Avaya Solution & Interoperability Test Lab

Application Notes for Inisoft Syntelate XA with Avaya Aura® Application Enablement Services - Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Inisoft Syntelate XA to successfully interoperate with Avaya Aura® Application Enablement Services using Computer Telephony Integration. Syntelate XA is a call center agent web application that allows inbound and outbound calls to be made using a web browser based interface. Syntelate XA was compliance tested against Avaya Aura® Application Enablement Services using inbound call center and direct voice calls.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as the 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.

©2018 Avaya Inc. All Rights Reserved.

1. Introduction

These Application Notes describe the configuration steps required for Inisoft Syntelate XA to successfully interoperate with Avaya Aura® Application Enablement Services using Computer Telephony Integration. Syntelate XA is a call center agent web application that allows inbound and outbound calls to be made using a web browser based interface. Syntelate XA was compliance tested against Avaya Aura® Application Enablement Services using inbound call center and direct voice calls.

2. General Test Approach and Test Results

The interoperability compliance testing evaluated the ability of Syntelate XA to carry out call handling functions in a variety of scenarios through its Telephony Services Application Programming Interface (TSAPI) interface with Application Enablement Services. The feature test cases were performed manually. Inbound calls were manually placed and delivered to Syntelate XA by Communication Manager. Different types of actions were initiated from Syntelate XA, to verify proper handling of supported messages from Application Enablement Services Device, Media and Call Control sessions. The verification included checking the display of fields, options, and values on Syntelate XA, and checking the exchanged API messages in the designer and agent logs. All test cases were executed.

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 Syntelate did not include use of any specific encryption features as requested by Inisoft.

©2018 Avaya Inc. All Rights Reserved.

2.1. Interoperability Compliance Testing

The feature testing focused on verifying proper display of the calls made to Syntelate XA with appropriate options, fields, and values for the following scenarios:

- Inbound and Outbound calls
- Log in and logoff
- Hold, retrieve, call transfer, conference, place manual call, agent drop, customer drop, release line/hang-up, and finish work.

2.2. Test Results

All test cases that were executed have successfully passed.

2.3. Support

For technical support for Syntelate XA, please contact Inisoft Support:

- Phone: +44 (0)800 668 1290
- Email: support@inisoft.com

3. Reference Configuration

The configuration used for the compliance testing is shown in **Figure 1**. In the compliance testing, Syntelate XA used Application Enablement Services DMCC to control Communication Manager agent deskphones and take calls for the agents.

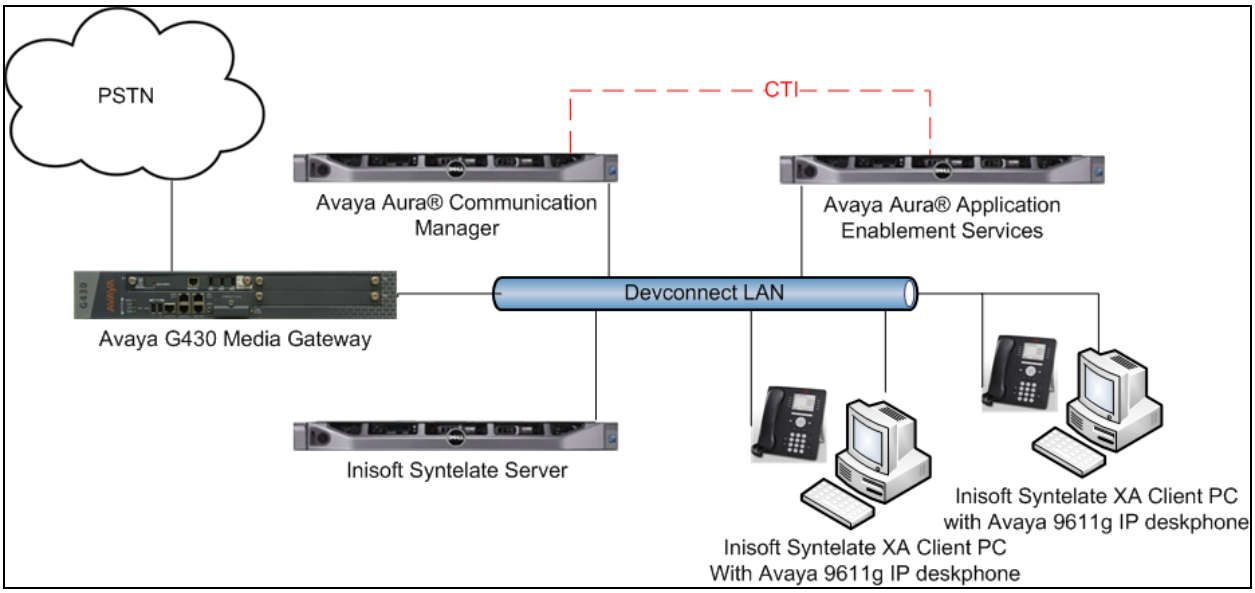


Figure 1: Inisoft Syntelate tested configuration

.

©2018 Avaya Inc. All Rights Reserved.

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communicaiton Manager running on a VMware virtual machine	R017x.01.0.532.0 CM 7.1.2.0.0.532.24184 CM 7.1.2.0.0 FP2 KERNEL-3.10.0-693.e17.AV1 PLAT-rhel17.2-0010
Avaya Aura® Application Enablement Services	R7.1.2.0.0.3-0
Avaya G430 Media Gateway	R38.21.1/1
Avaya 9611g H323 IP Deskphones	R6.6229
Inisoft Syntelate XA server	1.4.0

5. Configure Avaya Aura® Communication Manager

The information provided in this section describes the configuration of Communication Manager relevant to this solution. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section 10**.

The configuration illustrated in this section was performed using Communication Manager System Administration Terminal (SAT).

5.1. Verify System Features

Use the **display system-parameters customer-options** command to verify that Communication Manager has permissions for features illustrated in these Application Notes. On **Page 3**, ensure that **Answer Supervision by Call Classifier?** is set to **y** and **Computer Telephony Adjunct Links?** is set to **y** as shown below.

```
display system-parameters customer-options                      Page   3 of  11
                               OPTIONAL FEATURES

    Abbreviated Dialing Enhanced List? y          Audible Message Waiting? y
        Access Security Gateway (ASG)? n              Authorization Codes? y
        Analog Trunk Incoming Call ID? y                      CAS Branch? n
 A/D Grp/Sys List Dialing Start at 01? y                        CAS Main? n
Answer Supervision by Call Classifier? y                Change COR by FAC? n
                                 ARS? y  Computer Telephony Adjunct Links? y
                ARS/AAR Partitioning? y  Cvg Of Calls Redirected Off-net? y
          ARS/AAR Dialing without FAC? y                      DCS (Basic)? y
          ASAI Link Core Capabilities? n                DCS Call Coverage? y
          ASAI Link Plus Capabilities? n               DCS with Rerouting? y
       Async. Transfer Mode (ATM) PNC? n
  Async. Transfer Mode (ATM) Trunking? n    Digital Loss Plan Modification? y
              ATM WAN Spare Processor? n                          DS1 MSP? y
                                 ATMS? y             DS1 Echo Cancellation? y
                  Attendant Vectoring? y
```


©2018 Avaya Inc. All Rights Reserved.

5.2. Display Node Names for Avaya Aura® Application Enablement Services Connectivity

Display the **procr** IP Address by using the command **display node-names ip** and noting the IP address for the **procr** and AES (**Aes71678**).

```
display node-names ip                                          Page   1 of   2
                                IP NODE NAMES
    Name                  IP Address
SM100                   10.10.40.34
Aes71678                10.10.16.78
default                 0.0.0.0
g430                    10.10.40.15
procr                   10.10.16.27
```

5.3. Configure AE service for Avaya Aura® Application Enablement Services Connectivity

To administer the transport link to AES use the **change ip-services** command. On **Page 1** add an entry with the following values:

- **Service Type**: should be set to **AESVCS**.
- **Enabled**: set to **y**.
- **Local Node**: set to the node name assigned for the **procr** in **Section 5.2**
- **Local Port**: retain the default value of **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
```

Go to **Page 4** of the **ip-services** form and enter the following values:

- **AE Services Server**: Name obtained from the AES server, in this case **aes71678**.
- **Password**: Enter a password to be administered on the AES server.
- **Enabled**: Set to **y**.

Note: The password entered for **Password** field must match the password on the AES server in **Section 6.2**. The **AE Services Server** should match the administered name for the AES server, this is created as part of the AES installation, and can be obtained from the AES server by typing **uname –n** at the Linux command prompt.

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

   Server ID    AE Services        Password          Enabled    Status
                   Server
      1:        aes71678           ********          y          idle
      2:
      3:
```


©2018 Avaya Inc. All Rights Reserved.

5.4. Configure CTI Link for TSAPI Service

Add a CTI link using the **add cti-link n** command. Enter an available extension number in the **Extension** field. Enter **ADJ-IP** in the **Type** field, and a descriptive name in the **Name** field. Default values may be used in the remaining fields.

```
add cti-link 1                                                Page   1 of   3
                                    CTI LINK
 CTI Link: 1
Extension: 2002
     Type: ADJ-IP
                                                                    COR: 1
     Name: aes71678
```


©2018 Avaya Inc. All Rights Reserved.

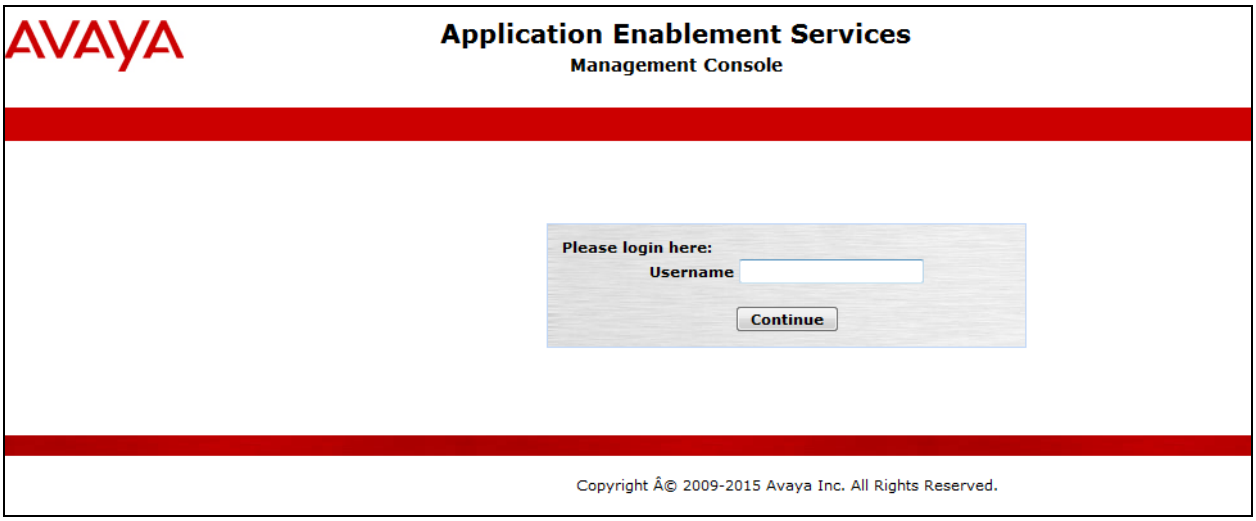
6. Configure Avaya Aura® Application Enablement Services

This section provides the procedures for configuring Application Enablement Services. The procedures fall into the following areas:

- Verify Licensing.
- Create Switch Connection.
- Administer TSAPI link.
- Create CTI User.
- Enable CTI Link User.
- Identify Tlinks.
- Enable DMCC ports.

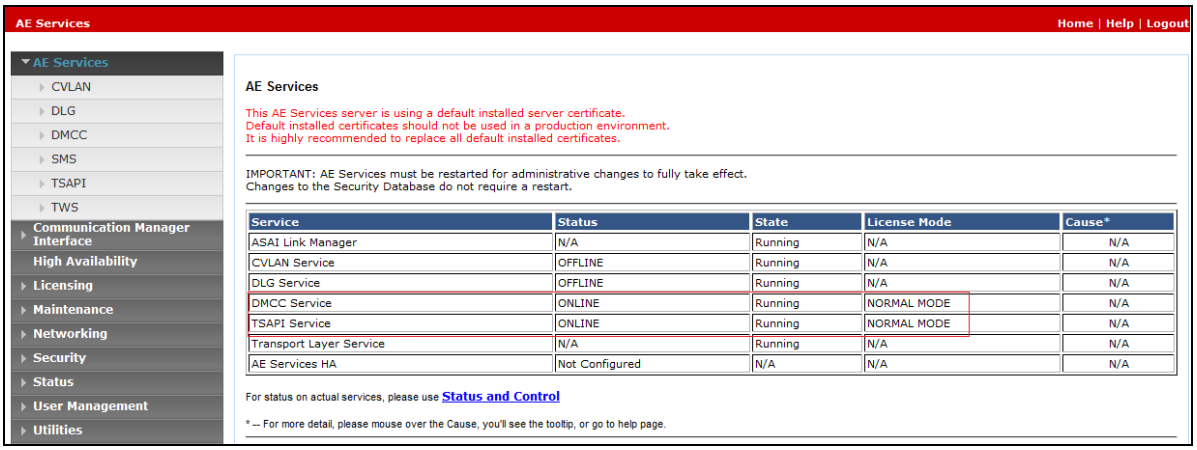
6.1. Verify Licensing

To access the maintenance console, enter **https://<ip-addr>** as the URL in an Internet browser, where <ip-addr> is the active IP address of AES. The login screen is displayed, enter the appropriate credentials and then select the **Login** button (not shown).



©2018 Avaya Inc. All Rights Reserved.

The Application Enablement Services Management Console appears displaying the **Welcome to OAM** screen (not shown). Select **AE Services** and verify that the TSAPI and DMCC Service is licensed by ensuring that **TSAPI and DMCC Service** is in the list of services and that the **License Mode** is showing **NORMAL MODE**. If not, contact an Avaya support representative to acquire the proper license for your solution.

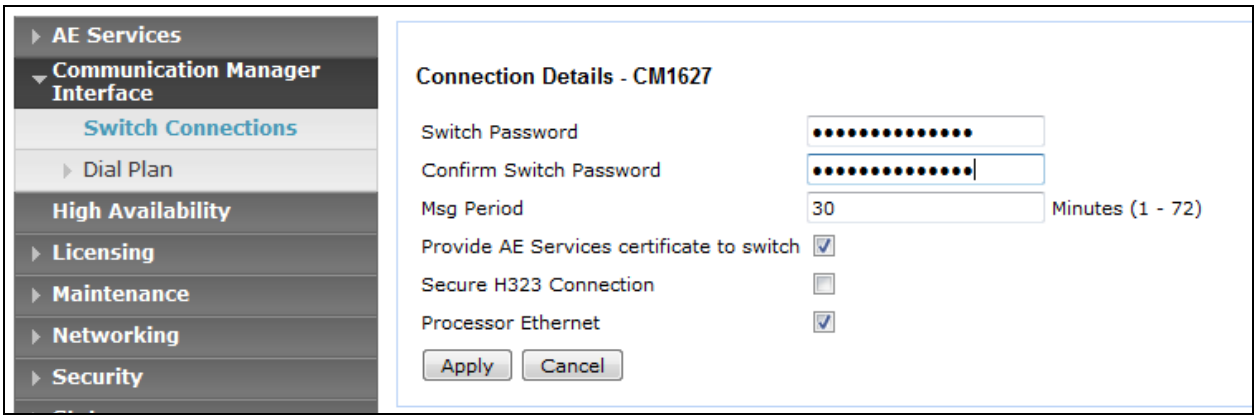


6.2. Create Switch Connection

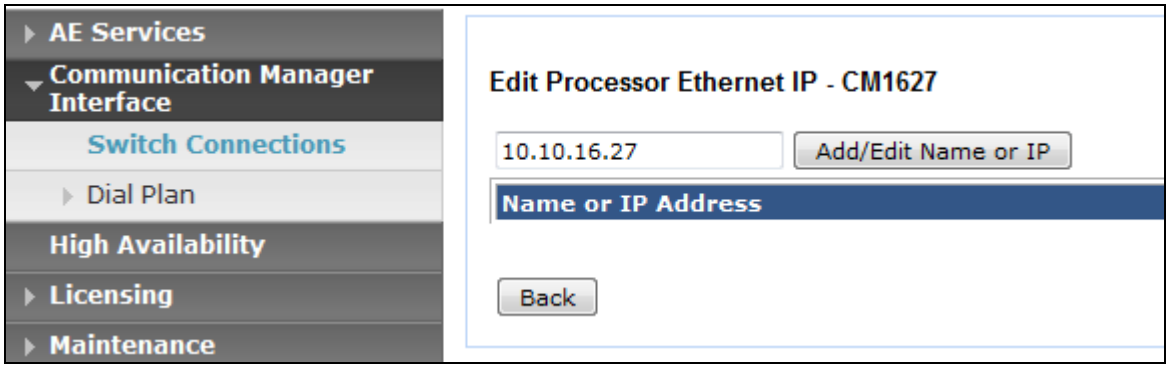
From the AES Management Console navigate to **Communication Manager Interface** → **Switch Connections** to set up a switch connection. Enter in a name for the Switch Connection to be added and click the **Add Connection** button.

©2018 Avaya Inc. All Rights Reserved.

In the resulting screen enter the **Switch Password,** the Switch Password must be the same as that entered into Communication Manager AE Services Administration screen via the **change ip-services** command, described in **Section 5.3** Default values may be accepted for the remaining fields. Click **Apply** to save changes.



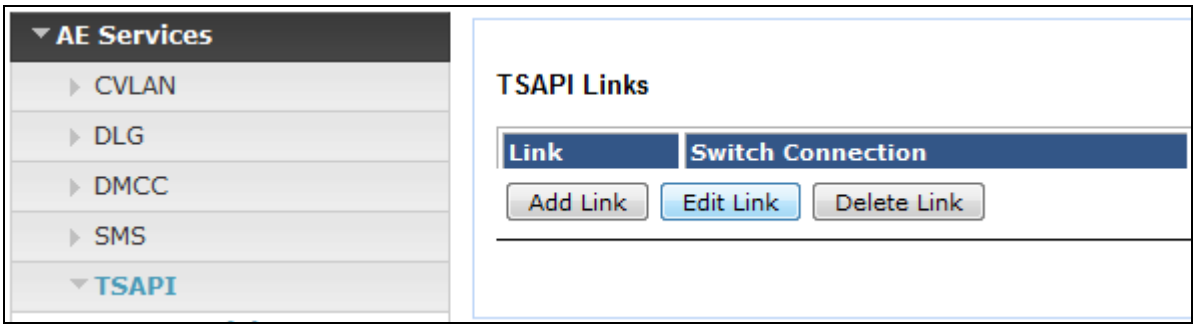
From the **Switch Connections** screen, select the radio button for the recently added switch connection and select the **Edit CLAN IPs** button (not shown). In the resulting screen, enter the IP address of the **procr** as shown in **Section 5.2** that will be used for the AES connection and select the **Add/Edit Name or IP** button.



©2018 Avaya Inc. All Rights Reserved.

6.3. Administer TSAPI link

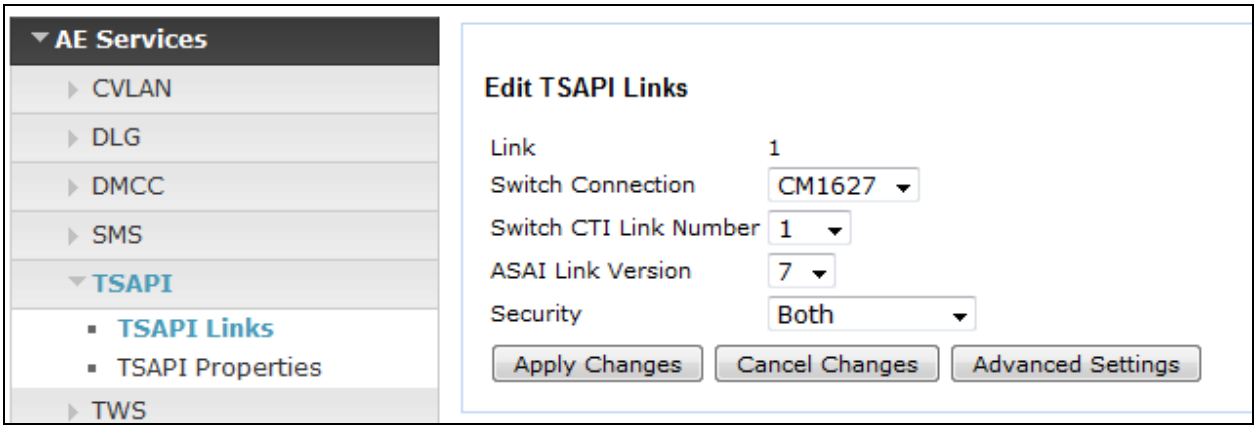
From the Application Enablement Services Management Console, select **AE Services → TSAPI → TSAPI Links**. Select **Add Link** button as shown in the screen below.



On the **Add TSAPI Links** screen, enter the following values:

- **Link:** Use the drop-down list to select an unused link number.
- **Switch Connection:** Choose the switch connection **CM1627**, which has already been configured in **Section 6.2**, from the drop-down list.
- **Switch CTI Link Number:** Corresponding CTI link number configured in **Section 5.4** which is **1**.
- **ASAI Link Version:** This can be left at the default value of **7**.
- **Security:** Select **Both** from the drop down.

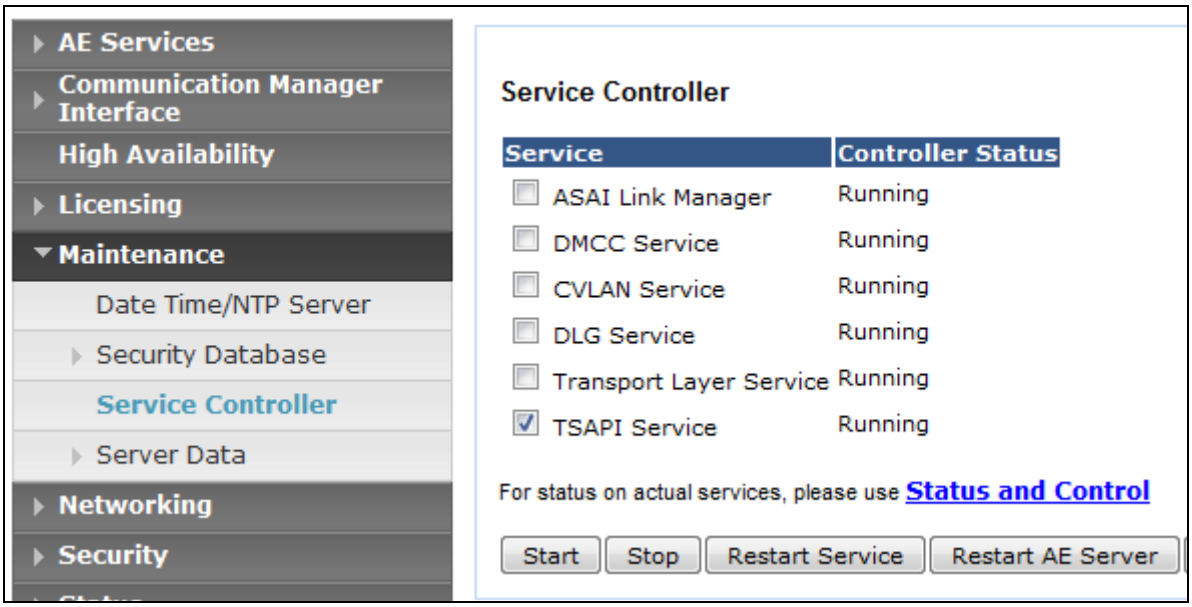
Once completed, select **Apply Changes**.



©2018 Avaya Inc. All Rights Reserved.

Another screen appears for confirmation of the changes. Choose **Apply** (not shown).

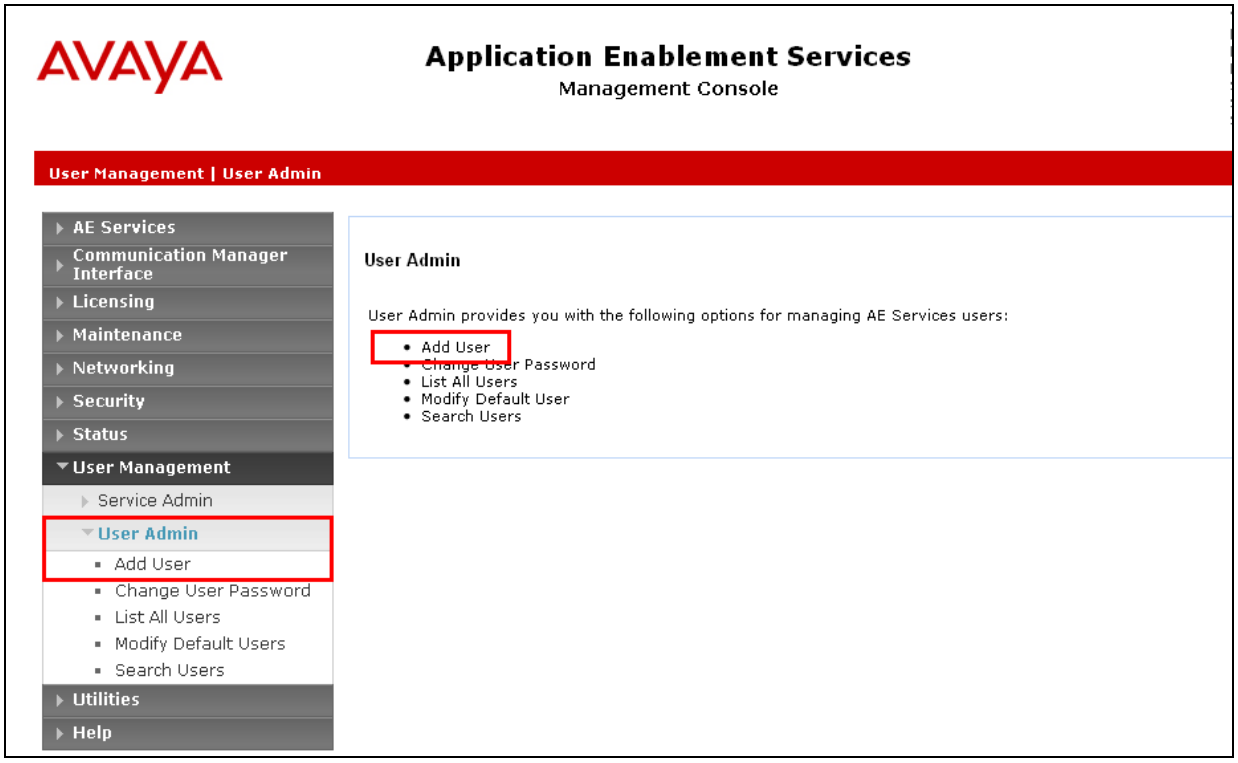
The TSAPI Service must be restarted to effect the changes made in this section. From the Management Console menu, navigate to **Maintenance → Service Controller**. On the Service Controller screen, tick the **TSAPI Service** and select **Restart Service**.



©2018 Avaya Inc. All Rights Reserved.

6.4. Create Avaya CTI User

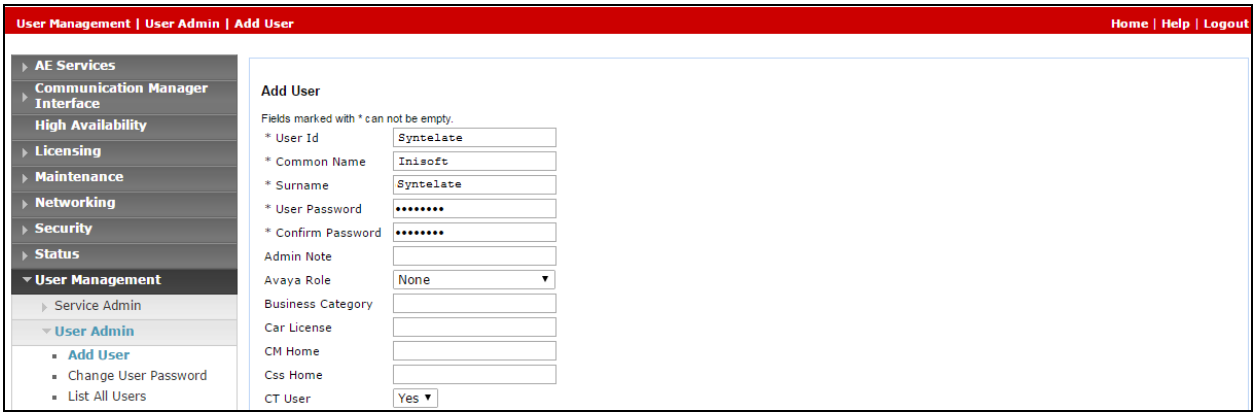
A User ID and password needs to be configured for the Syntelate Server to communicate as a TSAPI client with the Application Enablement Services server. Navigate to the **User Management → User Admin** screen then choose the **Add User** option.



©2018 Avaya Inc. All Rights Reserved.

In the **Add User** screen shown below, enter the following values:

- **User Id** - This will be used by the Syntelate Server to connect.
- **Common Name** and **Surname** - Descriptive names need to be entered.
- **User Password** and **Confirm Password** - This will be used with the **User Id** to connect.
- **CT User** - Select **Yes** from the drop-down menu.



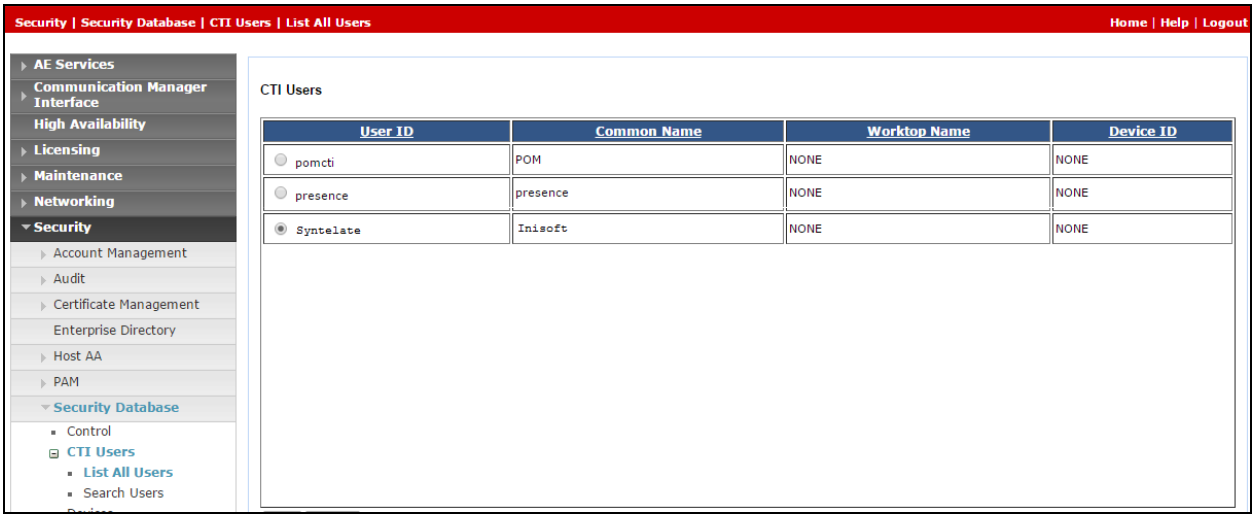
Complete the process by choosing **Apply** at the bottom of the screen (not shown).

The next screen will show a message indicating that the user was created successfully (not shown).

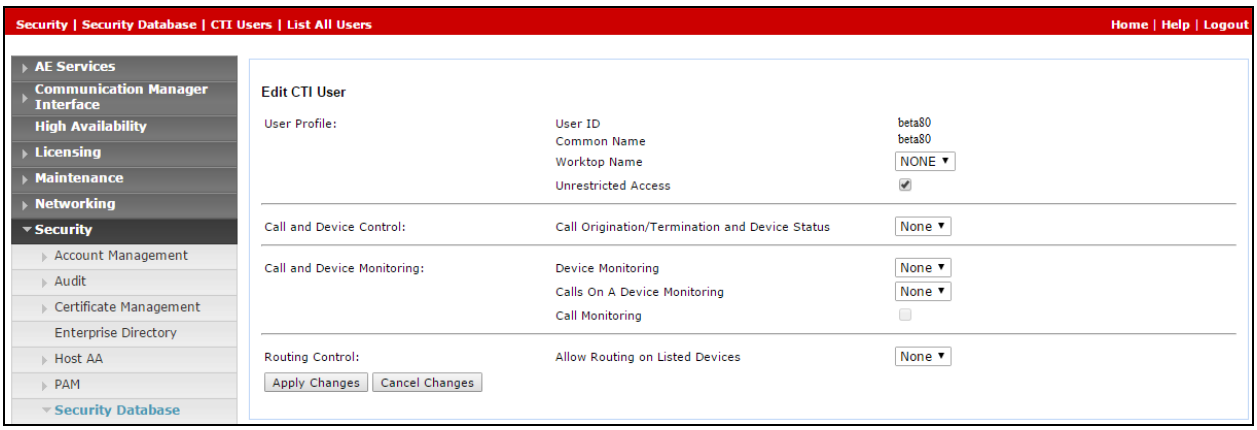
©2018 Avaya Inc. All Rights Reserved.

6.5. Enable Unrestricted Access for CTI User

Navigate to the **CTI Users** screen by selecting **Security → Security Database → CTI Users → List All Users**. Select the user that was created in **Section 6.4** and select the **Edit** option (not shown).



The **Edit CTI User** screen appears. Check the **Unrestricted Access** box and **Apply Changes** at the bottom of the screen.



A screen (not shown) appears to confirm applied changes to CTI User, choose **Apply**. This CTI user should now be enabled.

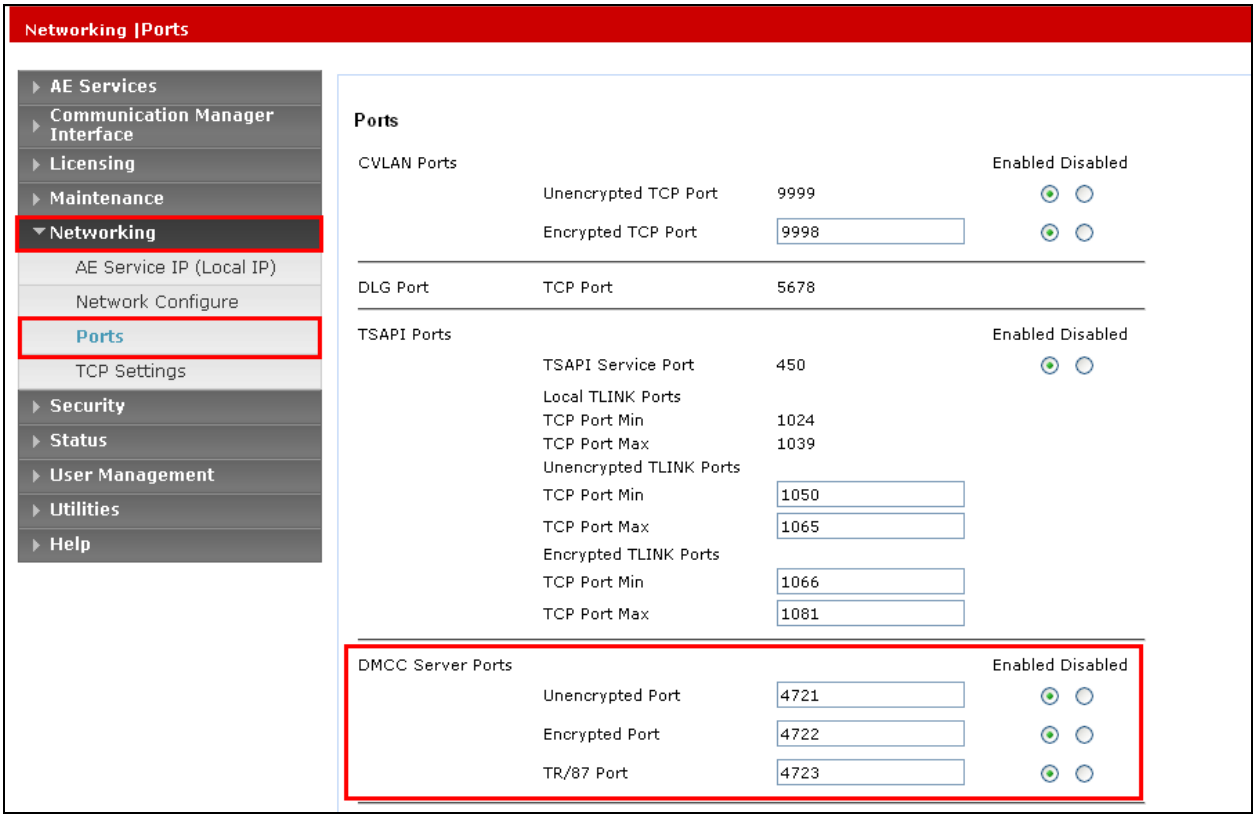
©2018 Avaya Inc. All Rights Reserved.

6.6. Enable DMCC ports

In order to enable DMCC for call control navigate to **Networking → Ports → DMCC Server Ports**.

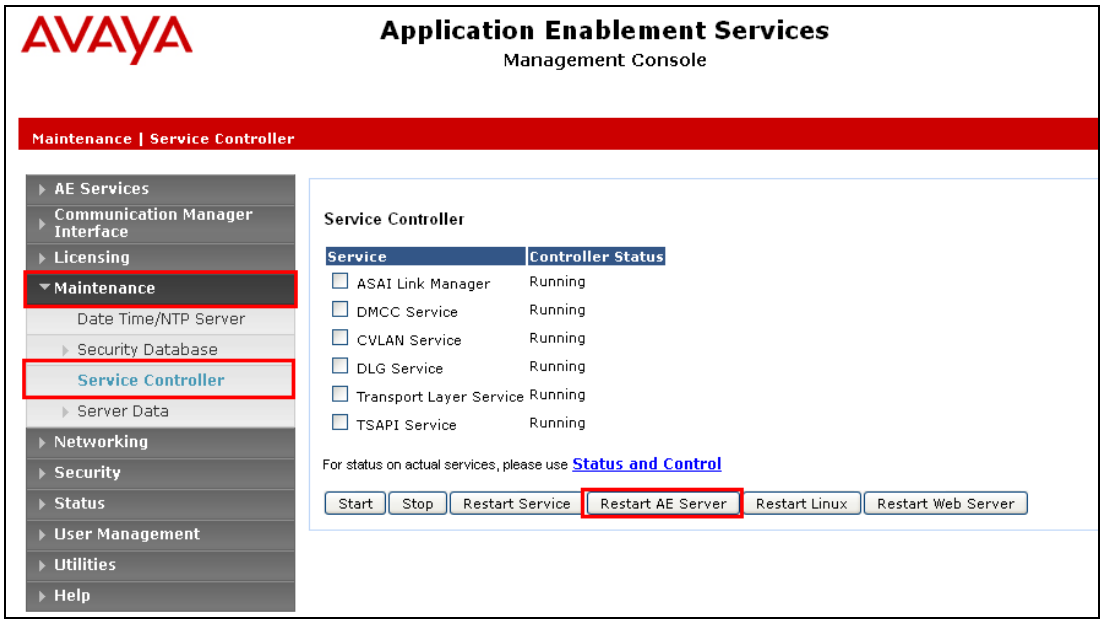
- Enable DMCC **Unencrypted Port**
- Enable DMCC **Encrypted Port**
- Enable DMCC **TR/87 Port**

Click on **Apply Changes** at the bottom of the screen (not shown).



©2018 Avaya Inc. All Rights Reserved.

Once this change is made a restart of the AE Server is required. Navigate to **Maintenance → Service Controller**. In the main screen select **Restart AE Server** highlighted.



©2018 Avaya Inc. All Rights Reserved.

7. Configure Inisoft Syntelate XA

This section describes how to configure Syntelate XA for TSAPI.

7.1. Install the TSAPI Client on the Syntelate XA Server

First, install the TSAPI Client on the server which has Syntelate XA on it. Make sure the correct addresses for the Application Enablement Servers is in the TSLIB.ini file

7.2. Configure Your Workzone for TSAPI

Syntelate XA allows the set up of multiple workzones that agents can use to log in to Syntelate XA. For each workzone that will support voice calls via TSAPI, perform this step.

In the table called WORKZONES in the Syntelate XA database, use a SQL UPDATE statement to insert the following into the CTICONFIG_JSON field for the workzone:

```
{
"CtiSource":"TSAPI", "CtiApiUrl": "http://localhost/NameOfTSAPIApplication",
"LoginRequired":true,
  "ServerName": "AESSERVER NAME",
  "Username": "username",
  "Userpassword": "password",
  "TimeoutSeconds": "10",
  "PrivateDataVersions": "8"
}
```

The CtiApiUrl is the URL used for the TSAPI application on the Default Web site. The server name is the AES Server name. The username and password is for a CT user on AES.

©2018 Avaya Inc. All Rights Reserved.

8. Verification Steps

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

8.1. Verify Avaya Aura® Communication Manager CTI Service State

The following steps can validate that the communication between Communication Manager and AES is functioning correctly. Check the AESVCS link status with AES by using the command **status aesvcs cti-link**. Verify the **Service State** of the CTI link is **established.**

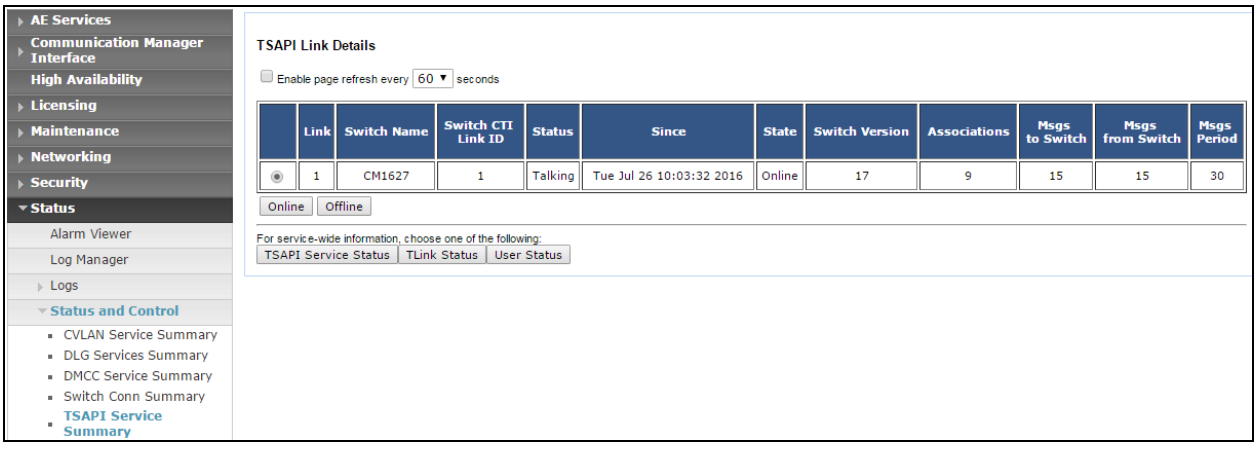
```
status aesvcs cti-link

                          AE SERVICES CTI LINK STATUS

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

1          4        no       aes71678       established    18        18
```

8.2. Verify TSAPI Link and DMCC

This section will verify both the TAPI and DMCC links between the AES and Communication Manager.

8.2.1. Verify TSAPI Link

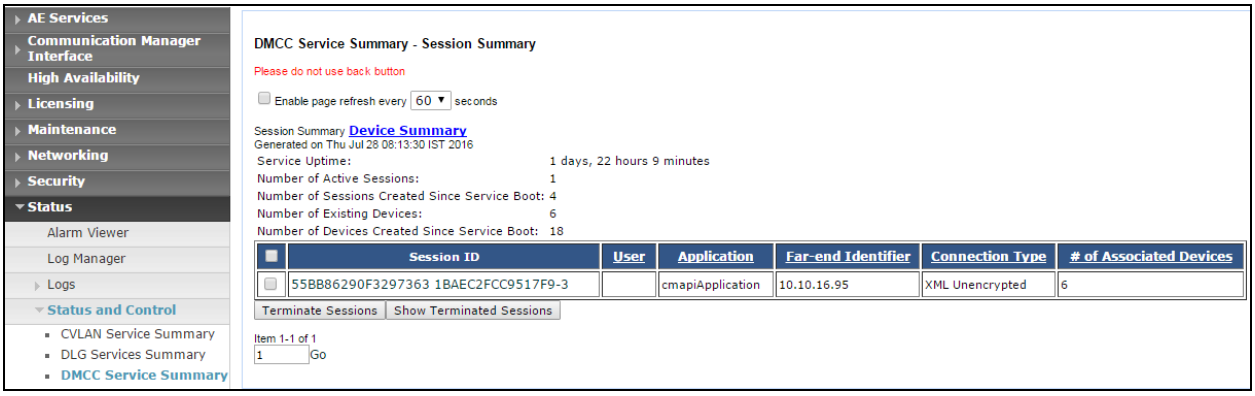
On the AES Management Console verify the status of the TSAPI link by selecting **Status → Status and Control → TSAPI Service Summary** to display the **TSAPI Link Details** screen. Verify the status of the TSAPI link by checking that the **Status** is **Talking** and the **State** is **Online**.



©2018 Avaya Inc. All Rights Reserved.

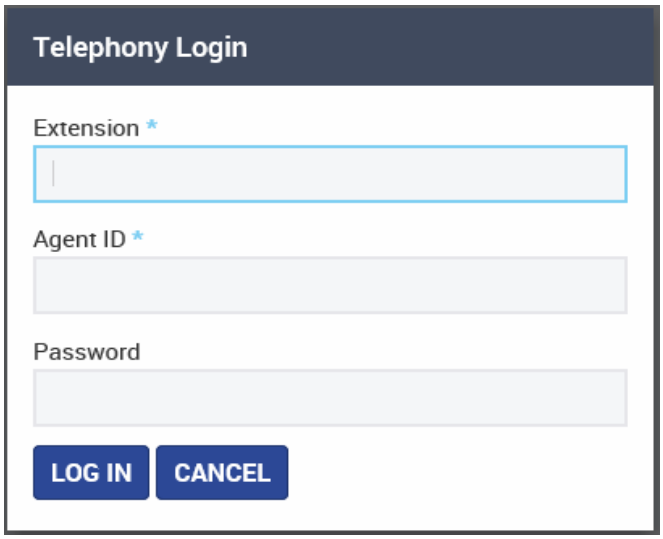
8.2.2. Verify Avaya Aura® Application Enablement Services DMCC Service

The following steps are carried out on AES to validate that the communication link between AES and the Syntelate 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 the Syntelate server IP address **10.10.16.95**. The **Application** is shown as **cmapiApplication,** and the **Far-end Identifier** is given as the IP address **10.10.16.95** as expected.



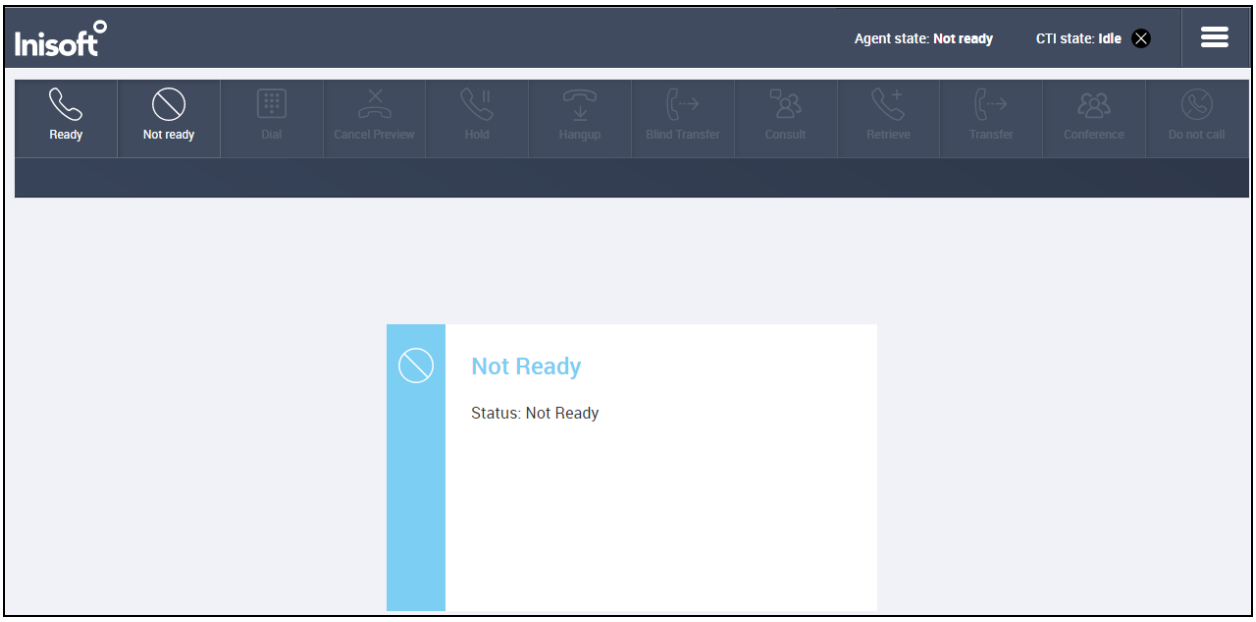
8.3. Verify Syntelate XA Connection

To verify the Syntelate XA connection to TSAPI, open Syntelate XA, select a TSAPI-enabled workzone, and then log in using an Agent Extension, Agent ID, and Password.



©2018 Avaya Inc. All Rights Reserved.

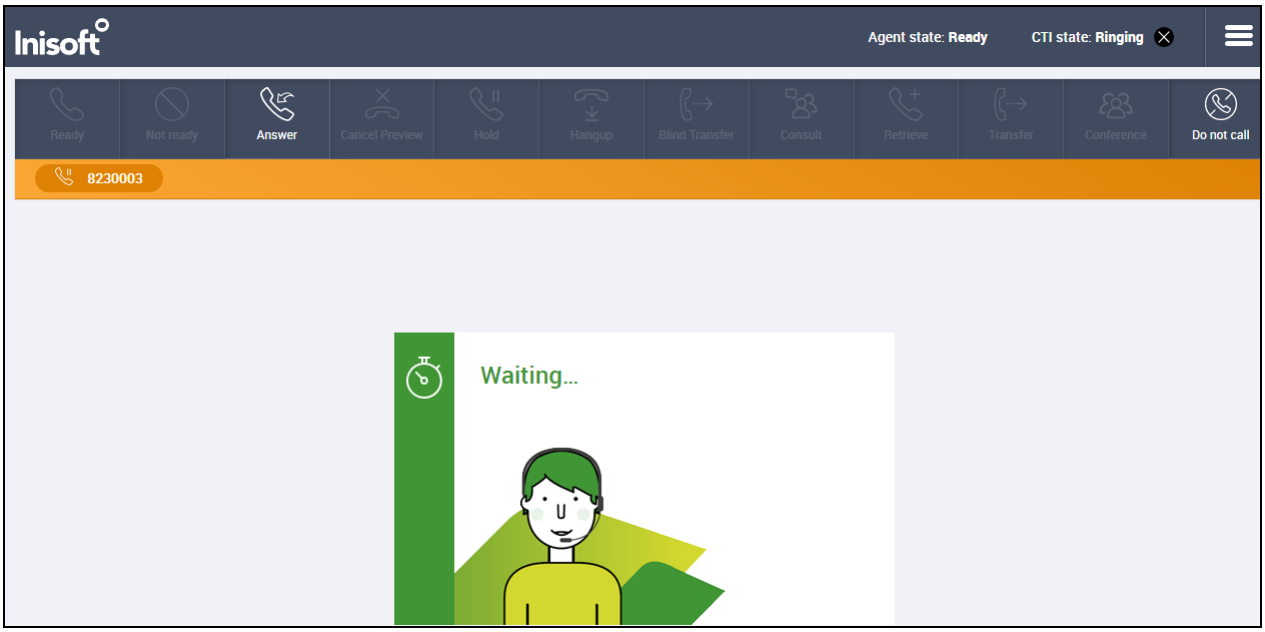
When the Syntelate XA is logged in, the agent will show in the Not Ready state. Click on the **Ready** button.



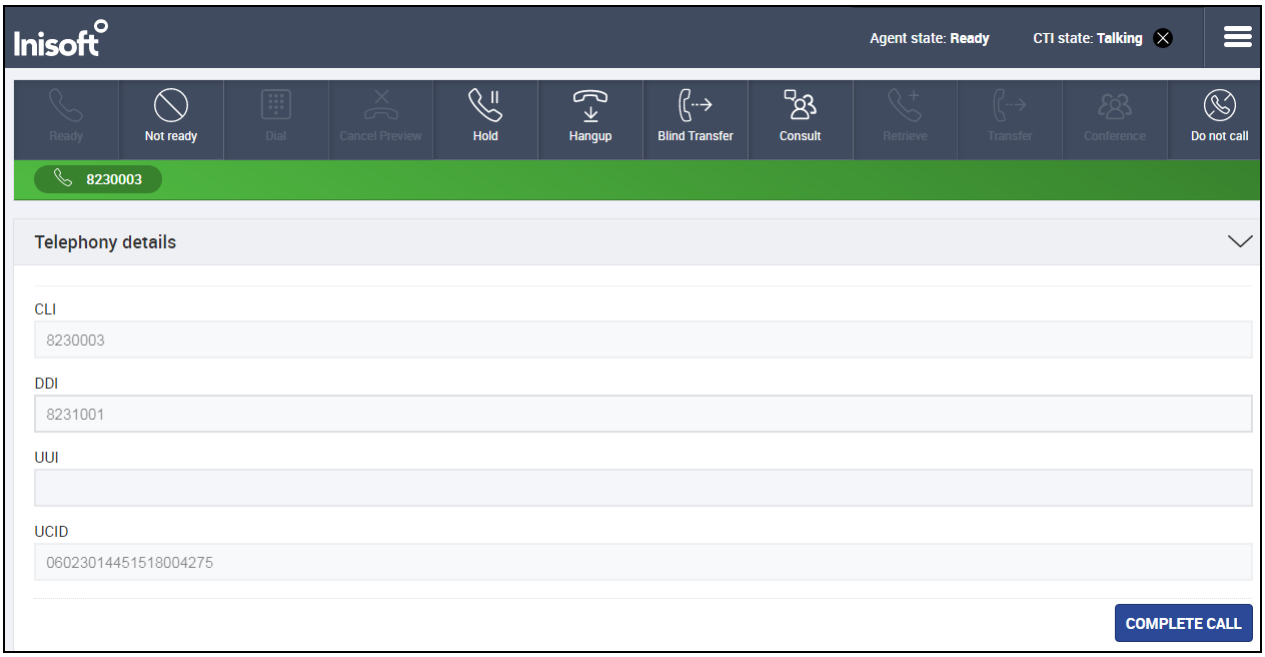
The screen will show as waiting.

©2018 Avaya Inc. All Rights Reserved.

Make a call directly to the agent, a VDN or Hunt group number. The bar under the menu options will show the calling number in orange. Click on the **Answer** button.



The bar now shows green meaning the call has been answered successfully and the in call options become available.



©2018 Avaya Inc. All Rights Reserved.

9. Conclusion

These Application Notes describe the configuration steps required for Inisoft Syntelate XA to successfully interoperate with Avaya Aura® Application Enablement Services. All feature functionality and serviceability test cases were completed successfully as outlined in **Section 2.2.**

10. Additional References

This section references the Avaya and Inisoft product documentation that are relevant to these Application Notes.

Product documentation for Avaya products may be found at *https://support.avaya.com*.

[1] *Administering Avaya Aura® Communication Manager*, Document ID 03-300509

[2] *Avaya Aura® Communication Manager Feature Description and Implementation*, Document ID 555-245-205

[3] *Avaya Aura® Application Enablement Services Administration and Maintenance Guide Release 7.1*

Product documentation for Inisoft can be obtained via the contact details listed in **Section 2.3**:

©2018 Avaya Inc. All Rights Reserved.

©2018 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.