



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Frox Communication Atiras 7.3 with Avaya Aura® Communication Manager 6.2 - Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Avaya Aura® Communication Manager and Frox Communications Atiras.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

Table of Contents

Table of Contents	2
1. Introduction	3
2. General Test Approach and Test Results	3
2.1. Interoperability Compliance Testing.....	4
2.2. Test Results	4
2.3. Support	4
3. Reference Configuration.....	5
4. Equipment and Software Validated	6
5. Configuration of Avaya Aura® Communication Manager	7
5.1. Create Node Name for the AES	8
5.2. Create a CTI Link to the AES	9
5.3. Define the AES Link	9
5.4. Configure Attendant Station.....	10
5.5. Add Vector for Atiras Attendant Console.....	13
5.6. Configure VDN for Atiras Attendant Console.....	14
6. Configuration of Avaya Aura® Application Enablement Services	14
6.1. Logging into the Application Enablement Services.....	15
6.2. Verify Avaya Application Enablement Services License	15
6.3. Create a Communication Manager Switch Connection	16
6.4. Create a TSAPI Link	19
6.5. Create CTI User	21
6.6. Configure DMCC Port	22
7. Configuration of Atiras Attendant Console module.....	23
7.1. Synchronize VDN and Vector.....	24
7.2. Associate Attendant extension with Atiras (Frox) Attendant Console	28
7.3. Create a Super User for the Attendant	30
7.4. Configuration Atiras Attendant Console.....	33
7.5. Configure Atiras Attendant Console to connect to Avaya Application Enablement Services	37
7.6. Restart the Nms Attendant Console	40
8. Configuration Atiras Configuration module.....	41
8.1. Configure Avaya Aura Communication Manager	41
8.2. Synchronize Telephony functions.....	47
8.3. Configure Atiras for Avaya Session Manager	50
8.4. Synchronize Session Manager	53
8.5. Configure Atiras for Avaya Message Storage Server	55
8.6. Synchronize Avaya Message Storage Server	57
9. Verification Steps	59
9.1. Verify Avaya Aura® Communication Manager CTI Service State	59
9.2. Verify Avaya Aura® Application Enablement Services DMCC.....	60
9.3. Verify Atiras Attendant Console extension is assigned to the Attendant	61
9.4. Verify Atiras Configuration module synchronization status.....	63
10. Conclusion	64
11. Additional References.....	64

1. Introduction

These Application Notes describe the configuration steps to integrate Frox Communications Atiras (Atiras) with Avaya Aura® Communication Manager (CM) and Avaya Aura® Application Enablement Services (AES). The Atiras Plus network management system is an extension to Private Branch Exchange (PBX) systems. Atiras is a modular software package with which can take full advantage of the options offered by the PBX. Atiras simplifies everyday telephone tasks and makes information available which allows optimization of the system management and provisioning. The Atiras functions are divided into modules which may be used individually or combined, as required. Based on Microsoft Windows computer systems, Atiras is able to support and relieve the central office in switching calls, preparing operating data and creating call charge data reports. The client/server structure enables the software components to be installed decentralized on each staff member's PC. The main components are installed on a Windows Server, which is also responsible for the communication with the PBXs. In addition, a Web client enables access to important Atiras functions by using any browser. During compliance testing, only the Atiras Configuration and Attendant Console modules were tested. The Atiras Configuration module enables the user to Add, Change and Delete stations and voice mailboxes on Communication Manager and Avaya Aura® Messaging (AAM). Session Initialization Protocol (SIP) stations can also be administered via the Avaya Aura® System Manager. The Atiras Attendant Console module is a Windows-based server/client system with an integrated central database. The server installation can also be used as a client with single-user systems, a specific server is not required in this case. Access to the various telephone directories can be restricted via user groups. Predefined query filters can also be configured for each user group to automatically control access to certain data.

Note: The Attendant Console station must be H.323

2. General Test Approach and Test Results

The general test approach was to configure the Atiras Attendant Console module to communicate to the Communication Manager via the AES) as implemented on a customer site. The Atiras Configuration module was configured to integrate with the Communication Manager and System Manager also as implemented on a customer site. See **Figure 1** for a network diagram. The interoperability compliance test included both feature functionality and serviceability tests.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

2.1. Interoperability Compliance Testing

Feature functionality testing included:

Atiras Attendant Console module

- Answer internal/external calls
- Calls to internal/external numbers
- Calls using telephone book
- Supervised and unsupervised transfers
- Conference calls

Atiras Configuration module

- Verify synchronization between Atiras and Communication Manager
- Verify synchronization between Atiras and Aura Messaging
- Add/Change/Delete Analog/Digital/IP stations (H323 and SIP)
- Add/Change/Delete Voice mail boxes
- Add/Change/Delete Speed Call lists
- Add/Change/Delete Hunt/Pickup groups
- Schedule jobs

Miscellaneous

- AES disconnect/reconnection
- Restart failed job synchronization

2.2. Test Results

Tests were performed to insure full interoperability between Atiras and the Communication Manager. The tests were all functional in nature and performance testing was not included. All the test cases passed successfully.

2.3. Support

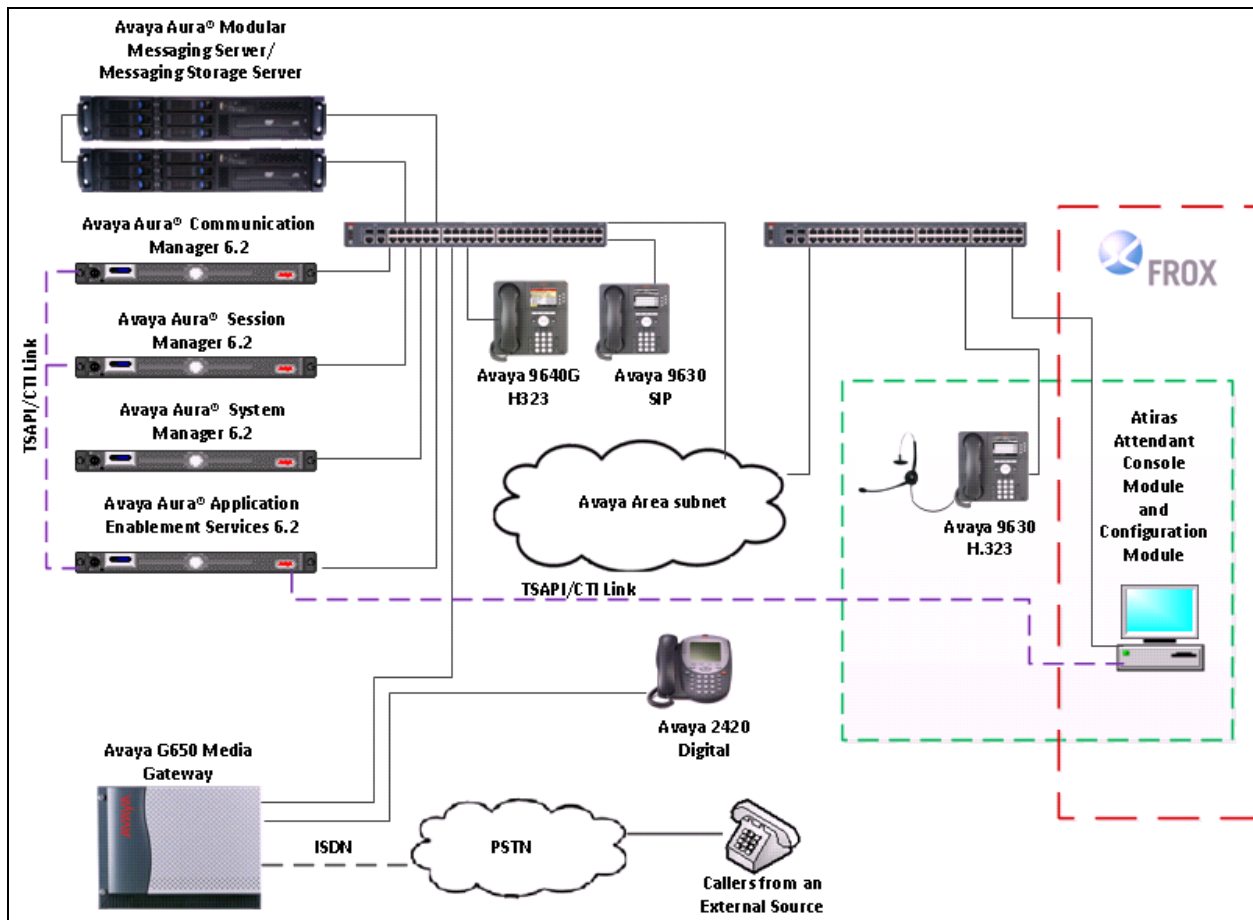
Technical support for Frox Communications products can be found as follows:

<http://www.frox.com/en/10052/Contact.html>

3. Reference Configuration

Figure 1 illustrates the network topology used during compliance testing. The Avaya solution consists of Avaya Aura® Communication Manager, Avaya Aura® System Manager, Avaya Aura® Session Manager, Avaya Application Enablement Services, Avaya Modular Messaging and a G650 Gateway. The Atriras Attendant Console had Computer-telephony Integration (CTI) control of the Attendant station using Telephony Server Application Programming Interface (TSAPI) on the Application Enablement Services. An Avaya 9630G was used as the Attendant station. Inbound and outbound calls to the PSTN were made via a G650 Media Gateway. Avaya 9640G, 9630 (H323), 9630 (SIP) and 2420 (Digital Deskphones were used as endpoints during compliance testing.

There is no configuration required on the Communication Manager or System Manager to interoperate with the Atriras Configuration module other than a Communication and System Manager user.



**Figure 1: Avaya Aura® Communication Manager and Application Enablement Services
Atriras Reference Configuration**

4. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

Avaya Equipment	Software / Firmware Version
Avaya Aura® Communication Manager running on Avaya S8800 Server	R6.2 Version 06.2-02.0.823.0
Avaya Aura® Application Enablement Services running on Avaya S8800 Server	R6.2 Build r6-2-18-0
Avaya Aura® System Manager running on Avaya S8800 Server	R6.2 SP4 Build 6.2.0.0.15669-6.2.12.408 Software Update Revision 6.2.16.1.1993
Avaya Aura® Session Manager running on Avaya S8800 Server	R6.2 Version 6.2.3.0.623006
Avaya Modular Messaging running on S3500 Servers	5.2 Patch 8 MAS - 9.2.150.13
Avaya G650 Media Gateway <ul style="list-style-type: none">• TN2602AP• TN799DP	HW8 FW61 HW01 FW040
Avaya Telephones <ul style="list-style-type: none">• 9640G (SIP)• 9630G (H323)• 2420D	2.6.84 S3.1055 6
Frox Communications Equipment	Software / Firmware Version
Atiras running on Windows server 2008 R2 SP1	Atiras 7.3

5. Configuration of Avaya Aura® Communication Manager

Configuration and verification operations on the Communication Manager illustrated in this section were all performed using Avaya Site Administrator Emulation Mode. The information provided in this section describes the configuration of Communication Manager for this solution. It is implied a working system is already in place including a Communication Manager user for Atiras. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section 11**. The configuration operations described in this section can be summarized as follows:

- Create Node Name for the AES
- Create a CTI Link to the AES
- Define the AES Link
- Configure Attendant station
- Add Vector for Atiras Attendant Console
- Configure VDN for Atiras Attendant Console

Note: There is no configuration required on the Communication Manager to interoperate with the Atiras Configuration module other than a Communication Manager user.

5.1. Create Node Name for the AES

A Node Name needs to be created to associate the Communication Manager with the AES. Use the **change node-names ip** command to configure the following:

Page 1

- **Name** Enter an informative name i.e. **aesserver62**
- **IP address** Enter the IP address of the **AES** (10.10.16.96)

Press **f3** button to save the new settings.

```
change node-names ip
Page 1 of 2

                                IP NODE NAMES

      Name                IP Address
KOFAX                    10.10.16.69
aesserver62            10.10.16.96
calacsy                  10.10.60.51
clan                     10.10.16.31
cmm                      10.10.16.142
cms                      10.10.16.175
default                  0.0.0.0
devconiq52all           10.10.16.125
gateway                  10.10.16.1
medprotn2302             10.10.16.32
procr                    10.10.16.142
procr6                   ::
sm62fo                   10.10.16.157
sm62sigint               10.10.16.148
tiger                    10.10.16.101

( 15 of 15   administered node-names were displayed )
Use 'list node-names' command to see all the administered node-
names
Use 'change node-names ip xxx' to change a node-name 'xxx' or add
a node-name
```


5.2. Create a CTI Link to the AES

A CTI Link needs to be created to enable the Communication Manager interoperate with the AES. Use the **add cti-link** command to configure the following: (during compliance testing cti link 1 was added)

Page 1

- **Extension** Enter the extension that will be used to call the Atrias Attendant Console (during compliance testing extension 5899 was used)
- **TYPE** Enter **ADJ-IP**
- **Name** Enter **aesserver62** (as created in **Section 5.1**)

Press **f3** button to save the new settings.

add cti-link 1		Page 1 of 3
CTI LINK		
CTI Link: 1		
Extension: 5899		
Type: ADJ-IP		COR: 1
Name: aesserver62		

5.3. Define the AES Link

To define the AES link use the **change ip-services** command and enter the following:

Page 1

- **Type** Enter **AESVCS**
- **Enabled** Enter **y**
- **Local Node** Enter **procr**
- **Port** Enter **8765**

change ip-services						
Page 1 of 4						
IP SERVICES						
Service Type	Enabled	Local Node	Local Port	Remote Node	Remote Port	
AESVCS	y	procr	8765			
PMS		procr	0	tiger	5004	
CDR1		procr	0	calacsy	9001	

Navigate to **Page 4** and enter the following:

- **Server ID** Enter **1**
- **AE Services** Enter **aesserver62** (The node created in **section 5.1**)
- **Password** Enter a password. This password will be used in **Section 6.3** to enable the AES to communicate with the Communication Manager.

Press **f3** button to save the new settings.

change ip-services				Page 4 of 4
AE Services Administration				
Server ID	AE Services Server	Password	Enabled	Status
1:	aesserver62	*	y	in use

5.4. Configure Attendant Station

The only distinctive requirement which the station to be used as the Attendant Console requires is that it must have 3 **BUTTON ASSIGNMENTS** for call appearances. To add the attendant station use the **change add station** command. The station configured during compliance testing (6001) is shown in the section below.

add station 6001		Page	1 of	5
STATION				
Extension: 6001	Lock Messages? n	BCC: 0		
Type: 9630	Security Code: *	TN: 1		
Port: S00007	Coverage Path 1:	COR: 1		
Name: Extn.6001	Coverage Path 2:	COS: 1		
	Hunt-to Station:			
STATION OPTIONS				
	Time of Day Lock Table:			
Loss Group: 19	Personalized Ringing Pattern: 1			
	Message Lamp Ext: 6001			
Speakerphone: 2-way	Mute Button Enabled? y			
Display Language: english	Button Modules: 0			
	Survivable GK Node Name:			
Survivable COR: internal	Media Complex Ext:			
Survivable Trunk Dest? y	IP SoftPhone? n			
	IP Video? n			
	Short/Prefixed Registration Allowed: default			
	Customizable Labels? y			

add station 6001

Page 2 of 5

STATION

FEATURE OPTIONS

LWC Reception: spe

Auto Select Any Idle Appearance? n

LWC Activation? y

Coverage Msg Retrieval? y

LWC Log External Calls? n

Auto Answer: none

CDR Privacy? n

Data Restriction? n

Redirect Notification? y

Idle Appearance Preference? n

Per Button Ring Control? n

Bridged Idle Line Preference? n

Bridged Call Alerting? n

Restrict Last Appearance? y

Active Station Ringing: single

EMU Login Allowed? n

H.320 Conversion? n

Per Station CPN - Send Calling Number? y

Service Link Mode: as-needed

EC500 State: enabled

Multimedia Mode: enhanced

Audible Message Waiting? n

MWI Served User Type:

Display Client Redirection? n

AUDIX Name:

Select Last Used Appearance? n

Coverage After Forwarding? s

Multimedia Early Answer? n

Direct IP-IP Audio Connections? y

Emergency Location Ext: 6001

Always Use? n

IP Audio Hairpinning? n

add station 6001

Page 3 of 5

STATION

Conf/Trans on Primary Appearance? n

Bridged Appearance Origination Restriction? n

Call Appearance Display Format: disp-param-default

IP Phone Group ID:

Enhanced Callr-Info Display for 1-Line Phones? n

ENHANCED CALL FORWARDING

Forwarded Destination

Active

Unconditional For Internal Calls To:

External Calls To: n

Busy For Internal Calls To: n

External Calls To: n

No Reply For Internal Calls To: n

External Calls To: n

SAC/CF Override: n

add station 6001

Page 4 of 5

STATION

SITE DATA

Room:

Headset? n

Jack:

Speaker? n

Cable:

Mounting: d

Floor:

Cord Length: 0

Building:

Set Color:

ABBREVIATED DIALING

List1: enhanced 1

List2: system

List3:

personal 1

BUTTON ASSIGNMENTS

1: call-appr

5: auto-in

Grp:

2: call-appr

6: aux-work

RC: 1

Grp: 1

3: call-appr

7: aux-work

RC: 3

Grp: 1

4: abrv-dial

List: 1

DC: 002

8: after-call

Grp:

voice-mail

add station 6001

Page 5 of 5

STATION

BUTTON ASSIGNMENTS

9:

10:

11:

12:

13:

14:

15:

16:

17:

18:

19:

20:

21:

22:

23:

24:

5.5. Add Vector for Atras Attendant Console

To add a vector for the Atras Attendant use the **add vector** command and enter the following:
(Vector 666 was used during compliance testing)

Page 1

- **Name** Enter an informative name (i.e. **Frox**)
- **Line 1** Enter **wait-time 2 secs hearing ringback**
- **Line 2** Enter **adjunct routing link 1** (CTI Link configured in **Section 5.2**)
- **Line 3** Enter **wait-time 600 secs hearing ringback**

Press **f3** button to save the new settings.

```
add vector 666                                     Page 1 of 6
                                                    CALL VECTOR
Number: 666                      Name: Frox
Multimedia? y  Attendant Vectoring? n  Meet-me Conf? n  Lock? n
Basic? y  EAS? y  G3V4 Enhanced? y  ANI/II-Digits? y  ASAI Routing? y
Prompting? y  LAI? y  G3V4 Adv Route? y  CINFO? y  BSR? Y  Holidays? y
Variables? y  3.0 Enhanced? y
01 wait-time      2  secs hearing ringback
02 adjunct        routing link 1
03 wait-time      600 secs hearing ringback
04
05
06
07
08
09
10
11
12
```

5.6. Configure VDN for Atiras Attendant Console

To add a VDN for the Atiras Attendant use the **add VDN** command and enter the following:
(Vector 666 was used during compliance testing)

Page 1

- **Name** Enter an informative name (i.e. **Atirasattendant**)
- **Destination** Enter **Vector Number 666** (Vector as configured in **Section 5.5**)
- **Attendant Vectoring?** Enter **n**

Press **f3** button to save the new settings.

```
add vdn 6666                                     Page 1 of 3
VECTOR DIRECTORY NUMBER
Extension: 6666
Name*: Atirasattendant
Destination: Vector Number 666
Attendant Vectoring? n
Meet-me Conferencing? n
Allow VDN Override? n
COR: 1
TN*: 1
Measured: none
VDN of Origin Annc. Extension*:
1st Skill*:
2nd Skill*:
3rd Skill*:
* Follows VDN Override Rules
```

6. Configuration of Avaya Aura® Application Enablement Services

This section provides the procedures for configuring Avaya Application Enablement Services. It is implied a working AES is already in place and the Security Database (SDB) is configured. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section 11**. The configuration operations described in this section can be summarized as follows:

- Logging into Application Enablement Services
- Verify Avaya Application Enablement Services License
- Create a Communication Manager Switch Connection
- Create a TSAPI Link
- Create CTI User
- Configure DMCC Port

6.1. Logging into the Application Enablement Services

To access the OAM web-based interface of the Application Enablement Services Server use the URL **http://x.x.x.x**, where **x. x. x. x** is the selected IP address of AES. The **Management console** is displayed. Log in using the appropriate credentials.

The screenshot shows the Avaya Application Enablement Services Management Console login page. At the top left is the Avaya logo. The title "Application Enablement Services Management Console" is centered. A red navigation bar at the top right contains a "Help" link. The main content area features a login box with the text "Please login here:" followed by "Username" and "Password" labels, each with a corresponding text input field. A "Login" button is positioned below the password field. At the bottom, a red bar contains the copyright notice: "© Copyright © 2009-2010 Avaya Inc. All Rights Reserved."

6.2. Verify Avaya Application Enablement Services License

Select **AE Services** on the left pane and verify that the **TSAPI Service** is licensed by ensuring that **TSAPI Service** is in the list of services and that the **License Mode** is showing **NORMAL MODE**.

The screenshot displays the Avaya Application Enablement Services Management Console with the "AE Services" section selected in the left-hand navigation pane. The main content area shows the "AE Services" page. At the top right, a welcome message for user "craft" is displayed, including login details and server information. Below this, a red navigation bar contains "Home | Help | Logout" links. The left pane lists various services, with "AE Services" expanded to show sub-items like CVLAN, DLG, DMCC, SMS, TSAPI, and TWS. The "Communication Manager Interface" section is also visible. The main content area contains an "IMPORTANT" notice about restarting services, a table of services, a link to "Status and Control", and "License Information".

Service	Status	State	License Mode	Cause*
ASAI Link Manager	N/A	Running	N/A	N/A
CVLAN Service	ONLINE	Running	NORMAL MODE	N/A
DLG Service	OFFLINE	Running	N/A	N/A
DMCC Service	ONLINE	Running	NORMAL MODE	N/A
TSAPI Service	ONLINE	Running	NORMAL MODE	N/A
Transport Layer Service	N/A	Running	N/A	N/A

For status on actual services, please use [Status and Control](#)

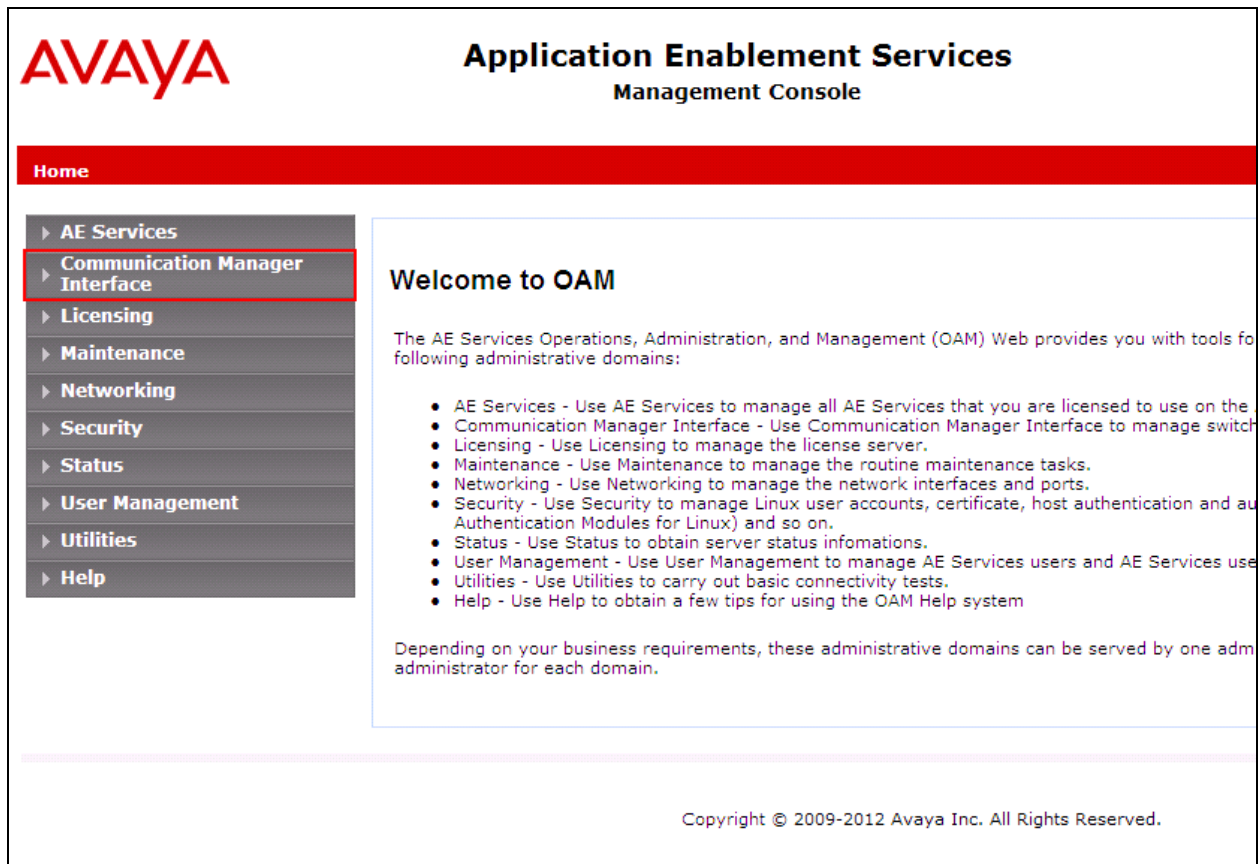
* -- For more detail, please mouse over the Cause, you'll see the tooltip, or go to help page.

License Information
You are licensed to run Application Enablement (CTI) release 6.x

Copyright © 2009-2012 Avaya Inc. All Rights Reserved.

6.3. Create a Communication Manager Switch Connection

A Communication Manager Switch Connection needs to be created to enable the AES to communicate with the Communication Manager. Select **Communication Manager interface**.



AVAYA

Application Enablement Services
Management Console

Home

- ▶ AE Services
- ▶ **Communication Manager Interface**
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▶ Security
- ▶ Status
- ▶ User Management
- ▶ Utilities
- ▶ Help

Welcome to OAM

The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for the following administrative domains:

- AE Services - Use AE Services to manage all AE Services that you are licensed to use on the system.
- Communication Manager Interface - Use Communication Manager Interface to manage switch connections.
- Licensing - Use Licensing to manage the license server.
- Maintenance - Use Maintenance to manage the routine maintenance tasks.
- Networking - Use Networking to manage the network interfaces and ports.
- Security - Use Security to manage Linux user accounts, certificate, host authentication and authentication modules for Linux) and so on.
- Status - Use Status to obtain server status information.
- User Management - Use User Management to manage AE Services users and AE Services user groups.
- Utilities - Use Utilities to carry out basic connectivity tests.
- Help - Use Help to obtain a few tips for using the OAM Help system.

Depending on your business requirements, these administrative domains can be served by one administrator for each domain.

Copyright © 2009-2012 Avaya Inc. All Rights Reserved.

Select **Switch Connections** and enter an informative name for Communication Manager (i.e. CM62). Click on the **Add Connection** button.

AVAYA **Application Enablement Services**
Management Console

Communication Manager Interface | Switch Connections

Navigation Menu:

- ▶ AE Services
- ▼ **Communication Manager Interface**
 - Switch Connections**
 - ▶ Dial Plan
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▶ Security
- ▶ Status
- ▶ User Management
- ▶ Utilities
- ▶ Help

Switch Connections

CM62 **Add Connection**

Connection Name	Processor Ethernet

Edit Connection **Edit PE/CLAN IPs** **Edit H.323 Gatekeeper** **Delete**

Once the **Connection Details** window opens enter the **Switch Password** as was configured in **Section 5.3** then **Confirm Switch Password** Click on the **Apply** button.

The screenshot displays the Avaya Application Enablement Services Management Console. On the left is a navigation menu with options: AE Services, Communication Manager Interface (expanded), Switch Connections (highlighted), Dial Plan, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. The main content area is titled 'Connection Details - CM62'. It contains a red-bordered box around the 'Switch Password' and 'Confirm Switch Password' input fields. Below these are fields for 'Msg Period' (set to 30) and 'SSL' (checked). The 'Processor Ethernet' checkbox is also checked. At the bottom of the form are 'Apply' and 'Cancel' buttons, with the 'Apply' button highlighted by a red box.

AVAYA **Application Enablement Services**
Management Console

Communication Manager Interface | Switch Connections

▶ AE Services
▼ Communication Manager Interface
 Switch Connections
 ▶ Dial Plan
▶ Licensing
▶ Maintenance
▶ Networking
▶ Security
▶ Status
▶ User Management
▶ Utilities
▶ Help

Connection Details - CM62

Switch Password
Confirm Switch Password

Msg Period Minutes (1 - 72)
SSL ☒
Processor Ethernet ☒

6.4. Create a TSAPI Link

A TSAPI Link needs to be created to interoperate with the Atiras. Navigate to **AE Services** → **TSAPI** → **TSAPI Links** and click on the **Add Link** button.

The screenshot displays the Avaya Application Enablement Services Management Console. The top left features the Avaya logo. The top right shows the title 'Application Enablement Services Management Console'. A red navigation bar contains the text 'AE Services | TSAPI | TSAPI Links'. On the left, a sidebar menu lists various services: 'AE Services' (expanded), 'CVLAN', 'DLG', 'DMCC', 'SMS', 'TSAPI' (expanded), 'TSAPI Links' (highlighted with a red box), 'TSAPI Properties', 'TWS', and 'Communication Manager Interface'. The main content area is titled 'TSAPI Links' and contains a table with three columns: 'Link', 'Switch Connection', and 'Swi'. Below the table are three buttons: 'Add Link' (highlighted with a red box), 'Edit Link', and 'Delete Link'.

Link	Switch Connection	Swi

[Add Link](#) [Edit Link](#) [Delete Link](#)

Once the **Add TSAPI Links** window opens enter the following:

- Select **CM62** from the **Switch Connection** dropdown box. (The Switch connection as created in **Section 6.3**)
- Select **1** from the **Switch CTI Link Number** dropdown box. (The CTI link as created in **Section 5.2**)

Click on the **Apply Changes** button.

The screenshot displays the Avaya Application Enablement Services Management Console. The left sidebar shows a navigation menu with 'AE Services' expanded, containing 'CVLAN', 'DLG', 'DMCC', 'SMS', 'TSAPI' (expanded to show 'TSAPI Links' and 'TSAPI Properties'), and 'TWS'. The 'Communication Manager' section is also visible. The main content area is titled 'Add TSAPI Links' and contains the following configuration fields:

- Link: 1
- Switch Connection: CM62
- Switch CTI Link Number: 1
- ASAI Link Version: 4
- Security: Unencrypted

At the bottom of the configuration area are two buttons: 'Apply Changes' and 'Cancel Changes'. Red boxes highlight the 'Switch Connection' and 'Switch CTI Link Number' dropdowns, and the 'Apply Changes' button.

6.5. Create CTI User

Navigate to **User Manager** → **User Admin**, then select **Add User**. On the **Add User** screen enter the following:

- Enter a **User Id**: in this case **ctiuser**, This ID will be required for the Atriras configuration.
- Enter a **Common Name**: in this case **ctiuser**
- Enter a **Surname**: in this case **ctiuser**
- Enter a **User Password**: This password will be required for the Atriras configuration.
- Enter the password again for **Confirm Password**
- Select **userservice.useradmin** from the **Avaya Role** dropdown box.
- Select **Yes** from the **CT User** dropdown box.

Click **Apply** at the bottom of the screen (not shown below)

User Management | User Admin | Add User

Add User

Fields marked with * can not be empty.

* User Id	ctiuser
* Common Name	ctiuser
* Surname	ctiuser
* User Password	••••••••
* Confirm Password	••••••••
Admin Note	
Avaya Role	userservice.useradmin ▼
Business Category	
Car License	
CM Home	
Cms Home	
CT User	Yes ▼
Department Number	
Display Name	
Employee Number	

Navigation Menu:

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▶ Security
- ▶ Status
- ▼ **User Management**
 - ▶ Service Admin
 - ▼ **User Admin**
 - **Add User**
 - Change User Password
 - List All Users
 - Modify Default Users
 - Search Users
- ▶ Utilities
- ▶ Help

6.6. Configure DMCC Port

On the AES Management Console navigate to **Networking → Ports**. In the **DMCC Server Ports** area Enter the **Unencrypted Port** and click on the **Enabled** radio button. During compliance testing, the **Unencrypted Port** was set to **4721**. Click the **Apply Changes** button (not shown) at the bottom of the screen to complete the process.

Note: Although the TSAPI feature is used, the DMCC port is configured.

The screenshot displays the Avaya Application Enablement Services Management Console. The left sidebar shows a navigation menu with 'Networking' expanded and 'Ports' selected. The main content area is titled 'Ports' and contains several sections: CVLAN Ports, DLG Port, TSAPI Ports, and DMCC Server Ports. The DMCC Server Ports section is highlighted with a red box, showing the 'Unencrypted Port' set to 4721 and the 'Enabled' radio button selected. Other sections include CVLAN Ports (Unencrypted TCP Port: 9999, Encrypted TCP Port: 9998), DLG Port (TCP Port: 5678), and TSAPI Ports (TSAPI Service Port: 450, Local TLINK Ports: TCP Port Min: 1024, TCP Port Max: 1039, Unencrypted TLINK Ports: TCP Port Min: 1050, TCP Port Max: 1065, Encrypted TLINK Ports: TCP Port Min: 1066, TCP Port Max: 1081).

Section	Parameter	Value	Enabled	Disabled
CVLAN Ports	Unencrypted TCP Port	9999	<input checked="" type="radio"/>	<input type="radio"/>
	Encrypted TCP Port	9998	<input checked="" type="radio"/>	<input type="radio"/>
DLG Port	TCP Port	5678		
TSAPI Ports	TSAPI Service Port	450	<input checked="" type="radio"/>	<input type="radio"/>
	Local TLINK Ports			
	TCP Port Min	1024		
	TCP Port Max	1039		
	Unencrypted TLINK Ports			
	TCP Port Min	1050		
DMCC Server Ports	Unencrypted Port	4721	<input checked="" type="radio"/>	<input type="radio"/>
	Encrypted Port	4722	<input checked="" type="radio"/>	<input type="radio"/>
	TR/87 Port	4723	<input checked="" type="radio"/>	<input type="radio"/>

7. Configuration of Atras Attendant Console module

This section describes the steps performed to configure the Atras Attendant Console module. It is implied that the Atras s Attendant Console module software is already installed and licensed. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section 11**. The configuration operations described in this section can be summarized as follows:

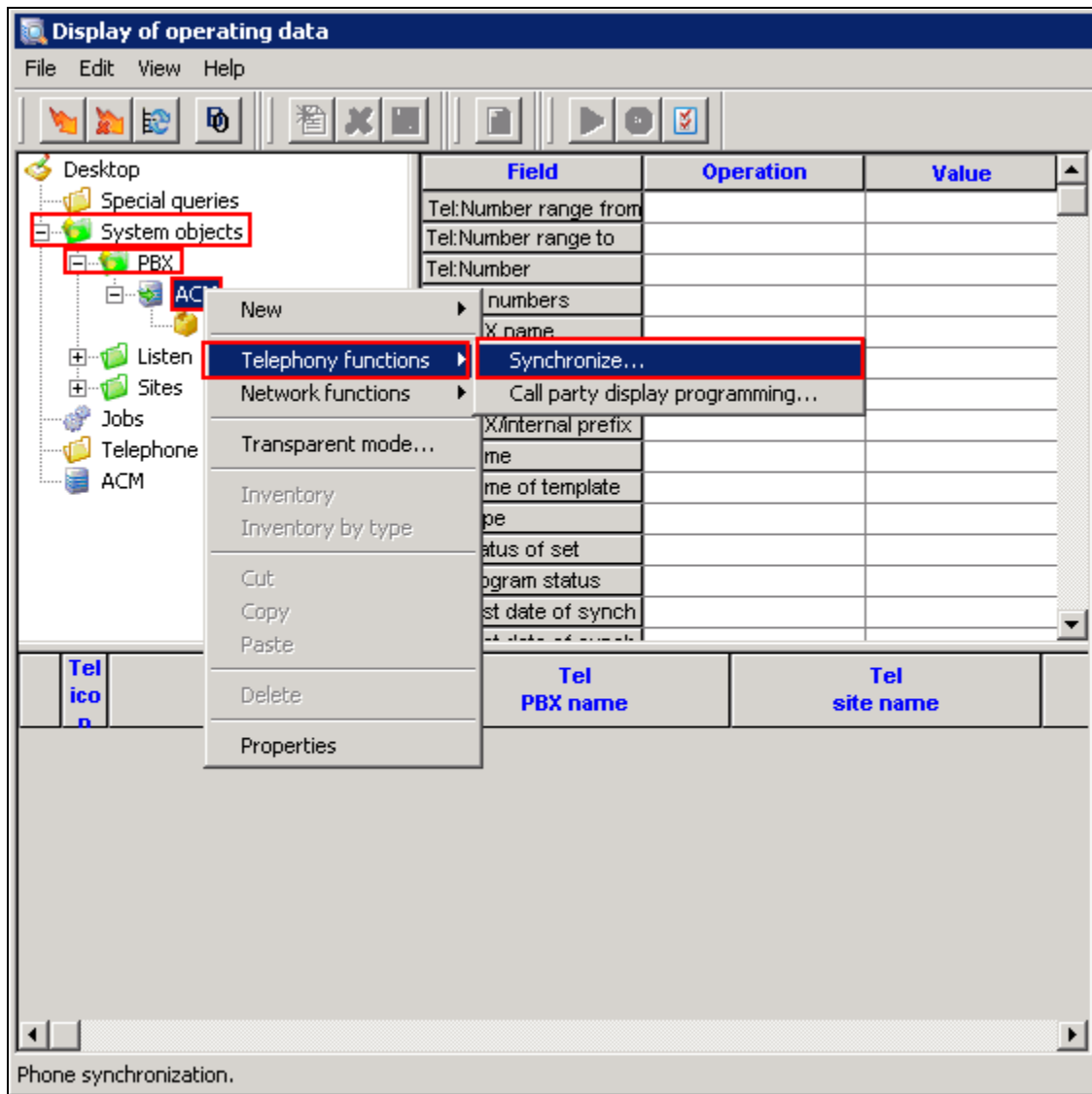
- Synchronize VDN and Vector
- Associate Attendant extension with Atras (Frox) Attendant Console
- Create a Super User for Attendant
- Configuration Atras Attendant Console
- Configure Atras Attendant Console to connect to Avaya Application Enablement Services
- Restart the Nms Attendant Console

7.1. Synchronize VDN and Vector

As part of the Atiras Attendant module configuration, the VDN and Vector must first be Synchronized. Navigate to **Start → All Programs → Atiras → atiras** (not shown) and log in with the appropriate credentials. Once the **Atiras Desktop** opens, click on the **Programs → Display of operating data**.



Once the **Display of operating data** window opens, navigate to **System objects** → **ACM** and select **Telephony functions** → **Synchronize**.



Once the **Synchronization wizard Selection** window opens, click the **VDN** and **Vector** check boxes followed by the **Next** button.

Synchronization wizard Selection - ACM

Select	Type	Description
<input type="checkbox"/>	AbbreviatedDialingGroup	Abbreviated Dialing Group
<input type="checkbox"/>	AbbreviatedDialingPersonal	Abbreviated Dialing Personal
<input type="checkbox"/>	AliasStation	Alias Station
<input type="checkbox"/>	Cabinet	Cabinet
<input type="checkbox"/>	CoveragePath	Coverage Path
<input type="checkbox"/>	CoverageAnswerGroup	Coverage Answer Group
<input type="checkbox"/>	HuntGroup	Hunt Group
<input type="checkbox"/>	PickUpGroup	Pickup Group
<input type="checkbox"/>	MediaGateway	Media Gateway
<input type="checkbox"/>	NodeNames	Node Names
<input type="checkbox"/>	SiteData	Site Data
<input checked="" type="checkbox"/>	VDN	Virtual Dial Number(VDN)
<input checked="" type="checkbox"/>	Vector	Vector
<input type="checkbox"/>	1408	Telephone set
<input type="checkbox"/>	1416	Telephone set
<input type="checkbox"/>	1603	Telephone set
<input type="checkbox"/>	1608	Telephone set
<input type="checkbox"/>	1616	Telephone set
<input type="checkbox"/>	16CC	Telephone set
<input type="checkbox"/>	2410	Telephone set
<input type="checkbox"/>	2420	Telephone set
<input type="checkbox"/>	2500	Telephone set
<input type="checkbox"/>	4620	Telephone set

☐ Only synchronize new objects

All telephone sets
All other objects
Accounts

< Back **Next >** Cancel Help

Ready

Once the **Synchronization wizard - Job - ACM** window opens, click on the **Immediate execution** radio button followed by the **Finish** button.


The screenshot shows a window titled "Synchronization wizard - Job - ACM". It contains two main sections: "Execution type" and "Batch execution".

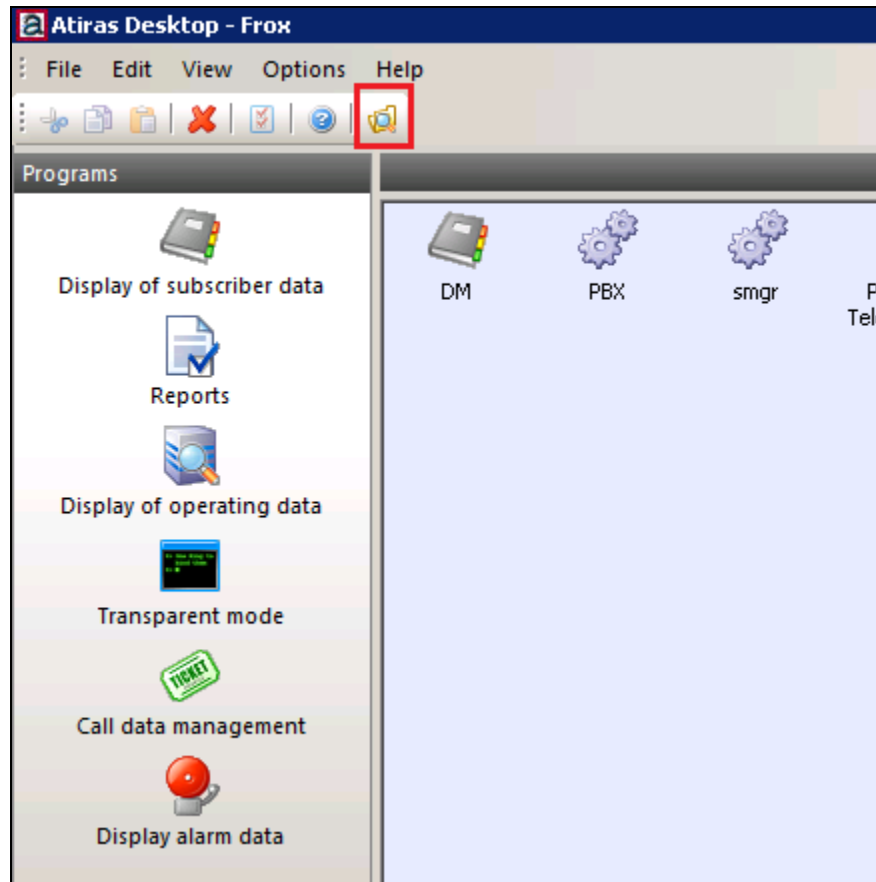
In the "Execution type" section, there are two radio buttons: "Immediate execution" (which is selected and highlighted with a red box) and "Batch execution".

The "Batch execution" section is also visible, showing options for "once" and "repeated" execution. The "once" option is selected. The "Batch execution" section includes fields for "on:" (17/01/2013), "at:" (09:24:00), "for the first time on:" (17/01/2013), "at:" (09:24:00), and "Repeat interval:" (0 00:00:00 [T HH:MM:SS]).

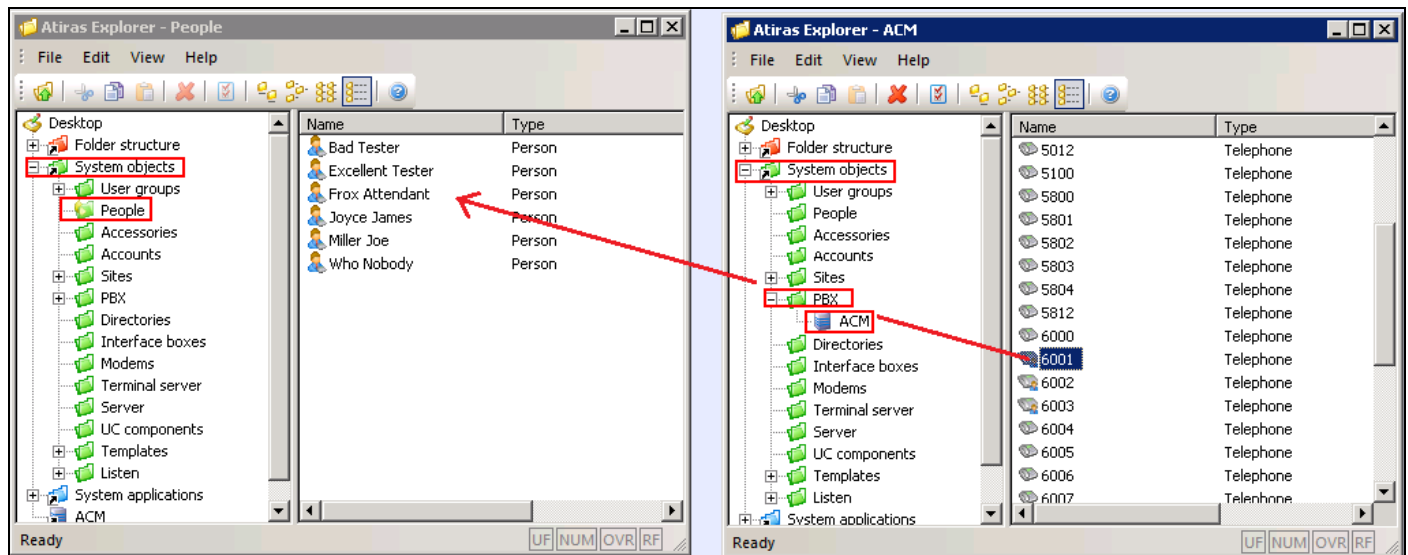
At the bottom of the window, there are four buttons: "< Back", "Finish" (highlighted with a red box), "Cancel", and "Help".

7.2. Associate Attendant extension with Atiras (Frox) Attendant Console

On the **Atiras Desktop**, click on the **Explorer** icon  two times to open two explorer windows.



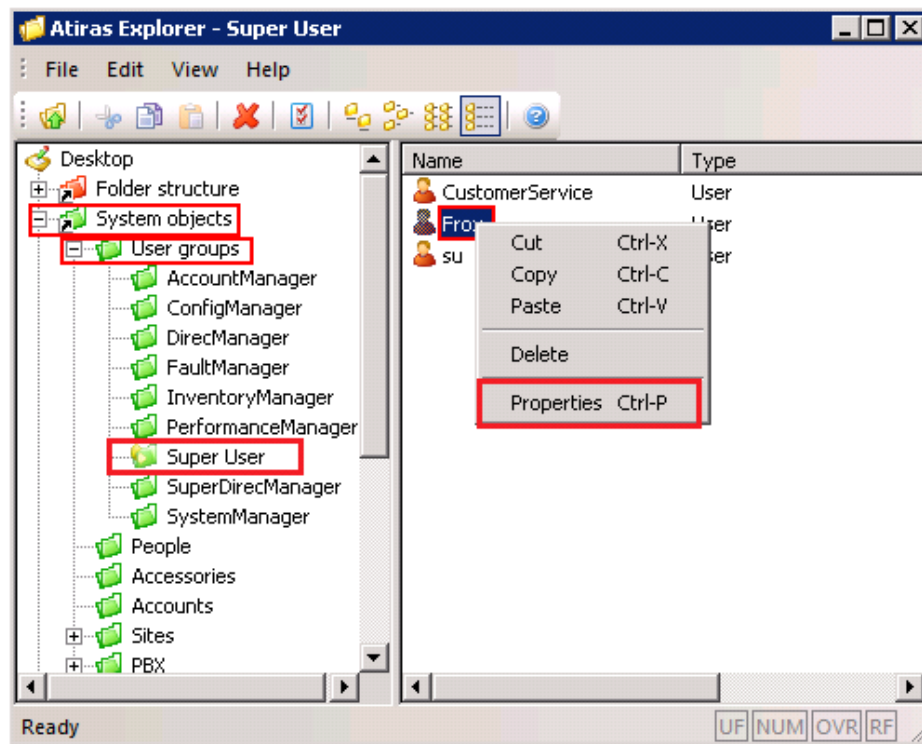
In the first window, navigate to **System objects** → **People**. In the second window, navigate to **System objects** → **PBX** → **ACM**. Drag the extension used for the Attendant console (During compliance testing extension 6001 was used) from the **Atiras Explorer ACM** window to **Frox Attendant** in the **Atiras Explorer People** window.



7.3. Create a Super User for the Attendant

Navigate to **System objects** → **User groups** → **Super User**, right-click on Frox and select **Properties**.

Note: During compliance testing, a **Super User** was used, a **DirectManager** user may also be used.



Once the **User** window opens, select the **Settings** tab and click on the **Select** button.

The screenshot shows a dialog box titled "User - Frox" with three tabs: "Settings", "References", and "Information". The "Settings" tab is selected and highlighted with a red box. The dialog contains several fields and buttons:

- User name:** Text field containing "Frox".
- User group:** Dropdown menu showing "Super User".
- Person:** Text field (empty) and a **Select...** button (highlighted with a red box).
- Language:** Dropdown menu showing "English".
- Startup interface:** Section containing a dropdown menu showing "System Startup Oberfläche" and a **Remove all...** button.
- Applications to be started:** A large empty text area.
- Password:** Section containing a **Validity period:** text field with "90" and "Days", and a **Password:** text field.
- Authorized to log in:** Section containing **from:** and **until:** dropdown menus.
- ☐ **Manage his own favorites**

At the bottom of the dialog are four buttons: **Ok**, **Cancel**, **Apply**, and **Help**. The status bar at the bottom left shows "Ready".

Once the **Select Person** window opens, click on the **Find** button and select **Frox Attendant** followed by the **OK** button.

The 'Select person' dialog box contains the following elements:

- Filter type:** Name (dropdown)
- Filter:** (text input)
- PBX:** (dropdown)
- People:** All (dropdown)
- Find** button (highlighted with a red box)
- Select person:** (label)
- Table:**

Name	Surname	First name	End User:User ID	End User:Last Name	End User:First Name
Bad Tester	Bad	Tester			
Excellent Tester	Excellent	Tester			
▶ Frox Attendant	Frox	Attendant			
Joyce James	Joyce	James			
Miller Joe	Miller	Joe			
Who Nobody	Who	Nobody			

At the bottom of the dialog box are the following buttons:

- New...
- Edit...
- OK (highlighted with a red box)
- Cancel

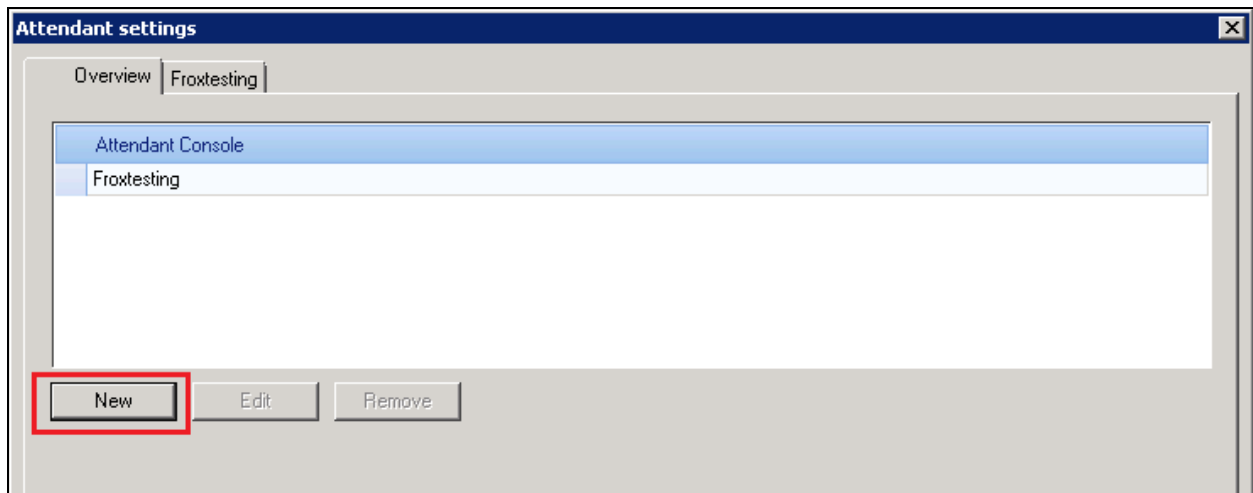
Ready

7.4. Configuration Atiras Attendant Console

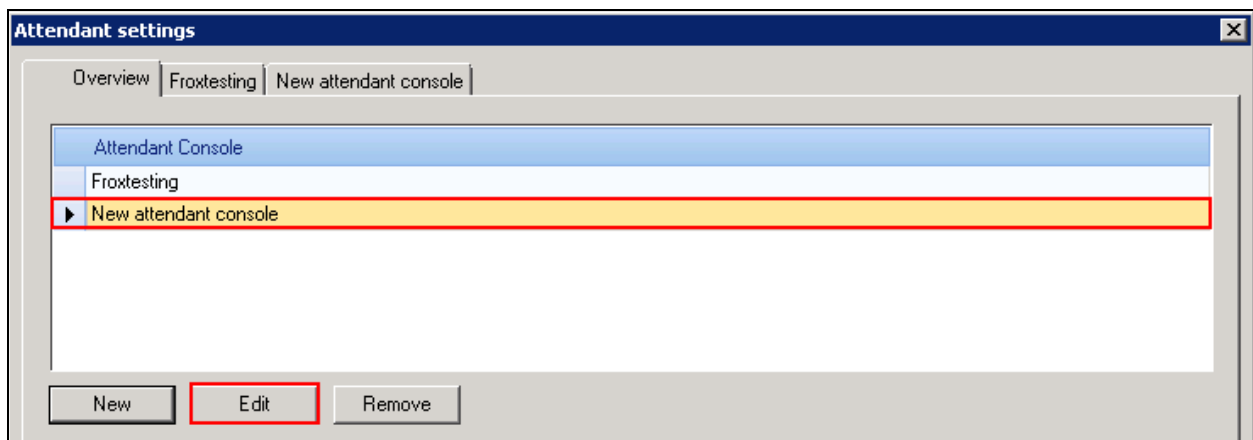
From the **Atiras Desktop** window, select **Configuration**



Once the **Attendant settings** window opens, select **New**.



After clicking the **New** button, a **New attendant console** appears in the **Attendant Console** window, click on the **Edit** button.



When the next window opens, enter an informative name (i.e. Frox) in the **Name** box. Select **ACM** and click on left arrow (<<) to move it into **Participating PBXs**. Click on the **New** button.

The image shows a software window titled "Attendant settings" with a close button (X) in the top right corner. The window has a tabbed interface with three tabs: "Overview", "Froxtesting", and "Frox" (which is currently selected and has a red 'X' icon next to it). Below the tabs, there is a "Name:" label followed by a text box containing "Frox", which is highlighted with a red rectangle. To the right of the text box is an "Active" checkbox, which is currently unchecked. Below the "Name" field is a large empty rectangular area. Underneath this area are three buttons: "New" (highlighted with a red rectangle), "Edit", and "Remove". To the right of these buttons is a "Public holidays..." button. Below the buttons, there are several input fields for queue settings: "Time before transition to next priority level:" with a value of "10", "Recall after:" with a value of "30", and "The call is considered to be" with a value of "30". Below these are "Call on hold" settings: "Threshold 1 (t1)" with a value of "20" and "Threshold 2 (t2)" with a value of "40". Below the thresholds is a section for "Text messages for notifications:" with a table that has columns for "No.", "German", "French", "Italian", and "English". Below the table are "New", "Edit", and "Remove" buttons. In the center of the window, there is a section titled "Participating PBXs" with two lists. The left list is titled "Pbx" and is empty. The right list contains the text "ACM", which is highlighted with a red rectangle. Between the two lists are two arrow buttons: "<<" (highlighted with a red rectangle) and ">>". At the bottom of the window are four buttons: "Ok", "Cancel", "Apply", and "Help". The status bar at the very bottom of the window displays the word "Ready".

Once the **New main number** windows opens, select **6666 'Atirasattendant' (ACM)** (configured in **Section 5.6**) Select **Frox Attendant** and click on left arrow (<<) to move it into **Select attendant** pane Click on the **OK** button.

New main number

Main number: 6666 'Atirasattendant' (ACM)

Name: Frox

Select attendant:

Attendant	Phone set	Group

<< >>

Frox Attendant
Bad Tester
Excellent Tester
Frox Attendant
Joyce James
Miller Joe
Who Nobody

Business hours:

WT	von	Ziel	bis	Mittagsziel	von	Ziel	bis	Nachtziel
Mon	08:00		12:00		13:30		17:00	
Tu...	08:00		12:00		13:30		17:00	
Wed	08:00		12:00		13:30		17:00	
Th...	08:00		12:00		13:30		17:00	
Fri	08:00		12:00		13:30		17:00	
Sat	08:00		12:00		13:30		17:00	
Sun	08:00		12:00		13:30		17:00	

Queue:

Priority: 3

Maximum cumulative priority: 3

Overflow: 2 Calls

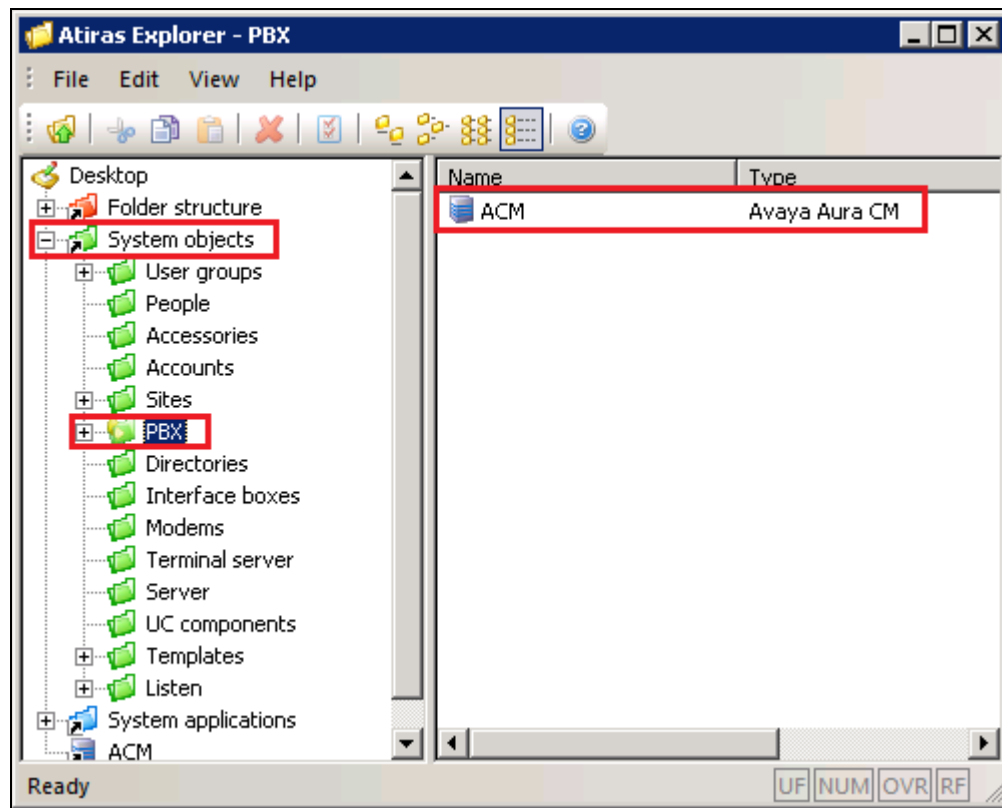
Welcome text:

OK Cancel Accept

Ready

7.5. Configure Atriras Attendant Console to connect to Avaya Application Enablement Services

To configure Atriras Attendant to connect to Avaya Application Enablement Services, navigate to **System objects** → **PBX**. Right-click on **ACM** and select **Properties** (not shown).



Once the **Avaya Aura CM** window opens, select the **Telephony** tab and enter the following:

- **Switch Connect Name:** Enter the Communication Manager as configured in **Section 6.3 (CM62)**
- **DMCC server port:** Enter the DMCC port as configured in **Section 6.6 (4721)**

Click on the **User name / Password...** button.

The screenshot shows the 'Avaya Aura CM - ACM' window with the 'Telephony' tab selected. The 'CTI settings on AES' section contains the following fields:

- 'CTI application user:' with a button labeled 'User name / Password...'.
- 'Switch Connection Name:' with the value 'CM62'.
- 'DMCC server port (unencrypted):' with the value '4721'.
- 'AES Protocol Version:' with a dropdown menu showing '6.1'.
- 'CDR Account Code Access Code (for Charge):' with the value '*43'.

Once the **User name/password** window opens, enter the following:

- **Enter user name:** Enter the CTI User as configured in **Section 6.5 (ctiuser)**
- **Enter new password:** Enter the CTI user password as configured in **Section 6.5**
- **Confirm new password** Confirm the password

Click on the **OK** button.

The screenshot shows the 'User name/password' dialog box with the following fields:

- 'Enter user name:' with the value 'ctiuser'.
- 'Enter new password:' with a masked password 'xxxxxxxx'.
- 'Confirm new password:' with a masked password 'xxxxxxxx'.

At the bottom, there are three buttons: 'OK', 'Cancel', and 'Help'. The 'OK' button is highlighted with a red border.

Click the **Ok** button

The image shows a screenshot of the 'Avaya Aura CM - ACM' configuration window. The window has a title bar with the text 'Avaya Aura CM - ACM' and a close button. Below the title bar is a tabbed interface with tabs for 'Settings', 'Network', 'Other Settings', 'Configuration', 'System Data', and 'Gateways'. The 'Settings' tab is selected, and within it, the 'Telephony' sub-tab is active. The main content area is divided into sections. The first section is titled 'CTI settings on AES' and contains four fields: 'CTI application user:' with a button labeled 'User name / Password...', 'Switch Connection Name:' with a text box containing 'CM62', 'DMCC server port (unencrypted):' with a text box containing '4721', and 'AES Protocol Version:' with a dropdown menu showing '6.1'. Below this section is a field for 'CDR Account Code Access Code (for Charge):' with a text box containing '*43'. At the bottom of the window is a status bar that says 'Ready'. In the bottom right corner, there are four buttons: 'Ok', 'Cancel', 'Apply', and 'Help'. The 'Ok' button is highlighted with a red rectangular border.

Avaya Aura CM - ACM

Settings | Network | Other Settings | Configuration | System Data | Gateways

Telephony | Site | References | Information

CTI settings on AES

CTI application user: User name / Password...

Switch Connection Name: CM62

DMCC server port (unencrypted): 4721

AES Protocol Version: 6.1

CDR Account Code Access Code (for Charge): *43

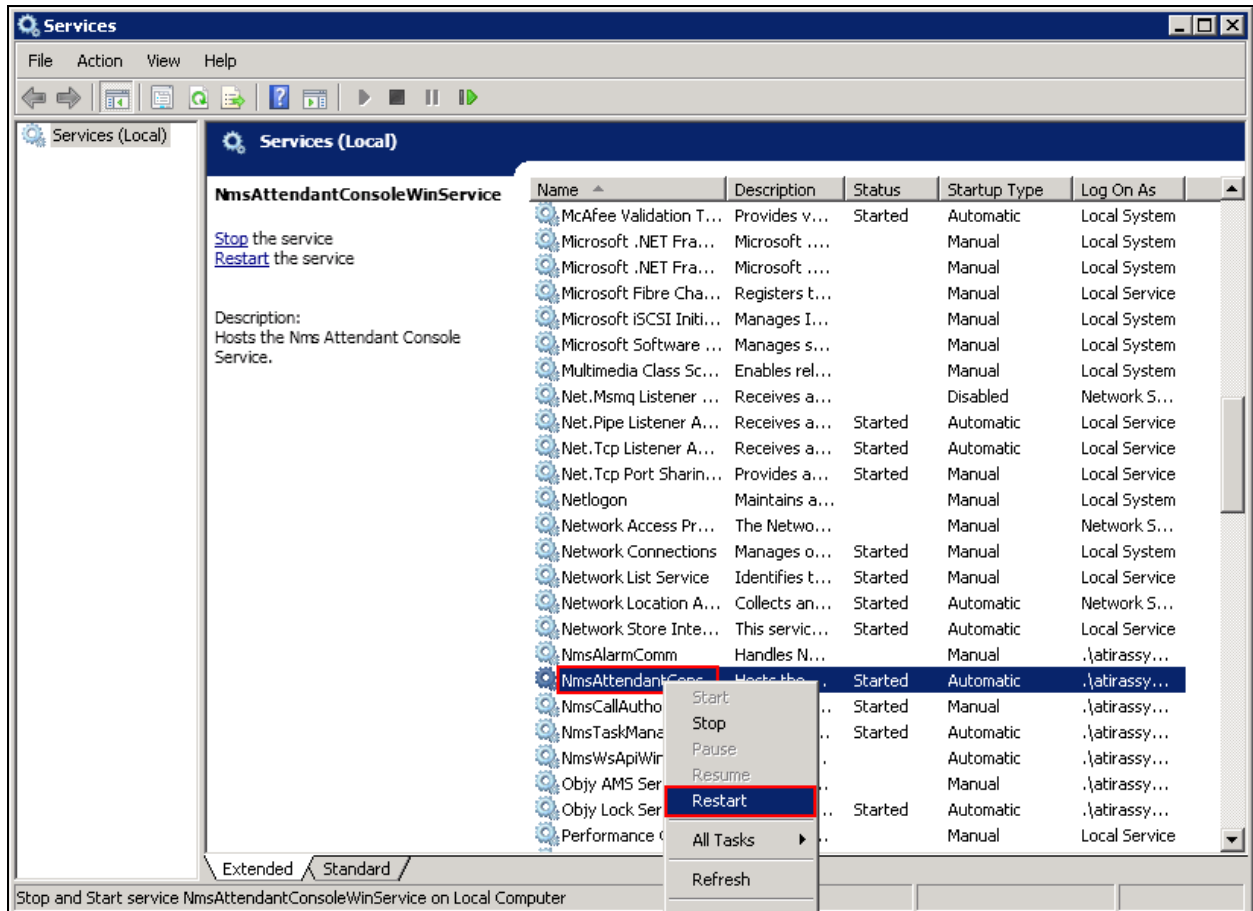
Ready

Ok Cancel Apply Help

7.6. Restart the Nms Attendant Console

Once the Atriras Attendant is configured, the Nms Attendant Console must be restarted. To restart the Nms Attendant Console, go to **Start → Run** and enter **services.msc**. Once the services window opens, right click on **Nms Attendant Console** and select **Restart**.

Note: The **Startup** type for **Nms Attendant Console** should be set to **Automatic**.



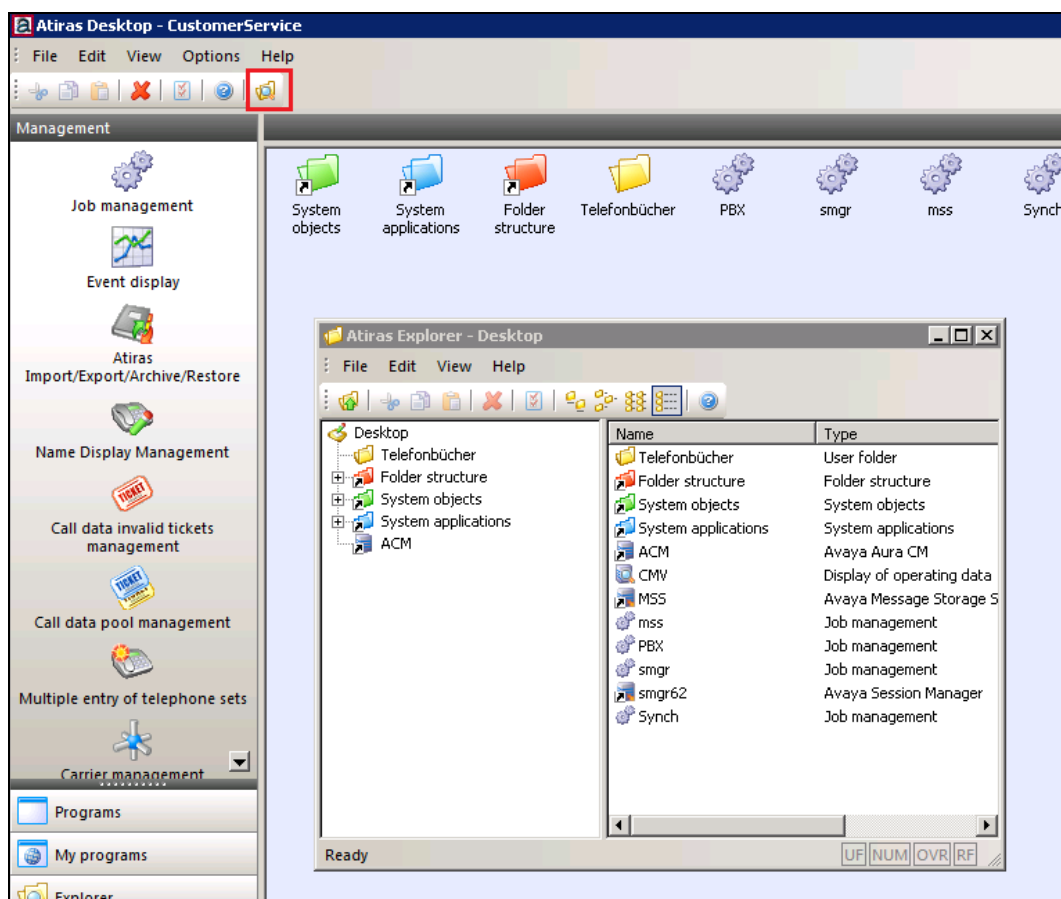
8. Configuration Atiras Configuration module

This section describes the steps performed to configure the Atiras Configuration module. It is implied that the Atiras Configuration module software is already installed and licensed. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section 10**. The configuration operations described in this section can be summarized as follows:

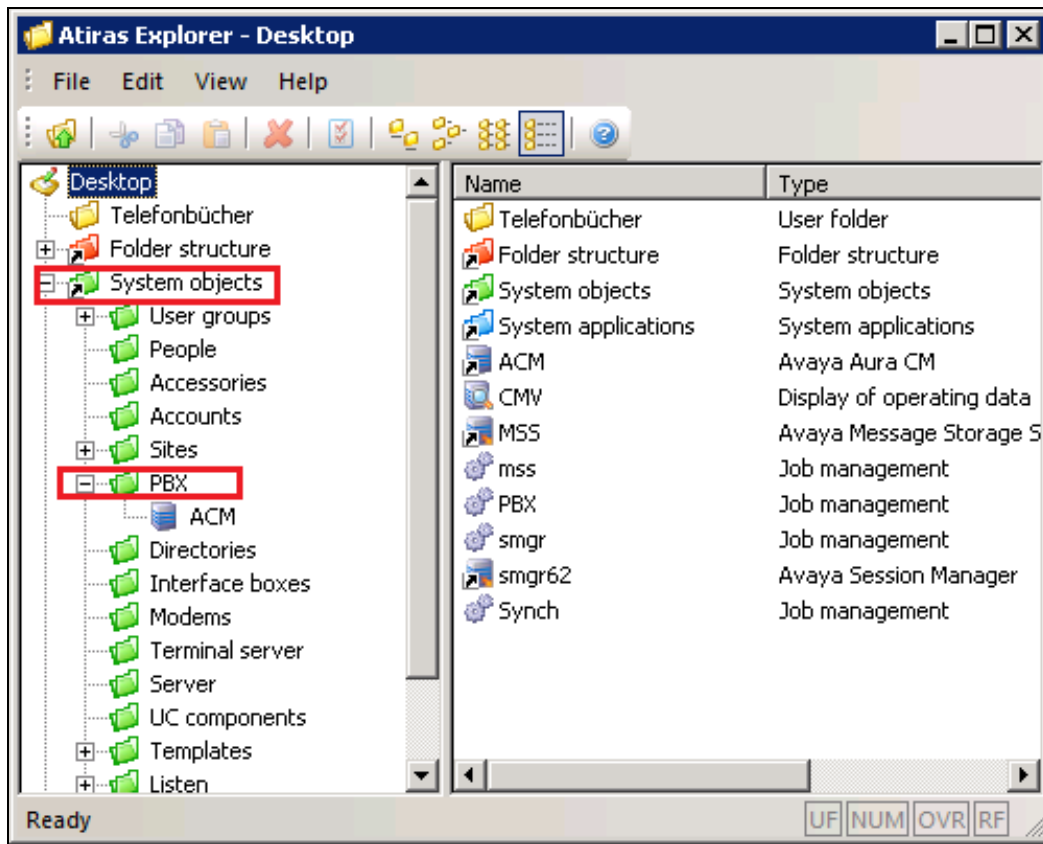
- Configure Communication Manager
- Synchronize Telephony functions
- Configure Session Manager
- Synchronize Session Manager
- Configure Atiras for Avaya Message Storage Server
- Synchronize Avaya Message Storage Server

8.1. Configure Avaya Aura Communication Manager

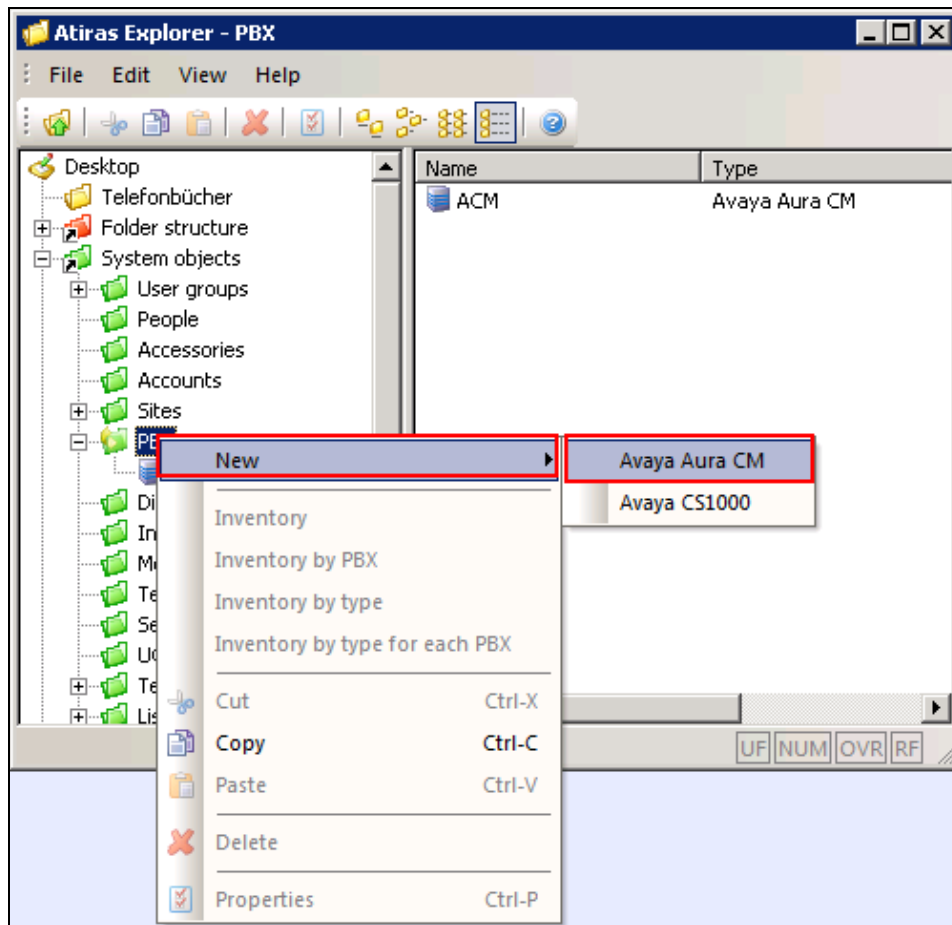
Navigate to **Start → All Programs → Atiras → atiras** (not shown) and log in with the appropriate credentials. Once the **Atiras Desktop** opens click on the **Explorer** icon .



When the **Atiras Explorer** window opens, navigate to **System objects**→ **PBX**.



Right-click on **PBX** and select **New → Avaya Aura CM**.



Once the **Avaya Aura CM** window opens click on the Settings tab and enter the following;

- **Name** Enter a informative name for Communication Manager (i.e. ACM)
- **Name of the ACM within System Manager** Enter **CM62** as was created in **Section 6.3**
- Click the **Switch on CM** check box
- **ACM** Enter the IP address of Communication Manager (10.10.16.142)
- **AES** Enter the IP address of AES (10.10.16.96)

Click on the **User name / Password** button

The screenshot shows the 'Avaya Aura CM - ACM' configuration window. The 'Settings' tab is active. The following fields and controls are highlighted with red boxes:

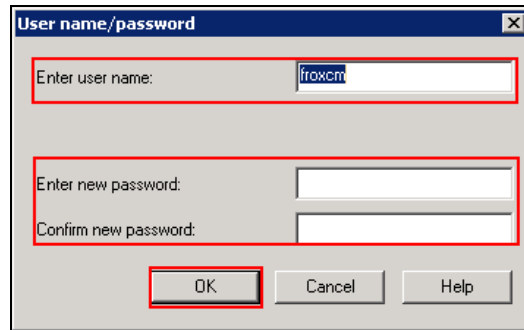
- Category:** Avaya Aura CM (dropdown)
- Name:** ACM
- Name of the ACM within System Manager:** CM62
- Switch on CM:** ☒
- Switch on AM:** ☐
- IP addresses/host names:**
 - ACM:** 10.10.16.142
 - AES:** 10.10.16.96
 - CMM:** (empty)
 - SES:** (empty)
 - Utility Server:** (empty)
 - VSP:** (empty)
- User name / Password...** (button)
- MIB description file (separate files with ;):** G3-AVAYA-MIB.ini
- MIB description management...** (button)
- AES Version:** 6.1 (dropdown)
- Synchronized ACM version:** R016x.02.0.823.0

At the bottom, there are buttons for 'Ok', 'Cancel', 'Apply', and 'Help'. The status bar at the bottom left shows 'Ready'.

In the **User name/Password** window enter the following:

- **Enter user name** Enter user ID required to log in to Communication Manager
- **Enter new password** Enter the user password required to log in to the Communication Manager
- **Confirm new password** Confirm the password

Click on the **OK** button



The screenshot shows a standard Windows-style dialog box titled "User name/password". It has a close button (X) in the top right corner. The dialog contains three input fields. The first field is labeled "Enter user name:" and contains the text "froxcm". The second field is labeled "Enter new password:" and is empty. The third field is labeled "Confirm new password:" and is empty. At the bottom of the dialog, there are three buttons: "OK", "Cancel", and "Help". The "OK" button is highlighted with a red rectangular box.

Click on the **OK** button.

Avaya Aura CM - ACM

Telephony	Site	References	Information
Settings	Network	Other Settings	Configuration
			System Data
			Gateways

Category: Avaya Aura CM

Name: ACM

Name of the ACM within System Manager: CM62

☒ Switch on CM

☐ Switch on AM

IP addresses/host names

ACM:	10.10.16.142	User name / Password...
AES:	10.10.16.96	
CMM:		
SES:		
Utility Server:		
VSP:		

MIB description file (separate files with ;): G3-AVAYA-MIB.ini

MIB description management...

AES Version: 6.1

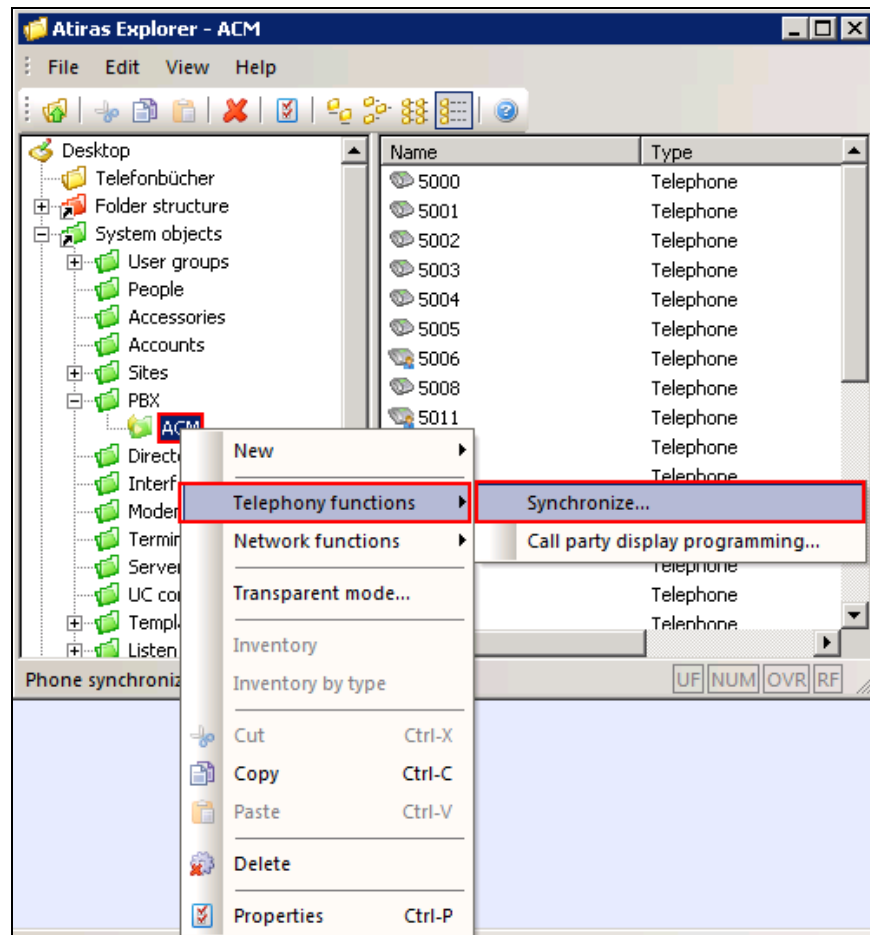
Synchronized ACM version: R016x.02.0.823.0

Ok Cancel Apply Help

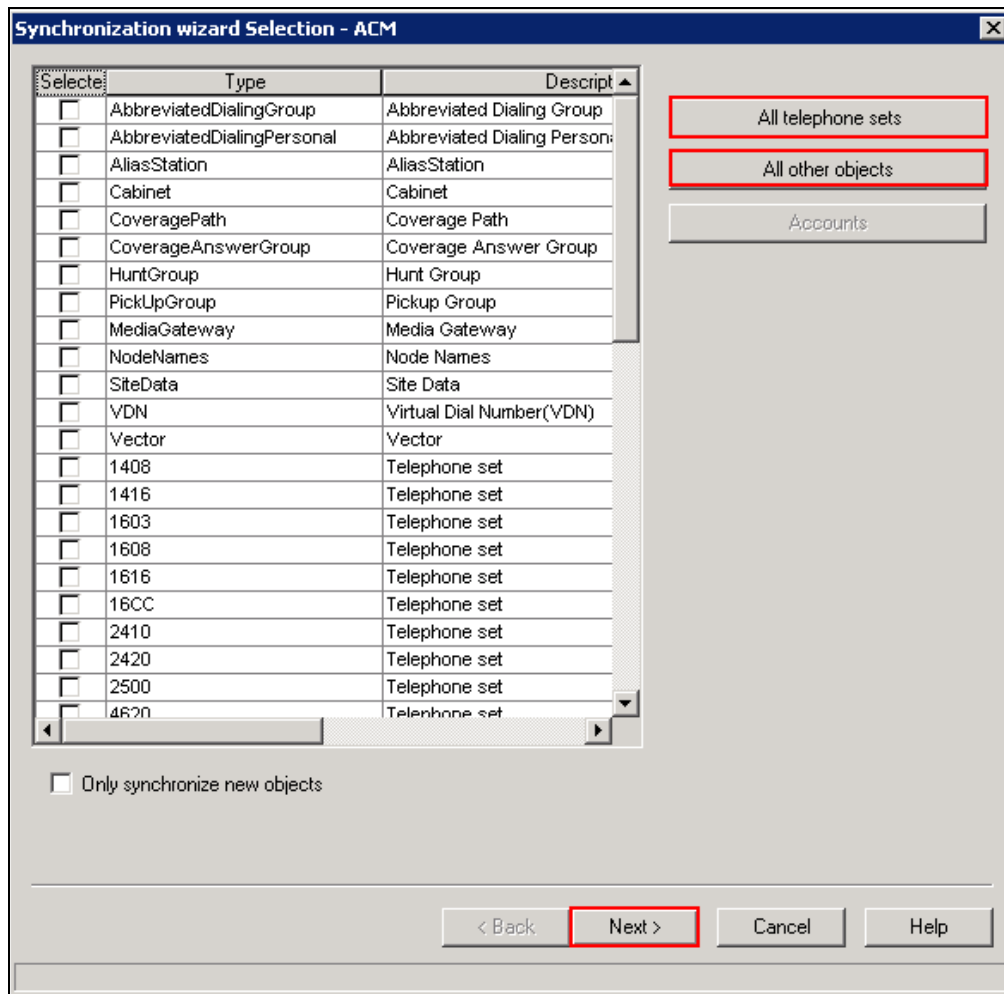
Ready

8.2. Synchronize Telephony functions

Once the Communication Manager is configured it must be synchronized. Right-click on the **ACM** just configured and select **Telephony functions** → **Synchronize**.



Once the **Synchronization wizard Selection** window open click on the **All telephone sets** and **All other objects** buttons followed by the **Next** button.



Once the **Synchronization wizard – Job- ACM** window opens, click on the **Immediate execution** radio button followed by the **Finish** button.

The screenshot shows a window titled "Synchronization wizard - Job - ACM". It contains two main sections: "Execution type" and "Batch execution".

Execution type: This section has two radio buttons. The "Immediate execution" button is selected and highlighted with a red rectangular box. The "Batch execution" button is unselected.

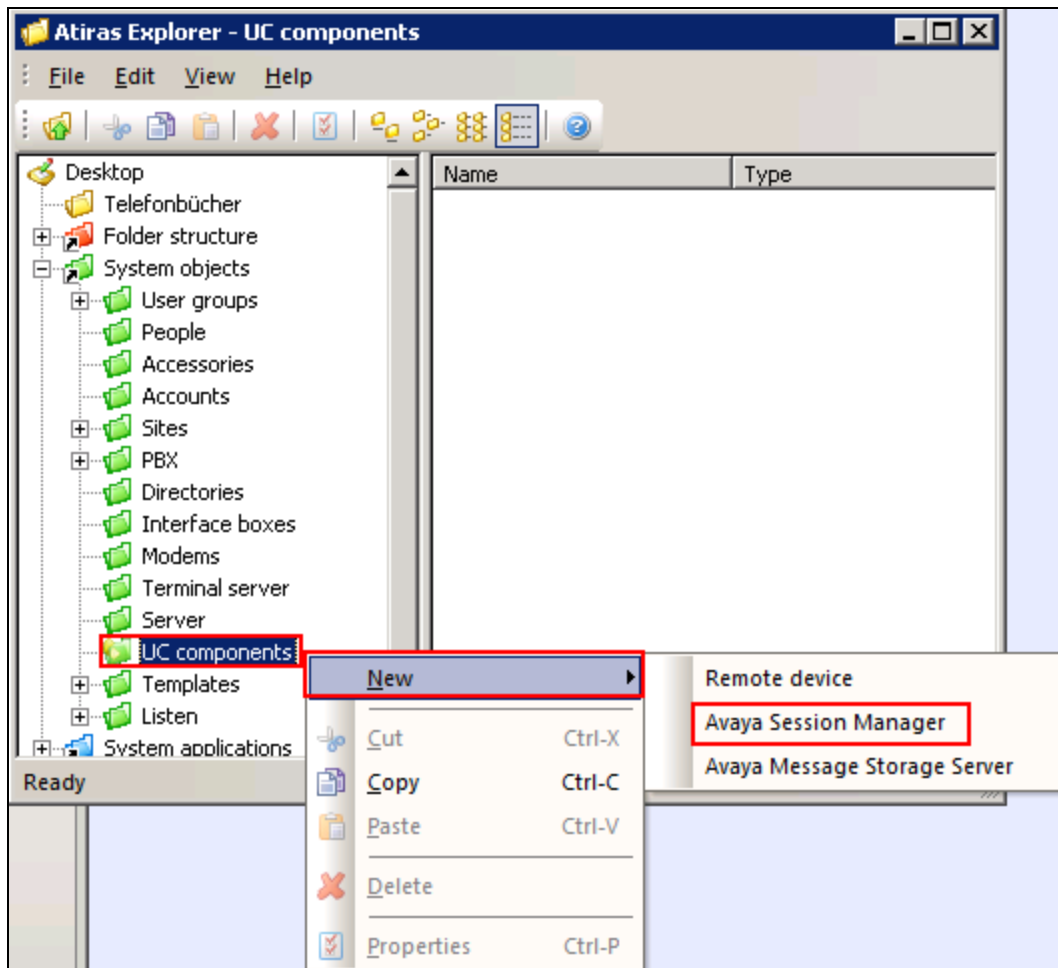
Batch execution: This section is currently disabled. It contains two radio buttons: "once" and "repeated". The "once" button is selected. To its right, there are two input fields: "on:" with the value "17/01/2013" and "at:" with the value "09:24:00". Below these, the "repeated" button is unselected. To its right, there are three input fields: "for the first time on:" with the value "17/01/2013", "at:" with the value "09:24:00", and "Repeat interval:" with the value "0 00:00:00" and a label "[T HH:MM:SS]".

At the bottom of the window, there are four buttons: "< Back", "Finish", "Cancel", and "Help". The "Finish" button is highlighted with a red rectangular box.

8.3. Configure Atriras for Avaya Session Manager

To enable SIP extension configuration by Atriras, right-click on **UC components** and select **New** → **Avaya Session Manager**.

Note: Although the SIP extensions are created on Session Manager, the configurations are done via System Manager.



Once the **Avaya Session Manager** window opens, click on the **Properties** tab and enter the following;

- **Name** Enter a informative name for System Manager (i.e. smgr62)
- **IP-Addr./Hostname:** Enter the Hostname of System Manager (i.e. smgr62.avaya.com)
- **Version:** Select **6.2** from the dropdown
- **Program:** Check the check box
- **SIP Domain Name:** Enter the Domain that System Manager resides on. (During compliance testing the Domain was Avaya.com)
- **Name of the Session-Manager in System-Manager:** Enter the Session Manager name. (During compliance testing the Session Manager name was SM62)

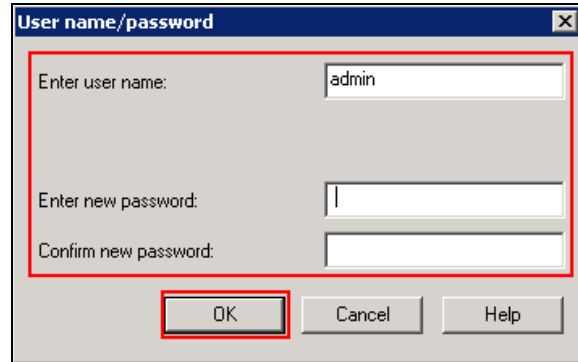
Click on the **User name / Password** button

The screenshot shows the 'Avaya Session Manager - smgr62' window with the 'Properties' tab selected. The 'Properties' tab is highlighted with a red box. Below the tabs, there are several input fields and a dropdown menu, all enclosed in a red rectangular box. These fields are: 'Name:' with the value 'smgr62', 'IP-Addr./Hostname:' with the value 'smgr62.avaya.com', 'Version:' with a dropdown menu showing '6.2', 'Program:' with a checked checkbox, 'SIP Domain Name:' with the value 'avaya.com', and 'Name of the Session-Managers in System-Manager:' with the value 'SM62'. Below these fields, there are three buttons: 'User name/password', 'SSH-Username/Password', and 'Connection test...'. The 'User name/password' button is highlighted with a red rectangular box. At the bottom of the window, there are four buttons: 'Ok', 'Cancel', 'Apply', and 'Help'.

In the **User name/Password** window enter the following:

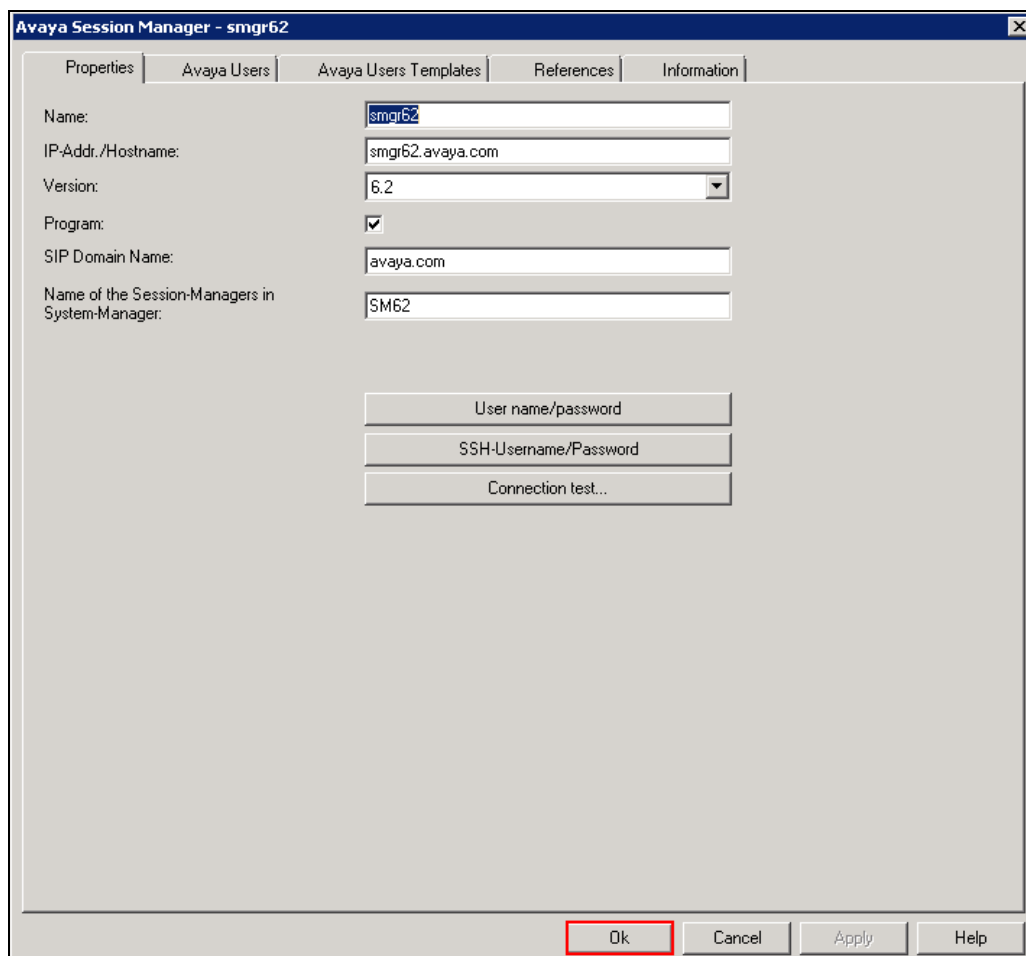
- **Enter user name** Enter an user ID required to log into System Manager
- **Enter new password** Enter the password required to log into System Manager
- **Confirm new password** Confirm the password

Click on the **OK** button



A dialog box titled "User name/password" with a close button (X) in the top right corner. It contains three input fields: "Enter user name:" with the text "admin", "Enter new password:" which is empty, and "Confirm new password:" which is empty. At the bottom, there are three buttons: "OK", "Cancel", and "Help". The "OK" button is highlighted with a red rectangle.

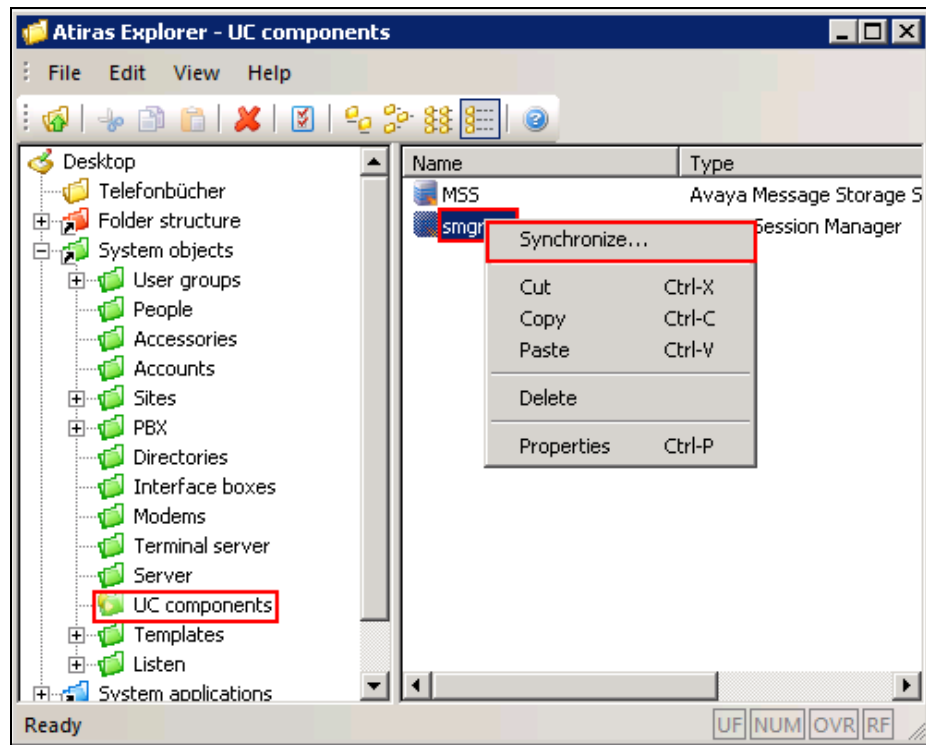
Click on the **OK** button.



A window titled "Avaya Session Manager - smgr62" with a close button (X) in the top right corner. It has a tabbed interface with tabs for "Properties", "Avaya Users", "Avaya Users Templates", "References", and "Information". The "Properties" tab is active, showing fields for "Name:" (smgr62), "IP-Addr./Hostname:" (smgr62.avaya.com), "Version:" (6.2), "Program:" (checked), "SIP Domain Name:" (avaya.com), and "Name of the Session-Managers in System-Manager:" (SM62). Below these fields are three buttons: "User name/password", "SSH-Username/Password", and "Connection test...". At the bottom of the window, there are four buttons: "Ok", "Cancel", "Apply", and "Help". The "Ok" button is highlighted with a red rectangle.

8.4. Synchronize Session Manager

Once the Avaya Session Manager is configured it must be synchronized. Right-click on Session Manager just configured (smgr62 as configured in **Section 8.3**) and select **Synchronize**.



Once the Avaya Session Manager window opens, click on the **Immediate execution** radio button followed by the **OK** button.

The screenshot shows a dialog box titled "Synchronize Avaya Session Manager". It contains two main sections: "Execution type" and "Batch execution".

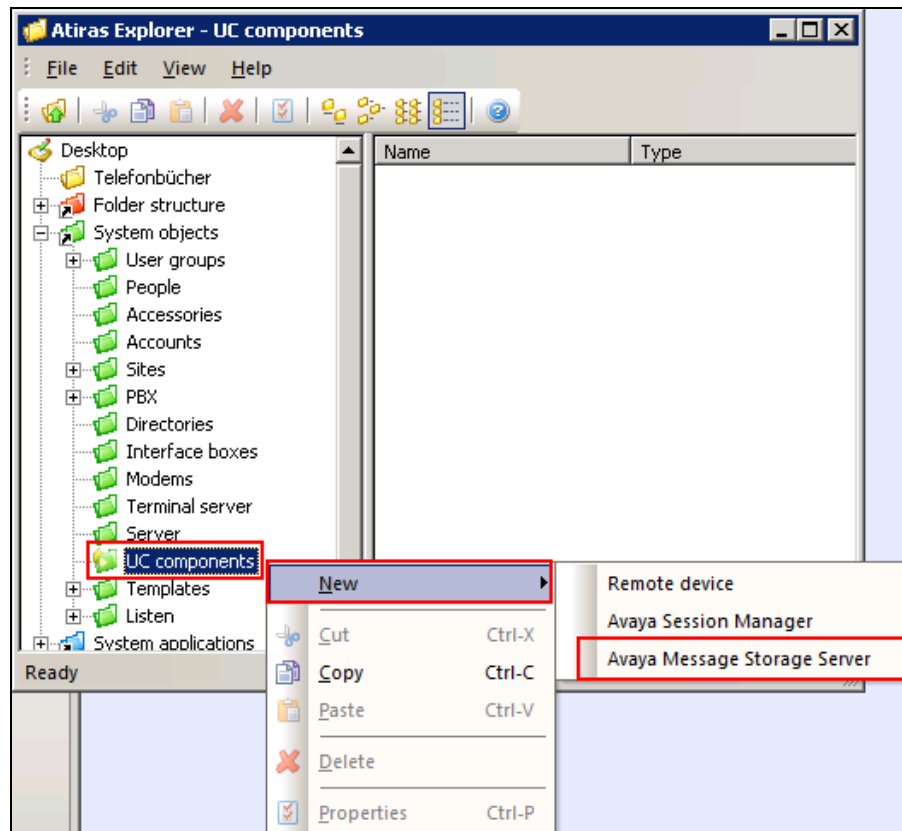
In the "Execution type" section, there are two radio buttons: "Immediate execution" (which is selected and highlighted with a red box) and "Batch execution".

The "Batch execution" section is currently inactive. It contains options for "once" and "repeated" execution. The "once" option is selected, with fields for "on:" (28/02/2013) and "at:" (08:38:19). The "repeated" option has fields for "for the first time on:" (28/02/2013), "at:" (08:38:19), and "Repeat interval:" (0 00:00:00 [T HH:MM:SS]).

At the bottom of the dialog, there are three buttons: "Ok" (highlighted with a red box), "Cancel", and "Help".

8.5. Configure Atras for Avaya Message Storage Server

To configure Atras to enable voicemail box configuration, right-click on **UC components** and select **New → Avaya Message Storage Server**.



Once the **Avaya Message Storage Server** window opens, select the **Properties** tab and enter the following;

- **Name:** Enter an informative name
- **IP address or host:** Enter the IP address of the Message Storage Server (10.10.16.25)
- **Password** Enter the password of the Message Storage Server

Click on the **OK** button.

The screenshot shows the 'Avaya Message Storage Server - MSS' window with the 'Properties' tab selected. The 'LDAP interface' section contains the following fields:

- Name:** MSS
- IP address or host:** 10.10.16.25
- Use SSL encryption:** ☐
- Port:** 389 (Example: 389 ohne SSL, 636 mit SSL)
- Subscriber basic DN:** ou=People,dc=Avaya (Example: ou=People,dc=Avaya)
- COS basic DN:** ou=COS,dc=Avaya (Example: ou=COS,dc=Avaya)
- Customer:** cn=atiras,dc=Avaya (Example: cn=AtirasServer,dc=Avaya)
- Password:** xxxxxxxx

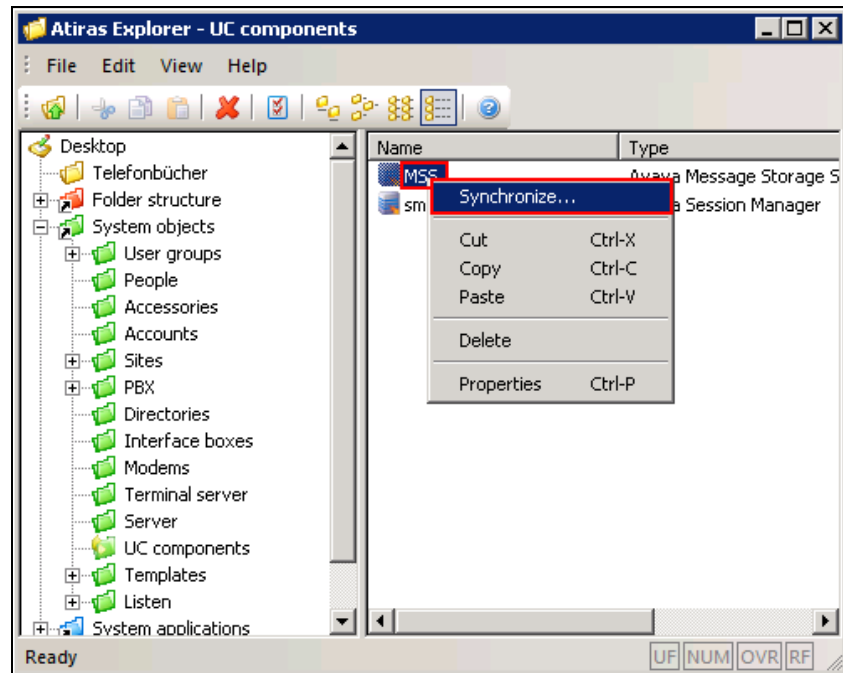
The 'Connected PBX:' section shows a table with one entry:

Name
ACM

At the bottom of the window, the 'Ok' button is highlighted.

8.6. Synchronize Avaya Message Storage Server

Once the Avaya Message Storage Server is configured it must be synchronized. Right-click on the Avaya Message Storage Server just configured (MSS as configured in **Section 8.5**) and select **Synchronize**.



Once the Avaya Message Storage Server window opens, click on the **Immediate execution** radio button followed by the **OK** button.

The screenshot shows a dialog box titled "Synchronize Avaya Message Storage Server". It contains two main sections: "Execution type" and "Batch execution".

In the "Execution type" section, there are two radio buttons: "Immediate execution" (which is selected and highlighted with a red box) and "Batch execution".

The "Batch execution" section is currently inactive. It contains options for "once" and "repeated" execution. The "once" option is selected, with fields for "on:" (27/02/2013) and "at:" (17:50:57). The "repeated" option has fields for "for the first time on:" (27/02/2013), "at:" (17:50:57), and "Repeat interval:" (0 00:00:00 [T HH:MM:SS]).

At the bottom of the dialog, there are three buttons: "Ok" (highlighted with a red box), "Cancel", and "Help".

9. Verification Steps

This section provides tests that can be performed to verify correct configuration of the Avaya and Frox Communication solution.

9.1. Verify Avaya Aura® Communication Manager CTI Service State

The following steps can ensure that the communication between Communication Manager and the Application Enablement Services server is functioning correctly. Check the AESVCS link status with Application Enablement Services by using the command **status aescvs cti-link**. The CTI link is 1. Verify the **Service State** of the CTI link is **established**.

status aescvs cti-link						
AE SERVICES CTI LINK STATUS						
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs Rcvd
1	5	no	aes1	established	15	15

9.2. Verify Avaya Aura® Application Enablement Services DMCC

The following steps are carried out on the Application Enablement Services to ensure that the communication link between Atiras and the Application Enablement Services server is functioning correctly. Verify the status of the DMCC service by selecting **Status → Status and Control → DMCC Service Summary**. The **DMCC Service Summary – Session Summary** screen is displayed as shown below. It shows a connection to **ctiuser** and the **Far-end Identifier** of **10.10.60.55** as expected.

Note: Although the TSAPI feature is used the DMCC Service is viewed.

The screenshot displays the Avaya Application Enablement Services Management Console. The left sidebar contains a navigation menu with categories like AE Services, Communication Manager Interface, Licensing, Maintenance, Networking, Security, Status, Logs, Status and Control, User Management, Utilities, and Help. The 'Status and Control' section is expanded, showing sub-items like CVLAN Service Summary, DLG Services Summary, DMCC Service Summary (highlighted), Switch Conn Summary, and TSAPI Service Summary. The main content area shows the 'DMCC Service Summary - Session Summary' page. It includes a session summary table with columns: Session ID, User, Application, Far-end Identifier, Connection Type, and # of Associated Devices. A single session is listed with Session ID 7B3C90124AAB383CF 01019128EB22080-121175, User ctiuser, Application NmsDrvDmcc, Far-end Identifier 10.10.60.55, Connection Type XML Unencrypted, and 0 associated devices. The page also shows session uptime, number of active sessions, and other statistics.

AVAYA Application Enablement Services Management Console

Welcome: User craft
Last login: Wed Feb 27 07:21:49 2013 from 10.10.60.55
Number of prior failed login attempts: 0
HostName/IP: aesserver62/10.10.16.96
Server Offer Type: TURNKEY
SW Version: r6-2-0-18-0
Server Date and Time: Thu Feb 28 08:42:19 GMT 2013

Status | Status and Control | DMCC Service Summary Home | Help | Logout

DMCC Service Summary - Session Summary

☐ Enable page refresh every 60 seconds

Session Summary [Device Summary](#)
Generated on Thu Feb 28 08:37:09 GMT 2013

Service Uptime: 42 days, 23 hours 2 minutes
Number of Active Sessions: 1
Number of Sessions Created Since Service Boot: 101
Number of Existing Devices: 0
Number of Devices Created Since Service Boot: 23

<input type="checkbox"/>	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/>	7B3C90124AAB383CF 01019128EB22080-121175	ctiuser	NmsDrvDmcc	10.10.60.55	XML Unencrypted	0

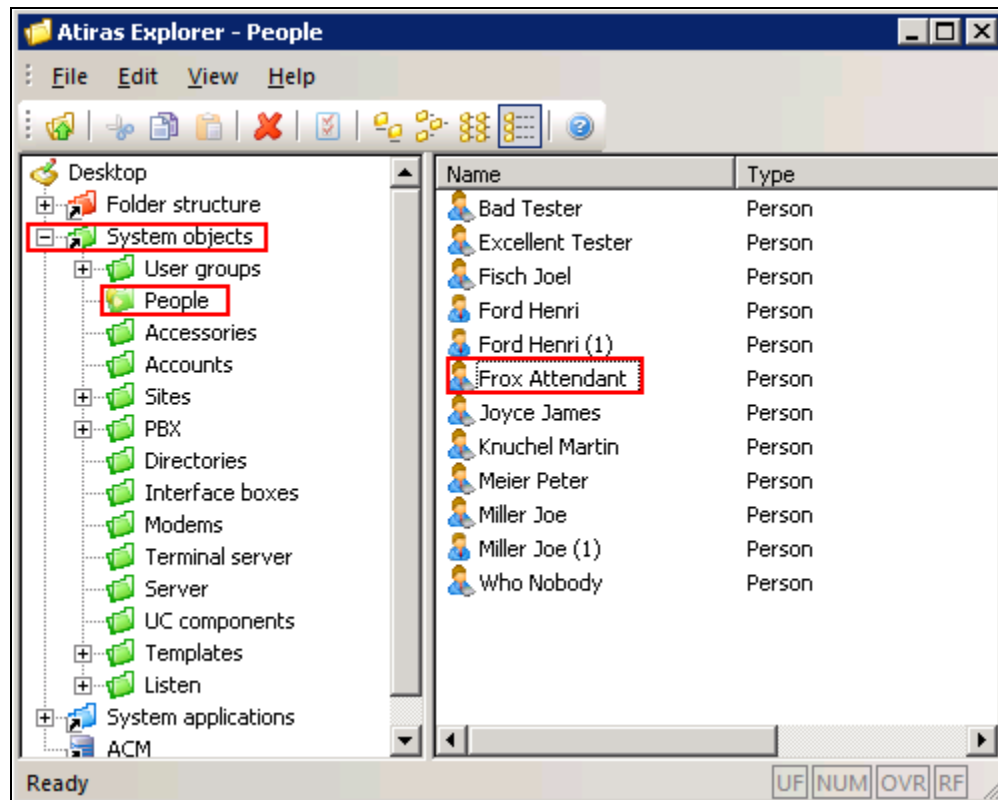
[Terminate Sessions](#) [Show Terminated Sessions](#)

Item 1-1 of 1

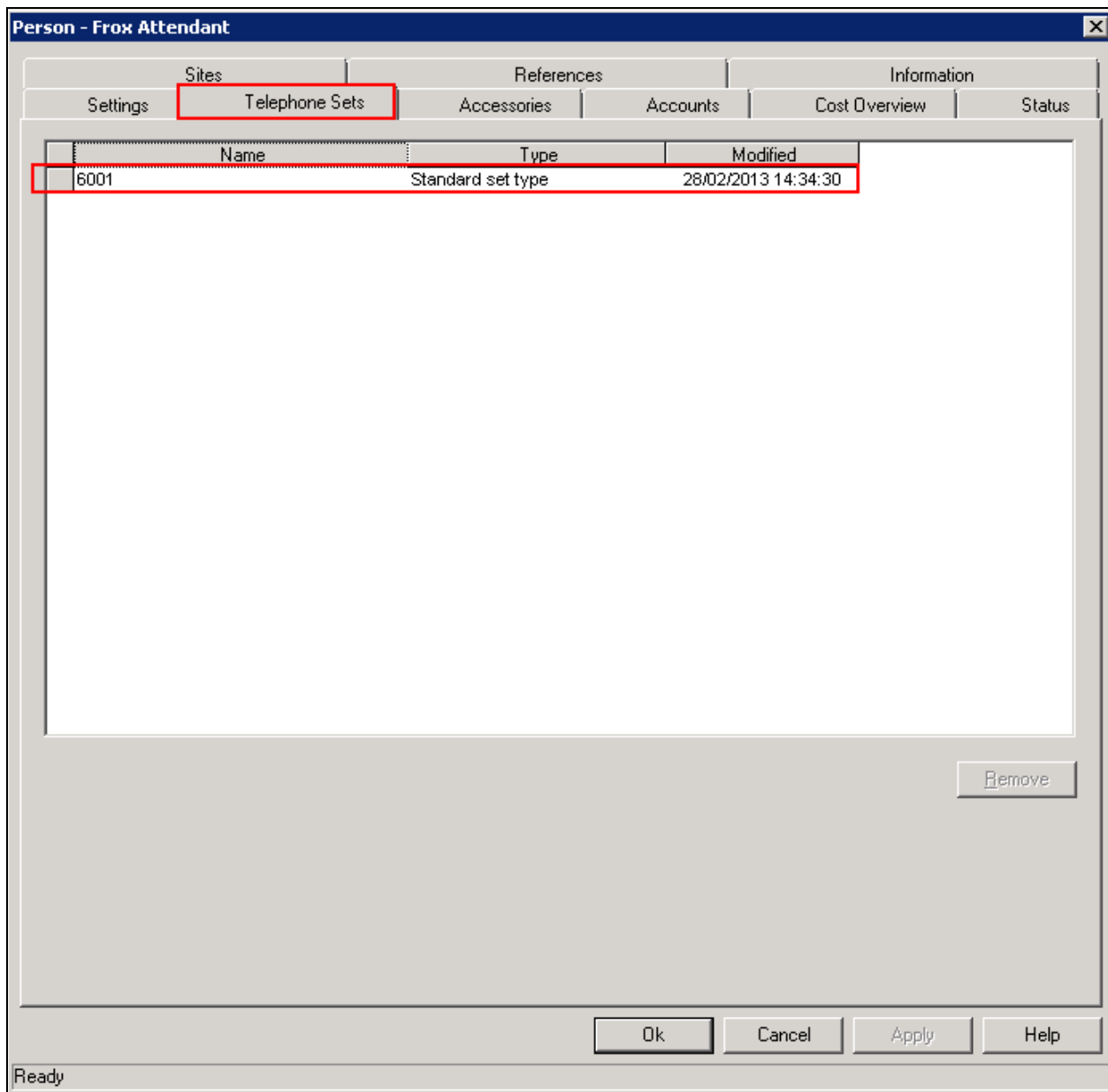
Copyright © 2009-2012 Avaya Inc. All Rights Reserved.

9.3. Verify Atiras Attendant Console Extension is Assigned to the Attendant

To verify that the Atiras Attendant Console extension is assigned to the Attendant, from the Atiras Explorer window navigate to **System objects** → **People** and right-click on the Attendant and select **properties**. (During compliance testing the Attendant was called **Frox Attendant**).

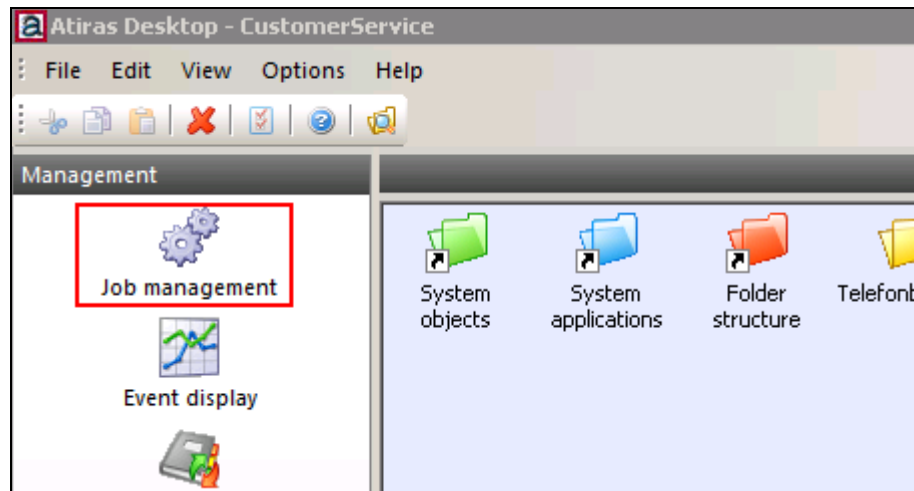


Once the **Person** window opens, select the **Telephone Sets** tab, and verify that the Atiras Attendant Console extension is assigned. (During compliance testing, the Atiras Attendant Console extension was 6001.)



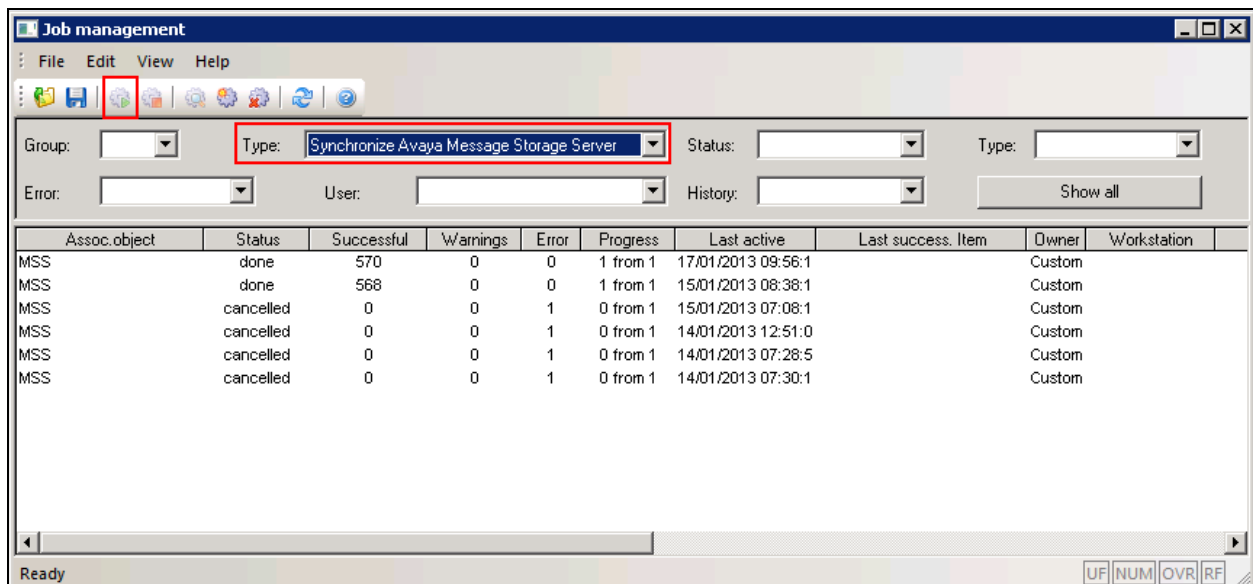
9.4. Verify Atiras Configuration Module Synchronization Status

It is possible to verify the synchronization status of the Communication Manager/Session Manager extensions and voicemail boxes between the Avaya solution and the Atiras Configuration module. Navigate to Start → All Programs → Atiras → atiras (not shown) and log in with the appropriate credentials. Once the **Atiras Desktop** opens click on the **Job management** icon on the left side of the window.



Once the **Job management** window opens, select **Synchronize Avaya Session Manager**, **Phone synchronization** or **Synchronize Avaya Message Storage Server** from the **Type** dropdown box and click on the **Start processing** icon.

Note: The screenshot below shows the **Synchronize Avaya Message Storage Server**.



10. Conclusion

A full and comprehensive set of feature functional test cases were performed during compliance testing. All test cases passed and met the objectives outlined in **Section 2.2**. Atiras 7.3 is considered compliant with Avaya Aura® Communication Manager.

11. Additional References

These documents form part of the Avaya official technical reference documentation suite. Further information may be had from <http://support.avaya.com> or from your Avaya representative.

- [1] Administering Avaya Aura® Communication Manager 03-300509 Release 6.0 Issue 6.0 June 2010*
- [2] Administering Avaya Aura® Session Manager 03-603324 Release 6.1 Issue 1.1 November 2010*
- [3] Administering Avaya Aura® System Manager Release 6.1 Issue 1.1 November 2010*
- [4] Avaya Aura® Application Enablement Services Administration and Maintenance Guide Release 6.1 Issue 2 February 2011*

Contact Frox Commutations at <http://www.frox.com/en/10052/Contact.html> for Product Documentation.

©2013 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.