Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Frox Communication Atiras 7.6 with Avaya Aura® Communication Manager 7.1 - Issue 1.0

Abstract

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

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as any observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

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

1. Introduction

These Application Notes describe the configuration steps required 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. 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.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in these DevConnect Application Notes included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with these Application Notes, the interface between Avaya systems and the Atiras did not include use of any specific encryption features as requested by FROX communication.

This solution uses the System Access Terminal (SAT) interface to interact with Avaya Aura® Communication Manager. While this solution has successfully completed Compliance Testing for the specific release levels as described in this Application Note, Avaya does not generally recommend use the SAT interface as a programmatic approach to integration of 3rd party applications. Avaya may make changes or enhancements to the SAT interface in any subsequent release, feature pack, service pack, or patch that may impact the interoperability of 3rd party applications using this SAT interface. Using the SAT interface in a programmatic manner may also result in a variety of operational issues, including performance impacts to the Avaya solution. If there are no other programmatic options available to obtain the required data or functionality, Avaya recommends that 3rd party applications only be executed during low call volume periods, and that real time delays be inserted between each command execution. NOTE: The scope of the compliance testing activities reflected in this Application Note explicitly did not include load or performance evaluation criteria, and no guarantees or assurances are made by Avaya that the 3rd party application has implemented these recommendations. The vendor of the 3rd party application using this interface remains solely responsible for verifying interoperability with all later Communication Manager releases, including feature packs, service packs, and patches as issued by Avaya. For additional details see Avaya Product Support Notices PSN002884u, PSN005085u, and PSN020295u, available at www.avaya.com/support.

2.1. Interoperability Compliance Testing

Feature functionality testing included:
Atiras Attendant Console module

- Inbound calls
- Outbound Calls
- Calls using telephone book
- Supervised and Unsupervised transfers

Atiras Configuration module

- Verify synchronization between Atiras and Communication Manager
- Verify synchronization between Atiras and System Manager for Session Manager's user settings.
- Add/Change/Delete Analog/Digital/IP stations (H323 and SIP)
- 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 ensure full interoperability between Atiras and the Communication Manager. The tests were all functional in nature and performance testing was not included. The following were the observations made:

1. Header name for Session Manager Access is inappropriate since System Manager is used for management of Session Manager.
2. Name of set for Station property is not correct station name.
3. Enhanced Callr-Info Display for 1-Line Phone feature is missing from station feature tab.
4. Call Pickup group name if it is blank or changed was not pickup even after it is synchronized.

2.3. Support

Technical support for Frox Communications products can be found as follows:
http://www.frox.ch/support/

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 Aura® Application Enablement Services, Avaya Aura® Media Server and a G430 Media Gateway. The Atiras 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 9641G (H.323) was used as the Attendant station. Inbound and outbound calls to/from the PSTN were made via a simulated PSTN. Avaya 9608 (H323), 9641 (SIP) and 9408 Digital Deskphones were used as endpoints during compliance testing.

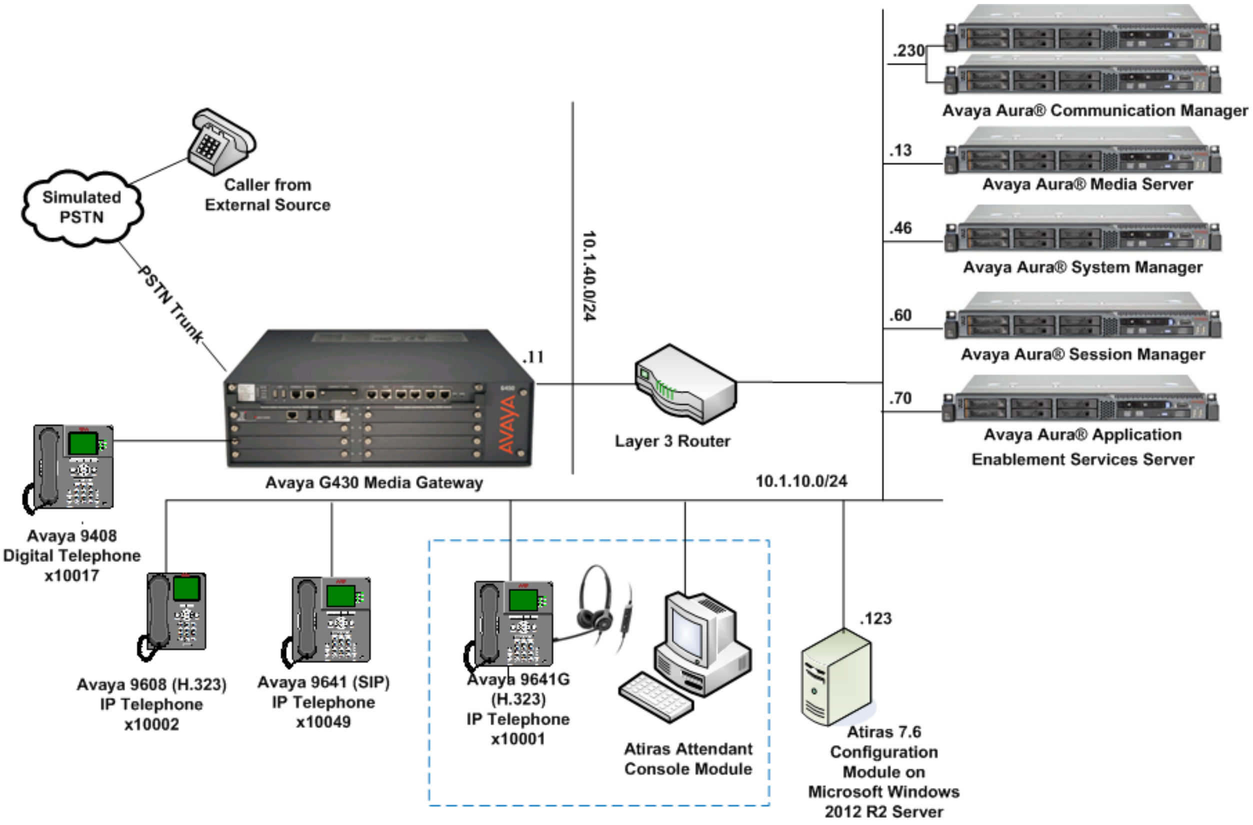

.230
Avaya Aura® Communication Manager
.13
Avaya Aura® Media Server
.46
Avaya Aura® System Manager
.60
Avaya Aura® Session Manager
.70
Avaya Aura® Application Enablement Services Server
Simulated PSTN
Caller from External Source
PSTN Trunk
10.1.40.0/24
.11
Layer 3 Router
Avaya G430 Media Gateway
10.1.10.0/24
Avaya 9408 Digital Telephone x10017
Avaya 9608 (H.323) IP Telephone x10002
Avaya 9641 (SIP) IP Telephone x10049
Avaya 9641G (H.323) IP Telephone x10001
Atiras Attendant Console Module
.123
Atiras 7.6 Configuration Module on Microsoft Windows 2012 R2 Server

Figure 1: Test 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 Virtualized Server	7.1.0.532.0-23985
Avaya G430 Media Gateway	MGP 38.20.1
Avaya Aura® Media Server	7.8.0.333
Avaya Aura® Application Enablement Services running on Virtualized Server	7.1.1.0.0.5-0
Avaya Aura® System Manager running on Virtualized Server	7.1.1.0 Build 7.1.0.0.1125193 Software Update Revision No: 7.1.1.0.046931 Feature Pack 1
Avaya Aura® Session Manager running on Virtualized Server	7.1.0.0.711008
Avaya Telephones • 9641 (SIP) • 9641G (H323) • 9608 (H.323) • 9408	 7.0.1.4.6 6.6506 6.6506 2.0 SP7 (R18)
Frox Communications Equipment	**Software / Firmware Version**
Atiras running on Windows server 2012 R2 SP1	Atiras 7.6

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

5.1. Note the Node Name of Avaya Aura® Communication Manager

Use **list node-names all** to note the IP address of the Ethernet Processor of the Communication Manager to associate with the AES, i.e. **10.1.10.230**.

```
list node-names all

                        NODE NAMES

Type     Name              IP Address
IP       aams2             10.1.10.12
IP       cms1              10.1.10.85
IP       default           0.0.0.0
IP       lsp-g430          10.1.40.18
IP       mypc              10.3.10.8
IP       n                 10.3.10.253
IP       procr             10.1.10.230
IP       procr6            ::
```

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 3 was added)

Page **1**

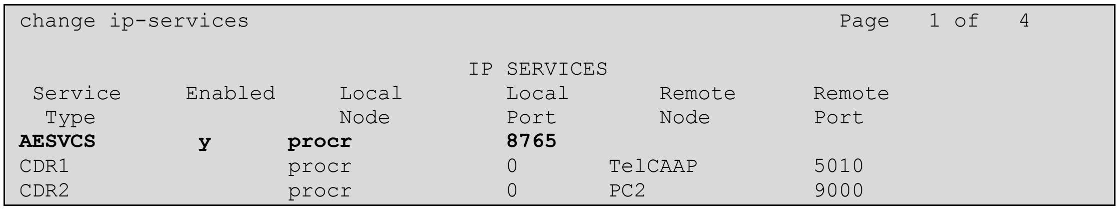
- **Extension** Enter an available extension
- **TYPE** Enter **ADJ-IP**
- **Name** Enter a name for identification

```
add cti-link 3                                                Page   1 of   3
                                    CTI LINK
 CTI Link: 3
Extension: 10093
     Type: ADJ-IP
                                                                       COR: 1
     Name: TSAPI Service - AES7x
```

5.3. Define the AES Link

To define the AES link use the **change ip-services** command and enter the following:
Page **1**

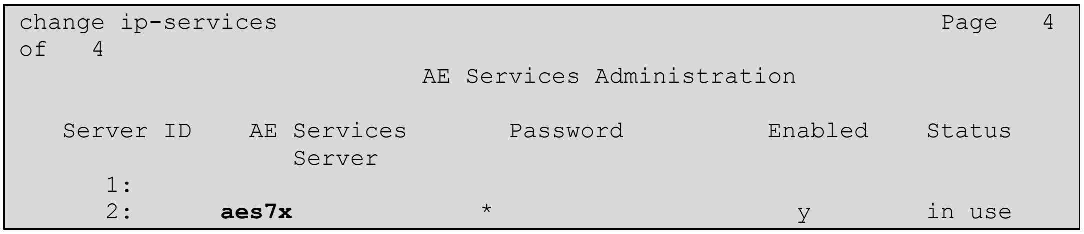
- **Type** Enter **AESVCS**
- **Enabled** Enter **y**
- **Local Node** Enter **procr**
- **Port** Enter **8765**



```
change ip-services                                            Page   1 of   4

                                  IP SERVICES
 Service     Enabled     Local        Local       Remote      Remote
  Type                   Node         Port        Node        Port
AESVCS         y      procr           8765
CDR1                  procr           0       TelCAAP         5010
CDR2                  procr           0       PC2             9000
```

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

- **AE Services** Enter a name for identification.
- **Password** Enter a password. This password will be used in **Section 6.3** to enable the AES to communicate with the Communication Manager.



```
change ip-services                                                  Page   4
of   4
                              AE Services Administration

   Server ID    AE Services       Password          Enabled    Status
                   Server
      1:
      2:      aes7x             *                     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 at least 3 **BUTTON ASSIGNMENTS** for call appearances. To add the attendant station use the **add station** command. The station configured during compliance testing (10001) is shown in the section below.

```
add station 10001                                               Page   1 of   5
                                     STATION

Extension: 10001                         Lock Messages? n              BCC: 0
     Type: 9641G                         Security Code: *               TN: 1
     Port: IP                          Coverage Path 1:                COR: 1
     Name: Attendant                   Coverage Path 2:                COS: 1
                                       Hunt-to Station:              Tests? y
STATION OPTIONS
                                             Time of Day Lock Table:
              Loss Group: 19         Personalized Ringing Pattern: 1
                                                   Message Lamp Ext: 10001
            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? y

                                                 IP Video Softphone? n
                              Short/Prefixed Registration Allowed: default

                                                 Customizable Labels? y
```

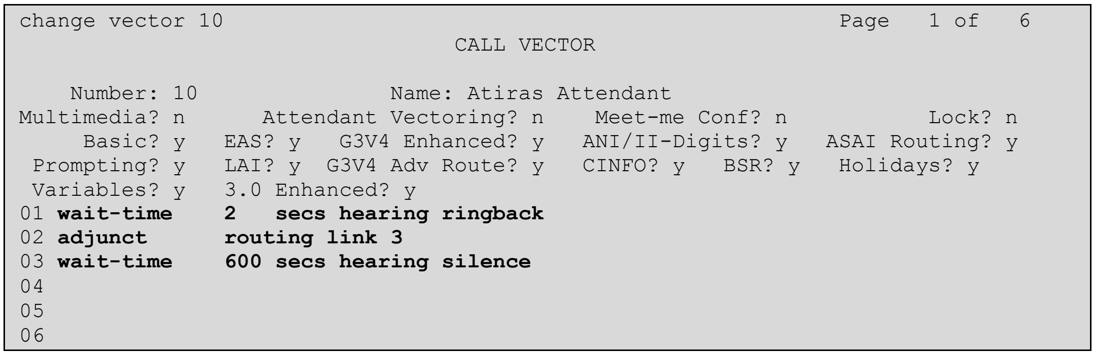
```
add station 10001                                               Page   4 of   5
                                     STATION
 SITE DATA
      Room:                                             Headset? y
      Jack:                                             Speaker? n
     Cable:                                            Mounting: d
     Floor: #03-09/10                              Cord Length: 0
  Building: Rutherford                               Set Color: blue

ABBREVIATED DIALING
     List1: system             List2:                   List3:



BUTTON ASSIGNMENTS
 1: call-appr                         5: call-appr
 2: call-appr                         6: call-appr
 3: call-appr                         7:
 4: call-appr                         8:

    voice-mail 10000
```

5.5. Create Vector for Atiras Attendant Console

To add a vector for the Atiras Attendant use the **change vector** command and enter the following: (**Vector 10** was used during compliance testing)

Page **1**

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



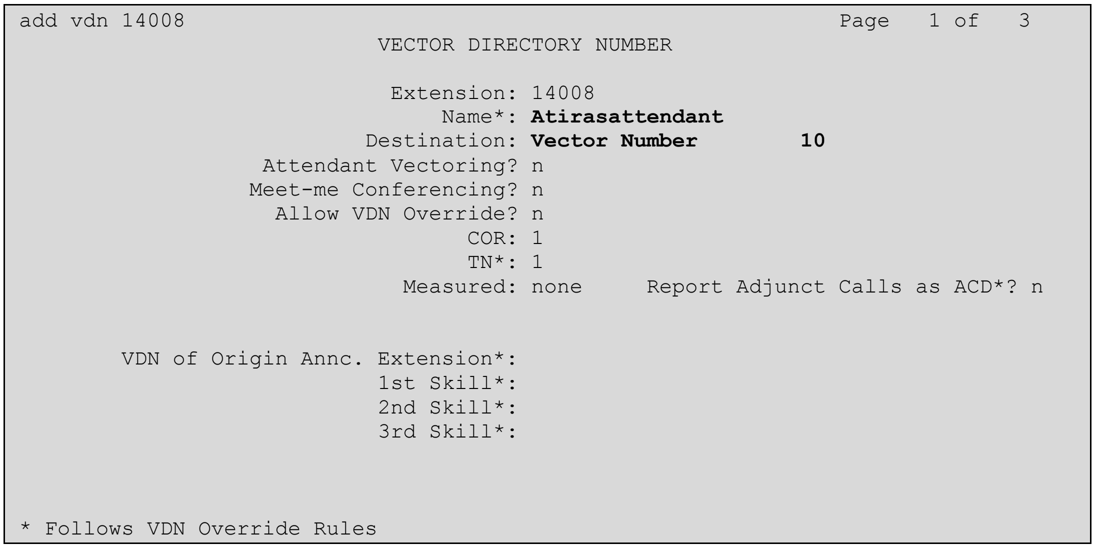
```
change vector 10                                                Page   1 of   6
                                  CALL VECTOR

    Number: 10               Name: Atiras Attendant
Multimedia? n      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 3
03 wait-time    600 secs hearing silence
04
05
06
```

5.6. Add VDN for Atiras Attendant Console

To add a VDN for the Atiras Attendant use the **add VDN** command and enter the following: (Vector 14008 was used during compliance testing)

Page **1**

- **Name** Enter an informative name (i.e. **Atirasattendant**)
- **Destination** Enter **Vector Number 10** (Vector as configured in **Section 5.5**)
- **Attendant Vectoring?** Enter **n**



```
add vdn 14008                                                   Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                             Extension: 14008
                                 Name*: Atirasattendant
                           Destination: Vector Number        10
                   Attendant Vectoring? n
                  Meet-me Conferencing? n
                    Allow VDN Override? n
                                   COR: 1
                                   TN*: 1
                              Measured: none     Report Adjunct Calls as ACD*? n


        VDN of Origin Annc. Extension*:
                            1st Skill*:
                            2nd Skill*:
                            3rd Skill*:



* Follows VDN Override Rules
```

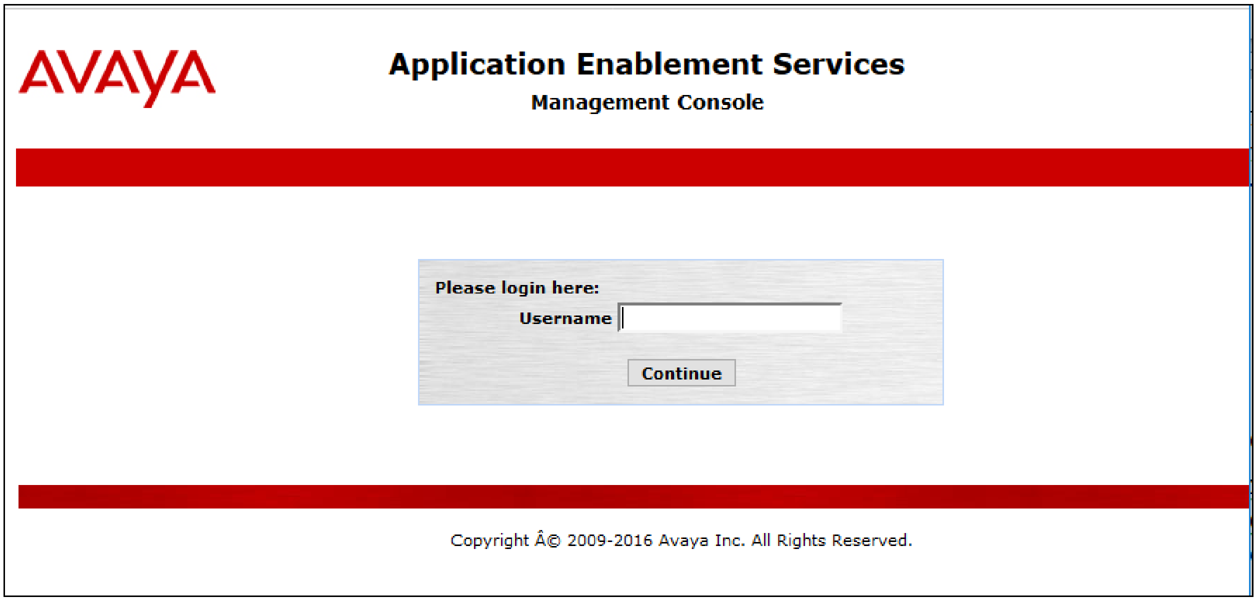
6. Configuration of Avaya Aura® Application Enablement Services

This section provides the procedures for configuring Avaya Application Enablement Services. It is implied that 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
- Disable Security Database
- Restart TSAPI and DMCC Service
- Create CTI User
- Administer CTI User Permissions
- Configure TSAPI and DMCC Port

6.1. Logging into the Avaya Avaya® Application Enablement Services

To access the OAM web-based interface of the Application Enablement Services Server use the URL https://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.


Application Enablement Services

Management Console

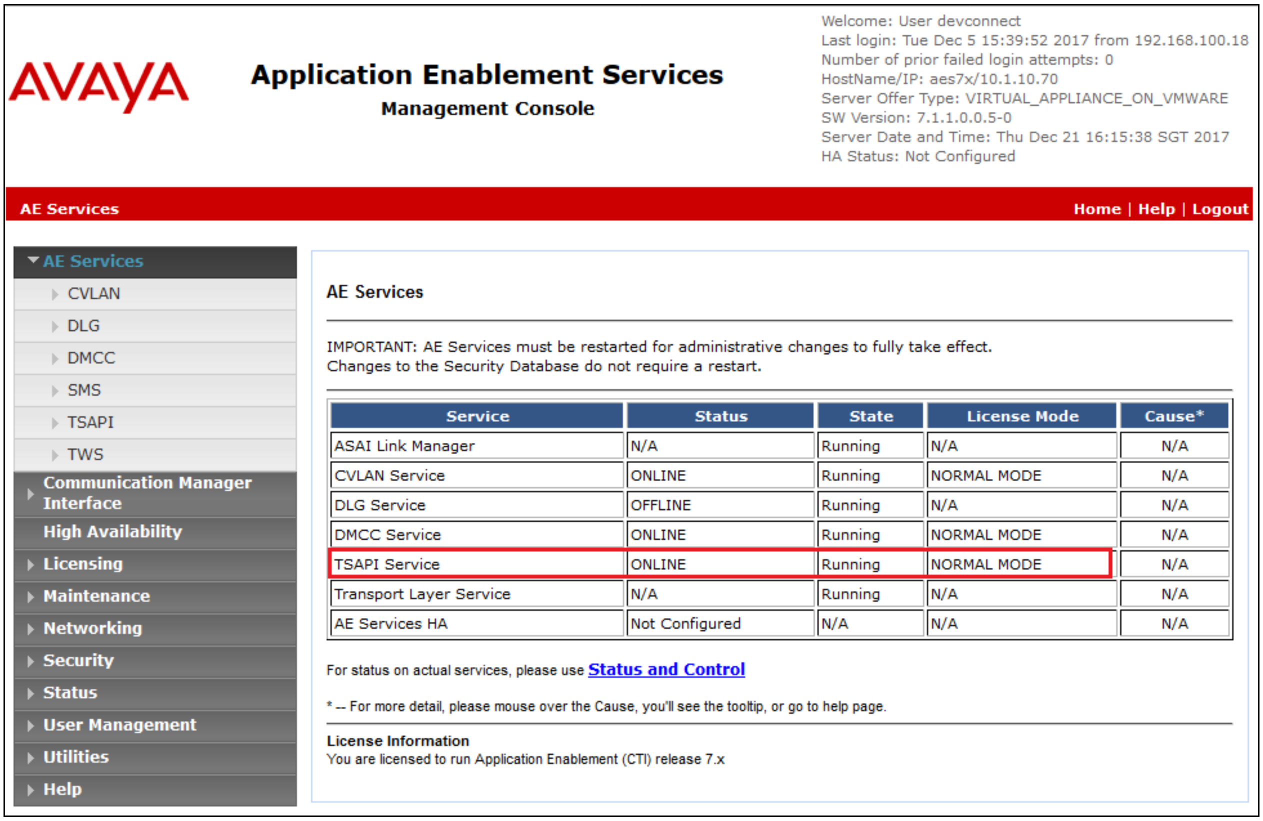
Please login here:

Username

Copyright Â© 2009-2016 Avaya Inc. All Rights Reserved.

6.2. Verify 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.**



Welcome: User devconnect
Last login: Tue Dec 5 15:39:52 2017 from 192.168.100.18
Number of prior failed login attempts: 0
HostName/IP: aes7x/10.1.10.70
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.1.0.0.5-0
Server Date and Time: Thu Dec 21 16:15:38 SGT 2017
HA Status: Not Configured

AE Services

IMPORTANT: AE Services must be restarted for administrative changes to fully take effect.
Changes to the Security Database do not require a restart.

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
AE Services HA	Not Configured	N/A	N/A	N/A

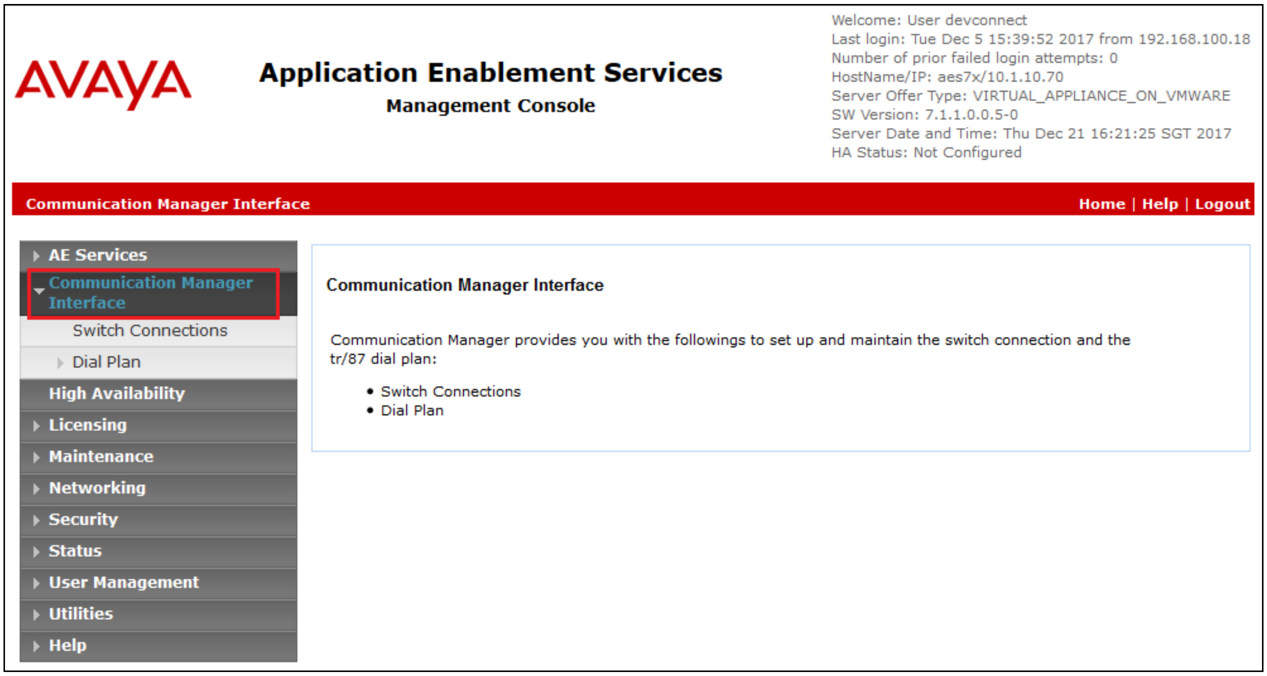
For status on actual services, please use Status and Control

* -- 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 7.x

6.3. Create an Avaya Aura® 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**.



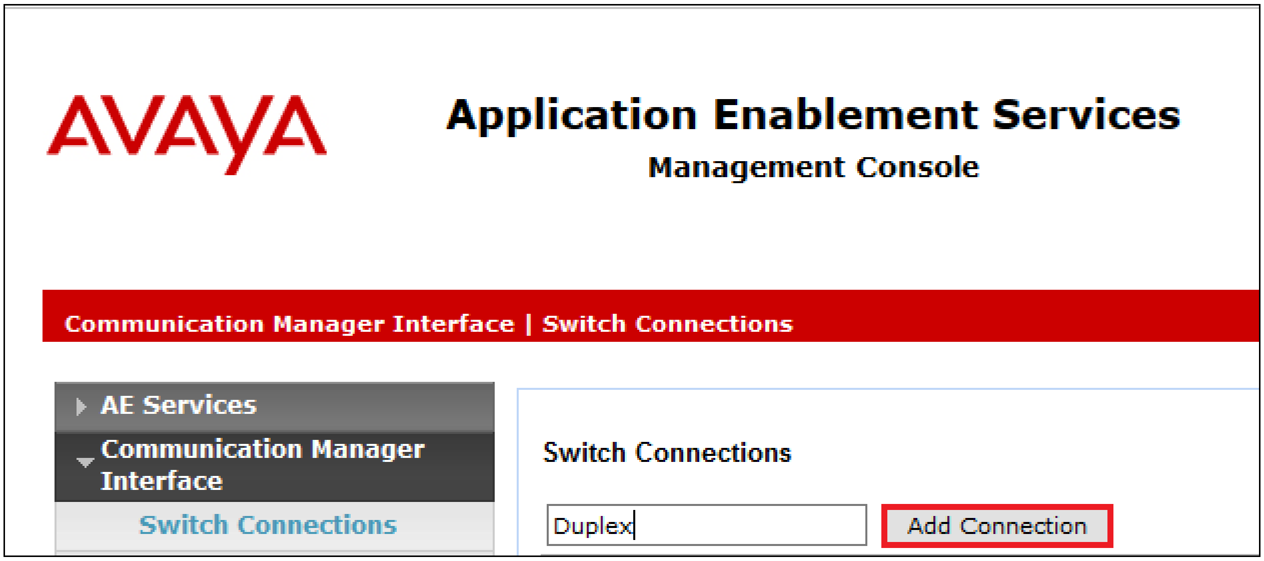
Welcome: User devconnect
Last login: Tue Dec 5 15:39:52 2017 from 192.168.100.18
Number of prior failed login attempts: 0
HostName/IP: aes7x/10.1.10.70
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.1.0.0.5-0
Server Date and Time: Thu Dec 21 16:21:25 SGT 2017
HA Status: Not Configured

Communication Manager Interface

Communication Manager provides you with the followings to set up and maintain the switch connection and the tr/87 dial plan:

- Switch Connections
- Dial Plan

Select **Switch Connections** and enter an informative name for Communication Manager (in this Compliance test, **Duplex** name was used). Click on the **Add Connection** button.

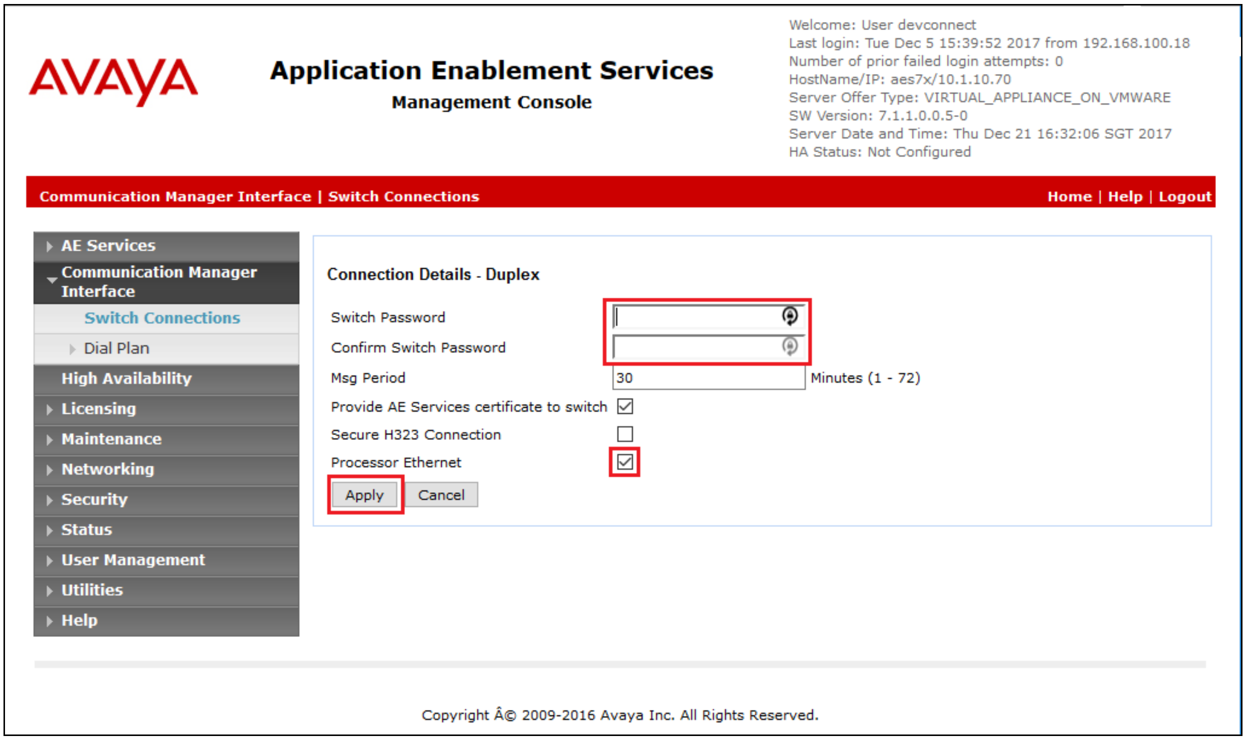


Switch Connections

Duplex

AVAYA
Application Enablement Services
Management Console
Communication Manager Interface | Switch Connections
AE Services
Communication Manager Interface
Switch Connections
Add Connection

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



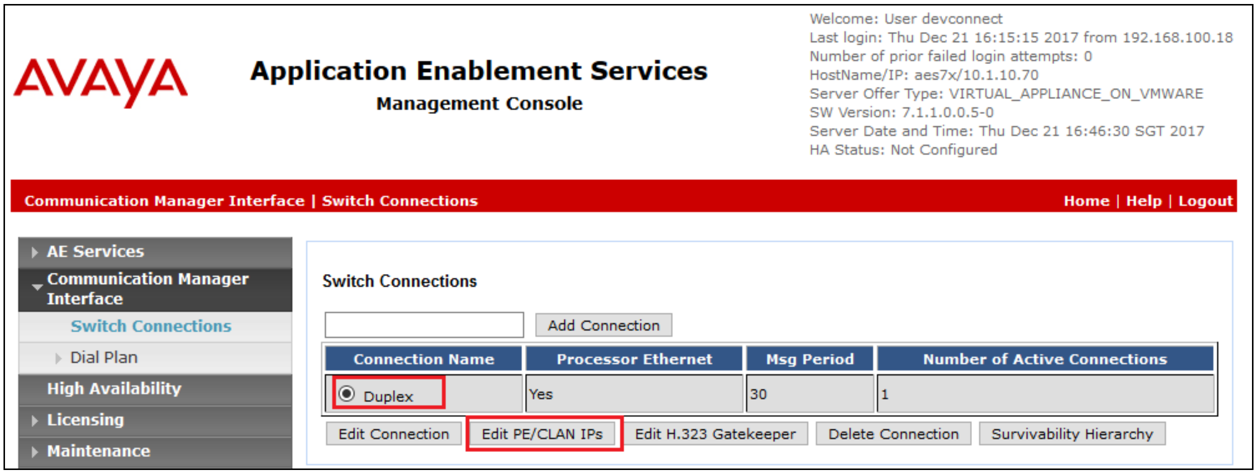
Welcome: User devconnect
Last login: Tue Dec 5 15:39:52 2017 from 192.168.100.18
Number of prior failed login attempts: 0
HostName/IP: aes7x/10.1.10.70
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.1.0.0.5-0
Server Date and Time: Thu Dec 21 16:32:06 SGT 2017
HA Status: Not Configured

Connection Details - Duplex

Switch Password		
Confirm Switch Password		
Msg Period	30	Minutes (1 - 72)
Provide AE Services certificate to switch	☑	
Secure H323 Connection	□	
Processor Ethernet	☑	

Copyright Â© 2009-2016 Avaya Inc. All Rights Reserved.

The **Switch Connections** screen is displayed. Select the newly added switch connection name and click **Edit PE/CLAN IPs**.

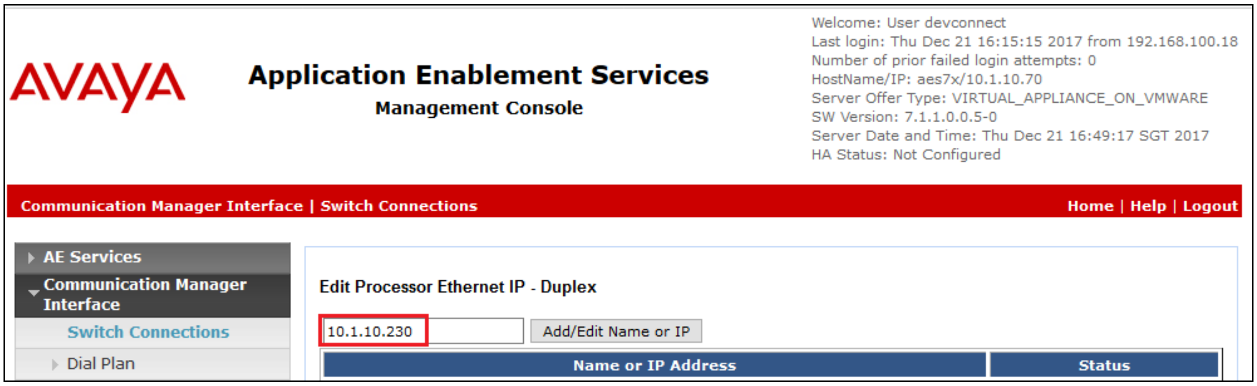


Welcome: User devconnect
Last login: Thu Dec 21 16:15:15 2017 from 192.168.100.18
Number of prior failed login attempts: 0
HostName/IP: aes7x/10.1.10.70
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.1.0.0.5-0
Server Date and Time: Thu Dec 21 16:46:30 SGT 2017
HA Status: Not Configured

Switch Connections

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
● Duplex	Yes	30	1

In the **Edit Processor Ethernet IP – Duplex** screen, enter the host name or IP address of the PE/C-LAN used for AES connectivity. In this case, **10.1.10.230** is used, which corresponds to the **procr** address of the Communication Manager in **Section 5.1**. Click **Add/Edit Name or IP**



Welcome: User devconnect
Last login: Thu Dec 21 16:15:15 2017 from 192.168.100.18
Number of prior failed login attempts: 0
HostName/IP: aes7x/10.1.10.70
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.1.0.0.5-0
Server Date and Time: Thu Dec 21 16:49:17 SGT 2017
HA Status: Not Configured

Edit Processor Ethernet IP - Duplex

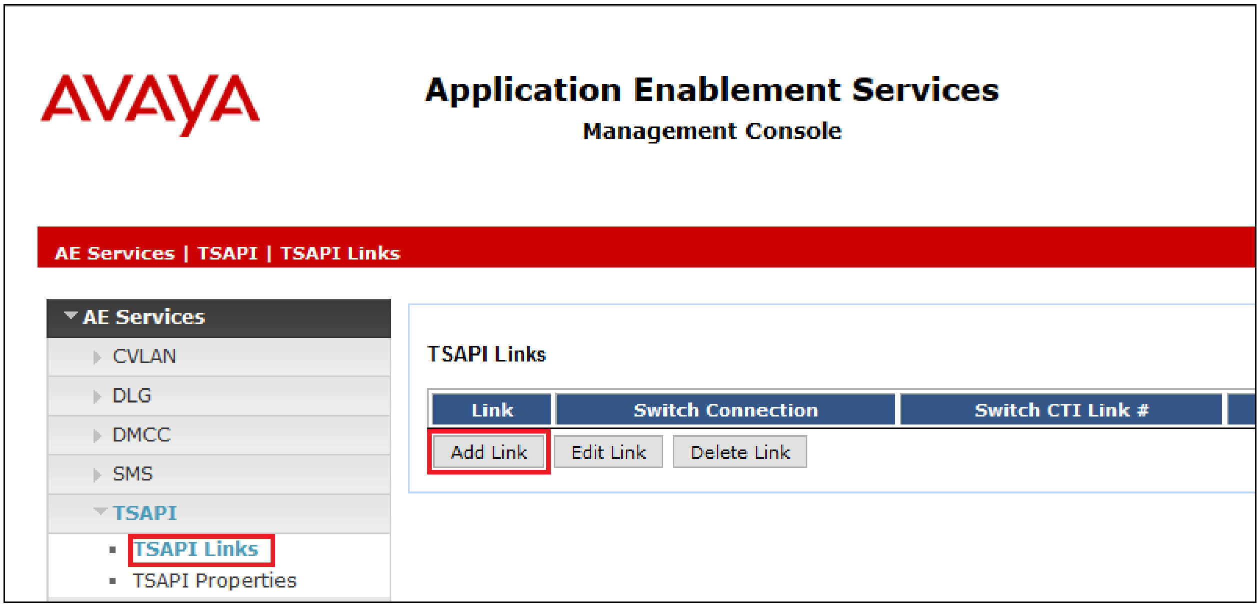
10.1.10.230

Name or IP Address	Status

AVAYA
Application Enablement Services
Management Console
Communication Manager Interface | Switch Connections
Home | Help | Logout
AE Services
Communication Manager Interface
Switch Connections
Dial Plan
Add/Edit Name or IP

6.4. Create a TSAPI Link

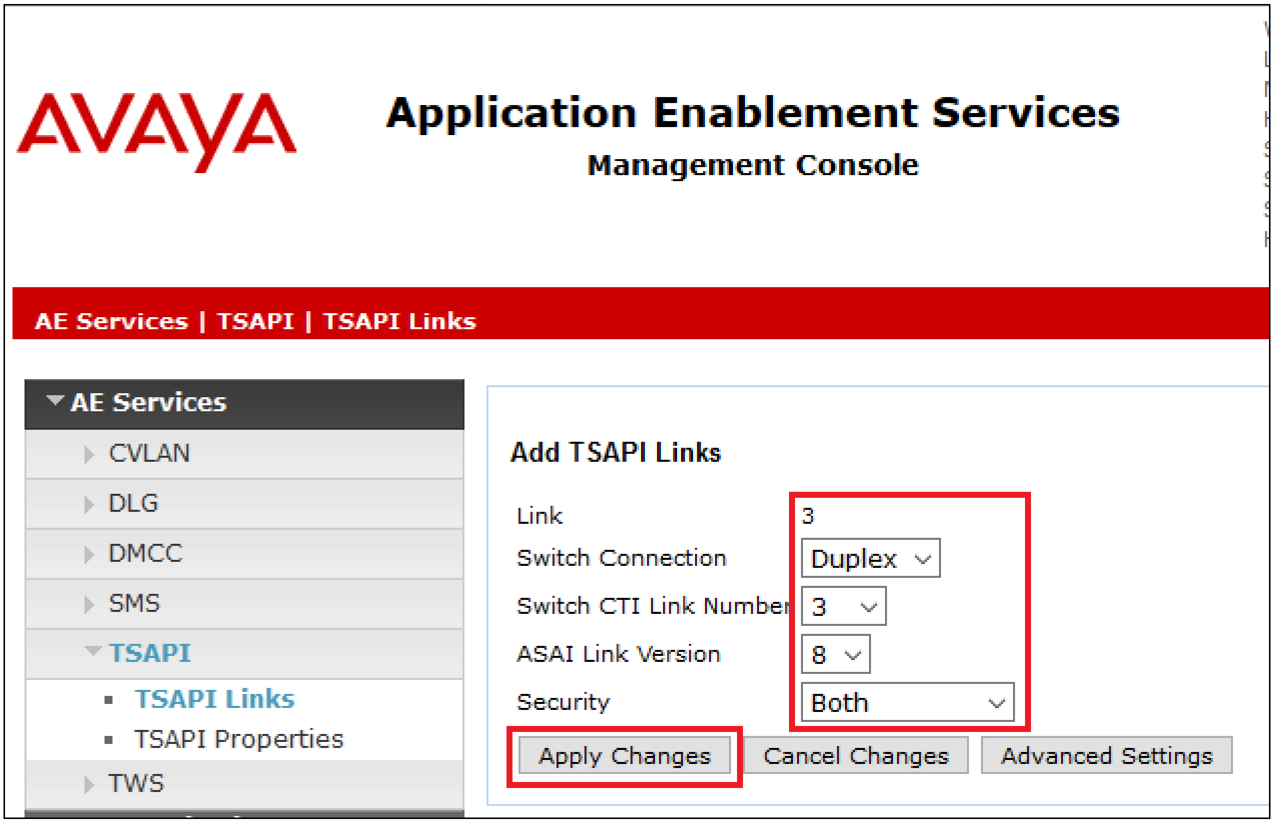
A TSAPI Link needs to be created to interoperate with the Atiras. Navigate to **AE Services → TSAPI → TSAPI Links** and click on the **Add Link** button.



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

- Select **Duplex** from the **Switch Connection** dropdown box. (The Switch connection as created in **Section 6.3**)
- Select **3** from the **Switch CTI Link Number** dropdown box. (The CTI link as created in **Section 5.2**)
- Select **ASAI Link Version** latest version **8**
- Select **Both** for the **Security** dropdown box (To allow for encrypted or unencrypted link)

Click on the **Apply Changes** button.

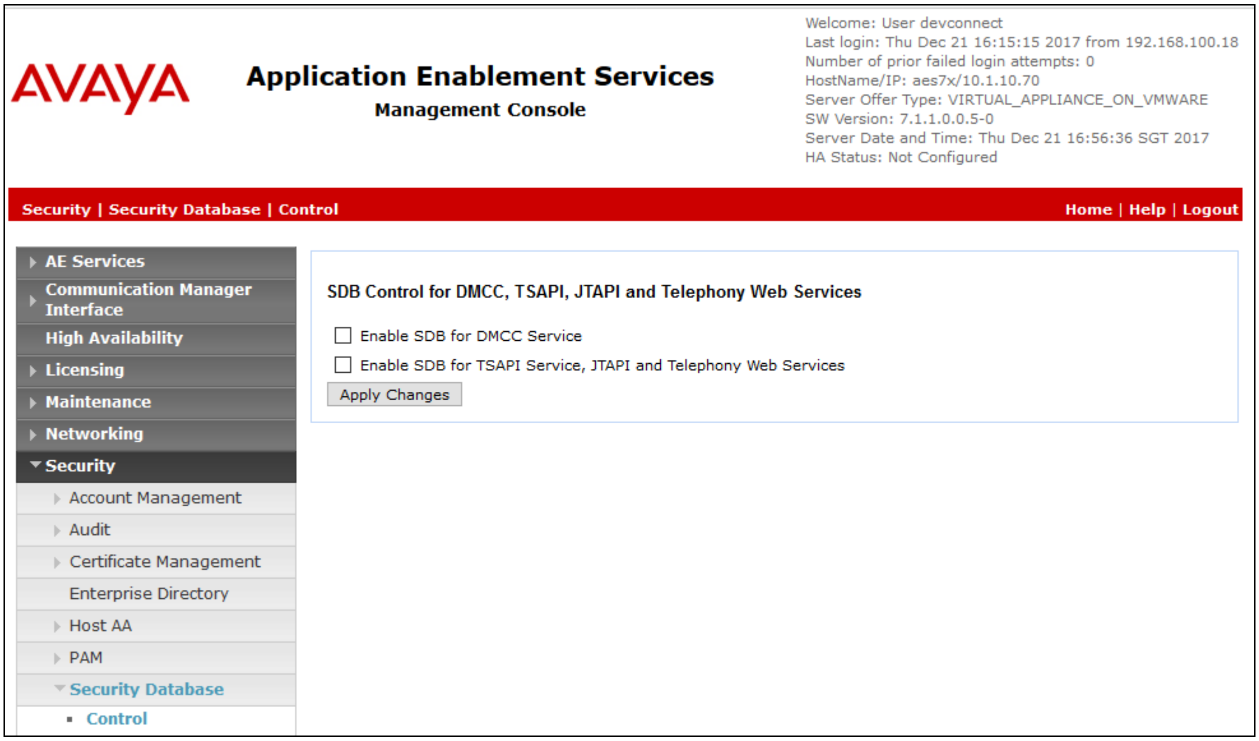


Add TSAPI Links

Link	3
Switch Connection	Duplex
Switch CTI Link Number	3
ASAI Link Version	8
Security	Both

6.5. Disable Security Database

Select **Security → Security Database → Control** from the left pane to display the **SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services** screen in the right pane. Clear the **Enable SDB for DMCC Service** and **Enable SDB for TSAPI Service, JTAPI and Telephony Web Services** if they are checked, and click **Apply Changes**.



Welcome: User devconnect
Last login: Thu Dec 21 16:15:15 2017 from 192.168.100.18
Number of prior failed login attempts: 0
HostName/IP: aes7x/10.1.10.70
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.1.0.0.5-0
Server Date and Time: Thu Dec 21 16:56:36 SGT 2017
HA Status: Not Configured

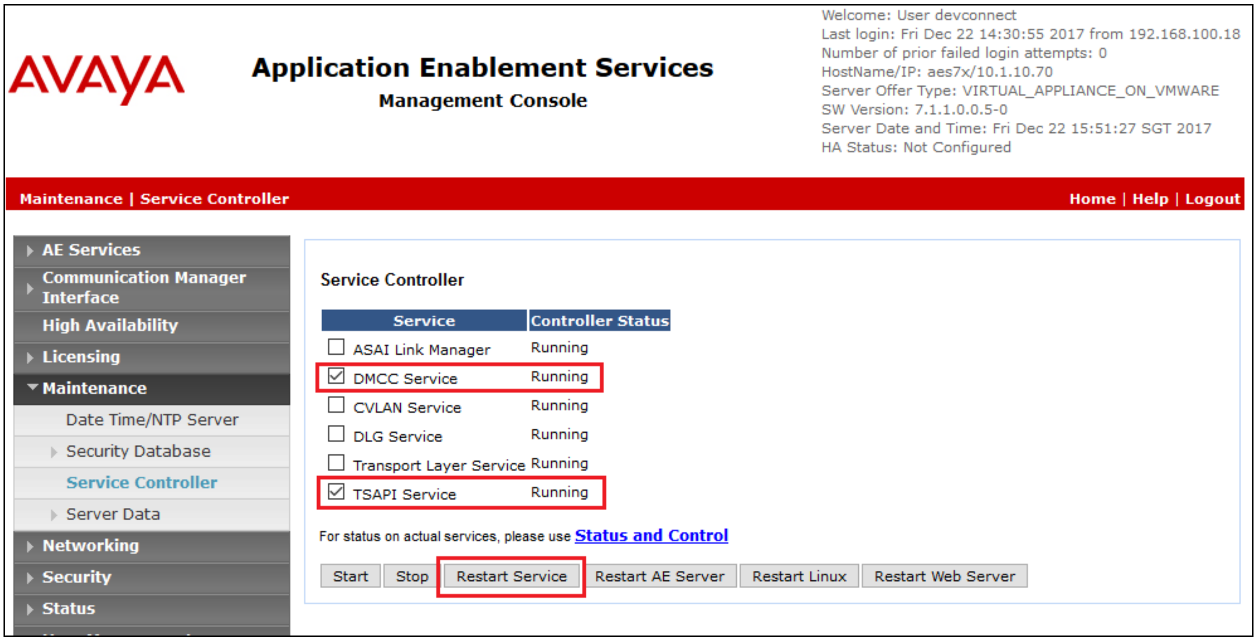
SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services

□ Enable SDB for DMCC Service

□ Enable SDB for TSAPI Service, JTAPI and Telephony Web Services

6.6. Restart TSAPI and DMCC Service

Select **Maintenance → Service Controller** from the left pane to display the **Service Controller** screen in the right pane. Check the **TSAPI Service** and **DMCC Service**, and click **Restart Service**.



Welcome: User devconnect
Last login: Fri Dec 22 14:30:55 2017 from 192.168.100.18
Number of prior failed login attempts: 0
HostName/IP: aes7x/10.1.10.70
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.1.0.0.5-0
Server Date and Time: Fri Dec 22 15:51:27 SGT 2017
HA Status: Not Configured

Service Controller

Service	Controller Status
☐ ASAI Link Manager	Running
☑ DMCC Service	Running
☐ CVLAN Service	Running
☐ DLG Service	Running
☐ Transport Layer Service	Running
☑ TSAPI Service	Running

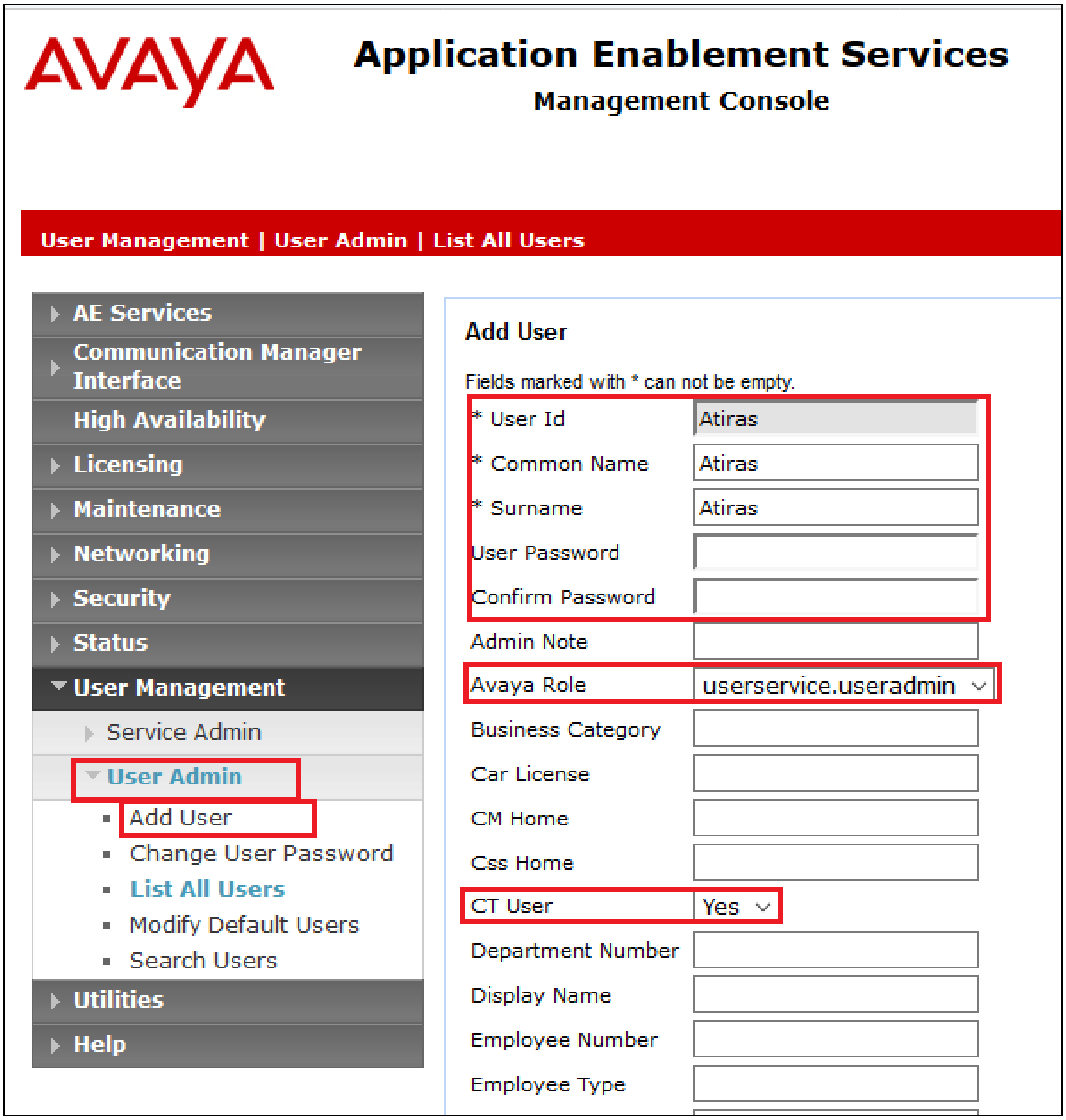
For status on actual services, please use Status and Control

6.7. Create CTI User

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

- Enter a **User Id** in this case **Atiras**, This ID will be required for the Atiras configuration.
- Enter a **Common Name** in this case **Atiras**.
- Enter a **Surname** in this case **Atiras**.
- Enter a **User Password**. This password will be required for the Atiras 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).



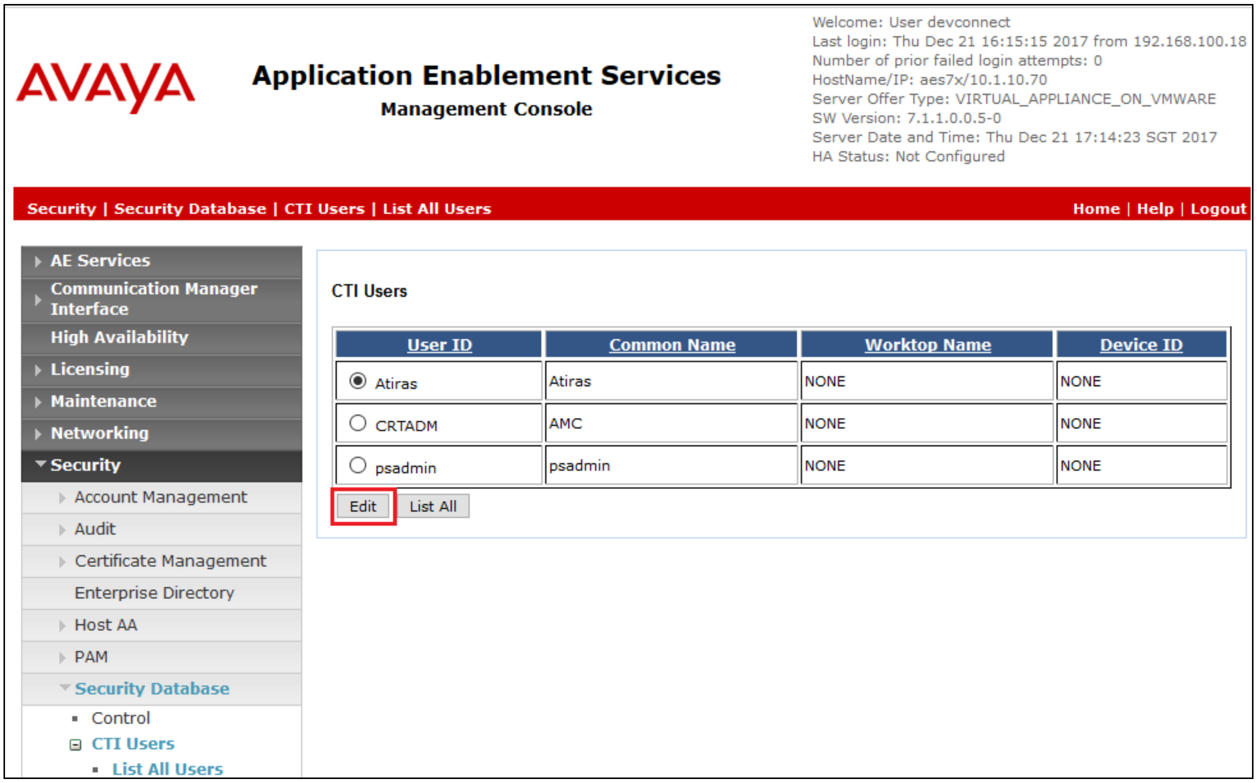
Add User

Fields marked with * can not be empty.

* User Id	Atiras
* Common Name	Atiras
* Surname	Atiras
User Password	
Confirm Password	
Admin Note	
Avaya Role	userservice.useradmin
Business Category	
Car License	
CM Home	
Css Home	
CT User	Yes
Department Number	
Display Name	
Employee Number	
Employee Type	

6.8. Administer CTI User Permissions

Select **Security → Security Database → CTI Users → List All Users** from the AES Management Console Home menu. Select the User ID created in **Section 6.7** and click **Edit**.

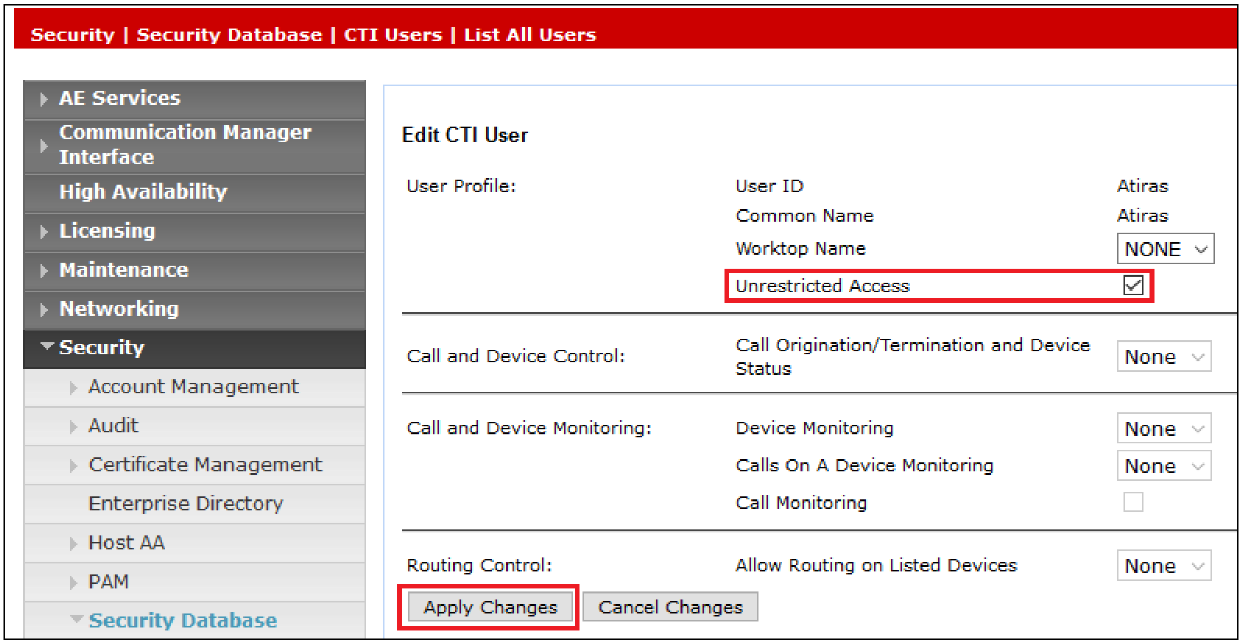


Welcome: User devconnect
Last login: Thu Dec 21 16:15:15 2017 from 192.168.100.18
Number of prior failed login attempts: 0
HostName/IP: aes7x/10.1.10.70
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.1.0.0.5-0
Server Date and Time: Thu Dec 21 17:14:23 SGT 2017
HA Status: Not Configured

CTI Users

User ID	Common Name	Worktop Name	Device ID
● Atiras	Atiras	NONE	NONE
○ CRTADM	AMC	NONE	NONE
○ psadmin	psadmin	NONE	NONE

Check the **Unrestricted Access** box. Click **Apply Changes**.

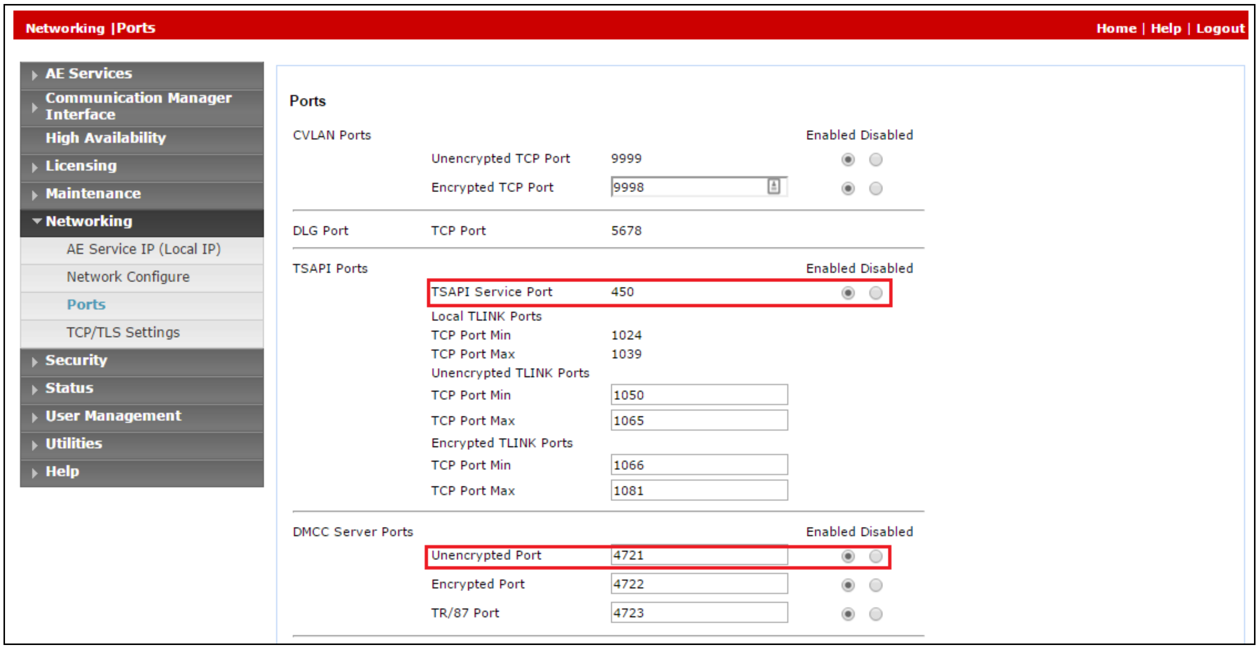


Edit CTI User

User Profile:	User ID	Atiras
	Common Name	Atiras
	Worktop Name	NONE
	Unrestricted Access	☑
Call and Device Control:	Call Origination/Termination and Device Status	None
Call and Device Monitoring:	Device Monitoring	None
	Calls On A Device Monitoring	None
	Call Monitoring	□
Routing Control:	Allow Routing on Listed Devices	None

6.9. Configure TSAPI and DMCC Port

On the AES Management Console, navigate to **Networking → Ports**. In the **DMCC Server Ports** area, for the **Unencrypted Port** and click on the **Enabled** radio button. During compliance testing, the **Unencrypted Port** was set to **4721**. Do the same for **TSAPI Ports** for **TSAPI Service Port** under the **Enabled** column for the port **450**. Click the **Apply Changes** button (not shown) at the bottom of the screen to complete the process.



Ports

			Enabled	Disabled
CVLAN Ports			Enabled	Disabled
	Unencrypted TCP Port	9999	●	○
	Encrypted TCP Port	9998	●	○
DLG Port	TCP Port	5678		
TSAPI Ports			Enabled	Disabled
	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		
DMCC Server Ports			Enabled	Disabled
	Unencrypted Port	4721	●	○
	Encrypted Port	4722	●	○
	TR/87 Port	4723	●	○

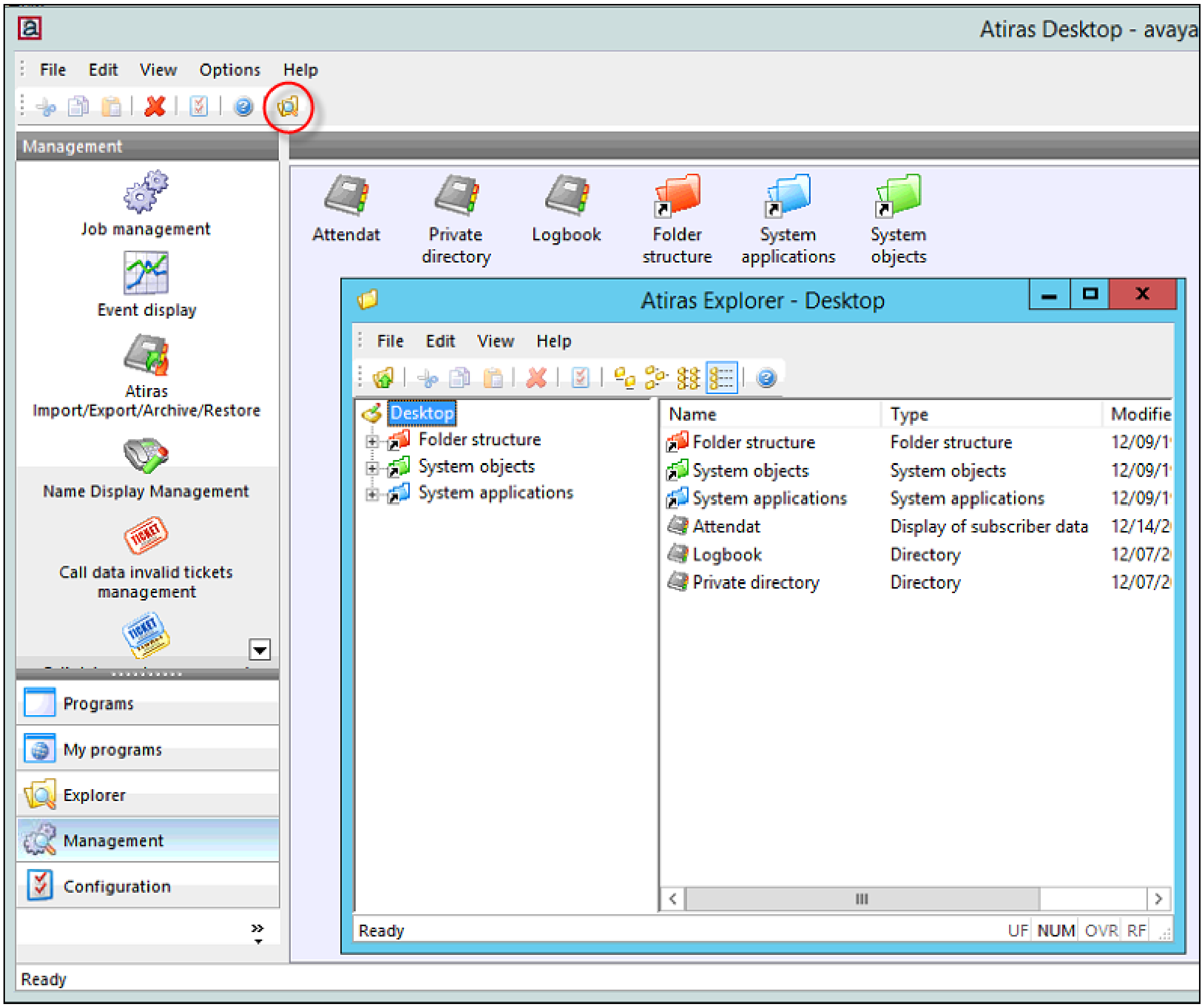
7. Configuring the Atiras Configuration module

This section describes the steps preformed 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 11**. The configuration operations described in this section can be summarized as follows:

- Configure Communication Manager
- Synchronize Telephony functions
- Configure Atiras for Session Manager
- Synchronize Session Manager

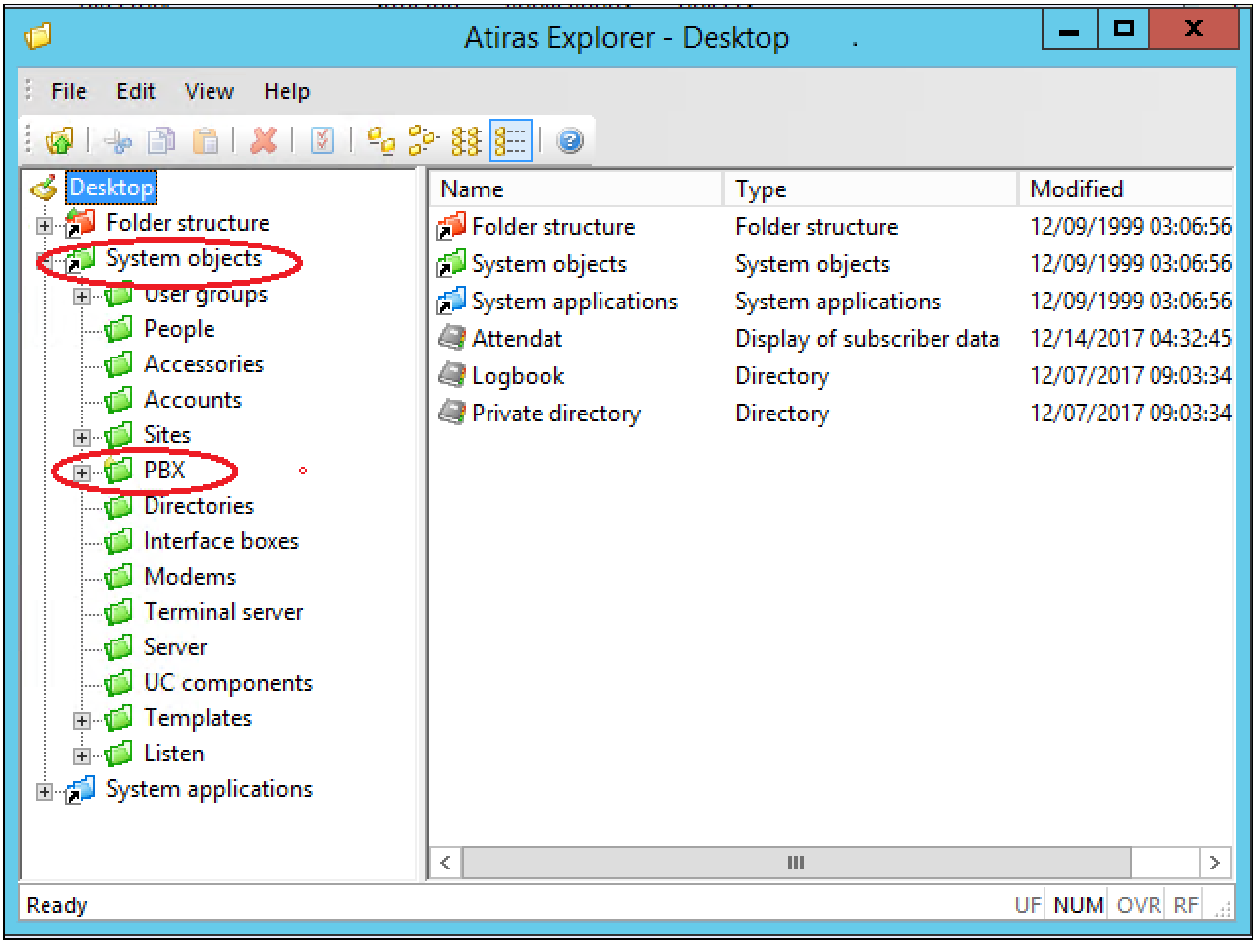
7.1. Configure Avaya Aura® Communication Manager on Atiras

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



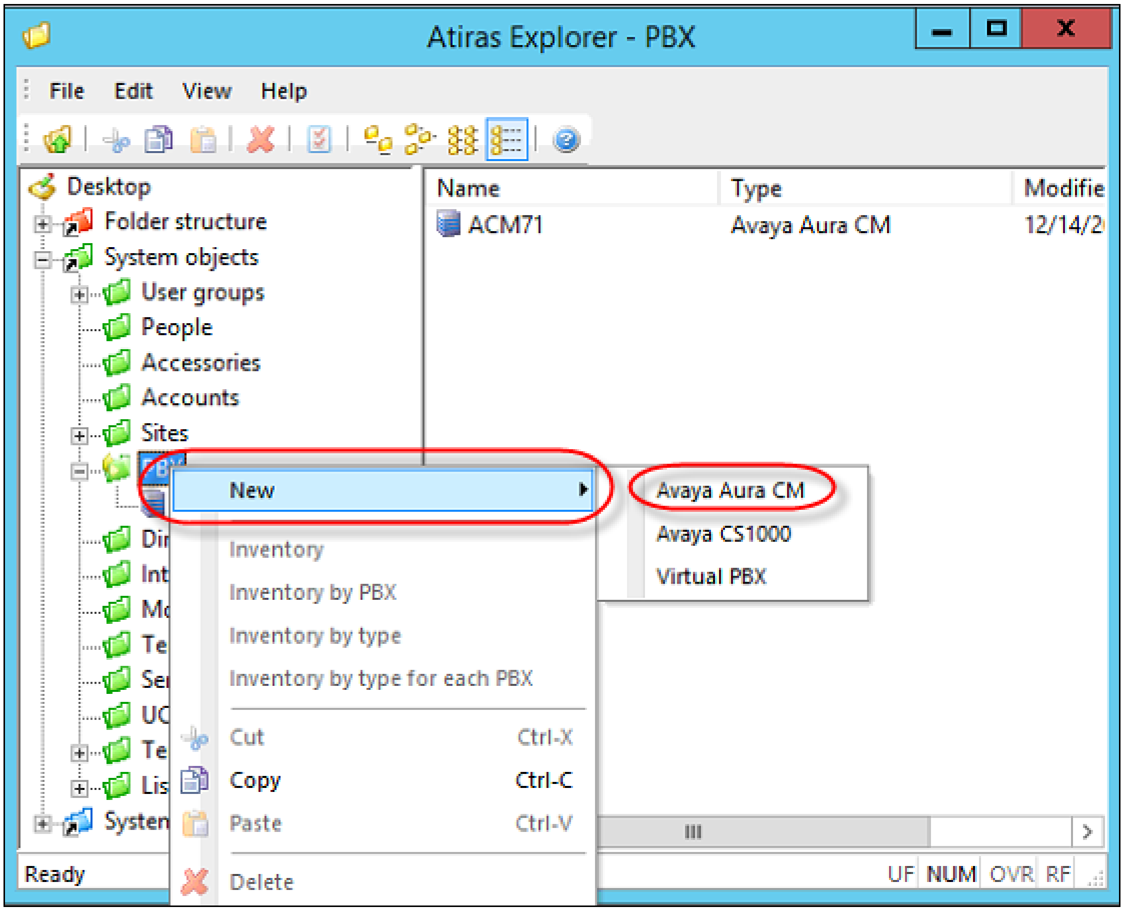
Name	Type	Modifie
Folder structure	Folder structure	12/09/1
System objects	System objects	12/09/1
System applications	System applications	12/09/1
Attendat	Display of subscriber data	12/14/2
Logbook	Directory	12/07/2
Private directory	Directory	12/07/2

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



Name	Type	Modified
Folder structure	Folder structure	12/09/1999 03:06:56
System objects	System objects	12/09/1999 03:06:56
System applications	System applications	12/09/1999 03:06:56
Attendat	Display of subscriber data	12/14/2017 04:32:45
Logbook	Directory	12/07/2017 09:03:34
Private directory	Directory	12/07/2017 09:03:34

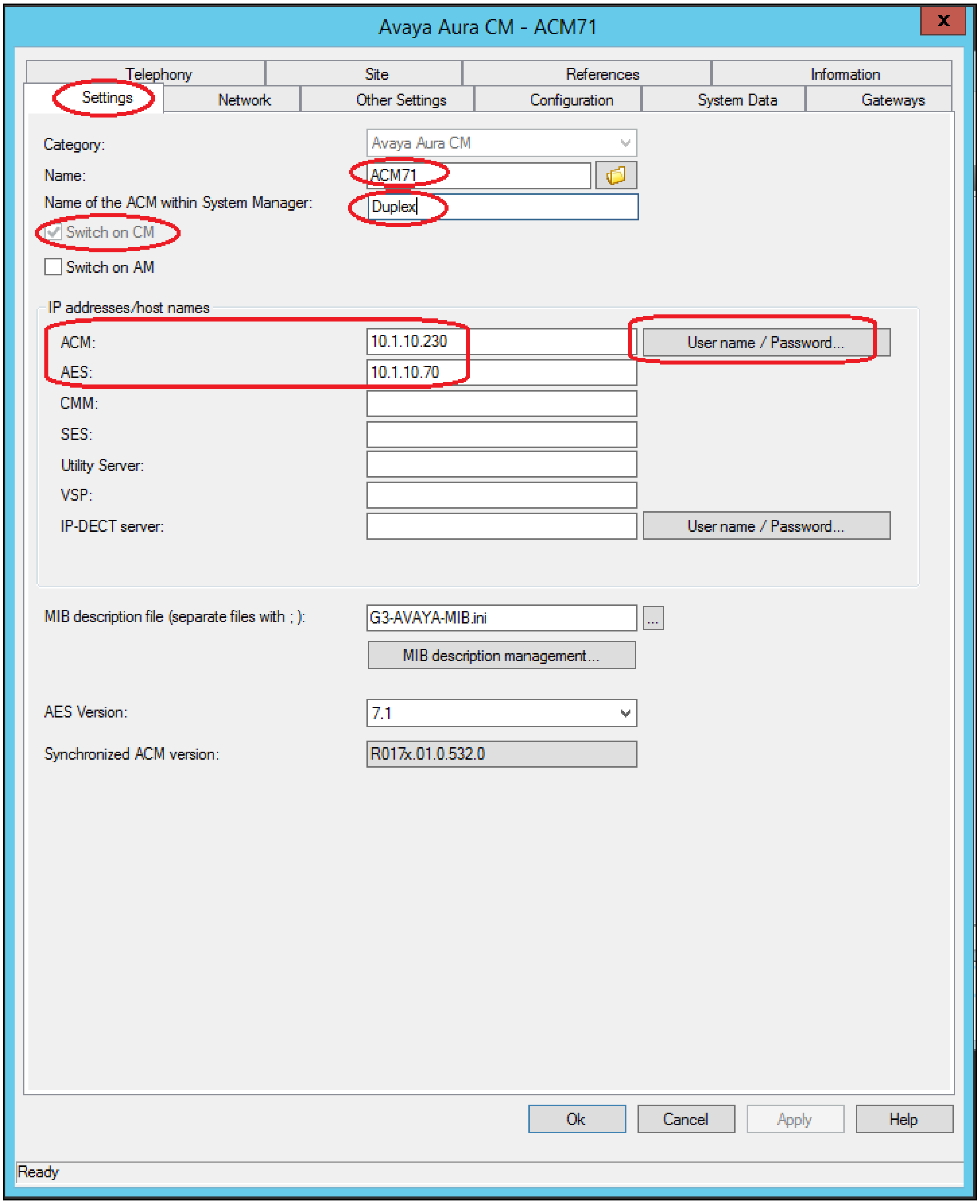
Right-click on **PBX** and select **New → Avaya Aura CM**.



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. ACM71)
- **Name of the ACM within System Manager** Enter **Duplex** as was created in **Section 6.3**
- Click the **Switch on CM** check box
- **ACM** Enter the IP address of Communication Manager
- **AES** Enter the IP address of AES

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



Category: Avaya Aura CM

Name: ACM71

Name of the ACM within System Manager: Duplex

☑ Switch on CM

☐ Switch on AM

IP addresses/host names

ACM: 10.1.10.230

AES: 10.1.10.70

CMM:

SES:

Utility Server:

VSP:

IP-DECT server:

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

AES Version: 7.1

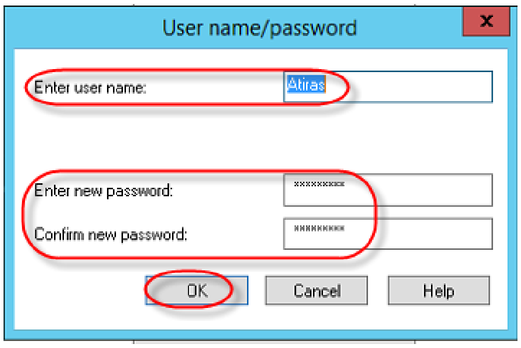
Synchronized ACM version: R017x.01.0.532.0

Ready

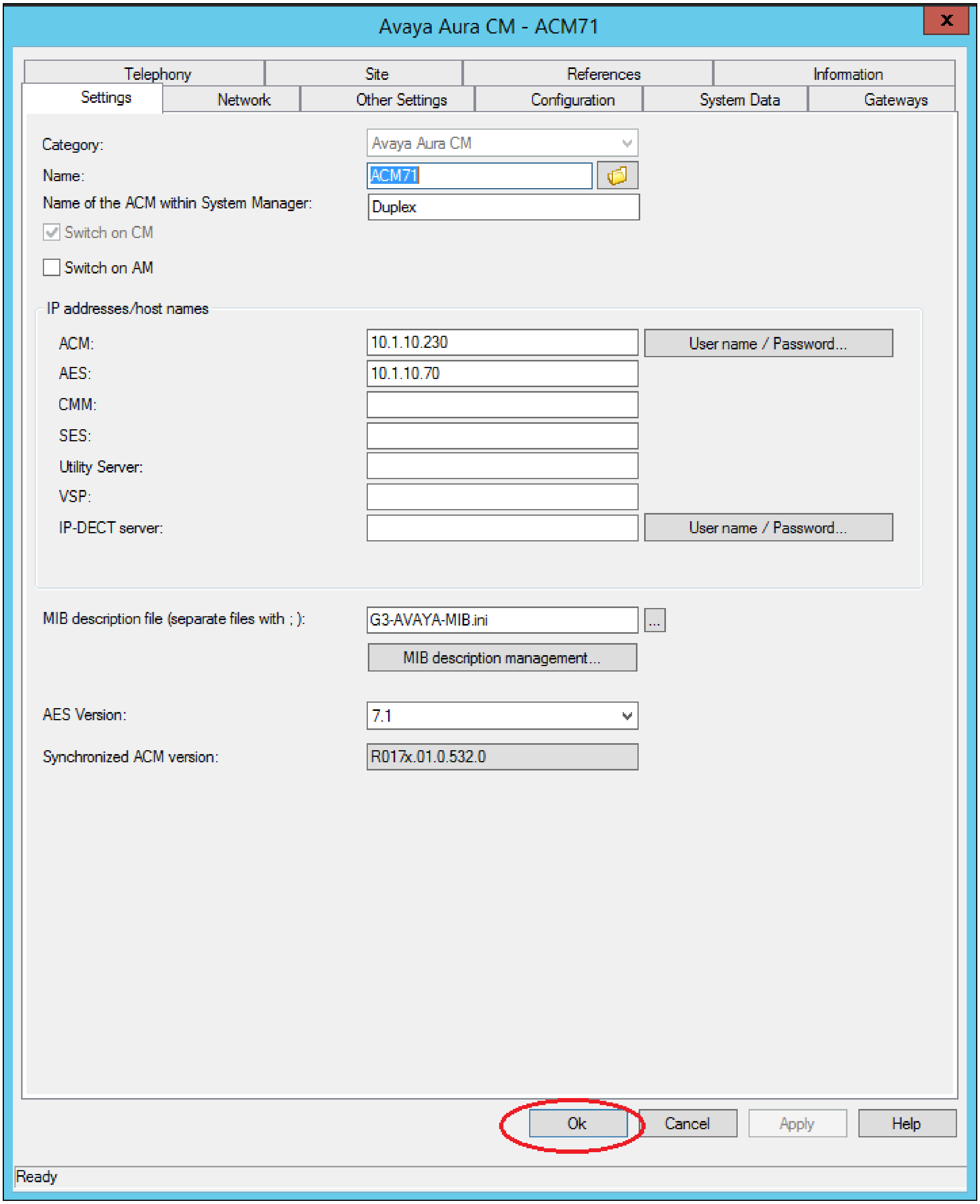
In the **User name/Password** window enter the following. Note that the user name/password has to be the configured the same in both AES and Communication Manager.

- **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.



Click on the **OK** button again.



Category: Avaya Aura CM

Name: ACM71

Name of the ACM within System Manager: Duplex

☑ Switch on CM

□ Switch on AM

IP addresses/host names

ACM: 10.1.10.230

AES: 10.1.10.70

CMM:

SES:

Utility Server:

VSP:

IP-DECT server:

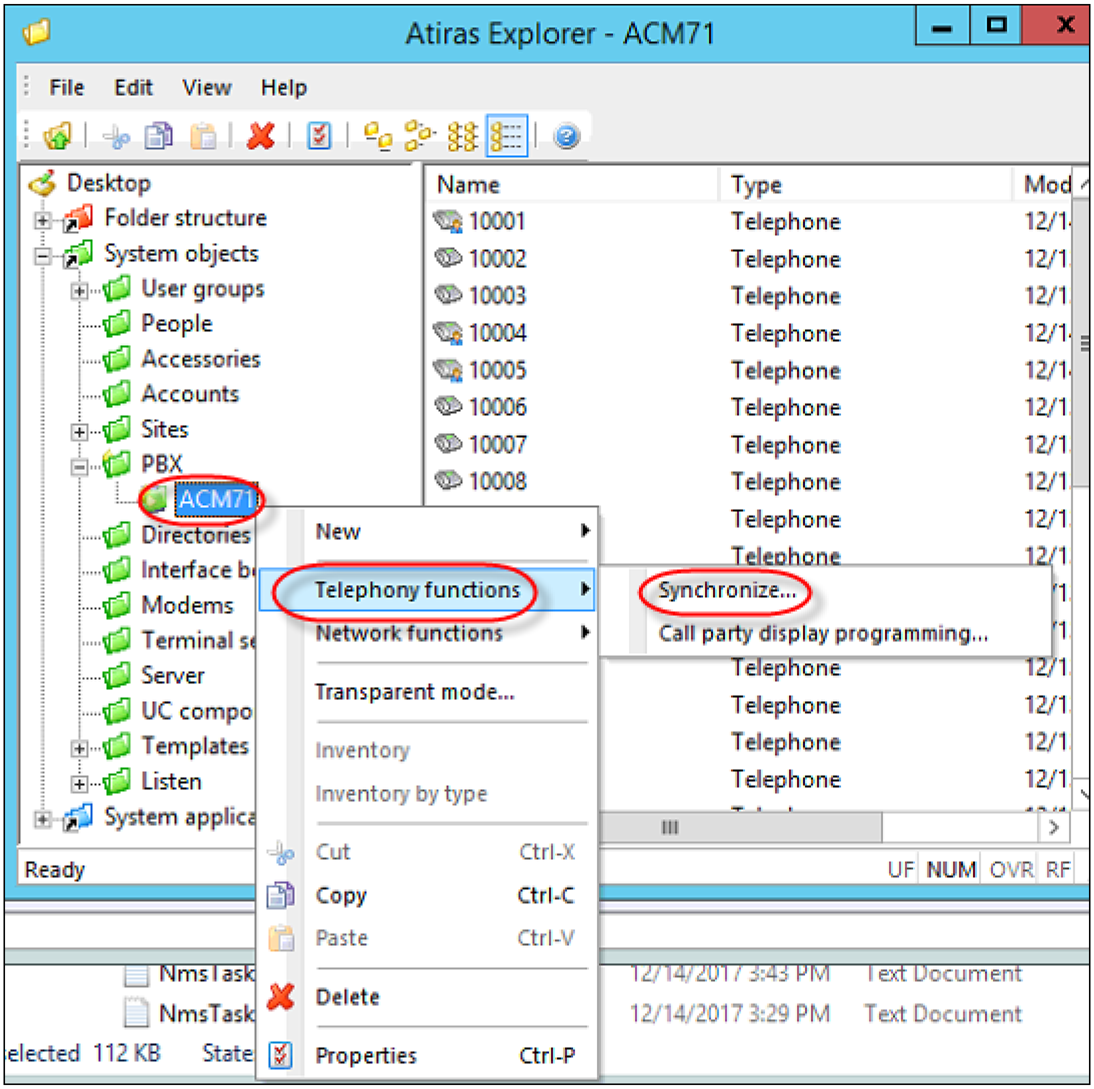
MIB description file (separate files with ;): G3-AVAYA-MIB.ini

AES Version: 7.1

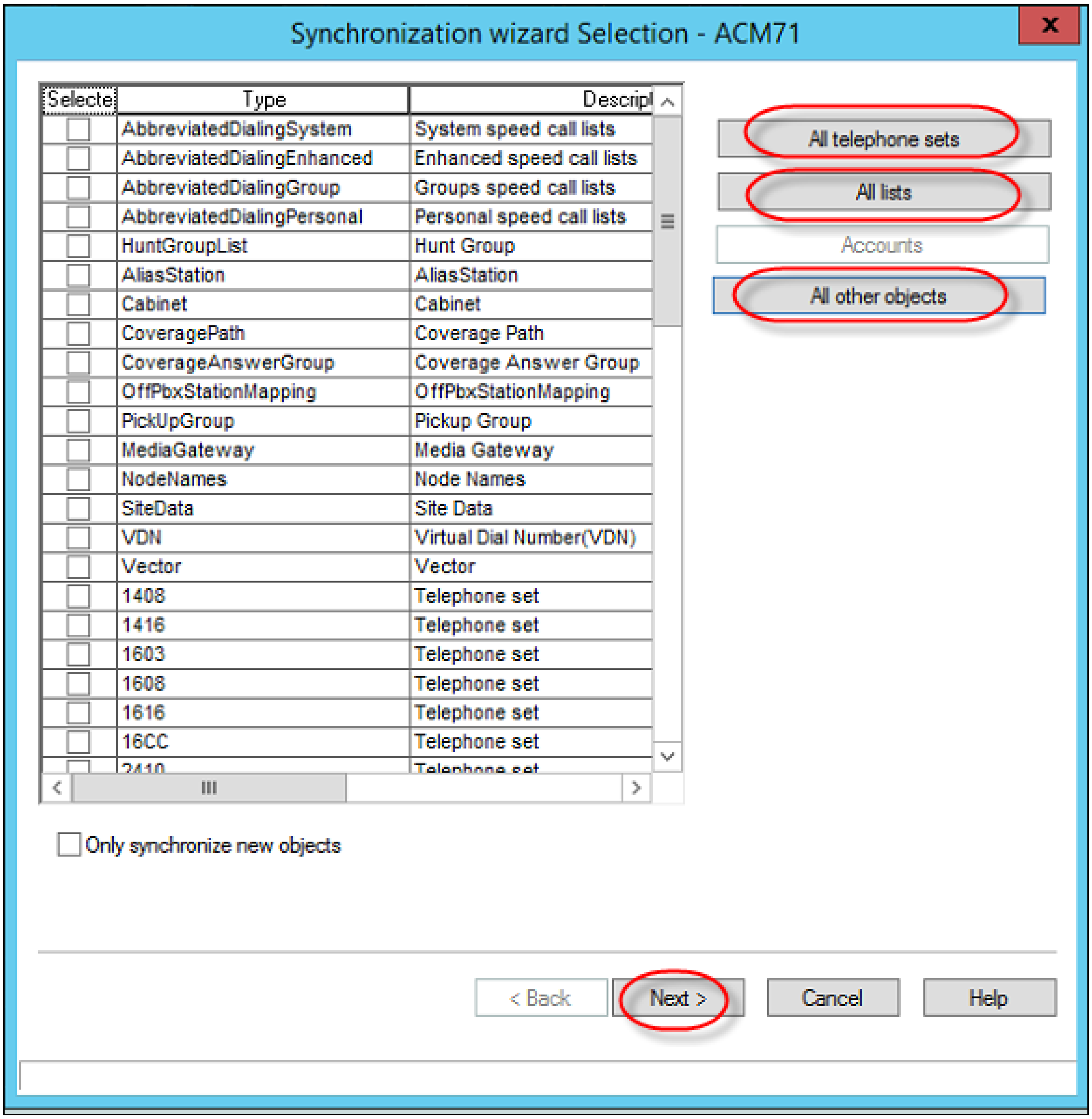
Synchronized ACM version: R017x.01.0.532.0

7.2. Synchronize Telephony functions

Once the Communication Manager is configured it must be synchronized. Right-click on the **ACM71** just configured and select **Telephony functions → Synchronize**.



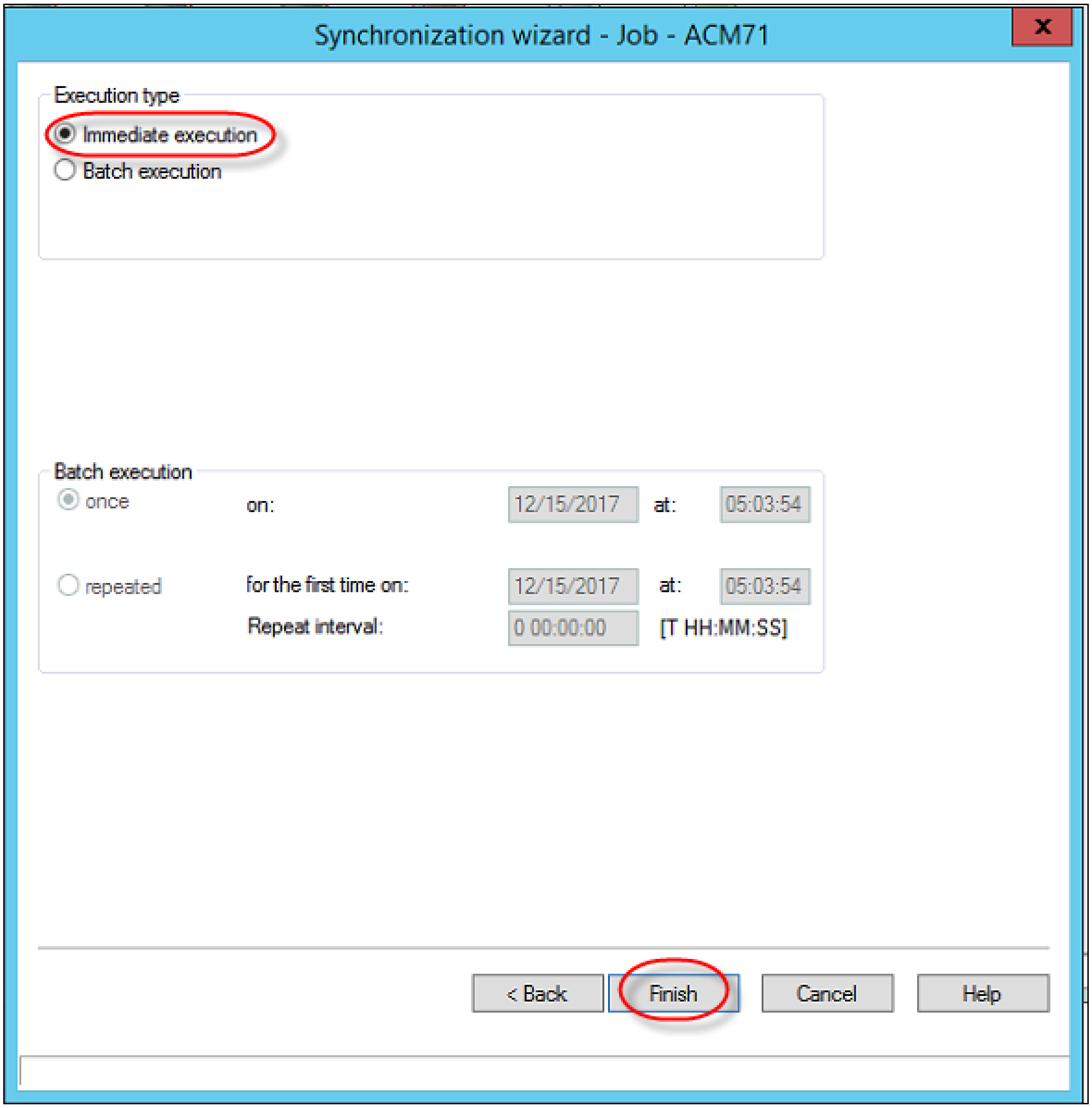
Once the **Synchronization wizard Selection** window open click on the **All telephone sets, All lists** and **All other objects** buttons followed by the **Next** button.



Selecte	Type	Descript
□	AbbreviatedDialingSystem	System speed call lists
□	AbbreviatedDialingEnhanced	Enhanced speed call lists
□	AbbreviatedDialingGroup	Groups speed call lists
□	AbbreviatedDialingPersonal	Personal speed call lists
□	HuntGroupList	Hunt Group
□	AliasStation	AliasStation
□	Cabinet	Cabinet
□	CoveragePath	Coverage Path
□	CoverageAnswerGroup	Coverage Answer Group
□	OffPbxStationMapping	OffPbxStationMapping
□	PickUpGroup	Pickup Group
□	MediaGateway	Media Gateway
□	NodeNames	Node Names
□	SiteData	Site Data
□	VDN	Virtual Dial Number(VDN)
□	Vector	Vector
□	1408	Telephone set
□	1416	Telephone set
□	1603	Telephone set
□	1608	Telephone set
□	1616	Telephone set
□	16CC	Telephone set
□	2410	Telephone set

□ Only synchronize new objects

Once the **Synchronization wizard – Job- ACM71** window opens, click on the **Immediate execution** radio button followed by the **Finish** button.



Synchronization wizard - Job - ACM71

Execution type

● Immediate execution

○ Batch execution

Batch execution

○ once on: 12/15/2017 at: 05:03:54

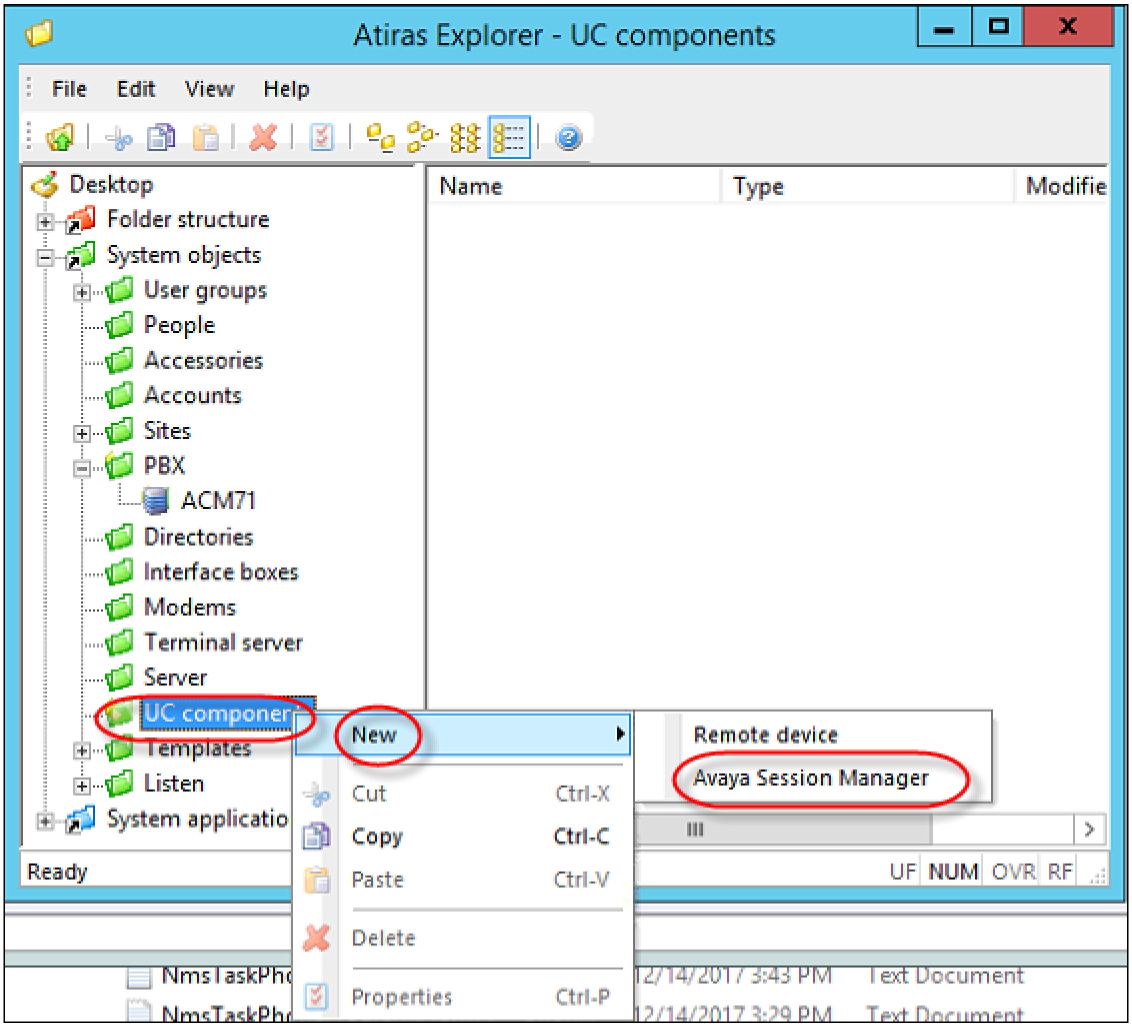
○ repeated for the first time on: 12/15/2017 at: 05:03:54

Repeat interval: 0 00:00:00 [T HH:MM:SS]

7.3. Configure Atiras for Avaya Aura® Session Manager

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

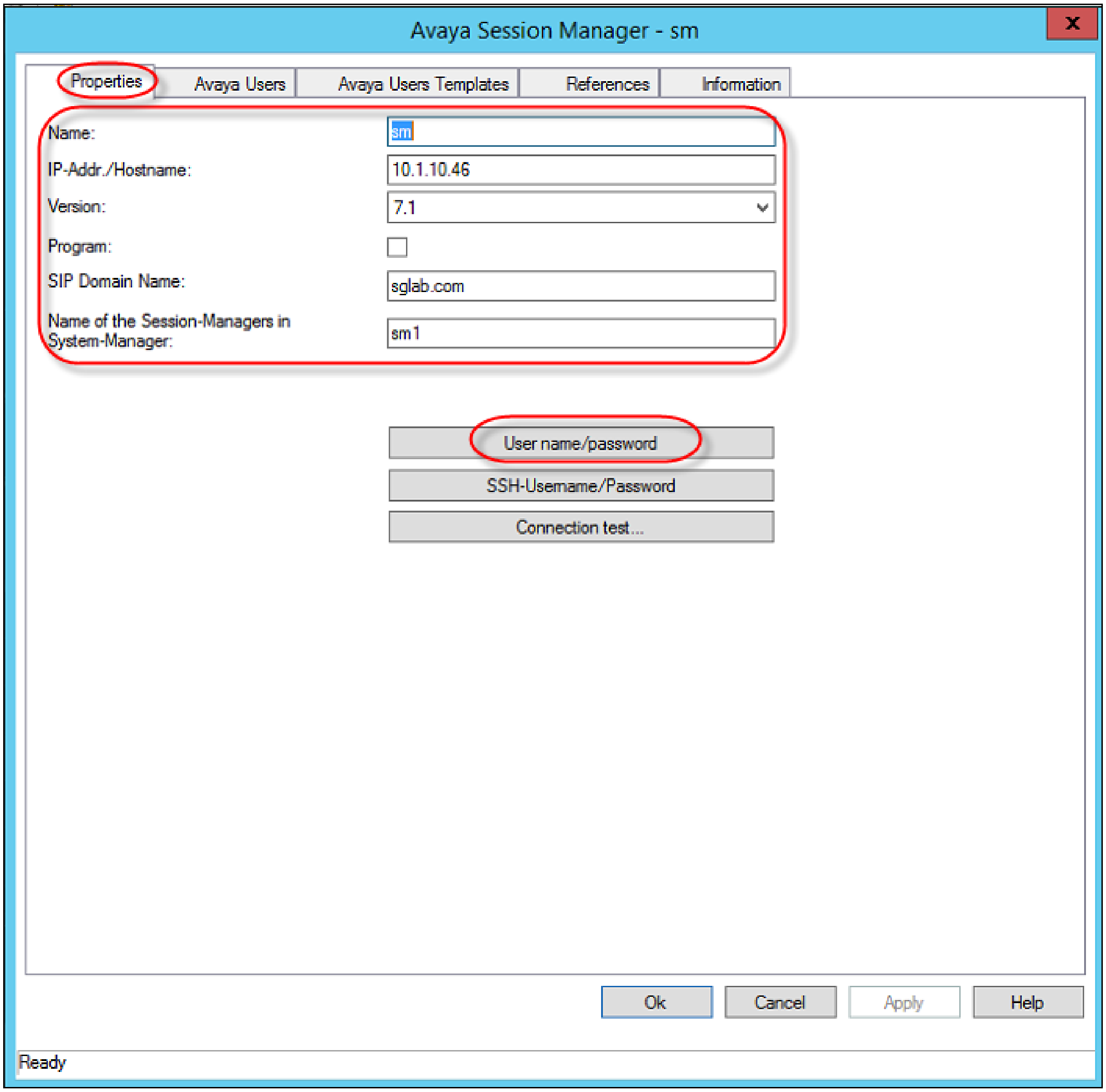
Note: Although the SIP extensions are created on Session Manager, the configurations are done via System Manager.



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. sm)
- **IP-Addr./Hostname:** Enter IP address of System Manager
- **Version:** Select **7.1** from the dropdown
- **Program:** Uncheck the check box
- **SIP Domain Name:** Enter the Domain that System Manager resides on (During compliance testing the Domain was **sglab.com**)
- **Name of the Session-Manager in System-Manager:** Enter the Session Manager name. (During compliance testing the Session Manager name was **sm1**)

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



Name: sm

IP-Addr./Hostname: 10.1.10.46

Version: 7.1

Program: □

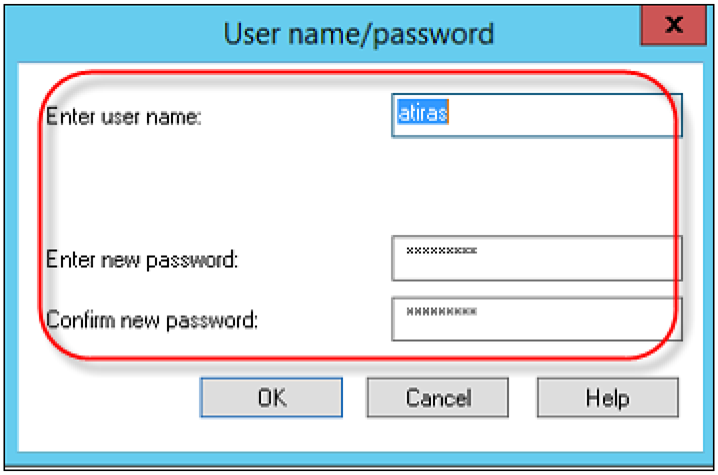
SIP Domain Name: sglab.com

Name of the Session-Managers in System-Manager: sm1

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.



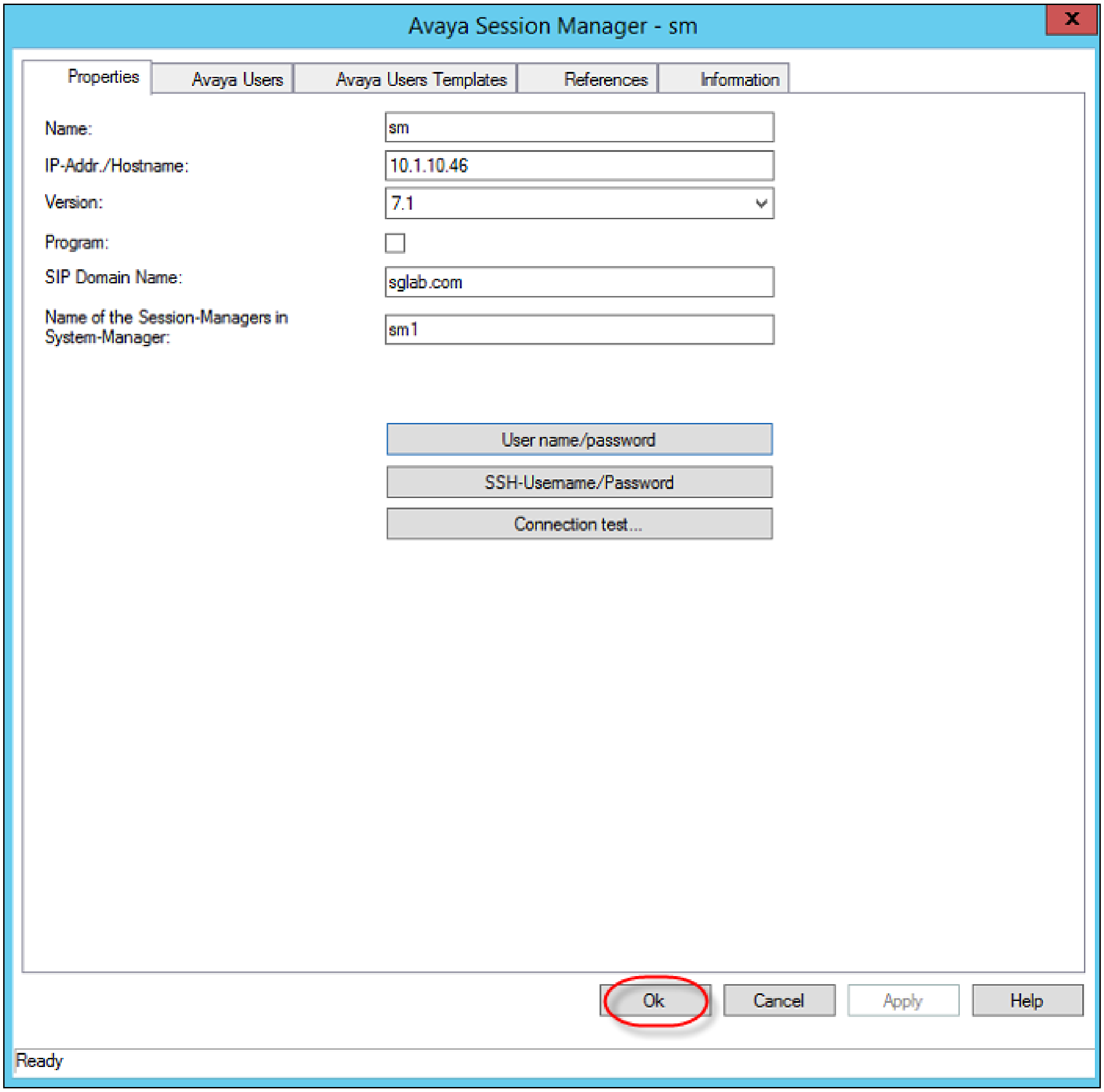
User name/password

Enter user name: atiras

Enter new password: **********

Confirm new password: **********

Click on the **OK** button again.



Name: sm

IP-Addr./Hostname: 10.1.10.46

Version: 7.1

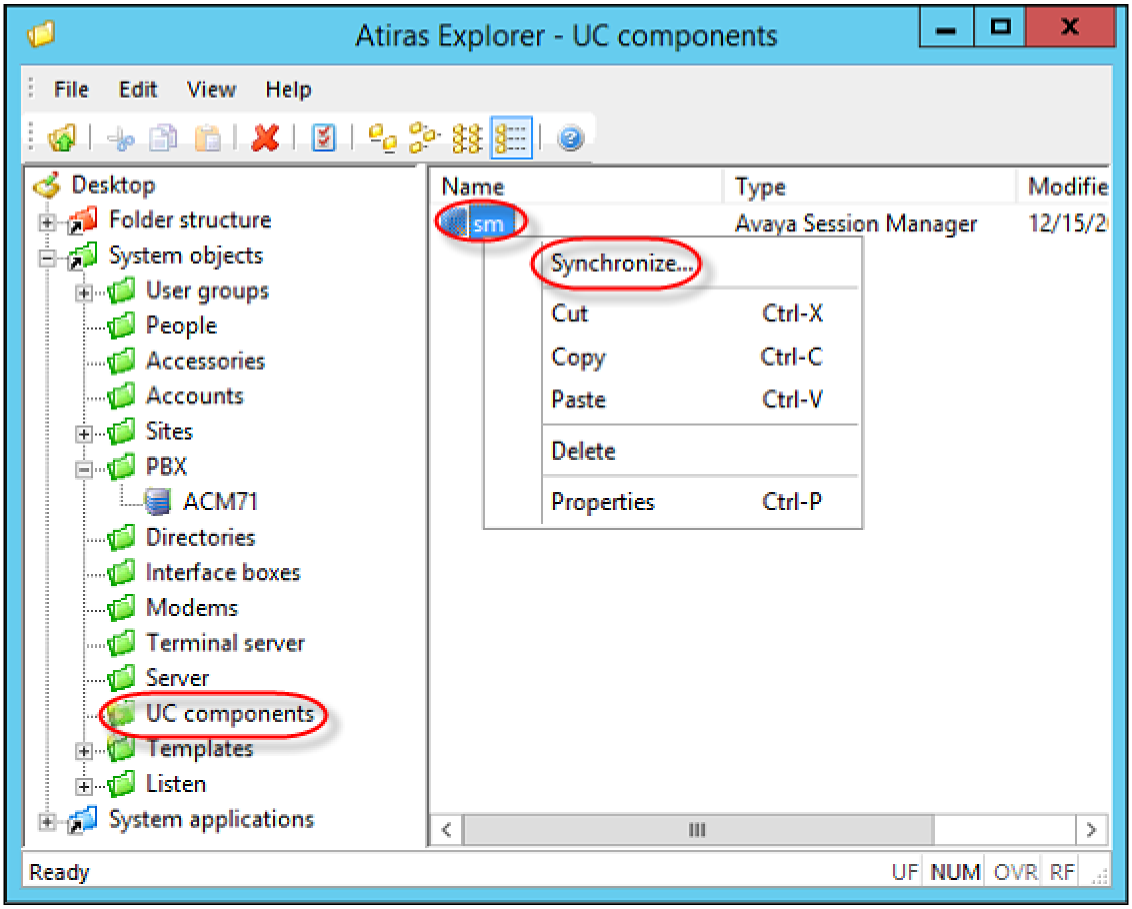
Program: □

SIP Domain Name: sglab.com

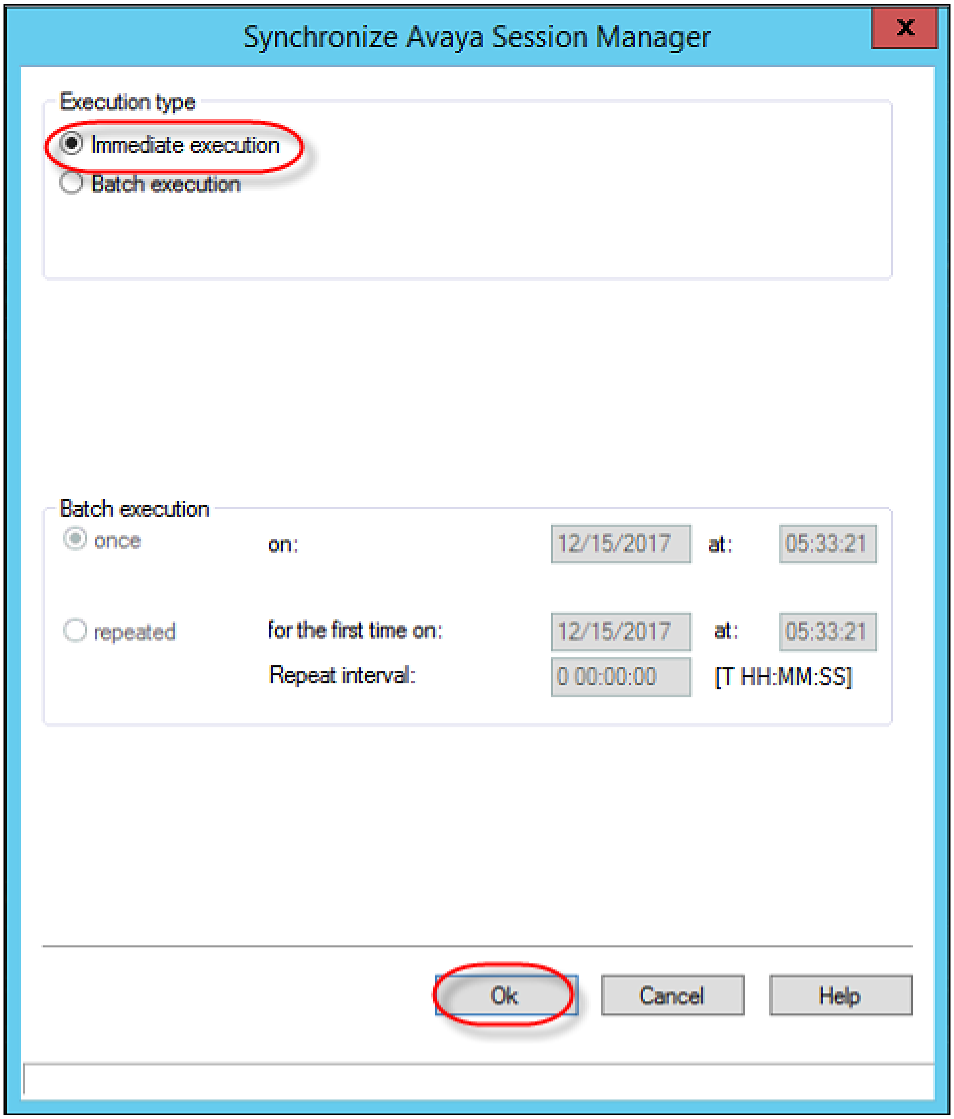
Name of the Session-Managers in System-Manager: sm1

7.4. Synchronize Avaya Aura® Session Manager

Once the Session Manager is configured it must be synchronized. Right-click on Session Manager just configured (sm as configured in **Section 7.3** and select **Synchronize**.



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



Execution type

● Immediate execution
○ Batch execution

Batch execution

○ once on: 12/15/2017 at: 05:33:21

○ repeated for the first time on: 12/15/2017 at: 05:33:21

Repeat interval: 0 00:00:00 [T HH:MM:SS]

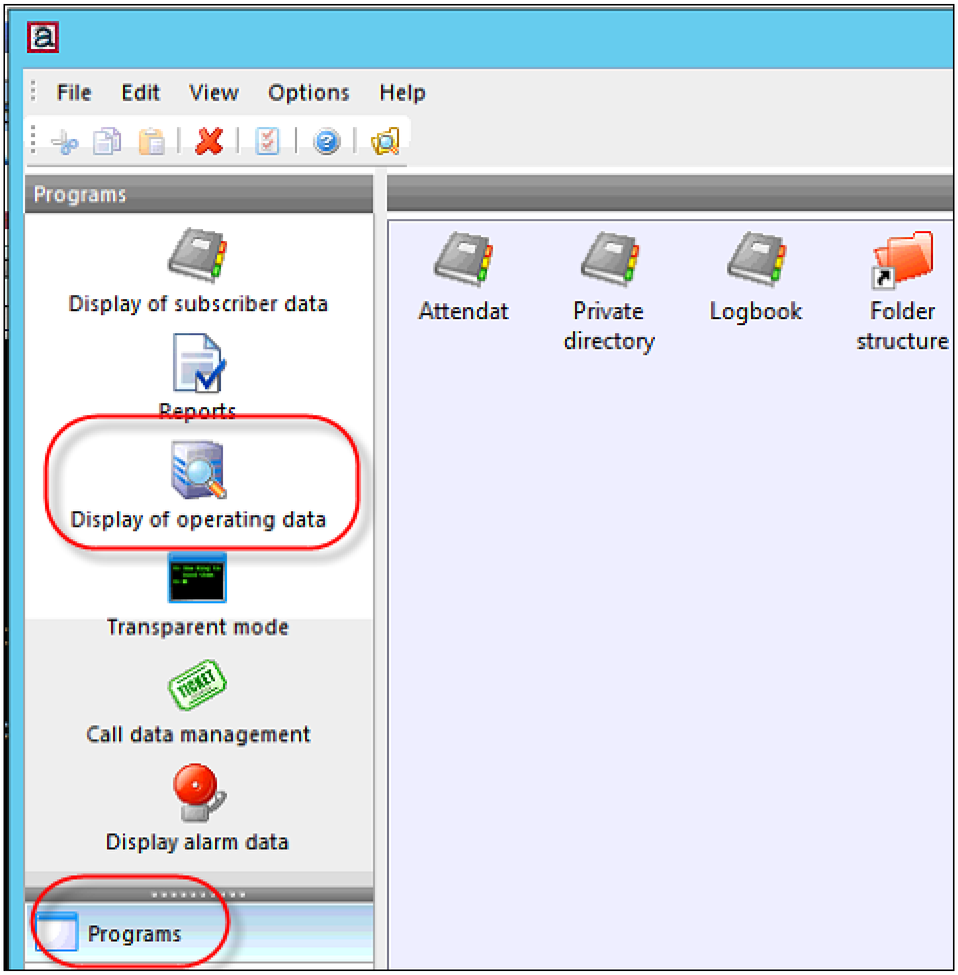
8. Configuration of Atiras Attendant Console module

This section describes the steps preformed to configure the Atiras Attendant Console module. It is implied that the Atiras 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:

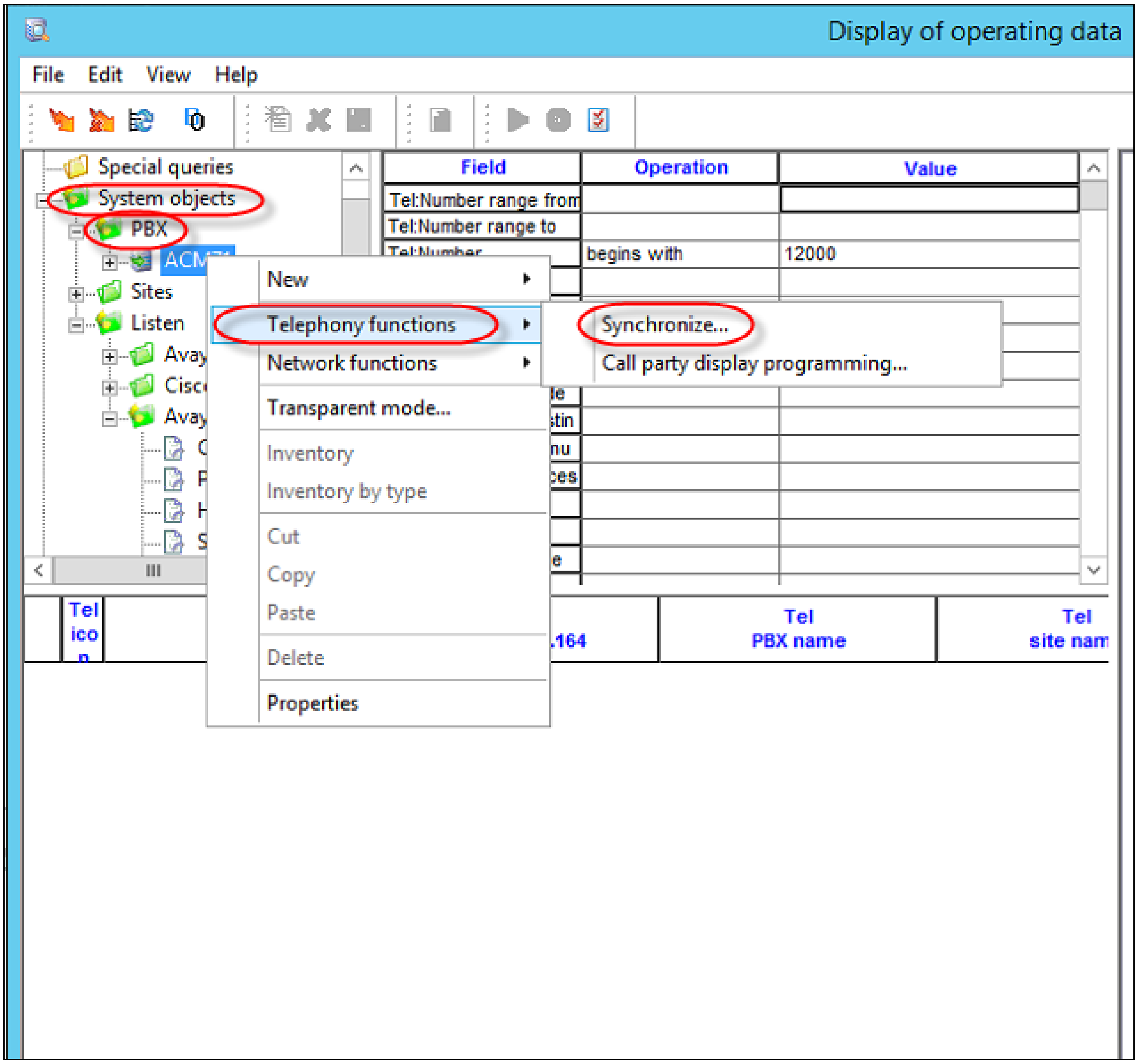
- Synchronize VDN and Vector
- Associate Attendant extension with Atiras (Frox) Attendant Console
- Create a Super User for Attendant
- Configuring the Atiras Attendant Console
- Configure Atiras Attendant Console to connect to Avaya Application Enablement Services
- Restart the Nms Attendant Console

8.1. 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** (not shown) and log in with the appropriate credentials. Once the **Atiras Desktop** opens, click on the **Programs → Display of operating data**.

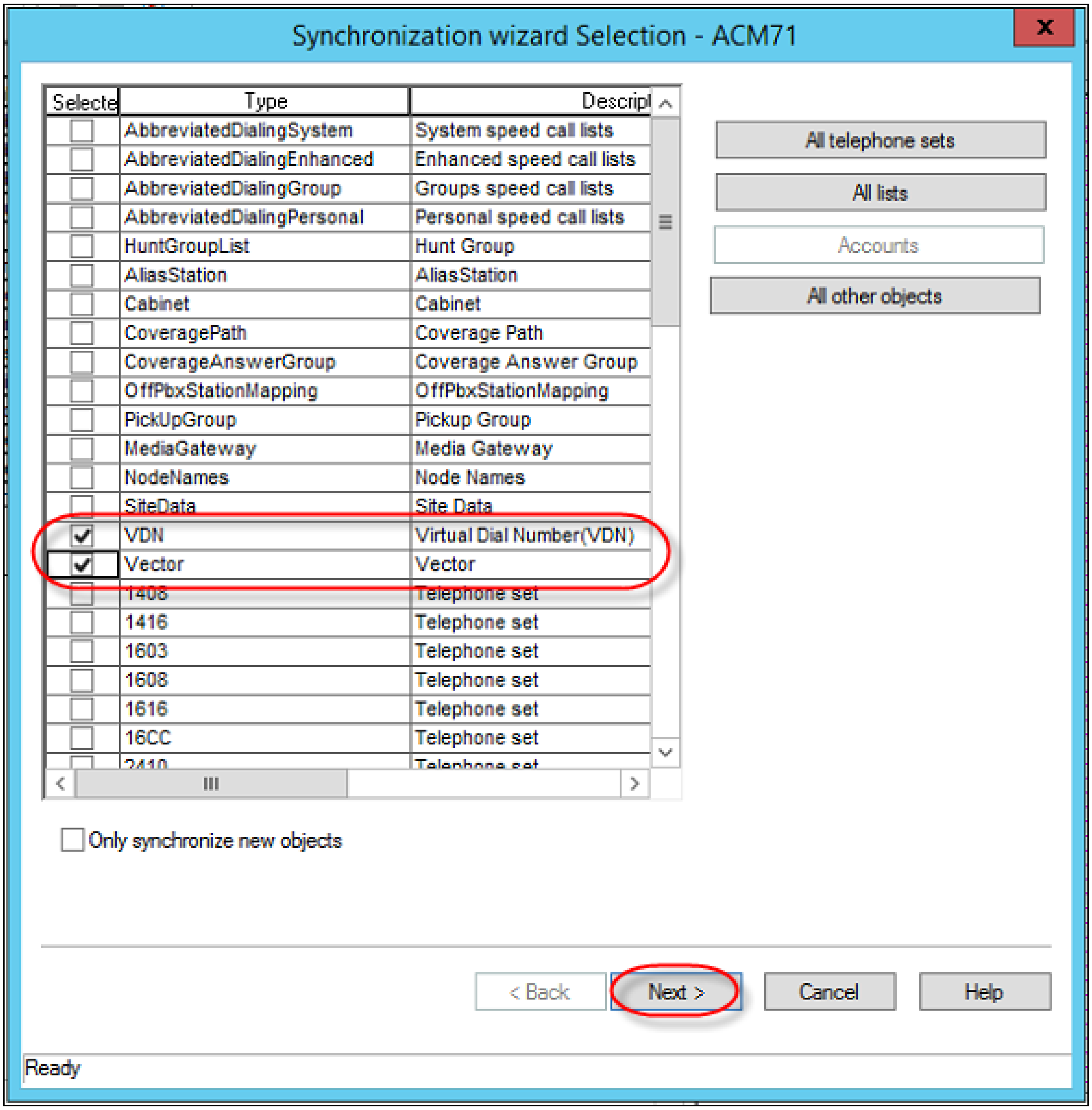


Once the **Display of operating data** window opens, navigate to **System objects → PBX →ACM71** and select **Telephony functions → Synchronize**.



Field	Operation	Value
Tel:Number range from		
Tel:Number range to		
Tel:Number	begins with	12000

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



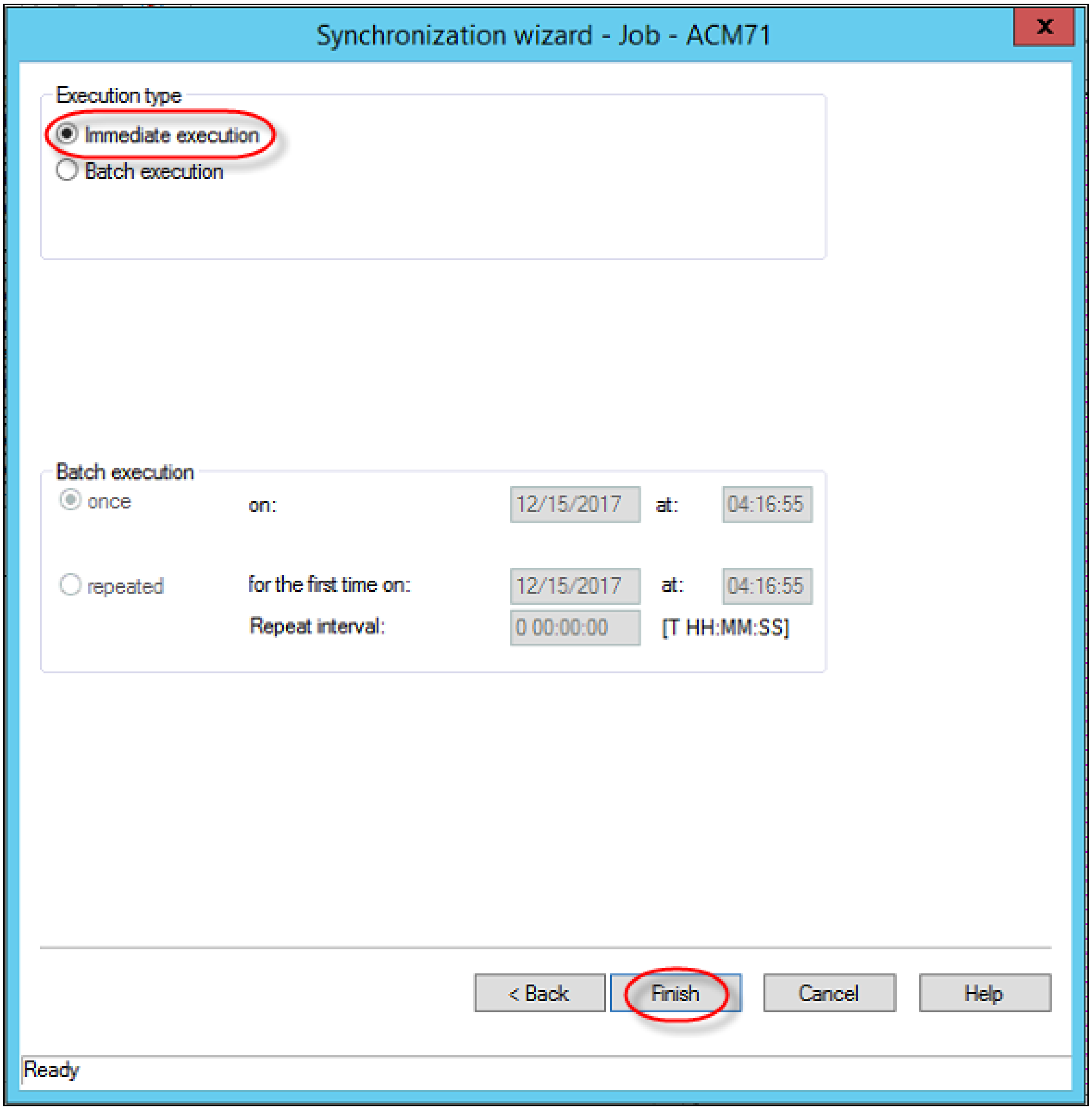
Synchronization wizard Selection - ACM71

Selecte	Type	Descript
□	AbbreviatedDialingSystem	System speed call lists
□	AbbreviatedDialingEnhanced	Enhanced speed call lists
□	AbbreviatedDialingGroup	Groups speed call lists
□	AbbreviatedDialingPersonal	Personal speed call lists
□	HuntGroupList	Hunt Group
□	AliasStation	AliasStation
□	Cabinet	Cabinet
□	CoveragePath	Coverage Path
□	CoverageAnswerGroup	Coverage Answer Group
□	OffPbxStationMapping	OffPbxStationMapping
□	PickUpGroup	Pickup Group
□	MediaGateway	Media Gateway
□	NodeNames	Node Names
□	SiteData	Site Data
☑	VDN	Virtual Dial Number(VDN)
☑	Vector	Vector
□	1408	Telephone set
□	1416	Telephone set
□	1603	Telephone set
□	1608	Telephone set
□	1616	Telephone set
□	16CC	Telephone set
□	2410	Telephone set

□ Only synchronize new objects

Ready

Once the **Synchronization wizard - Job – ACM71** window opens, click on the **Immediate execution** radio button followed by the **Finish** button.



Synchronization wizard - Job - ACM71

Execution type

● Immediate execution

○ Batch execution

Batch execution

○ once on: 12/15/2017 at: 04:16:55

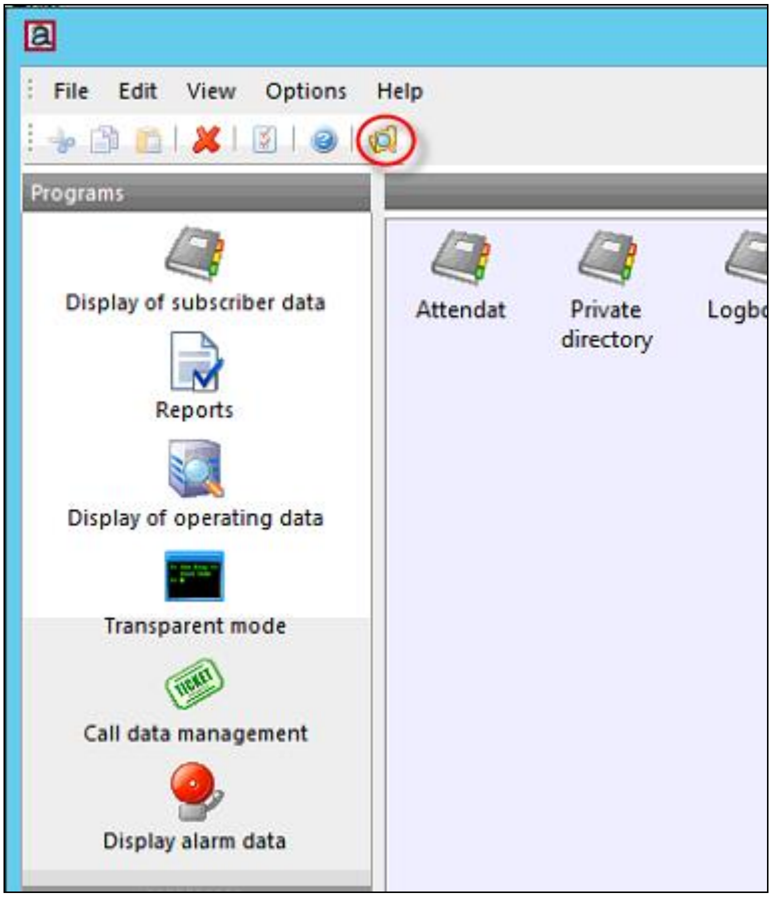
○ repeated for the first time on: 12/15/2017 at: 04:16:55

Repeat interval: 0 00:00:00 [T HH:MM:SS]

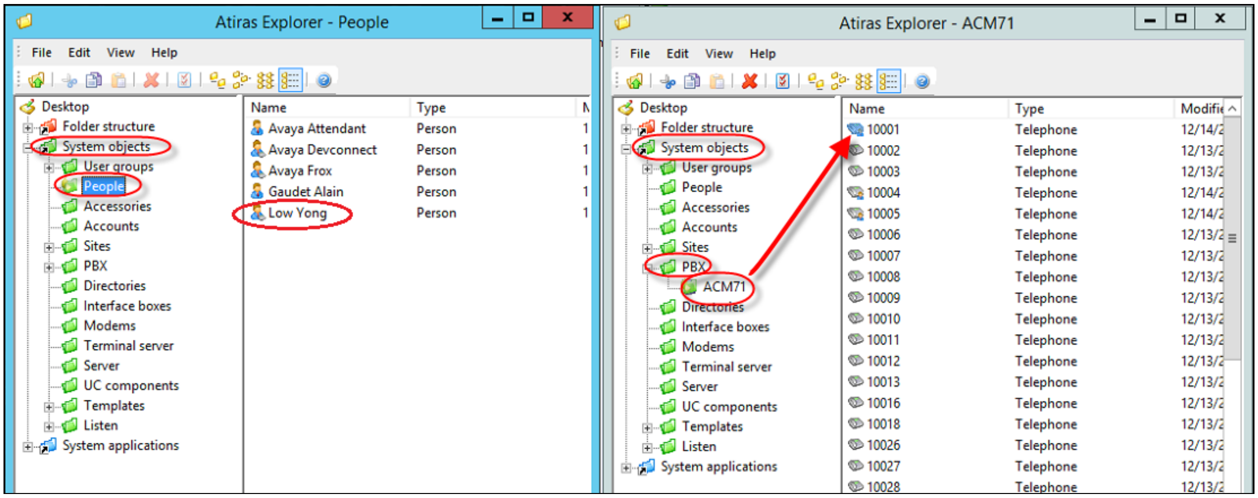
Ready

8.2. 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 → ACM71**. Drag the extension used for the Attendant console (During compliance testing extension **10001** was used) from the **Atiras Explorer ACM71** window to **Low Yong** in the **Atiras Explorer People** window.



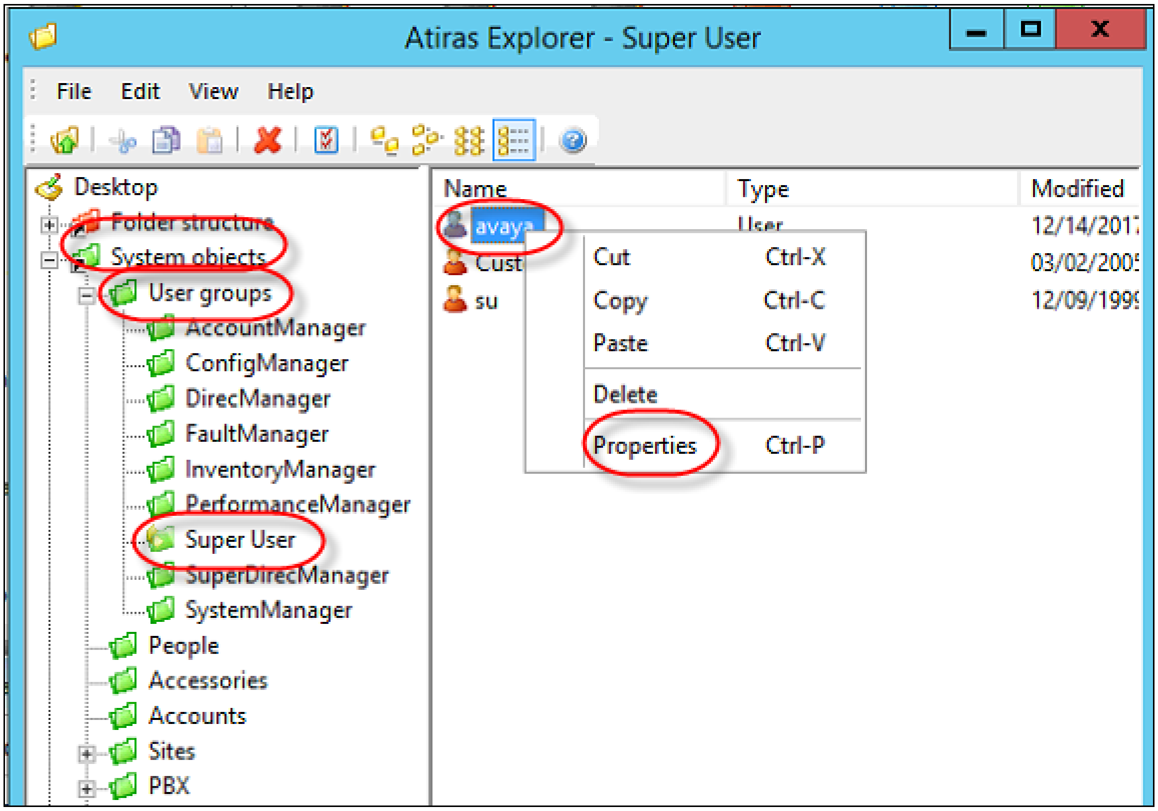
Name	Type	N
Avaya Attendant	Person	1
Avaya Devconnect	Person	1
Avaya Frox	Person	1
Gaudet Alain	Person	1
Low Yong	Person	1

Name	Type	Modifie
10001	Telephone	12/14/2
10002	Telephone	12/13/2
10003	Telephone	12/13/2
10004	Telephone	12/14/2
10005	Telephone	12/14/2
10006	Telephone	12/13/2
10007	Telephone	12/13/2
10008	Telephone	12/13/2
10009	Telephone	12/13/2
10010	Telephone	12/13/2
10011	Telephone	12/13/2
10012	Telephone	12/13/2
10013	Telephone	12/13/2
10016	Telephone	12/13/2
10018	Telephone	12/13/2
10026	Telephone	12/13/2
10027	Telephone	12/13/2
10028	Telephone	12/13/2

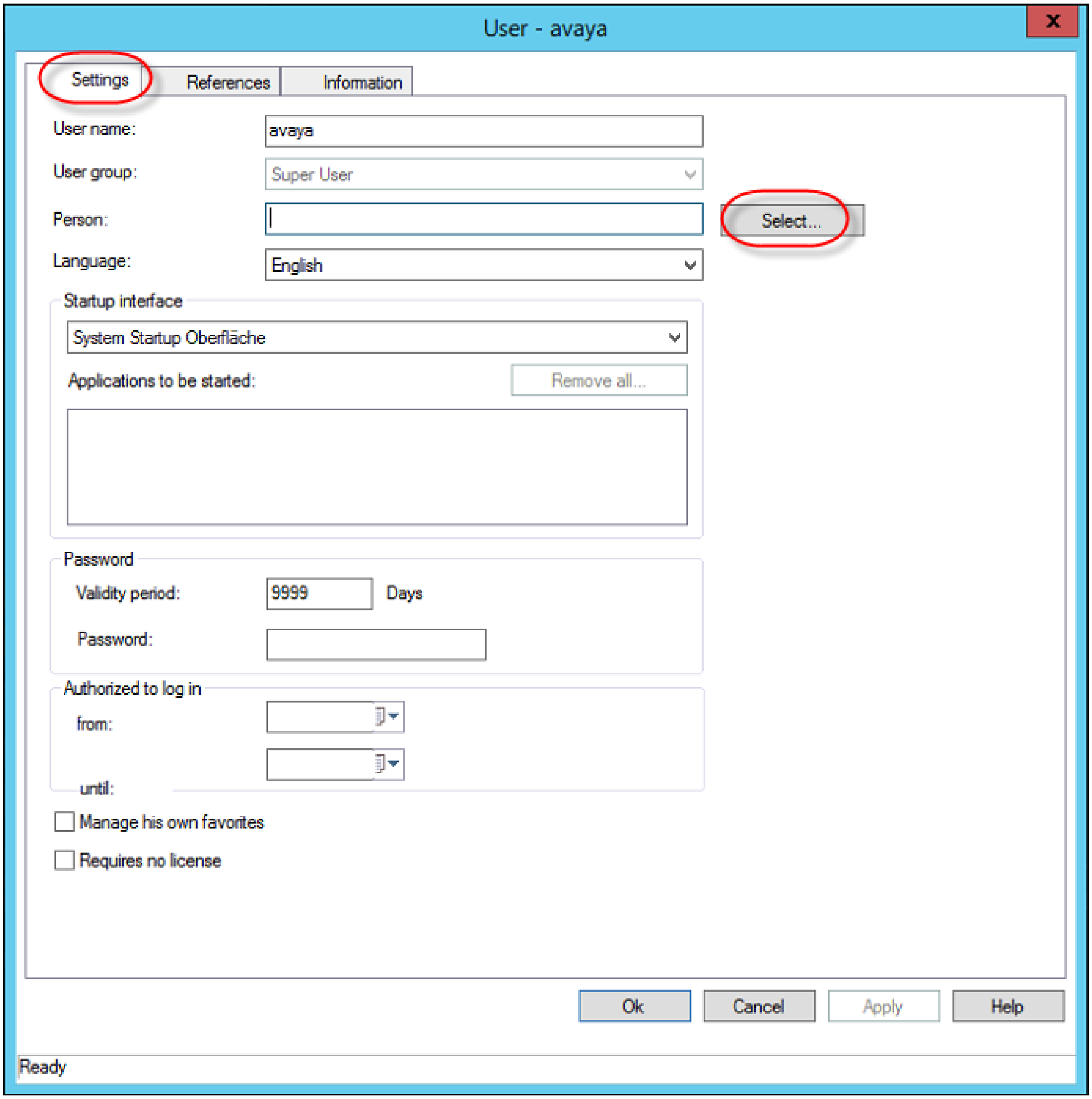
8.3. Create a Super User for the Attendant

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

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



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



User - avaya

User name: avaya

User group: Super User

Person:

Language: English

Startup interface: System Startup Oberfläche

Applications to be started:

Password

Validity period: 9999 Days

Password:

Authorized to log in

from:

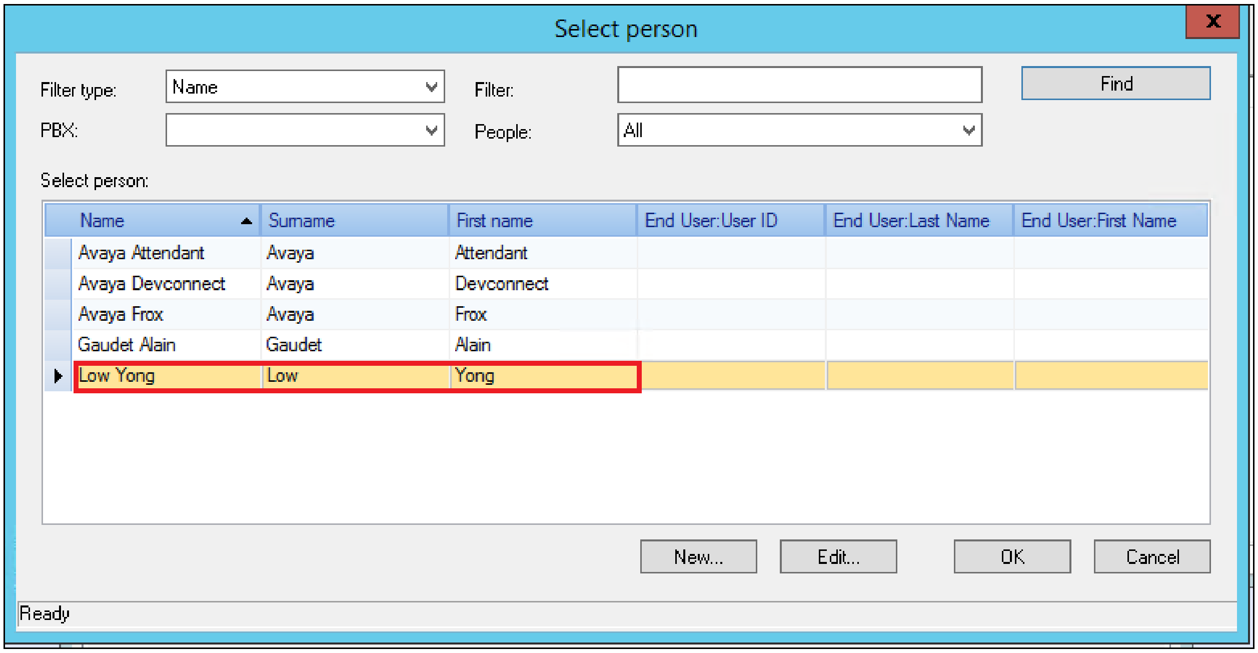
until:

□ Manage his own favorites

□ Requires no license

Ready

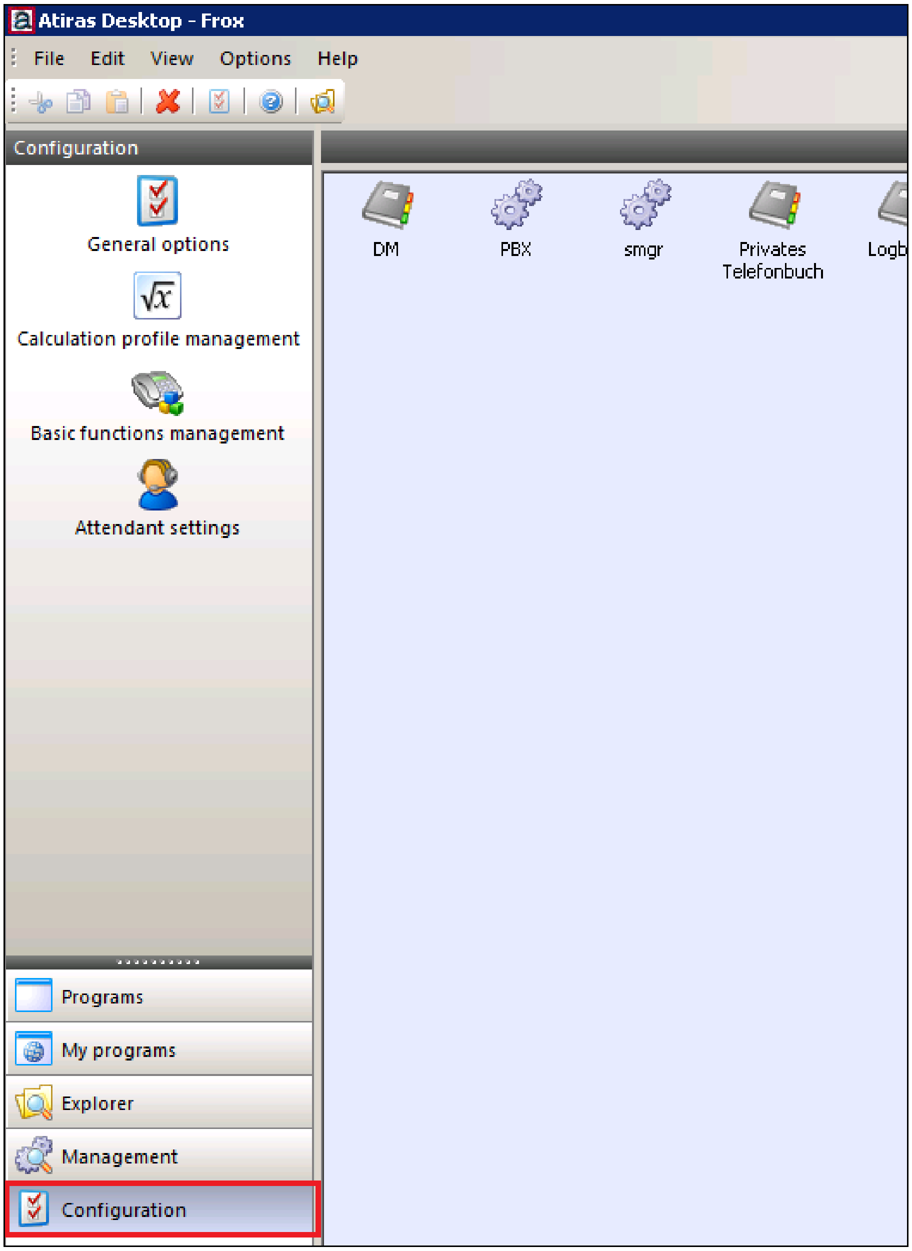
Once the **Select Person** window opens, click on the **Find** button and select **Low Yong** followed by the **OK** button.



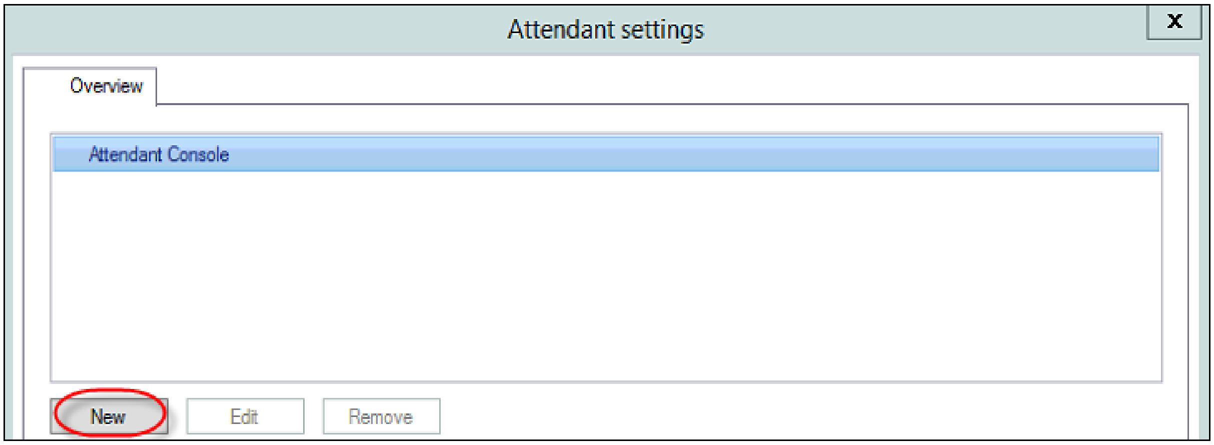
	Name	Surname	First name	End User:User ID	End User:Last Name	End User:First Name
	Avaya Attendant	Avaya	Attendant			
	Avaya Devconnect	Avaya	Devconnect			
	Avaya Frox	Avaya	Frox			
	Gaudet Alain	Gaudet	Alain			
▶	Low Yong	Low	Yong			

8.4. Configuring the Atiras Attendant Console

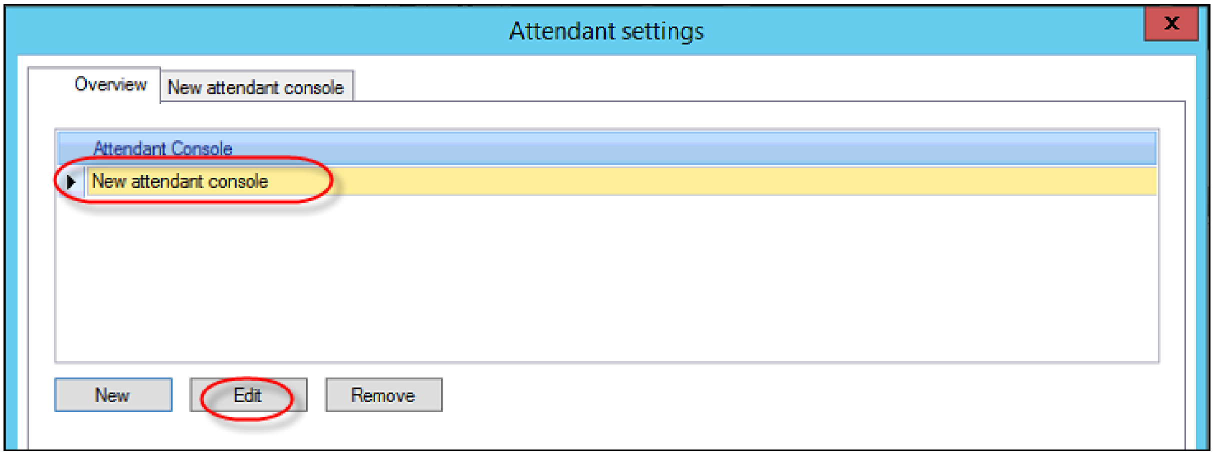
From the **Atiras Desktop** window, select **Configuration**.



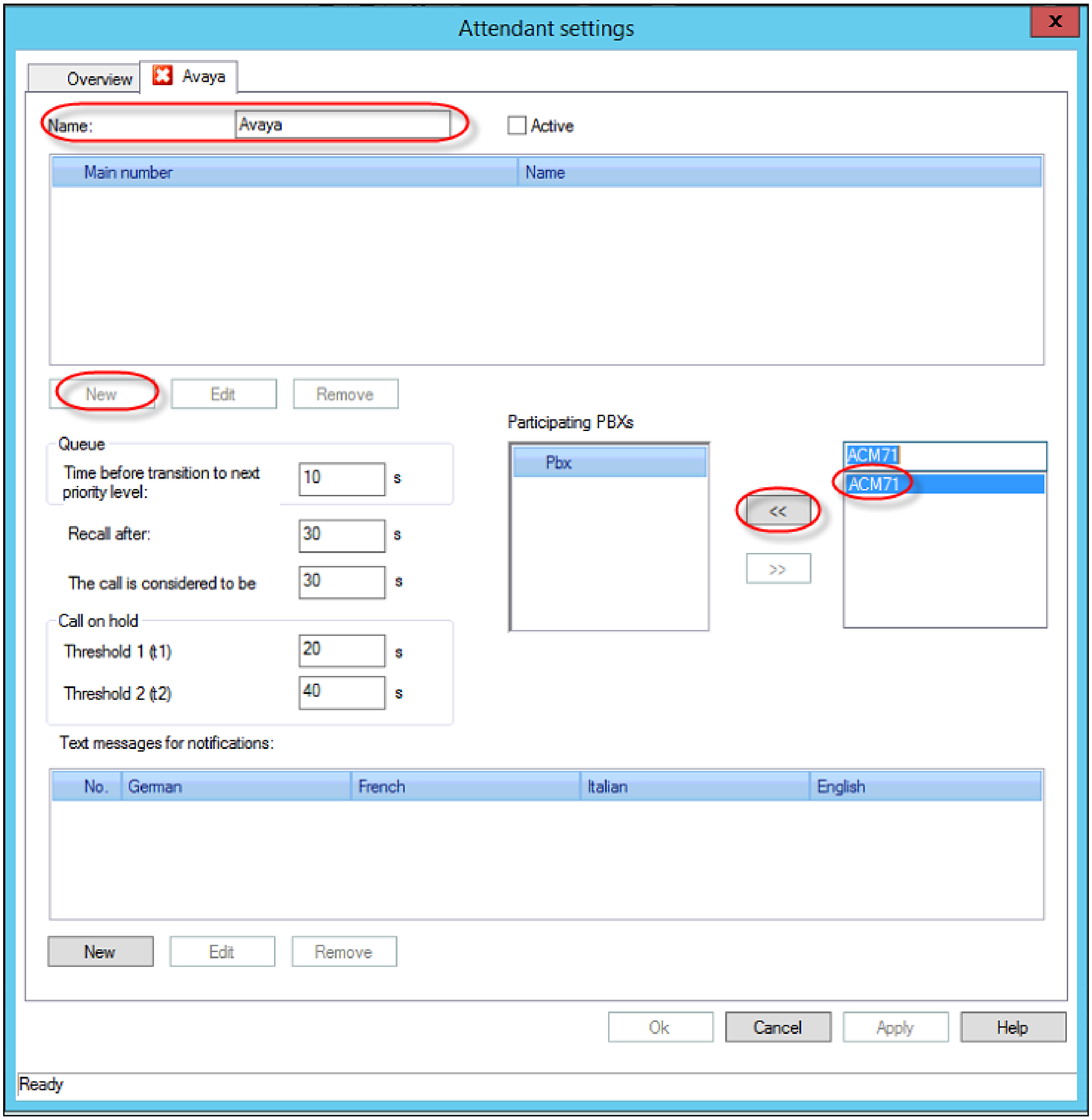
Once the **Attendant settings** window opens, select **New**.



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



When the next window opens, enter an informative name (i.e. Avaya) in the **Name** box. Select **ACM71** and click on left arrow (<<) to move it into **Participating PBXs**. Click on the **New** button.



Attendant settings

Name: Avaya

□ Active

Main number	Name

Queue

Time before transition to next priority level: 10 s

Recall after: 30 s

The call is considered to be 30 s

Call on hold

Threshold 1 (t1) 20 s

Threshold 2 (t2) 40 s

Participating PBXs

Pbx

ACM71

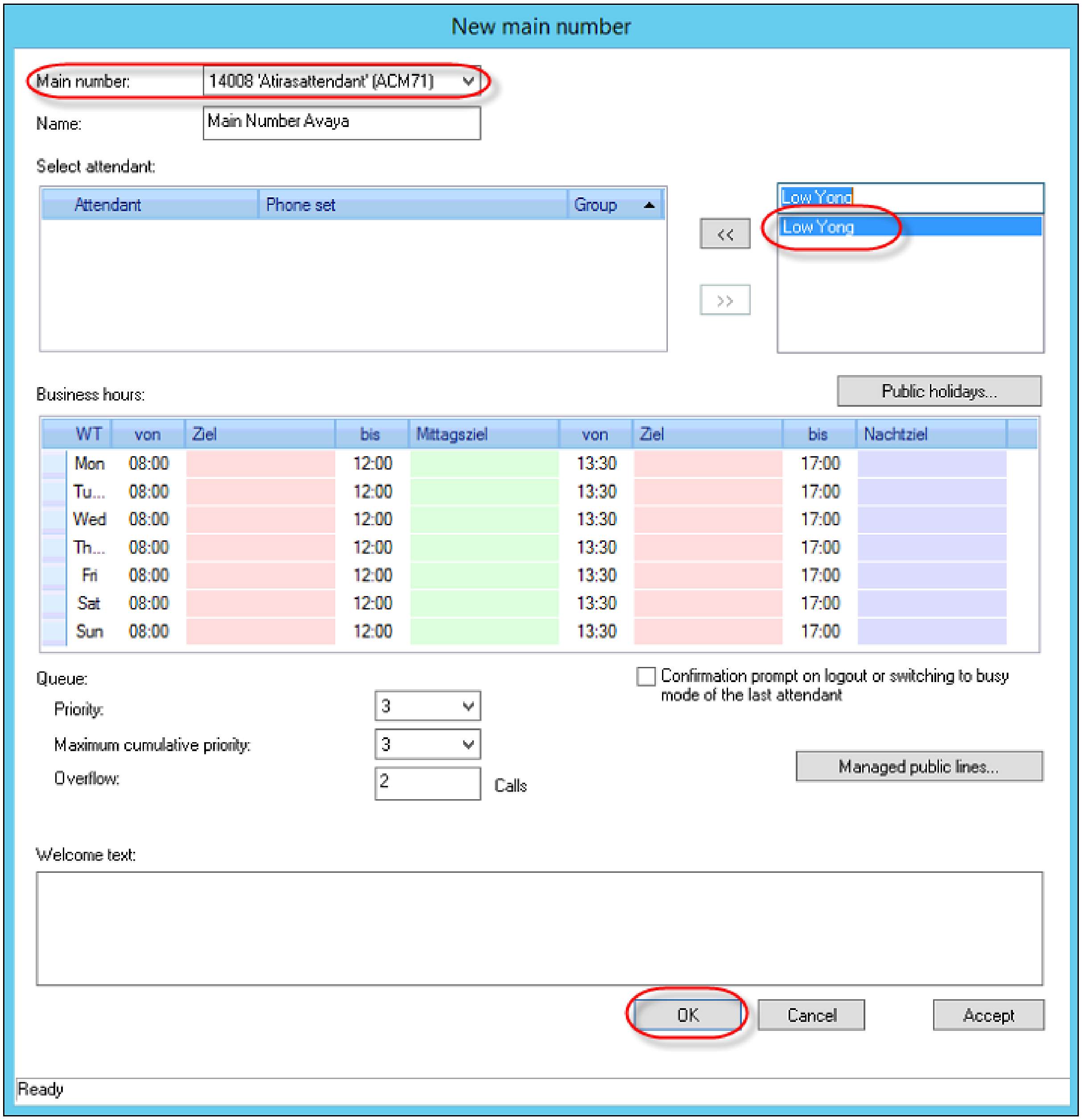
ACM71

Text messages for notifications:

No.	German	French	Italian	English

Ready

Once the **New main number** windows opens, select **14008 'Atirasattendant' (ACM71)** (configured in **Section 5.6**). Select person and click on left arrow (<<) to move it into **Select attendant** pane. Click on the **OK** button.



New main number

Main number: 14008 'Atirasattendant' (ACM71)

Name: Main Number Avaya

Select attendant:

Attendant	Phone set	Group

Low Yong

Low Yong

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

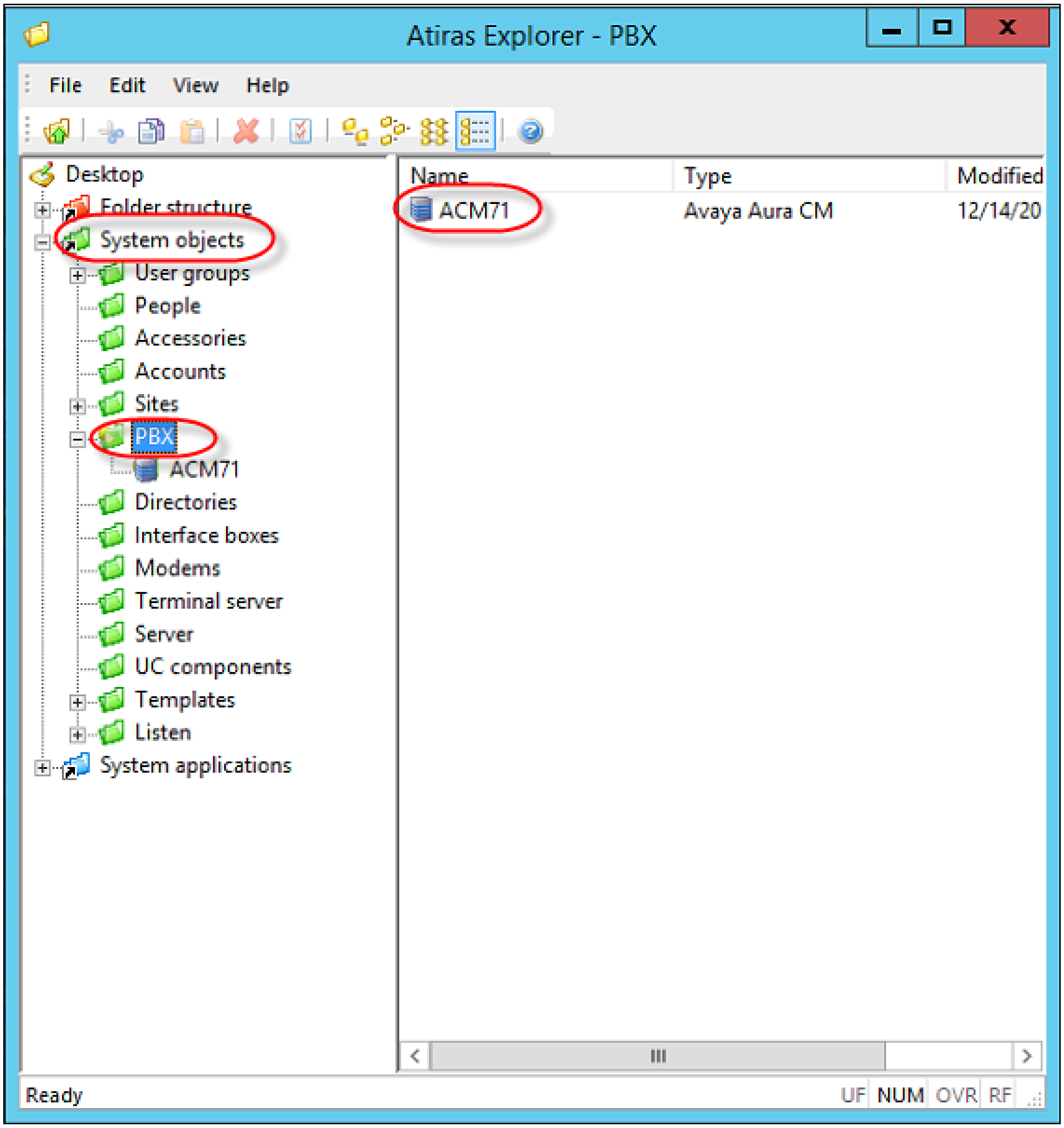
□ Confirmation prompt on logout or switching to busy mode of the last attendant

Welcome text:

Ready

8.5. Configure Atiras Attendant Console to connect to Avaya Aura® Application Enablement Services

To configure Atiras Attendant to connect to the Avaya Application Enablement Services, navigate to **System objects → PBX**. Right-click on **ACM71** and select **Properties** (not shown).

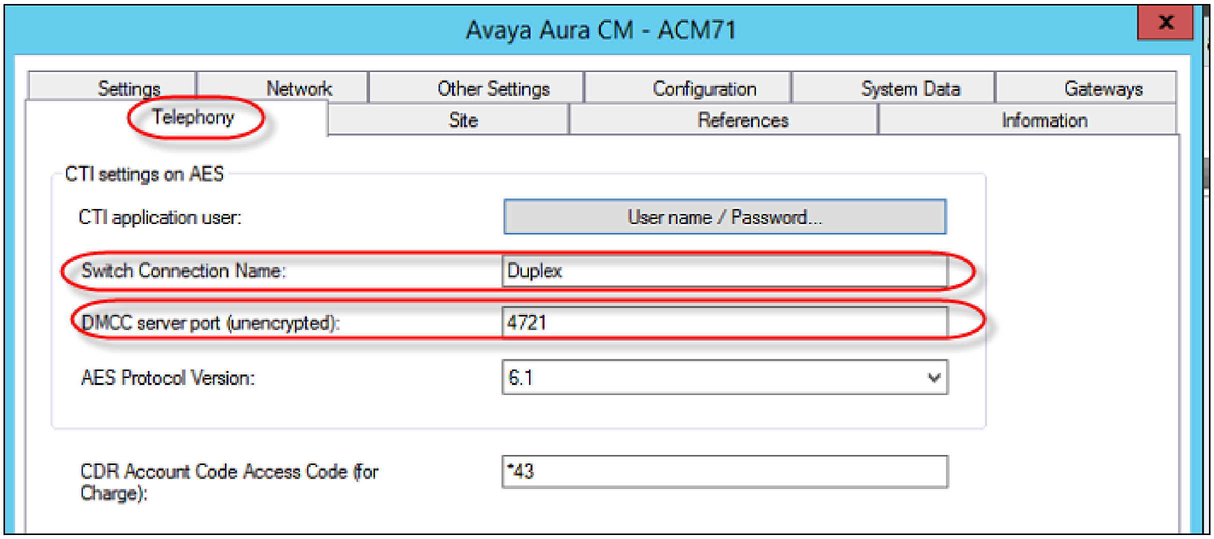


Name	Type	Modified
ACM71	Avaya Aura CM	12/14/20

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** (i.e. Duplex)
- **DMCC server port:** Enter the DMCC port as configured in **Section 6.9** (4721)

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



CTI settings on AES

CTI application user:

Switch Connection Name: Duplex

DMCC server port (unencrypted): 4721

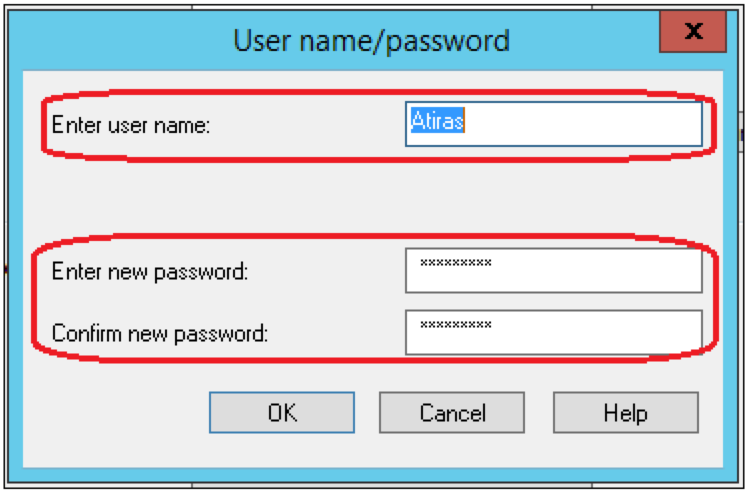
AES Protocol Version: 6.1

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

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

- **Enter user name:** Enter the CTI User as configured in **Section 6.7** (Atiras)
- **Enter new password:** Enter the CTI user password as configured in **Section 6.7**
- **Confirm new password** Confirm the password

Click on the **OK** button.

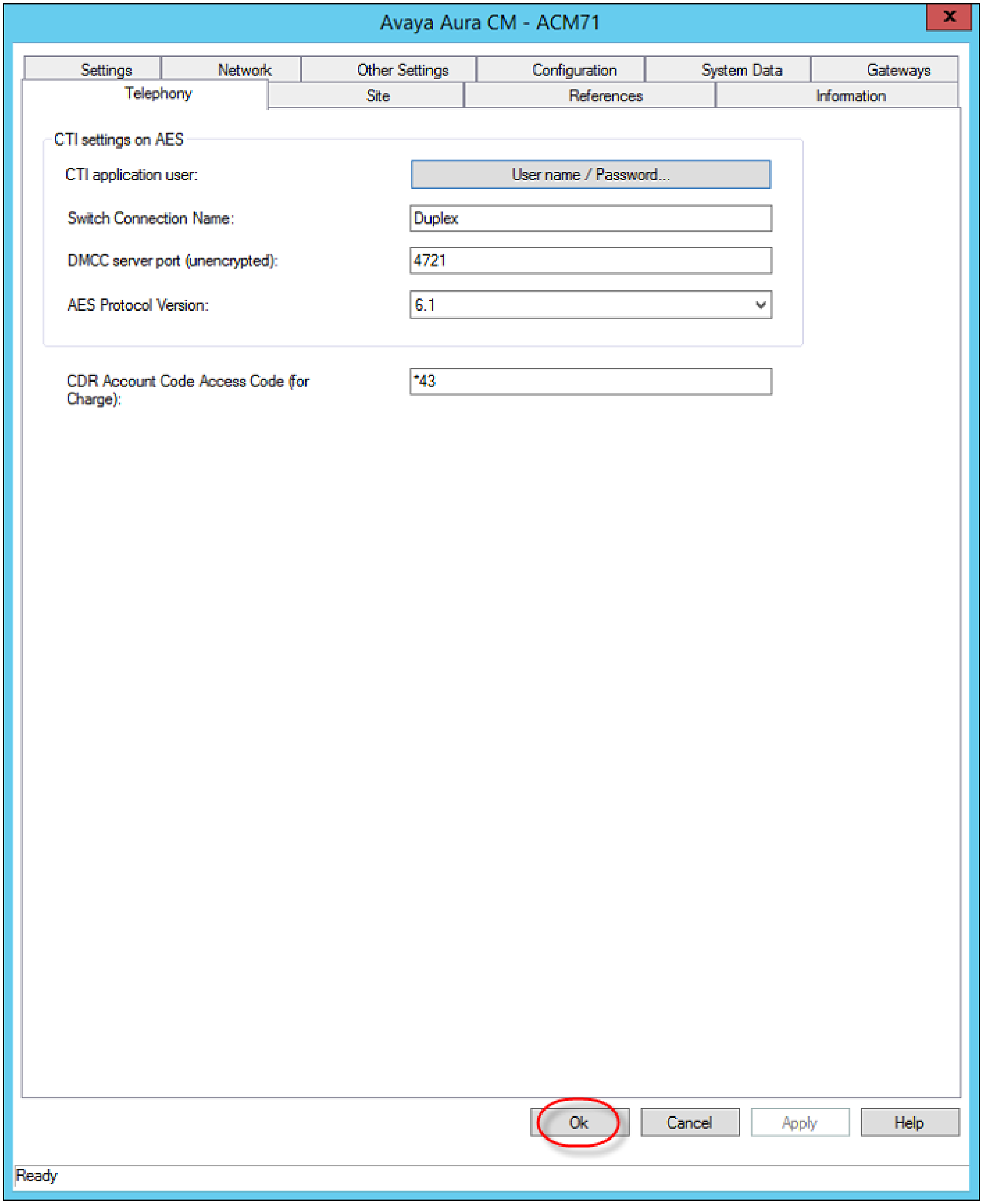


Enter user name: Atiras

Enter new password: *********

Confirm new password: *********

Click the **Ok** button again.



CTI settings on AES

CTI application user: User name / Password...

Switch Connection Name: Duplex

DMCC server port (unencrypted): 4721

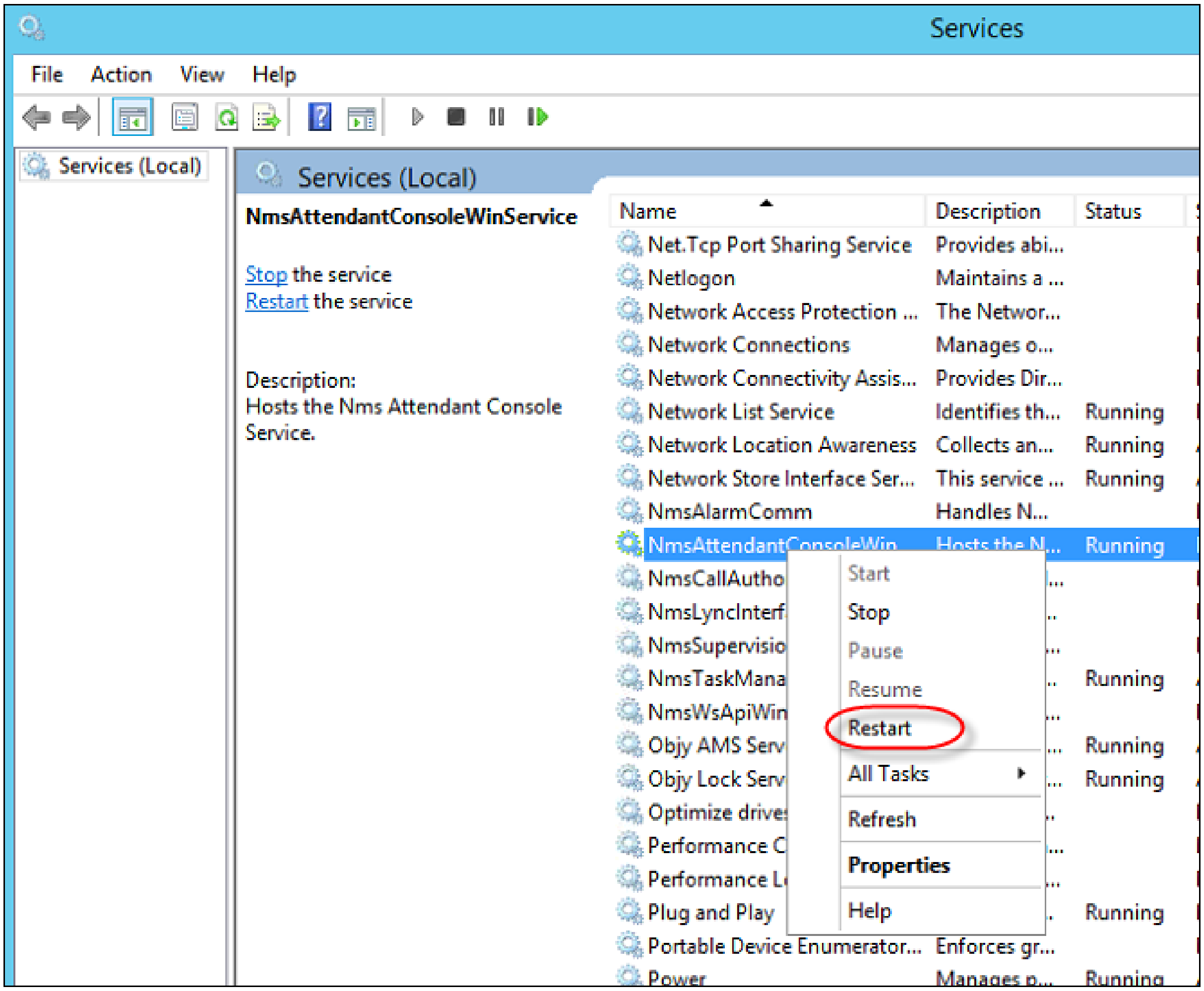
AES Protocol Version: 6.1

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

8.6. Restart the Nms Attendant Console

Once the Atiras 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**.



NmsAttendantConsoleWinService

Stop the service
Restart the service

Description:
Hosts the Nms Attendant Console Service.

Name	Description	Status
Net.Tcp Port Sharing Service	Provides abi...	
Netlogon	Maintains a ...	
Network Access Protection ...	The Networ...	
Network Connections	Manages o...	
Network Connectivity Assis...	Provides Dir...	
Network List Service	Identifies th...	Running
Network Location Awareness	Collects an...	Running
Network Store Interface Ser...	This service ...	Running
NmsAlarmComm	Handles N...	
NmsAttendantConsoleWin	Hosts the N...	Running
NmsCallAutho	...	
NmsLyncInterf	..	
NmsSupervisio	...	
NmsTaskMana	..	Running
NmsWsApiWin	...	
Objy AMS Serv	...	Running
Objy Lock Serv	...	Running
Optimize drive	..	
Performance C	...	
Performance L	...	
Plug and Play	.	Running
Portable Device Enumerator...	Enforces gr...	
Power	Manages p...	Running

9. Verification Steps

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

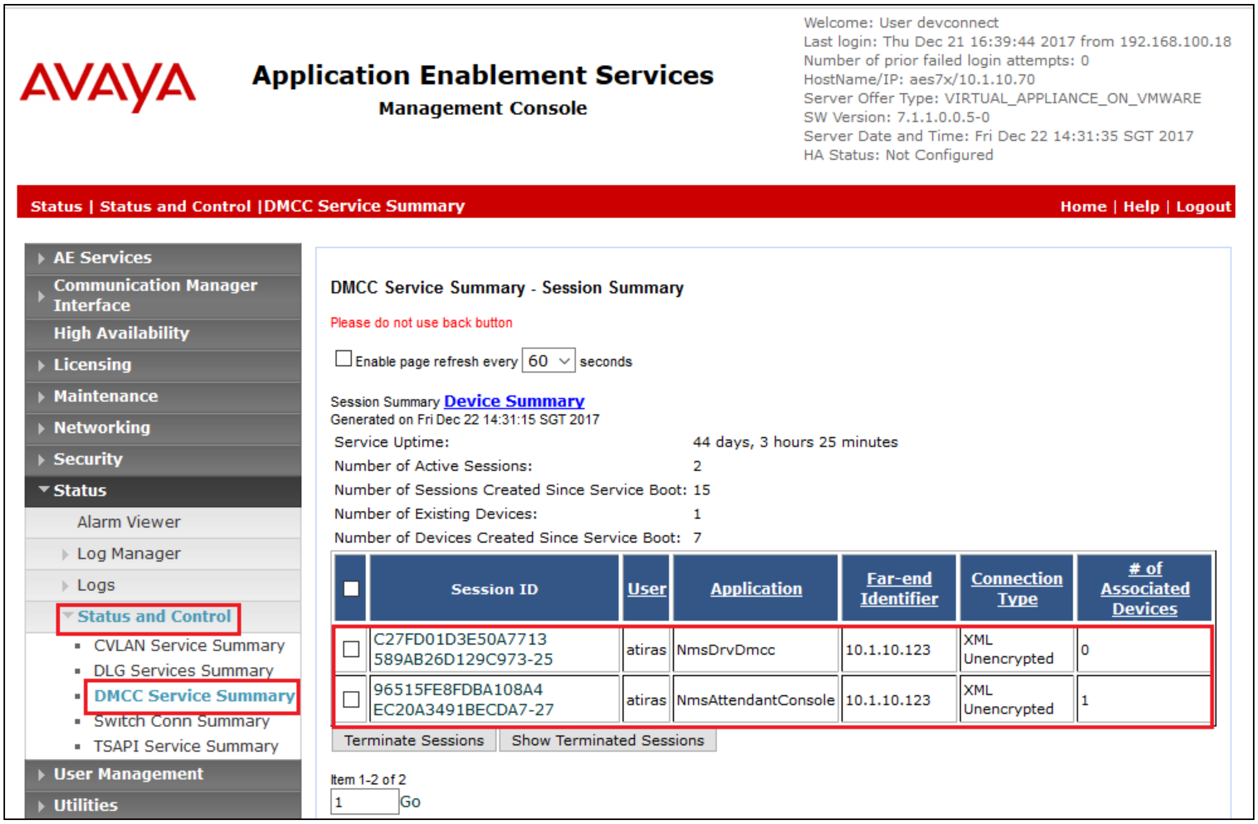
9.1. Verify Avaya Aura® Communication Manager CTI Service State

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 aesvcs cti-link**. The CTI link is **3**.Verify the **Service State** of the CTI link is **established.**

```
status aesvcs cti-link

                          AE SERVICES CTI LINK STATUS

CTI   Version  Mnt   AE Services      Service       Msgs     Msgs
Link           Busy  Server           State         Sent     Rcvd

3     8        no    aes7x            established   74       74
```

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 connections to **atiras** and the **Far-end Identifier** of the Atiras server **10.1.10.123** as expected.



Welcome: User devconnect
Last login: Thu Dec 21 16:39:44 2017 from 192.168.100.18
Number of prior failed login attempts: 0
HostName/IP: aes7x/10.1.10.70
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.1.0.0.5-0
Server Date and Time: Fri Dec 22 14:31:35 SGT 2017
HA Status: Not Configured

DMCC Service Summary - Session Summary

Please do not use back button

□ Enable page refresh every 60 seconds

Session Summary Device Summary
Generated on Fri Dec 22 14:31:15 SGT 2017

Service Uptime:	44 days, 3 hours 25 minutes
Number of Active Sessions:	2
Number of Sessions Created Since Service Boot:	15
Number of Existing Devices:	1
Number of Devices Created Since Service Boot:	7

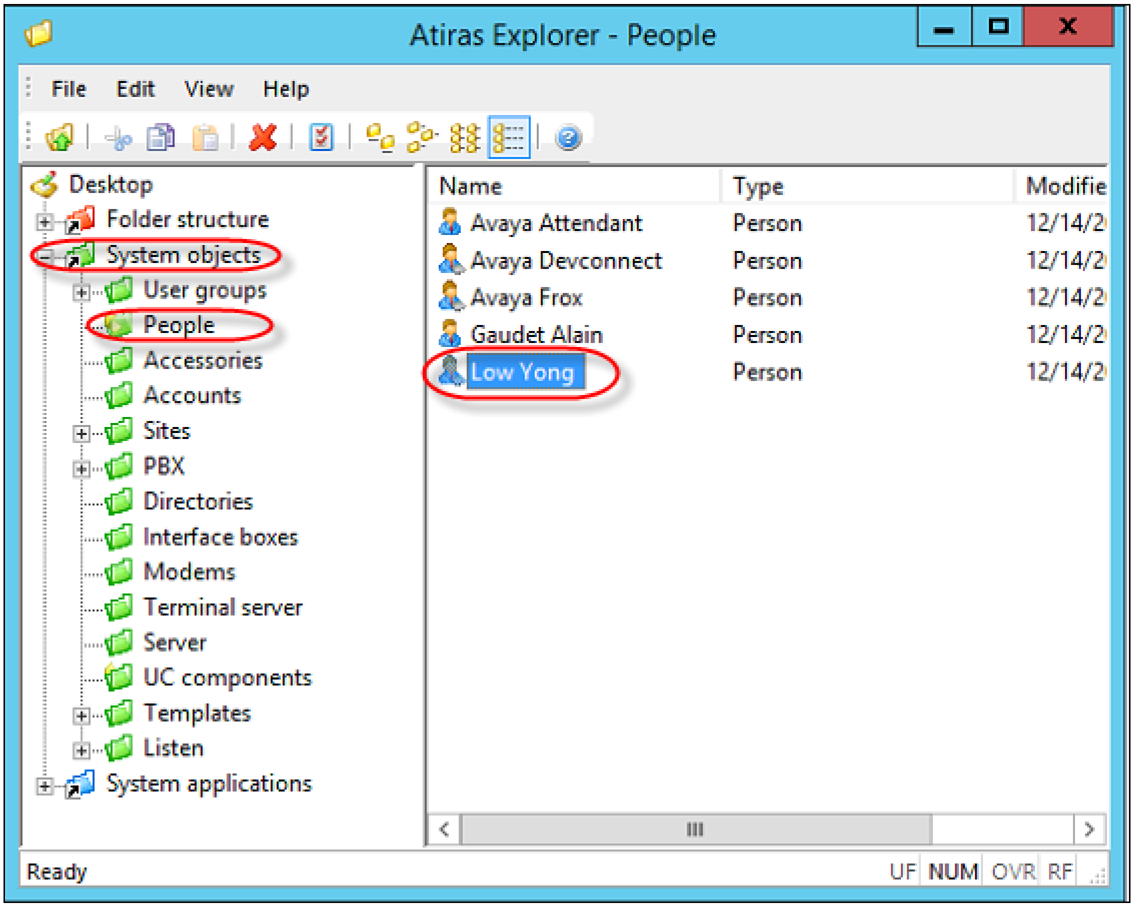
□	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
□	C27FD01D3E50A7713 589AB26D129C973-25	atiras	NmsDrvDmcc	10.1.10.123	XML Unencrypted	0
□	96515FE8FDBA108A4 EC20A3491BECDA7-27	atiras	NmsAttendantConsole	10.1.10.123	XML Unencrypted	1

Terminate Sessions | Show Terminated Sessions

Item 1-2 of 2
1 Go

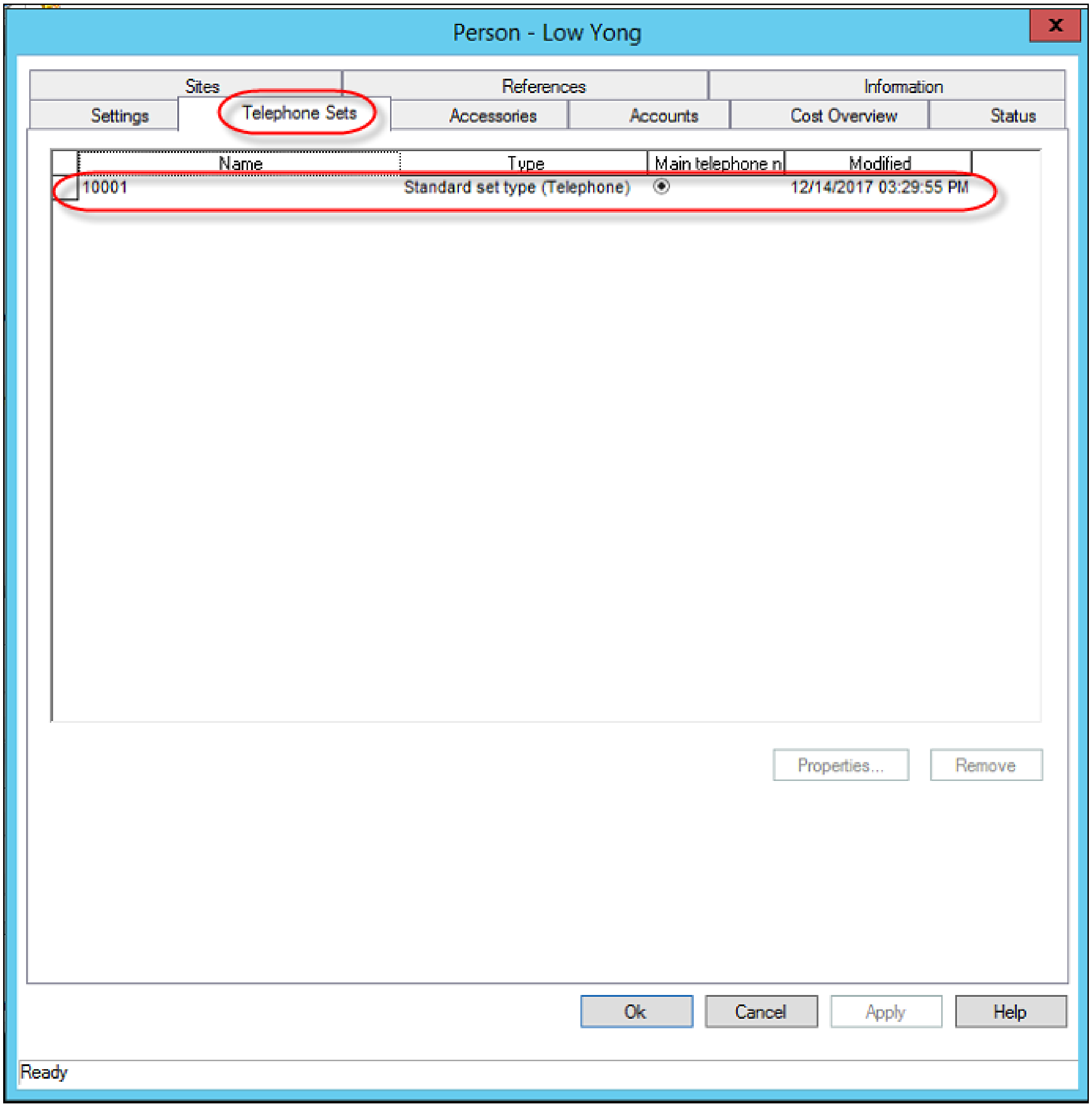
9.3. Verify Atiras Attendant Console Extension is assigned to the Attendant

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 people assigned as Attendant and select **properties.**



Name	Type	Modifie
Avaya Attendant	Person	12/14/2
Avaya Devconnect	Person	12/14/2
Avaya Frox	Person	12/14/2
Gaudet Alain	Person	12/14/2
Low Yong	Person	12/14/2

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 **10001**)



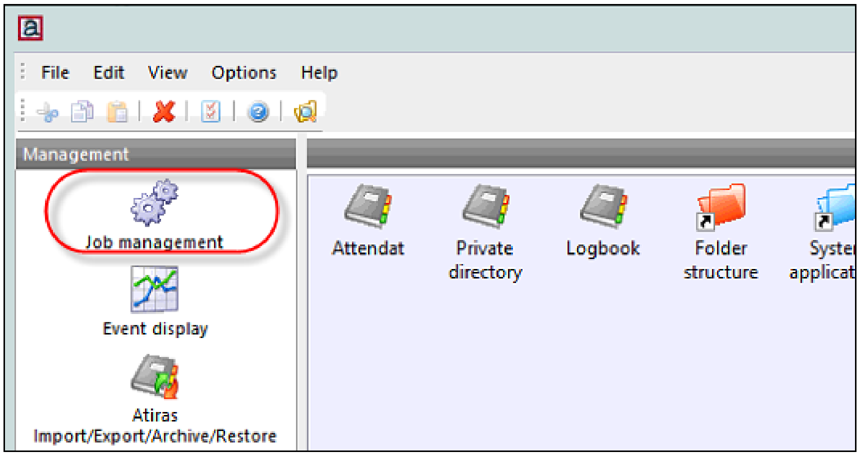
Person - Low Yong

Name	Type	Main telephone n	Modified
10001	Standard set type (Telephone)	●	12/14/2017 03:29:55 PM

Ready

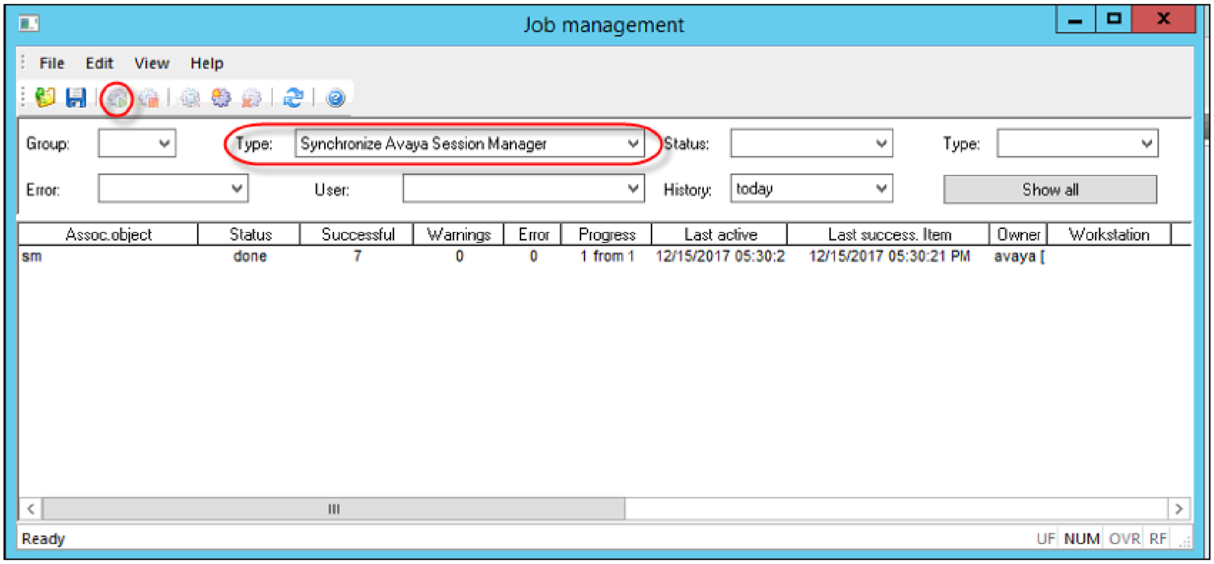
9.4. Verify Atiras Configuration Module Synchronization Status

It is possible to verify the synchronization status of the Communication Manager/Session Manager extensions between the Avaya solution and the Atiras Configuration module. Navigate to **Start → All Programs → 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** or **Phone synchronization** from the **Type** dropdown box and click on the **Start processing** icon.

Note: The screenshot below shows the **Synchronize Avaya Session Manager.**



Group:
Type: Synchronize Avaya Session Manager
Status:
Type:
Error:
User:
History: today

Assoc.object	Status	Successful	Warnings	Error	Progress	Last active	Last success. Item	Owner	Workstation
sm	done	7	0	0	1 from 1	12/15/2017 05:30:2	12/15/2017 05:30:21 PM	avaya [	

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 with observations made in **Section 2.2**.

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 Release 7.1.2*, *Issue 3*, *December 2017*

[2] *Administering Avaya Aura® Session Manager Release 7.1.1, Issue 2, August 2017*

[3] *Administering Avaya Aura® System Manager Release 7.1.2, Issue 9, December 2017*

[4] *Administering and Maintaining Avaya Aura® Application Enablement Services Release 7.0.1, Issue 2, August 2016*

Contact Frox Communications at http://www.frox.ch/support/ for Product Documentation.

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.