   The **Edit Data** dialog for SVA manager opens. If you want to use a network wide busy display you must enter the following data:
   Host
   Enter the host name of the PC running SVA Manager.
   Port
   Enter the port for accessing SVA Manager.
   Choice Avaya AURA Presence Server.
   Enter the host names of Presence Server and SMGR as well as user and password for SMGR.
8. Click **Next**. A new **Setup type** dialog opens. If you wish to use theMasterDirectory application, select the ”Yes” option.
9. Click **Next**. The **Edit Data** dialog for the Web server opens.
   Port
   Enter the port used to access the web server.
10. Click Next. The Ready to install the program dialog opens.
11. Click **Install**. The installation starts. This process takes several minutes. The **Setup status** dialog indicates the progress of the installation.
12. If you wish to install an SVA Manager, the setup for the **Avaya AE Services TSAPI Client** now starts.
13. After prompting for the save location, the **TCP/IP Name Server**
    Configuration dialog opens.
    Host name or IP Address:
    If you wish to display the busy states of a CM which is located in your network, enter the name or the IP address of the AES server.

Port:
Enter the AES server port through which it communicates with the TSAPI client.

14. Click on the button **Add to list**.The application checks whether you can access the AES server.
15. Repeat steps 11 and 12 if necessary and add further existing AES servers to the list.
16. End the installation of the **TSAPI Client** with **Finish**.
17. A log in dialog opens. You must log in to the **QConfig** tool**.** Enter the password “Recall”.
18. Click **Next**. QConfig opens the configuration user interface for the file SVA_Manager.xml.
    All the input needed for configuration of the SVA Manager is described in the section **SVA Manager Configuration** .
19. Click on **Save**.
20. End the configuration with **File** > **Exit**. The SVA Manager installation is now complete.
    Next, the InstallShield Wizard starts the following services: Avaya Phonebook Server,
    Avaya Phonebook Server – Absence Info Pusher,
    Avaya Phonebook Server – Update Service.
21. The one-X Attendant Configuration Tool Collection then starts.
    Log on as the default user “Avaya” with the password “000000”.
    All settings are described in the one-X Attendant Configuration Tool Collection section .Save your values for the address parser here and test them.
22. Close the application. The last installation dialog, **InstallShield Wizard Complete**, opens. To end the installation, click **Finish**.

Installing components later

If you open the setup again, you can change, repair or uninstall the program.

If you select the ”Change” option, the ”Custom” setup is entered.

UninstallYou can uninstall the **one-X Attendant** components at any time.

To uninstall **all** components, follow these steps.

1. In Control Panel, click Add or Remove Programs.
2. Click Avaya one-X Attendant.
3. Click **Remove**.
4. Select **Remove** and then click **Next**. After another prompt one-X Attendant will be uninstalled from your PC.

Note:

It is not possible to remove one-X Attendant components individually.

Additional components

Network–wide busy display (SVA Manager)

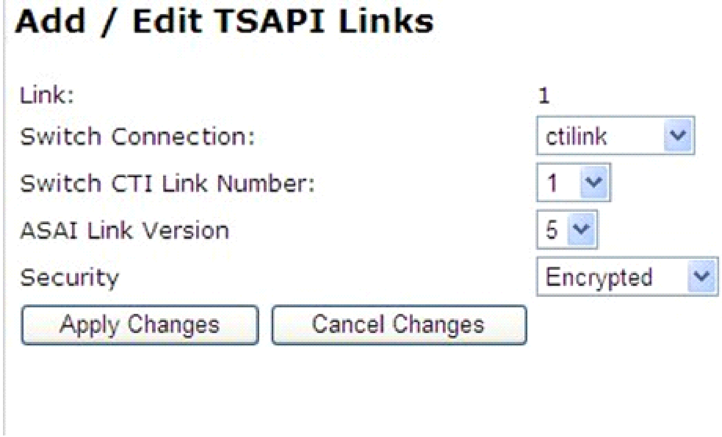
About SVA Manager
General information about SVA Manager is provided in the sections about the various one-X Attendant components.

Prerequisites for installation

You must have licenses to use the network–wide busy display.
FEAT_1XATTD_EXTENDED_BUSY_LAMP

AES Configuration:

An AES with version 4.2.1 or higher ist requested and the TSAPI Link has to be configured like this:



Add / Edit TSAPI Links

Link:	1
Switch Connection:	ctilink
Switch CTI Link Number:	1
ASAI Link Version	5
Security	Encrypted

CTI\OAM\Administration\Administration\CTI Link Admin\TSAPI Links\Add/Edit TSAPI–Links

Switch Connection: Select a Switch Connection name from the list of administered connection names.

Switch CTI Link Number: Select a CTI link number from 1 to 64. Select a number that corresponds to an appropriate CTI link number on Communication Manager. By default this field is blank.

ASAI Link Version: Use Link Version 5

Security: Select ’Encrypted’ (if you use only SVAManager) or ’Both’ (if your organization uses multiple TSAPI applications, some applications can be set up with secure links and others can be set up with nonsecure links).

[config]

If your using Telephony Services via a secure, encrypted connection the AES server sends its certificate to the TSAPIU client and the TSAPI client verifies that the certificate is signed by a trusted Certificate Authority (CA).

If your Organisation has installed its own certificate on the AE Server, then the TSAPI client must have access to the trusted CA certificate(s) for the AE Services server certificate. Provide the location of a file containing the trusted CA certificate(s) here. For example: “Trusted CA File=c:\certificates\verisign.cer”

Installation

The installation can also be carried out together with the one-X Attendant server installation

The following describes a subsequent installation, which involves using a separate setup, which you can open from the Custom setup.

The setup includes the installation of SVA Manager as a service and of the TAPI Framework.

You have begun the installation and selected Custom as the setup type.

1. The **Select Features** dialog opens. Select the check box SVA Manager”. Remove the check marks from all the other check boxes.
2. Click **Next**. The **Edit data** dialog requests the URL for the WebLM server (license server). The adress is entered by default if it was set up on your PC with standard paths. Use the default setting.
3. Click **Next**. The **Choose destination path** dialog opens. You can select the folder into which the ata for the different server components will be copied. Use the default setting. (The path must **not c**ontain any spaces.)
4. Click Next. The Ready to install the program dialog opens.
5. Click **Install**. The installation starts. The **Setup status** dialog indicates the progress of the installation.
6. After the installation finishes the Login dialog for the SVA Manager’s **QConfig** configuration tool pens. The default password is “Recall”. The table on the following page shows the relevant settings.
7. Click Exit. The SVA Manager installation is complete and the service will be started.

Configuration using QConfig

When you start SVA Manager, the configuration is imported from the xml file SVA_Manager.xml.

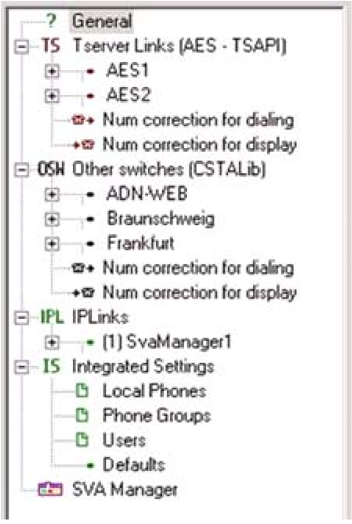
The file is in the SVA Manager directory.

To make editing configuration parameters in the xml file easier, a configuration tool (**QConfig**) is installed along with SVA Manager.

Start program

Start the program using the Start menu: **Start > Programs > Avaya > SVAManager Config**. Enter “Recall” as the password.

Program window



```
? General
TS Tserver Links (AES - TSAPI)
    AES1
    AES2
    Num correction for dialing
    Num correction for display
OSW Other switches (CSTALib)
    ADN-WEB
    Braunschweig
    Frankfurt
    Num correction for dialing
    Num correction for display
IPL IPLinks
    (1) SvaManager1
IS Integrated Settings
    Local Phones
    Phone Groups
    Users
    Defaults
SVA Manager
```

The program window is split in a tree view on the left and a work area on the right.

The tree view allows you to select settings for various tasks. The possible settings for the topic marked in blue are sown in the work area.

The settings for SVA Manager have to be made under the various topic areas.

The following table lists all the settings necessary for configuration of a SVA Manager to an Avaya Communication Manager. Further information on all the settings which can be made using **QConfig** is provided in reference /3/.

Note:

For security reasons, please change the login password immediately after the first start of **QConfig**. The change is made in the topic **General > Config Protection > Password > Set ...**

Topic, Data entry	Setting	Meaning
TS		List with AES servers and your system settings relevant to one-X Attendant. New AES servers can be connected using the **New** button.
<AES server>	Primary Server ID	“Scan” polls all possible AES inputs. Select the ones you require.
	Login: Username, Password	User and password (1024 Bit RSA encryption) for system access
	Public network location: Country code, Gateway location: - Area code, - Prefix, - Max. length of internal numbers	Settings as under **OSW** (see below).
	Dialing rules	According to the ACM settings / local factors
CTI specials	System monitors: Add ..., Edit ...: Ext./From, To	Here you give in which stations you want to monitor. Settings as under **OSW** (see below).
TSLib.ini	Host, Port	Address and port of the connected AES servers; use **Add** to add new ones
Miscelaneuos	Max. number of simultaneous monitor	Throttling of simultaneous monitor starts (Default 10), see also notes on operation.
OSW		List of telephone systems and the corresponding one-X Attendant system settings
<Telephone system>	Manufacturer	Manufacturer
	Type	System type
	Login: Username, Password	User and password (1024 Bit RSA encryption) for system access
	Link(s): Add ..., Edit ...: Host, Port	Network name or IP address of the system board and the port enabled there.

Topic, Data entry	Setting	Meaning
	Public network location: Country code, Gateway location: - Area code, - Prefix, - Max. length of internal numbers	Configuration of the trunk lines for the PBX. Use **Add** **...** to add more if required. Maximum length of internal numbers. Longer numbers will be regarded as external numbers.
CTI specials	System monitors: Add ..., Edit ...: Ext./From, To	Number or number range to be shown in the network–wide busy display. Operator sets *and* agent numbers need to be entered.
IPL		
OSPC Link	Port, Gateway	Port of SVAManager for the QTAPI functionality (Default = 10405), to which the operator sets are connected. .
CTI specials	Auto-transfer on hangup	Select, if one-X Attendant should directly initiate an outgoing call without the operator picking up the handset.
IS		
	Search local phones by the host	Select which entry type you wish to use for assigning one-X Attendant client PCs to operator sets.
Local phones	Add ..., Edit ...: Hostname, Extension	Host name for the one-X Attendant PC and if Telecommuter Mode is switched on, number of the associated operator set.
SVA Manager		
	port number	Port of SVAManager for the Extended Busy Lamp functionality (Default = 10405)6
	data file	File in which the SVA Manager saves data. Default: SVAManager.dat
	Enable Call list and Redial list	Not applicable for operation on ACM.
	TTrace Server	Host IP and Port

Notes:

If the network–wide display does not correctly distinguish between internal and external calls, this may be due to an incorrect setting in “Max. length of internal numbers”.

For changes to take effect, you must restart the service.

Notes on operation

Maximum Values of supported SVA Manager Configurations

- Tserver Links: 20
- Monitorpoints: 10000

If you have more than 1500 monitor points in the extended busy lamp field, the environment variables MAXMESSAGESIZE and MAXBUFFERSIZE has to be inserted/set to a value of ‘50 times <number of monitor points>’.

SVA Manager should have completely finished its startup routine before you start one-X Attendant.

If SVA Manager is not ready for operation during login, an error button opens. When logged in, this is shown by an icon labeled SVA:

- A red icon indicates that there is no connection to SVA Manager
- A yellow icon indicates that SVA Manager is not yet ready for operation

The network–wide busy display only functions correctly when SVA Manager is not just running but also when it is ready to operate, i.e. all monitor points are licensed and initialized.

Because overload in AES can lead to complete failure of cti, the usage of a throttle for simultaneous monitor starts was necessary. This throttle was generalized, so it could be used for integral enterprise. Because of that overload in that case could be eliminated two.

The procedure works as follows: For every system all monitor start and monitor stop reqeuest will be written in a cache. One thread for every system gets a configurable maximum number of actions out of the cache and completes them. The default value of this maximum is 10. The value can be changed with the configuration tool under – Tserver Links – Miscellaneous – 04.03– respectively – Other switches – Miscellaneous –04.03 –.

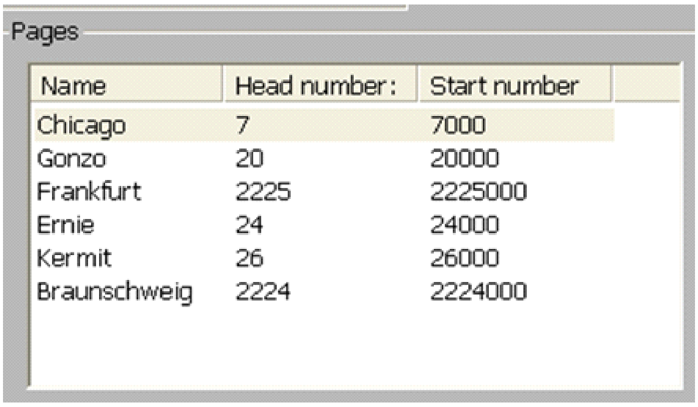
Every time a action is finished the next will be started. When CTI–server gets a monitor stop request for one action, that is still in the cache, it will be eliminated from cache.

Additional note for configuration

With „head number“ and „start number“ you can configure a special sort when pressing the „Load“ button an putting numbers received by SVAManager in net wide busy view.

Head number is the number all numbers of specified page start with.
Start number is lowest possible number of this page.

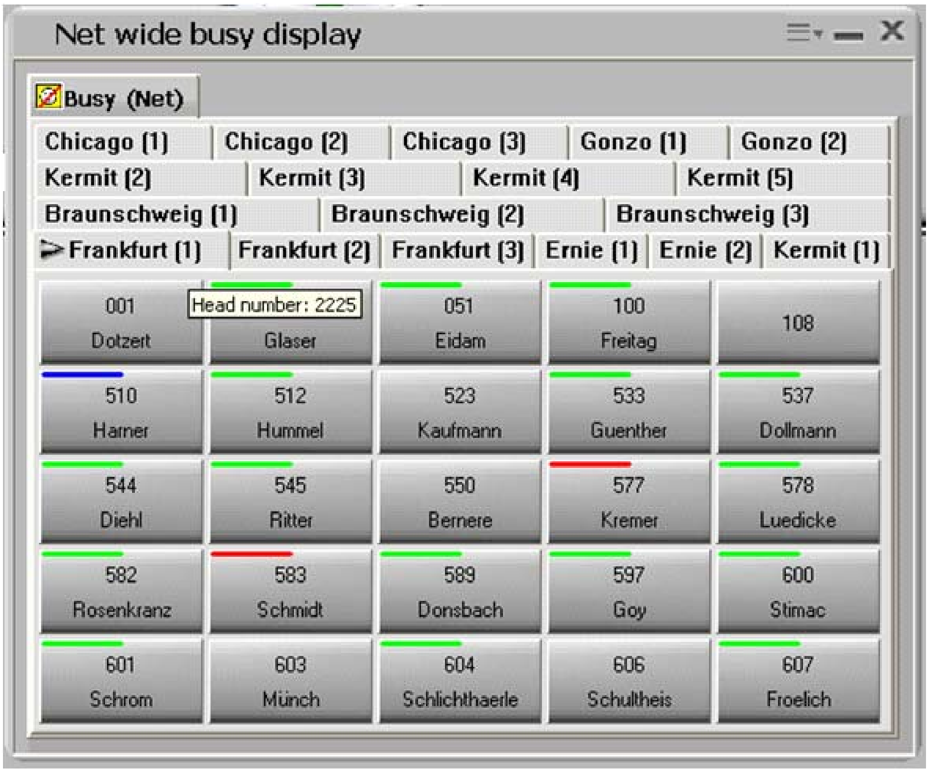
Example:



Pages

Name	Head number:	Start number
Chicago	7	7000
Gonzo	20	20000
Frankfurt	2225	2225000
Ernie	24	24000
Kermit	26	26000
Braunschweig	2224	2224000

No when pressing the load button we get the following net wide busy view later:



Net wide busy display

Busy (Net)

Chicago (1) | Chicago (2) | Chicago (3) | Gonzo (1) | Gonzo (2)
Kermit (2) | Kermit (3) | Kermit (4) | Kermit (5)
Braunschweig (1) | Braunschweig (2) | Braunschweig (3)
Frankfurt (1) | Frankfurt (2) | Frankfurt (3) | Ernie (1) | Ernie (2) | Kermit (1)

001 Dotzert	Head number: 2225 Glaser	051 Eidam	100 Freitag	108
510 Hamer	512 Hummel	523 Kaufmann	533 Guenther	537 Dollmann
544 Diehl	545 Ritter	550 Bernere	577 Kremer	578 Luedicke
582 Rosenkranz	583 Schmidt	589 Donsbach	597 Goy	600 Stimac
601 Schrom	603 Münch	604 Schlichthaerle	606 Schultheis	607 Froelich

Notice: Head number is not displayed in number buttons of net wide busy view. It is only displayed in tooltip of page or page name (if you configure it).

System Requirements Presence Server

Version

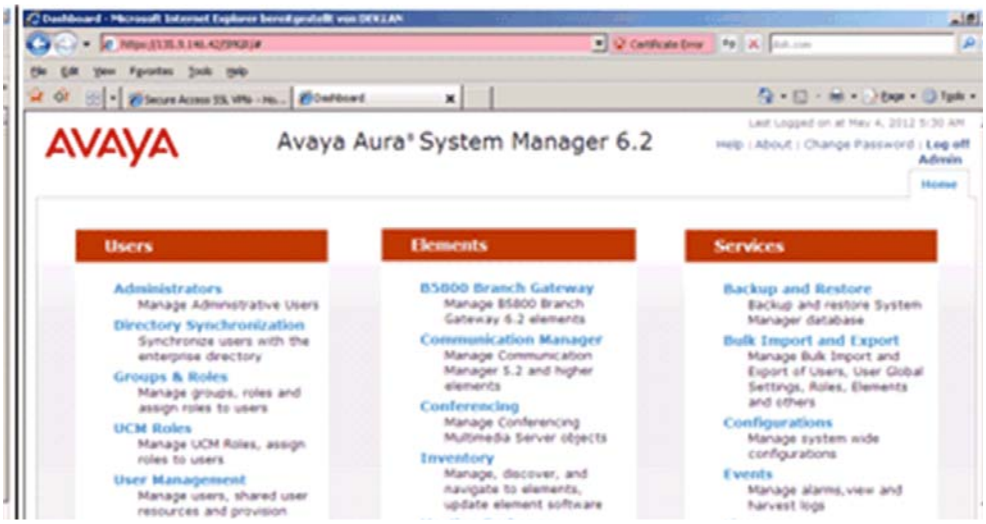
Aura 6.2 including

- CM 6.2
- SM 6.2
- Presence Server 6.1
- AES 4.2.1 or higher
- SMGR 6.2.

How to check the version of SMGR

1. Check if SMGR is up and running:

Log on to SMGR web console. The SMGR is running, if you can see the SMGR dashboard



Dashboard - Microsoft Internet Explorer bereitgestellt von DEKLAN
Certificate Error
File Edit View Favorites Tools Help
Secure Access SSL VPN - Ho...
Dashboard
Page
Tools
AVAYA
Last Logged on at Mai 4, 2012 5:30 AM
Help | About | Change Password | Log off Admin
Home

Avaya Aura® System Manager 6.2

Users

Administrators
Manage Administrative Users

Directory Synchronization
Synchronize users with the enterprise directory

Groups & Roles
Manage groups, roles and assign roles to users

UCM Roles
Manage UCM Roles, assign roles to users

User Management
Manage users, shared user resources and provision

Elements

B5800 Branch Gateway
Manage B5800 Branch Gateway 6.2 elements

Communication Manager
Manage Communication Manager 5.2 and higher elements

Conferencing
Manage Conferencing Multimedia Server objects

Inventory
Manage, discover, and navigate to elements, update element software

Services

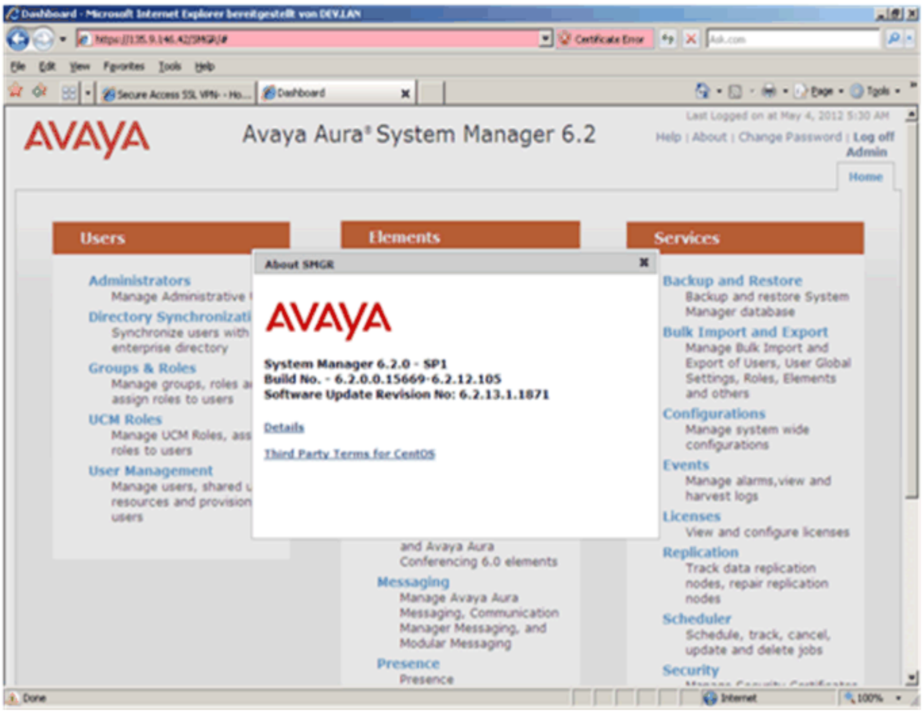
Backup and Restore
Backup and restore System Manager database

Bulk Import and Export
Manage Bulk Import and Export of Users, User Global Settings, Roles, Elements and others

Configurations
Manage system wide configurations

Events
Manage alarms,view and harvest logs

2. Check the SMGR Version



About SMGR

System Manager 6.2.0 - SP1
Build No. - 6.2.0.0.15669-6.2.12.105
Software Update Revision No: 6.2.13.1.1871

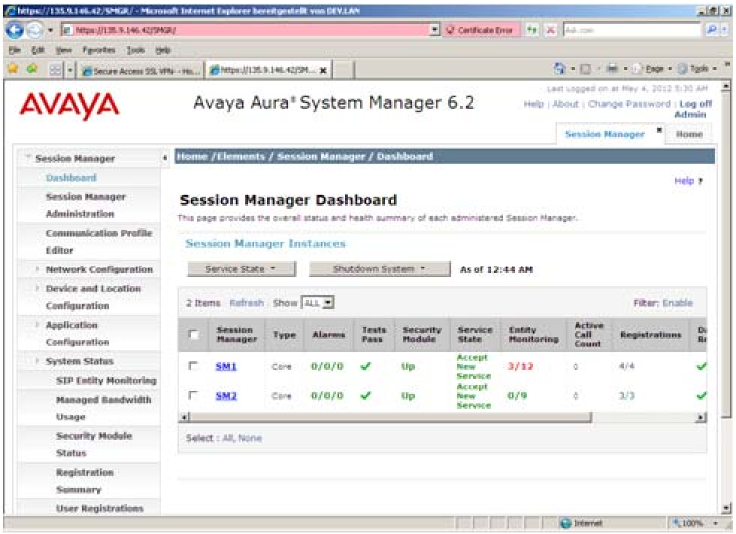
Details

Third Party Terms for CentOS

Log on to SMGR web console. Click **About** to get SMGR release information.

Check whether Session Manager is up and running

Log on to SMGR web console and select menu **Elements/Session Manager/Dashboard**



Home /Elements / Session Manager / Dashboard

Session Manager Dashboard

This page provides the overall status and health summary of each administered Session Manager.

Session Manager Instances

Service State ▾ Shutdown System ▾ As of 12:44 AM

2 Items Refresh Show ALL Filter: Enable

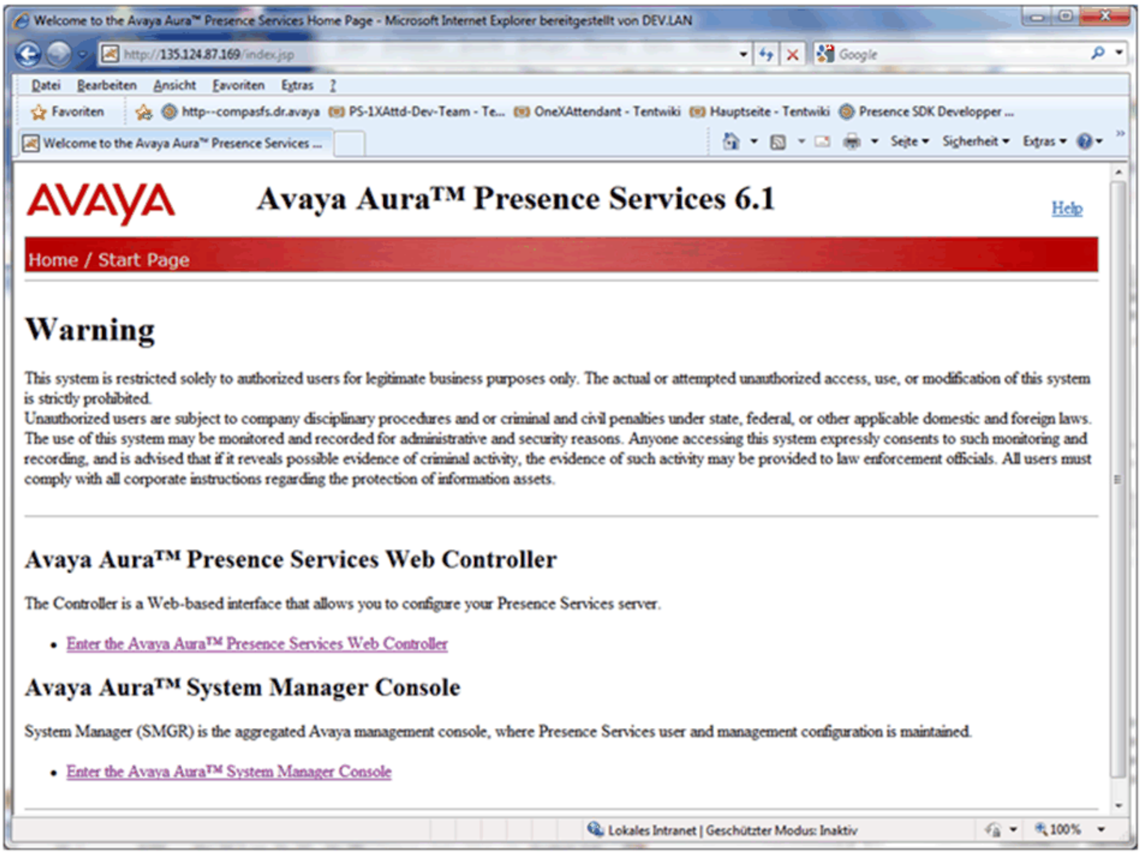
□	Session Manager	Type	Alarms	Tests Pass	Security Module	Service State	Entity Monitoring	Active Call Count	Registrations	D B
□	SM1	Core	0/0/0	✓	Up	Accept New Service	3/12	0	4/4	✓
□	SM2	Core	0/0/0	✓	Up	Accept New Service	0/9	0	3/3	✓

Select : All, None

Start of PS XCP Controller

To configure the Presence XCP server the Presence XCP controller is available. It is a web-based administration console and from its main page you can access information on the server's core router and on all the plug-ins and components running on the server. You can start and stop the server and its components from this location and also view a XML summary of your server configuration.

Log in to Presence Services XCP Controller Web interface using your Presence Services servers host name, it is automatically converted to the servers IP address.



Welcome to the Avaya Aura™ Presence Services Home Page - Microsoft Internet Explorer bereitgestellt von DEV.LAN
http://135.124.87.169/index.jsp
Google
Datei Bearbeiten Ansicht Favoriten Extras ?
Favoriten
http--compasfs.dr.avaya
PS-1XAttd-Dev-Team - Te...
OneXAttendant - Tentwiki
Hauptseite - Tentwiki
Presence SDK Developper ...
Welcome to the Avaya Aura™ Presence Services ...
Seite Sicherheit Extras
AVAYA
Help
Lokales Intranet | Geschützter Modus: Inaktiv
100%

Avaya Aura™ Presence Services 6.1

Home / Start Page

Warning

This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited.
Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws. The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials. All users must comply with all corporate instructions regarding the protection of information assets.

Avaya Aura™ Presence Services Web Controller

The Controller is a Web-based interface that allows you to configure your Presence Services server.

- Enter the Avaya Aura™ Presence Services Web Controller

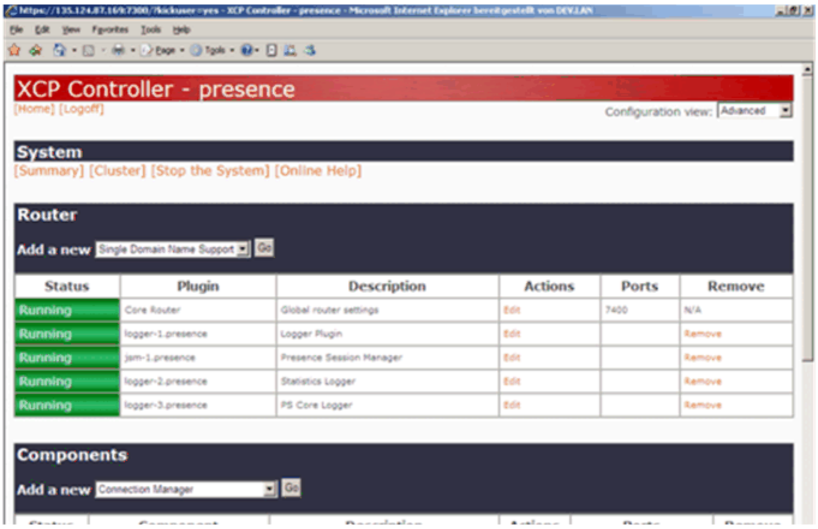
Avaya Aura™ System Manager Console

System Manager (SMGR) is the aggregated Avaya management console, where Presence Services user and management configuration is maintained.

- Enter the Avaya Aura™ System Manager Console

Choose Enter the Avaya Aura™ Presence Services Web Controller (IP-adress is a example): https://135.124.87.169/admin

Top right select **Advanced** in drop down box **Configuration View**.



XCP Controller - presence

[Home] [Logoff]

Configuration view: Advanced

System

[Summary] [Cluster] [Stop the System] [Online Help]

Router

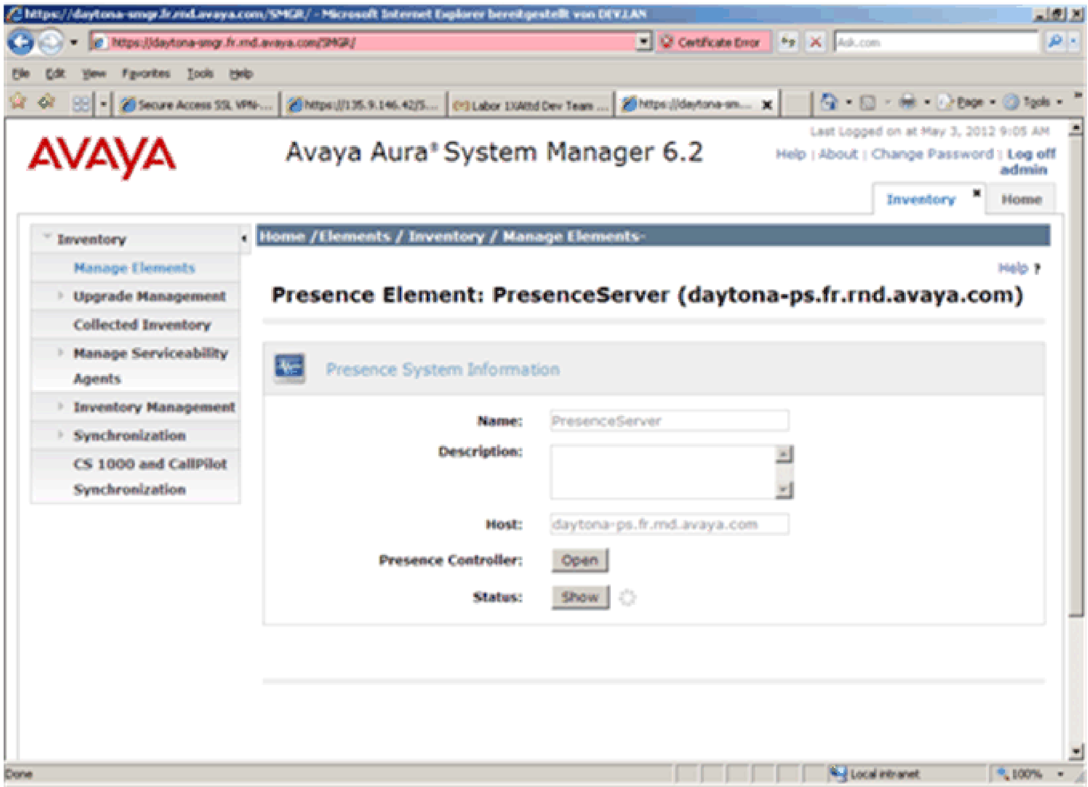
Add a new Single Domain Name Support Go

Status	Plugin	Description	Actions	Ports	Remove
Running	Core Router	Global router settings	Edit	7400	N/A
Running	logger-1.presence	Logger Plugin	Edit		Remove
Running	jsm-1.presence	Presence Session Manager	Edit		Remove
Running	logger-2.presence	Statistics Logger	Edit		Remove
Running	logger-3.presence	PS Core Logger	Edit		Remove

Components

Add a new Connection Manager Go

The Presence Services XCP controller can also be launched from SMGR web console:
select menu **Elements/Inventory/Manage Elements** and click on configured Presence Services:



Avaya Aura® System Manager 6.2

Last Logged on at May 3, 2012 9:05 AM

Home / Elements / Inventory / Manage Elements

Presence Element: PresenceServer (daytona-ps.fr.rnd.avaya.com)

Presence System Information

Name: PresenceServer

Description:

Host: daytona-ps.fr.rnd.avaya.com

Presence Controller: Open

Status: Show

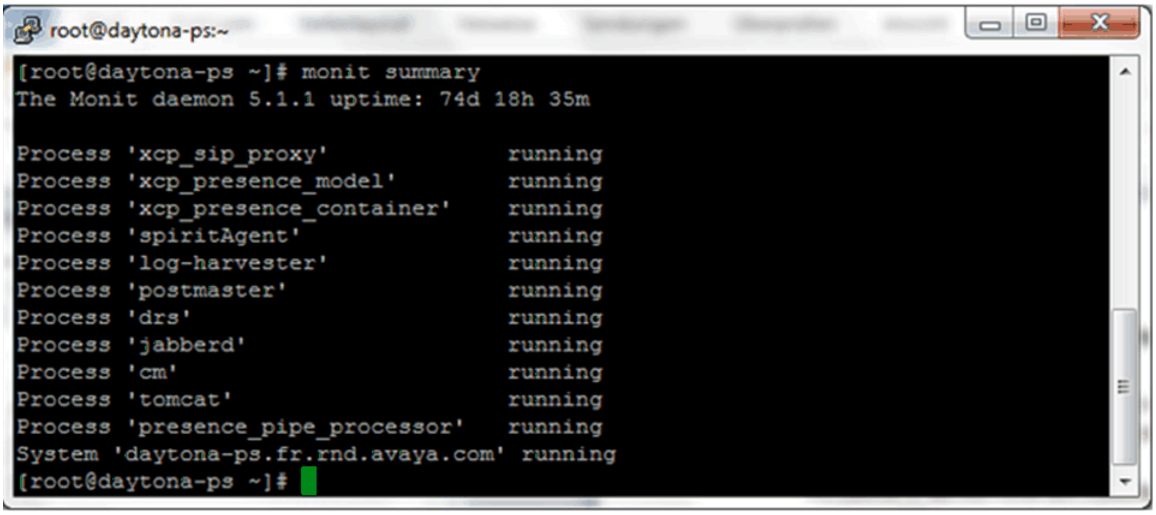
Check whether PS is up and running

Although it is offered by XCP controller to check if the services are running or to restart them. But it is not recommended to use the XCP controller for this because the restart often does not work in this way.

To check if all services are running log in to PS as ROOT user and execute the following command:

```
monit summary
```

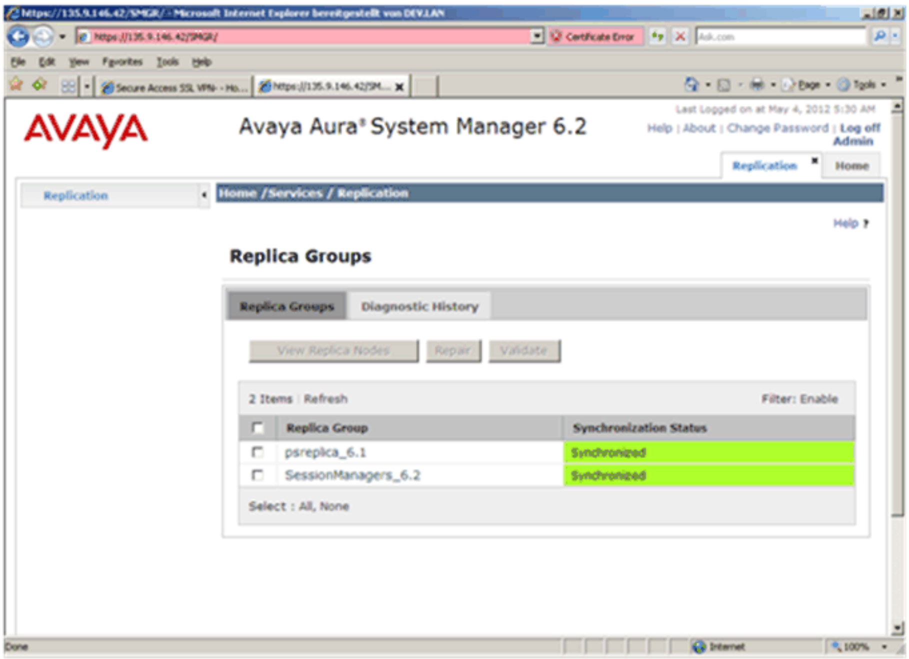
If all services show "running" the start of PS has finished successfully. Otherwise restart the PS as described in chapter Restart PS.



```
[root@daytona-ps ~]# monit summary
The Monit daemon 5.1.1 uptime: 74d 18h 35m

Process 'xcp_sip_proxy'               running
Process 'xcp_presence_model'          running
Process 'xcp_presence_container'      running
Process 'spiritAgent'                 running
Process 'log-harvester'               running
Process 'postmaster'                  running
Process 'drs'                         running
Process 'jabberd'                     running
Process 'cm'                          running
Process 'tomcat'                      running
Process 'presence_pipe_processor'     running
System 'daytona-ps.fr.rnd.avaya.com'  running
[root@daytona-ps ~]#
```

Check whether PS is synchronized

Log on to SMGR web console and select menu **Services/Replication/Replica Groups**.
The replica group **psreplica_6.1** has to show green-colored status **Synchronized**



https://135.9.146.42/SMGR/ - Microsoft Internet Explorer bereitgestellt von DEV.LAN
https://135.9.146.42/SMGR/
Certificate Error
Ask.com
File Edit View Favorites Tools Help
Secure Access SSL VPN - Ho...
https://135.9.146.42/SM...
Page Tools
AVAYA
Avaya Aura® System Manager 6.2
Last Logged on at May 4, 2012 5:30 AM
Help | About | Change Password | Log off Admin
Replication
Home
Replication
Home /Services / Replication
Help ?

Replica Groups

Replica Groups
Diagnostic History
View Replica Nodes
Repair
Validate
2 Items | Refresh
Filter: Enable

□	Replica Group	Synchronization Status
□	psreplica_6.1	Synchronized
□	SessionManagers_6.2	Synchronized

Select : All, None
Done
Internet
100%

Check the PS release information

IMPORTANT: the System Platform hosting Presence Services NEITHER shows the correct PS version NOR any detailed PS release information.

The PS release information has to be checked on PS server itself on command-line level, therefore connect to PS using PuTTY:

Enter user name:	craft
Enter password:	********

Then switch to **root** user:

Execute command:	su root
Enter root password:	*********

The PS release information can be retrieved as follows:

Execute command: `/opt/Avaya/Presence/presence/bin/swversion.sh`

Postgres database

The database of PS (Presence Services) is shared because one-X Attendant does not have data replication with SMGR. So it is necessary to allow the access to the postgres database of PS.

Therefore add the IP address (example) of one-X Attendant server (here 135.124.73.25) as following:

- Log in as user ROOT to PS using Putty 135.124.70)
- **cd /var/lib/pgsql/data**
- **vi pg_hba.conf**
  The entry must look like the following:
  host all all 135.124.73.25/32 trust (allows access of 135.124.73.25)
- host all all 135.124.73.0/24 trust (allows access of all addresses beginning with 135.124.73)

Modify listen address of PS database

- **cd /var/lib/pgsql/data**
- **vi postgresql.conf**
  Assign listen address as following:
  listen_addresses = '*' # what IP address(es) to listen on;
- restart database:
  /etc/rc.d/init.d/postgresql restart

PS Connection

The connection between LPS and PS is protected by TLS, therefore mutual trust is required between LPS and PS. To build up this SSL connection the PS certificate and the SMGR certificate must be added as trusted entries to the LPS keystore of one-X Attendant and the LPS certificate must be added as trusted entry to PS keystore. Because the Data Replication Service of the SMGR uses the same keystore as Presence Server, the one-X Attendant certificate only needs to be entered in the PS keystore.

One-X Attendant keystore (here 1XAttd.keystore) and certificate (here 1XAttd.pem) are existing after installation of one- X Attendant on one-X Attendant server (c:\Avaya\Servers).

Requirements

On the PC the one-X Attendant server is installed, the following tools must be available:

- Winscp
- Putty
- Keytool (available in folder c:\Avaya\Servers\JDK\jre\bin of one-X Attendant server)
- Openssl (available in folder c:\Avaya\Servers of one-X Attedant server)

Add one-X Attendant certificate to PS keystore

- Copy 1XAttd.pem from oneXAttendant-Server (c:\Avaya\Servers) with WINSCP to PS folder /home/craft
- Login to PS with Putty as ROOT user
- Change to /opt/Avaya/Presence/jabber/xcp/certs:
  cd /opt/Avaya/Presence/jabber/xcp/certs
  Move 1XAttd.pem from /home/craft to /opt/Avaya/Presence/jabber/xcp/certs:
  mv /home/craft/1XAttd.pem
- Add certificate to JKS keystore of PS:
  /opt/Avaya/Presence/presence/bin/./prescert addTrusted pem 1XAttd.pem alias 1xa
  (Undo of import is possible with:
  /opt/Avaya/Presence/presence/bin/./prescert delete alias 1xa)
- After import of certificate into PS keystore the PS must be restarted:
  /opt/Avaya/Presence/presence/bin/./stop.sh
  /start.sh

Note:

In some cases, the "-" (hyphen) is not copied correctly into the DOS Windows when dealing w/ Keytool commands, so if you get an error message like

```
keytool error: java.lang.RuntimeException:
Usage error, ûimport is not a legal command
```

please check syntax of copied command, then delete wrong copied char "û" and replace it manually by "-" (hypen) char.

Please establish PuTTY session to PS server using craft as username, then switch user to root (as described in chapter PS release information).

Please establish WinSCP session to PS server using craft as username

Add PS certificate to One-X Attendant keystore

The certificates of PS are located in /opt/Avaya/Presence/jabber/xcp/certs.

- **cd /opt/Avaya/Presence/jabber/xcp/certs**
- Convert export-xxx.pem from PEM format to DER format:
  openssl x509 -in export-xxx.pem -inform pem -out export-xxx.cer -outform der
- Move PS certificate to /home/craft:
  mv export-xxx.cer /home/craft/export-xxx.cer
- Copy export-xxx.cer via WINSCP to one-X Atttendant server (c:\Avaya\Servers)
- Go to one-X Attendant server, open DOS window:
  cd c:\Avaya\Servers
- Import PS certificate in one-X Attendant keystore:
  keytool -import -alias ipskey -file export-xxx.cer -keypass oneXAtt -keystore 1XAttd.keystore
  Password: oneXAtt
  Trust: Yes

Add SMGR certificate to one-X Attendant keystore

For Data Replication and UPM Services it is necessary to enter the SMGR certificate into the LPS (one-X Attendant) keystore, too.

- Open SMGR Web ConsoleUnder CA Functions select Download pem file and save the certificate to a file.
- Navigate to Services > Security > Certificates > Authority.
- Under CA Functions select **Download pem file** and save the certificate to a file:
  Filename: default.cacert.jks
  Directory: c:\Avaya\Servers
- Convert SMGR certificate from PEM to DER format:
  cd c:\Avaya\Servers
  pathToOpenSSL…/openssl x509 -in default.cacert.pem -inform pem -out default.cacert.cer -outform der
- Import SMGR certificate in one-X Attendant keystore
  keytool -import -alias SMGR_key -file default.cacert.cer -keypass oneXAtt -keystore 1XAttd.keystore
- Password: oneXAtt
- Trust: Yes

Helpful commands around keystores and certificates:

- Conversion from PEM format to text:
  Openssl x509 –in filename.pem –text –out filename.txt
- View keystore:
  Keytool –list .keystore keystorename
- Remove keystore entry:
  Keytool –delete –alias aliasname –keystore keystorename
- Export certificate from keystore:
  Keytool –export –frc –alias aliasname –file filename.cer –keystore filename.keystore –storepass password

Limitations

SVAManager and Avaya AURA Presence Server can’t be used together in the one-X Attendant.

Absence Info Server (AIS)

The one-X Attendant Absence Info Server is a separate program for monitoring the out–of–office (OOF) status of all mailboxes of an exchange server (out–of–office reply in Microsoft Outlook enabled). It works with the Exchange Versions 2007, 2010.

The absence display for **one-X Attendant** is updated regularly (using the web server).

Requirements

An outlook client has to be available on the PC

You must have FEAT_1XATTD_PRESENCE licenses to use the absence notice.

Preparations on Exchange

A user is identified between one-X Attendant and Exchange by the email address. This email address can be made available to one-X Attendant in its own database or in a connected customer database. Each record used must contain both the email address **and** the number.

- General preparations on Exchange:

Absence Info-Server (AIS) generates its own Mapi-profile and establishes a Mapi-connection if one has not been established (for example, on PCs that are not part of a domain). The rights of the local user running the service apply to the Mapi-connection. This user must be set up on the Exchange Server. Notes on setting up Exchange can be found in this manual.

Preparations for Exchange Server 2010 (Exchange 2007 Server)

A user (for example "OOFReply") (with a mailbox and Windows account) must be set up on the Exchange Server. Use "Delegate Control..." at the top Exchange Server level ("First Organization (Exchange)") to assign the user the following function: "Exchange Administrator – View Only" at the organizational level (so the user has read rights for all mailboxes). The rights must then be inherited to the lower levels.

To view the individual rights, go to "Administrative Groups/First Administrative Group/Servers/<Your Exchange-Server> Properties" and go to the Security tab.

- Setting up local users

On the PC where you want to install Absence Info Server, you must set up a local user (for example, with the name "OOFReply"). The user must have the mailbox set up on Exchange Server (for example "OOFReply"). In other words, the user must have the same name and password.
The user must have the local right to start services (Administrative Tools > Local Security Settings > Local Policies > User Rights Assignment > Log on as a service).

The user does not need administrator rights for the system. The user only needs to be a member of the users group.

For AIS to work, an Outlook client must be installed on this PC and configured for this user with a connection to Exchange.

Installation

The installation program installs AIS as an NT service. You are prompted to enter all necessary parameters. Before the installation is complete, AIS starts in configuration mode. This lets you change or set the parameters

you entered and other parameters.

You can start the AIS service from the **AIS Config User Interface (UI)** .

Or you must start the service using Computer Management/Services or by restarting the PC. The installation does not start the service.

Parameters that are required during installation:

1. Installation path
   Use the default path or specify a path.
2. Local User
   These parameters define the local Windows user under which you want the service to run. These settings can be changed later under Computer Management/Services/Log on.
3. Connection parameters to Exchange Server
   These parameters define which mailbox you wish to use to authenticate to
   Exchange Server.
   You can change these parameters using the AIS Config UI.
   Example:
   Server: exchange; User: OOFReply; Domain: AVAYA; Password: *****
4. Connection parameters for one-X Attendant Web Server
   These parameters define the connection to the one-X Attendant Web server.
   Example:
   host: one-X Attendant_Server; port: 21080
5. Connection parameters for the TTrace server (optional component)
   These parameters define the connection to the TTrace server. You can change them using the AIS Config UI.
   Example:host: localhost; port: 10300

   The AIS Config UI is started automatically at the end of the installation.

AIS Config UI

You can use the **AIS Config UI** to set all connection parameters, set additional options, select mailboxes, and start and stop the service.

Start the AIS Config UI using a shortcut in the Start menu or on the desktop.

Main dialog:	**Button**	
	Connection opens	the Connection dialog
	Option	Opens the Options dialog
	Selection	Opens the Selections dialog
	Stop	Stops the service
	Start	Starts the service
	Refresh (icon) Quit	Determines the current status of the service
	Quit	Ends the AIS Config UI

Connection:	Group	Function
	Exchange Server	Here you can adjust the connection parameters forExchange Server.The Check button tests the connection to the server The result is displayed in a dialog box and output via TTrace. You must restart the service and Config UI for changes to the settings to take effect.
	Web server	Here you can adjust the connection parameters to the web server. The **Check** button tests the connection to the web server. The result is displayed in a dialog box and output via TTrace. You must restart the service and Config UI for changes to the settings to take effect.
	TTrace	The level defines the outputs that are generated in addition to the general Information. The options are: *Error*: Information messages and errors are output. *Warning*: Information messages, errors and warnings are output. *Debug*: Information messages, errors, warnings and detailed troubleshooting messages are output. The default setting is Warning. These settings take effect as soon as you click OK.

Options:	Option	Effect
	Poll interval	Specifies the minimum time there must be between the starts of two polling cycles. Default: 14400 seconds (240 minutes). If a cycle lasts longer than the set polling time, the next cycle starts 30 seconds after the previous cycle.
	Delay	Waiting time in milliseconds after an individual mailbox has been processed. Default: 0.

Effect Selection:	Button	Function
	Select	Selects the checked mailboxes for processing using AIS.The selection is saved in the **AbsenceInfoServer.sel** file. The file is located in the same directory as **AbsenceInfoServer.exe**.
	Deselect	Clears a selection
	Select all	Selects all listed mailboxes for processing using AIS
	Deselect all	Clears the selection for all mailboxes
	Select all (dynamic)	The complete list of mailboxes are prompted from the server in each update cycle and compared with the list of actual selected. If the option is set, all mailboxes are set processed automatically. If the option isn't set, only the selected and newly found mailboxes are processed.

Entries in the Windows Registry

Various entries are written to the Registry during installation. TTrace entries are located under the key

HKEY_LOCAL_MACHINE\Software\avaya\AIS

The remaining entries are located under the key
HKEY_LOCAL_MACHINE\System\CurrentContolSet\Services\AbsenceIN foServer\Parameters

Note on absence display

In the one-X Attendant, an absence notice is only displayed for a subscriber.

The subscriber is also listed as absent in Outlook.

Calendar information

You can use Microsoft Outlook or Lotus Notes to query calendar information (although you can only use one or the other at a time).
one-X Attendants busy display, network–wide busy display or phone book then shows the relevant information for all subscribers.

If neither Outlook nor Notes integration is used, it is strongly recommended to deactivate the "calendar usage" option in the Config Tool (item one-X Attendant).

Requirements

The user of the client computer must have access rights to the calendar data of all subscribers.

You must have FEAT_1XATTD_PRESENCE licenses to use the calendar information.

Exchange Server

The user of the client computer must have access rights to the calendar data of all subscribers.

You must have FEAT_1XATTD_PRESENCE licenses to use the calendar information.

If Outlook is installed on the same PC as the One-X Attendant client, please ensure that the Outlook client is always up and running otherwise the One-X Attendant client could stop running. Also the

Exchange cache should not be turned off for the Outlook client

Configuration 1:

- The autodiscover functionality for the outlook client has to be configured. This can be tested in this way:
  While Outlook 2007 is running, hold down the CTRL key, right-click the Outlook icon in the notification area, and then select **Test E-mail AutoConfiguration**.
  Verify that the correct e-mail address is in the box next to **E-mail Address**.
  Clear the check boxes next to **Use Guessmart** and **Secure Guessmart Authentication**.
  On the **Test E-mail AutoConfiguration page**, verify that the check box next to **Use AutoDiscover** is selected, and then click the **Test** button.
- The SMTP Addresses of the users in the address book has to belong to the same domain as the exchange server. The following request should return an xml file with an “autodiscover” "element within:
  https://<SMTP address domain>/autodiscover/autodiscover.xml.
- For further information's please look here: http://technet.microsoft.com/en-us/library/bb124251.aspx

Configuration 2:

- The exchange server has to be configured to use public folders for free/busy (as it works with outlook 2003). In Exchange 2003 this was the default configuration.
- For further information's please look here:
  http://blogs.technet.com/b/exchange/archive/2010/04/23/3409853.aspx
  http://technet.microsoft.com/en-us/library/bb397221.aspx
  http://technet.microsoft.com/en-us/library/bb124411.aspx

If you have problems you can also use the RedemptionTestTool or the VisualBasic Test SourceCode which you can find on CD in the folder: software\Service-Tools\RedTest

Installation

No installation is required. The calendar information is automatically available with the client installation.

WebAccess

Note
WebAccess is not relevant when Presence Server Option is turned on!

Web interface

One–X Attendant provides a web interface for subscribers (called WebAccess). This interface allows a subscriber to indicate absence nformation (e.g., out–of–office) from any PC with a browser..
Standard access is via the web address
https://host:port/one-XAttendantwebaccess/Login.jsp,
which you can enter directly into your browser. “host” and “port” must be replaced with the machine name and port of the Tomcat web server (JOnAs), e.g.
https://localhost:21080/one-XAttendantwebaccess/Login.jsp.
This interface can also be accessed using program commands. This requires that the programming language used must offer web programming capability. Current programming languages such as Visual Basic, Visual C++, Java, etc. meet this requirement.

Programmable functions

You can use the following five functions:

Login, Logout, Set password, Set presence/absence, Query presence/absence.

The way you access these functions depends on the programming language. In general, however, you use commands which will be sent via the HTTPS protocol. The parameters and associated URLs are listed in the following paragraph.

Command-overview

If you are using the following commands you have to specify in the URL the computer name of the Tomcat web server “host” and the “port” that it listens on (default: 21080).

- **Login:**

Before you can use any further commands you need to log in as a specific user.

Query type:	HTTPS POST
Parameters:	firstName, lastName, phone, passwd
Target URL:	https://host:port/one-XAttendantwebaccess/LoginChecker.jsp

Using this command you log in the user using the last name “lastName” and first name “firstName”. “phone” is the user’s phone number and “passwd” the corresponding password.

Note:

A one-X Attendant subscriber only has a password once it has been set for the first time.

- **Simple login (SLogin)**

Query type:	HTTPS POST
Parameters:	phone
Target URL	https://host:port/one-XAttendantwebaccess/SLoginChecker.jsp

This command is used to log in a user. Contrary to the “normal” login procedure (Login - see above) the login occurs *without* password and *without* name information. The phone number (phone) is the only identification used for the user.

Note:

This command is only recommended in systems where the same phone number is not used by several one-X Attendant subscribers.

- **Logout:**

After you have finished the entries for a user, you must log out again without fail.

Query type:	HTTPS GET or HTTPS POST
Parameters:	–
Target URL:	https://host:port/one-XAttendantwebaccess/Logout.jsp

You use this command to log out the user who was previously logged in.

- **Set password:**

To make logging in more secure, each user has a password. The password can be set with this command.

Query type:	HTTPS POST
Parameter:	passwdFirst, passwdSecond
Target URL:	https://host:port/one-XAttendantwebaccess/SetPassword.jsp

This command sets the password for the user who is currently logged in. “passwdFirst” and “passwdSecond” *must* be identical.

- **Set presence / absence:**

This command allows you to set the presence / absence of the user who is currently logged in.

Query type:	HTTPS GET
Parameter:	FROM, TILL, CAUSE
Target URL:	https://host:port/one-XAttendantwebaccess/SaveData.jsp

FROM and TILL contain time and date information using the format dd.mm.yyyy HH.MM.
FROM is the start time and TILL is the end time for the absence.
If you wish to set the user as present, leave FROM and TILL empty.
CAUSE can contain any text. This is usually a short message specifying the reason for the absence.

- **Query presence / absence:**

This command queries the current absence status for the logged in user.

Query type:	HTTPS GET or HTTPS POST
Parameters:	–
Target URL:	https://host:port/one-XAttendantwebaccess/ one-XAttendantWebAccess.jsp
Result:	HTML page containing results

To find out the start and end times as well as the comment you need to parse the resulting HTML page. The start time can be found in the text entry line called FROM. The end time can be found in the text entry line called TILL. The comment is in the text entry line called CAUSE.

- **Buttons/Test Connection**

The check connection button checks whether the Web server component connects correctly to the phone book server component.

- **Buttons/Save**

Saves configuration data in the one-X Attendant database. This data is only active when the JOnAS is stopped and then restarted.

- **Buttons/ Restart JOnAs**

The **Restart JOnAS** button stops the service and restarts it with the modified settings.

Host	Name of the host on which Web Access is installed
Web server port	Port on which the web Access is listening

Note:
You need to specify the Web Server Port entered here if you are using AIS or operating the absence display via a browser

WebAccess Admin Tool

Installing

This tool is used for resetting user passwords for WebAccess.

To use the WebAccess admin tool, a new link must be set up. To do so, in Windows Explorer go to the one-X Attendant directory (c:Program FilesAvayaAvaya one-X Attendant).

1. Select the **StartAbsenceAdmin.bat** file. Create the link.
2. Open **StartAbsenceAdmin.bat** in Notepad. Copy the line.
3. Edit the link. Delete the destination and insert the copied line.

You may need to adjust the port number in this line according to the server installation.

Connecting to external databases

Tool

You can link external databases to one-X Attendant using the one-X Attendant configuration tool set (one-X Attendant ConfigTool).

It provides the phone book tool especially for this task .

Note:

Subscriber data can also be imported into the MasterDirectory. You will find information on this in /11/.

Rules

You **must** follow these rules when working with this tool.

- You need good good knowledge of databases. You must be able to create SQL queries and you also need knowledge of ODBC data source configuration.
- Only 32 Bit ODBC Drivers can be used. Therefore on 64 Bit system the ODBC data source configuration has to be done with the 32 Bit ODBC Admin program: %WINDIR%\SysWOW64\odbcad32.exe
- Only System Data Sources can be used. User Data Sources are recognized by the Config-Tool but not by the Update Service because the Update Service is running under the SYSTEM Account.
- No one-X Attendant client should be running while you configure these settings. Exit all one-X Attendant client applications. The one-X Attendant database must be up and running.
- Use only one data source at a time (Only **one** worksheet in the tree view of the one-X Attendant configuration tool collection).

Import ACM subscriber data into the one-X Attendant database

It is very simple to import the subscriber data including name, number and room from the Avaya Communication Manager into the one-X Attendant phone book.

First the telephone book data must be exported from CM as following:

- Start Avaya Site Administration (ASA) configuration toll.
- Start GEDI
- Type “list station” and then click right in the station area. Select “export”.
- Select where you want to save the exported file, enter as field delimiter a semi-colon, deselect “Export column titles on first row”. Click “OK” when done.

:

1. Select in the menu **Edit** > **Phone book** > **Import**. The ITB data import dialog opens.
2. You can choose whether the existing records should be replaced or the new records appended. Select the desired option.
3. Select the control box “Default CM Format”.
4. Click on the “...”-button and select the exported file.
5. Click on “Start”. Please note that depending on the volume of your data the import may take a few minutes. There is a bar showing the progress of the import.

Configuring the software

Export / Import of System Manager Data

With the help of the Update Services it is now possible to import the System Manager Data.

Export of SMGR Data

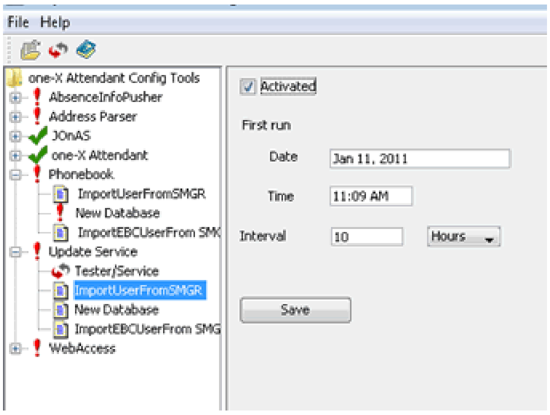
In System Manager you can export users in bulk from the System Manager database. You will find this utility in directory *$MGMT_HOME*/upm/bulkexport, where MGMT_HOME represents the System Manager HOME path (e.g. /opt/Avaya/Mgmt/6.1.5).

Procedure

- At the command prompt change to directory *$MGMT_HOME*/upm/bulkexport/exportutility (here you find also a file “readme.txt” containing a description how to export user.

- Execute shell script
  exportUpmUsers.sh:
  sh exportUpmUser.sh [-u] <user> [-p] <password> … [options]
  User name and password are mandatory parameter. Optional parameter include:
  -f File name prefix of the file that you want to export.
  -r Number of records per file.
  -d Location of the file that you want to export.
  -e Number of records you want to export.
  -t Job scheduling time in format YYYY:MM:DD:HH:MM:SS If no time is specified the job runs immediately.
  You can modify the optional parameter by changing file config/bulkexportconfig.properties.

- A zip file will be generated containing the desired XML-Datei (to find in folder MGMT_HOME/upm/bulkexport)



☑ Activated

First run

Date: Jan 11, 2011

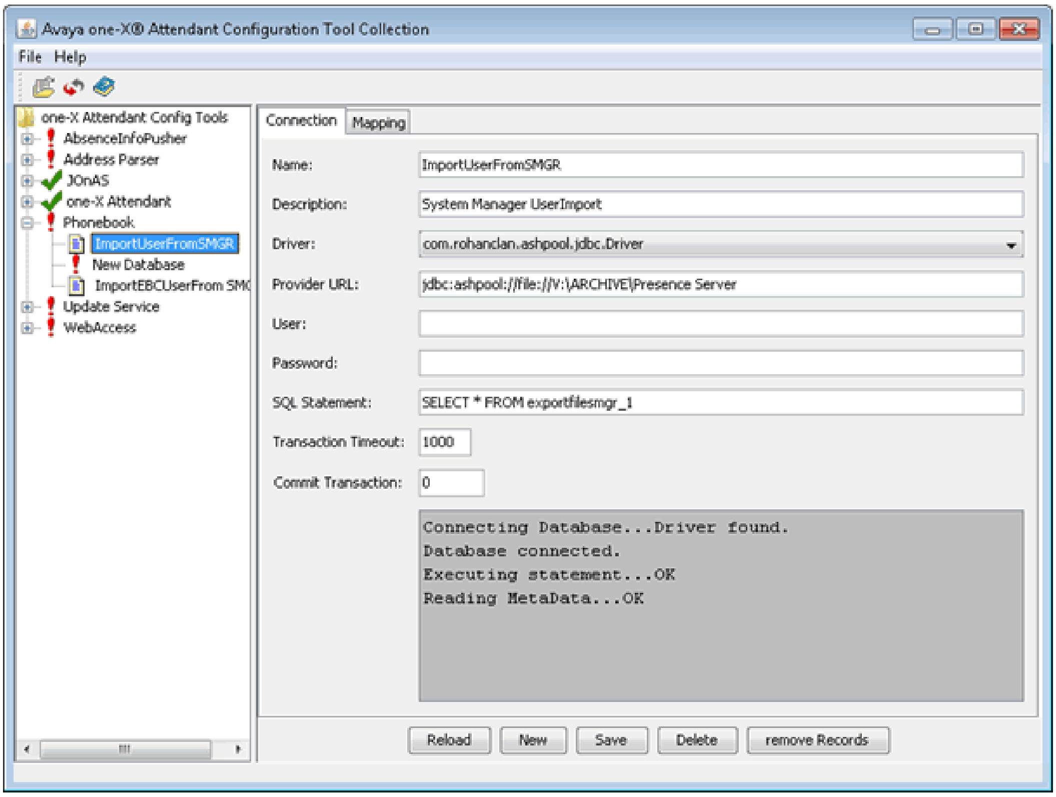
Time: 11:09 AM

Interval: 10 Hours

Unfortunately no filter can be set in SMGR 6.1 so all user are exported.

Import

To import the exported SMGR user in „Avaya one-X Attendant configuration tools collection“ you must install a phonebook connection as following:
Start „Avaya one-X Attendant configuration tools collection“



Name: ImportUserFromSMGR

Description: System Manager UserImport

Driver: com.rohanclan.ashpool.jdbc.Driver

Provider URL: jdbc:ashpool://file://V:\ARCHIVE\Presence Server

User:

Password:

SQL Statement: SELECT * FROM exportfilesmgr_1

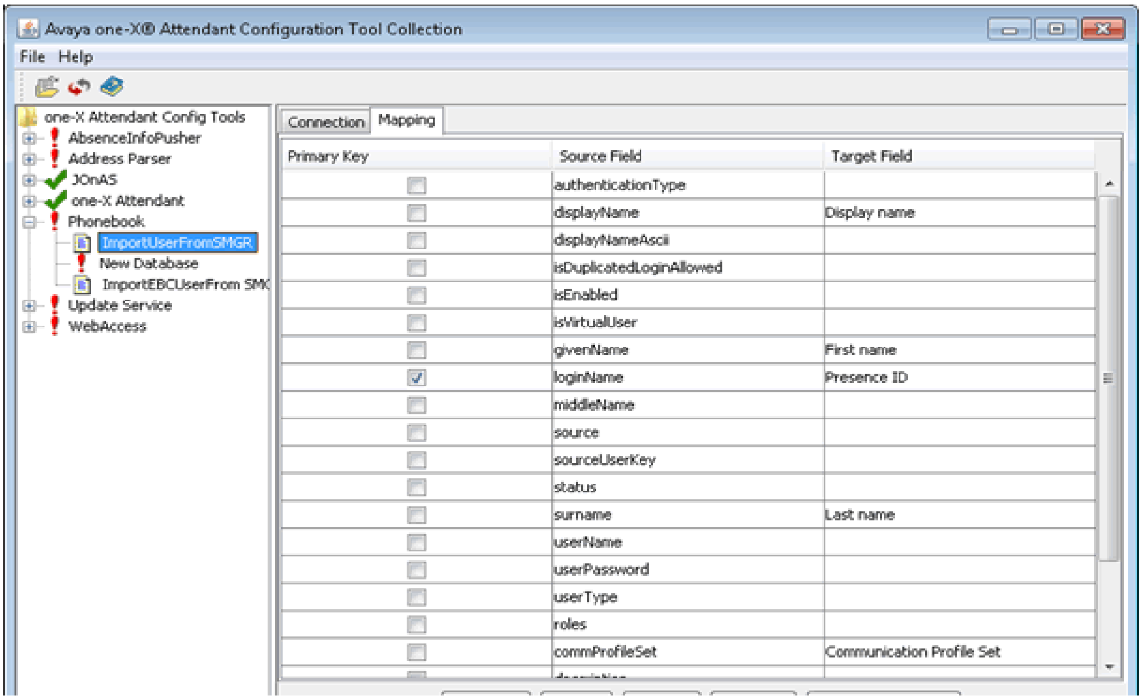
Transaction Timeout: 1000

Commit Transaction: 0

```
Connecting Database...Driver found.
Database connected.
Executing statement...OK
Reading MetaData...OK
```

- Choose Phonebook – ImportUserFrom SMGR
  Choose driver com.rohandan.ashpool.jdbc.Driver.
- In Provider URL add t
- In provider URL add the path of the xml file generated by SMGR export.
- In SQL Statement the name of the xml file (without extension) must be used as table name.
- In assignment table the target field „Communication Profile Set“ must be assigned to source field „commProfileSet“.

In the mapping the following source and target fields have to be assigned:



Primary Key	Source Field	Target Field
□	authenticationType	
□	displayName	Display name
□	displayNameAscii	
□	isDuplicatedLoginAllowed	
□	isEnabled	
□	isVirtualUser	
□	givenName	First name
☑	loginName	Presence ID
□	middleName	
□	source	
□	sourceUserKey	
□	status	
□	surname	Last name
□	userName	
□	userPassword	
□	userType	
□	roles	
□	commProfileSet	Communication Profile Set

No phone number has explicitly to be mapped. All numbers are contained in communication profile set. Dependent on the type of handle the data are entered in different phonebook fields:

- SIP	-> business 1-3
- XMPP	-> IM Handle 1-3
- SMTP and IBM	-> eMail 1-3

Date and frequency of import can now be configured in Update Service.

PS configuration for one-X® Attendant & certificates

Note that this has to be done **only on the 1XATTD server**. Four tools have to be installed on one-X Attd server to be able to execute the configuration steps listed above and the later following steps concerning the certificate exchange:

- PuTTY
- WinSCP
- Keytool
- openSSL

The configuration steps require the input of some commands on command-line level. As some commands require quite a few parameters, the commands can be taken from this document (copy & paste).

> **Note:**
> Please establish PuTTY session to PS server using craft as username, then switch user to root.

Precondition

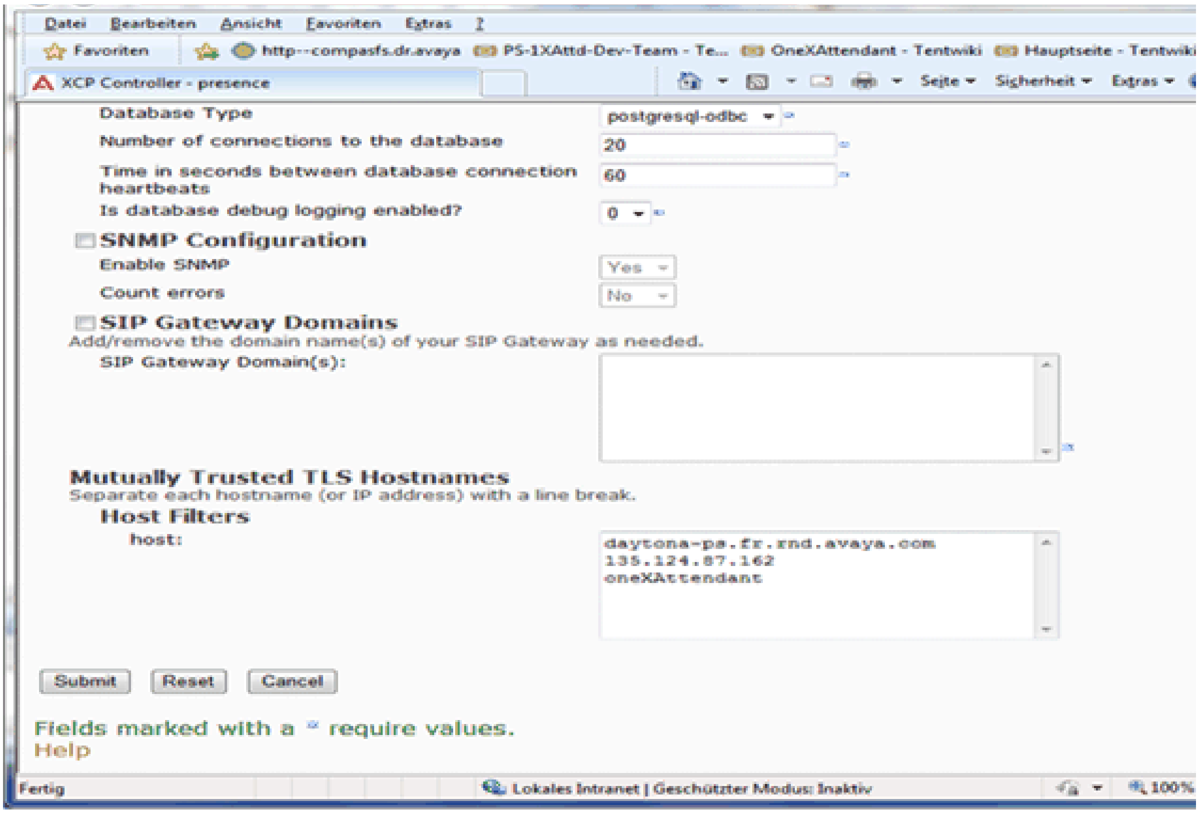
The connection between one-X® Attendant and Presence Services only can be configured and established successfully, if the following preconditions are met:

- All servers of the solution have a static IP address
- All server IP addresses can be resolved by DNS, the FQDN and IP address resolution works in both directions
- In case a firewall exists, it is configured according to one-X™ Attendant IP port matrix document
- SMGR & one-X Attd users & passwords have been entered correctly during the installation of one-X® Attendant

Add one-X® Attendant CN to PS mutually trusted host list

- Log on to the Presence Services XCP Controller Web interface as an administrator. Select **Advanced** in drop down box **Configuration View**
- Edit **Global Router Settings** for **Core Router** plugin
- Add common name (CN) of the oneX Attd certificate named **oneXAttendant** to **Mutually Trusted TLS Hostnames / Host Filters**, then click Submit

One-X Attd certificate name administration in PS XCP controller



Database Type: postgresql-odbc

Number of connections to the database: 20

Time in seconds between database connection heartbeats: 60

Is database debug logging enabled?: 0

□ SNMP Configuration

Enable SNMP: Yes

Count errors: No

□ SIP Gateway Domains

Add/remove the domain name(s) of your SIP Gateway as needed.

SIP Gateway Domain(s):

Mutually Trusted TLS Hostnames

Separate each hostname (or IP address) with a line break.

Host Filters

host:

```
daytona-ps.fr.rnd.avaya.com
135.124.87.162
oneXAttendant
```

Fields marked with a * require values.

Help

Grant one-X Attendant Access to PS

Add one-X® Attendant Server Address to PS

Add IP Address of PC/Server where X Attendant Server is installed using Putty as ROOT user.
In this example the IP address which is newly added is 135.124.73.25 so the second entry allows exactly this address to access to PS postgres database.

```
cd /var/lib/pgsql/data/
vi pg_hba.conf
# IPv4 local connections:

host    all        all        127.0.0.1/32          md5
host    all        all        135.124.73.25/32    trust
```

Save file and exit vi: :wq!

Modify Listen Address of Database PS using Putty SSH

Modify listen address in file postgresql.conf from localhost to '*' and leave the port.

```
cd /var/lib/pgsql/data/

vi postgresql.conf

#------------------------------------------------------------------------------
# CONNECTIONS AND AUTHENTICATION
#------------------------------------------------------------------------------

# - Connection Settings -

listen_addresses = '*'              # what IP address(es) to listen on;
                                    # comma-separated list of addresses;
                                    # defaults to 'localhost', '*' = all
                                    # (change requires restart)
```

Save file and exit vi: :wq!

Restart Database

Restart postgresql using Putty as ROOT user:

```
/etc/rc.d/init.d/postgresql restart
```

> **Note**
> The restart of the PS doesn't restart the database which is necessary to activate the new listen address.

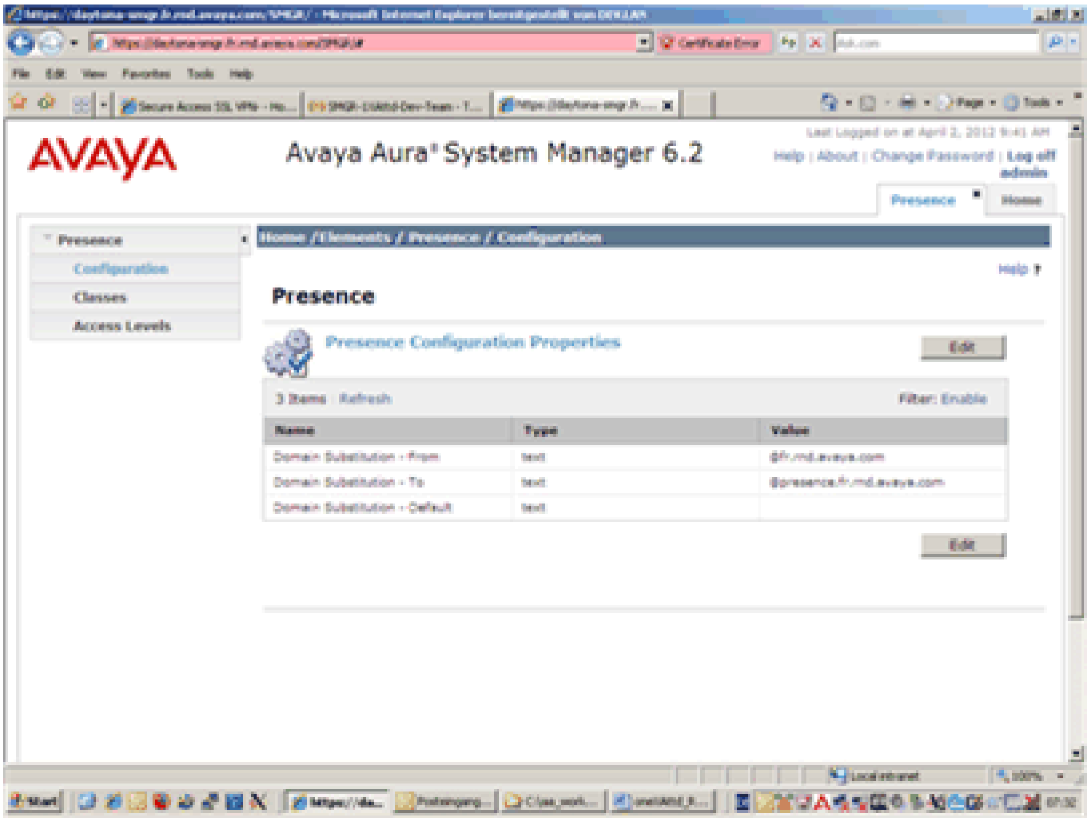
PS need a virtual SIP domain

Presence Services need a virtual SIP domain (please see Presence Services Administration Guide for further details [7], chapter **Understanding Presence Services domain, Domain substitution rule and user global login**).

Therefore configure the SIP domain substitution for Presence in System Manager menu **Elements/ Presence/Configuration**:

Example

- User Testuser works for company fr.rnd.avaya:
- Testuser's company domain: fr.rnd.avaya.com
- User login of Testuser in Presence Services: testuser@fr.rnd.avaya.com.com
- In Presence Services domain (ROUTER_SERVICE_NAME) Testuser's domain changes to: presence.fr.rnd.avaya.com
- Testuser's ID in Presence Services is: testuser@presence.fr.rnd.avaya.com



Avaya Aura® System Manager 6.2

Home /Elements / Presence / Configuration

Presence

Presence Configuration Properties

3 Items Refresh

Name	Type	Value
Domain Substitution - From	text	@fr.rnd.avaya.com
Domain Substitution - To	text	@presence.fr.rnd.avaya.com
Domain Substitution - Default	text	

SIP Domain Substitution for Presence Services (Screenshot)

One-X Attendant configuration tools overview

one-X Attendant configuration tools collection

The **one-X Attendant configuration tools collection (Configuration Tools)** is a set of tools which allow you to configure one-X Attendant. It is automatically installed when you install a one-X Attendant server.

The collection contains the following tools:

- AbsenceInfoPusher
- Address parser
- JOnAS Server (phone book server)
- Central one-X Attendant- configuration data
- Phone book
- Update service
- WebAccess

Starting and logging in

The program is started from Start > Programs > Avaya > one-X Attendant >one-X Attendant configuration tools.

All system engineers saved in the one-X Attendant database are authorized to use the tool collection. The user name and password are the same as for one-X Attendant.

Note when editing configuration data for the first time:

After installing one-X Attendant the central one-X Attendant configuration data can only be edited once one-X Attendant has been started.

Reason:

The database cannot be accessed during setup. For this reason the one-X Attendant configuration data is placed in the Registry first (key “Setup”). The one-X Attendant transfers this information into the database on first startup.

User interface

The menu bar

The menu bar contains the menu **File** with the menu entries *Properties, Log in / Log out* and *Finish* available to use.

The menu **Help** contains the entry *About...* to open an info box about the tool.

The work area

The work area is divided into the tree view on the left and the respective open worksheets on the right.

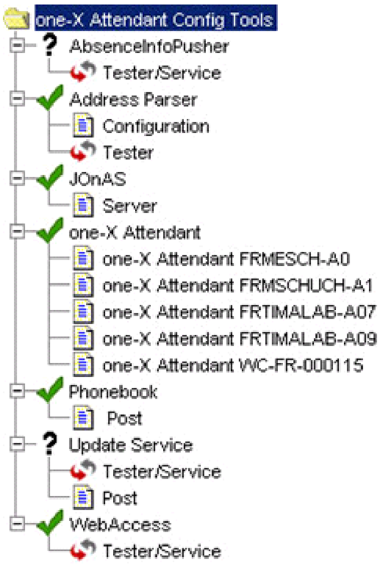
The toolbar

Opens the *Properties* of the one-X Attendant configuration tools collection

Starts a test of all components

Opens the Info Box

Treeview



- one-X Attendant Config Tools
  - ? AbsenceInfoPusher
    - Tester/Service
  - ✓ Address Parser
    - Configuration
    - Tester
  - ✓ JOnAS
    - Server
  - ✓ one-X Attendant
    - one-X Attendant FRMESCH-A0
    - one-X Attendant FRMSCHUCH-A1
    - one-X Attendant FRTIMALAB-A07
    - one-X Attendant FRTIMALAB-A09
    - one-X Attendant WC-FR-000115
  - ✓ Phonebook
    - Post
  - ? Update Service
    - Tester/Service
    - Post
  - ✓ WebAccess
    - Tester/Service

The tree view contains all the tools. The tool currently shown in the work area is highlighted in blue.

A **green check mark** indicates that the tool test was successful. A **red exclamation mark** indicates a problem with this tool. A **black question mark** indicates that the tool cannot be tested.

Click on a tool to load it to the work area.

Properties

Properties opens a dialog which you can use to edit the program settings (one-X Attendant Config tool, properties).
The drivers listed in the table below are available for selection when you define a data source. When you make a selection, the corresponding default URL is entered.

Key	Value	Note
DBPwd	sql	Password for the one-X Attendant database
DNS	one–X Attendant	ODBC link to the one-X Attendant database
Language	DE	Language of the one-X Attendant configuration tools collection
jdbc.driver.class.1	sun.jdbc.odbc.JdbcOdbcDriver	Driver 1 for accessing ODBC data sources
jdbc.driver.class.2	com.sybase.jdbc3.jdbc.SybDriver	Driver 2 for direct access to Sybase databases (ASA and ASE) without ODBC
jdbc.driver.class.3	com.octetstring.jdbcLdap.sql.JdbcLdapDriver	Driver 3 for accessing LDAP data sources
jdbc.driver.class.4	ianywhere.ml.jdbcodbc.jdbc3.IDriver	Driver for direct acces to Sybase Database (ASA and ASE) from Version 9 and higher.
jdbc.driver.class5	jstels.jdbc.csv.CsvDriver	Driver 5 for accessing Text respectively CSV- Files
jdbc.driver.default_url.1	jdbc \:odbc \:<Enter DSN here>	Default provider URL for driver 1
jdbc.driver.default_url.2	jdbc \:sybase \:Tds \:<server>\:<port>	Default provider URL for driver 2
jdbc.driver.default_url.3	jdbc \:ldap \://<server>\:389/ [BASE_DN]?SEARCH_SCOPE \:\=subTreeScope[&pageSize \:\=n]	Default provider URL for driver 3
jdbc.driver.default_url.4	jdbc.ianywhere:<Enter DSN here>	Default Provider URL for Driver 4
jdbc.driver.default_url.5	jdbc:jstels:csv:<Enter directory here>?separator=;&charset=utf-8	Default provider URL for driver 5
phonebookhost	localhost	Host on which the phone book server (JOnAS) runs
phonebookport	21099	Port on which the phone book server listens

Tools: AbsenceInfoPusher

Settings

cycle (sec)	AIP query interval Host-
AIP	host name
Test Port	AIP port

Buttons

The **Save** button saves the changes to the database.

The **Check connection** button checks whether AIP can connect to the

JOnAS server using the URL. The result is displayed in the gray text box.

The **Start** button launches the AbsenceInfoPusher. The **Stop** button stops the AbsenceInfoPusher.

Testing

To check the connection, proceed as follows:

1. Enter a new free **Test Port**.
2. Save the new setting with the **Save** button**.**
3. Stop the AIP with the **Stop** button.
4. Start the AIP again with the **Start** button.
5. Test the connection using the **Check connection** button.

Tools: Address parser

Introduction

In case of a phonebook application entries have to be found by the phone number. Therefore each entry bears a phone number in a visible user format and in a invisible normalized format (ShadowNumber). When an entry is written into the database the normalized phone number is generated by the AddressParser.

If the parser configuration is left with empty fields: All imported numbers will be left inchanged and are copied in the shadow number.

The type of number must be ‘unknown’. That means the number consists from the digits that would be used in public network (the digits so seize the trunk line are not part of such a number) plus internal numbers (as the one-X Attendant would receive them in an internal call to identify the caller).

This document describes how the AddressParser works and how it has to be configured.

Definitions

Numbering Plan

DA numbering plan is a type of numbering scheme used in telecommunications. This is a set of rules used for making numbers. A telephone numbering plan is a plan for allocating telephone number ranges to countries, regions, areas and exchanges and to non-fixed telephone networks such as mobile phone networks.

Open Numbering Plan

Open numbering plans have phone numbers that vary in length like in Germany.

Closed Numbering plan

Phone numbers in a closed numbering plan have a fixed length like in the USA.

Dial Plan

A dial plan specifies the actual digits dialed within the constraints of a defined numbering plan. A typical dialed telephone number comprises digits that need not always be dialed (codes) and digits that must always be dialed (local number). If a dial plan consists of slices (blocks) of DIDs where station numbers are ambiguous it is called **heterogeneous**.

Example:

Dial plan consists of two blocks of numbers.
Slice 1 from 908-969-5000 to -7000
Slice 2 from 908-484-5000 to –5500
Stations 5000 to 5500 are in both slices.

If a dial plan consists of slices (blocks) of DIDs where station numbers are unique it is called **homogeneous**.

Example:

Dial plan consists of two blocks of numbers.

Slice 1 from 908-969-5000 to -7000

Slice 2 from 908-484-1000 to –1500

No station is in both slices.

ShadowNumber

The ShadowNumber is the invisible unique version of an arbitrary phone number. It is used as a key to searches in the phone book database.

Dialable number

The dial able number is that number that can be dialed after AddressParser processed a ShadowNumber.

Mode of operation

The AddressParser has two basic functionalities.

Normalization:

This is parsing and converting an arbitrary phone number into a world wide unique phone number (ShadowNumber).

Reduction:

This is parsing and converting a normalized phone number into a dial able phone number.

For both functionalities the AddressParser needs Information about different elements of a phone number. These are country code, international code, national long distance code, area code, the number of the local PBX or DIDs.

Note:

The AddressParser itself does not deal with trunk codes. Once the AddressParser has identified a dialable number as an external number, the trunk code is added afterwards. The AddressParser tester indicates an external dialable number by adding a leading "+".

How the phone numbers are parsed and converted depends on the used public numbering plan and the dial plan.

Next chapter describes, which algorithms are implemented and in which countries they can be applied.

How to select the appropriate Address Parser?

Please select the appropriate one-X Attendant address parser in the following steps:

- Determine the country, which your one-X Attendant server has to support.
- Check whether your country is supported in one-X Attendant *Configuration Tool Collection* (in *Address Parser / Configuration* tree view node, *Code Numbers* tab, parser *Mode* radio):

Standard parser supports Open Numbering Plans for

- Austria
- Australia
- Bolivia
- Brazil
- China
- Germany
- Hungary
- Italy
- Japan
- Mexico
- Netherlands
- Republic of Korea (South Korea)
- Sweden
- United Kingdom

France parser supports 10-digit Closed Numbering Plans with Provider Codes for

- France
- Switzerland

***Spain* parser supports 9 digit *Closed Numbering Plan* without *Area Codes* for**

- Spain

USA parser supports NANP (10 digit Closed Numbering Plan) for

- United States of America
- Canada
- Anguilla
- Antigua & Barbuda
- Bahamas
- Barbados
- Bermuda
- British Virgin Islands
- Cayman Islands
- Dominica
- Dominican Republic
- Grenada
- Jamaica
- Montserrat
- St. Kitts and Nevis

- St. Lucia
- St. Vincent and the Grenadines
- Trinidad and Tobago
- Turks & Caicos

Russia parser supports 10 digit Closed Numbering Plan without National Code for

- Russian Federation
- Republic of Kazakhstan

Norway parser supports 8 digit Closed Numbering Plans with Area Codes for

- Norway

Note:

In case your country is not listed in *Configuration Tool Collection* use the Universal Parser.
The Universal Parser supports homogenous and heterogeneous *Open Numbering Plan* and *Closed Numbering Plan* with and without *Area/City codes.*

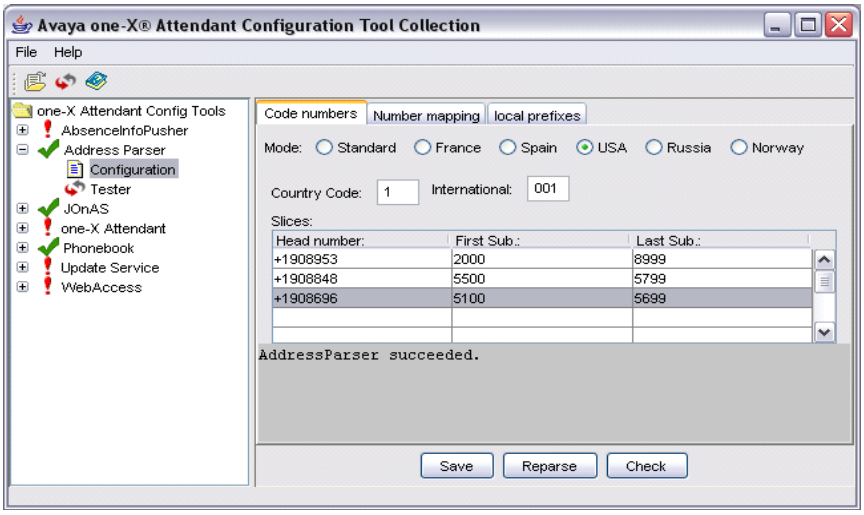
How to configure and test the AddressParser?

The Configuration Tool Collection allows configuring and testing the AddressParser.

Depending on the selected parsing algorithm (= Mode), the code numbers tab differs because each algorithm needs a different configuration. The following picture shows an example configuration for USA. The next picture shows a possible Tester scenario for this configuration.

Configuring the Address Parser

The configuration also depends on the dial plan.



Mode: ○ Standard ○ France ○ Spain ● USA ○ Russia ○ Norway

Country Code: 1 International: 001

Slices:

Head number:	First Sub.:	Last Sub.:
+1908953	2000	8999
+1908848	5500	5799
+1908696	5100	5699

```
AddressParser succeeded.
```

Configurator example: USA

Code numbers

This page takes the AddressParser mode and depending on the selected mode the basic configuration.

Number mapping

Number mapping is a feature that can be used to map an arbitrary number of digits from left of the number. This is for use with two or more PBX interconnected via QSIG and run a 1XA on each PBX with one central phonebook server.

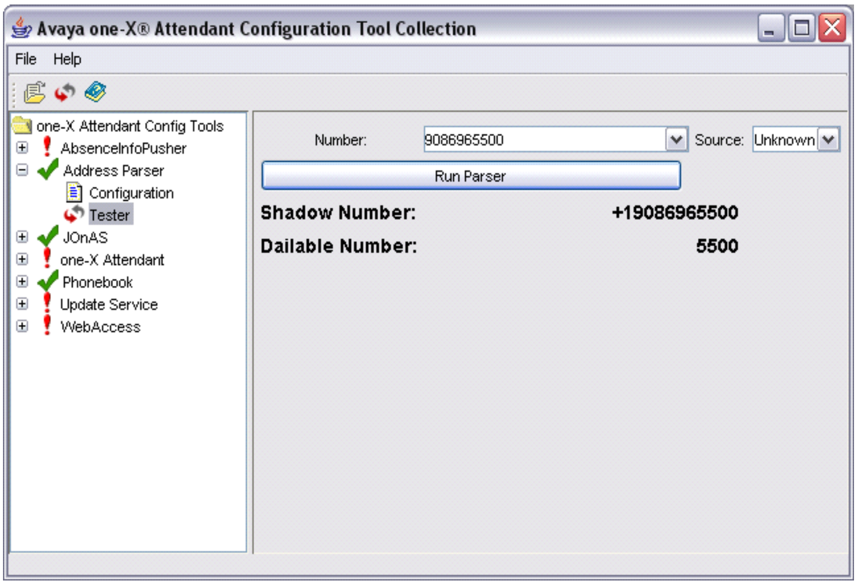
Local prefixes

Locale prefixes is a feature to map DIDs to a prefix that is configured in CM to extend the station number but is not included in the DIDs.

Testing the Address Parser

For testing the AddressParser the Configuration Tool contains a Tester node. It generates the ShadowNumber and the dial able number of the entered number.

ATTENTION: if the dialable number starts with + the number is marked for dialing external. one-X Attendant will replace it by configured trunk code.



Number: 9086965500 Source: Unknown

Shadow Number: +19086965500

Dailable Number: 5500

Testsettings example for USA

When is AddressParser invoked?

AddressParser **Normalization** is invoked when ever a phone number has to be searched in the phone book.

On start up for each number in

- BA
- NBA
- VIP View
- Redial List
- Calling List

On Runtime when ever

- a phone number is transferred from the connected PBX to the UI. For outgoing calls identification of a phone number is done when call state indicates dial complete.
- a phone number is transferred form SVAManager (Redial List, Calling List)
- a entry is written into the phone book (from UI, Import, Update Service)

AddressParser **Reduction** is invoked when ever a phone number has to be dialed from

- the phonebook (Phonebook window, ITB List window, Operator window)
- the NBA
- a speed dial button

AddressParser Modes

Abbreviations

The diagrams shown in this chapter are using the following abbreviations:

CC	Country Code
IC	International Code
NC	National Code
AC	Area Code (also called City Code)
NPA	Numbering Plan Area (= NANP Area Code)
NSN	National Significant Number
LDN	Long Distance Call
NANP	North American Numbering Plan

Settings: Code numbers

When you enter an internal subscriber in the phone book, the address parser adds the number and corresponding code number.

The user cannot see the converted number. The number is saved in a shadow database. The user always sees the number in the phone book in the form he or she entered it.Universal, Standard, France, Spain, Russia, Norwegian and USA modes are possible.

Name	Comment	Example
Country Code	Indicates the international country code	49 for Germany
International	Indicates the international prefix	00
National	indicates the national prefix	0
Area code	Indicates the area code	711 for Stuttgart
Local PBX	Indicates the PBX number	13586
Max. length internal	Indicates the maximum length of internal call numbers. All call numbers which are shorter or from equal length are treated as internal call numbers.	4

Slices (defining ranges of DIDs given from the network provider)

In Universal mode:

PBX-Number Start	Holds the beginning of the first number.
PBX-Number End	Holds the beginning of the last number.
Number of local digits	Defines the number of digits included in PBX-Number Start and PBX-Number End that remains to internal numbers.

In France, Spain, Norwegian and USA mode:

Head Number	Defines the PBX-number of the slice
First Sub	Holds the first number.
Last Sub	Holds the last number.

Example

If you enter an internal subscriber with the number 1234, the converted shadow number looks like this:

+49	711	13586	1234
Countrycode	Area code	Local PBX	Extensioncode

Settings: Call Number Replacement

one-X Attendant uses the settings on the Call Number Replacement tab to identify a subscriber of a networked system even if the subscriber places an external call.

The PBX handles subscribers in a networked system like internal subscribers. The address parser always creates a shadow number with its own code numbers for this purpose. Therefore, when there is a call, the PBX-numbers of external locations must be re–evaluated using the own code numbers and if necessary the node numbers.

Note the following regarding call number replacement

You must always enter numbers with the country code and area code, for example +49711135.

Settings: Area codes

In a PBX or PBX network, there may be differences in how external connections are dialed and how they are stored in ACM. For example, in the Paris subsidiary, all the internal numbers could be saved with a preceding 123 in ACM: Number saved in ACM +33017505**123**4712, external number

+330175054712.

In the **Area codes** tab under **Prefix** enter the access number for the PBX (7505) including all prefixes, e.g. +33017505 and under **subst. head** the associated digits of the internal number, as they are stored in CM, e.g. 123.

Fixed Numbers

In some cases with outgoing dialing (e.g. out of phonebook), the numbers must not be parsed. In Germany for example, there are some special numbers like 112 and 110 where it isn't allowed to put the area code in front (069112 isn't possible).

Enter such numbers in the tab **Fixed numbers**, they would be dialed without putting trunk code or area code in front. This means here and in the phonebook the number has to be inserted with trunk code (e.g. 0112 if 0 is trunk code).

Example for call number replacement with a closed numbering scheme

PBX 1 in Stuttgart

Number: +4971113586

PBX 2 in Frankfurt

Number: +49697505

<u>We are at PBX 1 in Stuttgart. The Parser is programmed for this PBX.</u>

If you want to enter a subscriber from Frankfurt with internal number 1234 in the phone book, the address parser generates the following shadow number:

+49	711	13586	1234
Country code	Area code	Local PBX	Extension

Settings in call number replacement

You must enter the following information for the example.

From	**To**
+49697505	+4971113586
PBX number of the external location	PBX number of own location

Example of call number replacement with an open numbering scheme

PBX 1 in Stuttgart
Number: +4971113586
Node number: 88

PBX 2 in Frankfurt
Number: +49697505
Node number: 99

We are at PBX 1 in Stuttgart.

If you want to enter a subscriber from Frankfurt with internal number 991234 in the phone book (99 is the node number for Frankfurt), the address parser generates the following shadow number:

+49	711	13586	991234
Country code	Area code	Local PBX	Extension

Settings in call number replacement

You must enter the following information for the example.

From	To
+49697505	+497111358699

Country settings

If you select France, Spain, Russia or USA from the mode-option fields, other country-specific configuration field will be offered to you.

Settings: Code numbers for France

Name	Explanation	Example
Country code	Indicates the international country code. (max. 2 Digits)	33 for France
International	Indicates the international prefix. (max. 2 Digits)	00
Provider	Provider code. (Max. 1 Digit)	0 for France Telecom
Area code	Shows the regional/area code. (Max. 1 Digit)	1 for the Paris region
Range:		
First Subs.	First subscriber number in the number block (3-6 Digits)	.000
Last Subs.	Last subscriber number in the number block(3-6 Digits) .	500
Head number	Shows the fixed digits of a PBX number block(2-5 Digits).	12345

Example

If you enter into the phone book an internal subscriber with the number 222, the converted shadow number looks like this:

+33	0 1	12345	222
Country	Provider+Area	Head	Subscribernumber

Settings: Code numbers for Spain

The explanation of code numbers for France also applies for Spain. Only the Country Code, International and Range fields are available.

Settings: Code numbers for Norway

The explanation of the code numbers again applies in a corresponding manner. Only the Country Code, International and Range fields are available. It is furthermore taken into account that all national numbers in Norway consist of 8 digits.

Settings: Code numbers for the USA

Name	Explanation	Example
Country code	Indicates the international country code.	1 for the USA
International	Indicates the international prefix for international dialing from the USA. Example: 01149 for USA –> Germany	011
Area code	Indicates the regional/area code.	585 for part of New York
Local PBX	Indicates the PBX number.	13586

Example

If you enter into the phone book an internal subscriber with the number 1234, the converted shadow number looks like this:

+1	585	13586	1234
Country code	Area code	Local PBX	Extension

Settings: Code numbers for Russia

Name	Explanation	Example
Country code	Indicates the international country code.	7 for Russia
International	Indicates the international prefix for dialing from Russia to another country. Example: 81049 for Russia –> Germany	810
Area code	Indicates the regional/area code.	495 for Moscow
Local PBX	Indicates the PBX number.	13586

Example

If you enter into the phone book an internal subscriber with the number 1234, the converted shadow number looks like this:

+7	495	13586	1234
Country	Area code	Local PBX	Extension

USA

This algorithm is built for NANP only. The NANP format can be summed as:

NPA Nxx Station
where

NPA = [2-9][0-8][0-9]
Nxx = [2-9][0-9][0-9]
Station = [0-9][0-9][0-9][0-9]

NPA is the 3 digit Area Code, Nxx and Station together form the local 7 digit telephone number.

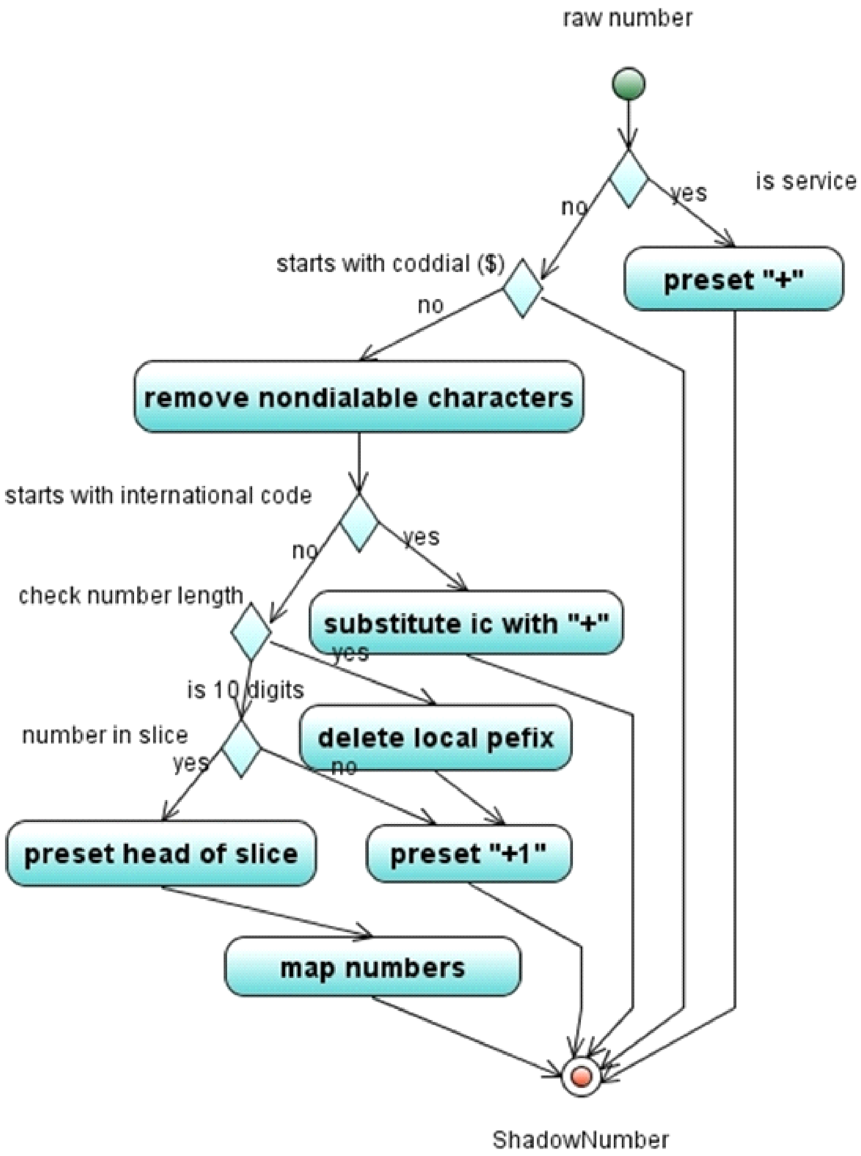
Digit 1 is used to pre-indicate 10-digit number, this is called a national long distance call.

Service code format = X11

- e.g. Emergency Call Number 911
- International access = 011

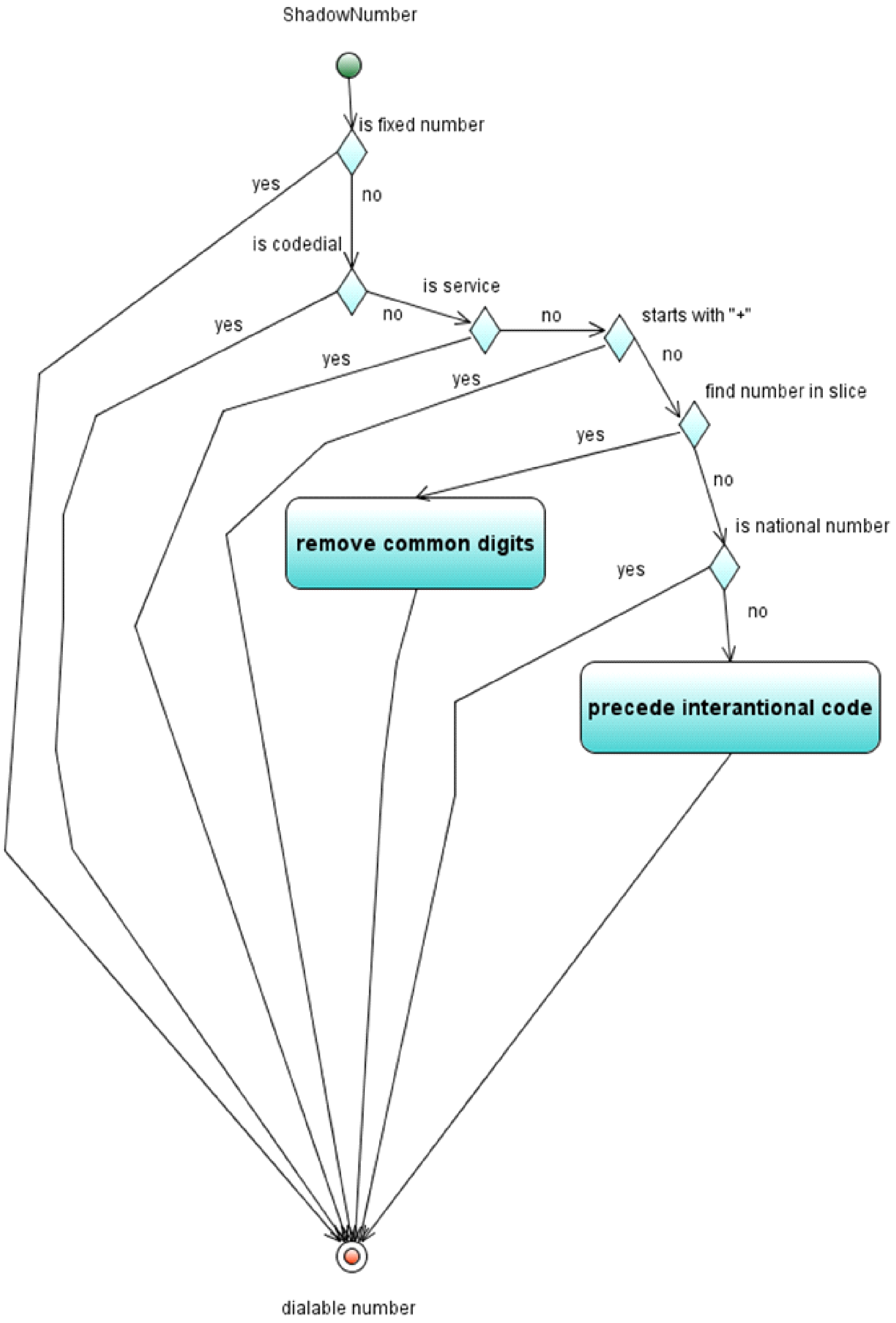
Normalization

Normalization takes a raw number and builds the ShadowNumber. The following steps are done.



Reduction

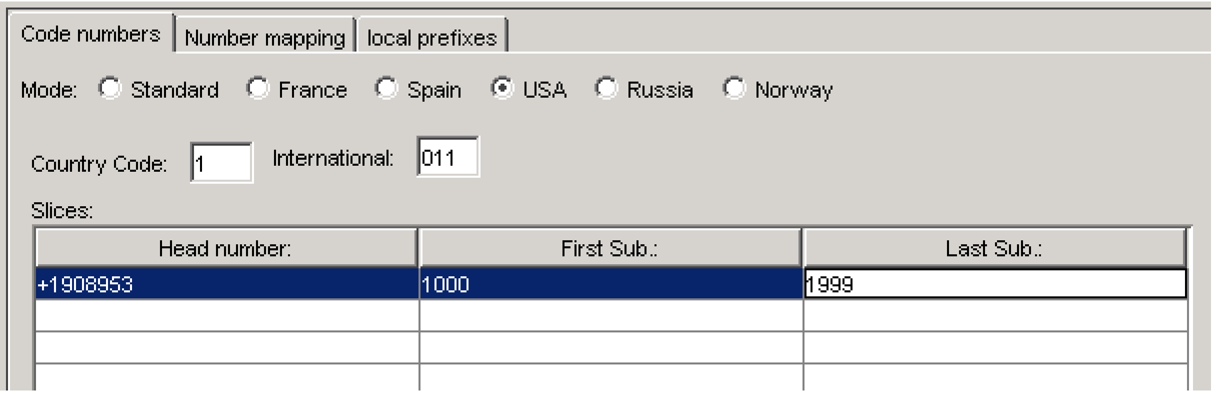
Reduction takes a ShadowNumber and transform it into a dial able number. The following steps are done



Examples

One block of DIDs

908-953-1000 to 1999, number mapping and local prefixes are not required.



Mode: ○ Standard ○ France ○ Spain ● USA ○ Russia ○ Norway

Country Code: 1 International: 011

Slices:

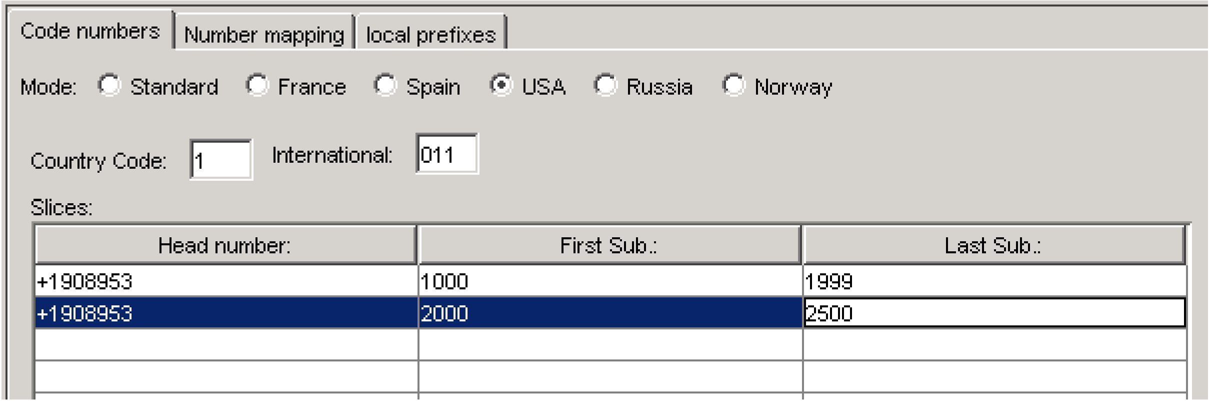
Head number:	First Sub.:	Last Sub.:
+1908953	1000	1999

Displayed number	ShadowNumber	Dialable number	Dial external	Comment
908-953-1000	+19089531000	1000		DID 1000 is in a slice
9089532000	+19089532000	19089532000	x	DID 2000 is not in a slice
1500	+19089531500	1500		DID 1500 is in a slice
911	+911	911	x	Emergency Call number
+49-69-7505-5000	+496975055000	011496975055000	x	International Callnumber
953-1000	9531000	9531000		This is an illegal number, but will be dialed internal
1-555-666-7894	+15556667894	15556667894	x	National long distance call

ATTENTION: the AddressParser Tester will show a leading “+” in case the dialable number is external, thus one-X Attendant software will replace the leading “+” by configured trunk code afterwards. In column “Dialable number” above, the leading “+” is not listed, therefor external calls are marked in column Dial external.

Two blocks of DIDs homogeneous

908-953-1000 to 1999 and 908-953-2000 to 2500, no overlapping in station numbers, number mapping and local prefixes are not required.



Mode: ○ Standard ○ France ○ Spain ● USA ○ Russia ○ Norway

Country Code: 1 International: 011

Slices:

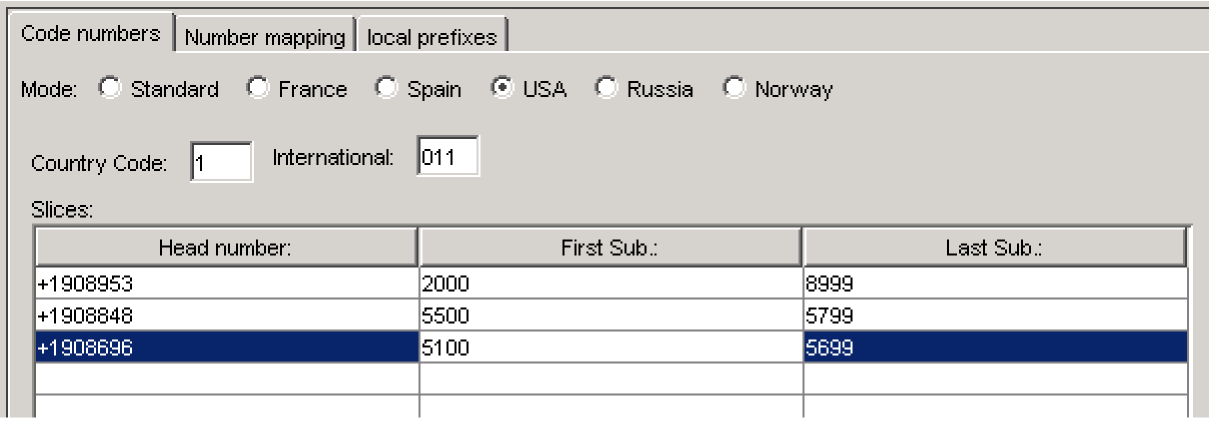
Head number:	First Sub.:	Last Sub.:
+1908953	1000	1999
+1908953	2000	2500

Displayed number	ShadowNumber	Dialable number	Dial external	Comment
908-953-1000	+19089531000	1000		DID 1000 is in a slice
9089532000	+19089532000	2000		DID 2000 is in a slice
1500	+19089531500	1500		DID 1500 is in a slice
911	+911	911	x	Emergency Call number
+49-69-7505-5000	+496975055000	011496975055000	x	International Call
953-1000	9531000	9531000		This is an illegal number, but will be dialed internal
1-555-666-7894	+15556667894	15556667894	x	National long distance call

ATTENTION: the AddressParser Tester will show a leading “+” in case the dialable number is external, thus one-X Attendant software will replace the leading “+” by configured trunk code afterwards. In column “Dialable number” above, the leading “+” is not listed, therefor external calls are marked in column Dial external.

Three blocks of DIDs heterogeneous

908-953-2000 to 8999, 908-848-5500 to 5799 and 908-696-5100 to 908-696-5699, overlapping in station numbers, number mapping is not required.



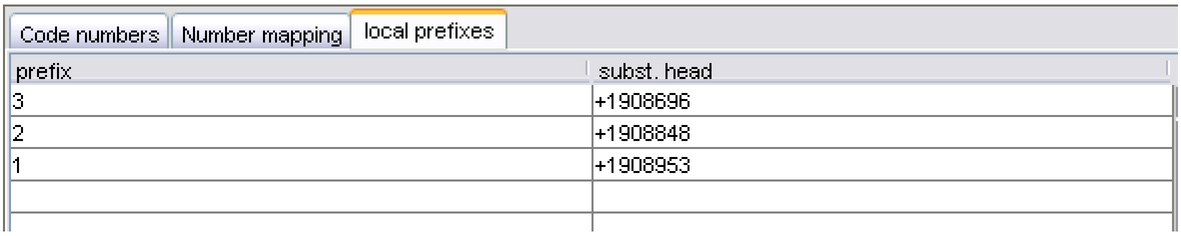
Mode: ○ Standard ○ France ○ Spain ● USA ○ Russia ○ Norway

Country Code: 1 International: 011

Slices:

Head number:	First Sub.:	Last Sub.:
+1908953	2000	8999
+1908848	5500	5799
+1908696	5100	5699

Since station numbers 5100 to 5799 are included in more than one slice, for each slice a local prefix has to be defined. The prefix must be the same as configured in the PBX. A call to station 908-848-5500 can be reached by one-X Attendant when dialing **2**5500. A call from 908-848-5500 to the attendant has to be signaled as **2**5500 or as 908-848-5500.



prefix	subst. head
3	+1908696
2	+1908848
1	+1908953

Displayed number	ShadowNumber	Dialable number	Dialex-ternal	comment
908-953-2000	+19089532000	**1**2000		Prefix 1, DID 2000
25500	+19088485500	**2**5500		Prefix 2, DID 5500
+19086965500	+19086965500	**3**5500		Prefix 3, DID 5500
911	+911	911	x	Emergency Call
+49-69-7505-5000	+496975055000	011496975055000	x	International Call
953-1000	9531000	9531000		This is an illegal number, but will be dialed internal
1-555-666-7894	+15556667894	15556667894	x	National long distance call

ATTENTION: the AddressParser Tester will show a leading “+” in case the dial able number is external, thus one-X Attendant software will replace the leading “+” by configured trunk code afterwards. In column “Dial able number” above, the leading “+” is not listed, there for external calls are marked in column Dial external.

Standard

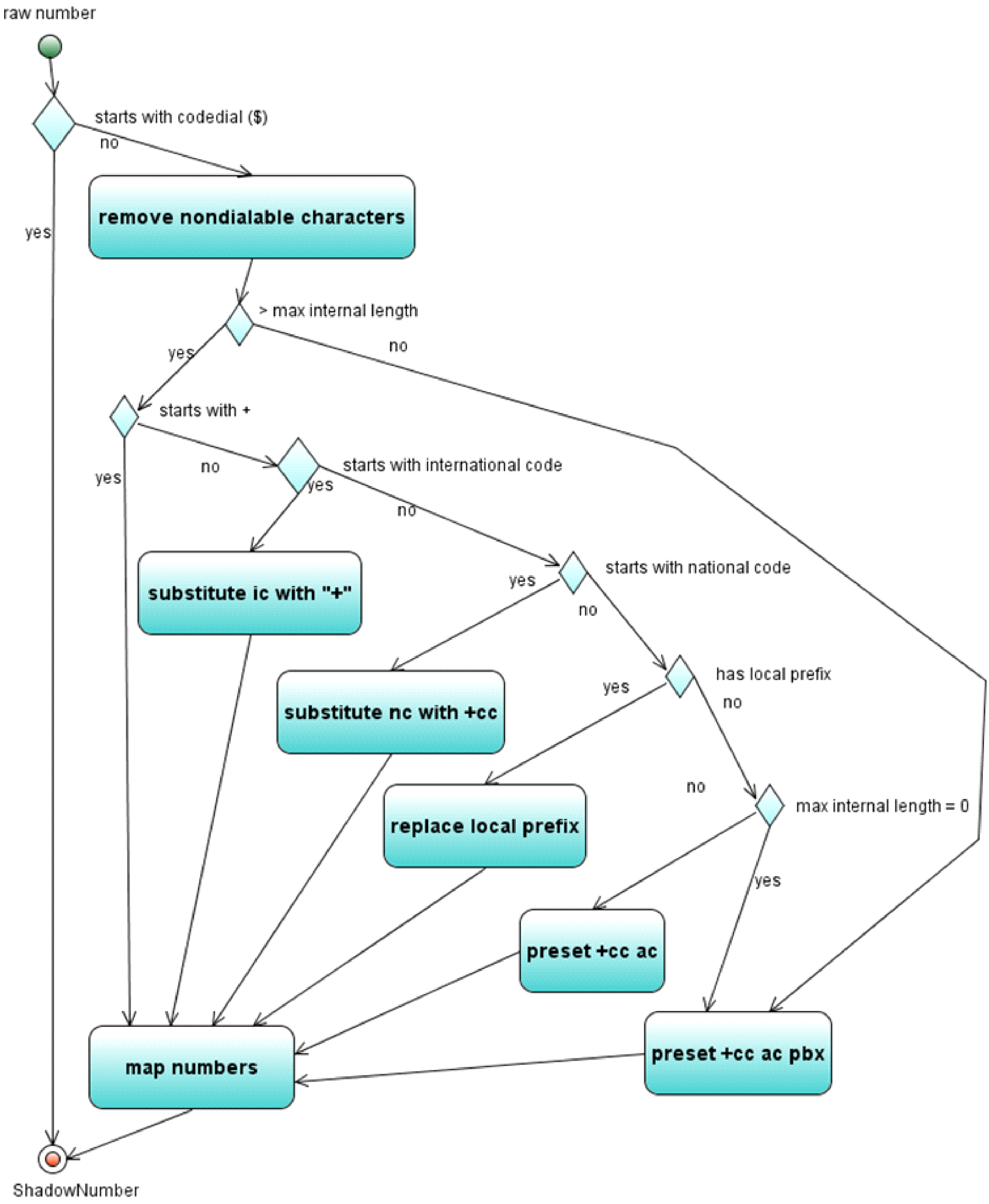
This algorithm is built for open dial plans like in Germany. It may also be used for Closed Numbering Plans as described in chapter 4.

Phone numbers in Germany consists of:

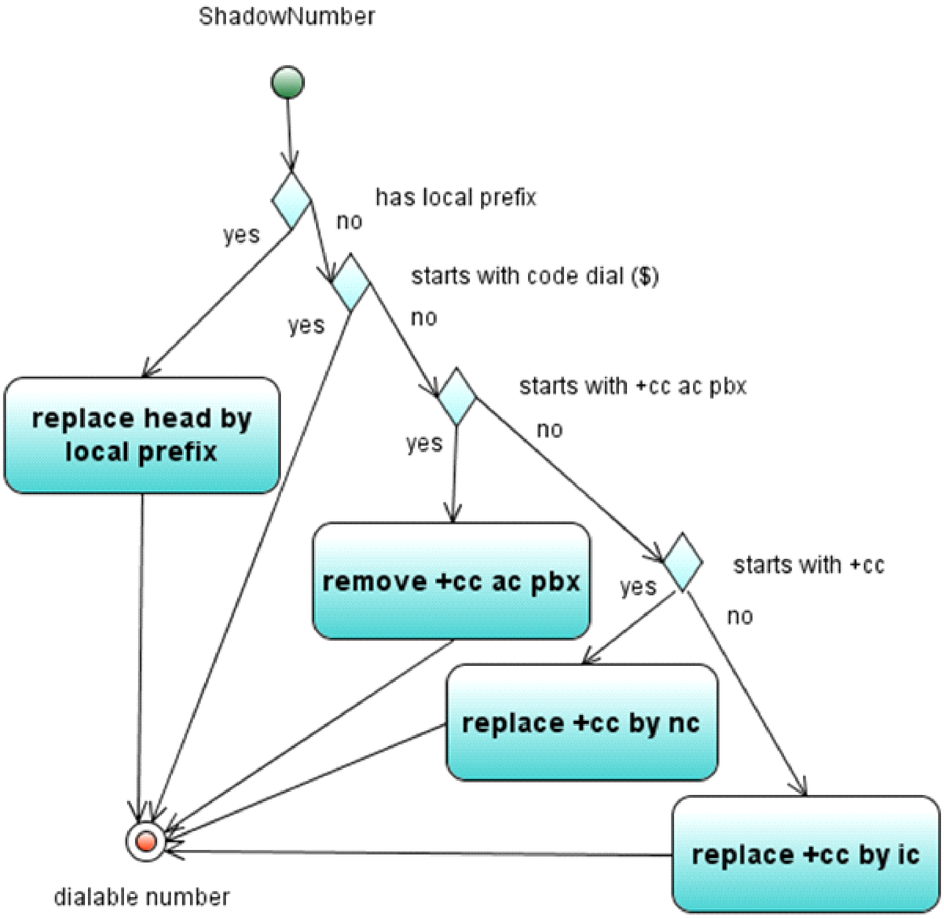
country code	49
area code	2-5 digits
local PBX	4-9 digits
station	private network, depends on PBX

National long distance call are indicated by	0
International access is indicated by	00
Total number length for DID max.	15 digits.

Normalization



Reduction


ShadowNumber
has local prefix
yes
no
starts with code dial ($)
yes
no
replace head by local prefix
starts with +cc ac pbx
yes
no
remove +cc ac pbx
starts with +cc
yes
no
replace +cc by nc
replace +cc by ic
dialable number

France

French telephone numbers (10 digits) are usually stored within an exchange database in the following format:

+33 (P)Z ABPQ-MCDU

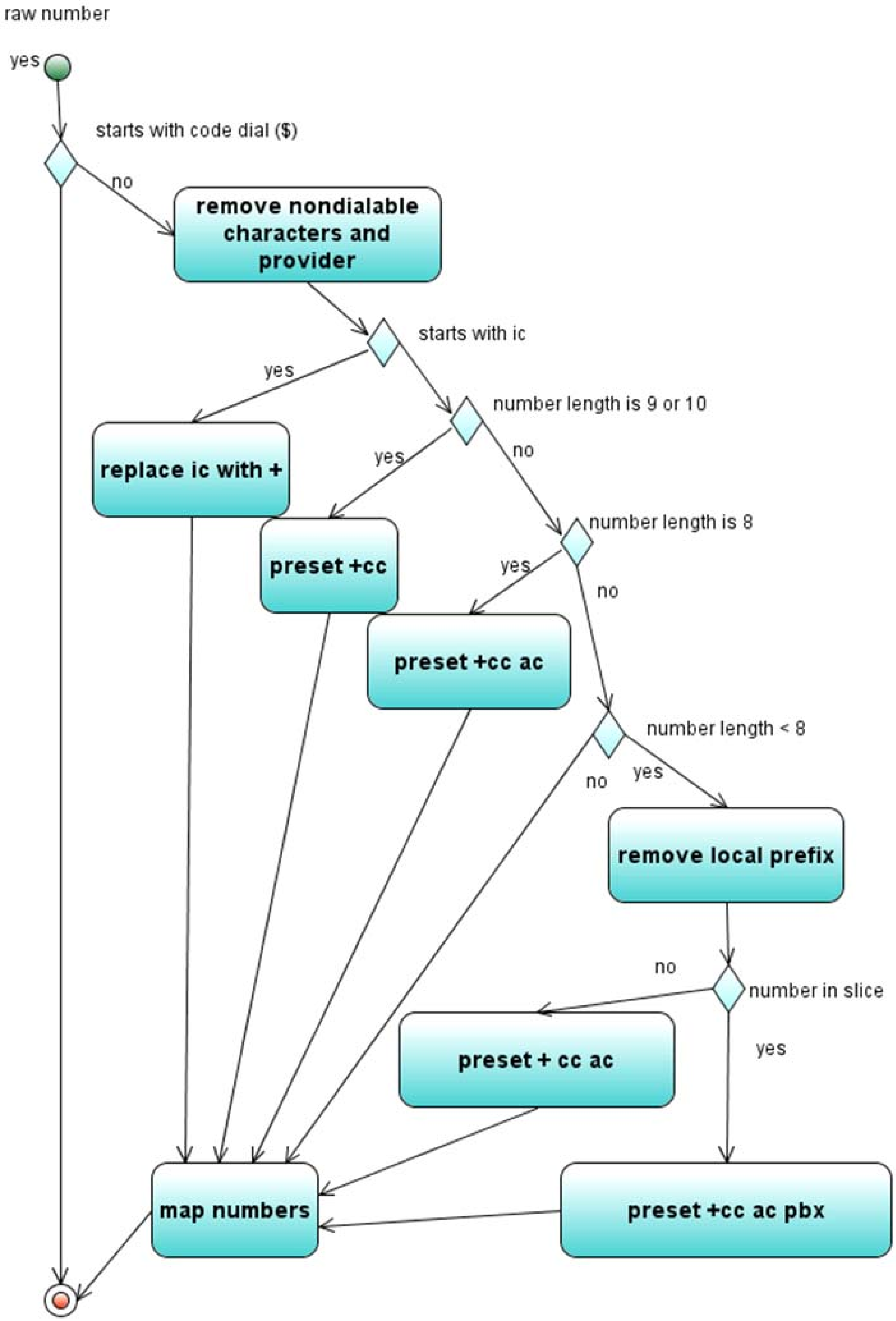
where

+33	French country code
(P)	1 digit code (put into brackets) for a provider (e.g. “0” = France Telecom)
Z	1 digit code for a region/zone within France

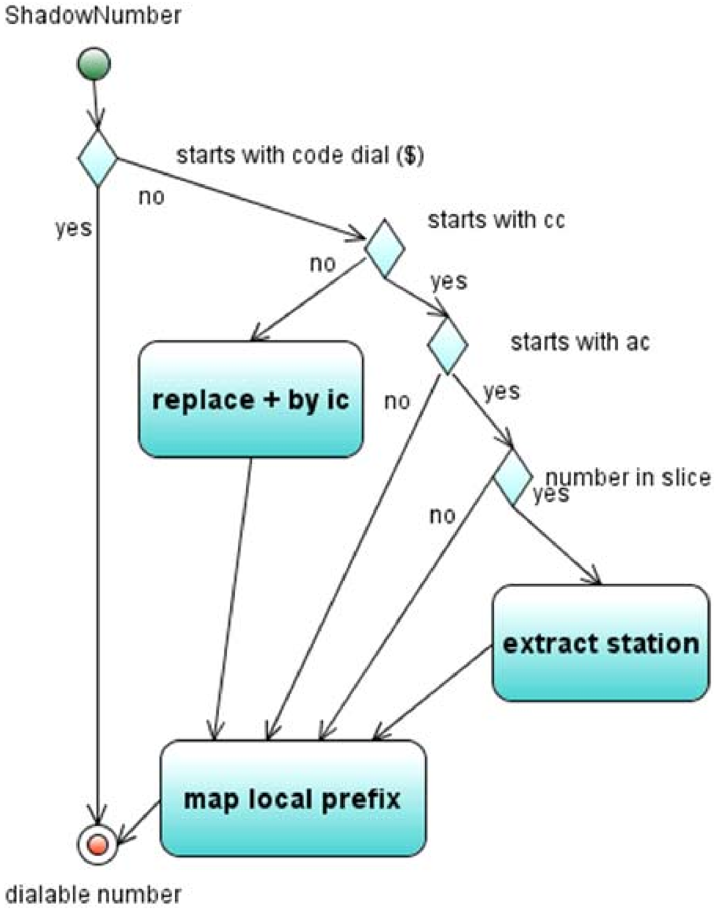
The hyphen separates the remaining 8 digits into common digits
(“ABPQ”, sometimes called "local PBX number" which may have 3, 4, 5 or 6 digits)
subscriber number
(digits unique to one customer, DID digits, “MCDU” may have have 5, 4, 3 or 2 digits)

In France subscriber numbers are allocated to customers in slices.

Normalization
(see next page)


raw number
yes
starts with code dial ($)
no
remove nondialable characters and provider
starts with ic
yes
replace ic with +
number length is 9 or 10
yes
preset +cc
no
number length is 8
yes
preset +cc ac
no
number length < 8
no
yes
remove local prefix
no
number in slice
preset + cc ac
yes
map numbers
preset +cc ac pbx

Reduction


ShadowNumber
starts with code dial ($)
yes
no
starts with cc
no
yes
replace + by ic
starts with ac
no
yes
number in slice
yes
no
extract station
map local prefix
dialable number

Examples

		French APPS1
	French Address parser parameter settings:	
	Country Code:	33
	International Code:	00
	Provider Code:	0
	Area Code:	1
	Range 1 Common Digits:	1234
	Range 1 First Subscriber No	5000
	Range 1 Last Subscriber No	5999
	Range2 Common Digits:	1234
	Range2 First Subscriber No:	9000
	Range2 Last Subscriber No:	9999
	Access code: ⓪	
	Number Reduction:	
R1	+49 69 7505 3609	⓪ 00 49 69 7505 3609
R2	+33 01 1222 5678	⓪ 01 1222 5678
R3	+33 51 1222 5678	⓪ 01 1222 5678
R4	+33 11 1222 5678	⓪ 01 1222 5678
R5	+33 01 1234 4444	⓪ 01 1234 4444
R6	+33 01 1234 5555	5555
	Number Normalisation:	
N1	+33 (0)1 1234 5678	+33 1 1234 5678
N2	+33 (5)1 1234 5678	+33 1 1234 5678
N3	+33 (0)1 1234 9999	+33 1 1234 9999
N4	+49 69 7505 3609	+49 69 7505 3609
N5	00 49 69 7505 3609	+49 69 7505 3609
N6	00 33 0 1 1234 5678	+33 1 1234 5678
N7	0 1 1234 5678	+33 1 1234 5678
N8	5 1 1234 5678	+33 1 1234 5678
N9	5678	+33 1 1234 5678
N10	9999	+33 1 1234 9999
N11	2 1234 5678	+33 2 1234 5678
N12	1347 6713	+33 1 1347 6713
N13	6713	+33 1 1234 6713

Spain

Spanish telephone numbers have 9 digits, starting either with “9”, “8” or “6”. The next two or three digits are used to identify a Spanish region (e.g. “91” = Madrid).
In Spain subscriber numbers of one PBX are allocated to customers into so-called “slices” (similar as in France).

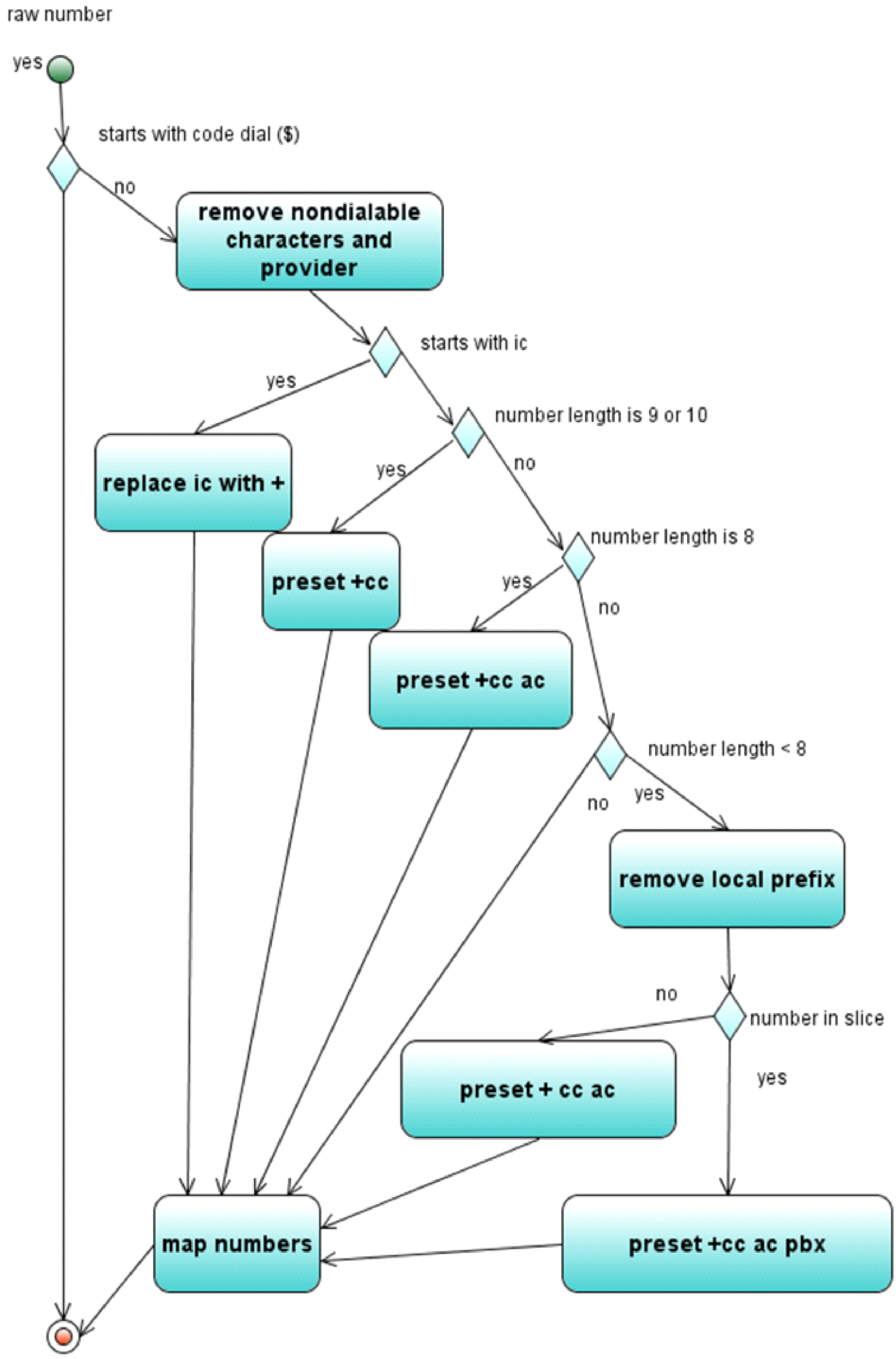
Examples

A customer may have slices:

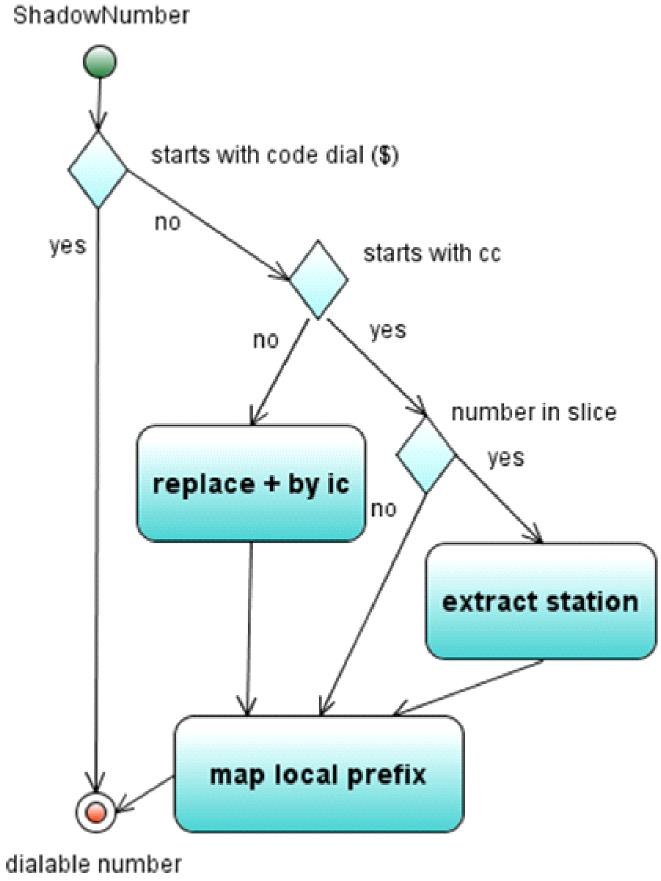
Slice A1:	912051500 to 912051599	head number 912051 stations 500 to 599
Slice A2:	913279200 to 913279899	head number 913279 stations 200 to 899
Slice A3:	914104000 to 914104199	head number 914104 stations 000 to 199
Slice 4:	914061045 to 914061046	head number 9140610 stations 45 to 46

In Spain doesn’t exist any national code or area code.

Normalization



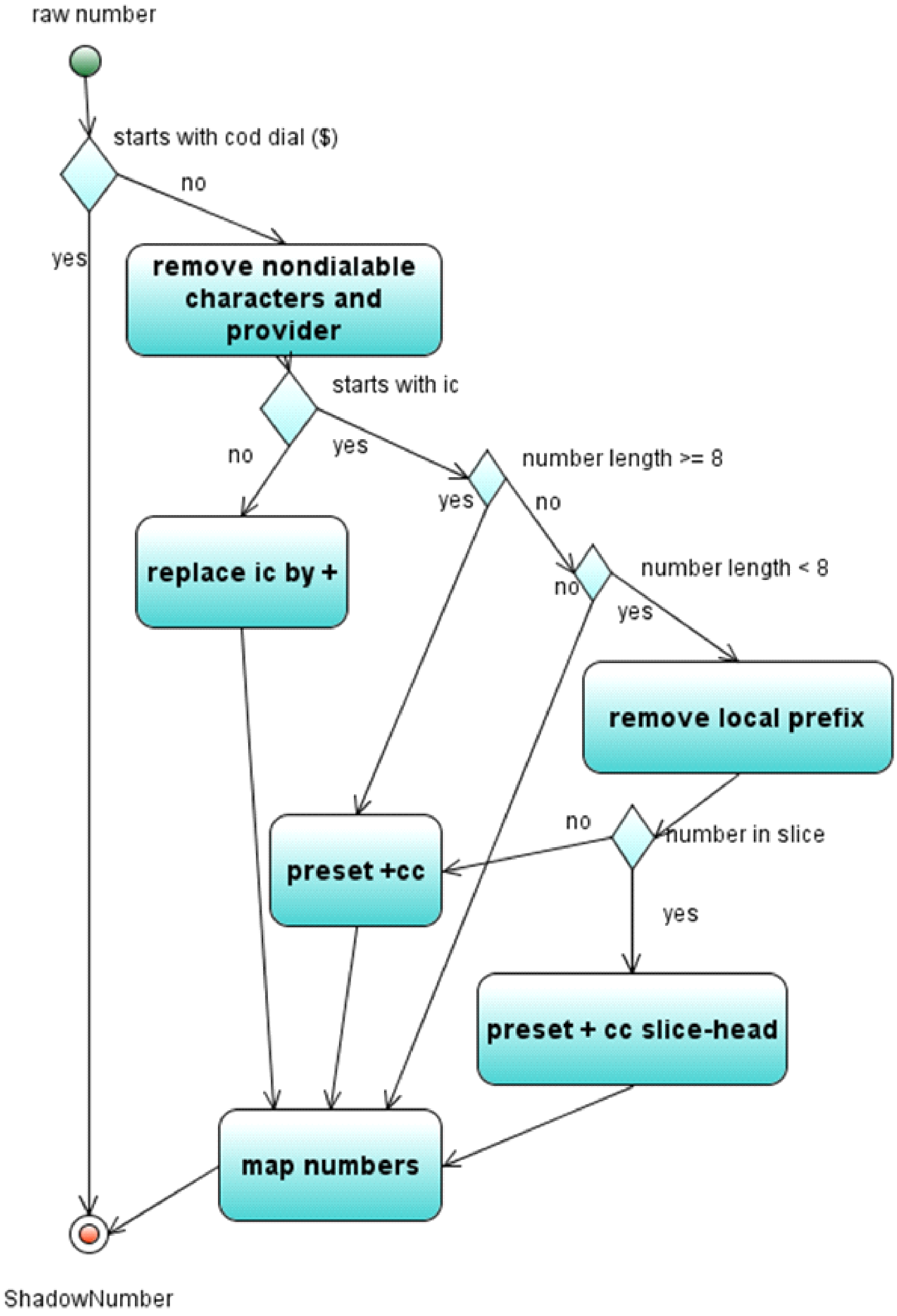
Reduction


ShadowNumber
starts with code dial ($)
yes
no
starts with cc
no
yes
number in slice
yes
replace + by ic
no
extract station
map local prefix
dialable number

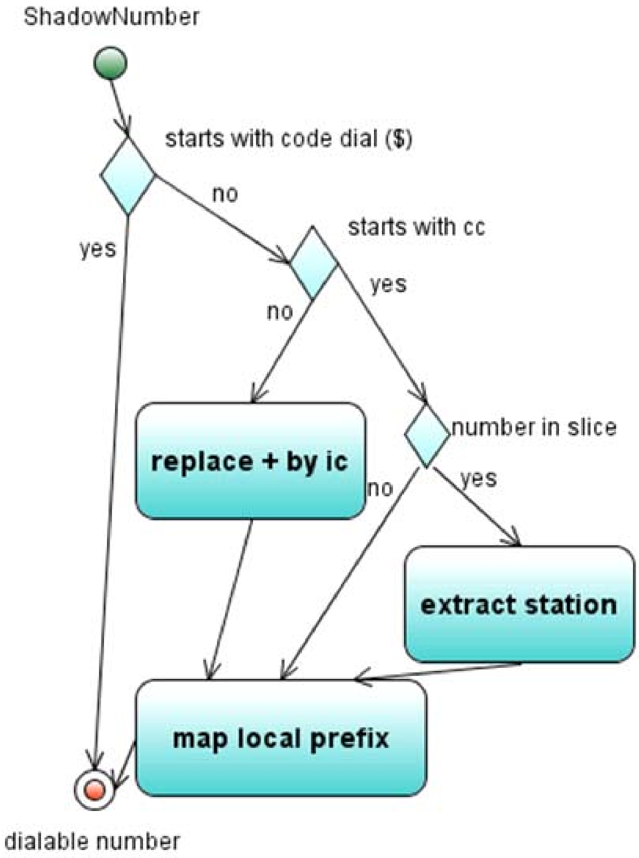
Norway

Phone numbers in Norway have 8 digits. 4 digits area code and 4 subscriber number. Area code can not be omitted.

Normalization



Reduction


ShadowNumber
starts with code dial ($)
no
yes
starts with cc
yes
no
replace + by ic
number in slice
no
yes
extract station
map local prefix
dialable number

Universal Parser

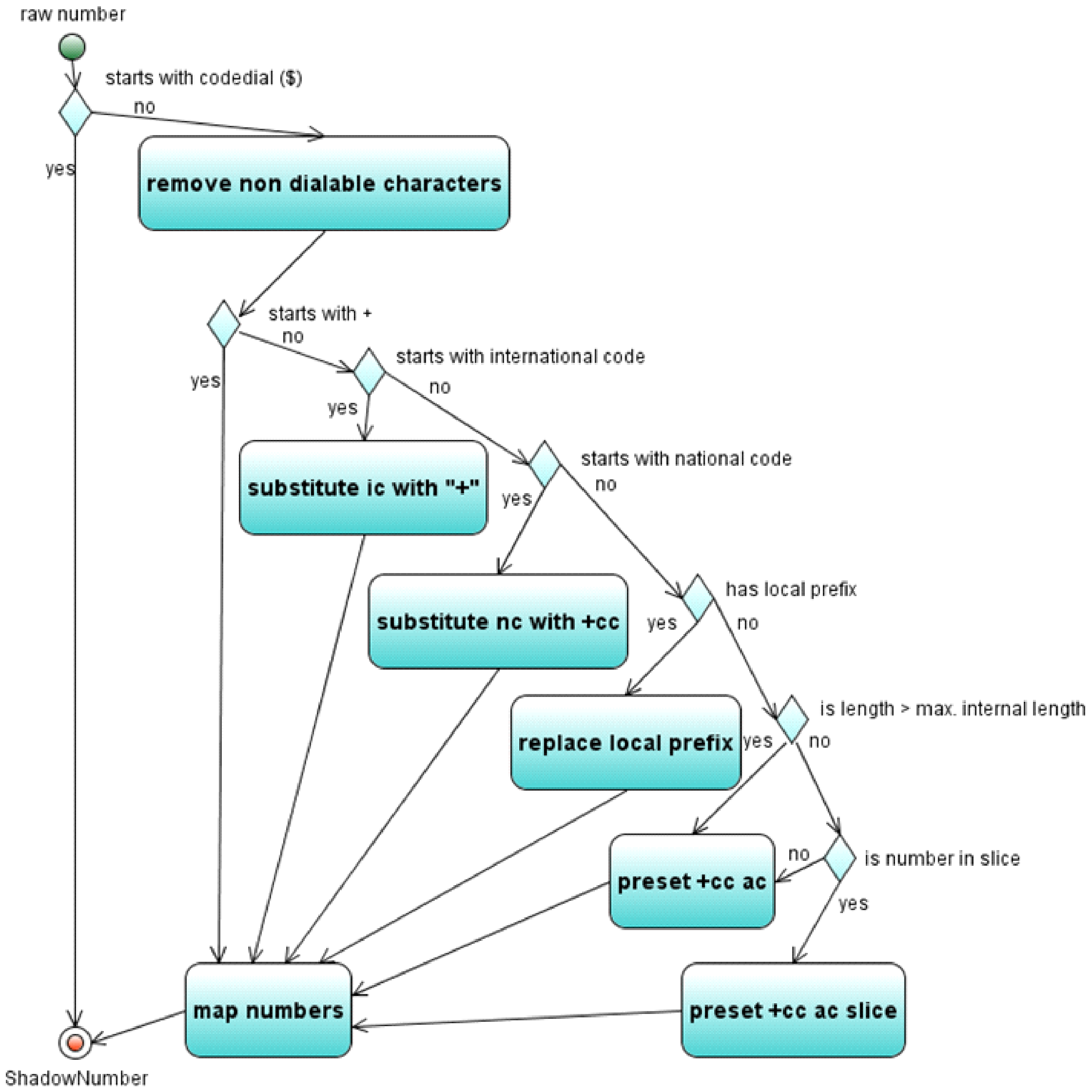
The new Universal Parser can be used for open dial plans with slices. This is e.g. in Germany in areas where free numbers are running low. It can also be used in countries like Nicaragua, Luxembourg or Iceland. The fields National and Area Code are optional and can be left empty.

The field “max. length internal” defines how long internal numbers are in maximum. This is used to detect internals if the field National is empty. If “max. length internal” is 0 the length is ignored.

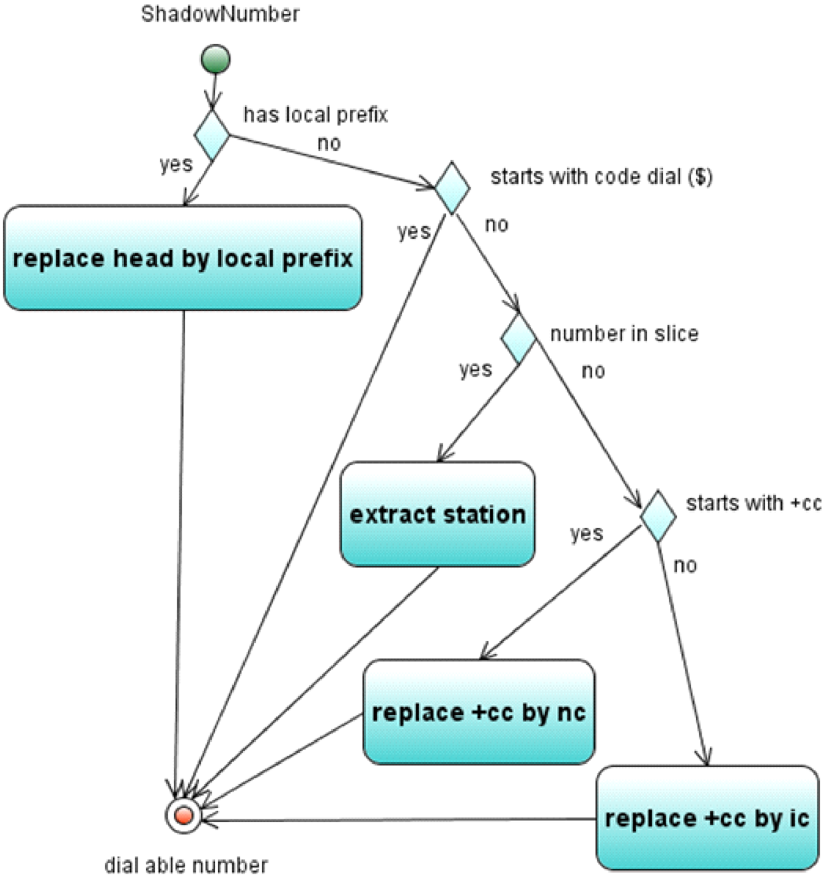
Slices defining ranges of DIDs given from the network provider. PBX-Number Start holds the beginning of the first number, PBX-Number End holds the beginning of the last number. Number of local digits defines the number of digits included in PBX-Number Start and PBX-Number End that remains to internal numbers. See examples.

Number mapping and local prefixes are also supported

Normalization

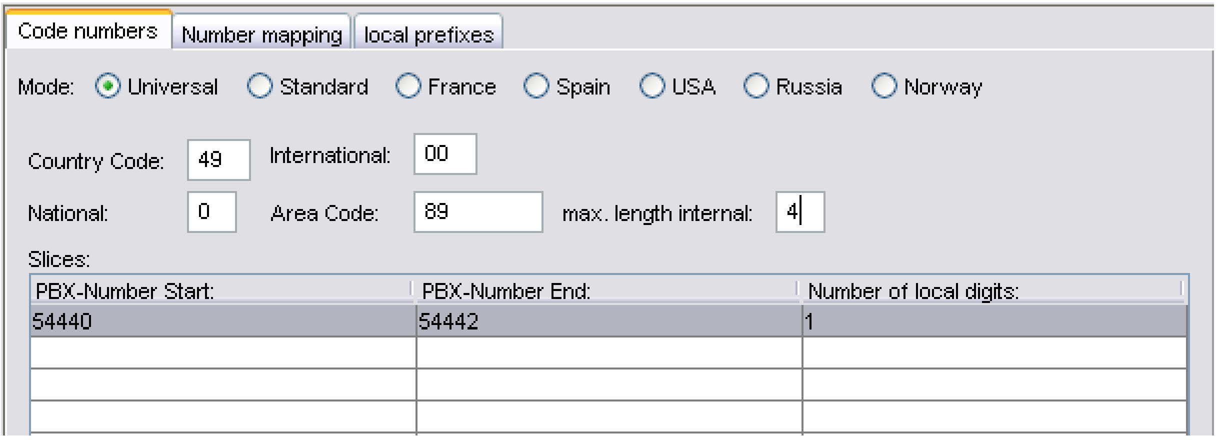


Reduction


ShadowNumber
has local prefix
yes
no
replace head by local prefix
starts with code dial ($)
yes
no
number in slice
yes
no
extract station
starts with +cc
yes
no
replace +cc by nc
replace +cc by ic
dial able number

Examples

Open numbering plan with slices



Mode: ● Universal ○ Standard ○ France ○ Spain ○ USA ○ Russia ○ Norway

Country Code: 49 International: 00

National: 0 Area Code: 89 max. length internal: 4

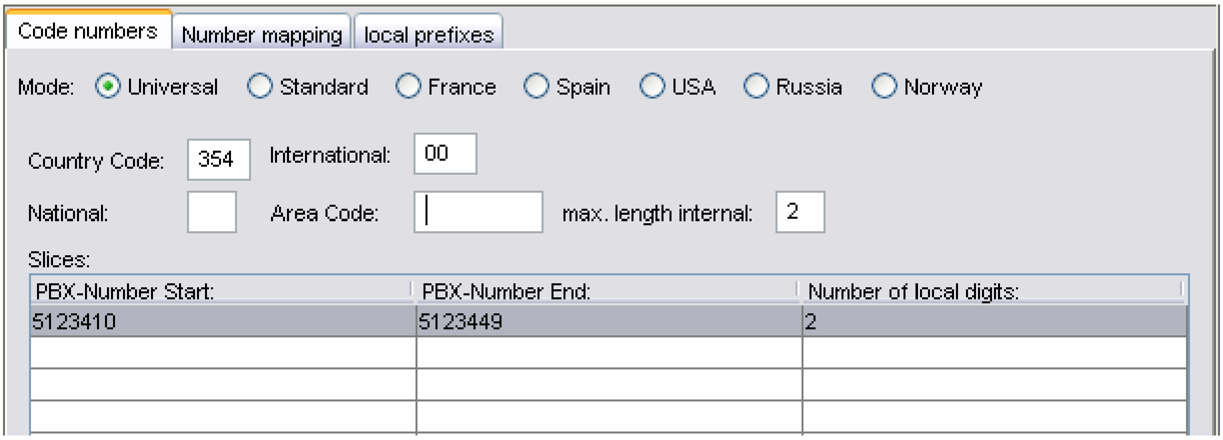
Slices:

PBX-Number Start:	PBX-Number End:	Number of local digits:
54440	54442	1

This example defines numbers from +49 89 5444 **0** to +49 89 5444 **2**999. The last one digit of PBX-Number Start defines the lowest digit an internal number can start with. The last one digit of PBX-Number End defines the highest digit an internal number can start with. The length of internal numbers can vary from 1 up to 4 digits.

Displayed number	ShadowNumber	Dialable number	Dial external	Comment
10	10	10		
2500	2500	2500		
089 5444-5000	+498954445000	08954445000	X	5000 is not in slice, so it is external
25000	+498925000	08925000	X	25000 is longer than max. internal length, so it is external
+49-69-7505-5000	+496975055000	06975055000	X	National long distance call

Iceland, Luxembourg, Nicaragua and others



Mode: ● Universal ○ Standard ○ France ○ Spain ○ USA ○ Russia ○ Norway

Country Code: 354 International: 00

National: Area Code: max. length internal: 2

Slices:

PBX-Number Start:	PBX-Number End:	Number of local digits:
5123410	5123449	2

This example shows the usage in countries with no national code and no area code and. The range of numbers contains 40 DIDs from +35451234**10** to +35451234**49.**

Displayed number	ShadowNumber	Dialable number	Dial external	Comment
10	10	10		
5123410	+3545123410	10		
+3545123450	+3545123450	5123450	X	50 is not in slice, so it is external
+49-69-7505-5000	+496975055000	00496975055000	X	National long distance call

Tools: one-X Attendant

A separate sheet is displayed in the tree view for each one-X Attendant client that has connected to the database at least once.

The selected sheet consists of two table columns. The Property Name and

Property Value columns let you edit the properties.

Buttons / Check

The **Save** button saves the changes to the database.

The **Check** button checks only the *EJBSrvHostName* and *EJBSrvPortNo* parameters.

If a check fails, the entry responsible is highlighted in red. Once this entry is corrected, it is displayed in black again.

Note on parameter NBVServer

This parameter determines which server will be used for the network-wide busy display.

„No = no server will be used

„SVA Manager = Operation over SVA Manager

„Presence Server“ = Operation over Presence Server

3rdPartymodeWithCIE	3rd party connection to BCC/CIE (0 = OFF (default), 1 = ON)
AnswerOnVKADD	+ key for querying in the standard phone window (0 = OFF (default), 1 = ON)
AssignOnDial	Assign a caller to a line which is currently in Dial status (0 = OFF, 1 = external calls only, 2= external and internal calls (default)
AutoStartFeatureCM	(0 = OFF (default), 1 = one-X Attendant will *not* send an “Attendant Start” signal to the
CalendarInterval	Interval for refreshing data from the Lotus Notes/Outlook calendar (min, default = 10)
CalendarUsage	Calendar function (No, Yes, Without password request) "Without password request" means that one-X Attendant isn't asking for the Lotus Notes password after login to the client. If this option is chosen and Lotus Notes started with the setting "File/Security/User Security/Don't prompt for a password from other Notes-based programs", no password is necessary to get the calendar information. Without the Lotus Notes setting, Notes will prompt for the password.
CallTransfDelayTime	Delay time for Dial & Assign operations (msec, default = 1000)
CFABActive	CallFromAnsweredBy-Criteria for detection of external call numbers (0=Off (Default) 1=On) see document ExternalCallDetection.pdf
ClearSearchOnNewCall	Clears the search screen in the phone book when a new call comes in 0 = OFF (default), 1 = ON
CutOnBusyTransfer	In case of a busy line the focus is on Clear in the calling card to be assigned (0 = OFF (default), 1 = ON)
DelayTimeCMUnpark	Delay in milliseconds between the dial of the unpark FAC and the unpark extension (only CM variant), (Default=0)

EJBSrvHostName	EJB server PC name (phone book server) (Default = “localhost”)
EJBSrvPortNo	EJB server port number (phone book server) (Default = 21099)
ExtNumberDigits	Call number length criteria for detection of external call numbers (0=Off, (Default)). See document ExternalCallDetection.pdf.
ForceBlockdialCM	When using block dialing, e.g. using a destination key, the CM sends the number immediately without waiting for further inputs (0 = OFF (default), 1 = ON)
GlbSearchFilterField	Prefilter for topic calls (all phone book fields listed; default = none
ImExportTransferMode	Codepage format of the ex/imported phone book data (0=Default Codepage, 1=ISO 8859_1, 2=UTF 8, 3=UTF 16 BE, 4=UTF 16 LE, 5=UTF 16)
IM Port	Instant Messaging Server Port (Presence Server: Port 5223)
IM Server	FQDN of Instant Messaging Server (Presence Server)
KeepAliveTimerSVA	Keep alive timer in milliseconds between 1XAttd and SVA Manager for NBV (CM+IE) and call/redial list (IE) (DEFAULT 0 = turned off)
KeepAliveTimerDB	Keep alive timer in milliseconds between 1XATTD ckient and database searches during calls if database is not reachable (DEFAULT 20000 / 0 = DEFAULT)
NbaPumDefault	Default size configuration for network–wide busy display (Default = 2000)
NBVServer	Operate with SVA Manager or PresenceServer (No, SVA Manager, Presence Server)
NoCallIdentification	Controls number identification (0 = number identifcation on incoming and outgoing calls (default), 1 = no number identification, 2 = number identification only for incoming calls, 3 = number identification only for outgoing calls)
OffsetSACSignalling	Offset for send all calls signalisation (Default:0)
OSType	OS hardware (“ACM”)
OSSoftwareVersion	OS software version “02.01” (Default), “02.00”, “01.51”, “01.61”)
PUMLOgginTimeout	Wait time for the PBX answer for PUM user logon (sec, default: 5)
SearchDelayTimeCC	Search delay time for the calling card (msec, default = 400)
SearchDelayTimeST	Search delay time for the lookup table in the phone book (msec, default = 150)

SearchNumberHead	Head number search (0 = OFF(default), 1 = ON) If turned on (in configtool): if the headnumber(s) of the trunk line(s) of an external caller is entered in the phonebook to identify the company and a user of that company calls in, the name of the company will be displayed if that user number is not in the phonebook. If present in the phonebook the exact name of the user is displayed. If turned off: the exact name of the user is displayed if present in the phonebook.
ShowEmoticons	Show Icons/Symbols for Call Types in operator window (0 = OFF, 1 = ON (Default))
ShowSubstituteRemark	Display substitute text as the topic (0 = OFF (default), 1 = ON)
SVAHostNameIPL	SVA Manager PC name for call control (not used in CM version)
SVAMHostName	SVA Manager PC name for NBA (Default = „localhost“)
SVAMPortNo	Port number of the SVA Manager for NBA (Default = 6006)
SVAMPortNoIPL	Port number of the SVA Manager for call control (not used in CM version)
SystemLanguage	System language (Default = “system_language”, e.g. en)
TransferOnBusy	Can be assigned to busy subscriber; no effect if one-X Attendant is connected to ACM (1 = ON (default), 0 = OFF)
TTracePortNo	TTrace server port number (Default = 10300)
TTraceHostName	TTrace server PC name (Default = “localhost”)

Tools: JOnAS (phone book server)

Buttons

The **Save** button saves all changes and configures all available clients accordingly.

The **Restart JOnAS** button stops the service and restarts it with the changes settings. The following table explains the text boxes and check boxes.

Note:

When you have restarted JOnAS, you also need to restart all related services, such as AbsenceInfoPusher, WebAccess and Update Service.

	Server
Registry Port	Port on which the phone book server listens. Default = 21099
Remote Object Port	Port which should be used to transfer the search results to the one-X Attendant. Define a porthere if a firewall is installed between one-X Attendant and the phone book server. (Default=0,i.e. dynamic)
Transaction timeout	Timeout in seconds, the maximum time that the processing of a search query may last. Default = 120
	Cache
Cache active	Select if you want to cache the search results. This can speed up a new search.
limit	Select if you want to restrict the memory for the cache.
max. size(number ofRecords)	The search result size entered here will not be exceeded. The oldest entries in the cache will bedeleted when more recent entries are to be written to the cache. The recommended max. size is 10,000 records.
	Search result
Search result-size	Number of records transferred from the server to one-X Attendant when a search returns moreresults. Default = 50
Search resulttimeout	The timeout time in seconds for which a search result remains valid on the server. Records thatare not queried are discarded after the timeout. Default = 240

Settings for large Databases

If you run one-X Attendant with a large database (> 5000 records) or if it is linked to large databases, you must assign JOnAS more memory. You can do this when you configure the JOnAS service (Avaya Phonebook Server) in the **wrapper_ext.conf** file.

1. Open the **wrapper_ext.conf** file in a text editor. It is located in: c:**\avaya\servers\serviceconf\**
2. Find the line “wrapper.java.maxmemory” in the wrapper properties.
3. Change the default-value from 64 (which means 64 MB) as required. 136 MB is enough for 15,000 records.
4. It may also be necessary to change the default time for transaction timeout. You can do so using the one-X Attendant config tool on the JOnAS tab. We recommend increasing the time to 300 seconds.

Tools: Phone book

A separate sheet is created for each data source. You can define data sources and configure the field assignment using an index definition on the sheet.

For examples of connecting to different data sources, see LDAP connection.

Connection tab

The **Reload** button discards the last changes, reloads the settings from the one-X Attendant database and runs the SQL statement. However, *no* data is loaded into the one-X Attendant database!

The **New** button creates a new data source and populates the fields with default values.

The **Save** button checks the settings and saves the configuration data in the one-X Attendant database

.The **Delete** button deletes the active data source. If a data source is deleted, all records of that data source are automatically deleted at the same time.

The **Remove records** button deletes all records of the data source just selected from the database.

Name and Description

The *Name* and *Description* fields describe the data source. The name is needed to uniquely identify a data stream. The name appears in the combo box of the one-X Attendant phone book.

Drivers

The field *Drivers* contains a list of the available JDBC drivers. The driver displayed is loaded. The list can be added to in the one-X Attendant- ConfigTool.properties file. If you select a driver from the list, the *Provider URL* box is populated with the corresponding URL schema by default.

The name of the JDBC database driver can be found in the database documentation or the driver documentation (e.g. for a JDBC-ODBC bridge it is sun.jdbc.odbc.JdbcOdbcDriver).

Provider URL

The *Provider URL* field contains the connection parameters. The URL points to the database to be connected, and has the following format:

jdbc:<subprotocol>:<subname>

subprotocol refers to the JDBC class with which you are working (e.g. for a JDBC-ODBC bridge, this is odbc).

subname provides information that is needed to locate the database (e.g. for a JDBC-ODBC bridge, this is a DSN from the ODBC data sources). The syntax of subname is dependent on the driver and can be found in the documentation for the

database or the driver.

For SYBASE, this information is in the SYBASE

manual.

User

Shows the *user* for the database.

Password

Shows the *password* for the database as “*”

SQL statement

The *SQL statement* field contains the SQL query used to retrieve the data from the data source.

Transaction timeout

The *Transaction timeout* contains the time in seconds after which a hanging transaction is ended if necessary. This information is also important for updates. The maximum value is 3600 seconds.

Commit Transaction

If a transaction takes longer than 1 hour it will automatically be canceled.

With the option ”Commit Transaction” you can configure the number of records, according to which the transaction is automatically confirmed (committed).

Then begins a new transaction and the timer can not strike if the number is selected small enough. This configured automatic ”commit” has the disadvantage that the final data will be stored into the database and if an error does occur the original state can‘t be restored.

A value of ’0’ disables the automatic ’Commit Transaction’.

Result (gray display window)

The *Result* field contains messages which give an indication of any possible errors.

Assignment tab

Index

The *Index* column selects the fields of the data source which make a record unique (the primary key).

one-X Attendant needs a primary key to be able to work with the customer data. This primary key can be the primary key of the customer database. You can also use several fields as the primary key. This is referred to as a composite primary key. one-X Attendant uses this primary key for the shadow database. **Caution**: None of the elements of the primary key can be blank for any of the records!

Source field

The *Source field* column contains all the fields read out of the database.

Target field

The *Target field* column contains the assigned destination fields of the one-X Attendant phone book.

All the fields which are defined in the one-X Attendant phone book are possible!

The fields are displayed in the language of the one-X Attendant configuration tool collection.

For the “Gender” field the source value must be “m” or “M” for male, and “f” or “F” for female. All other values will be interpreted as undefined.

CM Name (last name, first name)” isn’t a real phone book field. If you choose this as target field and the content of the source field has the format (last name, first name), then it will be split into the phonebook fields (last name) and (first name). This will be usually used for importing data from text files which are created via Avaya Site Administration (ASA) export.

CSV Import

The driver jstels.jdbc.csv.CSVDriver2 is used for the import of the CSV data.

In this case the URL has the following format: jdbc:jstels:csv:<Enter directory here>?separator=;&charset=utf-8

Parameter:

- <Enter directory here> Enter here the directory(incl. path) where the CSV-file located. The directory has to be on a local drive, otherwise the update service has to be started with a different account which has access to the corresponding network drive (See Control Panel\Adminstrative Tools\Services\Avaya Phonebook Server – UpdateService\Properties\Log On)
- separator Enter here the character with which the data are separated in the file (default=;)
- charset Enter here the character set with which the file is coded (default=utf-8)

SQL Statement

- Use as tablenam the name of the file without extension; the file has to have always the extension “txt”.

If you want to import stations and/or agents from CM, look for the chapter “Importing CM Station and Agent Data to one-X Attendant Phone book cyclically” in the appendix.

Tools: Update service

The update service connects the external data sources (Exchange, Domino) with the phone book server (JOnAS). A separate sheet is created for each data source that was created in the phone book. One click on a sheet opens the associated settings in the work area.

Data sources that do not have an enabled update service are not listed in one-X Attendant as data sources. **Caution:** Records from these data sources are nevertheless found when you search for all data sources!

Buttons

The **Save** button saves configuration data in the one-X Attendant database.

This data only becomes active after the update service has been stopped

and then restarted.

The **Check connection** button tests whether the data sources can be reached by the update service.

The **Start** button launches the update service. The **Stop** button stops the update service.

Check connection To check the connection, proceed as follows:

1. Enter a new free **Test Port**.
2. Save the new setting with the **Save** button.
3. Stop the update service with the **Stop** button.
4. Start the update service again with the **Start** button.
5. Test the connection using the **Check connection** button.

If necessary, you can read the results of the test in the **updateservice.log** logfile in the server directory Avaya**Servers**.

Tester/Services

Host

Name of the host on which the update service is installed.

Test Port

TCP server port of the update service.

Information for each database

Earliest run

(date, time)

The *Earliest run* (*date, time)* fields define the earliest time that the update service should start.

Interval	The *Interval* fields define the how often the update service should run (value and unit).
Activated	In the *Activated* check box, each database must be selected which should participate in the update service.

Tools: WebAccess

Buttons / connection testing

Lets you test whether the Web server (Tomcat) connects correctly to the phone book server (JOnAS).

The **Check connection** button checks whether the Web server connects correctly to the phone book server (JOnAS).

Save saves configuration data in the one-X Attendant database. This data is only active when the WebAccess is stopped and then restarted.

The **Start** button launches the WebAccess service. The **Stop** button stops the WebAccess service.

Host

Name of the host on which WebAccess is installed.

Web server port

Port on which the WebAccess is listening

Note

You need to specify the Web Server Port if you are using AIS or applying the absence displayvia a browser.

Tools: External Call Detection

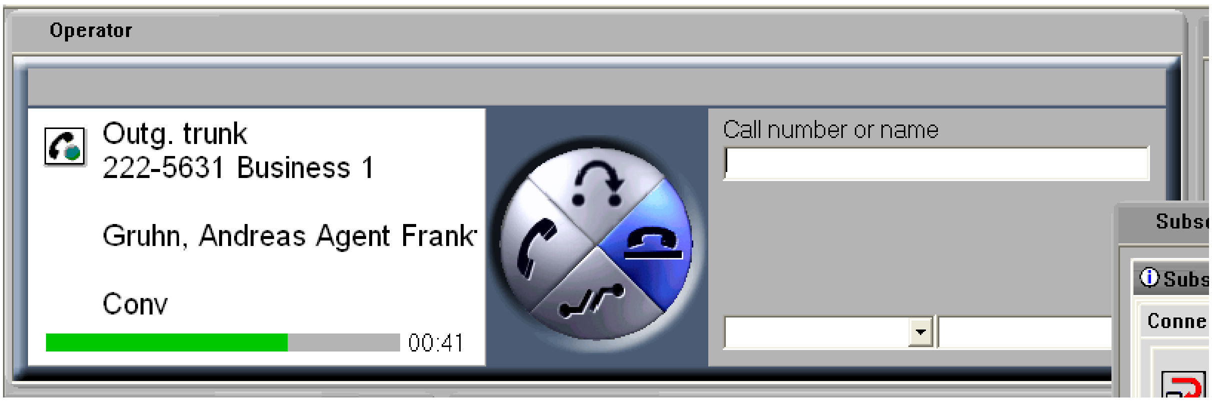
Motivation:

Avaya one-X Attendant Service and Installation Manual shows in chapter 1 the block diagram of one-X Attendant at CM. Scapi is the signalling interface between one-X Attendant client and CM. Scapi is an Api designed for Avaya SoftConsoleanother Avaya attendant. It doesn't provide direct Information whether a call is external or internal. For this reason one-X Attendant uses different indications in the from Scapi received events. The following chapters describe these indication and possible problems

One-X Attendant uses external number detection basically for redial and call list.

Because Scapi doesn't provide the ARS Code for public network with external numbers, one-X Attendant has to add this code for outgoing calls.

Operator Window



Outg. trunk
222-5631 Business 1

Gruhn, Andreas Agent Frank

Conv

Figure 1: one-X Attendant Operator Window showing an external call

The operator window of one-X Attendant GUI displays, whether an outgoing call is internal or external.

As shown above, the call number is marked “external” (by displaying the text label “Outg. Trunk”) because the following optional criteria has been configured with one-X Attendant GUI:

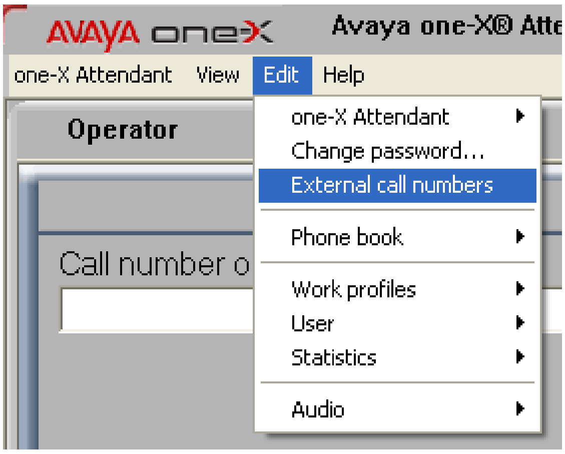
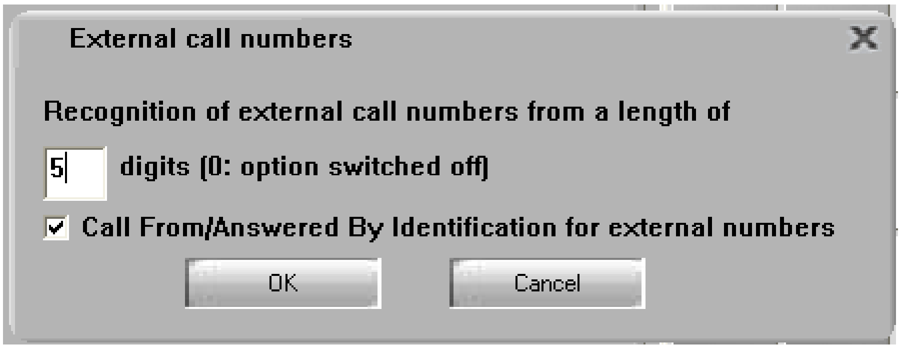


Figure 2: one-X Attendant menu item for external call numbers



External call numbers

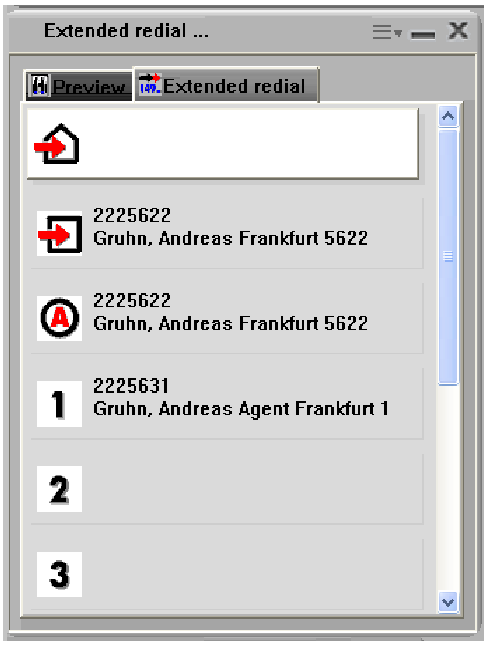
Recognition of external call numbers from a length of

5 digits (0: option switched off)

☑ Call From/Answered By Identification for external numbers

Figure 3: one-X Attendant configuration dialog for external call numbers

Extended Redial List



2225622
Gruhn, Andreas Frankfurt 5622

2225622
Gruhn, Andreas Frankfurt 5622

1 2225631
Gruhn, Andreas Agent Frankfurt 1

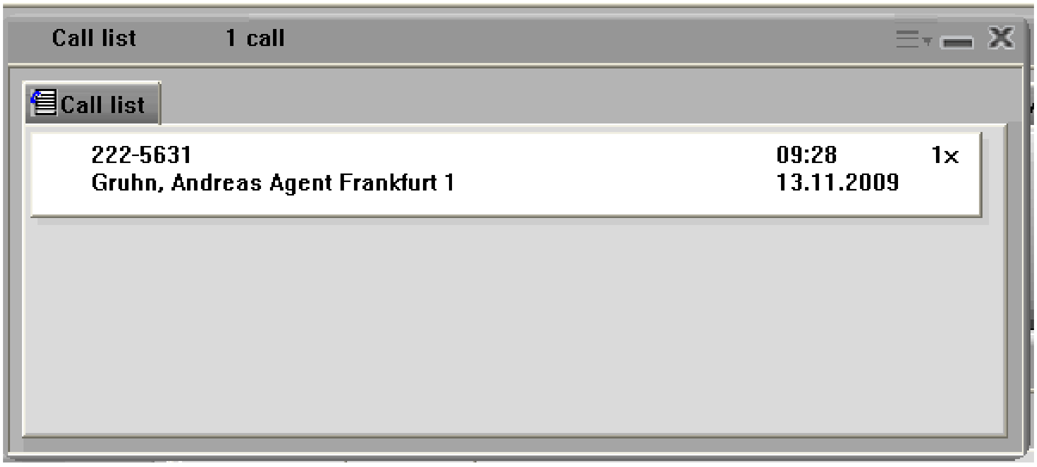
2

3

Figure 4: one-X Attendant Extended Redial List

A call number is marked external or internal in the extended redial list. A double click on the call number dials the ARS Code for public network in front of the call number in case of an external call.

Call List



222-5631 09:28 1x
Gruhn, Andreas Agent Frankfurt 1 13.11.2009

Figure 5: one-X Attendant Call List

A call number is marked internal or external in the call list (OneX-Attendant GUI doesn’t show it). A double click on the call number dials the ARS Code for public network in front of the call number in case of an external call and operator window shows “Outg. trunk”.

Hint:

All other dialing possibilities (net wide busy view, phone book, etc.) are handled with the Address Parser, that is handled in an extra chapter.

Criteria for external call detection in OneX-Attendant v3

Processing of incoming calls by one-X Attendant connected to CM

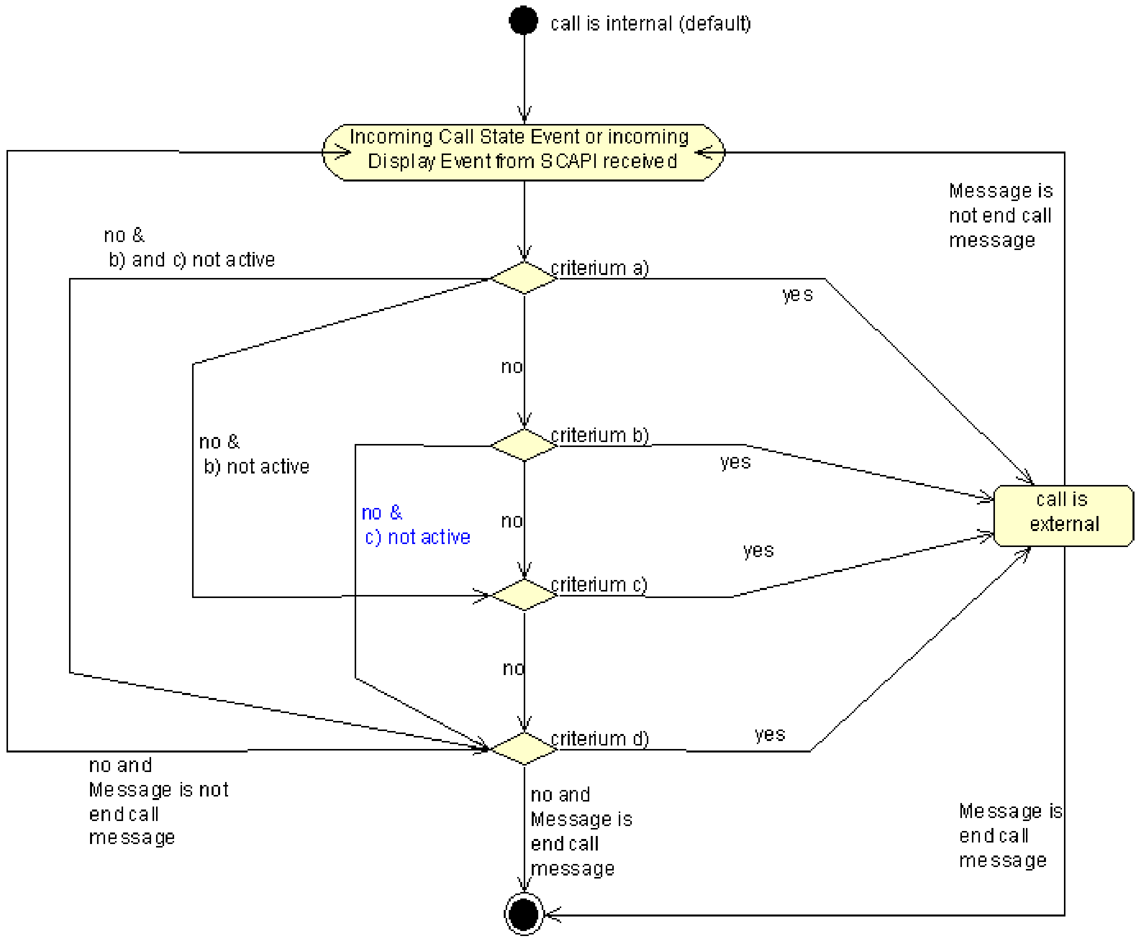
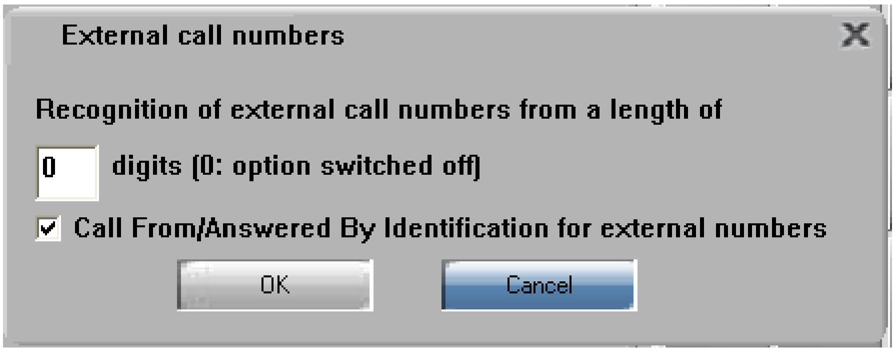

call is internal (default)
Incoming Call State Event or incoming Display Event from SCAPI received
Message is not end call message
no & b) and c) not active
criterium a)
yes
no
criterium b)
no & b) not active
yes
no & c) not active
no
yes
criterium c)
call is external
no
criterium d)
yes
no and Message is not end call message
no and Message is end call message
Message is end call message

Figure 6: one-X Attendant state machine for processing of incoming calls

The critera a) to d) shown above work as follows:

serial call criteria: calls with „sc“ as call type in display string received from Scapi (attendant serial calls) are marked as external (not configurable).

Incoming calls with call number length of the remote calling party greater than or equal to the in One-X Attendant menu for external call numbers configured number. are marked as external. “0 digits” means switch-off this criteria:


External call numbers

Recognition of external call numbers from a length of

0 digits (0: option switched off)

☑ Call From/Answered By Identification for external numbers

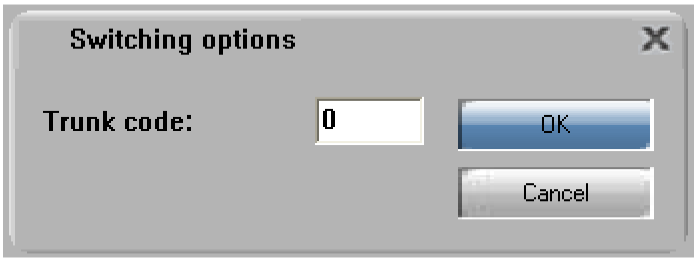
Figure 7: one-X Attendant configuration dialog for external call numbers

Checkbox “Call from/Answered By …” criteria: incoming calls with “call from” or “answered by” identification in display string are marked as external. This criteria is configurable simply by checking or unchecking it. (see Figure 7)

Incoming calls with „ldn“ identification in display string (ldn = long distance calls on DID trunks) are marked as external. This criteria is not configurable.

Processing of outgoing calls by one-X Attendant connected to CM

In addition to criteria for incoming call listed above, outgoing calls are marked “external”, if the ARS code for public network is dialled in front of the number call (i.e. in operator window). This criteria is configurable for a choosen one-X Attendant work profile.


Switching options

Trunk code: 0

Figure 8: one-X Attendant Switching Options dialog

The ARS code “0” configured in the figure above is automatically dialed in front of the call number in case

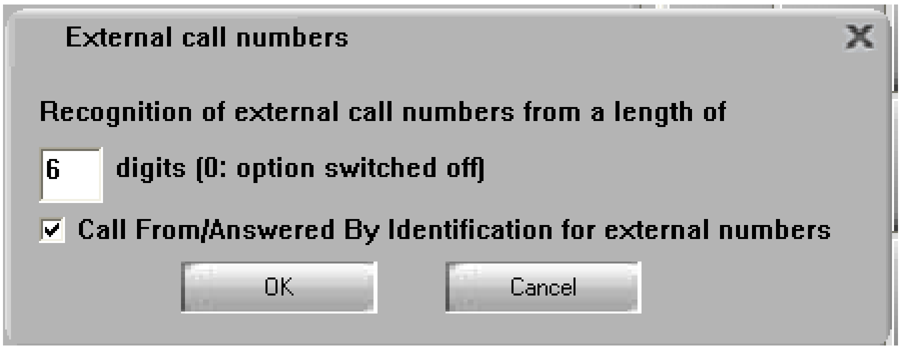
dialing an external number out of call list (see Figure 5)

dialing an external call number out of redial list (see Figure 4)

of an assigned dialed number or a block dialed number begins with “+”(i.e. out of phone book or NBA)

Example

The following example shows how criteria b) for incoming calls can influence the external call detection. Assume that “6” is the length configured as minimum length of external numbers and “0” is the configured ARS code:



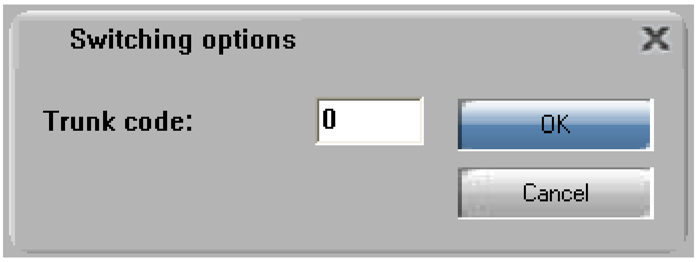
External call numbers

Recognition of external call numbers from a length of

6 digits (0: option switched off)

☑ Call From/Answered By Identification for external numbers

Figure 9: Example showing wrong external call number configuration

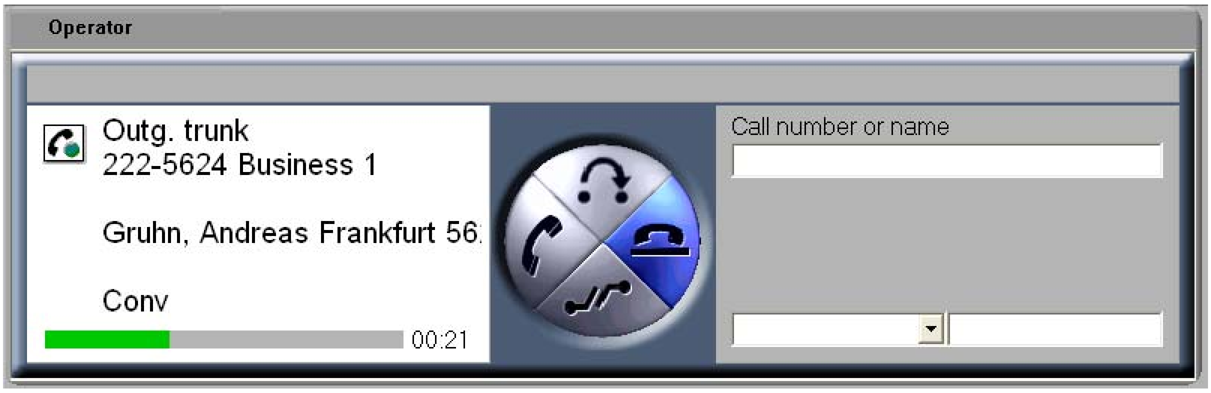


Switching options

Trunk code: 0

Figure 10: Example showing Switching Options configuration

Now we call an internal station via QSIG connection:



Operator

Outg. trunk
222-5624 Business 1

Gruhn, Andreas Frankfurt 56

Conv

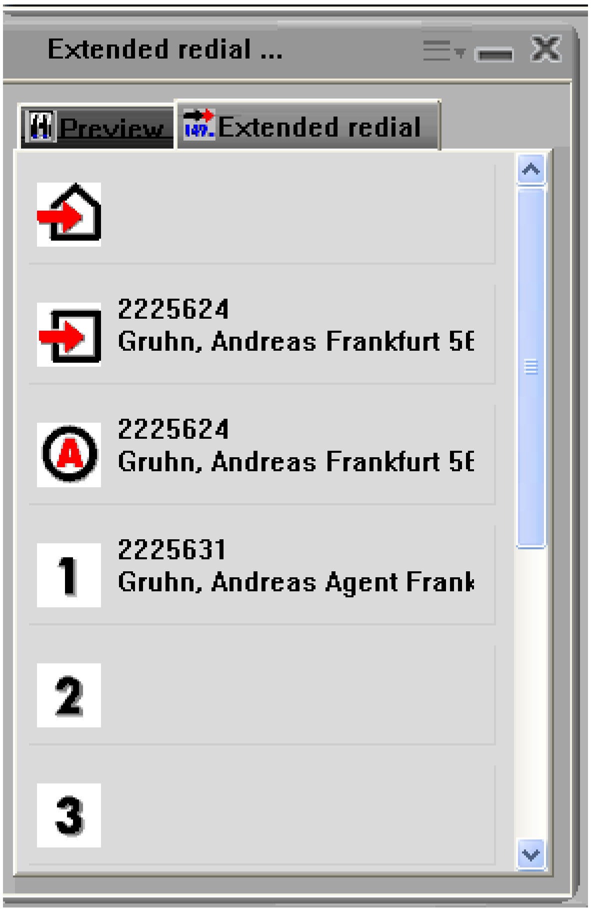
00:21

Call number or name

Figure 11: Example showing Operator Window

In the operator window, we see text label “Outg. Trunk” which classifies this call as external.

In the redial list we see that the called number has been added:


Extended redial ...

Preview | Extended redial

2225624
Gruhn, Andreas Frankfurt 5E

2225624
Gruhn, Andreas Frankfurt 5E

1 2225631
Gruhn, Andreas Agent Frank

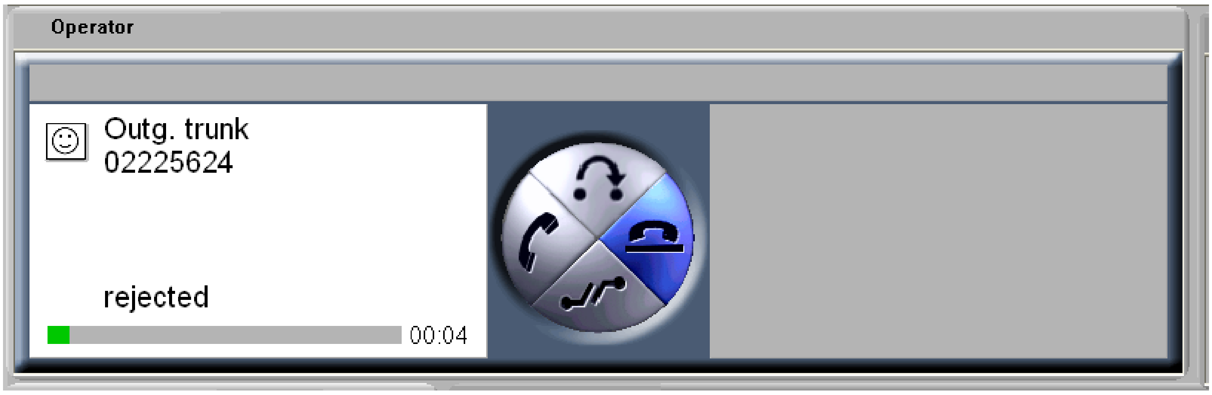
2

3

Figure 12: Example showing Extended Redial List

Now we double click on that number to dial it out of redial list.

In the operator window we obtain the following:


Operator

Outg. trunk
02225624

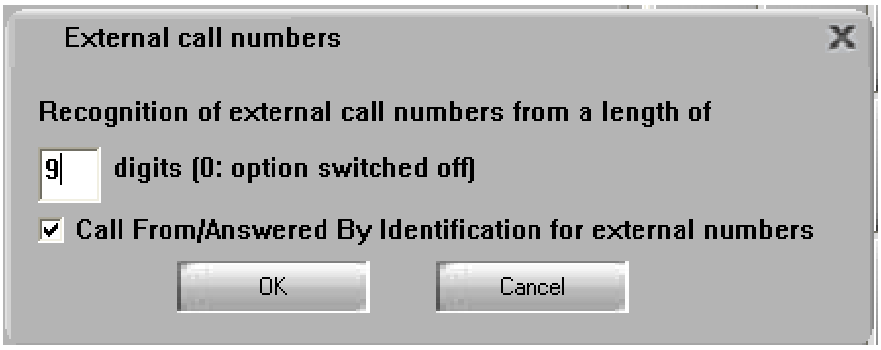
rejected

00:04

Figure 13: Example showing rejected call in Operator Window

The oneX-Attendant has added the above configured ARS code, because the call was marked external in redial list.

Now we change the configuration as follows:



External call numbers

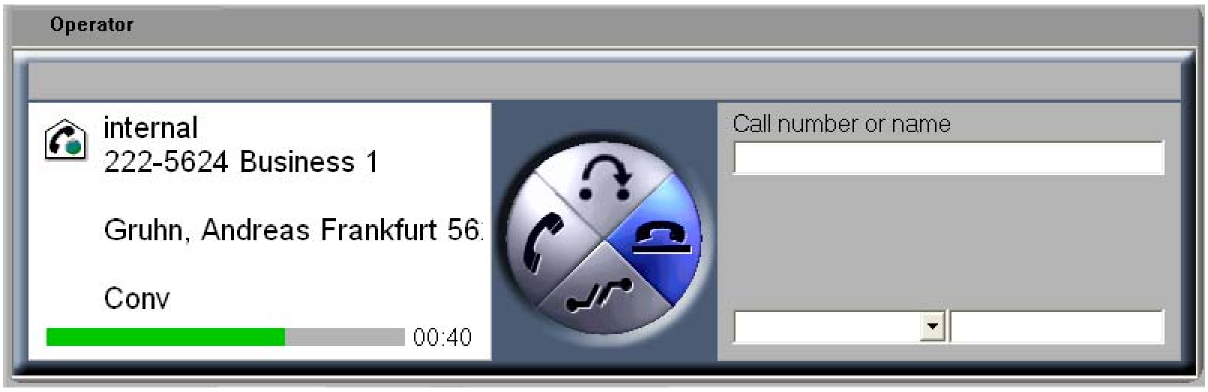
Recognition of external call numbers from a length of

9 digits (0: option switched off)

☑ Call From/Answered By Identification for external numbers

Figure 14: Example showing correct external call number confiduration

Now we call the same internal station via QSIG again:



Operator

internal
222-5624 Business 1

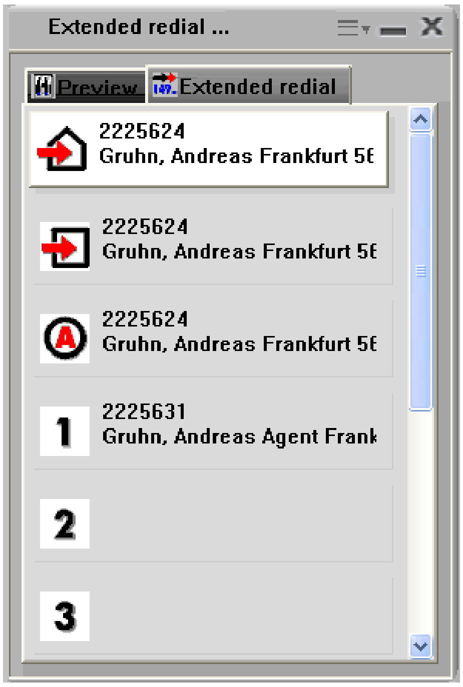
Gruhn, Andreas Frankfurt 56:

Conv

00:40

Figure 15: Example showing internal call in Operator Window

We see that now the call is marked internal. The redial list now also shows the call marked as “internal”:



Extended redial ...

Preview | Extended redial

2225624
Gruhn, Andreas Frankfurt 56

2225624
Gruhn, Andreas Frankfurt 56

2225624
Gruhn, Andreas Frankfurt 56

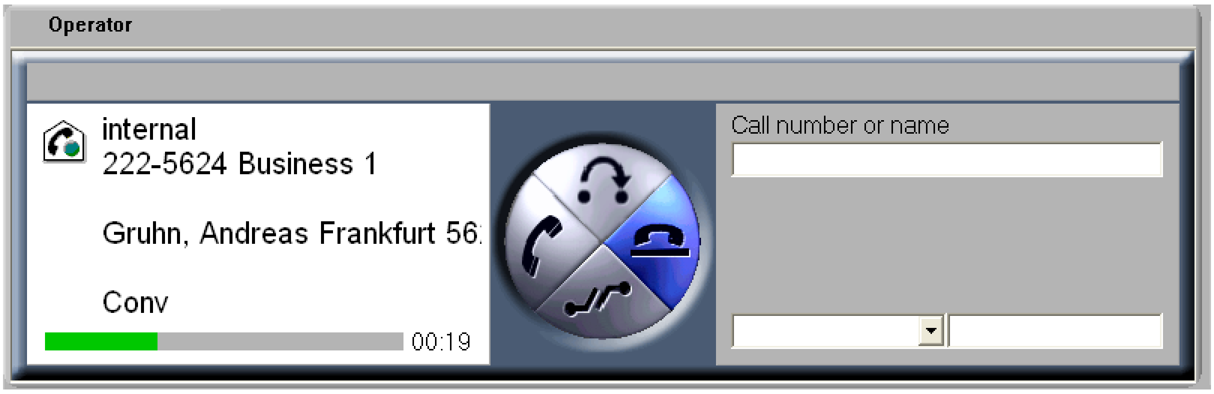
1 2225631
Gruhn, Andreas Agent Frank

2

3

Figure 16: Example showing internal call in Extended Redial List

We now double click on the selected call number and establish the call:



Operator

internal
222-5624 Business 1

Gruhn, Andreas Frankfurt 56

Conv

00:19

Call number or name

Figure 17: Example showing internal call established via QSIG.

The call was marked “internal” so the ARS has not been added.

Hint:

When you change the above configuration you have to restart oneX-Attendant to activate the changes.

Known Problems

The optional criteria do not work for every scenario.

For example:

Dial plans may exist that allows internal numbers to be longer than external numbers, so criteria 1.2.1. b) does not work.

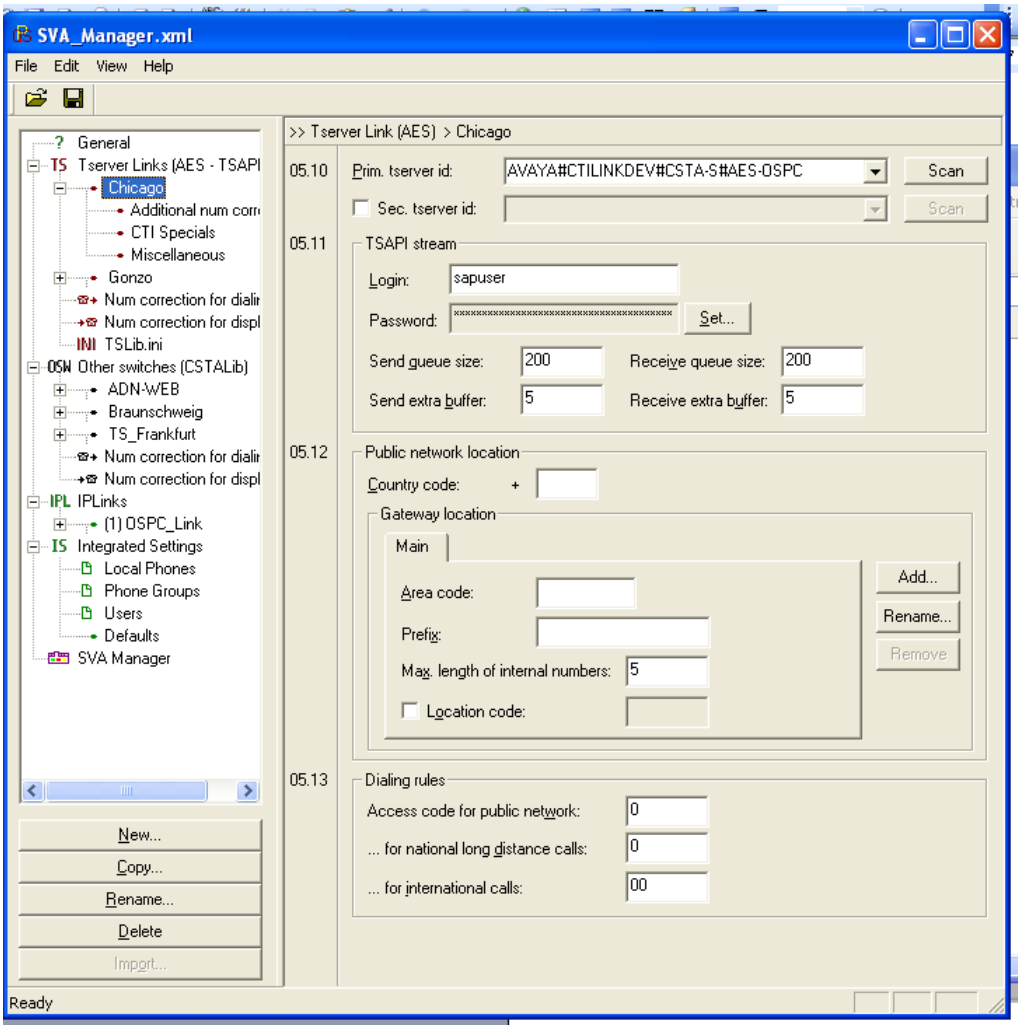
Sometime calls coming via QSIG or SIP trunks have a CALL FROM identification and it is not allowed to add the ARS for outgoing calls, so criteria 1.2.1. c) does not work.

By deactivation of these criteria it can happen that an external call, is not marked “external”, so when dialling the number out of call list or out of redial list, the ARS is not added automatically or in display “outg. Trunk” is missing.

Incoming and Outgoing calls on one-X Attendant I55 3rd party

External Call Number detection is also a point for one-X Attendant at I55 via 3rd party. In this scenario we have Qtapi-Framework(SVA Manager) instead of Scapi

The only criteria for incoming and outgoing calls is the length of the call number of the remote calling party. The difference to the CM version is, that call list and extended redial list are filled by the SVA Manager. That means a call number in call list or extended redial list is marked “external”, if the call number is longer than the with the SVA Manager Config-Tool configured value for “Max. length internal numbers”:



>> Tserver Link (AES) > Chicago

05.10 Prim. tserver id: AVAYA#CTILINKDEV#CSTA-S#AES-OSPC

□ Sec. tserver id:

05.11 TSAPI stream

Login: sapuser

Password: ************************************

Send queue size: 200 Receive queue size: 200

Send extra buffer: 5 Receive extra buffer: 5

05.12 Public network location

Country code: +

Gateway location

Area code:

Prefix:

Max. length of internal numbers: 5

□ Location code:

05.13 Dialing rules

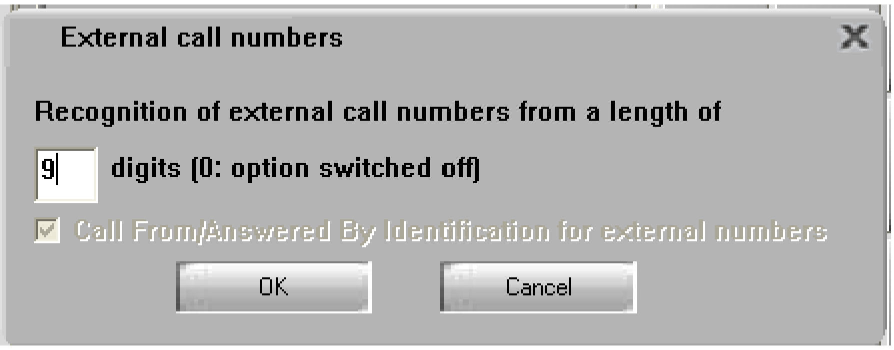
Access code for public network: 0

... for national long distance calls: 0

... for international calls: 00

Figure 18: SVA Manager Configuration Tool

In one-X Attendant operator window, a call is marked “external”, if the call number of the remote calling party is longer than the configured value in the one-X Attendant “external call number” dialog (see Figure 19)



Recognition of external call numbers from a length of

9 digits (0: option switched off)

☑ Call From/Answered By Identification for external numbers

Figure 19: Enternal call number dialog

Problems could be the same as described in 1.2.4. a) but normally I55 dial plan does not provide internal numbers longer than external numbers.

Maintenance, problem–solving

Trouble Shooting

TTrace

TTrace allows you to generate and administer log files. Specifically, it can be used to record the message traffic between the one-X Attendant client and OS_TAPI.

More detailed information on installation and operation can be found in references /7/ and /8/ .

The password for TTrace is “Recall”

If a login to one-X Attendant is not successful because a wrong password or an invalid user name has been entered then in the TTRACE category “TC_Warning” a message “`Failed login with user name <name>`” appears where <name> is replaced by the name the user had entered

TTrace installation

To install TTrace, follow these steps:

1. Insert the one-X Attendant installation CD in your CD drive. The Overview start page opens in your standard browser.
2. Click on **TTrace (logging tool)**. The TTrace window opens.
3. Click on **TTrace (logging tool)**. There is a program to guide you through the installation process.
4. Click on **TTrace Update**. This runs a batch file which replaces some program files.one-X Attendant/ SVA Manager connection

To record one-X Attendant, SVA Manager, AIS and other messages, you need to set the correct TTrace server’s host name and port number in the configuration tools, i.e. SVA Manager Configuration, one-X Attendant ConfigTools and AISConfig.

one-X Attendant Info

In case of problems with one-X Attendant you can use

Start > Programs > Avaya > one-X Attendant >Avaya one-X AttendantInfo

where you can record all your computer statuses and pass them over to the service department, who can then use this information to check your settings and applications.

The program creates a directory **C:\OneX–AttendantInfo** containing the informations in separate files. The directory should be zipped and provided to support.

SVA Manager: NBL-Link

Red SVA Status

First of all, check that SVA Manager Service is up and running:

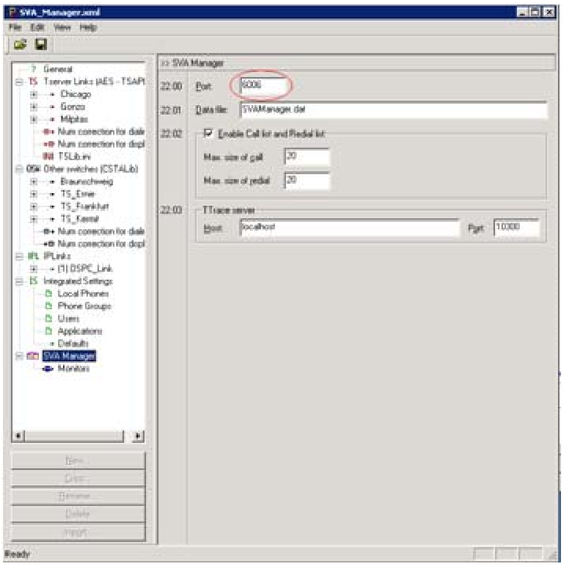
First please check that a red "SVA system" status in NOT shown on one-X Attd start screen.

Then check that all configured gateways and monitors are having status active:

1. SVA-Manager system service is started
2. Open TTrace Console on server: SVA-Manager is listed

3. Enter "printCtiGw" in TTrace Console command prompt
   => all configured gateways (CM, IE) are having status active
4. Enter "printDevice" in TTrace Console command prompt
   => all configured monitors are having status active

Then ensure that configured SVA Manager IP address & port are correct, which means that the same IP port (default: 6006) is configured in *SVA & one-X Attd Config Tool*:



>> SVA Manager

22.00 Port: 6006

22.01 Data file: SVAManager.dat

22.02 ☑ Enable Call list and Redial list

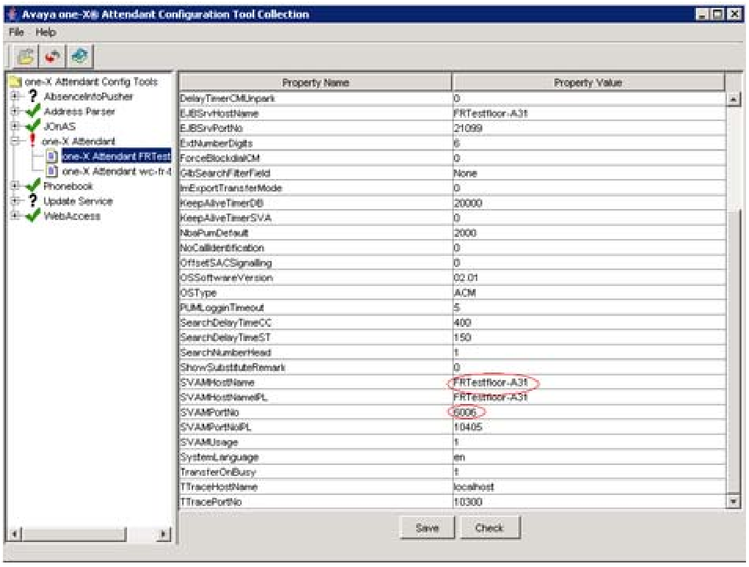
Max. size of call: 20

Max. size of redial: 20

22.03 TTrace server

Host: localhost Port: 10300

NBL-Link port administration in SVA-Manager config tool

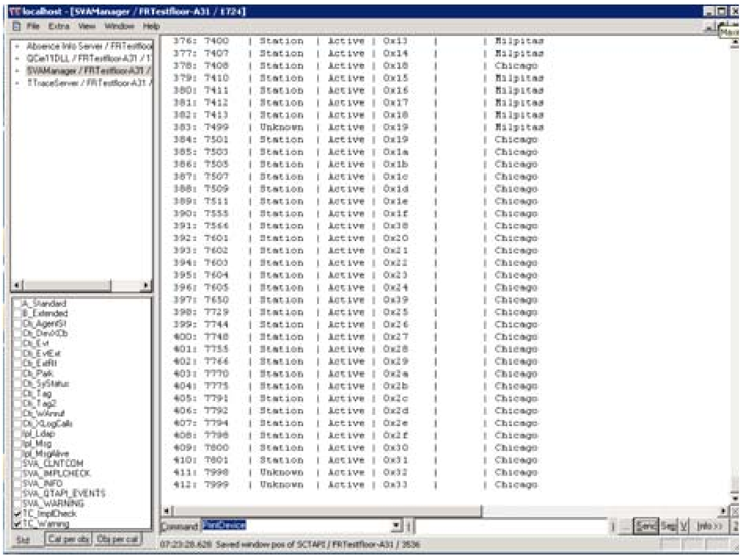


Property Name	Property Value
DelayTimerCMUnpark	0
EJBSrvHostName	FRTestfloor-A31
EJBSrvPortNo	21099
ExtNumberDigits	6
ForceBlockdialCM	0
GlbSearchFilterField	None
ImExportTransferMode	0
KeepAliveTimerDB	20000
KeepAliveTimerSVA	0
NbaPumDefault	2000
NoCallidentification	0
OffsetSACSignalling	0
OSSoftwareVersion	02.01
OSType	ACM
PUMLogginTimeout	5
SearchDelayTimeCC	400
SearchDelayTimeST	150
SearchNumberHead	1
ShowSubstituteRemark	0
SVAMHostName	FRTestfloor-A31
SVAMHostNameIPL	FRTestfloor-A31
SVAMPortNo	6006
SVAMPortNoIPL	10405
SVAMUsage	1
SystemLanguage	en
TransferOnBusy	1
TTraceHostName	localhost
TTracePortNo	10300

NBL-Link port administration in one-X Attd config tool

NBL does NOT show call states (e.g. busy / agent / call diversion)

First please check w/ the help of TTrace console and **PrintDevice** command, if configured monitors have been started and are logged as **Active**:



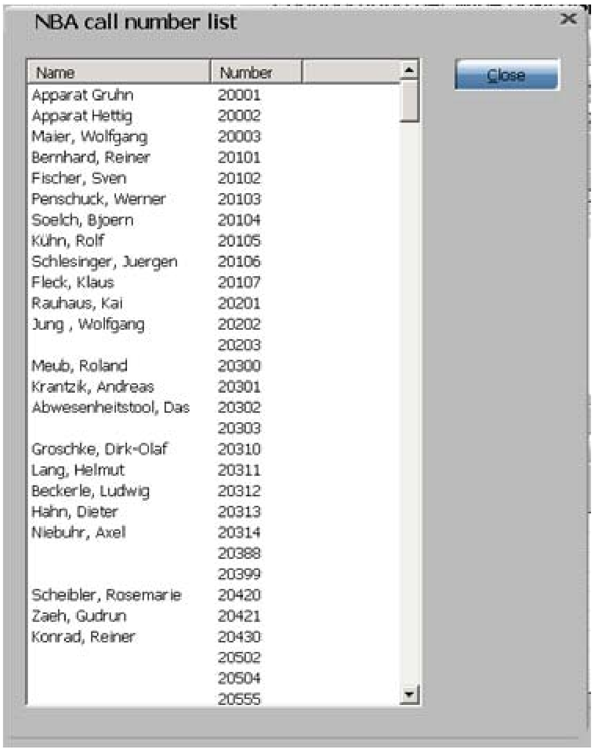
localhost - [SVAManager / FRTestfloor-A31 / 1724]
File Extra View Window Help
Command PrintDevice
Send Seg V Info >>

```
376: 7400   | Station  | Active | 0x13   |         | Milpitas
377: 7407   | Station  | Active | 0x14   |         | Milpitas
378: 7408   | Station  | Active | 0x18   |         | Chicago
379: 7410   | Station  | Active | 0x15   |         | Milpitas
380: 7411   | Station  | Active | 0x16   |         | Milpitas
381: 7412   | Station  | Active | 0x17   |         | Milpitas
382: 7413   | Station  | Active | 0x18   |         | Milpitas
383: 7499   | Unknown  | Active | 0x19   |         | Milpitas
384: 7501   | Station  | Active | 0x19   |         | Chicago
385: 7503   | Station  | Active | 0x1a   |         | Chicago
386: 7505   | Station  | Active | 0x1b   |         | Chicago
387: 7507   | Station  | Active | 0x1c   |         | Chicago
388: 7509   | Station  | Active | 0x1d   |         | Chicago
389: 7511   | Station  | Active | 0x1e   |         | Chicago
390: 7555   | Station  | Active | 0x1f   |         | Chicago
391: 7566   | Station  | Active | 0x38   |         | Chicago
392: 7601   | Station  | Active | 0x20   |         | Chicago
393: 7602   | Station  | Active | 0x21   |         | Chicago
394: 7603   | Station  | Active | 0x22   |         | Chicago
395: 7604   | Station  | Active | 0x23   |         | Chicago
396: 7605   | Station  | Active | 0x24   |         | Chicago
397: 7650   | Station  | Active | 0x39   |         | Chicago
398: 7729   | Station  | Active | 0x25   |         | Chicago
399: 7744   | Station  | Active | 0x26   |         | Chicago
400: 7748   | Station  | Active | 0x27   |         | Chicago
401: 7755   | Station  | Active | 0x28   |         | Chicago
402: 7764   | Station  | Active | 0x29   |         | Chicago
403: 7770   | Station  | Active | 0x2a   |         | Chicago
404: 7775   | Station  | Active | 0x2b   |         | Chicago
405: 7791   | Station  | Active | 0x2c   |         | Chicago
406: 7792   | Station  | Active | 0x2d   |         | Chicago
407: 7794   | Station  | Active | 0x2e   |         | Chicago
408: 7798   | Station  | Active | 0x2f   |         | Chicago
409: 7800   | Station  | Active | 0x30   |         | Chicago
410: 7801   | Station  | Active | 0x31   |         | Chicago
411: 7998   | Unknown  | Active | 0x32   |         | Chicago
412: 7999   | Unknown  | Active | 0x33   |         | Chicago
```

07:23:28.628 Saved window pos of SCTAPI / FRTestfloor-A31 / 3536

TTrace "PrintDevice" command displays start of monitors

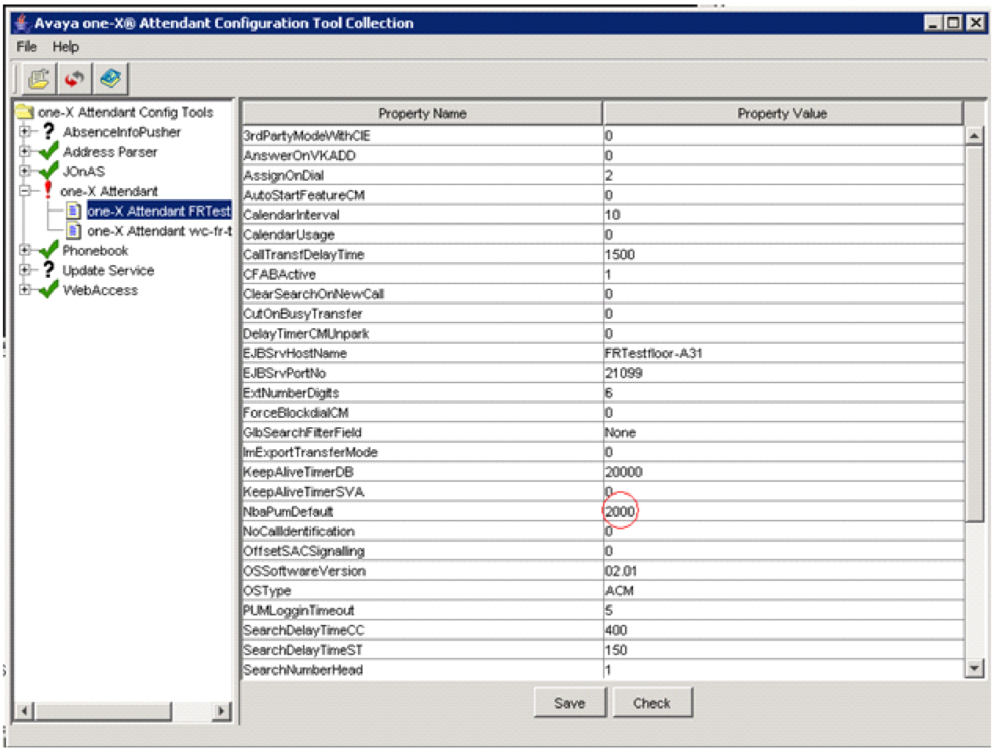
Look in 1XAttd work profile edit net wide busy display if there are numbers in number list (if not and above point is ok: try to disconnect all clients and restart SVA Manager):



Name	Number
Apparat Gruhn	20001
Apparat Hettig	20002
Maier, Wolfgang	20003
Bernhard, Reiner	20101
Fischer, Sven	20102
Penschuck, Werner	20103
Soelch, Bjoern	20104
Kühn, Rolf	20105
Schlesinger, Juergen	20106
Fleck, Klaus	20107
Rauhaus, Kai	20201
Jung , Wolfgang	20202
	20203
Meub, Roland	20300
Krantzik, Andreas	20301
Abwesenheitstool, Das	20302
	20303
Groschke, Dirk-Olaf	20310
Lang, Helmut	20311
Beckerle, Ludwig	20312
Hahn, Dieter	20313
Niebuhr, Axel	20314
	20388
	20399
Scheibler, Rosemarie	20420
Zaeh, Gudrun	20421
Konrad, Reiner	20430
	20502
	20504
	20555

NBA call number list

Check in 1XAttd config tool if value for **NbaPumDefault** is not below number of monitored extensions:



Property Name	Property Value
3rdPartyModeWithCIE	0
AnswerOnVKADD	0
AssignOnDial	2
AutoStartFeatureCM	0
CalendarInterval	10
CalendarUsage	0
CallTransfDelayTime	1500
CFABActive	1
ClearSearchOnNewCall	0
CutOnBusyTransfer	0
DelayTimerCMUnpark	0
EJBSrvHostName	FRTestfloor-A31
EJBSrvPortNo	21099
ExtNumberDigits	6
ForceBlockdialCM	0
GlbSearchFilterField	None
ImExportTransferMode	0
KeepAliveTimerDB	20000
KeepAliveTimerSVA	0
NbaPumDefault	2000
NoCallIdentification	0
OffsetSACSignalling	0
OSSoftwareVersion	02.01
OSType	ACM
PUMLogginTimeout	5
SearchDelayTimeCC	400
SearchDelayTimeST	150
SearchNumberHead	1

Administration of NbaPumDefault value in one-X Attd confi tool

Presence Information is not displayed at all

Please first check if Connection to Presence Server is okay (no PS icon shown after start of one-X® Attendant). If not check:

- In OSPCConfigTool under one-X® Attendant the NBV Server is set to Presence Server
- File c:\Avaya\Servers\AbsenceInfoPusher.properties contains entry "source=2"
- IP address of one-X® Attendant Server is allowed to access PS postgres database? Therefore
  1. The IP address must be entered in PS file /var/lib/pgsql/data/pg_hba.conf, the entries must look like the following:
  host all all 135.124.70.1/32 trust (for one special IP address)
  host all all 135.124.70.0/24 trust (for all IP addresses beginning with 135.124.70)
  2. The PS file /var/lib/pgsql/data/postgresql.conf must contain the entry
  listen_addresses = '*'.
- Have a look into c:\Avaya\Servers\absenceInfoPusher.log: If the file contains an error belonging to certificates please verify if all steps have been done referring certificates.
- Please check if AIP is running according to chapter "How to check Absence Info Pusher using Log files

If connection to Presence Server is okay but no presence is shown:

- Make sure that the users you want to get presence from are stored in one-X® Attendant with a Presence ID that is the same as the login name in SMGR.

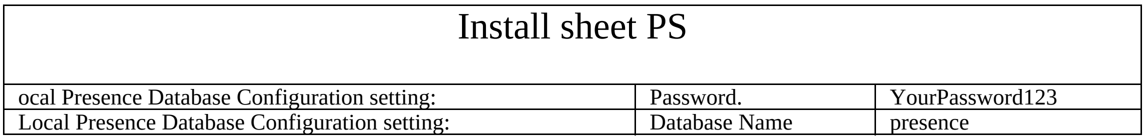
- Check if the presence states are stored in database. Therefore please start the database and have a look at table tbl_AbsenceState.
- Check in TTrace (OSPC, DBG_OSPC), if there are OnAbsenceStateChanged messages with the correct numbers (first of the two numbers is important). If the format (beginning) of the numbers is wrong, check the Addressparser configuration.

Error while starting AIP: "failed to access database"

```
INFO   | jvm 1    | 2012/05/08 11:24:25 | ERROR LPS - Can't start to LPS provider:
com.avaya.apas.exceptions.InvalidConfigurationException: Failed to access database with
parameters: Postgres, host=[135.9.146.35], port=[5432], dbname=[presence],
schema=[avaya_system_data], username=[presence_user], password = [***]
```

Please check the entries for data base access in c:\Avaya\Servers\LPS.properties. The entries must fit to your Presence Services Installation.

Especially be sure the password is the password you have entered at Presence Services Installation time.



Install sheet PS		
ocal Presence Database Configuration setting:	Password.	YourPassword123
Local Presence Database Configuration setting:	Database Name	presence

c:\Avaya\Servers\LPS.properties:

```
#default is presence
#localdb.dbname=presence

localdb.password=YourPassword123
```

Presence displayed in Phonebook, but not in Netwide Busy Display

Please configure the address parser.

Error while starting AIP: "Failed to access database"

```
INFO   | jvm 1    | 2012/05/08 11:24:25 | ERROR LPS - Can't start to LPS provider:
com.avaya.apas.exceptions.InvalidConfigurationException: Failed to access database with
parameters: Postgres, host=[135.9.146.35], port=[5432], dbname=[presence],
schema=[avaya_system_data], username=[presence_user], password = [***]
```

Is the one-X® Attendant Server IP Address constant or has it changed?
Is the one-X® Attendant Server IP Address in the PS file /var/lib/pgsql/data/pg_hba.conf?

Please check the entries for data base access in c:\Avaya\Servers\LPS.properties. The entries must fit to your Presence Services Installation.

Especially be sure the password is the password you have entered at Presence Services Installation time.

Install sheet PS

Local Presence Database Configuration setting:	Password.	YourPassword123
Local Presence Database Configuration setting:	Database Name	presence

c:\Avaya\Servers\LPS.properties:

```
                    #default is presence
                    #localdb.dbname=presence

                    localdb.password=YourPassword123
```

Error while starting AIP: "Unknown host name"

```
INFO   | jvm 1    | 2012/05/23 23:46:19 | ERROR com.avaya.mgmt.upm.client.common.UPMClient -
UPM_1078 Unable to lookup remote interface of UPM EJBs [detail:
javax.naming.CommunicationException [Root exception is java.rmi.UnknownHostException: Unknown
host: smgr.global2.avaya.com; nested exception is:
INFO   | jvm 1    | 2012/05/23 23:46:19 | java.net.UnknownHostException: smgr.global2.avaya.com]]
```

One-X® Attendant Server PC can't resolve host name of SMGR. Please provide host name resolution for SMGR on one-X® Attendant Server PC by making an entry in DNS.

Error while starting AIP: "Bad Firewall configuration"

```
INFO   | jvm 1    | 2012/05/24 01:00:01 | DEBUG
com.avaya.apas.lps.impl.transport.s2s.sip.utils.SipUtils - Sending Subscribe Request
INFO   | jvm 1    | 2012/05/24 01:00:01 | DEBUG
com.avaya.apas.lps.impl.transport.s2s.sip.utils.SipUtils -
==========================================
INFO   | jvm 1    | 2012/05/24 01:00:01 | DEBUG
com.avaya.apas.lps.impl.transport.s2s.sip.utils.SipUtils - Request Details:
INFO   | jvm 1    | 2012/05/24 01:00:01 | SUBSCRIBE sip:lps-rls@135.9.146.35:5061;transport=tls SIP/
2.0
INFO   | jvm 1    | 2012/05/24 01:00:01 | Call-ID:
60294799e25379df8c8044b99463d592@135.122.77.20
INFO   | jvm 1    | 2012/05/24 01:00:01 | CSeq: 1 SUBSCRIBE
INFO   | jvm 1    | 2012/05/24 01:00:01 | From: "lps" <sip:lps@135.122.77.20;transport=tls>;tag=12345
INFO   | jvm 1    | 2012/05/24 01:00:01 | To: "lps-rls" <sip:lps-rls@135.9.146.35>
INFO   | jvm 1    | 2012/05/24 01:00:01 | Via: SIP/2.0/TLS 135.122.77.20:9072
INFO   | jvm 1    | 2012/05/24 01:00:01 | Max-Forwards: 70
INFO   | jvm 1    | 2012/05/24 01:00:01 | Expires: 600
INFO   | jvm 1    | 2012/05/24 01:00:01 | Event: presence
INFO   | jvm 1    | 2012/05/24 01:00:01 | Supported: eventlist
INFO   | jvm 1    | 2012/05/24 01:00:01 | Require: adhoclist
INFO   | jvm 1    | 2012/05/24 01:00:01 | Accept: application/rlmi+xml,application/pidf+xml,multipart/
mixed,multipart/related
INFO   | jvm 1    | 2012/05/24 01:00:01 | Contact: "lps" <sip:lps@135.122.77.20:9072;transport=tls>
INFO   | jvm 1    | 2012/05/24 01:00:01 | Content-Type: application/adrl+xml
INFO   | jvm 1    | 2012/05/24 01:00:01 | Content-Length: 93
INFO   | jvm 1    | 2012/05/24 01:00:01 |
INFO   | jvm 1    | 2012/05/24 01:00:01 | <?xml version="1.0" ?><adhoclist uri="listUri-66331ecd"
name="lps-list"><create/></adhoclist>
……
INFO   | jvm 1    | 2012/05/24 01:00:38 |  INFO LPS - State of PS service changed (S2S): ERROR
```

LPS sends presence subscription suggesting port 9072. The firewall blocks the answer from the PS on inbound port 9072 and the LSP state changes to ERROR.

Check the Firewall.

Other Errors during AIP Start

AIP Start parameter:
Keystore relevant parameters are taken from:
c:\Avaya\Servers\absenceinfopusher.conf
Other data (e.g. data base and SMGR parameter):
c:\Avaya\Servers\LPS.properties

Be sure the entries fit to your Aura™ Installation:

- Is SMGR username and password the admin user in SMGR?
- Again: Database password of AIP (c:\Avaya\Servers\LPS.properties) same as the Presence Services password for the database?

Presence Server

Red PS button shown on one-X Attd start screen

Checklist:

- Restart one-X® Attendant
- Network ok? (Ping: one-X® Attendant Server PC ' Presence Server)
- Presence Services running?
- "Avaya Phonebook - AbsenceInfoPusher" Service running?
- 1XAttd ? ' Presence Services connection configured successfully?

One-X Attd client shows red PS button on start screen

If you have a one-X® Attendant client only installation and the one-X® Attendant server has no FQDN the red PS button may appear at the one-X® Attendant client.

If the TCP/IP number (IP address) is used for the phonebook connection, be sure that the number is also used for the host in the following file of the server: <ServerDirectory>\JONAS\conf\joramAdmin.xml (for the 3 occurrences of the hostname: substitute hostname by IP address).

In general the one-X® Attendant server should have a FQDN.

PS logging

Logging for Presence Services is described in "Administering Avaya Aura™ Presence Services" (Chapter: Logging Configuration).

Generate log files for Presence Issues with SIP 1XC:
PS logs:

- Output of $PRES_HOME/presence/bin/presstatus
- /var/log/messages
- This log file contains all SIP messages.
- /var/log/presence/presence-container-1.presencel.log and /var/log/presence/presence-container-1.presence_local.log
  In this log files all AES messages are contained, e.g. if the endpoint profile does not fit or no E.164 number is available.

1XC:

- SIPMessages.txt

SM:

- traceSM

Presence Services Diagnostics - Helpful Commands

Login:
Username: craft
Password:
Su –
Password:

Helpful commands:
cd /opt/Avaya/Presence/presence/bin

```
    Show Presence Status (includes license info):
        ./presstatus
    List Presence Certificate Configuration:
        ./prescert list
    Show PS software version
        ./swversion.sh
```

Log Files:
cd /var/log/presence

```
    Various Log files
        presence_core.log
        presencestatus.log
        presence-container-1.presence.log
        presence-container-1.presence_local.log
        presence_debug.log
```

Increase/Decrease Log Level:
cd /opt/Avaya/Presence/jabber/xcp/bin/

```
    ./updateLogLevel.sh
    Please enter the component name and the action:
    increase      -i | --increase
    decrease       -d | --decrease
    check        -c | --check
    E.g. To increase the log level for the  sip-ps-1 component
    ./updateLogLevel.sh sip-ps-1 -i
```

Increase Log Level:

```
./updateLogLevel.sh CORE-ROUTER -i
```

Attention: PS can crash!

Decrease Log Level:

```
./updateLogLevel.sh CORE-ROUTER -d
```

Check log level of component “SIP Bulk Subscription Server”

```
./updateLogLevel.sh sip-bulksub-1 -c
```

You can check the log level of many other components in the XCP controller.
Log in to the Presence Services XCP Controller Web interface as an administrator.
E.g. the AES Collector (Description: Connection Manager):

```
./updateLogLevel.sh cm-1 -c
```

```
[root@daytona-ps bin]# ./updateLogLevel.sh sip-bulksub-1 -c
sip-bulksub-1 is now logging at level (WARNING)
[root@daytona-ps bin]# ./updateLogLevel.sh sip-bulksub-1 -i
sip-bulksub-1 is now logging at level (INFO)
[root@daytona-ps bin]# ./updateLogLevel.sh sip-bulksub-1 -i
sip-bulksub-1 is now logging at level (VERBOSE)
[root@daytona-ps bin]# ./updateLogLevel.sh sip-bulksub-1 -i
sip-bulksub-1 is now logging at level (DEBUG)
[root@daytona-ps bin]#
```

Default level is WARNING
Available Levels: ERROR, WARNING, INFO, VERBOSE, DEBUG

one-X® Attendant: Logging of Presence Services

If you have any issues displaying correct absent states in one-X® Attendant this may have different reasons.

First of all it's not an easy job to configure your Aura™ System correct manner so presence is displayed correctly. One-X® Attendant may also be configured wrong.

Looking at the interface between one-X® Attendant and Presence Services probably can help to clarify where to solve an issue: on Aura™ side or in one-X® Attendant.

To get absence info from the Presence Services the Absence Info Pusher (AIP) Service makes a subscription for all users having a presence ID in the phonebook of one-X® Attendant server. The Presence Services publish the absent states by sending SIP Notify Messages to the AIP.

Basic prerequisites to display the absent states in X Attendant:

- Subscription must be ok.
- The received Absent states must be stored in data base table tbl_AbsentState
- Therefore Presence Info

The first two bullets can be checked by looking into the data base, all bullets can be checked by logging. To look into the data base you’ll need a data base view tool like SQL Anywhere scjview.

The received absent states are stored in one-X® Attendant server data base table tbl_AbsentState. This example shows the user with the internal phone number 6100 in the SIP Domain fr.rnd.avaya.com. Subscription is ok and the user is absent.

stateID	absent	passwd	psSubscription
1__6100@fr.rnd.avaya.com	ABSENT		SUBSCRIBED

The logging output for the AIP is in the file absenceinfopusher.log in the directory where the AIP is started (c:\Avaya\Servers if you use an installed version).
To change the log option you may edit the file pomlog.properties in the same directory.

```
#log4j.rootLogger=INFO, stdout
log4j.rootLogger=DEBUG, stdout

log4j.appender.stdout=org.apache.log4j.ConsoleAppender
log4j.appender.stdout.layout=org.apache.log4j.PatternLayout
log4j.appender.stdout.layout.ConversionPattern=%d %5p %c - %m%n

#log4j.logger.AIP=DEBUG
#log4j.logger.LPS=DEBUG
#log4j.logger.UPDS=DEBUG
#log4j.logger.WEB=DEBUG
#log4j.logger.LDAP=DEBUG
```

Example of successful subscription: (absenceinfopusher.log)

```
2012-04-05 13:16:47,170 | DEBUG | LPS-Callback - 3 | LPS - State of subscription changed (USER 102 - '6100@fr.rnd.avaya.com'): SUBSCRIBED
```

Example of Presence Message with content (ok): (absenceinfopusher.log)

```
<presence entity='pres:6202@presence.fr.rnd.avaya.com' xmlns='urn:ietf:params:xml:ns:pidf' xmlns:a='urn:avaya:com:presence:rpid:availability' xmlns:d='urn:ietf:params:xml:ns:pidf:data-model' xmlns:r='urn:ietf:params:xml:ns:pidf:rpid'><tuple id='oneXC'><status><basic>open</basic></status><r:activities><a:available/></r:activities><r:class>Enterprise IM</r:class><contact priority='1'>xmpp:6202@presence.fr.rnd.avaya.com</contact></tuple><d:person id='ps_generated'><r:activities><a:available/></r:activities></d:person></presence>
--9b9pBSWgSi1OEY94VRNX
Content-Type: application/pidf+xml
Content-ID: 240
Content-Transfer-Encoding: binary
```

Example: Presence Message w/o content (not ok): (absenceinfopusher.log)

```
<presence entity='pres:6200@presence.fr.rnd.avaya.com' xmlns='urn:ietf:params:xml:ns:pidf'/>
--9b9pBSWgSi1OEY94VRNX
Content-Type: application/pidf+xml
Content-ID: 239
Content-Transfer-Encoding: binary
```

TTrace

The final states received at one-X® Attendant Client can be logged using TTrace
In TTrace OSPC window switch on the categories DBG_OSPC and DBG_NBAPUM.

Example output:

```
H4690a 06:46:08.538 DBG_OSPC     OSPC:
AbsenceStateMonitor::OnAbsenceStateChanged(6100;+496975056100;ABSENT)
H4691a 06:46:08.538 DBG_NBAPUM   NBAPUM: CMainFrame::NewPresenceBVState: number=6100,
state==17
```

SVA-Manager

First please check that a red "**SVA system**" status in NOT shown on one-X Attd start screen.
Then check that all configured gateways and monitors are having status **active**:

1. SVA-Manager system service is started
2. Open TTrace Console on server: SVA-Manager is listed
3. Enter "printCtiGw" in TTrace Console command prompt
   => all configured gateways (CM, IE) are having status **active**
4. Enter "printDevice" in TTrace Console command prompt
   => all configured monitors are having status **active**

Local Presence Services

First please check that red "PS connection" status in NOT shown on one-X Attd start screen.
Then check that all Local Presence Services (managed by one-X Attd absence info pusher service) have been started successfully, which becomes logged in one-X Attd log file absenceInfoPusher.log.

Please browse log file `absenceInfoPusher.log` for text strings

```
State of PS service changed”  and “STARTED
2012-05-10 14:01:59,263 | INFO | LPSWorker - 2 | LPS - State of PS service changed
(S2S): STARTED
2012-05-10 14:01:59,310 | INFO | LPSWorker - 3 | LPS - State of PS service changed
(SIP-PS): STARTED
```

IM does NOT work at all

one-X® Attendant logs in to Jabber Sever during user login. Probably one-X® Attendant can't login to Jabber Server:
First please check:

- IM-Server (=Presence Server) in Configuration Data one-X® Attendant, use one-X® Attendant Config Tool
- IM-Port 5223 in Configuration Data one-X® Attendant, use one-X® Attendant Config Tool
- IM-User name in user data one-X® Attendant (User logged in: Edit User, Edit, choose user, Edit, Instant Messaging, Username) and System Manager, Users, User Management, Manage Users, Select user and edit, Communication Profile, Communication Address, Avaya XMPP (SMGR 6.2) or Jabber (SMGR 6.1) must match
- Be sure IM-Password in user data one-X® Attendant (User logged in: Edit User, Edit, choose user, Edit, Instant Messaging, Username) and System Manager, Users, User Management, Manage Users, Select user and edit, Communication Profile, Communication Profile Password is the same
- Replication of IM username and password to Presence Server

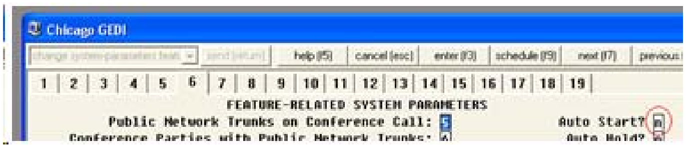
To check if one-X® Attendant logs in to Jabber Server please run OSPC-TTrace while logging in and look at the trace (DBG_IM must be active):

- IM: CXMPPAdaptor::Login Connecting to PS/IM: Server ok? User name ok?
- IM: OSPCIMHandler::IncomingMessage Login Status event: bRegistered 1: logged in, bRegistered 0: not logged in

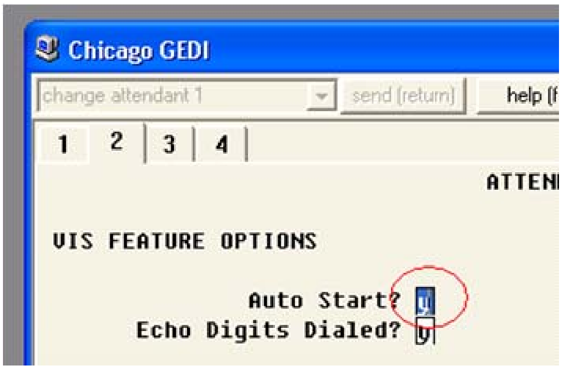
Telecommuter & Road Warrior Mode

one-X Attd does NOT dial any call number

Solution:
In CM configuration check if autostart is enabled for your attendant:



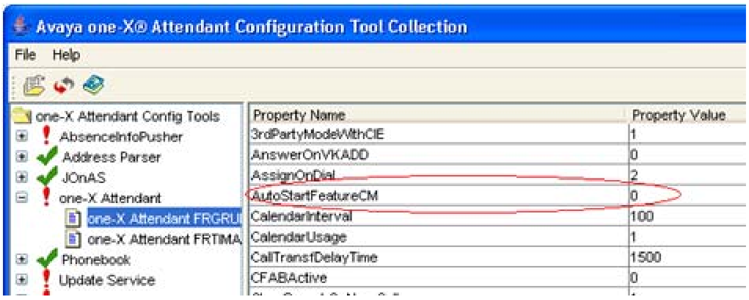
```
                 FEATURE-RELATED SYSTEM PARAMETERS
      Public Network Trunks on Conference Call: 5          Auto Start? n
   Conference Parties with Public Network Trunks: 6         Auto Hold? n
```



```
                               ATTEN

 VIS FEATURE OPTIONS

                   Auto Start? n
            Echo Digits Dialed? y
```

Autostart is enabled for your Attendant if both of these values are "y".

Depending on Autostart the following value in 1XAttendant config tool has to be set to the right value:

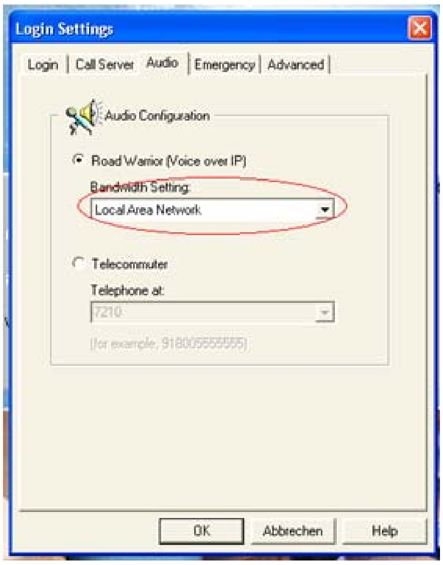


Property Name	Property Value
3rdPartyModeWithCIE	1
AnswerOnVKADD	0
AssignOnDial	2
AutoStartFeatureCM	0
CalendarInterval	100
CalendarUsage	1
CallTransfDelayTime	1500
CFABActive	0

Road Warrior mode: Not able to dial numbers in operator window

When switching from Telecommuter to Road Warrior after 1XAttendant login, user is not able to dial numbers by typing them in operator window.

Solution:
Check that in the login settings "Local Area Network" is selected for bandwidth:



● Road Warrior (Voice over IP)

Bandwidth Setting: Local Area Network

○ Telecommuter

Telephone at: 7210

(for example, 918005555555)

Telecommuter mode: Block dialing (e.g. from NBL) does NOT work

Solution
In CM configuration autostart is enabled for your attendant. In one-X® Attendant Configuration Tool the parameter AutoStartFeatureCM has to be set to "1".

Telecommuter mode: one-X Attd shows a call while calling a busy phone

Solution
In CM configuration autostart is enabled for your attendant. In one-X® Attendant Configuration Tool the parameter AutoStartFeatureCM has to be set to "1".

CM - AES Connection

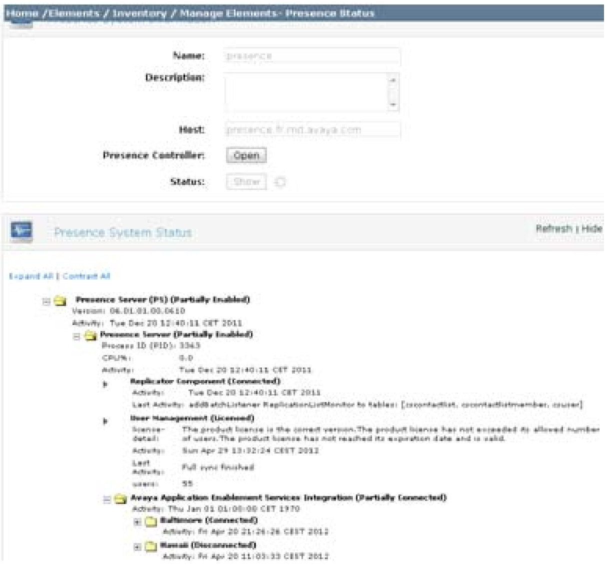
Check CM-AES connection in SMGR web console

Log on to SMGR web console and select menu **Elements/Inventory/Manage Elements.**

Notice: The assignment name of the CM here must be the same as the name of the switched connection in AES.

Then select onto the configured PS and click on button **Show:Status**, now the **Presence System Status** window opens.

Now please expand the node **Avaya Application Enablement Services Integration** and check, that the configured CM is displayed w/ status **Connected**:



Home /Elements / Inventory / Manage Elements- Presence Status

Name: presence

Description:

Host: presence.fr.md.avaya.com

```
Presence Server (PS) (Partially Enabled)
  Version: 06.01.01.00.0610
  Activity: Tue Dec 20 12:40:11 CET 2011
  Presence Server (Partially Enabled)
    Process ID (PID): 3363
    CPU%:             0.0
    Activity:         Tue Dec 20 12:40:11 CET 2011
      Replicator Component (Connected)
        Activity:      Tue Dec 20 12:40:11 CET 2011
        Last Activity: addBatchListener ReplicationListMonitor to tables: [cscontactlist, cscontactlistmember, csuser]
      User Management (Licensed)
        license-  The product license is the correct version.The product license has not exceeded its allowed number
        detail:   of users.The product license has not reached its expiration date and is valid.
        Activity: Sun Apr 29 13:32:24 CEST 2012
        Last
        Activity: Full sync finished
        users:    55
    Avaya Application Enablement Services Integration (Partially Connected)
      Activity: Thu Jan 01 01:00:00 CET 1970
      Baltimore (Connected)
        Activity: Fri Apr 20 21:26:26 CEST 2012
      Hawaii (Disconnected)
        Activity: Fri Apr 20 11:03:33 CEST 2012
```

SMGR showing status of CM <-> AES connection

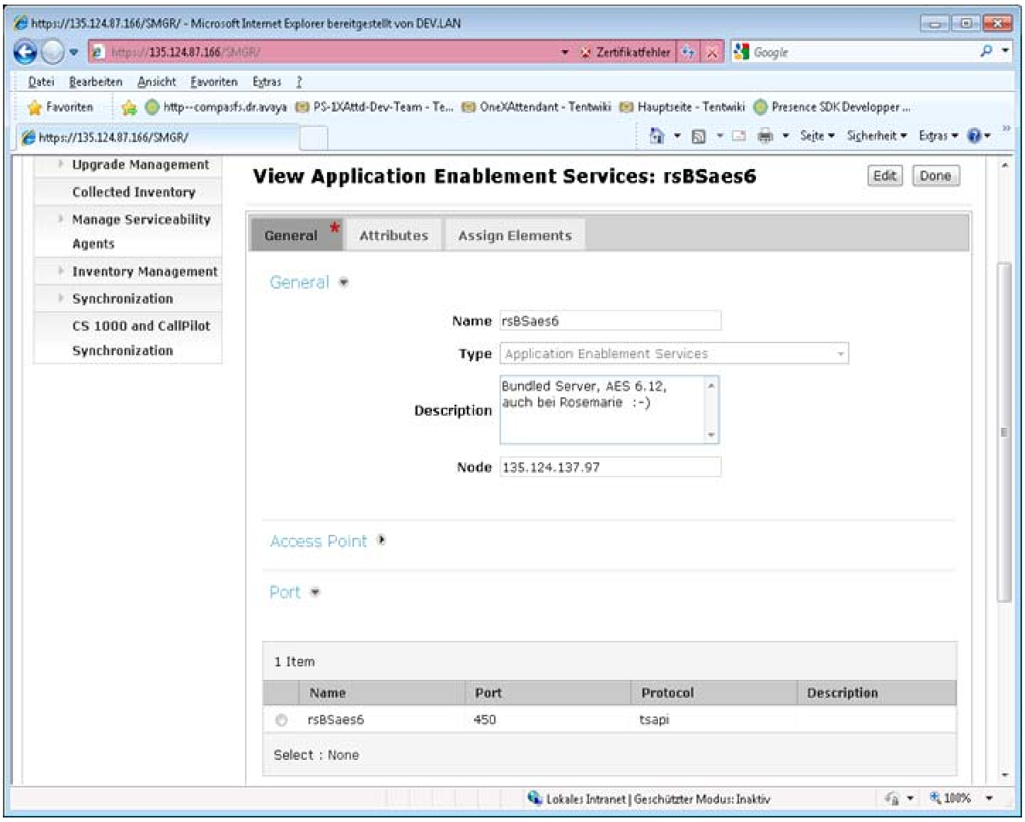
Note:

- The CM appears here as connected not before at least one user is created in SMGR with an E164 number and logged in.
- During installation of user in SMGR it is important (for AES) to fill the Endpoint Profile. The Session Manager Profile is only necessary in case of SIP user.
- The Jabber handle is automatically entered for the user in SMGR after replication with Presence Server. Please do not enter yourself!

Check AES Port

Log on to SMGR web console and select menu Elements/Inventory/Manage Elements.

View element AES and check if a Port has been entered:



View Application Enablement Services: rsBSaes6

General

Name: rsBSaes6

Type: Application Enablement Services

Description: Bundled Server, AES 6.12, auch bei Rosemarie :-)

Node: 135.124.137.97

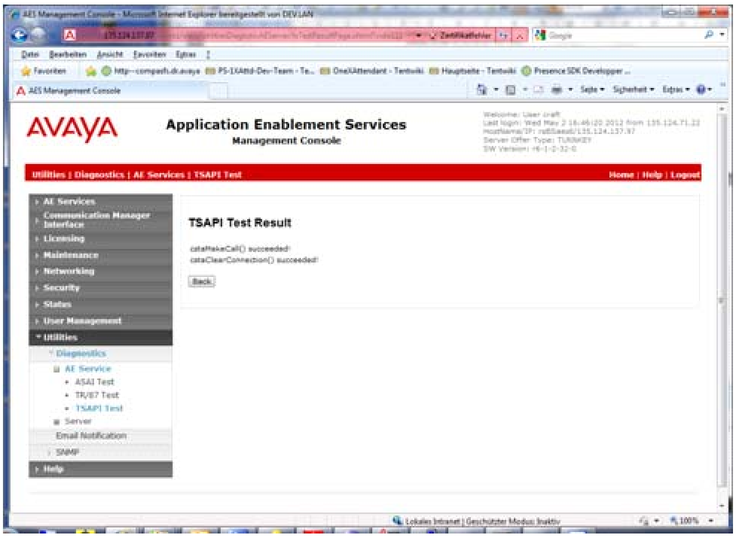
1 Item

	Name	Port	Protocol	Description
○	rsBSaes6	450	tsapi	

Select : None

Execute TSAPI test function "MakeCall"

In AES Management Console chose menu Utilities/Diagnostics/AE Service/TSAPI Test. Next please enter TSAPI Link, CTI user, calling and called party. If the connection is okay, the test result is shown as follows:



TSAPI Test Result

cstaMakeCall() succeeded!
cstaClearConnection() succeeded!

Successful execution of TSAPI test function "MakeCall"

Check TSAPI Service

Please select menu **ASA Management Console/Maintenance/Service Controller** in AES Management Console.

Hint: if Controller Status of TSAPI Service is not "running", please execute "Restart Service"

Now select menu ASA Management Console/Status/Status and Control/TSAPI Service Summary and check that the states of the link(s) between Avaya Aura™ AES and the the different Avaya Aura™ Communication Manager is shown as **Online**.

Evaluate TSAPI logfile

In case of an error during TSAPI Test (MakeCall) have a look at the TSAPI logfile.

- Start Putty
- Connect to AES
- Analyse /opt/mvap/logs/TSAPI/csta_trace_xxx.trace.out

Reset TSAPI Link

ASA - busyout cti-link xxx   (cti-link xxx down)
          release cti-link xxx   (cti-link xxx established)

SMGR Import fails

In case of an error during SMGR import check the file c:\Avaya\Servers\sercieconf\updateservice.conf

If updateservice.conf contains an error message like the following

```
INFO   | jvm 1    | 2012/06/11 09:37:00 |  INFO UPDS - Starting update for datasource ImportUserFromSMGR
INFO   | jvm 1    | 2012/06/11 09:37:04 |  INFO UPDS -
========================================================
INFO   | jvm 1    | 2012/06/11 09:37:04 |  INFO UPDS - Configuration:
INFO   | jvm 1    | 2012/06/11 09:37:04 |  INFO UPDS - connection string: jdbc:ashpool://file://
C:\Install\XML\user_1XA
INFO   | jvm 1    | 2012/06/11 09:37:04 |  INFO UPDS - id: 1
INFO   | jvm 1    | 2012/06/11 09:37:04 |  INFO UPDS - jdbc driver class name:
com.rohanclan.ashpool.jdbc.Driver
INFO   | jvm 1    | 2012/06/11 09:37:04 |  INFO UPDS - sql statement: SELECT * FROM SMGR_2000
INFO   | jvm 1    | 2012/06/11 09:37:04 |  INFO UPDS - transaction timeout 1000 sec
INFO   | jvm 1    | 2012/06/11 09:37:04 |  INFO UPDS - auto commit after 0 entries
INFO   | jvm 1    | 2012/06/11 09:37:04 |  INFO UPDS - update cycle: 142560
INFO   | jvm 1    | 2012/06/11 09:37:04 |  INFO UPDS -
========================================================
INFO   | jvm 1    | 2012/06/11 09:37:04 |  INFO UPDS - Starting to read...
INFO   | jvm 1    | 2012/06/11 09:37:09 | Exception in thread "Timer-0" java.lang.OutOfMemoryError:
Java heap space
```

edit c:\Avaya\Servers\sercieconf\updateservice.conf and increase Java Heap Size
(default value is 56):
Wrapper.java.maxmemory=256

Final Checks

View one-X Attendant keystore

If you like to be sure view one-X Attendant keystore.

```
keytool -list -keystore 1XAttd.keystore
```

Password: oneXAtt

Now one-X® Attendant keystore must three entries with the aliases:

- 1xA
- ipskey
- smgr key

Restart Absence Info Pusher Service

Navigate to “Services” on the one-X® Attendant Server PC:

Stop and Start the Service “Avaya Phonebook – AbsenceInfoPusher”.

Optional:

If the certificates exchange is done and the AIP started successful you will find the following outputs in the log file c:\Avaya\Servers\absenceInfoPusher.log:
(Generate a fresh log file for the AIP Start)

```
2012-05-10 14:01:59,263 | INFO | LPSWorker - 2 | LPS - State of PS service changed (S2S): STARTED
2012-05-10 14:01:59,310 | INFO | LPSWorker - 3 | LPS - State of PS service changed (SIP-PS): STARTED
INFO   | jvm 1    | 2012/05/24 08:01:44 | DEBUG com.avaya.apas.lps.impl.LPSProviderImpl - LPS Started
```

If you have any trouble with the Absence Info Pusher, generate a fresh log file for the AIP Start:
Stop “Avaya Phonebook – AbsenceInfoPusher”
Delete c:\Avaya\Servers\absenceInfoPusher.log
Start “Avaya Phonebook – AbsenceInfoPusher”
Edit c:\Avaya\Servers\absenceInfoPusher.log
Search for: error

PS Button

Restart one-X® Attendant Client.

The red PS button must not appear.

→ **Connection to PS is ok**

The red button appears? Follow chapter

Log File Generation for issues with 1XAttd ← → PS

If you have any trouble with the Absence Info Pusher, generate a fresh log file for the AIP Start:
Stop “Avaya Phonebook – AbsenceInfoPusher”
Delete c:\Avaya\Servers\absenceInfoPusher.log
Start “Avaya Phonebook – AbsenceInfoPusher”
Edit c:\Avaya\Servers\absenceInfoPusher.log
Search for: error

How to check Absence Info Pusher using log files

The logging output for the AIP is in the file absenceinfopusher.log in the directory where the AIP is started (c:\Avaya\Servers if you use an installed version).
To change the log option you may edit the file pomlog.properties in the same directory.

```
#log4j.rootLogger=INFO, stdout
log4j.rootLogger=DEBUG, stdout

log4j.appender.stdout=org.apache.log4j.ConsoleAppender
log4j.appender.stdout.layout=org.apache.log4j.PatternLayout
log4j.appender.stdout.layout.ConversionPattern=%d %5p %c - %m%n

#log4j.logger.AIP=DEBUG
#log4j.logger.LPS=DEBUG
#log4j.logger.UPDS=DEBUG
#log4j.logger.WEB=DEBUG
#log4j.logger.LDAP=DEBUG
```

If the certificates exchange is done and the AIP started successful you will find the following outputs in the log file
c:\Avaya\Servers\absenceInfoPusher.log:
(Generate a fresh log file for the AIP Start)

```
2012-05-10 14:01:59,263 | INFO | LPSWorker - 2 | LPS - State of PS service changed (S2S): STARTED
2012-05-10 14:01:59,310 | INFO | LPSWorker - 3 | LPS - State of PS service changed (SIP-PS): STARTED
INFO   | jvm 1    | 2012/05/24 08:01:44 | DEBUG com.avaya.apas.lps.impl.LPSProviderImpl - LPS Started
```

Then AIP subscribes to presence and renews subscription every 9 minutes due to Expire in 200 OK (currently 600 seconds).

Configuration of CM <-> AES Connection

- Select in AES Management Console:
  > Communication Manager Interface >Switch Connection >add Connection

- **in ASA:**
- choose CM
  (set target system)
- start Gedi
- status aesvcs link
  (shows already existing connections to an AES)
- display cti-link 2
  (try to find an already existing CTI link, e.g. number 2 and assume its data)
- add cti-link 3
  (add a new CTI link)
- change node-names ip
  (use “change node-names ip xxx” to change a node-name xxx of to add a node-name)
- change ip-services
  (add new CTI link on page 3)
- status aesvcs cti-link
  (check status of CTI link, should be “established”)

- status aesvcs interface
  (checks status of AE Services, should be listening)
- save translation

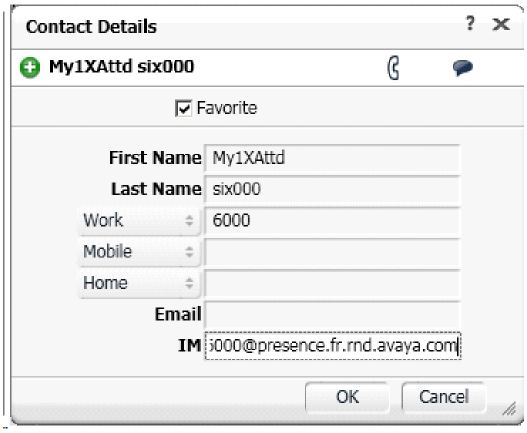
- Enter the appropriate date in AES Management Console:
  >User Management>User Admin>Add User
  >AEServices >TSAPI >TSAPI Links>Add Link (Security = both)
  >Choose Security>Security Database>CTI Users>List all users>edit>unrestricted
  Acces

Configuration of 1XC

Hint for 1XC w/o Public Directory: To add one-X® Attendant to the contact list:
Menu, Contacts, Add Contact as Favorite

Prerequisite: IM and presence is enabled

Example:



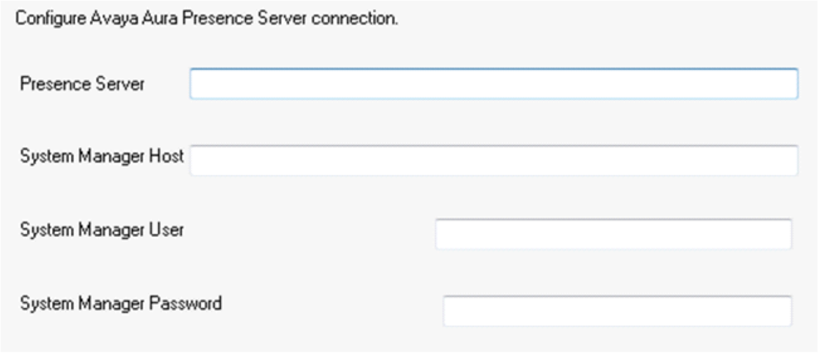
☑ Favorite

First Name My1XAttd
Last Name six000
Work 6000
Mobile
Home
Email
IM 5000@presence.fr.rnd.avaya.com

SMGR access data changed

If System Manager Host (name of IP address), User or Password or Presence Server Host has changed the concerned data have to be updated as following:

- Start Avaya one-X Attendant Configuration Tool Collection
- Choose AbsenceInfoPusher configuration
- Enter the changed data in the following fields and SAVE



Configure Avaya Aura Presence Server connection.

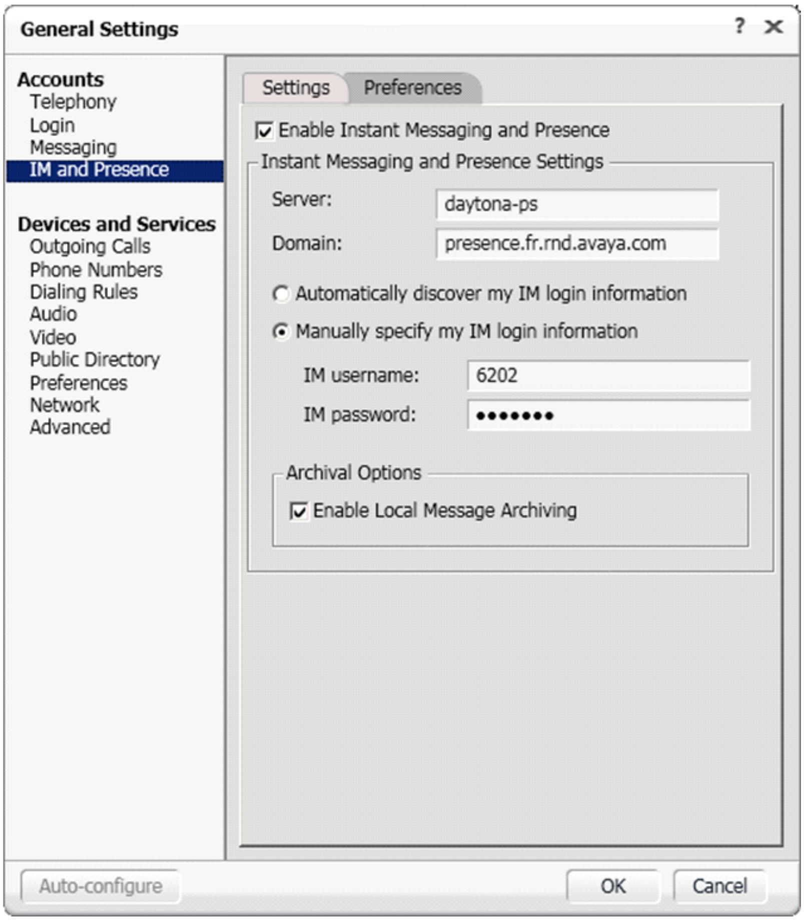
Presence Server

System Manager Host

System Manager User

System Manager Password

- Stop and start absence info Pusher



☑ Enable Instant Messaging and Presence

Instant Messaging and Presence Settings

Server: daytona-ps

Domain: presence.fr.rnd.avaya.com

○ Automatically discover my IM login information

● Manually specify my IM login information

IM username: 6202

IM password: •••••••

Archival Options

☑ Enable Local Message Archiving

IM username. 6202@presence.fr.rnd.avaya.com

Backing up and restoring the database

Application

Once you have created all users and work profiles, you can back up the database and all entries. You can revert to this data at any time and restore the data. These functions help you to quickly and easily set up an operator position with the usual work profiles and users, if for example you reinstall the operating system.

The file **OSPCdb.db** contains the entire one-X Attendant database. You can use tools to back up the database while it is running and restore it when it is switched off. The appropriate tools are set up during the installation

process.

Backup

You can back up the database during operation. Proceed as follows:

1. Click **Start**.
2. Click **Programs**.
3. Click **Avaya**.
4. Click on Backup one-X Attendant.
5. If no **backup** folder exists, the following prompt appears: **Directory does not exist. Create it.** Acknowledge this prompt with **Y** (yes).

The **backup** folder is created, and the **OSPCdb.db** database and the JOnAS and Serviceconf directories are copied to the folder. If the

OSPCdb.db file already exists, a prompt is displayed asking whether you want to replace the file.

6. You can back up the **OSPCdb.db** file and both directories on a single drive (for example, a tape drive).

It is recommended to change the file names afterwards and adding the one-X Attendant version and date, for example

OSPCdb_3v00_091019.db or moving all files to a suitably named

folder.

Restore

Before you restore the database, you must make sure that the backed up database file **OSPCdb.db** is located in the **backup** folder, as subdirectory to the server installation directory (Default: C:\Avaya\Servers).

You **cannot** restore a database when it is running. Proceed as follows:

1. Shut down all one-X Attendant clients.
2. Click on **Start**.
3. Click on **Programs**.
4. Click on **Avaya**.
5. Click on **Restore one-X Attendant**. This copies the database and the JOnAS and Serviceconf folders.
6. Press any key.

Note:

If necessary a database update will be done during a restore. This will be logged in the directory “<Serverdirectory>\Update\log”.

Avaya one-X Attendant migration from OSPC v2.5x

Performing migration

If you wish to migrate from an OSPC version 2.5x to one-X Attendant v3.00, proceed as follows:

First of all:

<Serverdirectory new> is by default: C:\Avaya\Servers

<Serverdirectory old> is by default: C:\Avaya\Servers

The following steps are only for a database update necessary, this will occur if for the according version a update_xxx_xxx.sql file is available. For example at the update from 3.00.006 to 3.00.008 the file update_v300_v300007.sql.

Configuration(Database/SVAManager/JONAS) backup

’Start –> Programs –> Avaya –> Avaya OSPC – > Backup Avaya OSPC’

respectively

’Start –> Programs –> Avaya –> Avaya one–X Attendant –> Backup Avaya one–X Attendant’

1. Recommendation:
   For safety reasons export the Profiles, Users, Phone Book and make screenshots of the Connection\Mapping data for the external Phone Directory in the one–X Attendant Configuration Tool. If something goes wrong, you can reimport/enter them after a normal installation of the next version.
2. Deinstall old version..
   Important: Please note database user and database password, because during the installation of the new version these should be used again, otherwise after the update the database access works no more.
3. Install the new one-X Attendant version .
4. Copy files:
   Copy the files ’updatedb.bat’ and all ’update_vxxx–vxxx.sql’, which are necessary for this step of the update, from the Update–Directory of the CD ’\software\one–X Attendant\DBUpdate’ into <Serverdirectory new>.
   For an update from 2.50 towards 3.00.007 these files are ’update_v250_v251.sql’, ’update_v251_v300.sql’ and ’update_v300_v300007.sql’.

If now the Master Directory Application is installed and in the old version not, the entries for an automatic update of the phone book will be deleted during the restore of the configuration(database). If they should be restored, then also the file ’One–XAttendantAutoImport.sql’ out of the directory <Serverdirectory new>\MasterDirectory\Data> have to be copied in the <Serverdirectory new>. .

5. Customize updatedb.bat
   Open the file update.bat with a text editor (e.g. Notepad) and change the following texts:
   – ’SERVERNAME_1XA’ in the name of the database server as stated during the installation respectively located in the registry under the Key
   [HKEY_LOCAL_MACHINE\SOFTWARE\Avaya\Avaya\OSPC\Setup]
   in the value ’DBServer’
   ’SERVERNAME’ in the name of the PC as stated under Control Panel –> System –> Computer name

If during the installation the default values haven’t been used, then possibly the following texts has to be changed:

- The value for ’ServerDrive’ (default is ’C:’)
- The value for ’ServerDir’ (’default is C:\Avaya\Servers’)
- The value for ’BACKUPPATH’ (’default is C:\Avaya\Servers\Backup’)
- The value for ’DBUser’ in the user name for the database server as stated during the installation
- The value for ’DBPwd’ in the password for the database server as stated during the installation
- The value for ’DBPort’ in the port for the database server as stated during the installation respectively located in the registry under the Key [HKEY_LOCAL_MACHINE\SOFTWARE\Avaya\Avaya OSPC\Setup] in the value ’DBPort’

6. Update database
   Call updatedb.bat (with Windows VISTA and Windows 7 as administrator).
7. If you have chosen the usage of the SVAManager during the installation and you didn’t have use before, the entry ’SVAMUsage’ in the one–X Attendant Config Tools after the restore of theconfiguration(database) is possibly set to ’0’. This means that usage of the SVAManager is deactivated and the extended busy lamp doesn’t work. If you want to use this feature, you have to set entry ’SVAMUsage’ to ’1’ again.

Note

An upgrade **should not** be installed over an existing version.

one-X Attendant update

Carry out update

The installation supports updates from Version 3.01.000 and higher, no further actions are necessary.

Use old databases

For databases of the OSPC version 2.5x: See chapter “Avaya one-X Attendant migration from OSPC v2.5x”.

For databases of the one-X Attendant 3.01.000 version and higher: Copy the database in the “restore” subdirectory and call the restore function. See chapter “Backing and restoring the database”.

Tips and tricks

Starting one-X Attendant without ACM

For servicing, it is possible to log on to **one-X Attendant** even while it is not connected to ACM. This lets you, for example, set up users and create work profiles.

To start the **one-X Attendant** application without an ACM connection, follow these steps:

1. Start one-X Attendant adding the following:
   OSPC.exe -o (space, minus sign, letter o)
   the shortcut is: „C:\Program Files (x86)\Avaya\Avaya one-X Attendant\OSPC.exe“-o
   In case of a working connection to CM, put a wrong CM IP adress or push the cancel tab at the iClarity login.

Note

If you start one-X Attendant with the “–o” extension, with a **functioning** ACM
connection, it will work as if it had been started without “–o”.

Connection to ACM after Login

If at least one Hundred Group is activated as Busy Lamp Field, one-X Attendant every 250 ms senda messages to the SCAPI. The SCAPI will answer immediately with messages as long as the connenction is ok.
If the one-X Attendant has to wait more than about 500ms for an answer, the status of the connenction goes to disurbed and a yellow hammer appears in the right bottom corner of the one-X Attendant window.
If the disruption persists longer than 25 seconds the statusof the connection goes to offline, and the colour of the hammer will change to orange.
As soon as the connection will be ok again the hammer disappears from the right bottom corner of the one-X Attendant window.

Checking the connection to Web server when Outlook out–of–office is switched on

To use an activated out–of–office notice in Microsoft Outlook, the Absence Info Server (AIS) must be installed. There must be a connection to the one-X Attendant web server (Tomcat). The operating system Internet options are used to establish the connection. If there is a registered proxy server, it must find the one-X Attendant web server.
To check the connection, follow these steps.

1. Open a browser, such as Microsoft Internet Explorer.
2. Enter the following address.
   https://Name of the Web server PC:21080 (Port as set in the WebAccess tool).
3. The browser must display a page with a certification error.

Registry

Advanced users can modify the settings in the Registry.
All registry entries are located in:
HKEY_LOCAL_MACHINE\SOFTWARE\Avaya and
HKEY_CURRENT_USER\SOFTWARE\Avaya

Information for service or hotline

- Select START > PROGRAMS > Avaya > one-X Attendant Info

This creates a directory **oneX–AttendantInfo** on the **C:\** drive. This file contains all necessary data for one-X Attendant and the PC. This directory contains the following information:

1. one-X Attendant full version
2. Software version of the optional software (WEB, NBA, etc.)
3. Operating system and version, if required, service pack
4. Version of the program libraries used (DLL, VBX, OCX or others)
5. Associated Registry entries (one-X Attendant, license server, all modules, etc.)
6. Network settings (IP, subnet mask, default gateway, DHCP server, routes)
7. Errors detected and logged at runtime are written to the event log(separate logs)
8. A selection of settings from the one-X Attendant configuration tools collection
9. Description of the one-X Attendant environment, names of, for example: Exchange server, one-X Attendant server, one-X Attendant clients
10. ODBC Administration settings (System DSN)
11. HOSTS file entries

Unknown host name

You must use the host name when you enter the name of a server.
This is how you find out the host name:

1. In order to find out the hostname, open a command prompt (DOS window) on the relevant PC.
2. Enter ipconfig /all.
3. Press **ENTER**. This displays the host name and other IP settings.

Sybase database in the network with the same name

If there is a Sybase database with the same name (one-X Attendant) in the network (LAN), a message to this effect is displayed.

Note:

The name for the one-X Attendant database can only be entered during installation. The name of the one-X Attendant database cannot be changed later on.

Distinction between external and internal numbers is not working

Sometimes, the distinction between external and internal phone numbers in the one-X Attendant phone book does not work.

Make sure that all external numbers are entered with a prefix, even if they are in the same area code as you. This is the only way to save numbers so that they are unique.

one-X Attendant does not start at all

Problem: When starting one-X Attendant, the splash screen (welcome screen) only appears briefly.

There is a problem with the Java installation! In the Control Panel, the Java plugin must be set to Default, and under the PATH system variable, no path to a JRE should be entered.

one-X Attendant shows message "java.lang.OutOfMemoryError: Java heap space"

If the client shows a window with this message then the heap space for the JVM has to increased. This has to be done in the file deployment.properties which you can find the folder C:\Documents and Settings\<username>\Application Data\Sun\Java\Deployment (Windows XP/2003) or C:\Users\<username>\AppData\LocalLow\Sun\Java\Deployment (Windows 7/2008/VISTA). Add the following line: deployment.javaws.jre.0.args=-Xmx256m -Xms64m. The '0' corresponds to the JRE you want to set these parameters for. There could be multiple JREs with different numbers (0,1,2..), do this for the JRE with version "1.6.0_23".one-X

Attendant does not start after a restart

Please note that one-X Attendant will not start while the iClarity process is still running. This can happen if the one-X Attendant did not close properly.

End the OSPC.exe process and restart one-X Attendant.

one-X Attendant does not dial

If the one-X Attendant seems to be working correctly but still will not dial, this can be due to an incorrect configuration of the bandwidth settings.

Access the system configuration and correct any incorrect settings in the

TEL tab.

Recommendations on configuring feature buttons

For the feature buttons you should only use the pre–set functions (see appendix) or such functions that can be called using an access code. The special characteristic of these functions is that they can also be run using individual dialing in one-X Attendant (e.g. access code for trunk line, ACW/Wrap–up time, speed dialing keys, etc.).

Other functions may cause the ACM to send responses to the one-X Attendant, which are then displayed there in a misleading way and may cause a malfunction.

Name reconciliation on the one-X Attendant / ACM database

When a number is redialed, deflected to one-X Attendant or diverted, ACM transfers only the *name* of the person being called as entered in the ACM database to the one-X Attendant, not the internal number.

For normal calls, the *number* is transferred from the ACM to the one-X Attendant. The number is identified and the name displayed using the one-X Attendant database.

In order for a subscriber to always be displayed with the same name within the one-X Attendant, the records within the ACM and the one-X Attendant databases must be identical. You can achieve this by importing the records from the ACM into the one-X Attendant database .

Additional tips

For more tips and tricks, visit the Avaya Enterprise Portal

Once there, go to the **Technical Center** and, under Applications, look for

“one-X Attendant”.

One-X Attendant in Telecommuter Mode

Don’t use feature buttons on telephone when handling an attendant call. Allways use feature buttons on attendant in that case.

For example pressing hold/retrieve button on telephone when having an attendant call leads to lost of communication path (Workarround: Hold/Retrieve call via one-X Attendant GUI)

Appendix

LDAP connection (LDAP browser) examples

LDAP connection

(LDAP browser)

Before configuring an LDAP connection you should first check the connection using the **LDAP browser\editor** tool.

For this, copy the “LDAPBrowser” directory from the CD in directory

’software\Service–Tools’ to a local drive (with write access rights).

To start the tool double–click **lbe.jar** or if the system does not detect Java Runtime (basic *one-X Attendant* installation), double–click OSPC-**lbe.bat**. The **Connect** window opens. The **Session list** tab contains a few sample connections.

Use the **Edit** button to view and modify the settings. If the name is changed

(tab: **Name**), then a new connection configuration (session) will be created. The **Connection** tab displays the connection parameters.

In Exchange, be sure to enter the PC which is running Active Directory. This is not necessarily the Exchange Server.

Next click **Fetch DNs** to obtain a list of **Base DN**s (Domino (the IBM MAil

Server, Lotus Domino) shows an empty list). Select the shortest entry.

First, select an anonymous connection (**Anonymous bind**), click **Save** and in the Connect window click **Connect**.

You should be able to see at least the BaseDN entry.

Now enter an appropriate user and the user’s password. You may be required to enter the user with the complete path (see Exchange2k_Lab login and Exchange2003_Lab login examples). To do so, you will need the support of your system administrator who will advise you in which substructure the user that you are utilizing is located.

Once you have successfully set up the connection, you can transfer the parameters to the phone book tool.

The Select-statement in the phone book tool must contain any field you may want to retrieve. After you have selected a user the field names will display in the **LDAP browser\editor** under attributes. Accept the names. Note that names are case-sensitive.

Example 1 for data source using a JDBC-ODBC bridge

The table below shows an example of the parameters on the Connection tab if you connect to a database using a JDBC-ODBC bridge.

Parameter	Setting
Name	JDBC-ODBC bridge Description
Driver	sun.jdbc.odbc.JdbcOdbcDriver
Provider URL	jdbc:odbc:SampleDSN User admin
Password	
SQL statement	SELECT * FROM SampleTable

Example 2 for data source directly via JDBC

The table below shows an example of the parameters on the Connection

tab if you connect to a database directly using a JDBC driver. The database with the name DBN is a Sybase ASA type and is located on the PC with the host name dbserver with port 4321.

Parameter	Setting
Name	AdaptiveServerAnywhere
Driver	com.sybase.jdbc3.jdbc.SybDriver
Provider URL	jdbc:sybase:Tds:dbserver:4321 [?ServiceName=DBN]
User	dba
Password	sql
SQL statement	SELECT * FROM SampleTable

Example 3 for MEDCOM data source using a JDBC-ODBC bridge

The table below shows an example of the parameters on the Connections tab if you connect to a MEDCOM database. You have to configure a system DSN for the MEDCOM database. The data source name for this example is Medcom_W2k.

In the one-X Attendant tool collection, you normally generate two data streams in the phone book tool which both point to the data source Medcom_W2k (in this example). The data streams could be called Staff and Patients, for example. You must use the appropriate SQL query for each data stream.

Parameter	Setting
Name	JDBC–ODBC bridge
Driver	sun.jdbc.odbc.JdbcOdbcDriver
Provider URL	jdbc:odbc:Medcom_W2k *or* jdbc:odbc:; Driver={Adaptive Server Anywhere 6.0}; SRVR=Medcom_W2k
User	dba passwordsql
SQL statement	SELECT * FROM mcuser

Example 4 for an LDAP data source using a JDBC-LDAP bridge with general settings

The table below shows an example of the parameters on the Connections tab if you connect to an LDAP database.

Parameter	Setting
Name	Exchange
Driver	com.octetstring.jdbcLdap.sql.JdbcLdapDriver
Provider URL	see below

jdbc:ldap://<server>:389/[BASE_DN]?SEARCH_SCOPE:=subTreeScope [&pageSize:=n]

Note:

The URL must not contain spaces (except for immediately in front of the “?”).

LDAP connection (LDAP browser) examples

Parameter	Setting
User	<Domain>\<User ID> or<Distinguished Name of the user (DN)>

Examples:

- Domain\User ID:tnbk1\bek2fr
- distinguishedName: CN=BEK2FR,OU=Users,OU=Fr, OU=Germany, DC=Avaya,DC=corp,DC=lan

Password	SamplePassword
SQL statement	select DN,givenName,sn,cn,title,mail,telephoneNumber,mobile,homePhone,otherHome-Phone, ipPhone,pager,facsimileTelephoneNumber,description,info,physicalDeliveryOfficeName,streetAddress,postOfficeBox,postalCode,l,st,co,company,department, extensionAttribute5,wWWHomePage,url from ou=OrgUnit “select from ou=OrgUnit” also works, but is not recommended.

Example 5 for Exchange 2007/2010 data source using a JDBC–LDAP bridge

The table below shows an example of the parameters on the Connections tab if you connect to an Exchange 2007/2003/2000 database.

Parameter	Setting
Name	ADS 2000/2003
Driver	com.octetstring.jdbcLdap.sql.JdbcLdapDriver
Provider URL	see below

jdbc:ldap://FR135120:389/DC=iccdomain,DC=com?SEARCH_SCOPE:=subTreeScope&pageSize:=90

User	cn=Administrator,cn=users,dc=iccdomain,dc=com
Password	SamplePassword
SQL statement	select DN,sn,givenName,cn,mail,telephoneNumber,department from ou=cdm–test where sn=*

Example 6 for Domino 6 data source using a JDBC-LDAP bridge

The table below shows an example of the parameters on the Connections tab if you connect to a Domino 6 database.

Parameter	Setting
Name	Domino 6
Driver	com.octetstring.jdbcLdap.sql.JdbcLdapDriver
Provider URL	jdbc:ldap://FR146025:389?SEARCH_SCOPE:=subTreeScope
User	Avaya
Password	SamplePassword
SQL statement	select givenname,sn,cn,mail,telephonenumber from o=OSPc_Org

Example 7 for Domino 5 data source using a JDBC-LDAP bridge

The table below shows an example of the parameters on the Connections tab if you connect to a Domino 5 database. The pagesize attribute in the url is not mandatory.

Parameter	Setting
Name	Domino 5
Driver	com.octetstring.jdbcLdap.sql.JdbcLdapDriver
Provider URL	jdbc:ldap://FR146025:389?SEARCH_SCOPE:=subTreeScope&pageSize:=90
User	Avaya
Parameter	Setting
Password	SamplePassword
SQL statement	select givenname,sn,cn,mail,telephonenumber from o=OSPc_Org

Example 8 for connection of the MasterDirectory

The following table shows an example with the default settings for connection of the MasterDirectory.

Parameter	Setting
Name	MasterDirectory
Driver	sun.jdbc.odbc.JdbcOdbcDriver
Provider URL	jdbc:odbc:MasterDirectory

Note:

see *SQL Statement* for the name

User	
Password	
SQL statement	SELECT * FROM directory

Note:

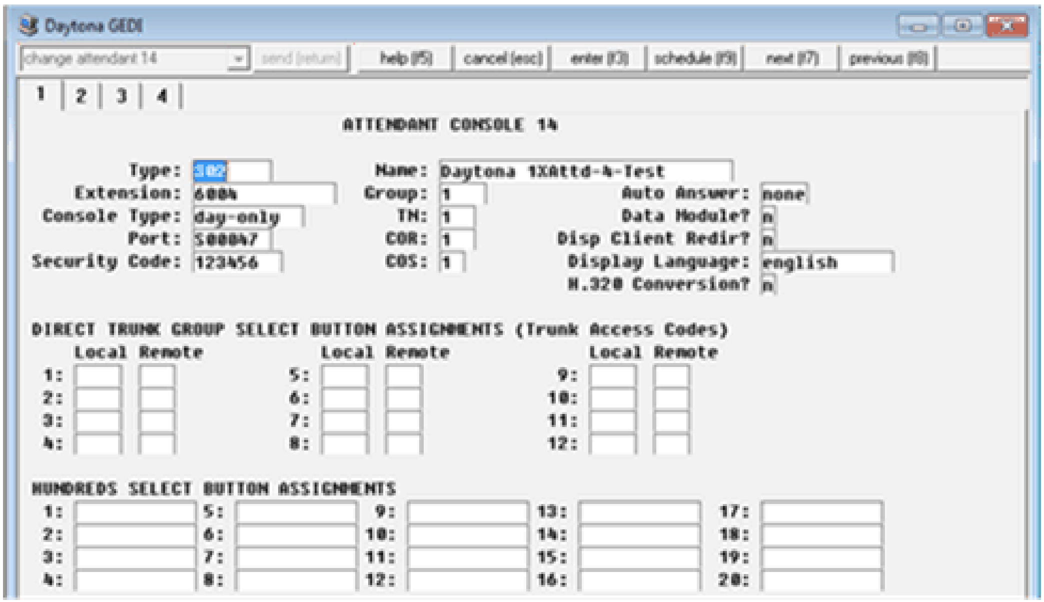
“directory” stands for the name of the ODBC database without file extension. It can be found under **System control > Administration > Data sources (ODBC) >** Register **System DNS > MasterDirectory** (must correspond to the name quoted in the *Provider URL*) **> Path**. There will be found for instance **directory.md**.

Avaya Communication Manager configuration for 1XATTD

Start Site Administration Tool or putty or command prompt and connect to CM

1. List attendant (to look which numbers are already occupied)
2. Add attendant 15 (example that already 14 attendants available)

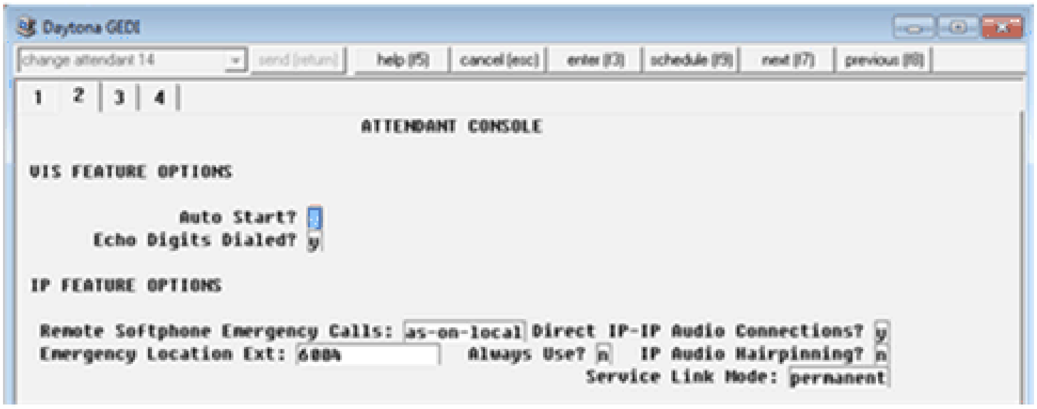
Page 1



```
                          ATTENDANT CONSOLE 14

          Type: 302              Name: Daytona 1XAttd-4-Test
     Extension: 6004            Group: 1                  Auto Answer: none
  Console Type: day-only          TN: 1                  Data Module? n
          Port: S00047            COR: 1             Disp Client Redir? n
 Security Code: 123456            COS: 1              Display Language: english
                                                      H.320 Conversion? n

DIRECT TRUNK GROUP SELECT BUTTON ASSIGNMENTS (Trunk Access Codes)
     Local Remote             Local Remote              Local Remote
  1:                    5:                        9:
  2:                    6:                       10:
  3:                    7:                       11:
  4:                    8:                       12:

HUNDREDS SELECT BUTTON ASSIGNMENTS
  1:           5:           9:           13:           17:
  2:           6:          10:           14:           18:
  3:           7:          11:           15:           19:
  4:           8:          12:           16:           20:
```

- Type: 302
- Console Type: "principal" for a single one-X Attendant. Only one "principal and one "night (day/night)" is possible per system
- Port: IP
- Security code: code which also must be entered during login of one-X Attendant at CM

Page 2



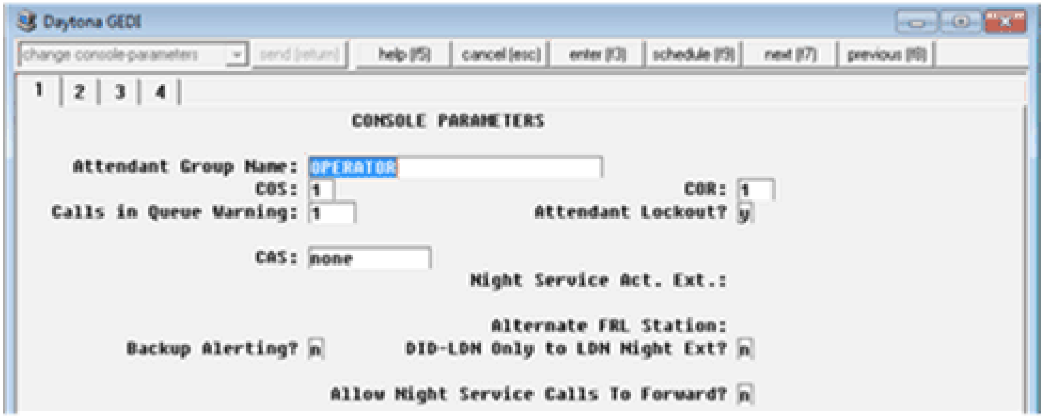
```
                          ATTENDANT CONSOLE

VIS FEATURE OPTIONS

                   Auto Start? n
           Echo Digits Dialed? y

IP FEATURE OPTIONS

 Remote Softphone Emergency Calls: as-on-local Direct IP-IP Audio Connections? y
 Emergency Location Ext: 6004              Always Use? n   IP Audio Hairpinning? n
                                                      Service Link Mode: permanent
```

The **Auto Start** should be set to to "n", because one-X Attendant initiates a start itself.

The Feature Button Assignments on page 3 list up to 24 functions which you can assign to the keypad and hotkeys in one-X Attendant. You can call each of these functions using the corresponding button (1-24). You can create user-defined labels for the feature buttons assigned functions 1-24. More detailed information to the feature buttons is available in one-X Attendant Installation and Administration Manual.

3. Change Console Parameters

Page 1

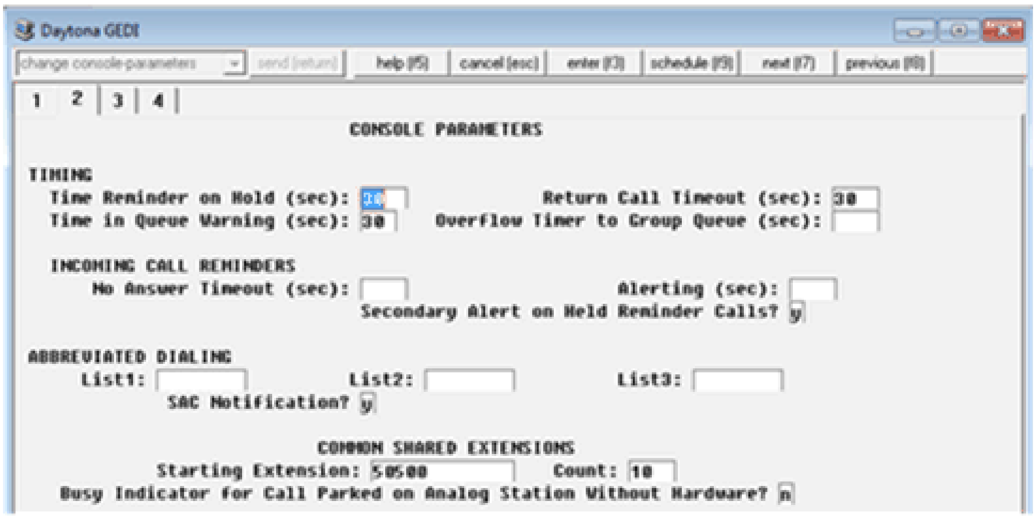


```
                         CONSOLE PARAMETERS

     Attendant Group Name: OPERATOR
                      COS: 1                          COR: 1
   Calls in Queue Warning: 1            Attendant Lockout? y

                      CAS: none
                                 Night Service Act. Ext.:

                                   Alternate FRL Station:
          Backup Alerting? n     DID-LDN Only to LDN Night Ext? n

                            Allow Night Service Calls To Forward? n
```

Enter the following values:

- **COS, COR:** for one-X Attendant enter the desired classes
- **Calls in Queue Warning:** Specified from which number of waiting callers backup telephone become signaled.

Page 2

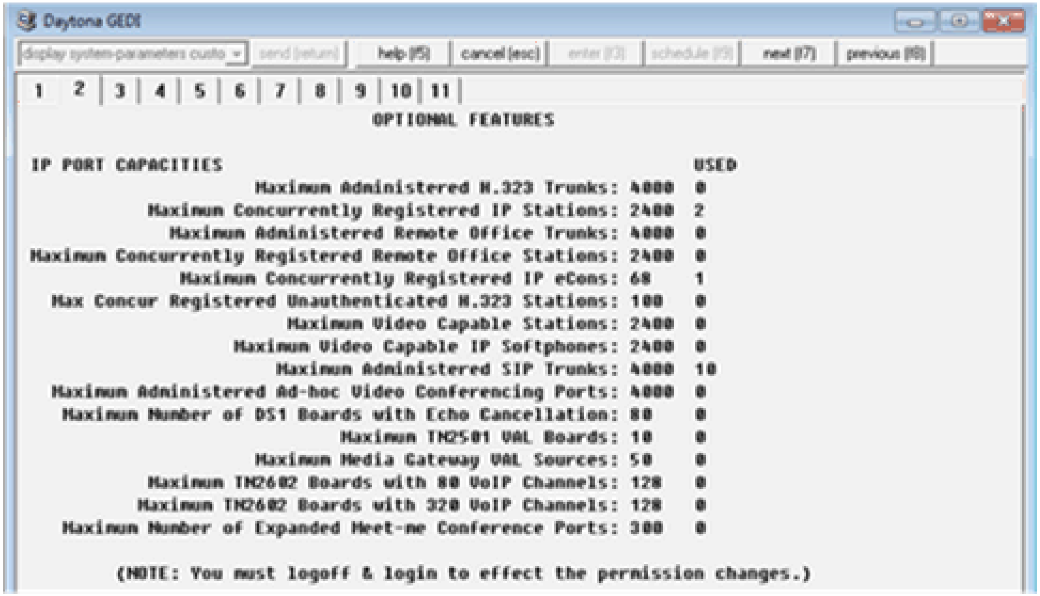


```
                         CONSOLE PARAMETERS

TIMING
  Time Reminder on Hold (sec): 30          Return Call Timeout (sec): 30
  Time in Queue Warning (sec): 30   Overflow Timer to Group Queue (sec):

  INCOMING CALL REMINDERS
      No Answer Timeout (sec):                    Alerting (sec):
                              Secondary Alert on Held Reminder Calls? y

ABBREVIATED DIALING
     List1:                   List2:                   List3:
            SAC Notification? y

                        COMMON SHARED EXTENSIONS
           Starting Extension: 50500           Count: 10
  Busy Indicator for Call Parked on Analog Station Without Hardware? n
```

- **Time Reminder on Hold:** Time after which the one-X Attendant will be reminded of a held call.
- **Return Call Timeout:** Time after which a waiting call will be included again in the call queue.
- **Time in Queue Warning:** Time after which the one-X Attendant will be reminded of a call waiting in a queue.
- **ABBREVIATED DIALING:** If you use abbreviated dialing you must specify here the names of the lists used.
- **COMMON SHARED EXTENSIONS:** If you use common shared extensions for parking calls enter the first extension number in the field Starting Extension and under COUNT the number of subsequent numbers.

4. Display system-parameters customer-options

Page 2 (shown)



```
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                                 USED
                      Maximum Administered H.323 Trunks: 4000      0
          Maximum Concurrently Registered IP Stations: 2400        2
            Maximum Administered Remote Office Trunks: 4000        0
Maximum Concurrently Registered Remote Office Stations: 2400       0
              Maximum Concurrently Registered IP eCons: 68         1
  Max Concur Registered Unauthenticated H.323 Stations: 100        0
                       Maximum Video Capable Stations: 2400        0
                  Maximum Video Capable IP Softphones: 2400        0
                      Maximum Administered SIP Trunks: 4000        10
  Maximum Administered Ad-hoc Video Conferencing Ports: 4000       0
   Maximum Number of DS1 Boards with Echo Cancellation: 80         0
                            Maximum TN2501 VAL Boards: 10          0
                    Maximum Media Gateway VAL Sources: 50          0
          Maximum TN2602 Boards with 80 VoIP Channels: 128         0
         Maximum TN2602 Boards with 320 VoIP Channels: 128         0
   Maximum Number of Expanded Meet-me Conference Ports: 300        0

        (NOTE: You must logoff & login to effect the permission changes.)
```

- **Maximum Concurrently Registered IP Stations:** The parameter must be sufficiently large to meet the requirements of the "IP Stations".
- **Maximum Concurrently Registered IP eCons:** The parameter must be at least as large as the number of one-X Attendants which can be connected.

Page 4 (not shown)

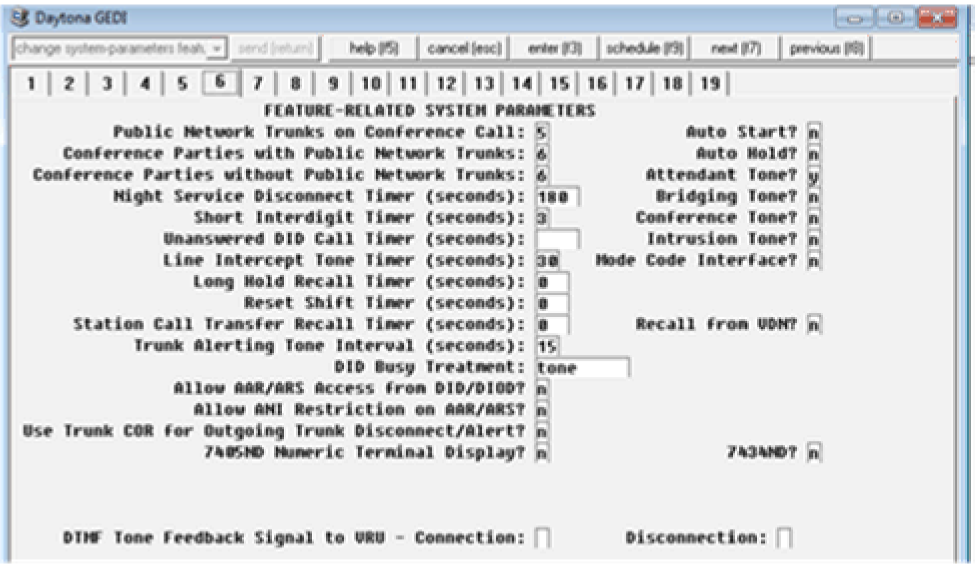
- **IP Stations** and **IP Attendant Consoles** must be set to “y”

Page 10 (not shown)

- **IP_eCons:** The parameter must be chosen to be at least as large as the maximum number of one-X Attendants which will be running at the same time.

5. Change system parameter features

Page 7



```
                        FEATURE-RELATED SYSTEM PARAMETERS
        Public Network Trunks on Conference Call: 5            Auto Start? n
     Conference Parties with Public Network Trunks: 6             Auto Hold? n
  Conference Parties without Public Network Trunks: 6        Attendant Tone? y
        Night Service Disconnect Timer (seconds): 180         Bridging Tone? n
                Short Interdigit Timer (seconds): 3         Conference Tone? n
             Unanswered DID Call Timer (seconds):            Intrusion Tone? n
             Line Intercept Tone Timer (seconds): 30   Mode Code Interface? n
                Long Hold Recall Timer (seconds): 0
                     Reset Shift Timer (seconds): 0
       Station Call Transfer Recall Timer (seconds): 0      Recall from VDN? n
          Trunk Alerting Tone Interval (seconds): 15
                             DID Busy Treatment: tone
              Allow AAR/ARS Access from DID/DIOD? n
               Allow ANI Restriction on AAR/ARS? n
 Use Trunk COR for Outgoing Trunk Disconnect/Alert? n
               7405ND Numeric Terminal Display? n                   7434ND? n



     DTMF Tone Feedback Signal to VRU - Connection:          Disconnection:
```

The screenshot shows typical settings for these parameters.

Auto Hold must be set to "y" so that "auto hold" can be used by one-x Attendant.

Auto Start must be set to "n".

Transfer Upon Hang-up must be set to "y", so that the Transfer key does not need to be pressed twice to transfer a call.

SMGR Configuration for one-X Attendant

Configure SMGR user of type Attendant for one-X® Attendant

In SMGR you cannot configure an attendant for the CM. The attendant has to be added to the CM using ASA.

Nevertheless we need a SMGR user for one-X® Attendant to

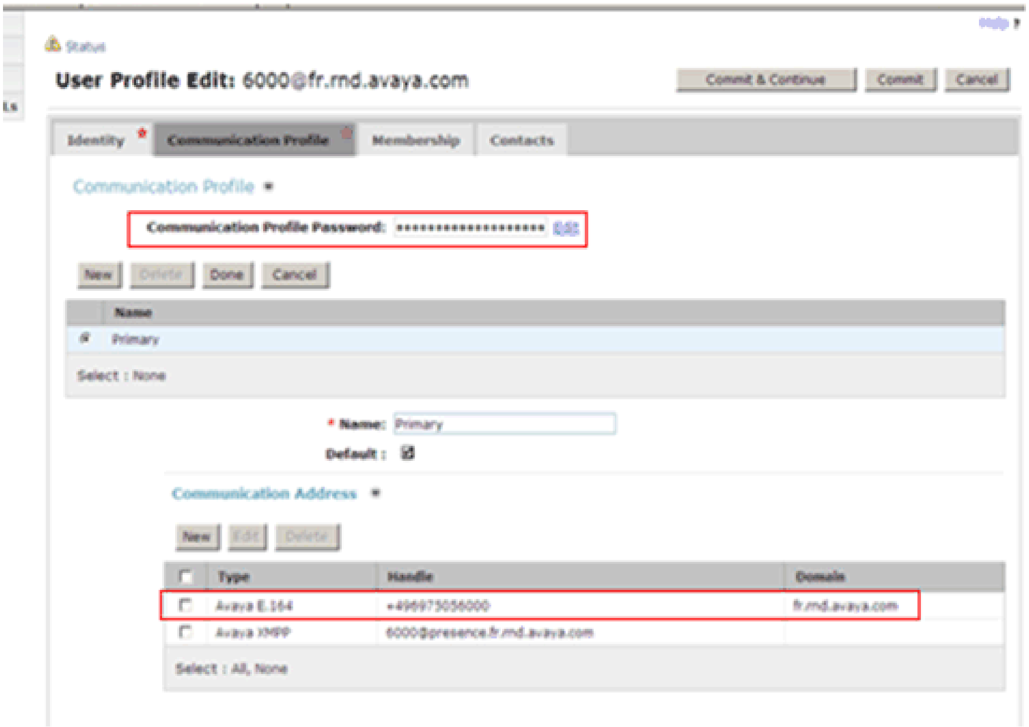
- have the Avaya XMPP communication address to register one-X® Attendant for Instant Messaging
- adding the one-X® Attendant to the contact list as presence buddy of another phone device like 1XC or ADVD

One-X® Attendant in SMGR needs an E.164 handle. The XMPP handle is automatically entered for the user in SMGR after replication with Presence Server. **Please do not enter yourself!** It is necessary to specify the communication profile password (this number is used when user logs into station).

The SMGR user for one-X® Attendant has no Session Manager Profile and no CM Endpoint profile, therefore the checkboxes "Session Manager Profile" and "CM Endpoint Profile" will remain empty. You can't use an existing endpoint in "CM Endpoint Profile".

Here an example for one-X® Attendant using extension.

Login Name is defined as 6000@fr.rnd.avaya.com on the Identity page.



User Profile Edit: 6000@fr.rnd.avaya.com

Communication Profile *

Communication Profile Password: ••••••••••••••••••••

	Name
●	Primary

Select : None

* Name: Primary

Default : ☑

Communication Address *

□	Type	Handle	Domain
□	Avaya E.164	+496975056000	fr.rnd.avaya.com
□	Avaya XMPP	6000@presence.fr.rnd.avaya.com	

Select : All, None

Bulk Users Export

System Manager is the central point of user administration for Avaya Aura™ solution.

SMGR provides a command line-based utility named `exportUpmUsers.sh` for bulk user export from SMGR’s database, that enables an administrator to import these users into the one-X® Attendant database, therefore *PuTTY* is needed. Remark: both SMGR 6.1 and 6.2 do NOT support a UI based bulk user export[1].

One-X attendant supports the SMGR Versions 6.1, 6.2, and 6.3 (6.2 FP1)

The SMGR bulk user export utility is stored in directory when you are using SMGR 6.1 or 6.2

```
$MGMT_HOME/upm/bulkexport/exportutility
```

The SMGR bulk user export utility is stored in directory when you are using SMGR 6.3

```
$MGMT_HOME/bulkadministration/exportutility
```

whereat `$MGMT_HOME` represents the System Manager’s home directory e.g.

```
/opt/Avaya/Mgmt/<version>
```

whereat `<version>` may look like *6.2.11* for SMGR 6.2 release.

In folder `$MGMT_HOME/upm/bulkexport/exportutility/exportutility`, file `readme.txt` is stored describing command line parameters for the bulk user export utility `exportUpmUsers.sh`:

1. -f	exported file name prefix (optional)
2. -r	number of records per file (optional)
3. -d	exported file location (optional)
4. -s	start index of record (optional)
5. -e	number of records to be exported(optional)
6. -t	job scheduling time (optional)

The job scheduling time format is: YYYY:MM:DD:HH:MM:SS.

Remark: SMGR 6.1 doesn't support any filter setting for bulk user export. Thus bulk user export utility for SMGR 6.1 will always export all users Bulk User Export.

It might be easier to modify the default parameters in property file

`bulkexportconfig.properpties`

located in sub folder

`$MGMT_HOME/upm/bulkexport/exportutility/config`

ATTENTION: Linux is case-sensitive, so please pay attention when using e.g. an WinSCP-integrated editor on Windows OS to modify bulkexportconfig.properpties saved on SMGR Linux server.

[1]

After having executed the bulk user export utility (shell script)

```
sh exportUpmUsers.sh
```

an `exportfile_<timestamp>.zip` file will be created in the directory specified by parameter exported file location . The `exportfile_<timestamp>.zip` file contains a XML file named `exportfile_1.xml w/` the exported users, next please use WinSCP to copy `exportfile_<timestamp>.zip` to one-X Attd server.

On one-X® Attendant server, please unzip `exportfile_<timestamp>.zip` to receive `exportfile_1.xml`.

Hint: for historical reasons, exportfile_1.xml is named exportfilesmgr_1 in IAM.

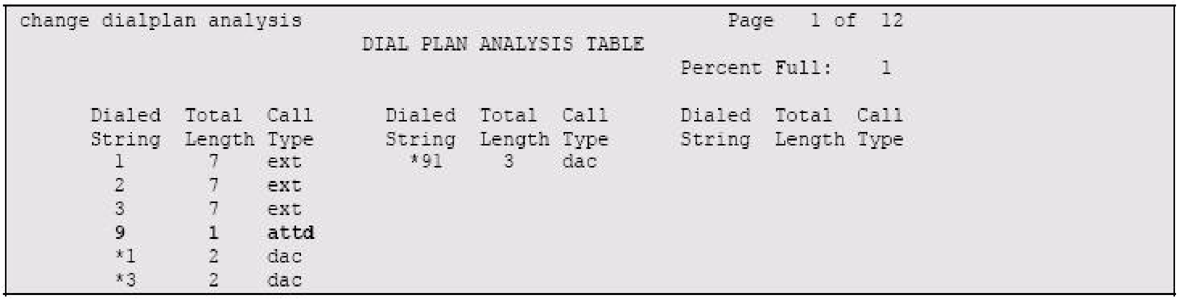
Avaya Communication Manager configuration examples

Configuration examples

General settings

The following screen shots are from the ASA configuration tool and depict example settings. They must of course be customized to your system configuration.

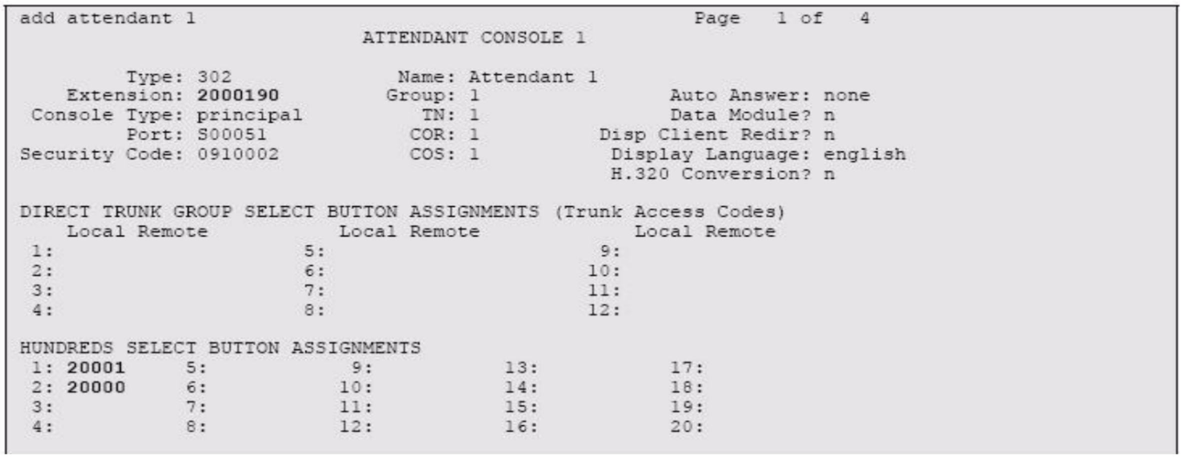
Note: In the text for the screen shots, only the settings which differ from the default settings or are absolutely necessary for one–X Attendant are referred to.Settings under DIAL PLAN ANALYSIS TABLE



```
change dialplan analysis                                    Page   1 of  12
                              DIAL PLAN ANALYSIS TABLE
                                                      Percent Full:    1

      Dialed  Total  Call       Dialed  Total  Call       Dialed  Total  Call
      String  Length Type       String  Length Type       String  Length Type
        1       7    ext          *91     3    dac
        2       7    ext
        3       7    ext
        9       1    attd
        *1      2    dac
        *3      2    dac
```

For the **Call Type** attd, a digit (**Dialed String**) must be predefined in “dialplan”, with which one-X Attendant can be called internally. You can use any digit that does not conflict with other settings (“9” in this example).

Settings under ATTENDANT CONSOLE



```
add attendant 1                                          Page   1 of   4
                             ATTENDANT CONSOLE 1

         Type: 302              Name: Attendant 1
    Extension: 2000190         Group: 1                Auto Answer: none
 Console Type: principal          TN: 1                Data Module? n
         Port: S00051            COR: 1          Disp Client Redir? n
Security Code: 0910002           COS: 1           Display Language: english
                                                  H.320 Conversion? n

DIRECT TRUNK GROUP SELECT BUTTON ASSIGNMENTS (Trunk Access Codes)
    Local Remote           Local Remote             Local Remote
 1:                     5:                       9:
 2:                     6:                      10:
 3:                     7:                      11:
 4:                     8:                      12:

HUNDREDS SELECT BUTTON ASSIGNMENTS
 1: 20001     5:             9:            13:            17:
 2: 20000     6:            10:            14:            18:
 3:           7:            11:            15:            19:
 4:           8:            12:            16:            20:
```

Here you set up one-X Attendant as “attendant console”.

Type: 302

Name: Arbitrary name.

Extension: Operator’s number of the one–X Attendant. You can accept operator calls in night service or with a locked operator set.

ConsoleType: “principal”, for a single one-X Attendant. Only one “principal”

and one “night (day/night)” is possible per system.

Security code: code which also must be entered during login of one-X Attendant at the CM.

Display language: “english”. This is the only setting that ensures that one-X Attendant is signaled correctly.

Hundreds select button assignment: Define the number range you want to be displayed in the internal busy display. Entries made using HUNDREDS SELECT BUTTON ASSIGNMENTS must always be in the format YYYxx.

Ones and tens places are not entered since the ranges always begin with 00

and end with 99.

The entries must always be started at the “1:” and none of the digits may be skipped. It would therefore be incorrect for instance to enter three number ranges under 1:, 2: and 4: (“3:” being omitted).

Example: For the range 2000100 to 2000199 enter 20001. For the range

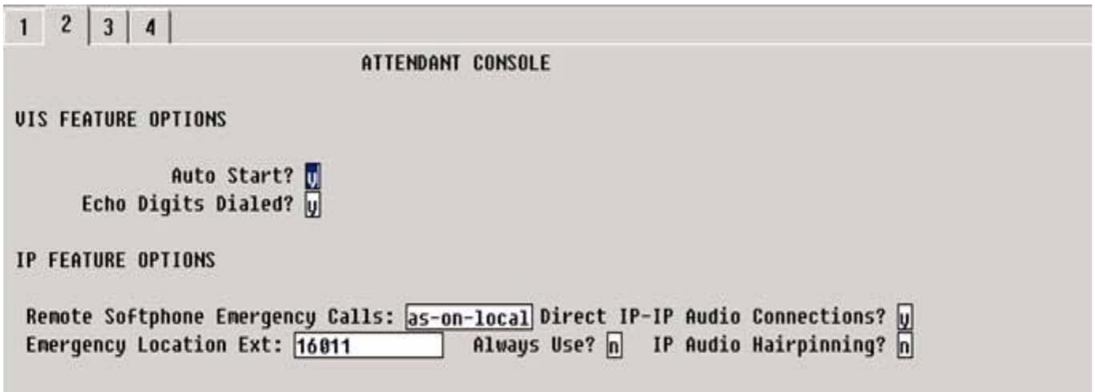
2001900 to 2001999 enter 20019.

HINT:

Configuring Call Park with 1XAttd:

Call Park with 1XAttd requires the used Common Shared Extensions are contained in a HUNDRED GROUP assigned the attendant in CM, and contained in the internal Busy Display assigned the Workprofile of 1XAttd client.

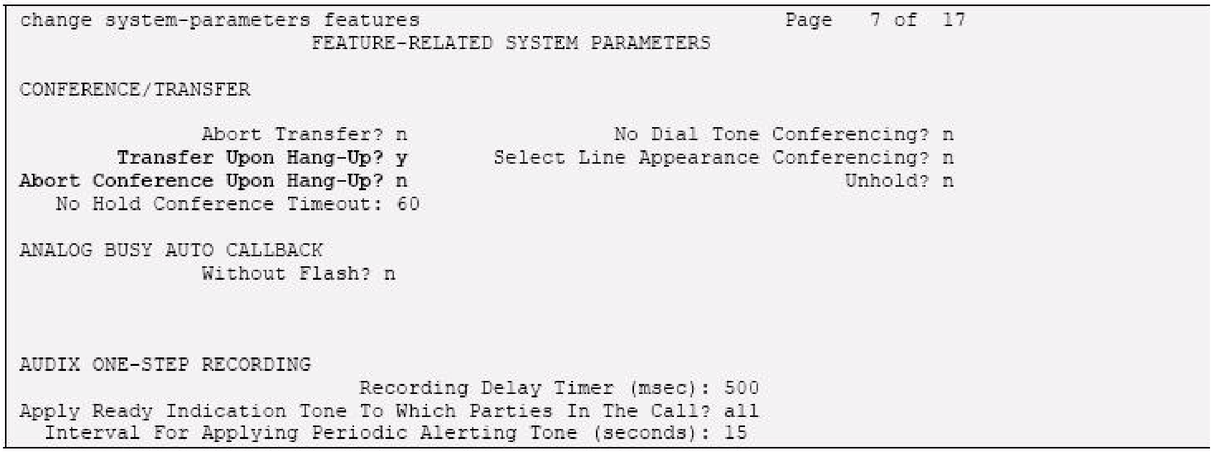
Otherwise the status display of the Park button doesn't work, also the status display in the Tooltip doesn't work, and the attendant is not able to un-park (pick up) a parked call.



```
                                 ATTENDANT CONSOLE

VIS FEATURE OPTIONS

              Auto Start? y
       Echo Digits Dialed? y

IP FEATURE OPTIONS

 Remote Softphone Emergency Calls: as-on-local Direct IP-IP Audio Connections? y
 Emergency Location Ext: 16011           Always Use? n   IP Audio Hairpinning? n
```

The **Auto Start** should be set to “n”, because one-X Attendant initiates a start itself.

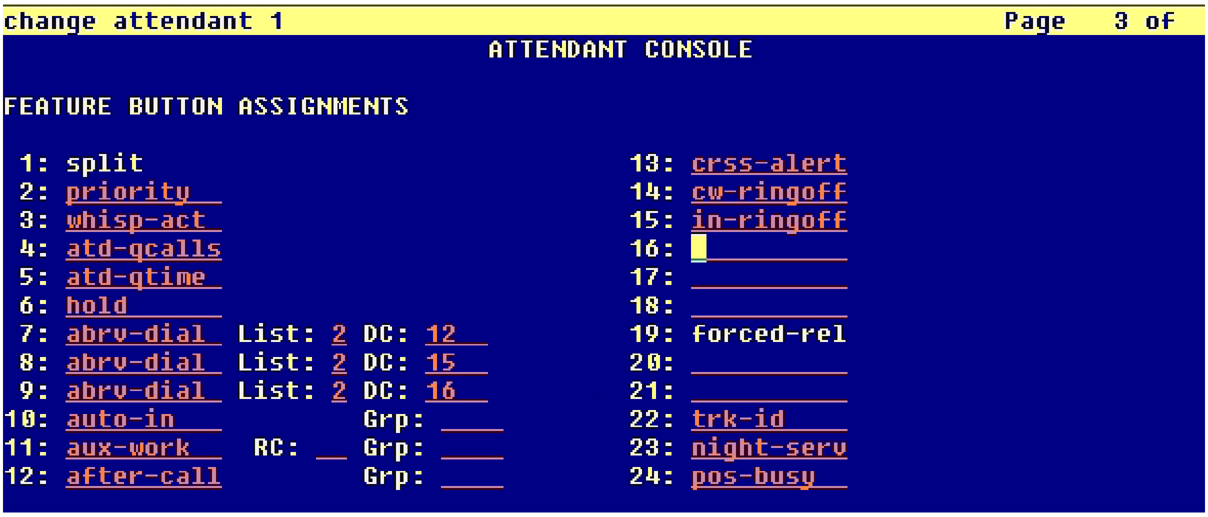
Feature buttons on the keypad



```
change system-parameters features                              Page   7 of  17
                        FEATURE-RELATED SYSTEM PARAMETERS

CONFERENCE/TRANSFER

               Abort Transfer? n                 No Dial Tone Conferencing? n
        Transfer Upon Hang-Up? y       Select Line Appearance Conferencing? n
Abort Conference Upon Hang-Up? n                                    Unhold? n
   No Hold Conference Timeout: 60

ANALOG BUSY AUTO CALLBACK
               Without Flash? n



AUDIX ONE-STEP RECORDING
                            Recording Delay Timer (msec): 500
Apply Ready Indication Tone To Which Parties In The Call? all
  Interval For Applying Periodic Alerting Tone (seconds): 15
```

FEATURE BUTTON ASSIGNMENTS lists up to 24 functions, which you can assign to the keypad and hotkeys in one-X Attendant. You can call each of these functions using the corresponding button (1–24). You can create user–defined labels for the feature buttons assigned functions 1-24.

.



```
change attendant 1                                          Page   3 of
                              ATTENDANT CONSOLE

FEATURE BUTTON ASSIGNMENTS

 1: split                                 13: crss-alert
 2: priority                              14: cw-ringoff
 3: whisp-act                             15: in-ringoff
 4: atd-qcalls                            16:
 5: atd-qtime                             17:
 6: hold                                  18:
 7: abrv-dial  List: 2 DC: 12             19: forced-rel
 8: abrv-dial  List: 2 DC: 15             20:
 9: abrv-dial  List: 2 DC: 16             21:
10: auto-in            Grp:               22: trk-id
11: aux-work    RC:    Grp:               23: night-serv
12: after-call         Grp:               24: pos-busy
```

The following buttons are pre–defined for one-X Attendant v4.00:

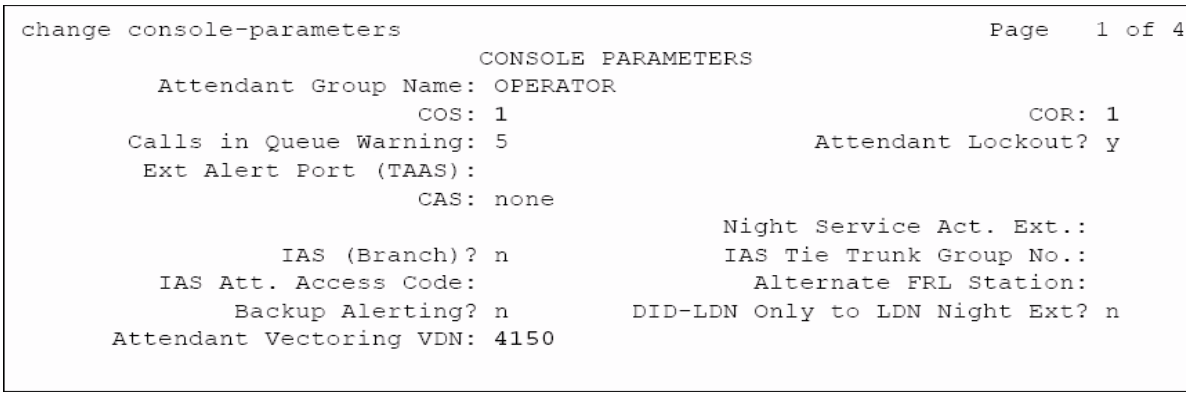
Name	Function
atd–qcalls	Shows the status of the queue. The queue contains all calls in the exchange group that have not yet been assigned to an operator.
**crss–alert	Indicates whether the pending call is an emergency call.
night-serv	Indicates the night service status of the entire exchange group.
*override	Requires that a call must have been made from your operator set but not yet answered. When you initiate a new call with this key, the previous call is deleted and replaced by the new call.
**priority	Initiates a prioritized call or prioritizes the current call.
*pos–busy	Places your operator set in “Off” mode.
*serial–cal	Changes the status of the current incoming call to a serial call.
*split	Initiates a conference between the current party and a waiting party.
hold	Used to place the current connection on hold. The waiting call is shown as a call on hold in the preview.

Notes:

You will have to set up a feature button with the **split-swap** function. Otherwise, one-X Attendant won’t be able to toggle between the two communications in the operator window.

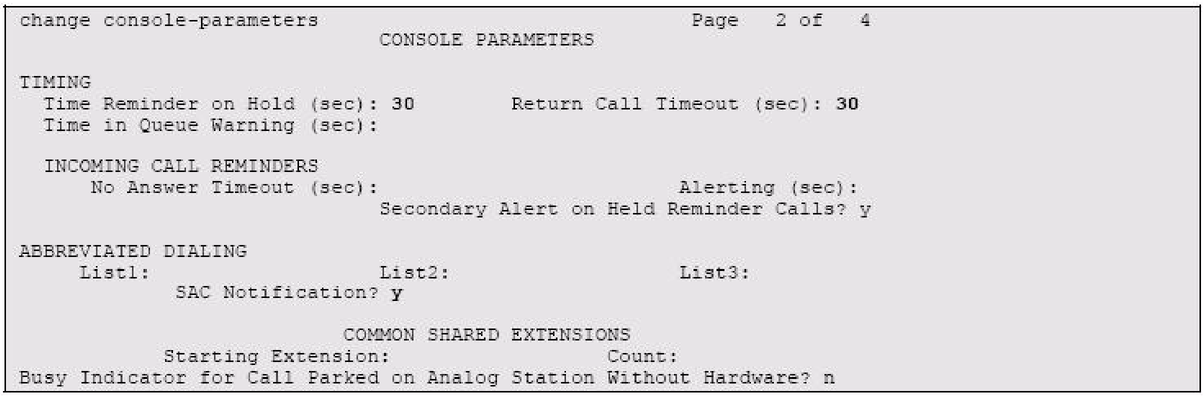
For convenience in operation we strongly recommend that you set up the following functions: **split**, **atd-qcalls**, **night-serv**, **pos-busy**. If you wish to use ACD call center functions, additional **q-calls**, so that you are shown the current waiting queue of the hunt group(s) (one-X Attendant displays only one unidentified current waiting queue, even with membership in several hunt groups).

Settings under CONSOLE PARAMETERS



```
change console-parameters                                       Page   1 of 4
                              CONSOLE PARAMETERS
         Attendant Group Name: OPERATOR
                          COS: 1                                    COR: 1
       Calls in Queue Warning: 5                  Attendant Lockout? y
        Ext Alert Port (TAAS):
                          CAS: none
                                                Night Service Act. Ext.:
                  IAS (Branch)? n               IAS Tie Trunk Group No.:
         IAS Att. Access Code:                    Alternate FRL Station:
               Backup Alerting? n        DID-LDN Only to LDN Night Ext? n
      Attendant Vectoring VDN: 4150
```

Enter the following values.
COS, COR: For one–X Attendant enter the desired classes
Calls in Queue Warning: Specifies from what number of waiting callers backup telephones become signaled.
Attendant Vectoring VDN: If you wish to use Attendant Vectoring , enter here the VDN of the desired vector.



```
change console-parameters                             Page   2 of   4
                              CONSOLE PARAMETERS

TIMING
  Time Reminder on Hold (sec): 30       Return Call Timeout (sec): 30
  Time in Queue Warning (sec):

  INCOMING CALL REMINDERS
      No Answer Timeout (sec):                       Alerting (sec):
                              Secondary Alert on Held Reminder Calls? y

ABBREVIATED DIALING
     List1:                   List2:                   List3:
             SAC Notification? y

                           COMMON SHARED EXTENSIONS
            Starting Extension:                 Count:
Busy Indicator for Call Parked on Analog Station Without Hardware? n
```

Select the following pages according to your requirements:

Time Reminder on Hold: Time after which the one–X Attendant will be reminded of a held call

Return Call Timeout: Time after which a waiting call will be included again in the call queue

Time in Queue Warning: Time after which the one–X Attendant will be reminded of a call waiting in a queue.

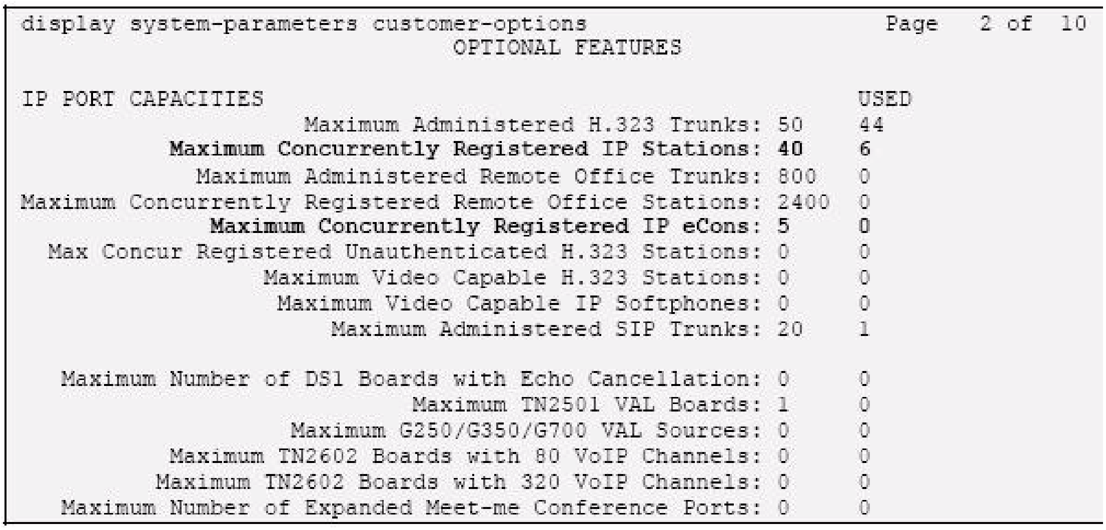
ABBREVIATED DIALING: If you use abbreviated dialing, you must specify here the names of the lists used. In the example, “group 5” will be used as list 2.

COMMON SHARED EXTENSIONS: If you use common shared extensions for parking calls, enter the first extension number in the field **Starting Extension** and under **COUNT** the number of subsequent numbers.

The numbers you want to use for parking calls, have to be assigned in this menu otherwise the parking will have failures in the way that the status display for the parked call will not be in function and parked calls can not be picked up.

Tab 3 (not shown) lets you change the priorities with which different call types are evaluated.
Tab 4, (not shown), displays all the attendants which are set up.

Settings under OPTIONAL FEATURES

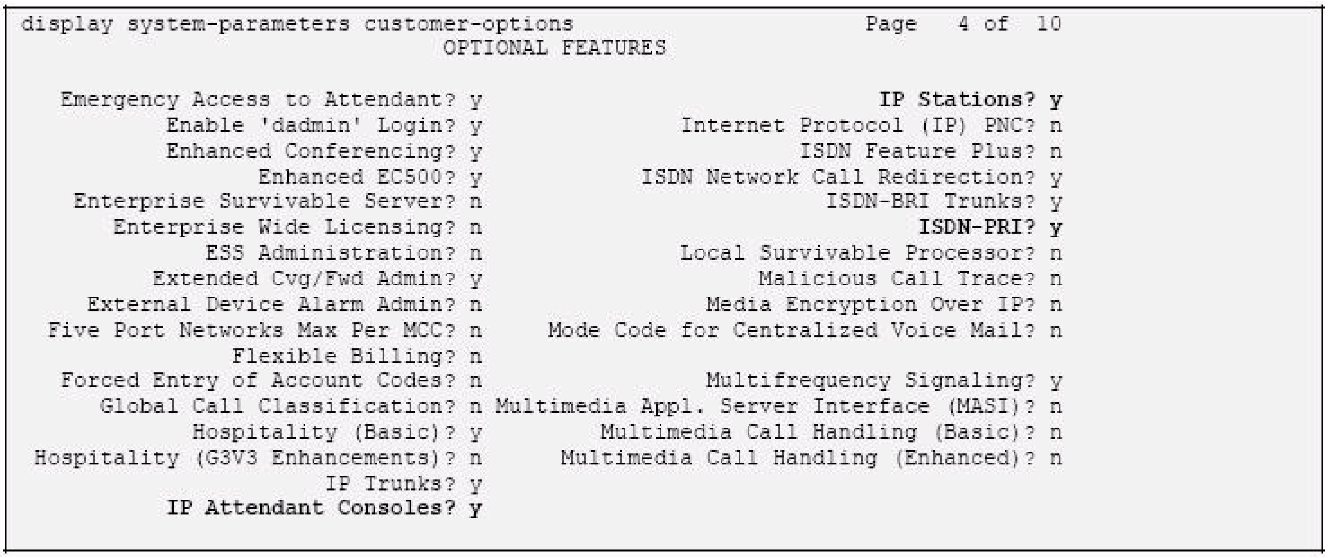


```
display system-parameters customer-options                      Page   2 of  10
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                              USED
                     Maximum Administered H.323 Trunks: 50      44
          Maximum Concurrently Registered IP Stations: 40       6
               Maximum Administered Remote Office Trunks: 800    0
Maximum Concurrently Registered Remote Office Stations: 2400    0
             Maximum Concurrently Registered IP eCons: 5        0
  Max Concur Registered Unauthenticated H.323 Stations: 0       0
                   Maximum Video Capable H.323 Stations: 0      0
                    Maximum Video Capable IP Softphones: 0      0
                        Maximum Administered SIP Trunks: 20     1

   Maximum Number of DS1 Boards with Echo Cancellation: 0       0
                              Maximum TN2501 VAL Boards: 1      0
                     Maximum G250/G350/G700 VAL Sources: 0      0
           Maximum TN2602 Boards with 80 VoIP Channels: 0       0
          Maximum TN2602 Boards with 320 VoIP Channels: 0       0
   Maximum Number of Expanded Meet-me Conference Ports: 0       0
```

The bold entries on the following screenshots show values for minimum system requirements. For more information, please contact your system specialist.

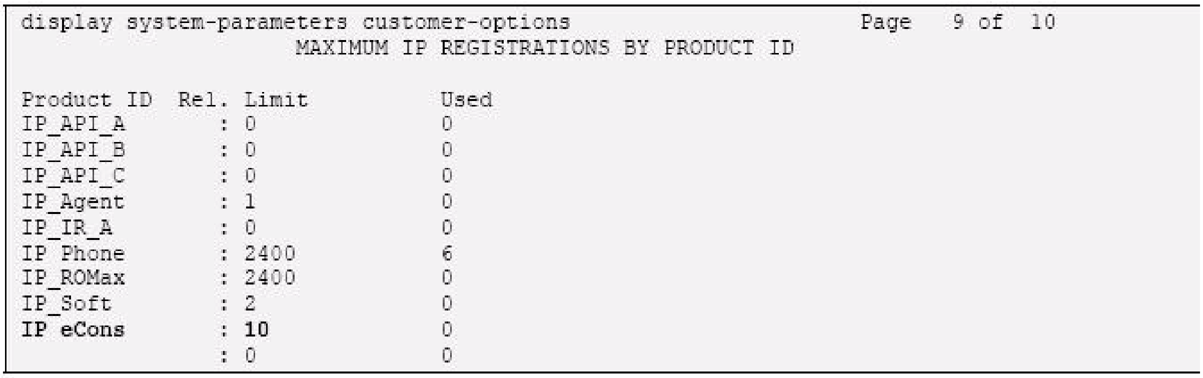
Maximum Concurrently Registered IP Stations: The parameter must be sufficiently large to meet the requirements of the "IP Stations".

Maximum Concurrently Registered IP eCons: The parameter must be at least as large as the number of one–X Attendants which can be connected.



```
display system-parameters customer-options                      Page   4 of  10
                                OPTIONAL FEATURES

    Emergency Access to Attendant? y                           IP Stations? y
            Enable 'dadmin' Login? y             Internet Protocol (IP) PNC? n
            Enhanced Conferencing? y                     ISDN Feature Plus? n
                   Enhanced EC500? y          ISDN Network Call Redirection? y
     Enterprise Survivable Server? n                        ISDN-BRI Trunks? y
         Enterprise Wide Licensing? n                              ISDN-PRI? y
                ESS Administration? n            Local Survivable Processor? n
           Extended Cvg/Fwd Admin? y                 Malicious Call Trace? n
       External Device Alarm Admin? n             Media Encryption Over IP? n
    Five Port Networks Max Per MCC? n    Mode Code for Centralized Voice Mail? n
                   Flexible Billing? n
    Forced Entry of Account Codes? n                 Multifrequency Signaling? y
       Global Call Classification? n Multimedia Appl. Server Interface (MASI)? n
              Hospitality (Basic)? y        Multimedia Call Handling (Basic)? n
  Hospitality (G3V3 Enhancements)? n     Multimedia Call Handling (Enhanced)? n
                        IP Trunks? y
             IP Attendant Consoles? y
```

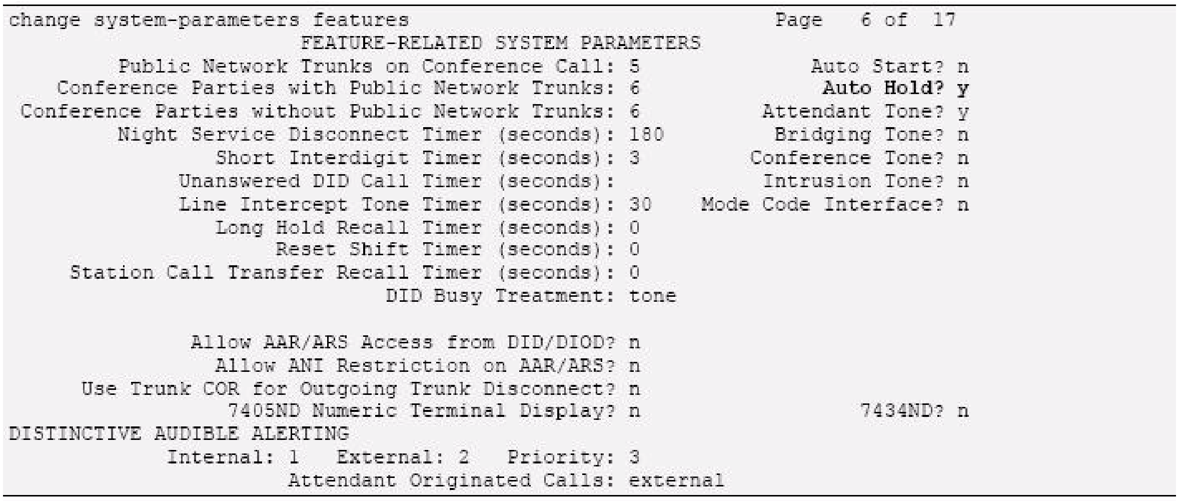
IP Stations, IP Attendant Console: Must be set to "y".



```
display system-parameters customer-options                    Page   9 of  10
                     MAXIMUM IP REGISTRATIONS BY PRODUCT ID

Product ID  Rel. Limit          Used
IP_API_A       : 0              0
IP_API_B       : 0              0
IP_API_C       : 0              0
IP_Agent       : 1              0
IP_IR_A        : 0              0
IP Phone       : 2400           6
IP_ROMax       : 2400           0
IP_Soft        : 2              0
IP eCons       : 10             0
               : 0              0
```

IP_eCons: The parameter must be chosen to be at least as large as the maximum number of one–X Attendants which will be running at the same time.

Settings under FEATURE RELATED SYSTEM PARAMETERS



```
change system-parameters features                              Page   6 of  17
                        FEATURE-RELATED SYSTEM PARAMETERS
         Public Network Trunks on Conference Call: 5               Auto Start? n
    Conference Parties with Public Network Trunks: 6                Auto Hold? y
 Conference Parties without Public Network Trunks: 6           Attendant Tone? y
         Night Service Disconnect Timer (seconds): 180          Bridging Tone? n
                 Short Interdigit Timer (seconds): 3          Conference Tone? n
              Unanswered DID Call Timer (seconds):             Intrusion Tone? n
              Line Intercept Tone Timer (seconds): 30    Mode Code Interface? n
                 Long Hold Recall Timer (seconds): 0
                      Reset Shift Timer (seconds): 0
     Station Call Transfer Recall Timer (seconds): 0
                               DID Busy Treatment: tone

               Allow AAR/ARS Access from DID/DIOD? n
                 Allow ANI Restriction on AAR/ARS? n
      Use Trunk COR for Outgoing Trunk Disconnect? n
                  7405ND Numeric Terminal Display? n                   7434ND? n
DISTINCTIVE AUDIBLE ALERTING
             Internal: 1   External: 2   Priority: 3
                       Attendant Originated Calls: external
```

The screenshot shows typical settings for these parameters. Settings in bold are the values for minimum system requirements. **Auto Hold** must be set to “y” so that “auto hold” can be used by one-X Attendant.

Auto Start must be set to “n”.

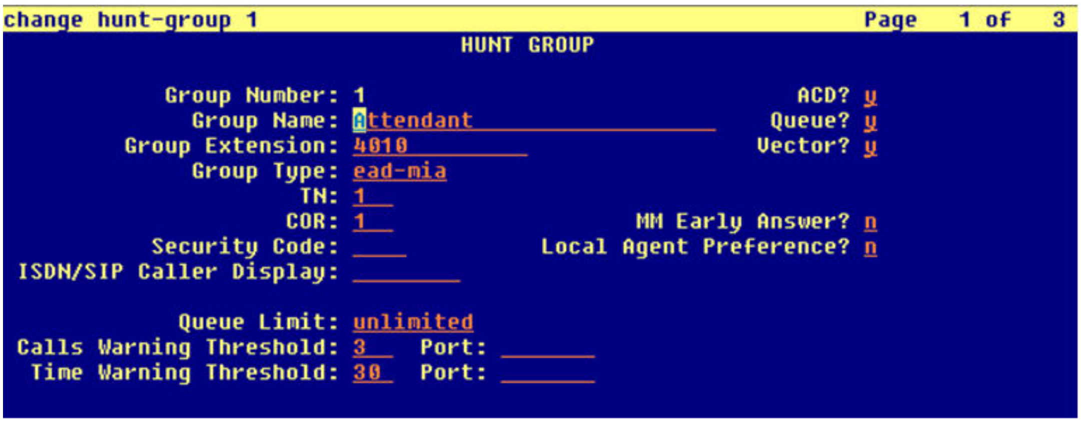
Transfer Upon Hang-up must be set to “y”, so that the Transfer key does not need to be pressed twice to transfer a call.

Settings under CLASS OF SERVICE (not shown)

In the settings for Console Parameters or Attendant Console, select only one COS-class which has the value “y” in the fields **Console Permissions**, **Call Forwarding** and **Priority Calling** (optional).

Using call center functions in a hunt group (optional)
All operator positions of the CM can be interconnected as agents into a hunt group. In a hunt group with call center functionality, call distribution can be even more finely configured than in the normal Attendant group, which usually controls the call distribution to the operator positions.
How call distribution within a hunt group takes place is configured in CM (see /2/, /3/)
The screen shots in this section correspond to the following scenario: Hunt group 1 **Attendant** is set up. It can be reached using the number 4010. An agent (= one-X Attendant) **Attendant2** belongs to the hunt group, and has the agent number 3109. There are various necessary function keys available for the agents, e.g. for logout.

Settings under HUNT GROUP



```
change hunt-group 1                                             Page   1 of   3
                                  HUNT GROUP

            Group Number: 1                                 ACD? y
              Group Name: Attendant                       Queue? y
         Group Extension: 4010                           Vector? y
              Group Type: ead-mia
                      TN: 1
                     COR: 1                       MM Early Answer? n
           Security Code:                  Local Agent Preference? n
 ISDN/SIP Caller Display:

             Queue Limit: unlimited
 Calls Warning Threshold: 3     Port:
  Time Warning Threshold: 30    Port:
```

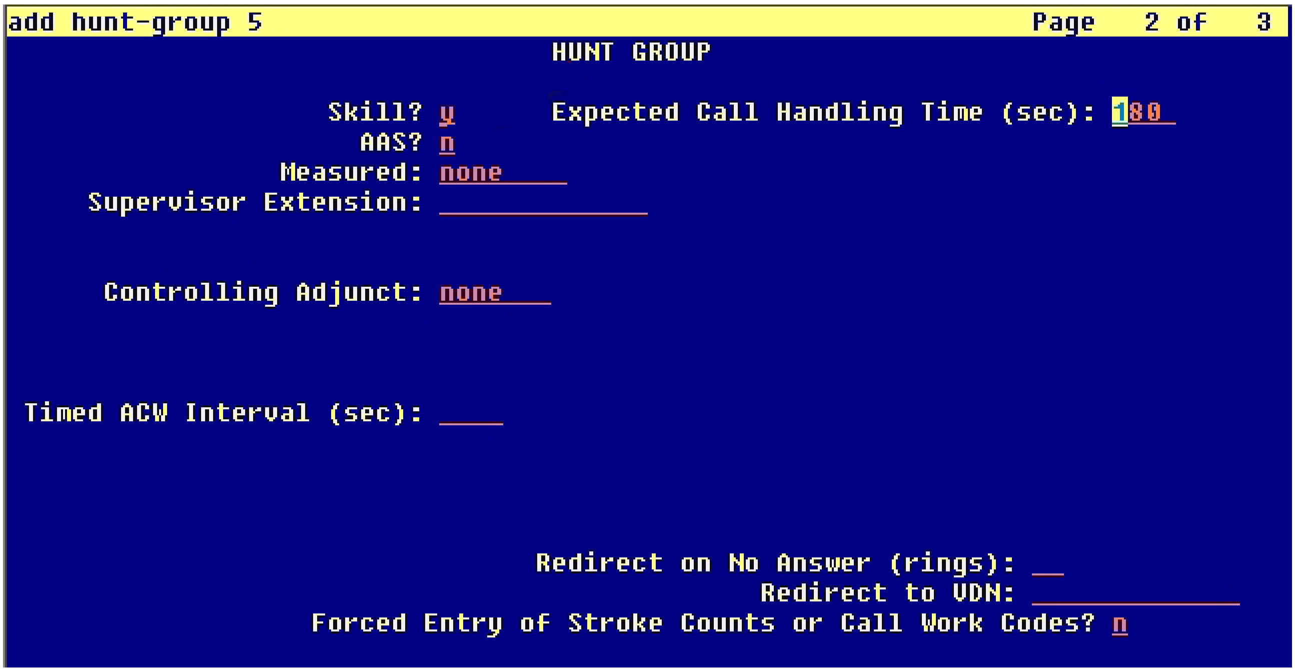
The screen shot shows the hunt group **Attendant**, which has also been prepared for Attendant Vectoring .

Group Name: Name of the Attendant hunt group

Group Extension: number of the hunt group

Group Type: “ead-mia” recommended for one-X Attendants

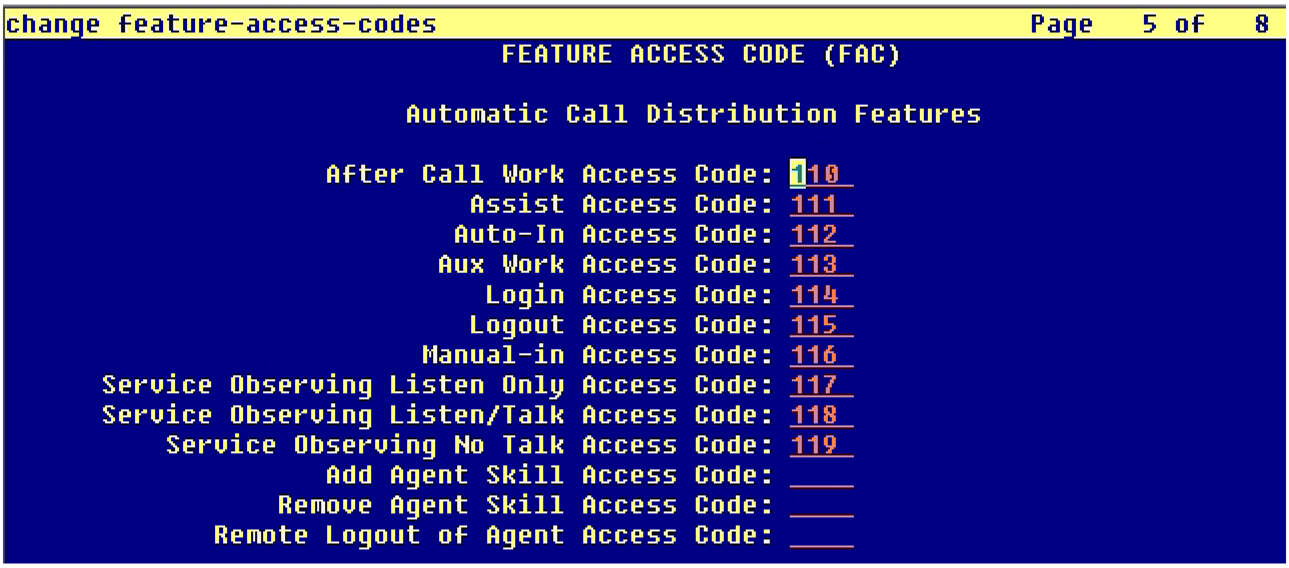
ACD, Queue, Vector: “y”



```
add hunt-group 5                                                Page   2 of   3
                                 HUNT GROUP

                    Skill? y     Expected Call Handling Time (sec): 180
                      AAS? n
                 Measured: none
     Supervisor Extension:


      Controlling Adjunct: none



 Timed ACW Interval (sec):




                                Redirect on No Answer (rings):
                                             Redirect to VDN:
                   Forced Entry of Stroke Counts or Call Work Codes? n
```

Answer **Skill?** with “y” and, if you wish to use attendant vectoring , under **Redirect to VDN** enter the VDN to which a call to the hunt group number should be forwarded.

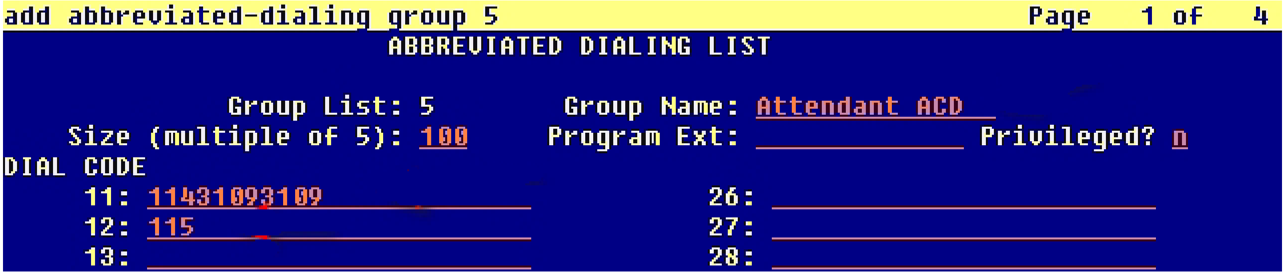
Setting of FEATURE ACCESS CODES (ACD Features)



```
change feature-access-codes                                 Page   5 of   8
                              FEATURE ACCESS CODE (FAC)

                         Automatic Call Distribution Features

                     After Call Work Access Code: 110
                            Assist Access Code: 111
                           Auto-In Access Code: 112
                          Aux Work Access Code: 113
                             Login Access Code: 114
                            Logout Access Code: 115
                         Manual-in Access Code: 116
     Service Observing Listen Only Access Code: 117
     Service Observing Listen/Talk Access Code: 118
         Service Observing No Talk Access Code: 119
                     Add Agent Skill Access Code: ____
                  Remove Agent Skill Access Code: ____
              Remote Logout of Agent Access Code: ____
```

Codes must be set for the following ACD features: **Login**, **Logout**, **Aux work**, **After Call Work** and **Auto-In**. The other settings are optional.

Allocating an ABBREVIATED DIALING LIST



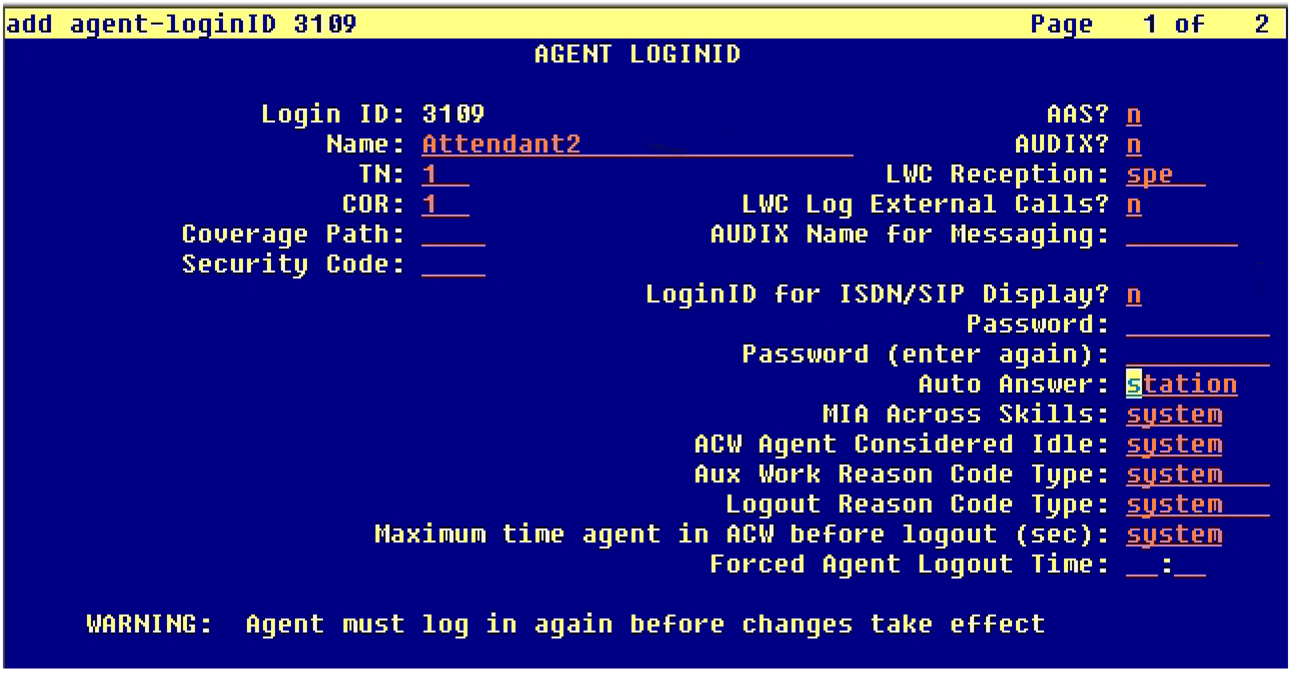
```
add abbreviated-dialing group 5                             Page   1 of   4
                         ABBREVIATED DIALING LIST

             Group List: 5          Group Name: Attendant ACD
   Size (multiple of 5): 100       Program Ext: _____________  Privileged? n
DIAL CODE
     11: 11431093109____________              26: ________________________
     12: 115________________________          27: ________________________
     13: ___________________________          28: ________________________
```

The DIAL CODES of the “feature access codes (fac)” set above are allocated in this list. Here the dial code **12** is allocated to **Logout** (fac = 115) and the dial code **11** to **Login** (fac = 114) of the agent with the number 3109 and whose password is 3109.

The dial codes are configured via FEATURE BUTTON ASSIGNMENTS as abbreviated dialing codes. In the example, key 7 is allocated the Abbreviated Dialing function abrv-dial. List 2 is consulted for the abbreviated code. In our example, this is list group 5, which was predefined in the CONSOLE PARAMETERS .

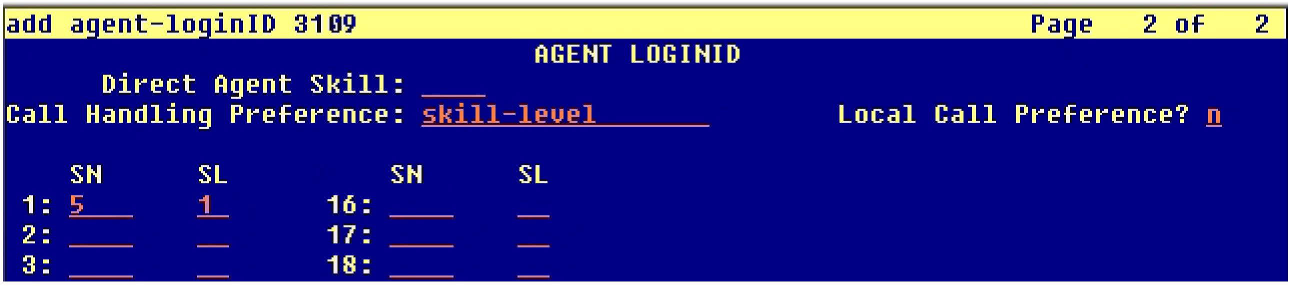
The digits which are provided under the abbreviated code (DC) 12 will be dialed. This is the fac 115, i.e. Logout. So if key 7 in one-X Attendant is now applied to a feature key, the agent can log out with it.

Settings under AGENT LOGINID



```
add agent-loginID 3109                                          Page   1 of   2
                                  AGENT LOGINID

                Login ID: 3109                                    AAS? n
                    Name: Attendant2                            AUDIX? n
                      TN: 1                            LWC Reception: spe
                     COR: 1                   LWC Log External Calls? n
           Coverage Path:                    AUDIX Name for Messaging:
           Security Code:
                                        LoginID for ISDN/SIP Display? n
                                                            Password:
                                              Password (enter again):
                                                         Auto Answer: station
                                                   MIA Across Skills: system
                                            ACW Agent Considered Idle: system
                                            Aux Work Reason Code Type: system
                                              Logout Reason Code Type: system
                       Maximum time agent in ACW before logout (sec): system
                                              Forced Agent Logout Time:   :

     WARNING:  Agent must log in again before changes take effect
```

Each one–X Attendant operator position corresponds to one agent. Important here are the **name** and the **password**, which are used to login to call distribution.



```
add agent-loginID 3109                                          Page   2 of   2
                                  AGENT LOGINID
      Direct Agent Skill:
Call Handling Preference: skill-level              Local Call Preference? n

    SN       SL           SN       SL
 1: 5        1       16:
 2:                  17:
 3:                  18:
```

On this panel you must still enter the agent’s skill numbers and the associated skill levels because skill was established as a distribution criteria in call distribution.

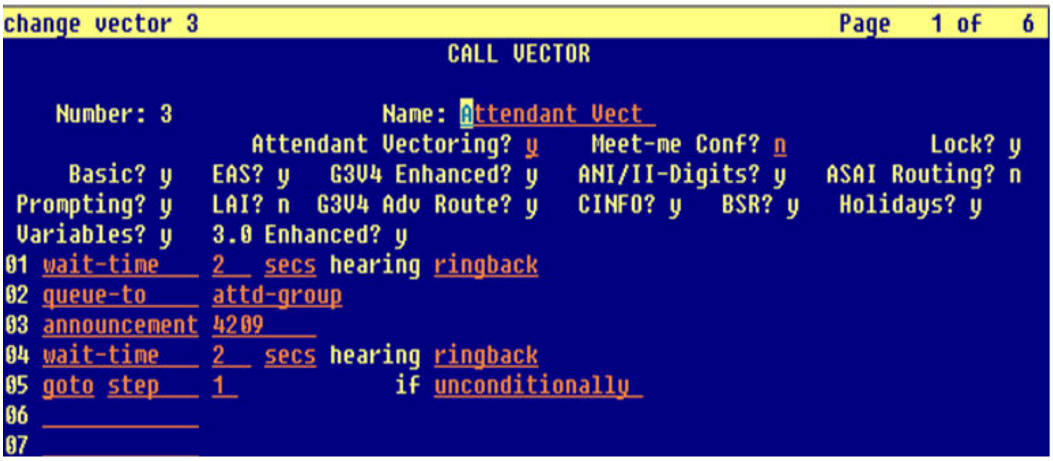
Using Attendant Vectoring (optional)

A vector is a sequence of commands. These tell the system how it should deal with incoming calls. They are used to control call forwarding and call processing. Vectors can be placed in a normal attendant group as well as in an automatic call distribution (ACD) hunt group.

Prerequisites:

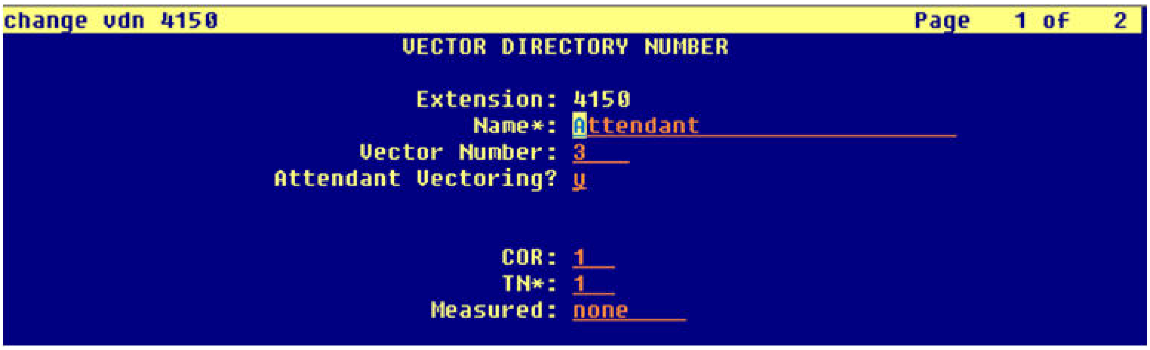
Attendant Group: Under OPTIONAL FEATURES (3#x), **Basic Call Vectoring** must be set to “y”.

Hunt group: Under HUNT GROUP (1#3), the field **Vector?** must be set to “y” and under HUNT GROUP (2#3), the appropriate VDN must be given at **Redirect to VDN**.



```
change vector 3                                               Page   1 of   6
                                  CALL VECTOR

   Number: 3                 Name: Attendant Vect
                     Attendant Vectoring? y    Meet-me Conf? n          Lock? y
    Basic? y   EAS? y   G3V4 Enhanced? y   ANI/II-Digits? y   ASAI Routing? n
 Prompting? y   LAI? n  G3V4 Adv Route? y   CINFO? y    BSR? y   Holidays? y
 Variables? y   3.0 Enhanced? y
01 wait-time    2   secs hearing ringback
02 queue-to     attd-group
03 announcement 4209
04 wait-time    2   secs hearing ringback
05 goto step    1             if unconditionally
06
07
```

The example shows a CALL VECTOR with the name “Attendant Vect”. For an interpretation of the command steps 01 to 05 see /4/.

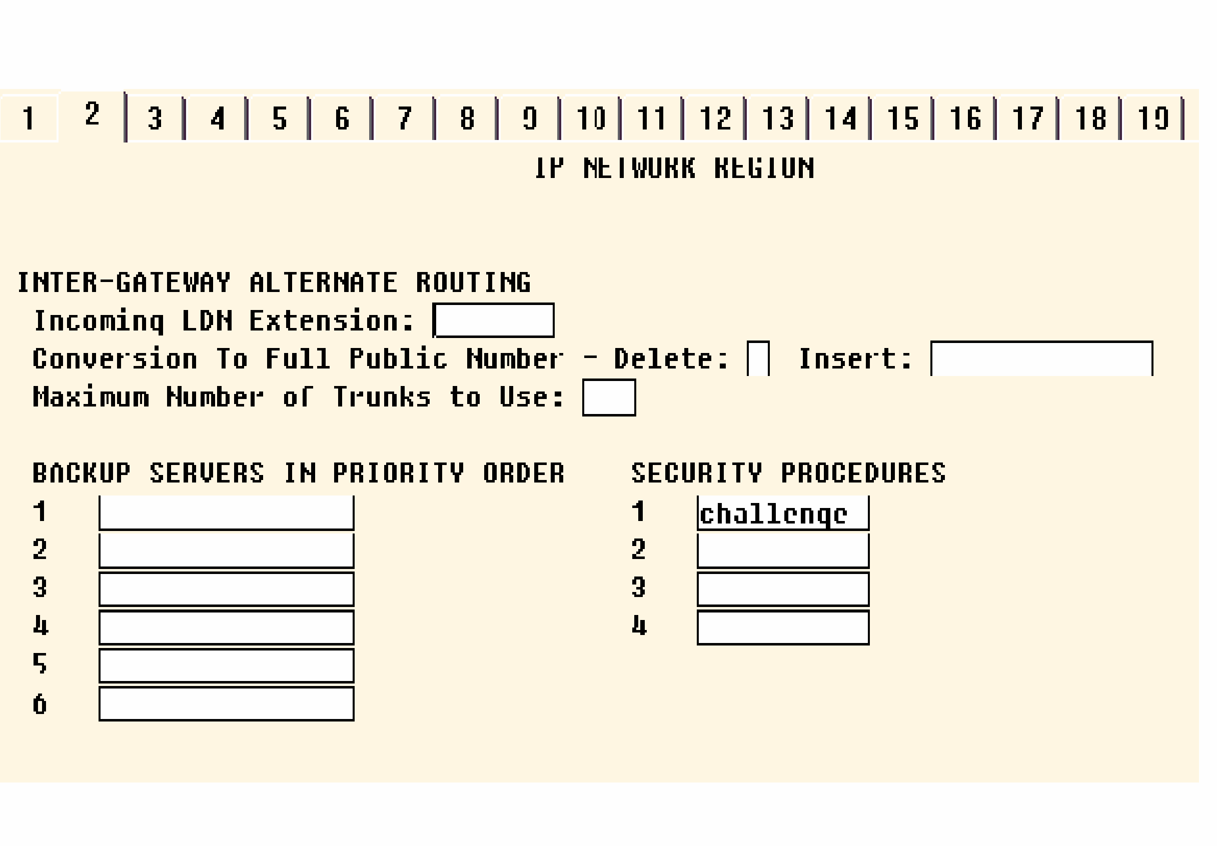


```
change vdn 4150                                               Page   1 of   2
                          VECTOR DIRECTORY NUMBER

                            Extension: 4150
                                Name*: Attendant
                        Vector Number: 3
                  Attendant Vectoring? y


                                  COR: 1
                                  TN*: 1
                             Measured: none
```

A vector directory number (VDN) is a virtual number which redirects calls to
a specified vector. The VDN is not assigned to a real extension. A VDN must conform to the number scheme.

In the example, calls to 4150 will be routed to vector 3.

Settings under IP–NETWORK–REGION



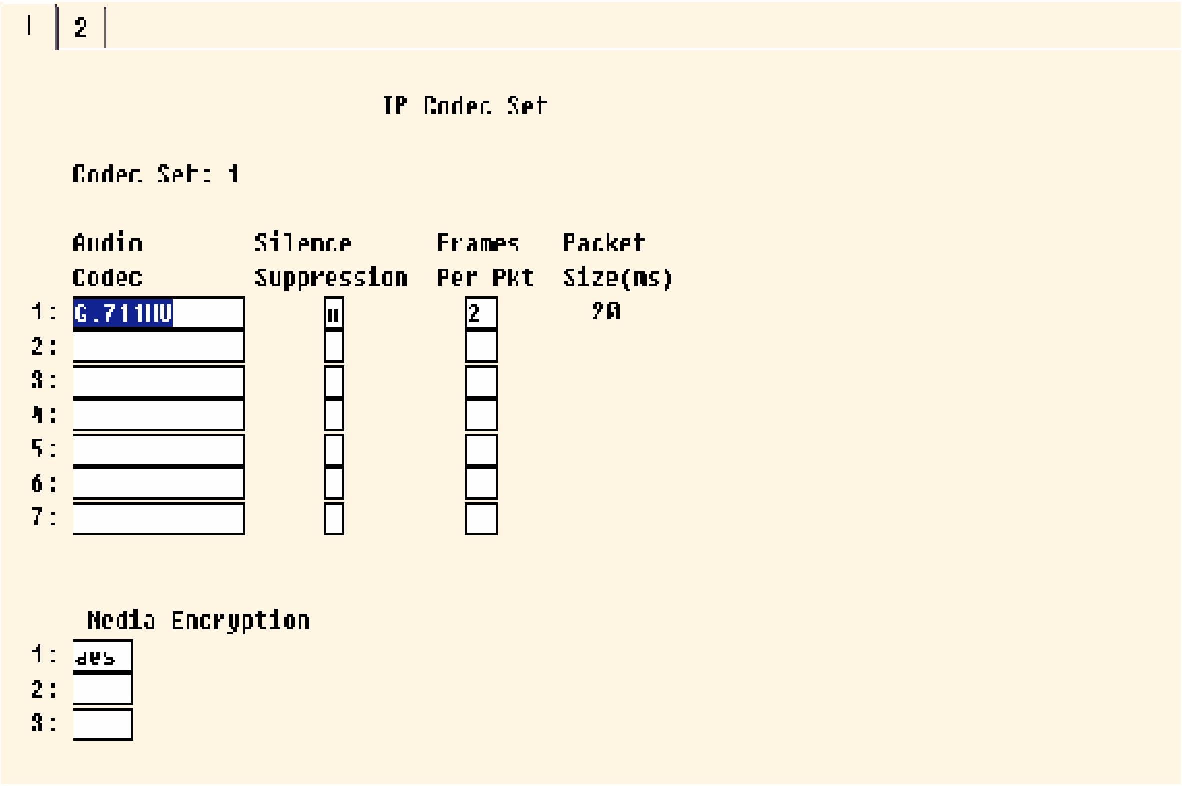
```
 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 |
                                IP NETWORK REGION


INTER-GATEWAY ALTERNATE ROUTING
 Incoming LDN Extension:
 Conversion To Full Public Number - Delete:    Insert:
 Maximum Number of Trunks to Use:

 BACKUP SERVERS IN PRIORITY ORDER       SECURITY PROCEDURES
 1                                      1    challenge
 2                                      2
 3                                      3
 4                                      4
 5
 6
```

For SECURITY PROCEDURES is only the value ’challenge’ allowed.

Using Media Encryption

Settings under OPTIONAL FEATURES
Media Encryption Over IP must be set 'y'

Settings under IP CODEC SET



```
 1 | 2 |

                         IP Codec Set

    Codec Set: 1

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.711MU          n          2        20
 2:
 3:
 4:
 5:
 6:
 7:


     Media Encryption
 1: aes
 2:
 3:
```

If Media Encryption Over IP is activated under Media Encryption it is possible to choose the algorithm (aea or aes), one–X Attendant supports both but possibly not other connected IP–Phones.

Additional configuration instructions

In ACM you must assign all connecting devices a name, or combination of letters, in the Name field. The Name in ACM can contain up to 27 letters. It could lead to problems if letter 17 to 27 of station name contains letters, that could be interpreted as signal word, for example "ringing", " to ", "busy". Pay attention that the same COS and COR classes are selected for all settings.

Registered services

Some one-X Attendant components are installed on the PC as services. These services are also available when no users are signed on.
During installation the following services are registered:

Service	Name displayed	Description

one-X Attendant database	Avaya one-X Attendant database	Setup during the installation process
one-X Attendant_JOnAS	Avaya phonebook server	Setup during the installation process
AbsenceInfoPusher	Avaya phonebook server – AbsenceInfoPusher	Set up during the installation process if WebAccess was selected
UPDService	Avaya phonebook server – UpdateService	Setup during the installation process
SVAManager	Avaya one-X Attendant SVAManager	Set up during the installation process if SVA Manager was selected

Port overview of one-X Attendant and accessories

The following table gives an overview of all the port default settings used by one-X Attendant and accessory components. A more detailed compilationof ports you will find under
http://support.avaya.com
Please search for one-X Attendant

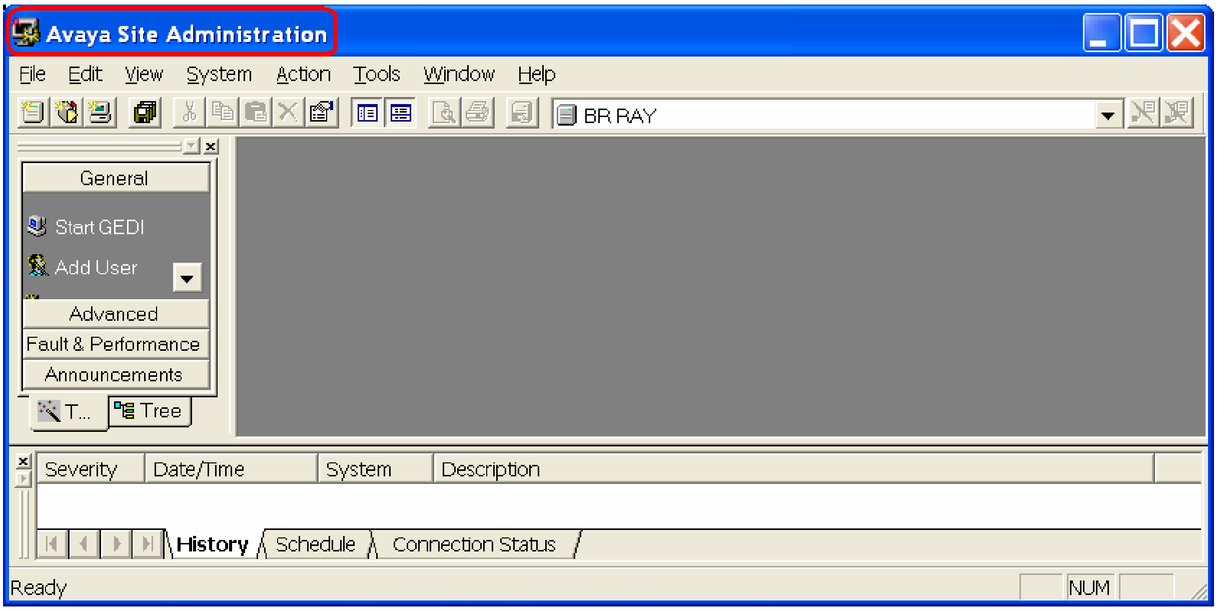
Application/Server	Port	Purpose
one-X Attendant		
Tomcat, WebAccess	21080	Internal Web server / https requests
Phone book server (JOnAS)	21099, 16010	RMI Registry, JMS
Phonebook Server (JOnAS) Remote Object Port	1050	RMI Remote Object Port
Database server	21638	
SVA Manager	6006	
IP Link (SVA Manager)	10405	
TTrace	10300, 10301, 10303, 10304	
AbsenceInfoPusher	9074, 9072, 9070	
Absence AURA PresenceServer (LPS)	5432	
Absence AURA Presence Server (IM)	5223	
Licensing		
WebLM	8443	License requests (for external access, depends on whether the license server is running locally or externally.)

Importing CM Station and Agent Data to one-X Attendant Phone book cyclically

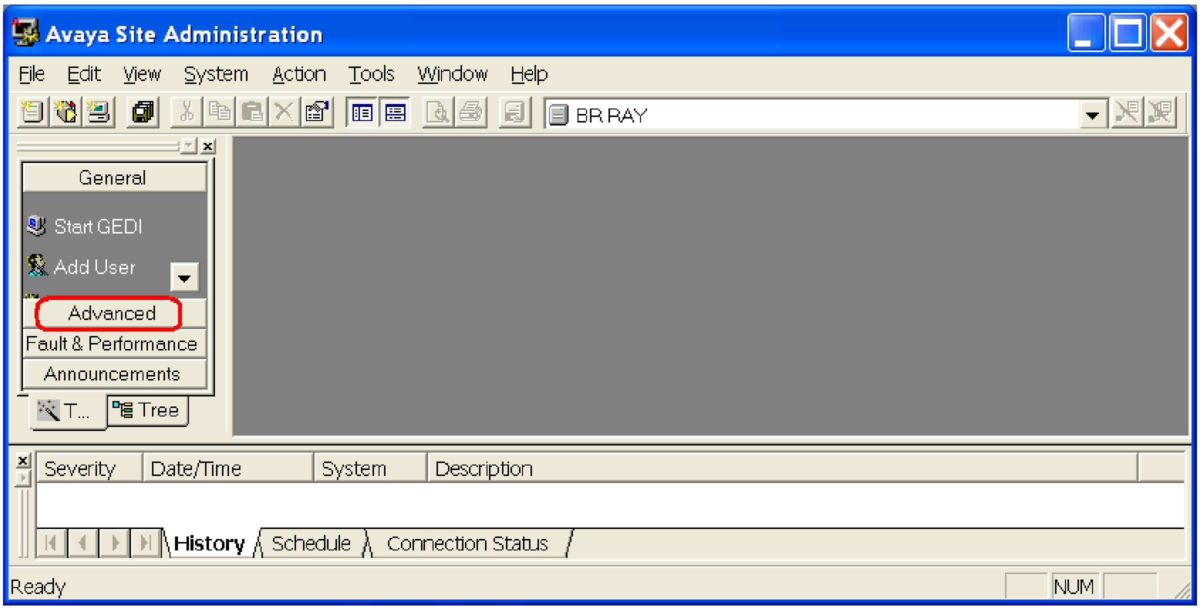
This document illustrates an easy way, with step-by-step instructions, of importing the Station and/or Agent Data of Avaya Aura^{TM} Communication Manager into the Avaya one-X Attendant Phone book cyclically. This is a two step procedure which first requires you to export the Station and/or Agent Data using the Avaya Site Administration (ASA) tool and then import the data into the Avaya one-X Attendant Phone book.

Create task for Exporting Station Data

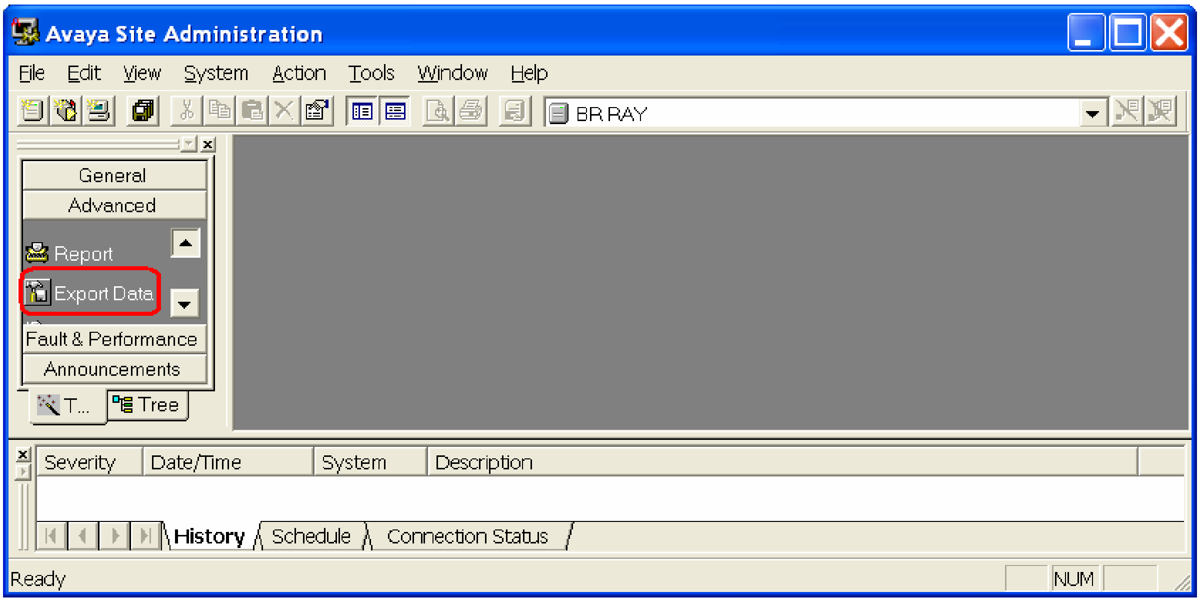
1. Start the Avaya Site Administration (ASA) application and select the PBX of interest.



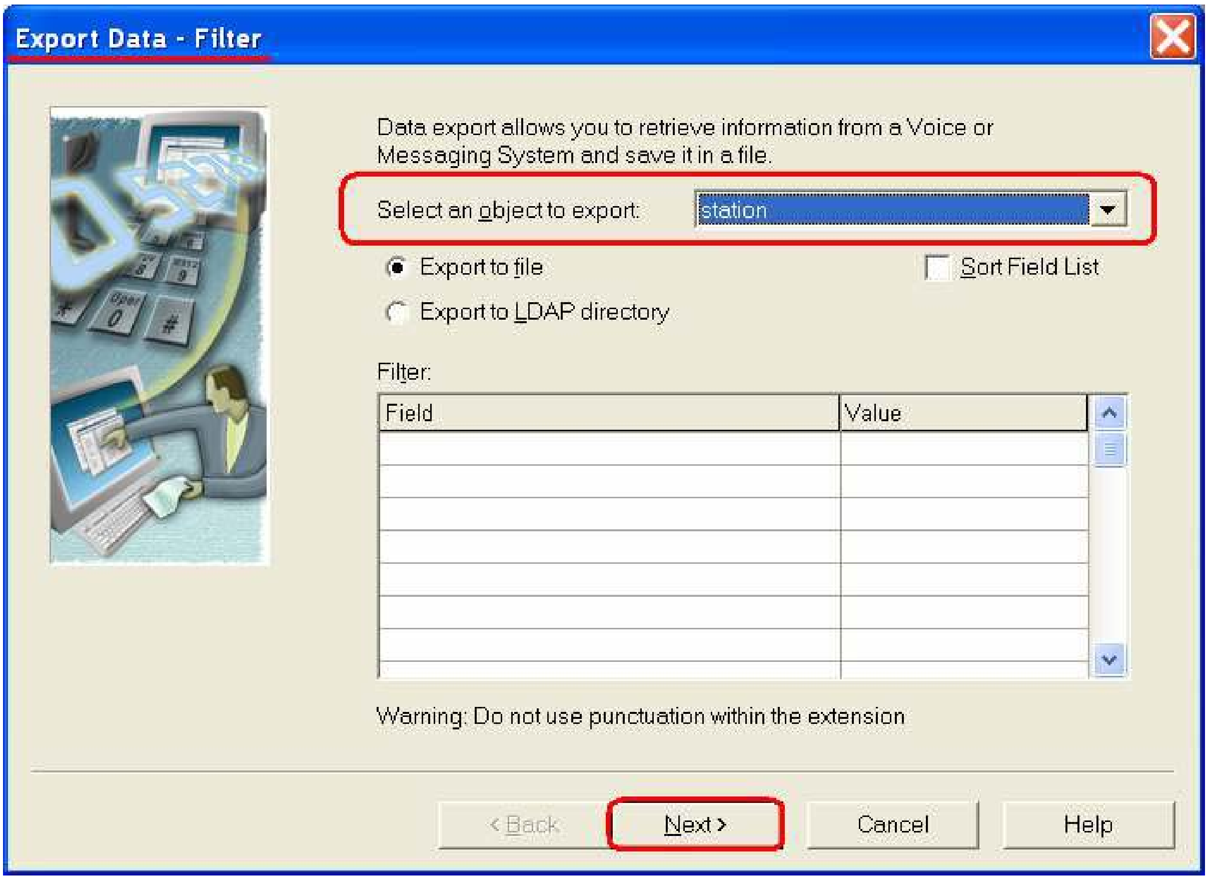
2. Click the Advanced bar from the ASA browser.



3. Click the Export Data wizard from the Advanced bar.



4. The Export Data dialog starts with object selection and record filtering. By default, the ‘station’ object is selected. If it is not, select ‘station’ object from the drop-down box (shown below). Select ‘Export to file’ option, if it is not already selected. Click the Next button.



Data export allows you to retrieve information from a Voice or Messaging System and save it in a file.

Select an object to export: station

● Export to file

○ Export to LDAP directory

□ Sort Field List

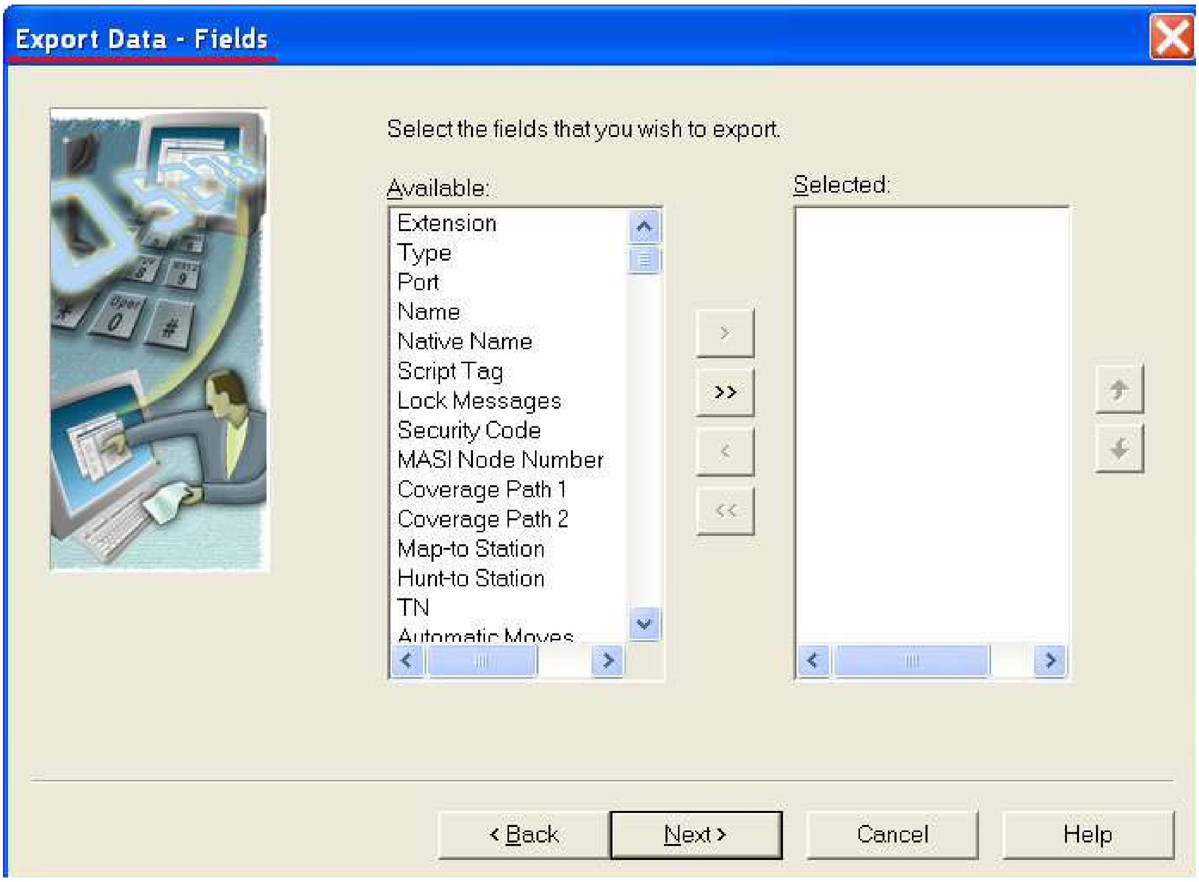
Filter:

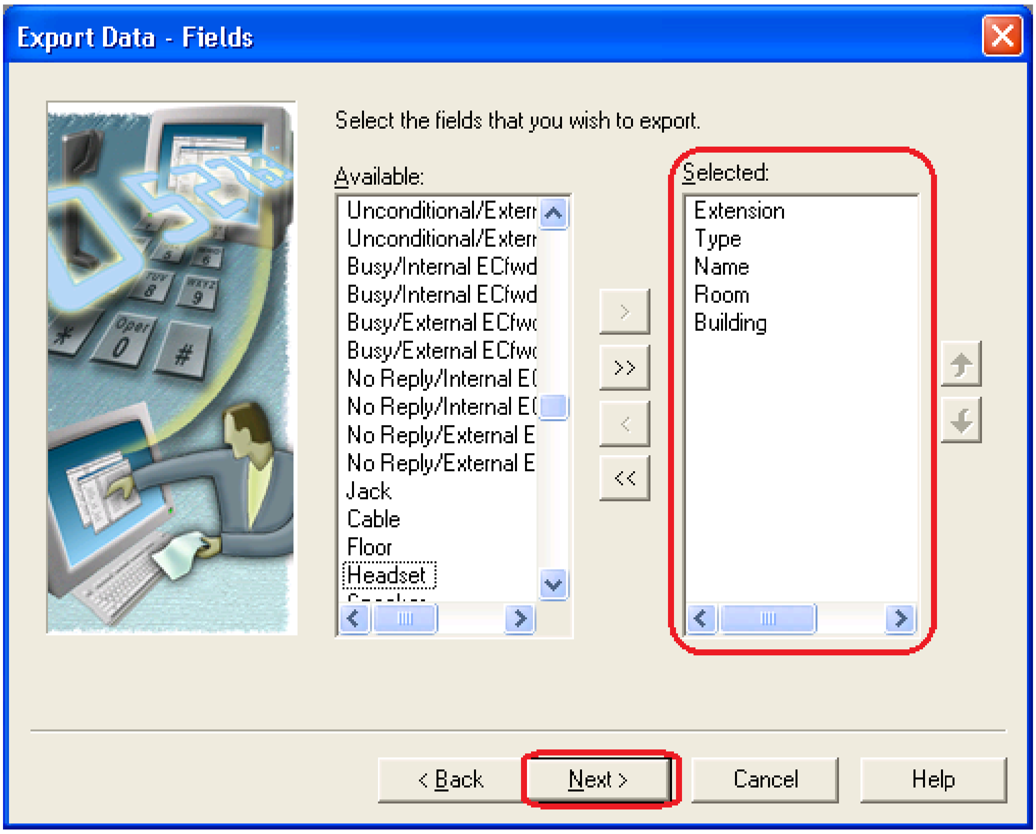
Field	Value

Warning: Do not use punctuation within the extension

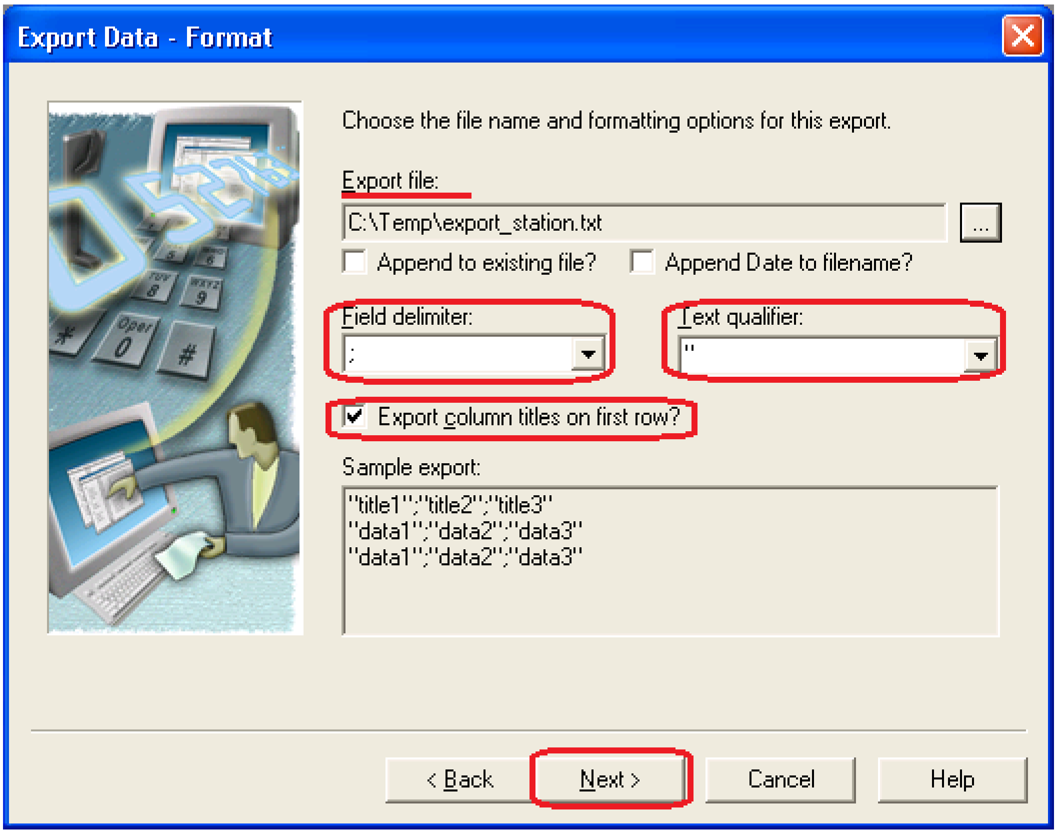
5. In this step, the desired fields are selected and moved from the available fields column to the selected fields column, one field at a time.

6. Select the fields from the available fields and move them to the selected fields column. When the fields have been moved to the selected column, click the Next button. For example, the following fields were selected for this document.
   - Extension
   - Type
   - Name
   - Room
   - Building





7. In this step, the file format details are selected. Select semi-colon (;) as the Field delimiter, select the quotation mark as the Text qualifier, select the 'Export column titles on first row?' check-box, click the browse button (the 3-dotted button to the right of Export file field) and select the file name and location. When complete, click the Next button.



Export Data - Format

Choose the file name and formatting options for this export.

Export file: C:\Temp\export_station.txt

□ Append to existing file? □ Append Date to filename?

Field delimiter: ;

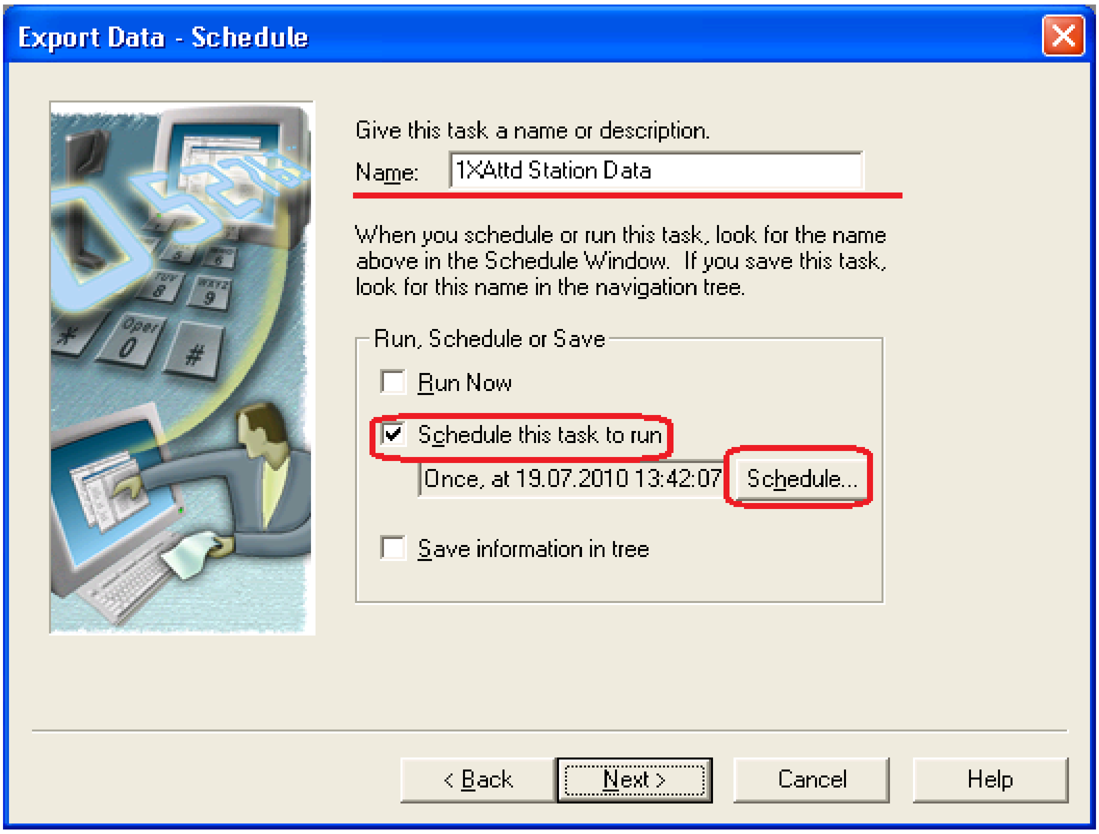
Text qualifier: "

☑ Export column titles on first row?

Sample export:

```
"title1";"title2";"title3"
"data1";"data2";"data3"
"data1";"data2";"data3"
```

8. In this step, the exporting of station data can be scheduled to automatically run at a specified date and time. Enter a meaningful name for this task in the Name field, unselect the ‘Run Now’ check-box, and then click the Schedule button.



Export Data - Schedule

Give this task a name or description.

Name: 1XAttd Station Data

When you schedule or run this task, look for the name above in the Schedule Window. If you save this task, look for this name in the navigation tree.

Run, Schedule or Save

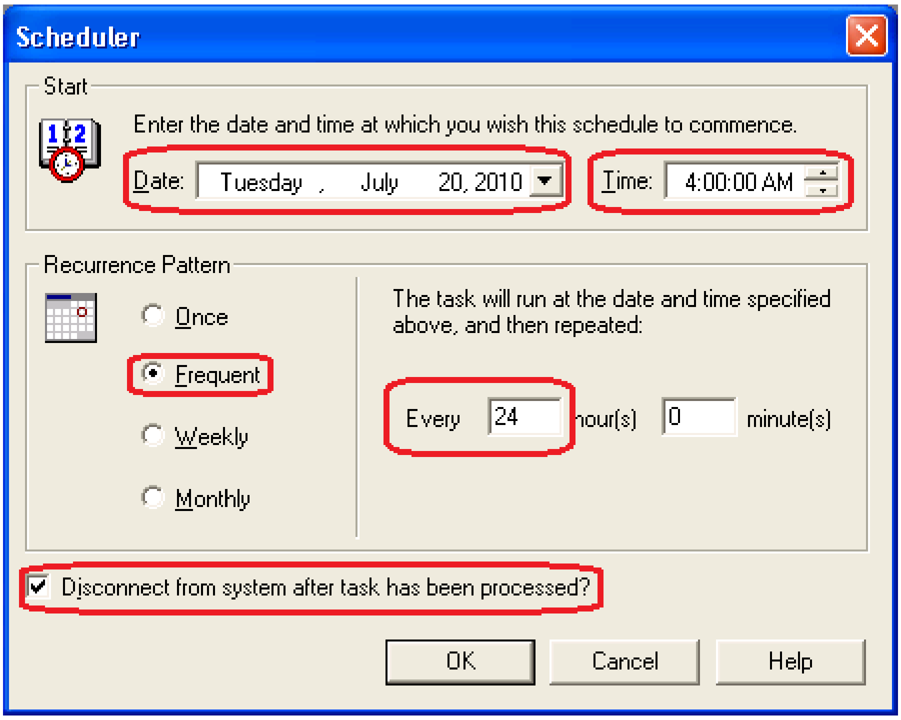
□ Run Now

☑ Schedule this task to run

Once, at 19.07.2010 13:42:07

□ Save information in tree

9. In the Scheduler step, select the date for the task to start, the time for task to run, the interval for when to run the task the next time, and make sure select the ‘Disconnect…’ check-box. When scheduling of the task is completed, click the OK button.



Enter the date and time at which you wish this schedule to commence.

Date: Tuesday , July 20, 2010

Time: 4:00:00 AM

○ Once

● Frequent

○ Weekly

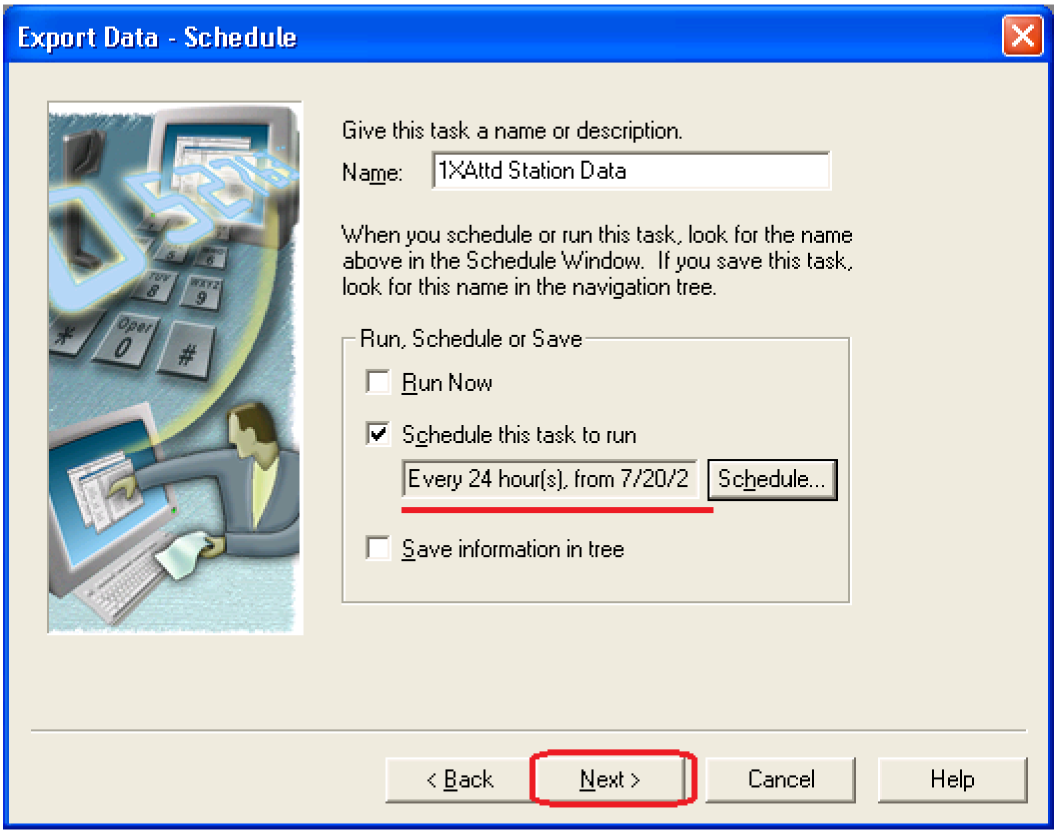
○ Monthly

The task will run at the date and time specified above, and then repeated:

Every 24 hour(s) 0 minute(s)

☑ Disconnect from system after task has been processed?

10.Verify the task is now scheduled to be run at a specified date and time. Click the Next button.



Export Data - Schedule

Give this task a name or description.

Name: 1XAttd Station Data

When you schedule or run this task, look for the name above in the Schedule Window. If you save this task, look for this name in the navigation tree.

Run, Schedule or Save

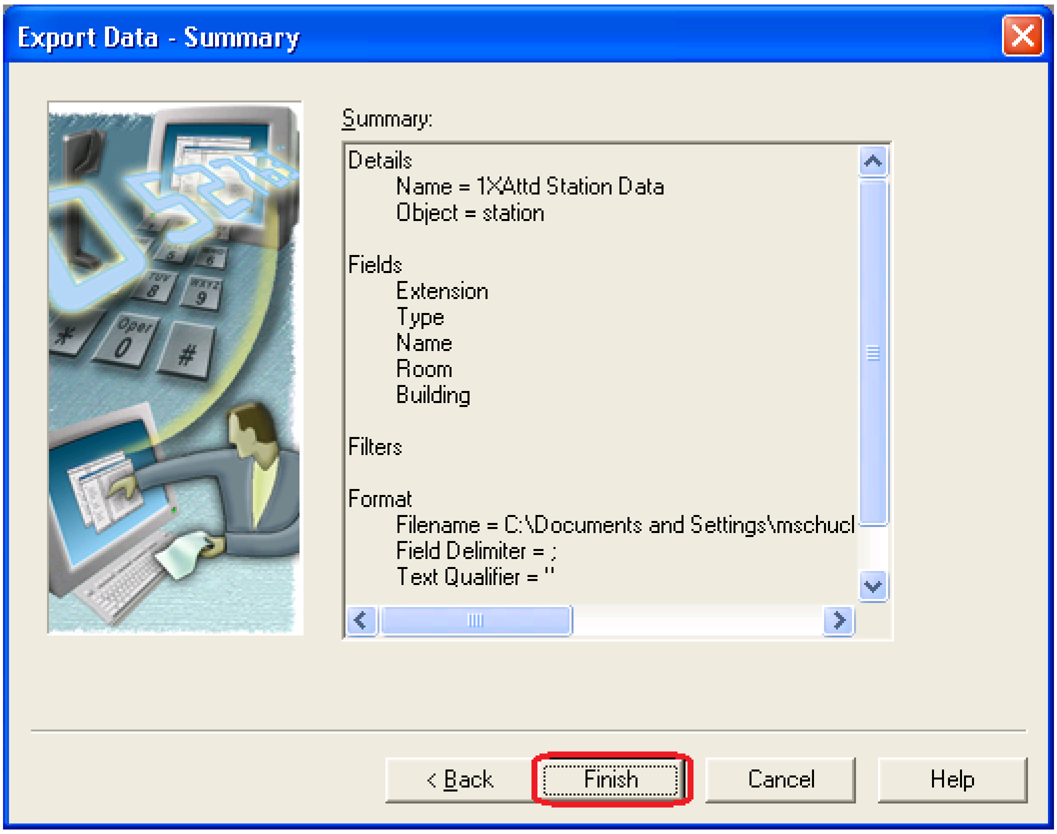
□ Run Now

☑ Schedule this task to run

Every 24 hour(s), from 7/20/2

□ Save information in tree

11. In this last step, details are summarized. Verify details and click the Finish button.



Export Data - Summary

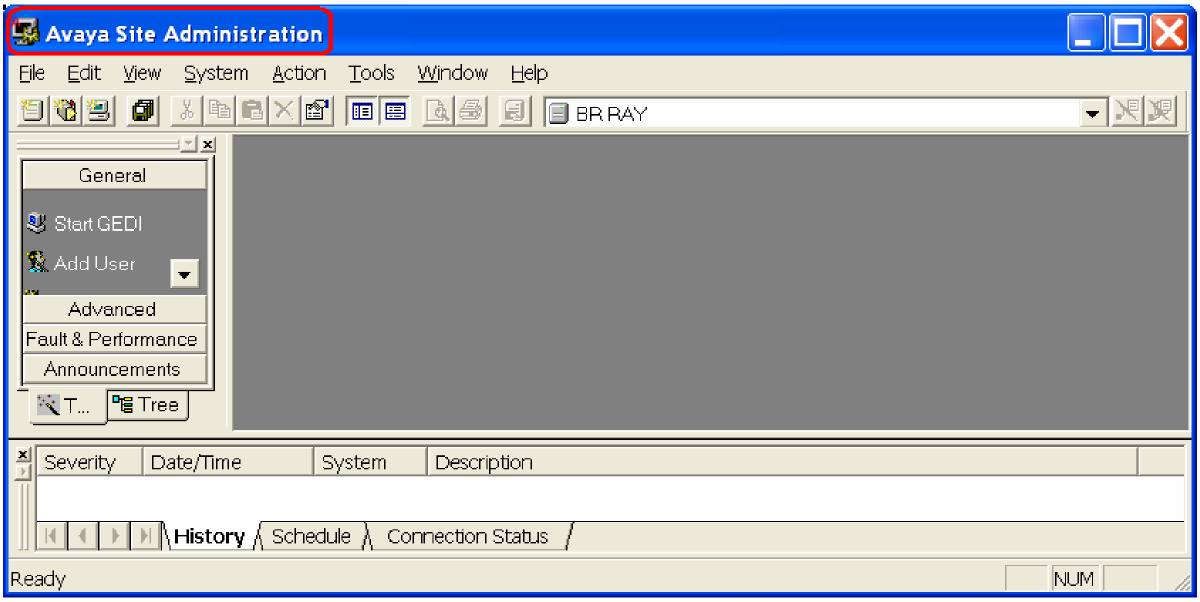
Summary:

```
Details
        Name = 1XAttd Station Data
        Object = station

Fields
        Extension
        Type
        Name
        Room
        Building

Filters

Format
        Filename = C:\Documents and Settings\mschucl
        Field Delimiter = ;
        Text Qualifier = "
```

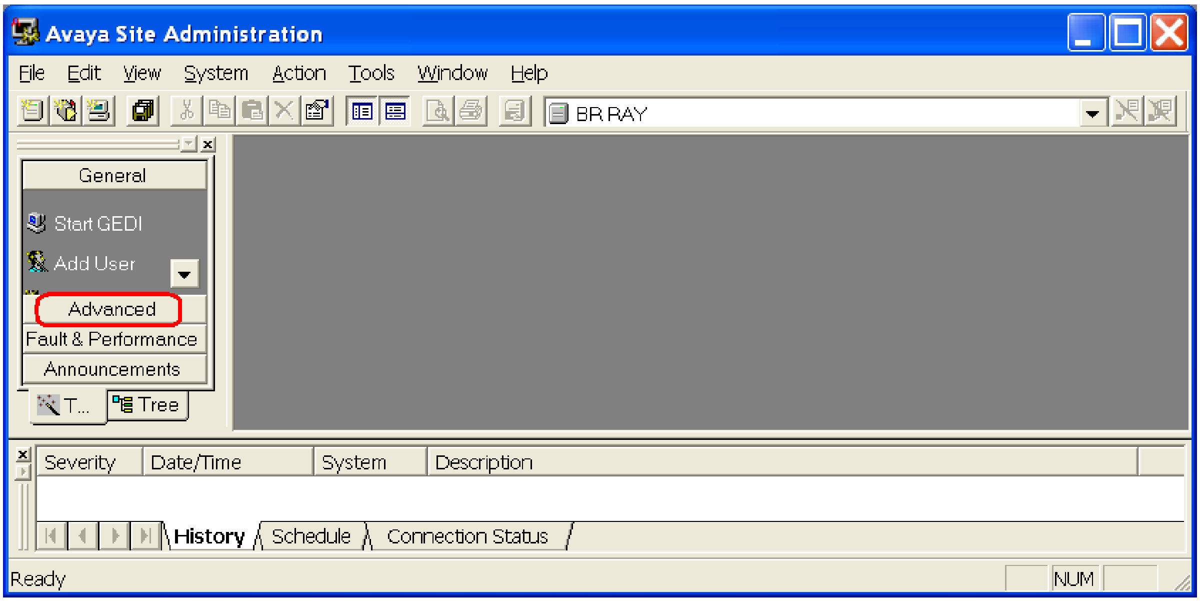
Create task for Exporting Agent Data

Similar to Exporting Station Data, the task is created for Exporting Agent Data in this section.

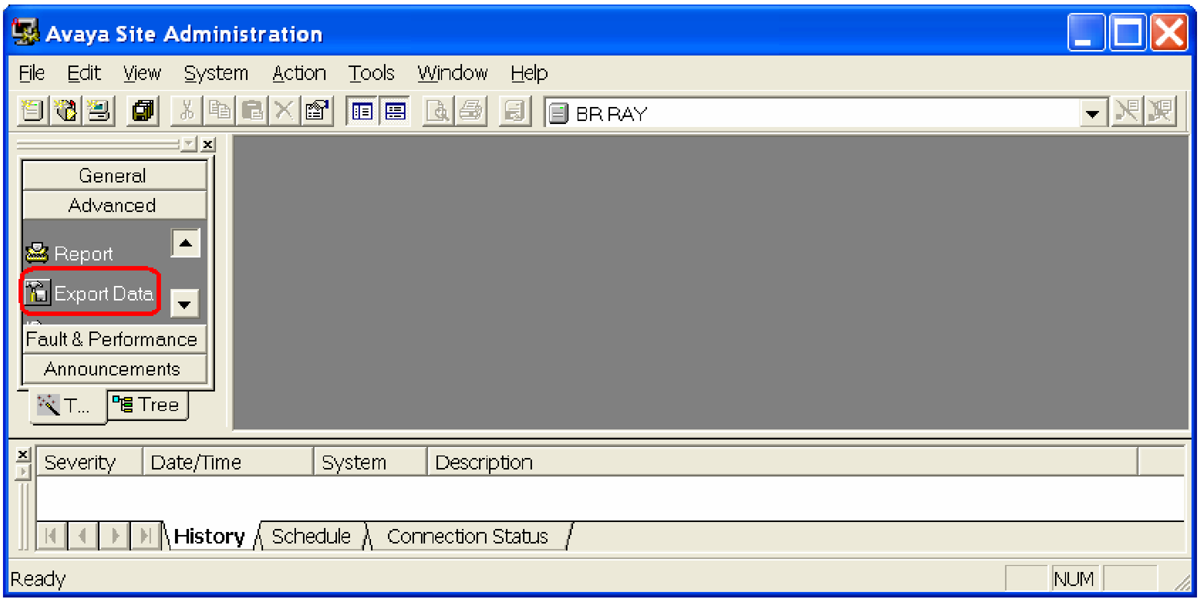
1. Start the Avaya Site Administration (ASA) application and select the PBX of interest.



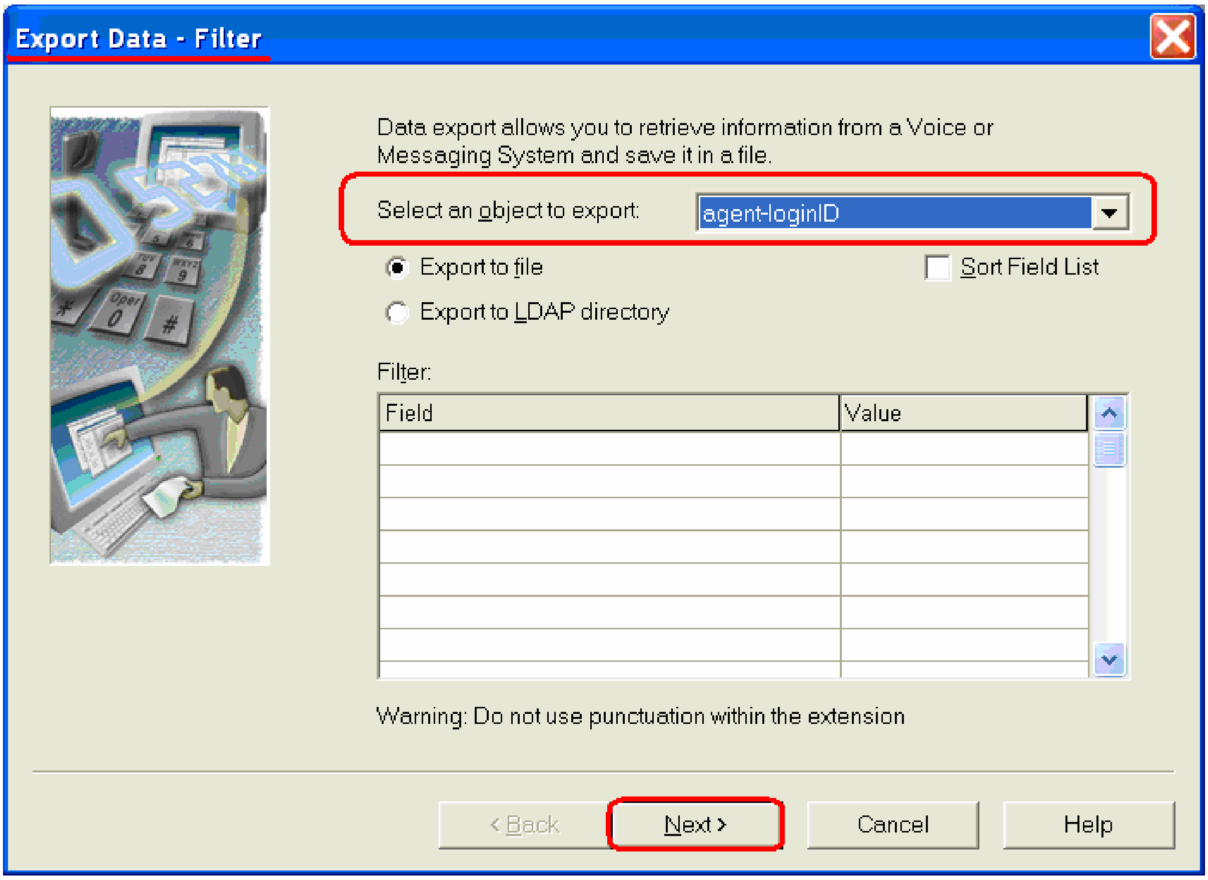
2. Click the Advanced bar from the ASA browser.



3. Click the Export Data wizard from the Advanced bar.



4. The Export Data dialog starts with object selection and record filtering. By default, the 'station' object is selected. Instead, select 'agent-loginID' object from the drop-down box (shown below). Select 'Export to file' option, if it is not already selected. Click the Next button.
5. In this step, the desired fields are selected and moved from the available fields column to the selected fields column, one field at a time.


Export Data - Filter

Data export allows you to retrieve information from a Voice or Messaging System and save it in a file.

Select an object to export: agent-loginID

● Export to file

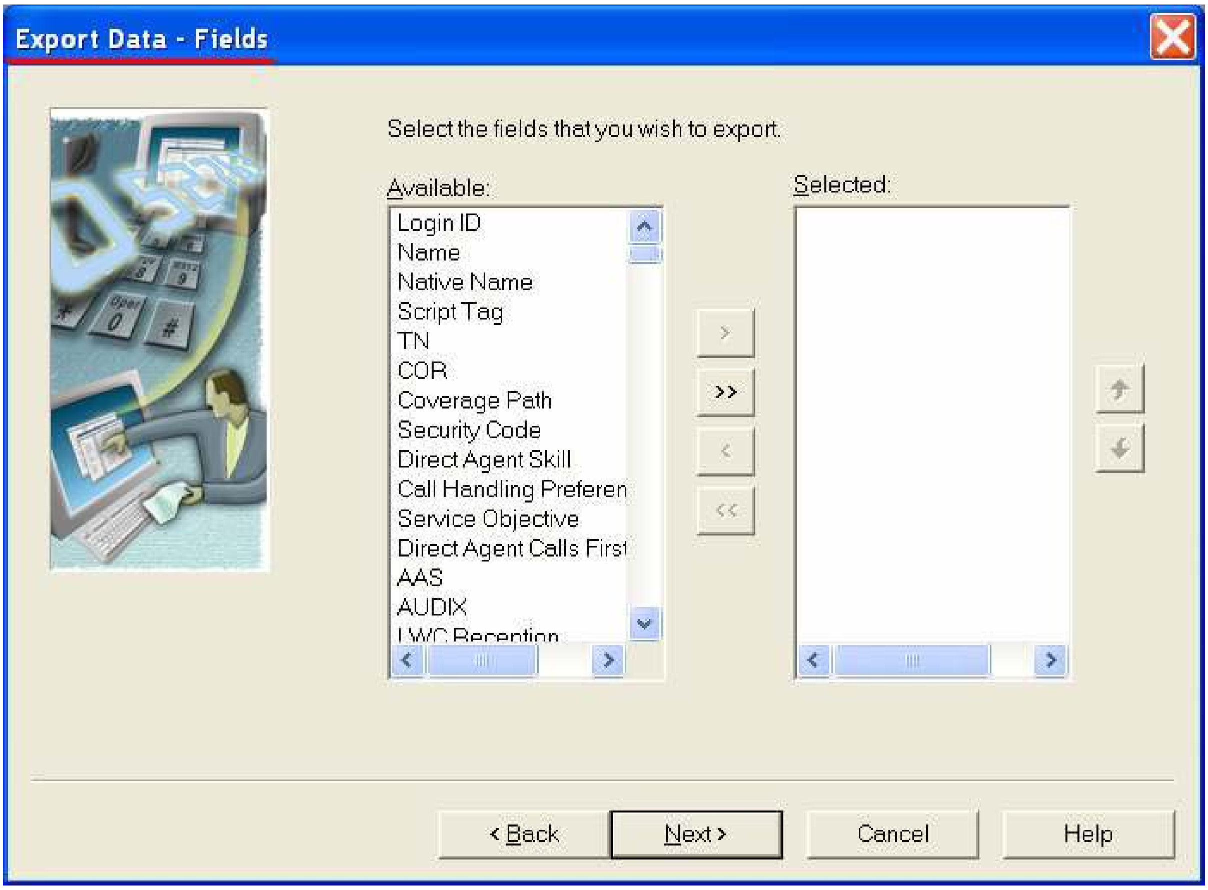
□ Sort Field List

○ Export to LDAP directory

Filter:

Field	Value

Warning: Do not use punctuation within the extension



Export Data - Fields

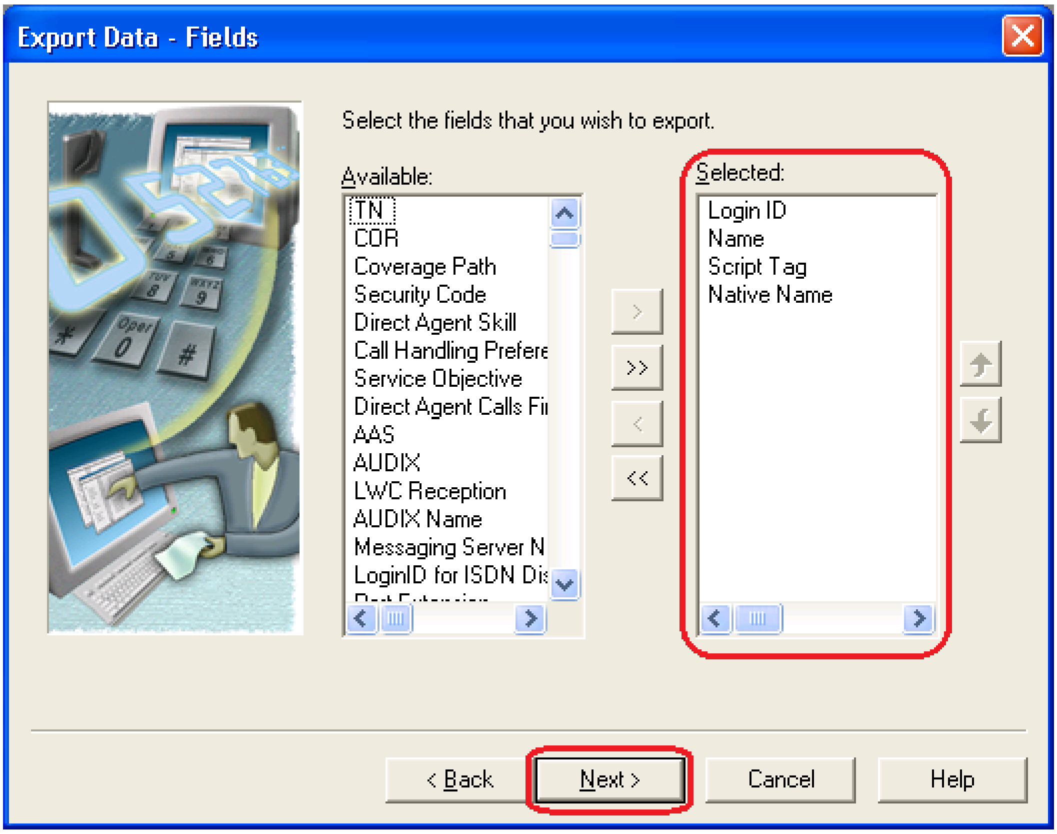
Select the fields that you wish to export.

Available:

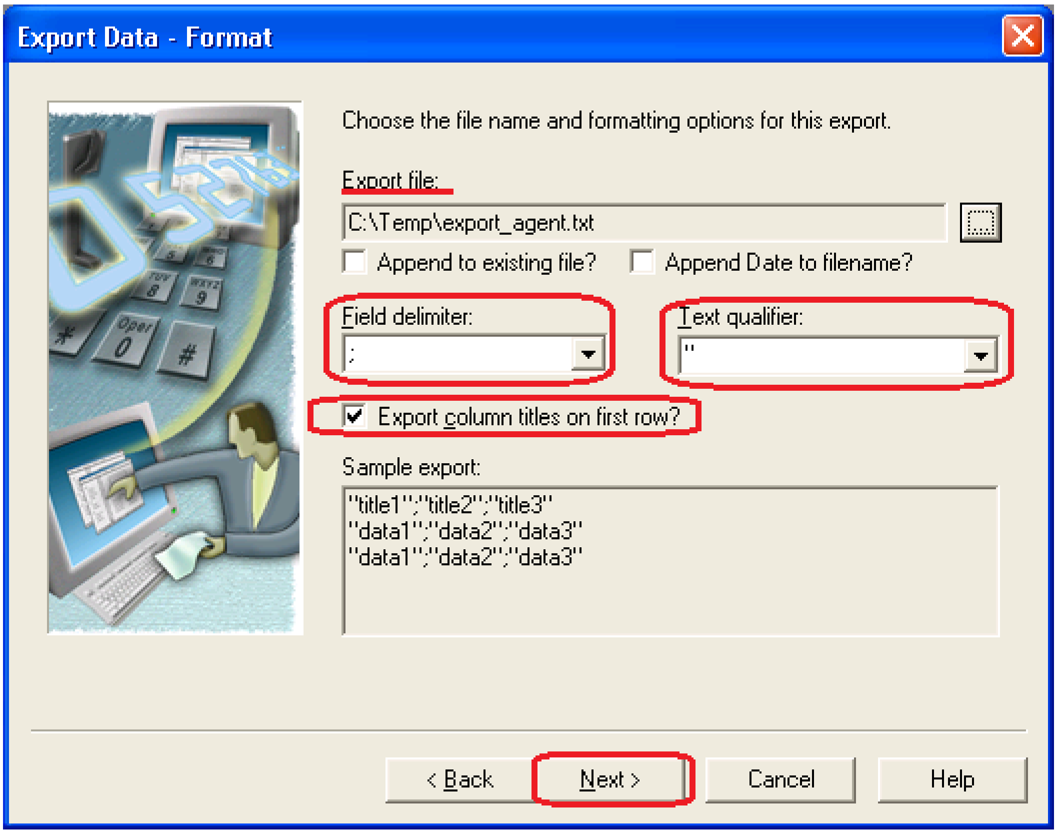
- Login ID
- Name
- Native Name
- Script Tag
- TN
- COR
- Coverage Path
- Security Code
- Direct Agent Skill
- Call Handling Preferen
- Service Objective
- Direct Agent Calls First
- AAS
- AUDIX
- LWC Reception

Selected:

6. Select the fields from the available fields and move them to the selected fields column. When all the fields have been moved to the selected column, click the Next button. For example, the following fields were selected for this document.
   - Login ID
   - Native Name
   - Script Tag
   - Name



7. In this step, the file format details are selected. Select semi-colon (;) as the Field delimiter, select the quotation mark as the Text qualifier, select the ‘Export column titles on first row?’ check-box, click the browse button (the 3-dotted button to the right of Export file field) and select the file name and location. When complete, click the Next button.



Export Data - Format

Choose the file name and formatting options for this export.

Export file:

C:\Temp\export_agent.txt

□ Append to existing file? □ Append Date to filename?

Field delimiter: ;

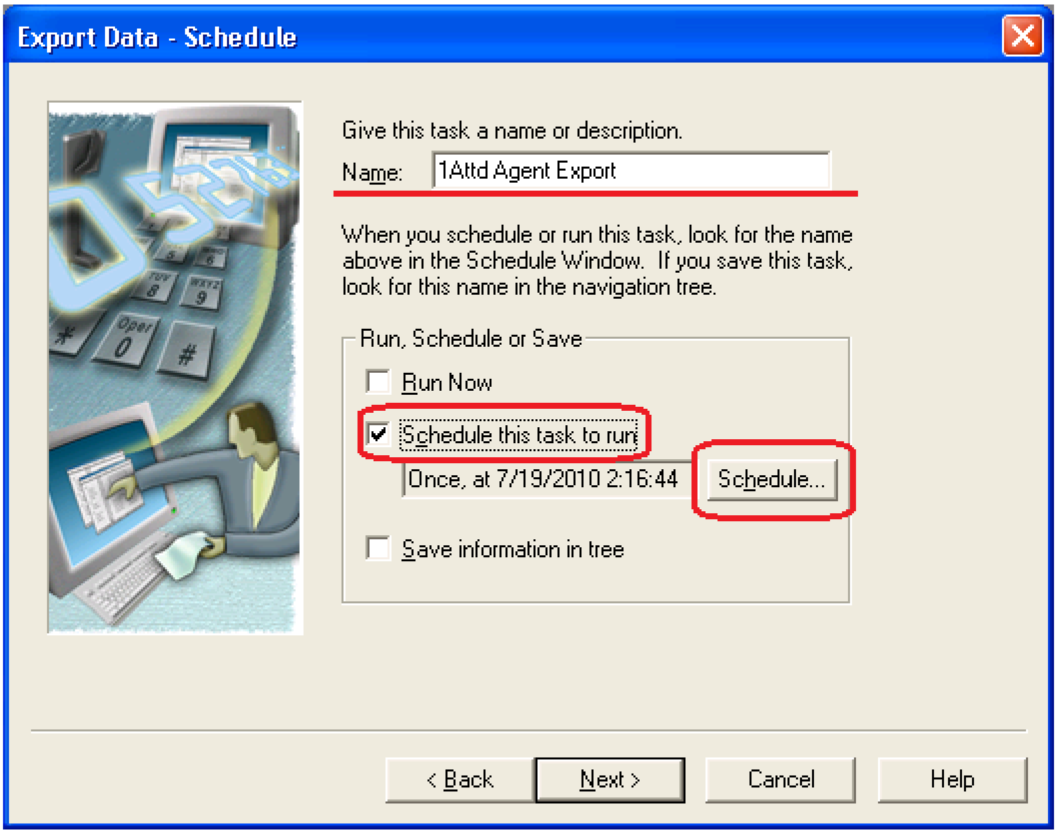
Text qualifier: "

☑ Export column titles on first row?

Sample export:

```
"title1";"title2";"title3"
"data1";"data2";"data3"
"data1";"data2";"data3"
```

8. In this step, the exporting of agent data can be scheduled to automatically run at a specified date and time. Enter a meaningful name for these task in the Name field, un-select the ‘Run Now’ check-box, and then click the Schedule button.



Export Data - Schedule

Give this task a name or description.

Name: 1Attd Agent Export

When you schedule or run this task, look for the name above in the Schedule Window. If you save this task, look for this name in the navigation tree.

Run, Schedule or Save

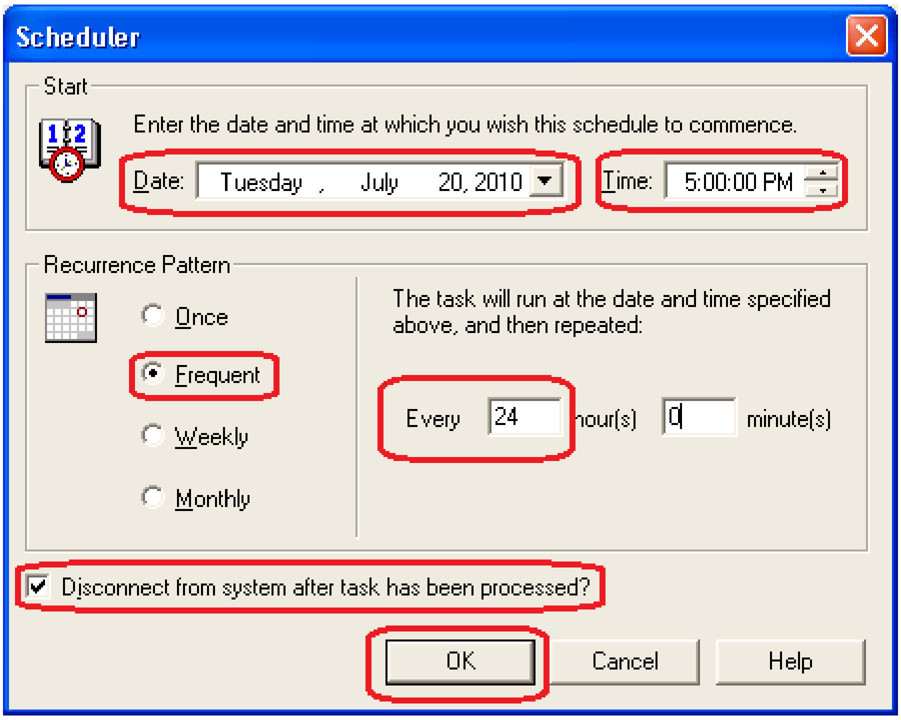
☐ Run Now

☑ Schedule this task to run

Once, at 7/19/2010 2:16:44

☐ Save information in tree

9. In the Scheduler step, select the date for the task to start, the time for task to run, the interval for when to run the task the next time, and make sure to select the 'Disconnect…' check-box. When scheduling of the task is completed, click the OK button.



Scheduler

Start

Enter the date and time at which you wish this schedule to commence.

Date: Tuesday , July 20, 2010

Time: 5:00:00 PM

Recurrence Pattern

○ Once

● Frequent

○ Weekly

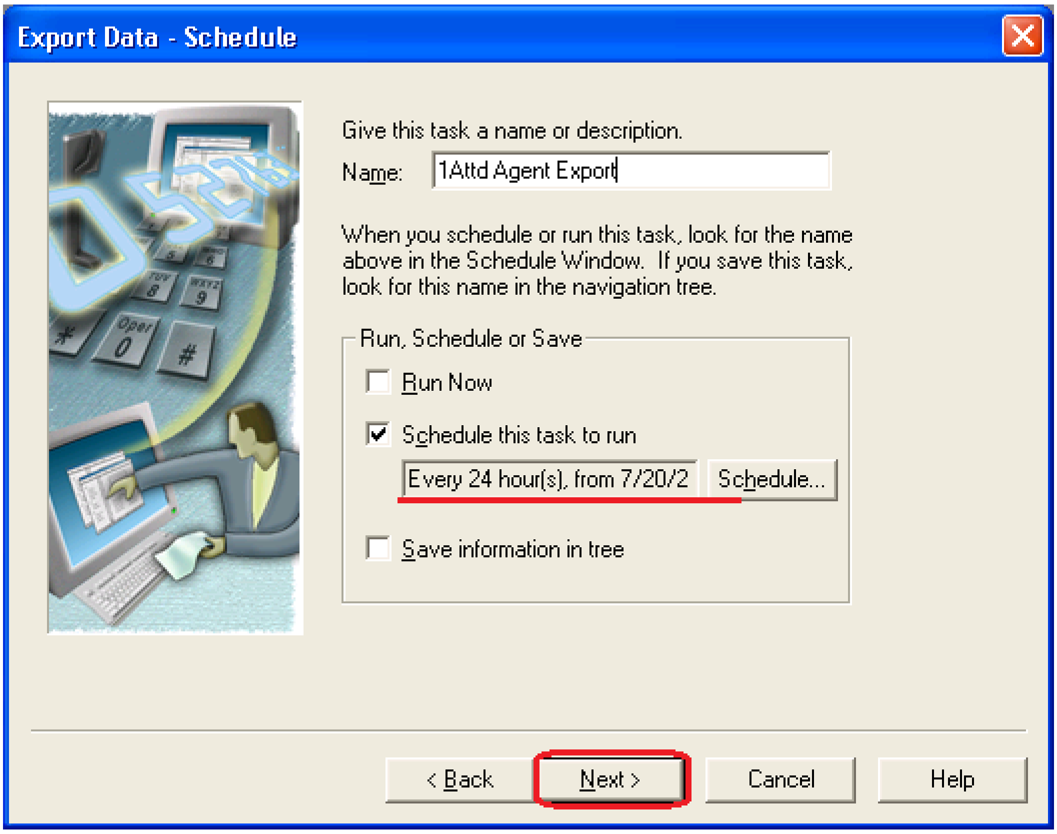
○ Monthly

The task will run at the date and time specified above, and then repeated:

Every 24 hour(s) 0 minute(s)

☑ Disconnect from system after task has been processed?

10. Verify the task is now scheduled to be run at a specified date and time. Click the Next button.



Export Data - Schedule

Give this task a name or description.

Name: 1Attd Agent Export

When you schedule or run this task, look for the name above in the Schedule Window. If you save this task, look for this name in the navigation tree.

Run, Schedule or Save

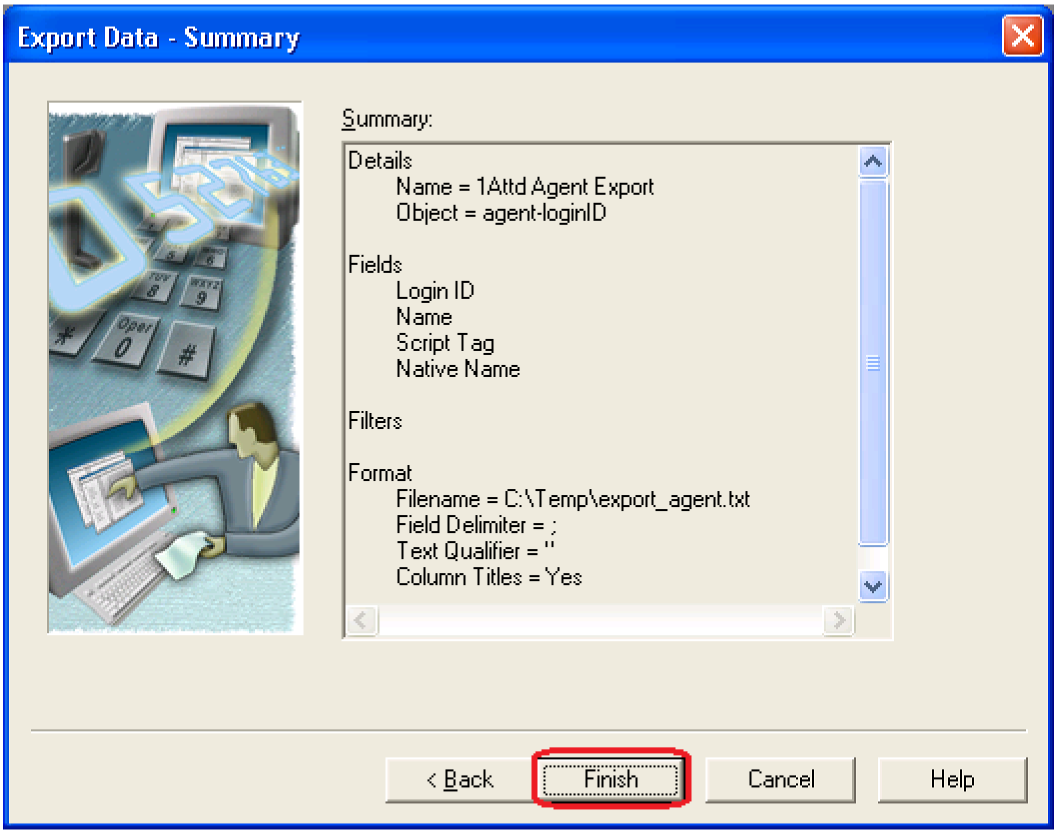
□ Run Now

☑ Schedule this task to run

Every 24 hour(s), from 7/20/2

□ Save information in tree

11. In this last step, details are summarized. Verify details and click the Finish button.

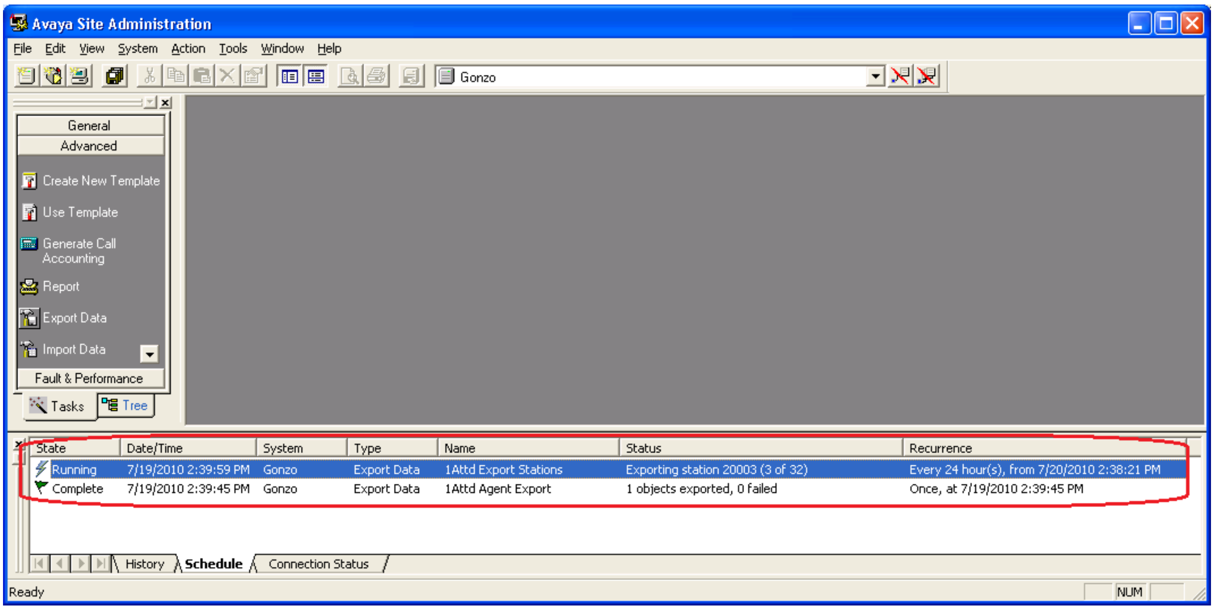


Export Data - Summary

Summary:

```
Details
      Name = 1Attd Agent Export
      Object = agent-loginID

Fields
      Login ID
      Name
      Script Tag
      Native Name

Filters

Format
      Filename = C:\Temp\export_agent.txt
      Field Delimiter = ;
      Text Qualifier = "
      Column Titles = Yes
```

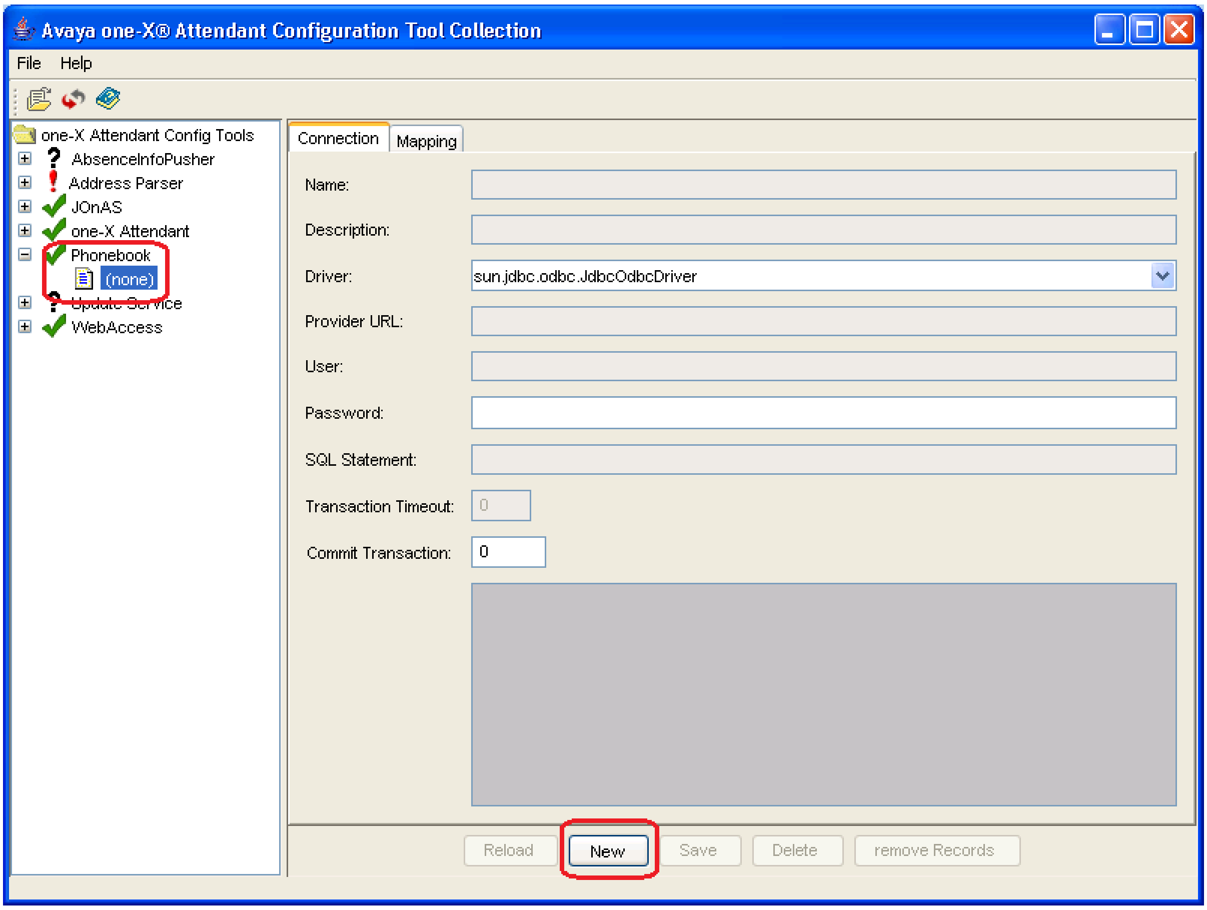
When the scheduled tasks are triggered and running, they are individually displayed in Schedule tab of Status window with all the gory details. For example, the screenshot below shows the status of two tasks; one ‘Complete’ and the other ‘Running’.



State	Date/Time	System	Type	Name	Status	Recurrence
Running	7/19/2010 2:39:59 PM	Gonzo	Export Data	1Attd Export Stations	Exporting station 20003 (3 of 32)	Every 24 hour(s), from 7/20/2010 2:38:21 PM
Complete	7/19/2010 2:39:45 PM	Gonzo	Export Data	1Attd Agent Export	1 objects exported, 0 failed	Once, at 7/19/2010 2:39:45 PM

Import Station Data into Phone book

1. Start the Avaya one-X Attendant configuration tools application, select an entry under the phone-book item and press the New button in this dialog.



Name:

Description:

Driver: sun.jdbc.odbc.JdbcOdbcDriver

Provider URL:

User:

Password:

SQL Statement:

Transaction Timeout: 0

Commit Transaction: 0

2. Choose the Connection tab

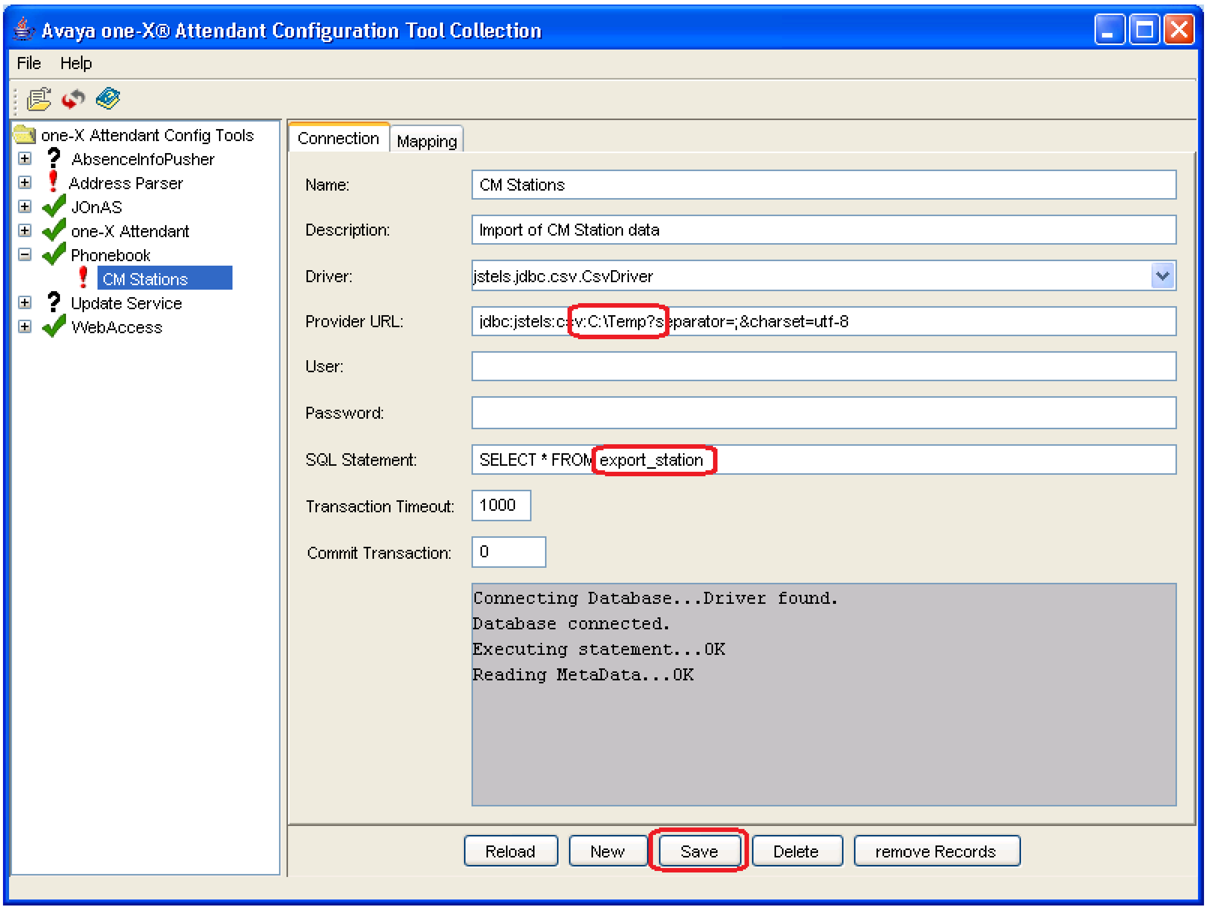
In the field Driver select the entry jstels.jdbc.csv.CsvDriver

Enter a meaningful Name and Description in the belonging fields,

In the field Provider URL replace the text <Enter directory here> with the directory path where the station data file saved in Step 7 of Create task for Exporting station data (The directory has to be on a local drive, otherwise the update service has to be started with a different account which has access to the corresponding network drive, see Control Panel\Adminstrative Tools\Services\Avaya Phonebook Server – UpdateService\Properties\Log On)

In the field SQL statement replace the text <enter tablename here> with the name of the station data file saved in Step 7 of Create task for Exporting station data (without file extension)

Click on the save button



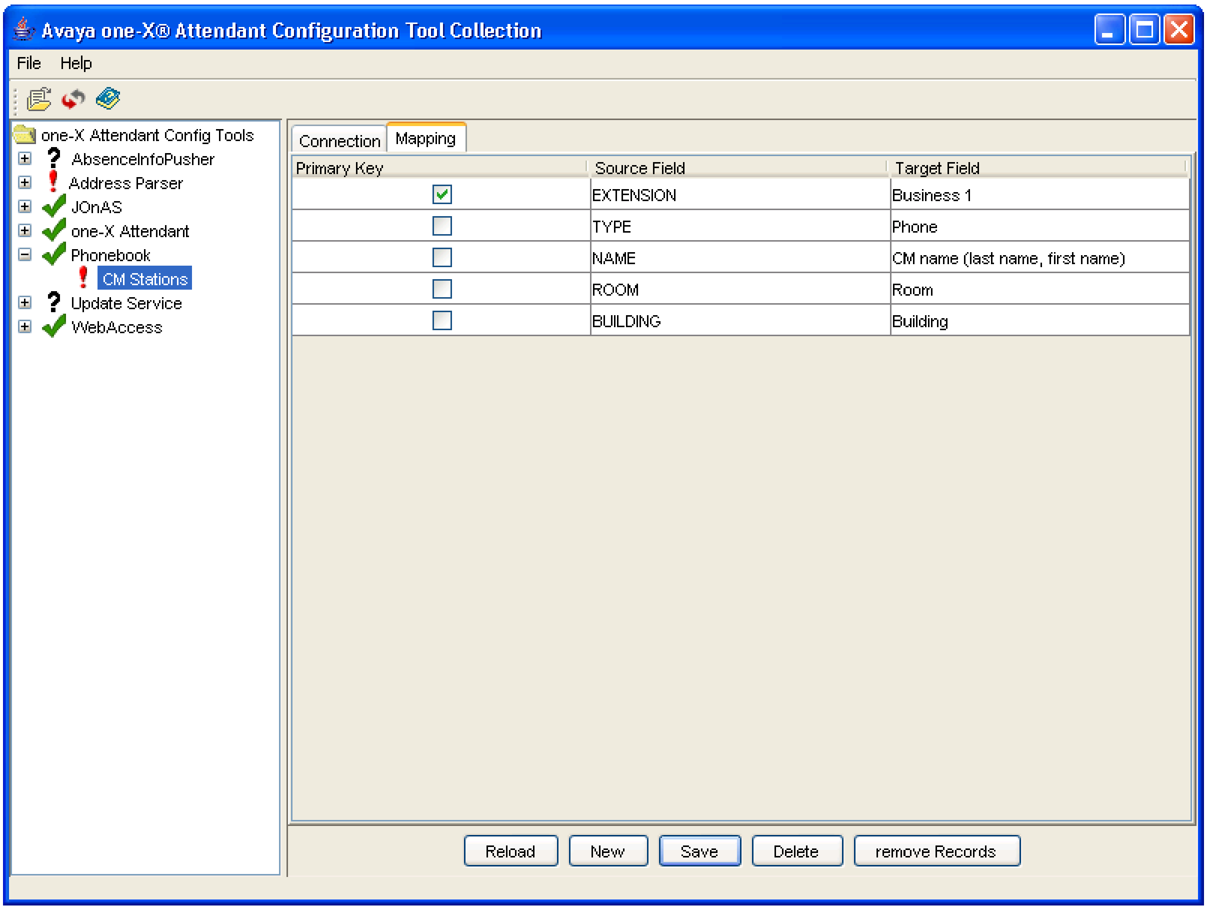
Name:	CM Stations
Description:	Import of CM Station data
Driver:	jstels.jdbc.csv.CsvDriver
Provider URL:	jdbc:jstels:csv:C:\Temp?separator=;&charset=utf-8
User:	
Password:	
SQL Statement:	SELECT * FROM export_station
Transaction Timeout:	1000
Commit Transaction:	0

```
Connecting Database...Driver found.
Database connected.
Executing statement...OK
Reading MetaData...OK
```

3. Choose the Mapping tab and select for the exported CM fields the belonging one-X Attendant phone book fields.

Here we do the following mapping:

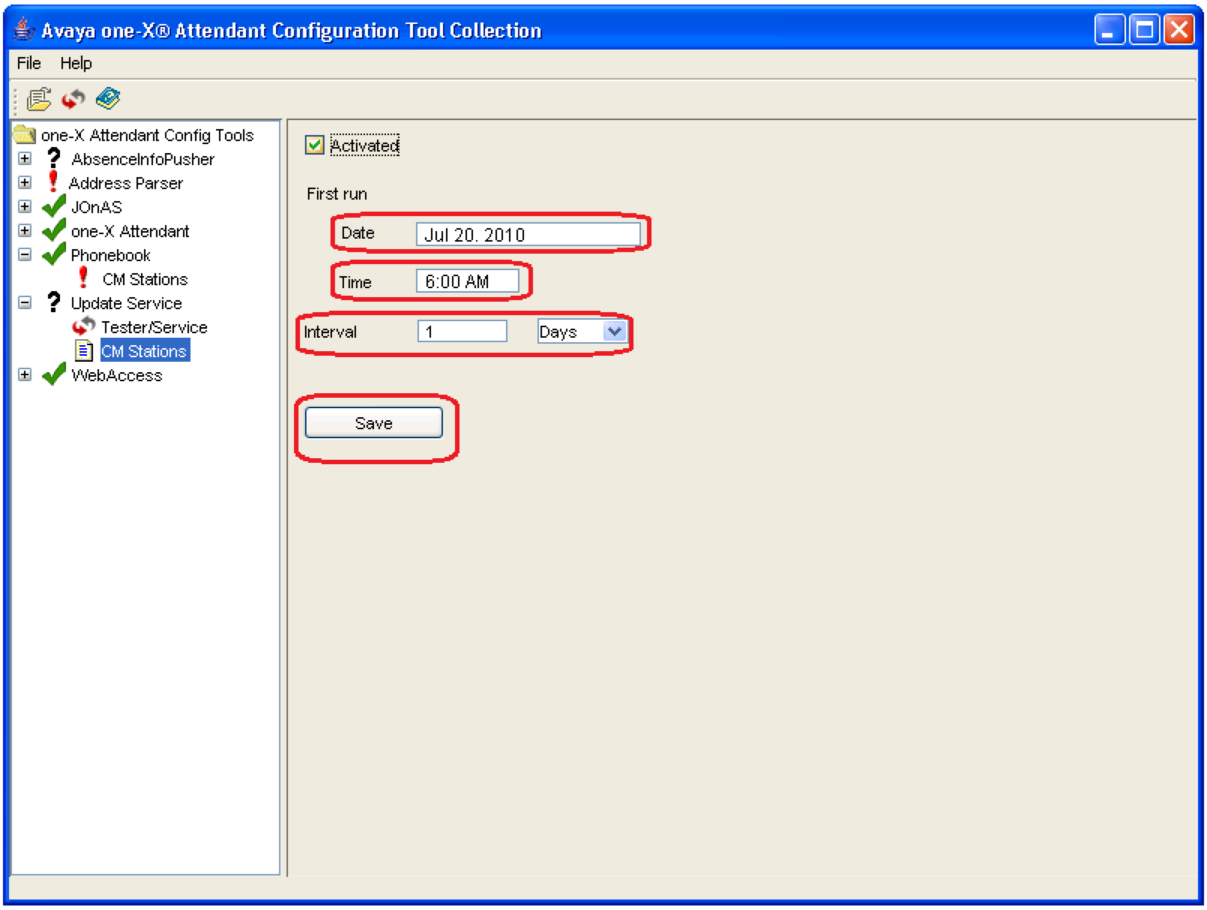
- EXTENSION -> Business 1 (main phone number)
- TYPE -> Phone
- NAME -> CM name (last name, first name)
- "CM Name (last name, first name)" isn't a real phone book field. If you choose this as target field and the content of the source field has the format (last name, first name), then it will be split into the phonebook fields (last name) and (first name).
- ROOM -> Room
- BUILDING -> Building
- As primary key the EXTENSION field should be checked.
- Don't forget to click on the save button again



Primary Key	Source Field	Target Field
☑	EXTENSION	Business 1
□	TYPE	Phone
□	NAME	CM name (last name, first name)
□	ROOM	Room
□	BUILDING	Building

4. In the Scheduler step, select the date for the task to start, the time for task to run,

the interval for when to run the task the next time. When scheduling of the task is completed, click the Save button.



☑ Activated

First run

Date: Jul 20, 2010

Time: 6:00 AM

Interval: 1 Days

Please also note,

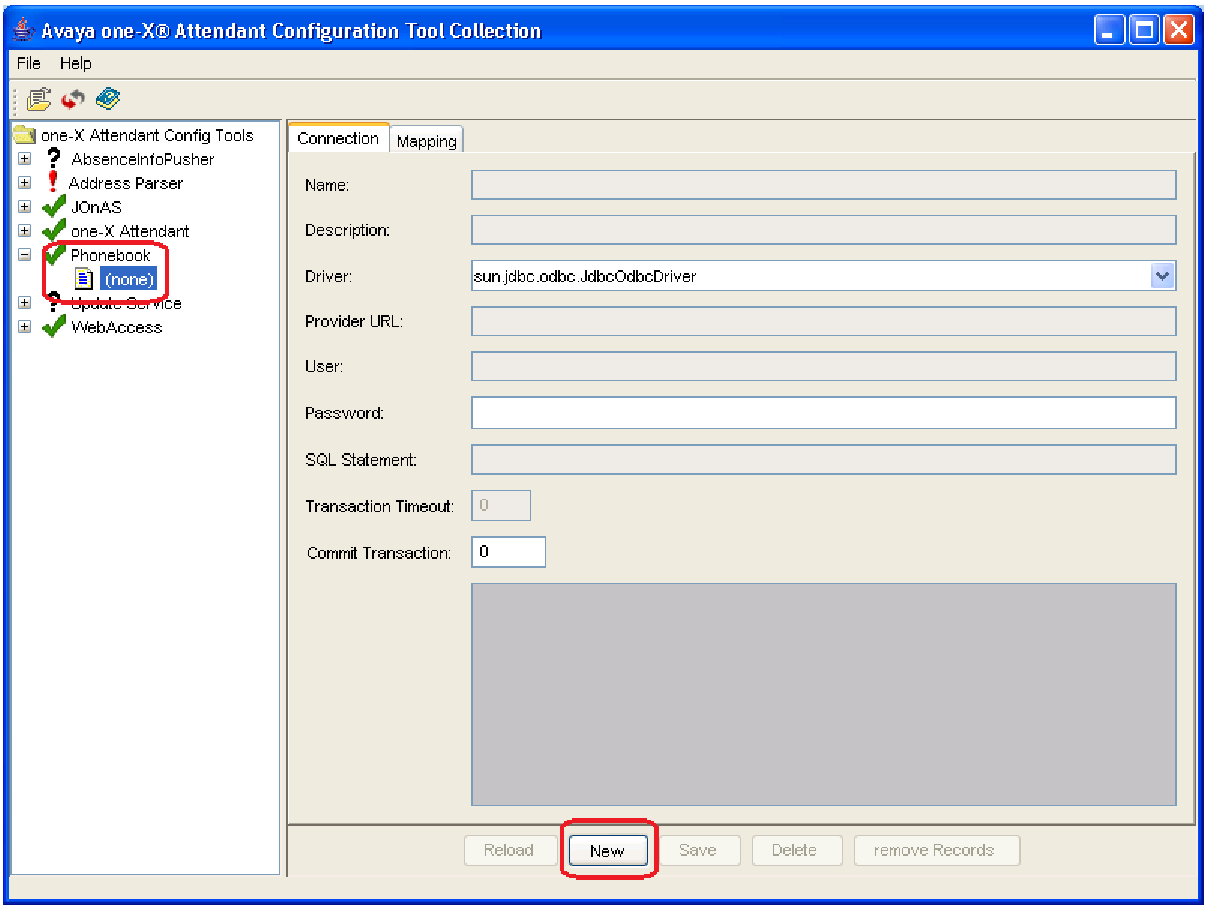
If the name has only one tilde character (~) before the name, the name is converted to Eurofont characters.

If the name has two tilde character (~~) before the name, this record is excluded from importing.

The number ('Primary call number' field) of the first record may require editing.

Import Agent Data into Phone book

1. Start the Avaya one-X Attendant configuration tools application, select an entry under the phonebook item and press the New button in this dialog.



Name:

Description:

Driver: sun.jdbc.odbc.JdbcOdbcDriver

Provider URL:

User:

Password:

SQL Statement:

Transaction Timeout: 0

Commit Transaction: 0

2. Choose the Connection tab

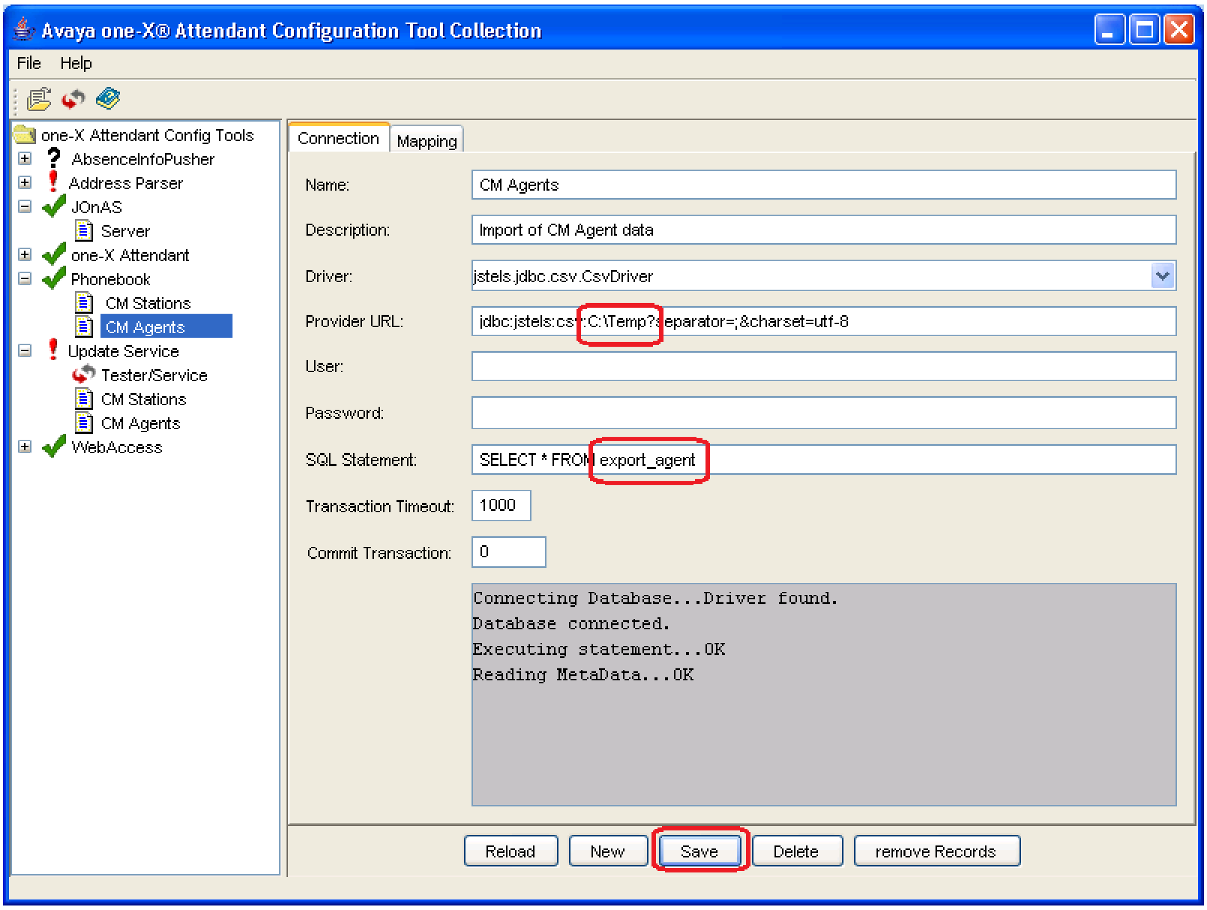
In the field Driver select the entry jstels.jdbc.csv.CsvDriver

Enter a meaningful Name and Description in the belonging fields,

In the field Provider URL replace the text <Enter directory here> with the directory path where the agent data file saved in Step 7 of Create task for Exporting Agent data

In the field SQL statement replace the text <enter tablename here> with the name of the agent data file saved in Step 7 of Create task for Exporting Agent data (without file extension)

Click on the save button



Name: CM Agents

Description: Import of CM Agent data

Driver: jstels.jdbc.csv.CsvDriver

Provider URL: jdbc:jstels:csv:C:\Temp?separator=;&charset=utf-8

User:

Password:

SQL Statement: SELECT * FROM export_agent

Transaction Timeout: 1000

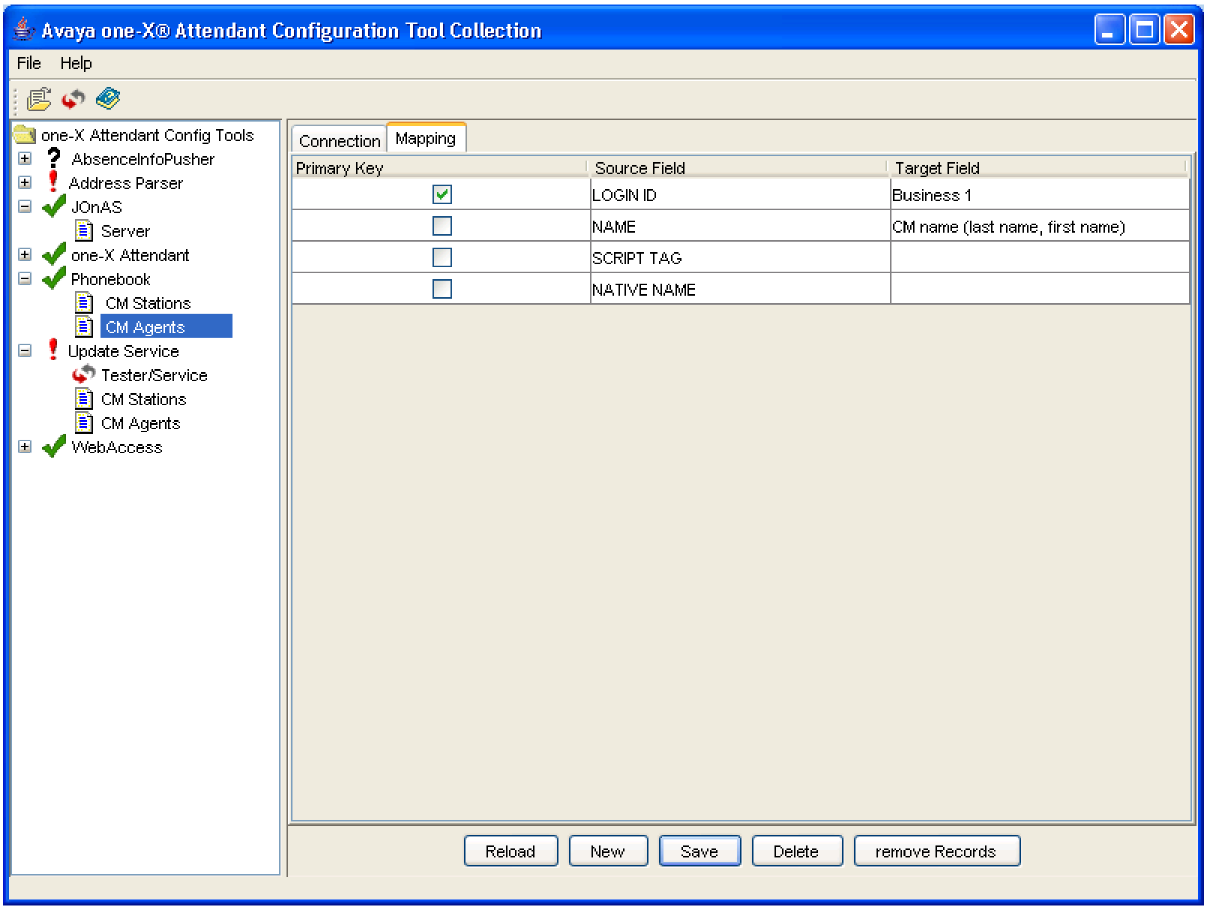
Commit Transaction: 0

```
Connecting Database...Driver found.
Database connected.
Executing statement...OK
Reading MetaData...OK
```

3. Choose the Mapping tab and select for the exported CM fields the belonging one-X Attendant phone book fields.

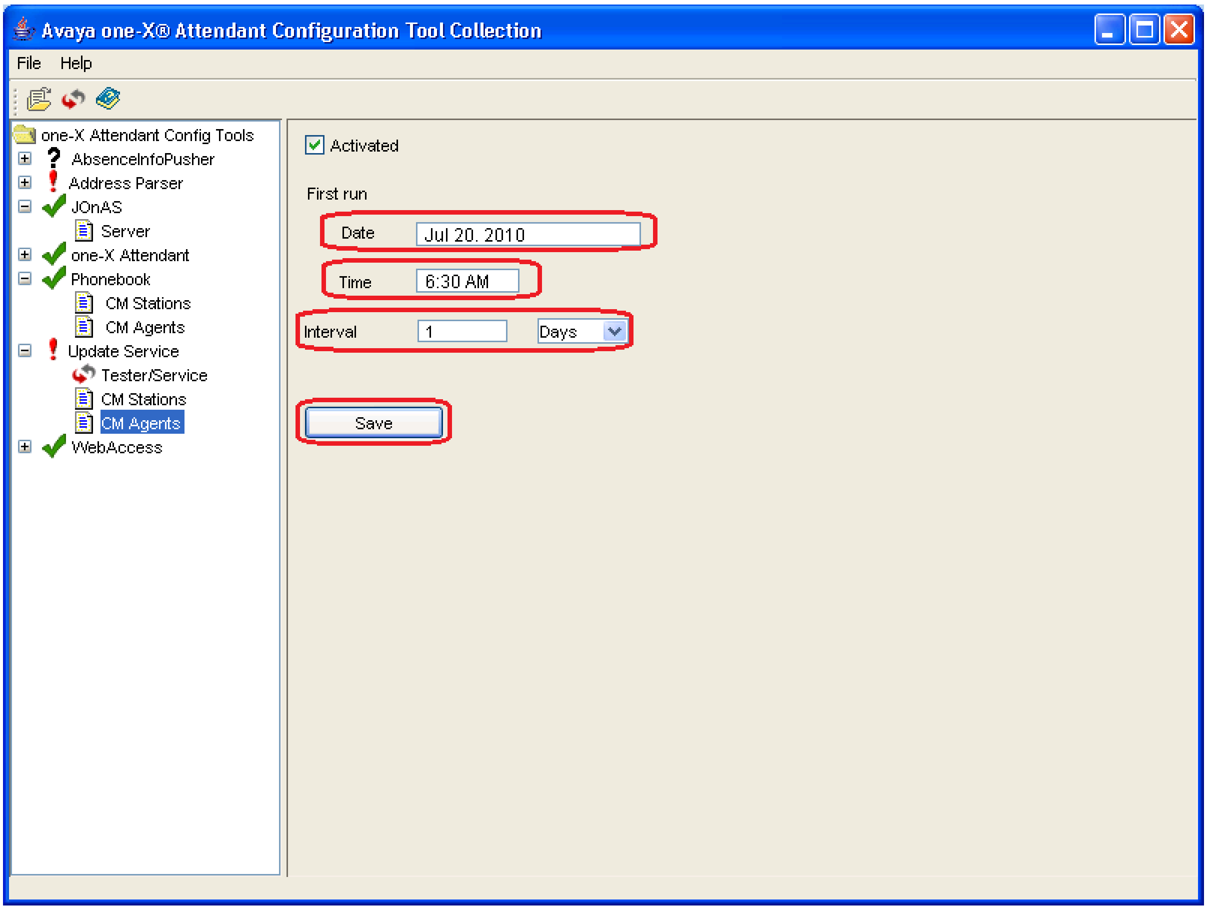
Here we do the following mapping:

- LOGIN ID -> Business 1 (main phone number)
- NAME -> CM name (last name, first name)
- “CM Name (last name, first name)” isn’t a real phone book field. If you choose this as target field and the content of the source field has the format (last name, first name), then it will be split into the phonebook fields (last name) and (first name).
- As primary key the LOGIN ID field should be checked.
- Don’t forget to click on the save button again



Primary Key	Source Field	Target Field
☑	LOGIN ID	Business 1
□	NAME	CM name (last name, first name)
□	SCRIPT TAG	
□	NATIVE NAME	

4. In the Scheduler step, select the date for the task to start, the time for task to run, the interval for when to run the task the next time. When scheduling of the task is completed, click the Save button.



☑ Activated

First run

Date Jul 20. 2010

Time 6:30 AM

Interval 1 Days

Save

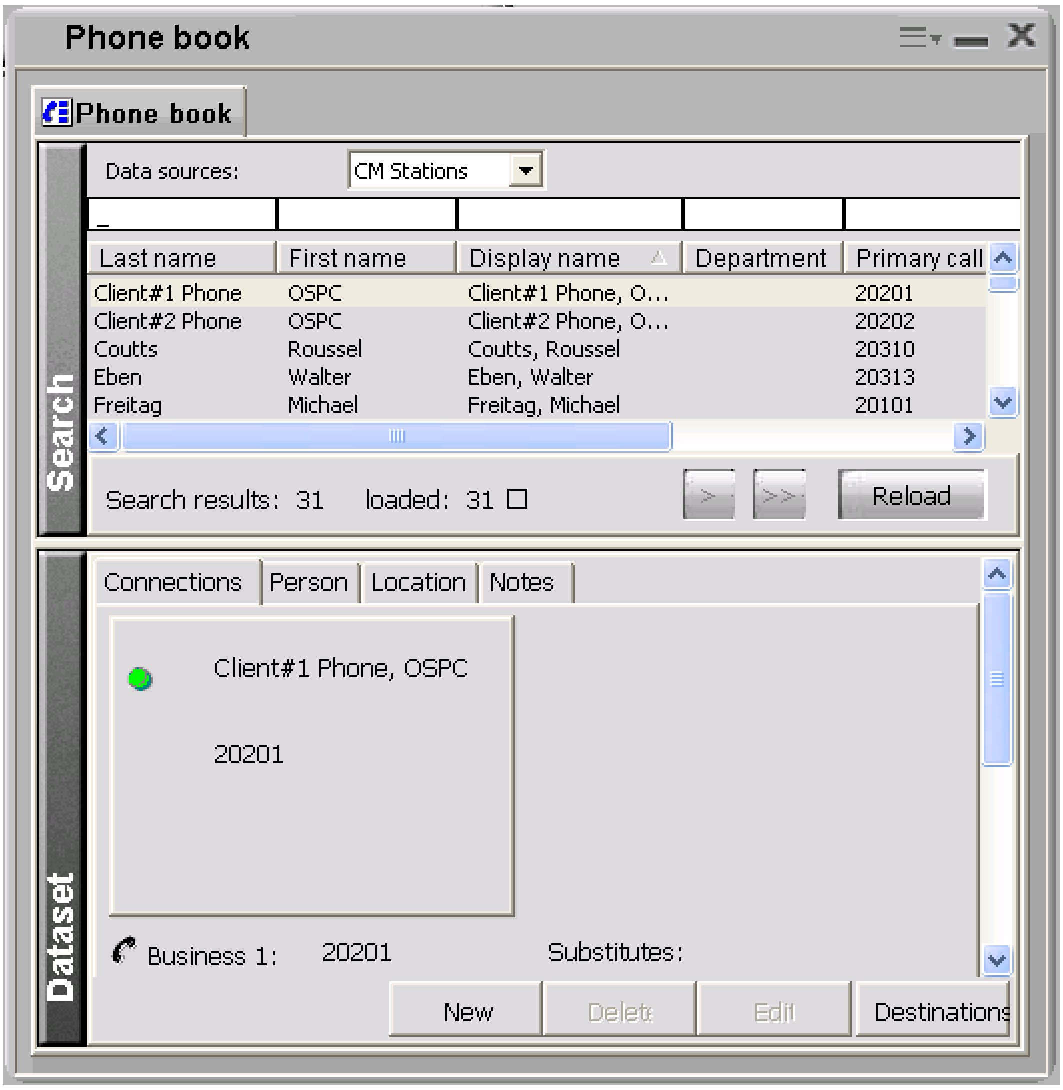
Please also note,

If the name has only one tilde character (~) before the name, the name is converted to Eurofont characters.

If the name has two tilde character (~~) before the name, this record is excluded from importing.

Verification of the Station and/or Agent Data can be done in two ways:

Select the corresponding Data sources (as defined in chapter 2 of Import Station Data into Phone book) in the Avaya one-X Attendant Phone Book and type the “_” character in the search area above the column headings and the records of imported station data are displayed with the total number of records.



Phone book

Data sources: CM Stations

_

Last name	First name	Display name	Department	Primary call
Client#1 Phone	OSPC	Client#1 Phone, O...		20201
Client#2 Phone	OSPC	Client#2 Phone, O...		20202
Coutts	Roussel	Coutts, Roussel		20310
Eben	Walter	Eben, Walter		20313
Freitag	Michael	Freitag, Michael		20101

Search results: 31 loaded: 31 □

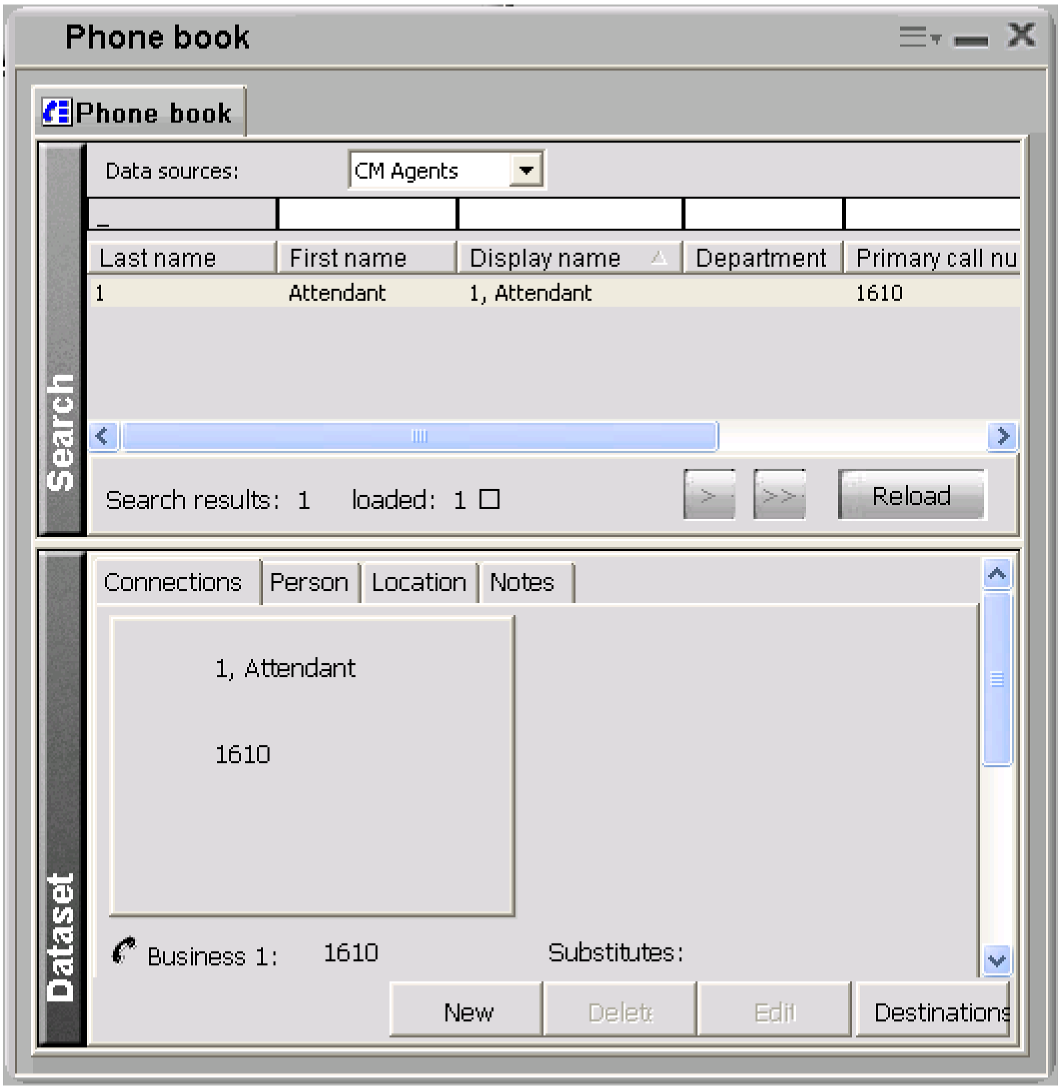
Client#1 Phone, OSPC

20201

Business 1: 20201

Substitutes:

Select the corresponding Data sources (as defined in chapter 2 of Import Station Data into Phone book) in the Avaya one-X Attendant Phone Book and type the “_” character in the search area above the column headings and the records of imported agent data are displayed with the total number of records.



Data sources: CM Agents

Last name	First name	Display name	Department	Primary call nu
_				
1	Attendant	1, Attendant		1610

Search results: 1 loaded: 1 □

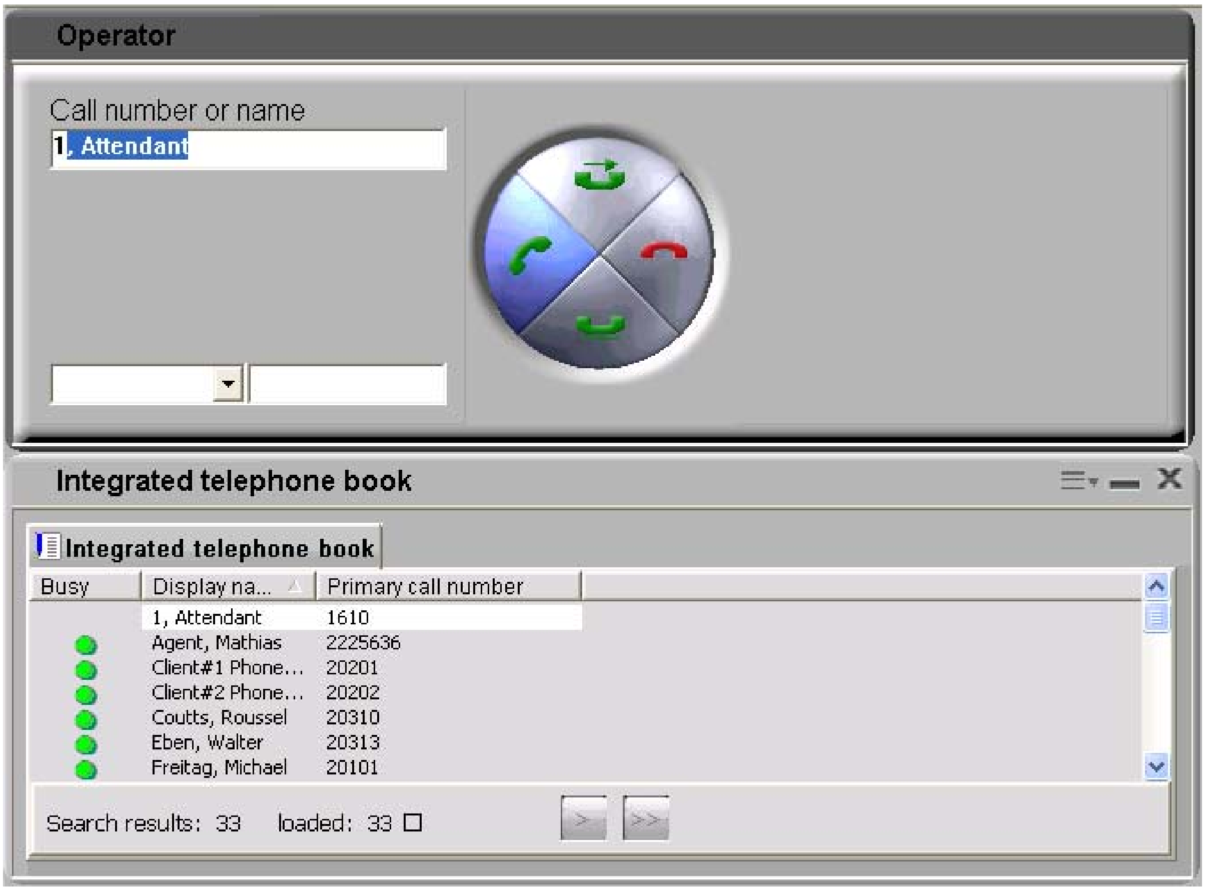
1, Attendant

1610

☎ Business 1: 1610

Substitutes:

Type the “_” character in the ‘Call number or name’ area of the Operator window and the records of imported station and/or agent data are displayed with the total number of records in the Avaya one-X Attendant Integrated telephone book (ITB).



Call number or name: 1, Attendant

Integrated telephone book

Busy	Display na...	Primary call number
	1, Attendant	1610
●	Agent, Mathias	2225636
●	Client#1 Phone...	20201
●	Client#2 Phone...	20202
●	Coutts, Roussel	20310
●	Eben, Walter	20313
●	Freitag, Michael	20101

Search results: 33 loaded: 33 □

In summary, the above step-by-step instructions in this document provides an easy way to cyclic import Station or/and Agent Data into the Avaya one-X Attendant Phone book.

AVAYA one-X Attendant features at a glance

The following table shows the performance features of Avaya one-X Attendant on Communication Manager.

Avaya one-X Attendant v3.00		
		3rd party CM
Switchboard features / Switching calls		
	Making calls with a locked operator set	
	Switch internal –> external	X
	Switch external –> internal	X
	Key block with function keys or destination keys	X
	Switching a call	X
	Three–way conference	X
	Connect an exchange line to an internal subscriber	X
	Serial call	X
	Switching on night service	X
	Priority call	X
	RUL override	X
	Post messages	X
Call types		
	Operator call	X
	Trunk line call	X
	Recall	X
	Emergency call	X
	CFWD (all busy)	X
	CFWD (busy)	X
	CFWD	X
	DND	X
	CFWD (after time)	X
	RecallGoToAttendant	X
	DIV	X
	Return to attendant	X
	Return to the night service station	X
	Return after time	X
	CFWD (SAC)	X
Applications		
	one-X Attendant internally	
	Display time zones	X
	ITB list	X
	Calendar functions	X
	Network–wide busy display	X

		3rd party CM
	Working with containers	X
	Call list	X
	Dial using destination dialing	X
	Redial	X
	Extended redial	X
	Caller ID display	X
	Emergency call	X
	Use phone book	X
	Use subscriber properties	X
	Busy display (max 10 tabs)	X
	- Signaling when subscriber busy on internal call	X
	- Signaling when subscriber busy on external call	X
	VIP display (max 10 tabs)	X
	Network–wide busy display using SVA–Manager	
	Internal/external busy status	X
	Use of 20 tabs	X
	- Signaling of name and telephone number	X
	- Signaling via call forwarding	X
	- Signaling of connection data	X
	Absences through AIS	
	Absences through Outlook and Exchange	X
	Absences in the ITB–window	X
	Absences in the phone book	X
	Absences in the network–wide busy display	X
	Calendar function	
	Calendar function through Outlook and Exchange	X
	Calendar function through Lotus Notes	X
	View subscribers' Outlook contacts	X
	Transfer presence and absence from calendar (Lotus Notes and	X
	External database connection	
	Connection to external databases through JDBC, ODBC or LDAP	X
Edit user		
	Start user administration	X
	User details	X
	Insert, change, copy or delete	X
	Assigning work profiles	X
Work profiles		
	Using different work profiles	X
	Destinations	X
	Features	X

		3rd party CM
	Macros	X
	Editing hotkeys	X
	Configuring the key block	X
	Configuring the busy display	X
	Network–wide busy display	X
	Configure VIP view	X
	Edit time zones	X
	Subscriber properties	X
	Assign users	X
Configuration		
	Acoustic settings	X
	Change password	X
	Entering an emergency number	X
	Changing fonts	X
	Phone book	X
	Absence management	X
Statistics		
	Create statistical data	X
	Configure statistics	X
	Views	X
	Export statistics	X
	Delete statistical data	X
Service and diagnostics		
	one-X Attendant database	
	- Backup	X
	- Restore	X
	Address parser	
	- Standard, France, Spain, Norway	X
	- USA, Russia	X
	Record messages	X
	Importing and exporting users	X
	Importing and exporting profiles	X
	Importing and exporting destinations	X
	Importing and exporting the phone book	X
	Importing CM data into One–X Attendant	X
	Select CTI server access	X
	one-X AttendantInfo	X
	one-X Attendant configtool	X

	Wizard (diagnostics)	X

Load of the system and the net through services of the One-X Attendant, some hints:

Calendar Status

The synchronization of the calendar status is between each individual one-X Attendant client and the appropriate mail server (eg Exchange).

The polling status of the calendar is done here only for those numbers that appear in the local busy indicator.

These are max. 2000 numbers.

The cycle for a maximum of 2000 numbers per client takes about 4 minutes in idealized test environment without burdening the network and the mail server.

The CPU Load of the one-X Attendant Clients rises up to 40% with this activity.

The The one-X Attendant server is on this synchronization not affected.

The interval of the query can be set with the configuration tools on the server (default 10 min.).

If the cycle takes longer than the set interval, the start is postponed for the time of one interval, as long until the running cycle is finished.

An upper limit for the number of mail server postboxes has not to be set from the view of the one-X attendant.

The calendar status is also displayed in the phone book. The client asks the information separately for each of the selected phonebook entry. So, this has no effect on load.

Absenceinformation

The synchronisation of the absence information runs between the one-X Attendant Server and the appropriate mail server (e.g.. Exchange).

The polling of the absence information is performed for all entries in the directory.

A cycle of 10000 mailboxes takes about 40 minutes in ideal test environment without load on the net and the mail server. The load of the one-X Attendant Server will be increased up to 75 % (maxima up to 100%) by this operation. The load is not dependend from the number of mailboxes, only the endurance of a cycle.

On the one-X Attendant Client no load increasing was detectable.

Parallel queries to the one-X Attendant Server will be worked out without nameable delay in cycle.

The interval of the query can be set with the configuration-tool AIS (default: 240 Min.).

If the cycle takes longer as the set interval, a waiting time of 30 seconds will be insert until the next cycle starts.

If a change in the absence information in a mailbox is detected, this information will be written into the one-X Attendant database. All running and registered clients will be informed about the change, to update their absence info displays.

An upper limit for the number of mail server postboxes has not to be calculated from load conditions from a technical point of view.

The upper would make sense in the expectation of a timely update of the information in the one-X Attendant Client.

As the endurance of a cycle increases with the number of postboxes, there could be the danger of an absence info display showing not current values.

Because of the not known for every customer individual net load and load on the mail server with other services, no detailed value can be named.
The up to. 70 % increased CPU workload has to be seen together with the workload of other running one-X Attendant services.

Abbreviations

A

A	Ampere
AC	External Line Code
ACM	Avaya Communication Manager
ACW	After Call Work
AE	Additional Equipment
AEI	Additional Equipment Interface AESApplications Enablement Services
API	Application Programming Interface ARVT Routing (Anrufverteilung)
ARS	Auto Route Selection
ASA	Adaptive Server Anywhere Avaya Site Administration
ASCII	American Standard Code for Information Interchange

B

BIOS	Basic Input Output System (operating system) Bit
Bit	Binary digit (binary digit 0 or 1, smallestinformation unit)
BLS1	Base PCB with S0 interface
Byte	Information unit consisting of 8 bits (= 1 character or code)

C

CCITT	International Telegraph and Telephone Consultative Committee (Comité Consultatif International Télégraphique et Téléphonique)
CE	European Community (CE mark)
CD	Compact Disc
CM	Communication Manager
CN	Telephone Number CORClass of Restriction COSClass of Service
CPU	Central Processing Unit
CSTA	Computer–Supported Telecommunication Applications
CTI	Computer Telephony Integration

D

DC	Direct current
DID	direct inward dial
DOS	Disc Operating System
DSS	Direct Station Select
DTMF	Dual–Tone Multi–Frequency Dialing
DUWA DID	direct inward dial (Durchwahl)

E

eCons	Electronic Consoles
EDS	Enterprise directory system (central electronic phone book)
EEPROM	Electrically Erasable Programmable Read Only Memory
EMC	Electromagnetic compatibility
ETB	Electronic Telephone Book
ETSI	European Telecommunication Standards Institute

H

HSG	Handset and headset unit (Hör- und Sprechgarnitur)
BIOS	Basic Input Output System (operating system) BitBinary digit (binary digit 0 or 1, smallest information unit)
BLS1	Base PCB with S0 interface
Byte	Information unit consisting of 8 bits (= 1 character or code)

I

I55	Integral 55
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
ITB	Integrated Telephone Book

J

JDK	Java Development Kit
JOnAS	Java Open Application Server

L

LAN	Local Area Network
LCD	Liquid Crystal Display
LDAP	Lightweight Directory Access Protocol
LDN	Long Distance Number
LED	Light Emitting Diode

M

MAC	Media Access Control
MS	Microsoft

N

NBA	Network–wide busy display

O

ODBC	Open Database Connectivity
OS	Operator Set Standard
OSM	Operator Service Manager
OSPC	Operator Set PC

P

PC	Personal computer
PROM	Programmable Read Only Memory PSTN Public Switched Telephone Network
PUM	Private User Mobility
PS	Presence Server

Q

QSIG	ISDN based signalling protocol for signalling between private branch extensions

R

RAM	Random Access Memory
RFA	Remote Feature Activation
ROM	Read Only Memory

S

SIP	Session Initiated Protocol
SQL	Structured Query Language
SRG	Feed module (Speisebaugruppe)
SVA	Smart operating device (Smart Vermittlungs Apparat)
SW	Software

T

TAPI	Telephone Application Programming Interface
TCP/IP	Transmission Control Protocol/Internet Protocol
TE	Terminal
TFT	Thin-Film Transistor
PBX	Private branch exchange

U

UAE	Universal connection unit (Universal-Anschluss-Einheit)
UI	User Interface
URL	Uniform Resource Locator

V

V	Volt
V.24	Interface for data transmission according to ITU-T Recommendation V.24
VGA	Video Graphics Adapter
VT	Switching–related (vermittlungstechnisch)

W

W	Watt
WE	Western Electric

References

1. Application Notes for Configuring Avaya WebLM License Manager for Avaya VPNremote; Phone Release 2, Issue 1.0; SPOC 10/25;

2. Administrator Guide for Avaya Communication Manager, Issue 04, Release 5.0 (2008), 03–300509;

3. Feature Description and Implementation for Avaya Communication Manager, Issue 6 (2008), 555–245–205;

4. Avaya Call Center Release 5.0, Call Vectoring and Expert Agent Selection, (EAS) Guide, 07–600780, 01/2008;

5. Administration Guide for Microsoft Exchange Server 2003; Microsoft Corporation; December 2006;

6. User manual licensing, 08/2001;

7. Operating instructions TTraceConsole, 11/2005;

8. Installation and Configuration TTrace (506 kb) , 10/2004;

9. User Manual Customer Interaction Express 1.0 System Administrator, 03/2007, 116791;

10. OSPC connected to Avaya Communication Manager; User’s guide; 03/2008;

11. MasterDirectory Data Manager; Application Notes; 10/1999;

12. This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

Or:

http://support.avaya.com/elmodocs2/vpn/weblm_vpnphone.pdf

http://support.avaya.com/elmodocs2/comm_mgr/r5.0/03–300509_4.pdf

http://support.avaya.com/elmodocs2/comm_mgr/r5.0/245205_6.pdf

https://enterpriseportal.avaya.com/ptlWeb/getfile?docID=MDAzOTYzOTEz

http://www.microsoft.com/downloads/details.aspx?familyid=98e45481–1458–4809–97d6–50d8aeebd8a1&displaylang=en

https://enterpriseportal.avaya.com/ptlWeb/getfile?docID=Mzk1Mjc2Nw

https://enterpriseportal.avaya.com/ptlWeb/getfile?docID=Mzk1Mjc2Mg==

https://enterpriseportal.avaya.com/ptlWeb/getfile?docID=Mzk1Mjc2Mw==

http://support.avaya.com/elmodocs2/cie/r1_0/cie_10_systemadministrator_en[1].pdf

http://support.avaya.com/japple/css/japple?PAGE=Area&temp.bucketID=160257

http://support.avaya.com/css/P8/documents/100010732

https://enterpriseportal.avaya.com/ptlWeb/getfile?docID=MDAzNjc5NDc3Glossary

Glossary

1st party call control

With 1st party call control, there is a clear relationship between the telephone and the PC at each workstation. Generally, the two devices are connected with a cable for the purpose of exchanging information.

3rd party call control

A large range of features can be used with what is known as 3rd party call control. Here, CTI-software controls not just one single telephone, but a private branch-exchange (PBX). As all information about the telephones is saved in the PBX, a direct connection between the computer and the telephone is not necessary. Instead, the PBX must have a CTI interface.
A CTI server is connected to this interface. The telephony software which now controls the PBX can be divided into two parts: Firstly, there is control software on the CTI server which communicates directly with the PBX.
And then there is a telephony program which runs on each PC and which establishes the connection to the CTI application. Apart from the functions offered by 1st party call control applications, 3rd party call control provides a number of additional features, such as switching of incoming calls to certain extensions based on the caller
call control is especially useful for call centers and telemarketing agencies. Incoming calls are routed to suitable agents according to different criteria, and an appropriate application is actuated on the particular PC. 3rd party call control is also useful for outgoing calls. For example, it can establish calls using a power or predictive dialer.

API

stands for Application Programming Interface.

Client

Client is a networking term. A client uses services, which is why a workstation connected to the server is called a client. The client sends user queries in a special protocol to the server and displays the server responses in readable form on the screen.

CSTA

stands for Computer Supported Telecommunications Application. This standard is an ECMA specification. For further information please refer to the manuals: Standard ECMA-179, Standard ECMA-180, Standard ECMA-217, Standard ECMA-218

CTI

means Computer Telephony Integration. In practice, the following CTI functions play a more important role. The ability to initiate a call from various applications by mouse click is especially convenient for everyday use. If the connection is not made, the number is redialed automatically later. The scope and options available in CTI integration depends greatly on the type of implementation.

DLL

stands for Dynamic Link Library.

ID

stands for Identification Number.

ISDN

ISDN stands for Integrated Services Digital Network.

JAVA

is a programming language developed by SUN.

JTAPI

stands for Java Telephony Application Programming Interface. JTAPI is an interface definition specified by a consortium of well–known telecommunications manufacturers for connecting Java applications to PBXs.

JVM

stands for Java Virtual Machine. Java Virtual Machine is required for running Java programs.

LAN

stands for Local Area Network.

NETBEUI

stands for NETBIOS Extended User Interface.

NETBIOS

stands for Network Basic Input Output System.

QTAPI

is a client-server based CTI server, which provides an interface for Microsoft TAPI applications (also Microsoft Outlook for example) and the ACM or the I55.

RPC

stands for Remote Procedure Call. An RPC is the call of a procedure in a module or task that is located on a (possibly) remote computer. Strictly speaking, a procedure is called on one computer (local host) and executed on the other computer (remote host). Any results and the notification that the procedure has ended are returned to the first computer (local host).

Server

The term server is derived from “to serve” (or “to provide service” to someone). A server is a central computer in a network that provides data, memory and resources to the workstations/clients.

Socket

A socket is a mechanism which allows a virtual connection between two processes. It is activated using a socket address. The socket address consists of a port number and a host address.

SPI

stands for Service Provider Interface. This interface is created by the corresponding manufacturer.

TAPI

stands for Telephony Application Programming Interface. TAPI is a telephony software interface from Microsoft.

TCP

stands for Transmission Control Protocol. IP stands for Internet Protocol.

TCP/IP

meets the two most important requirements to be fulfilled in a network. First, it ensures secure transmission. Second, TCP/IP offers an address scheme so that each computer can be assigned an unambiguous address. Computers are numbered by the IP protocol.

TSAPI

TSAPI stands for Telephony Server Application Programmer Interface.

Index