Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Aura® Session Manager R7.1 and Avaya Aura® Communication Manager R7.1 to interoperate with Zenitel Turbine - Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Zenitel Turbine to interoperate with Avaya Aura® Session Manager R7.1 and Avaya Aura® Communication Manager R7.1. The Zenitel Turbine is an IP Intercom that supports voice transmission using the Session Initiation Protocol (SIP).

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.

1. Introduction

These Application Notes describe the configuration steps required for Zenitel Turbine IP Intercom Substation to interoperate with Avaya Aura® Session Manager and Avaya Aura® Communication Manager. The Zenitel Turbine IP Intercom Substations is a communicator that supports voice transmission using the Session Initiation Protocol (SIP) in harsh environments in sectors like Maritime, Oil&Gas, Heavy Industry, Transportation, Building security and Public safety. In the compliance testing, the Zenitel Turbine IP Intercom Substation was set up as a SIP user on Avaya Aura® Session Manager and underwent testing of various call scenarios with other Avaya telephones and Zenitel Turbine IP Intercom Substations.

2. General Test Approach and Test Results

The general test approach was to place calls to and from Turbine and exercise basic telephone operations. For serviceability testing, failures such as cable pulls and hardware resets were performed.

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 Zenitel Turbine IP Intercoms utilized enabled capabilities of TLS/SRTP.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing. TCIS 1-3,TCIS 4-5, TCIV-3/TCIV6, TFIE 1-2 and TMIS-1 models were tested. The feature testing was to verify that:

- Turbine successfully registers with Session Manager using IP address and FQDN using UDP, TCP and TLS
- Turbine successfully establishes audio calls with good quality RTP and SRTP audio to Avaya H.323, SIP and digital endpoints registered to Session Manager and Communication Manager.
- Turbine successfully establishes audio calls with PSTN.
- Turbine IP successfully negotiates the appropriate audio codec.
- DTMF tones could be passed successfully to energize relay on Turbine unit and switch audio direction.
- Turbine successfully calls multiple destinations using a cover answer group.
- Turbine successfully calls a variety of endpoints in its call list.
- Correct handling of forwarded calls, cover paths and cover answer groups.
- Video was tested on the TCIV-3 model.

The serviceability testing focused on verifying the ability of Turbine to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet cable to the devices and denying service on Session Manager.

2.2. Test Results

All test cases passed successfully.

2.3. Support

Technical support on Zenitel Turbine can be obtained through the following:

- **Phone:** +47 4000 2700
- **Web:** https://www.zenitel.com/customer-service

3. Reference Configuration

Figure 1 illustrates a test configuration that was used to compliance test the interoperability of Turbine with Session Manager and Communication Manager. The configuration consists of Communication Manager, System Manager and Session Manager. Communication Manager has connections to 96x1 IP (H.323) deskphones. Session Manager has SIP registrations with, Turbine and 96x1 IP (SIP) deskphones. An ISDN-PRI trunk connects Communication Manager to the PSTN.

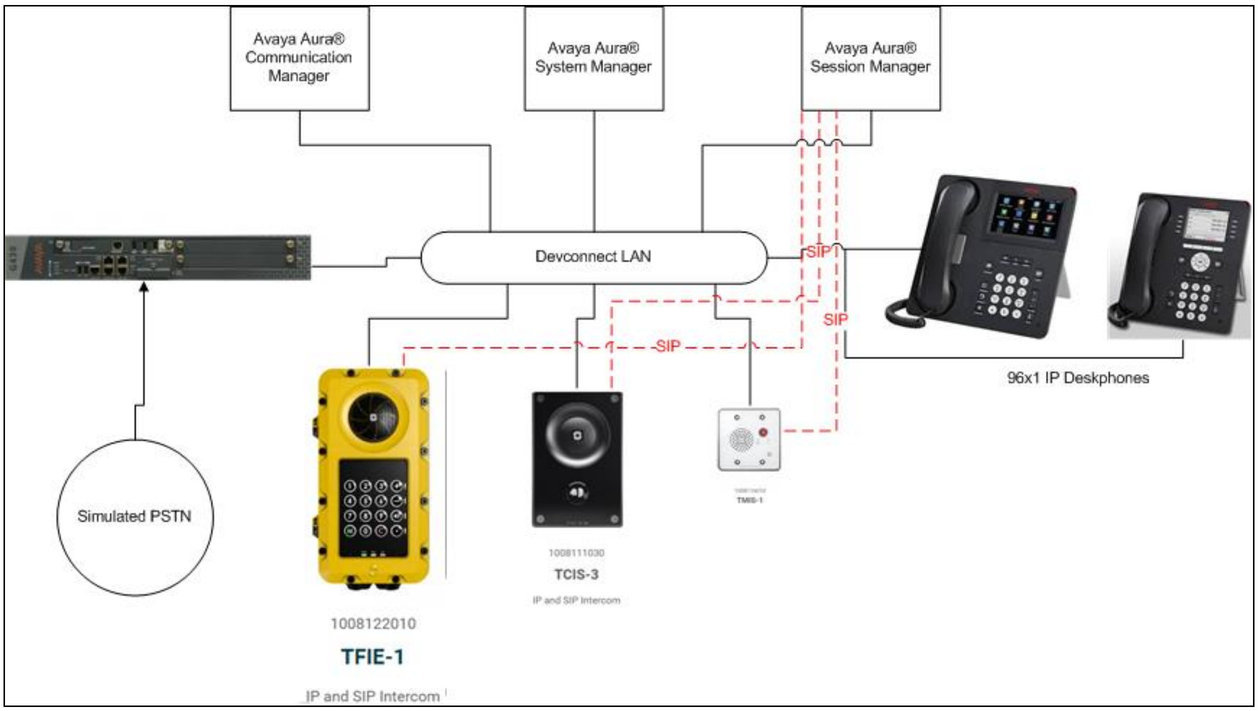


Figure 1: Avaya Aura® Session Manager and Avaya Aura® Communication Manager with Zenitel Turbine Configuration

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® System Manager running on VMware Virtual Machine	R7.1.1.0 Build 7.1.1.0.1125193 Software Update Revision 7.1.1.0.046931 Feature Pack 1
Avaya Aura® Communication Manager running on VMware Virtual Machine	R017x.01.0.532.0 Build 7.1.1.0.0.532.23955 Software Update Revision RHEL7.2-SSP001 KERNEL-3.10.0
Avaya G430 Media Gateway • MGP	38.20.1
Avaya Aura® Media Server	7.8.0.309
Avaya Aura® Session Manager running on VMware Virtual Machine	R7.0 SP1 7.1.1.0.711008
Avaya 9611G IP Telephone Avaya 9641G IP Telephone	Release 6.6229 H323 Release 6.6229 H323 Release 7.1.0.1.1 SIP Release 7.1.0.11 SIP
Zenitel Turbine	4.7.3

5. Configure Avaya Aura® Communication Manager

The configuration changes in this section for Communication Manager are performed through the Site Administration tool and via the System Manager web interface. Except where stated, the parameters in all steps are the default settings and are supplied for reference. For all other provisioning information such as provisioning of the trunks, call coverage, extensions, and voicemail, please refer to the Avaya product documentation in **Section 9.**

The procedures fall into the following areas:

- Configure IP Codec Set
- Configure SIP User

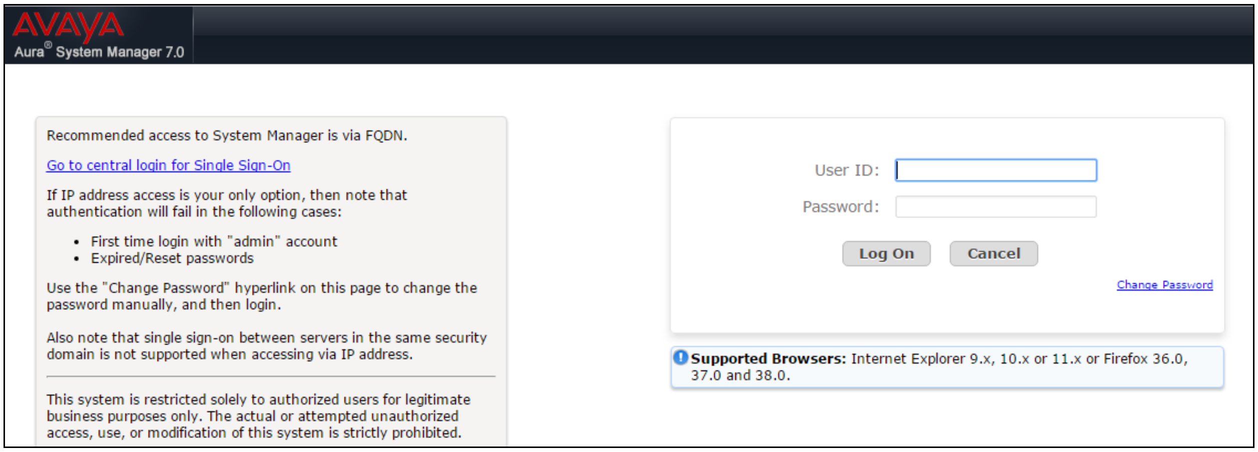
5.1. Configure IP Codec Set

The IP Codec set must be configured with the codecs for use by IP endpoints. Enter the command **change ip-codec-set x** where **x** is the relevant codec set and set the **Audio Codec** to be used on **Page 1**. In the example below, codecs **G.711MU** and **G.711A** are configured. Media Encryption (**1-srtp-aescm128-hmac80**) was set for this test with **Encrypted SRTP: best-effort**.

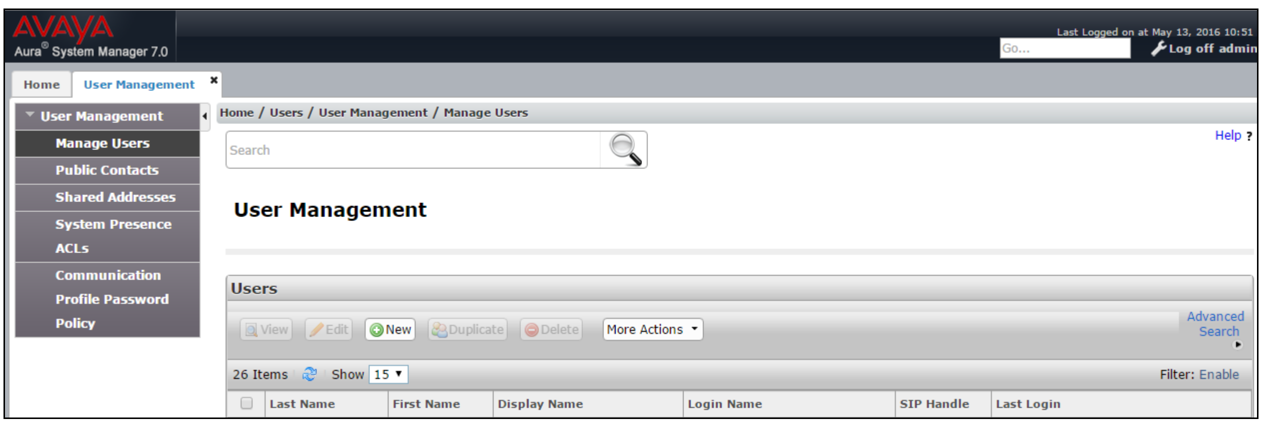
```
change ip-codec-set 1                                               Page   1 of   2

                          IP CODEC SET

    Codec Set: 1

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.711MU           n          2        20
 2: G.711A            n          2        20
 3:
 4:
 5:
 6:
 7:


     Media Encryption                  Encrypted SRTCP: best-effort
 1: 1-srtp-aescm128-hmac80
 2:
 3:
```

5.2. Configure SIP User

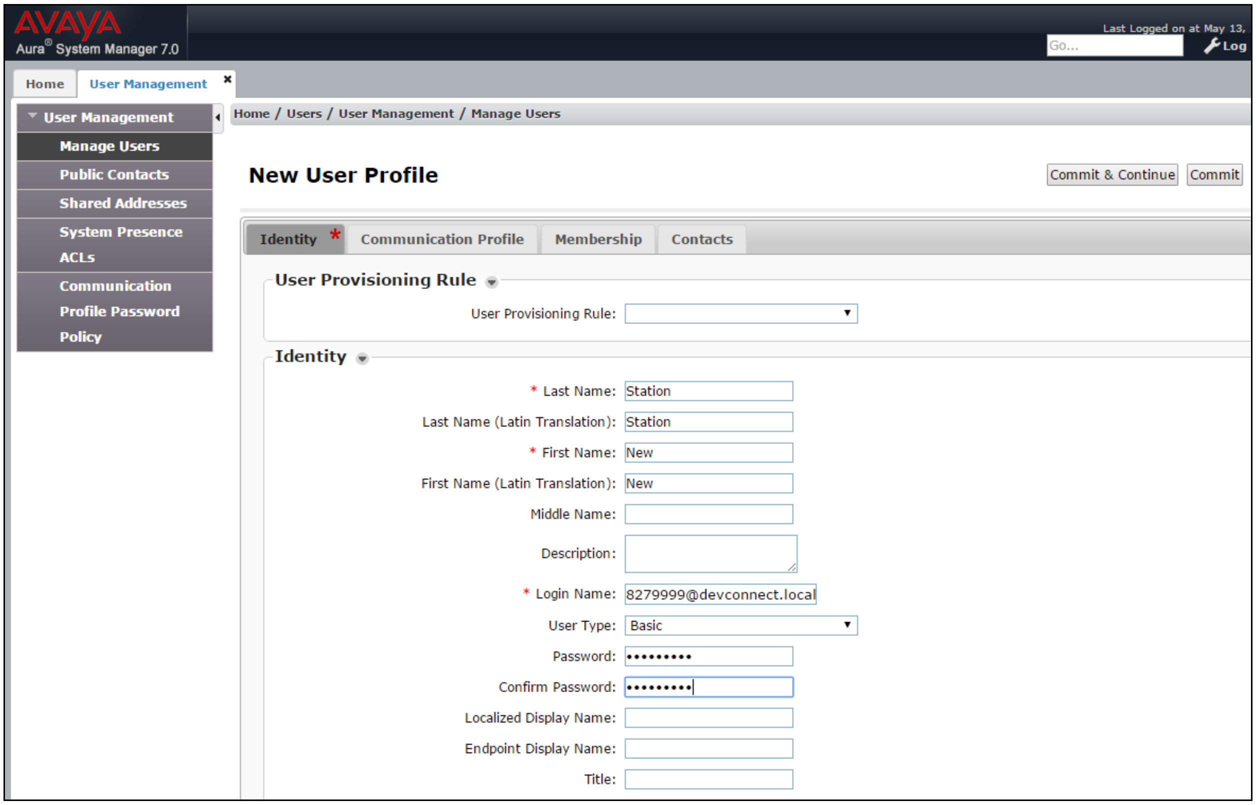
A SIP user must be added for each Turbine endpoint required. Navigate to the System Manager web interface, in this case **https://<IP Address>/SMGR** and log in with the relevant credentials.



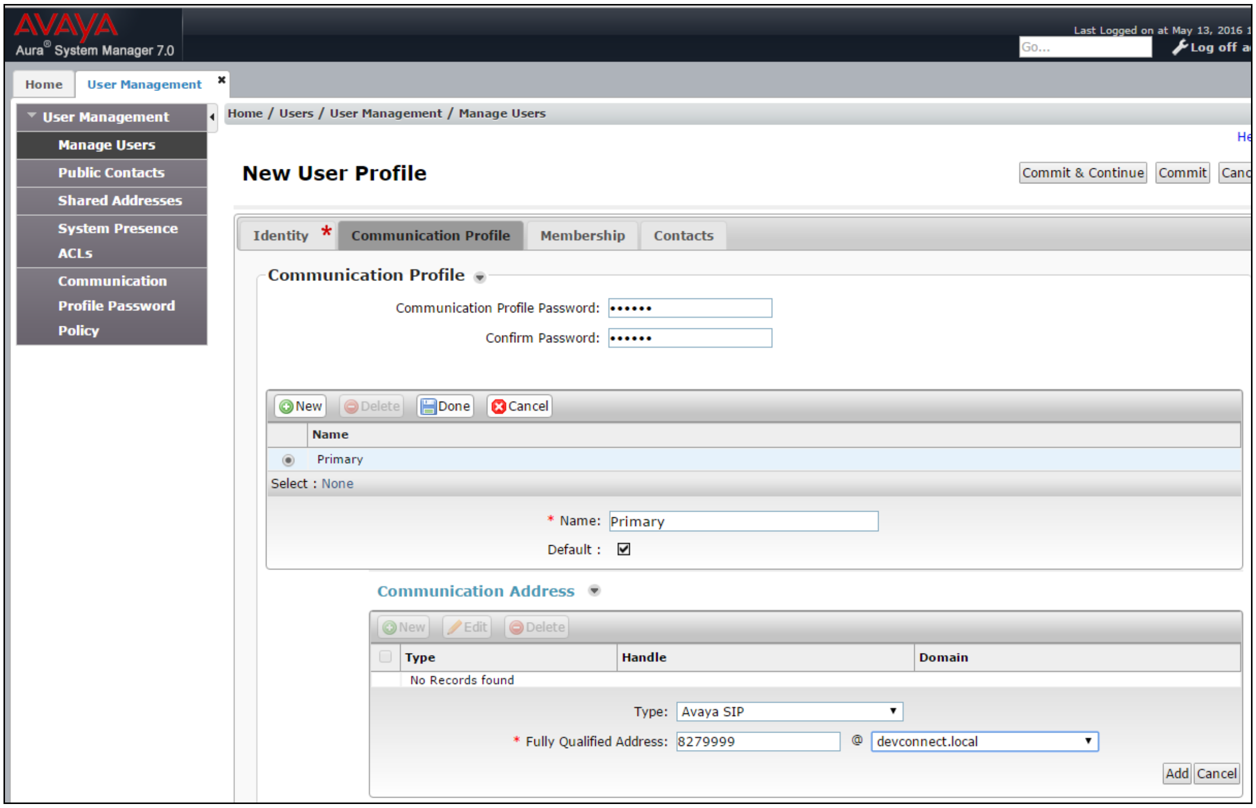
From the Dashboard, select **Users → User Management → Manage Users → New**



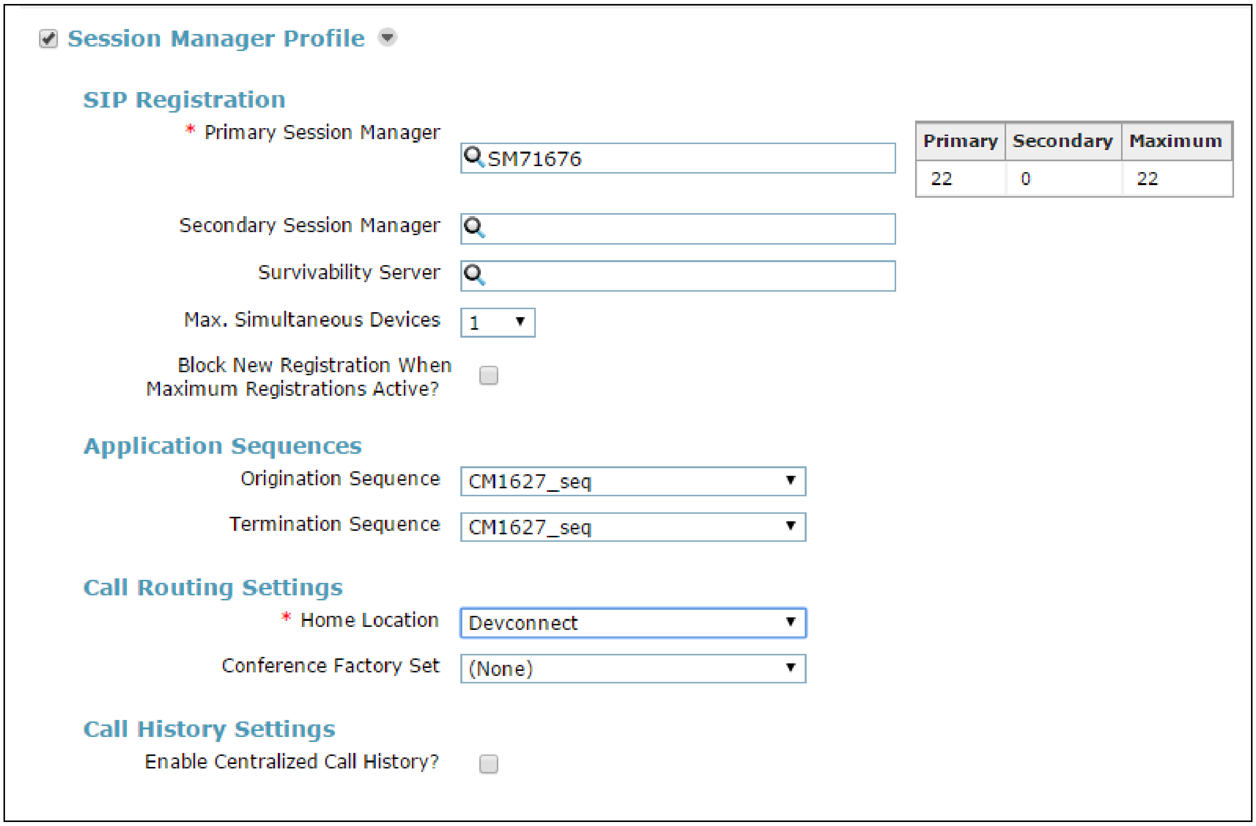
On the Identity tab enter an identifying **Last Name** and **First Name**, enter an appropriate **Login Name**, set **Authentication Type** to **Basic** and administer a password in the **Password** and **Confirm Password** fields.



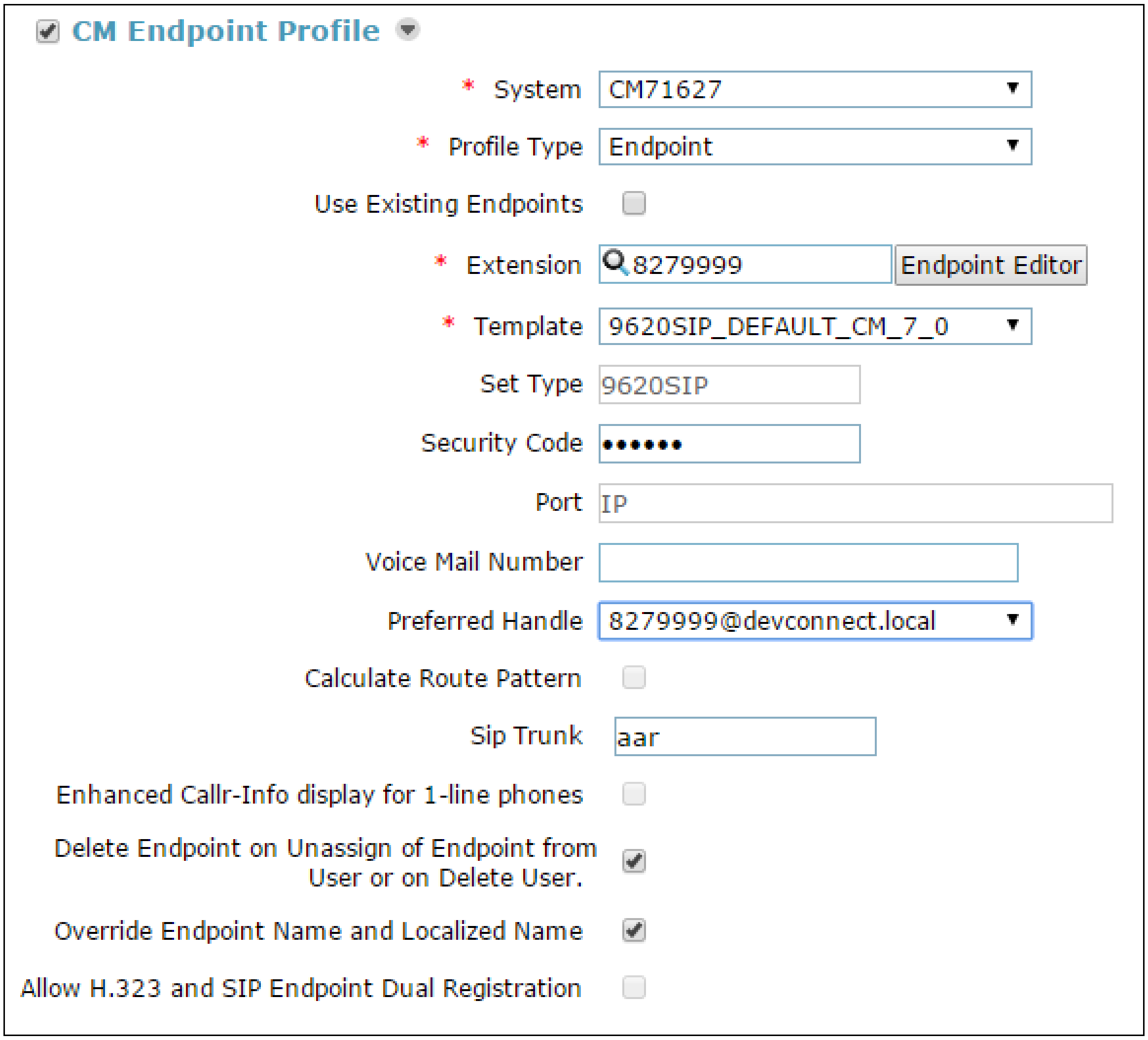
Click on the **Communication Profile** tab and enter and confirm a **Communication Profile Password**, this is used when logging in the SIP endpoint. Under **Communication Address** click **New**, select **Avaya SIP** from the **Type** drop down box and enter the **Fully Qualified Address** of the new SIP user. Click **Add** when done.



Continue to scroll down on the same page, enter the **Primary Session Manager, Origination Application Sequence, Termination Application Sequence** and **Home Location** relevant to the implementation.



Scroll down the page to the **CM Endpoint Profile** section. Select the Communication Manager system from the **System** drop down box, select **Endpoint** as the **Profile Type**, enter the **Extension** number, select **9620SIP_DEFAULT_CM_7_0** as the **Template** and ensure **IP** is configured as the **Port**, click Commit (not shown) when done. Repeat this for every SIP extension required.



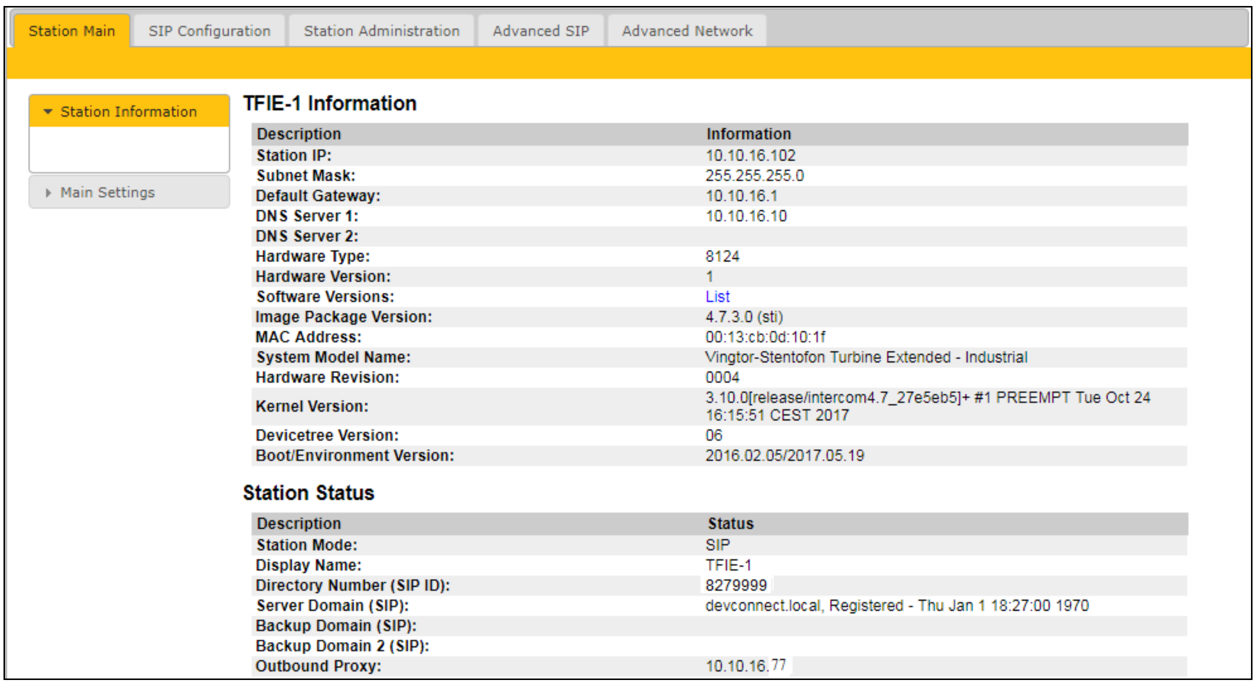
6. Configure Zenitel Turbine

The following steps detail the configuration for Turbine using the Web Interface. The steps include the following areas:

- Launch Web Interface
- Add Root Certificate
- Administer SIP Settings
- Configure Direct Access Key

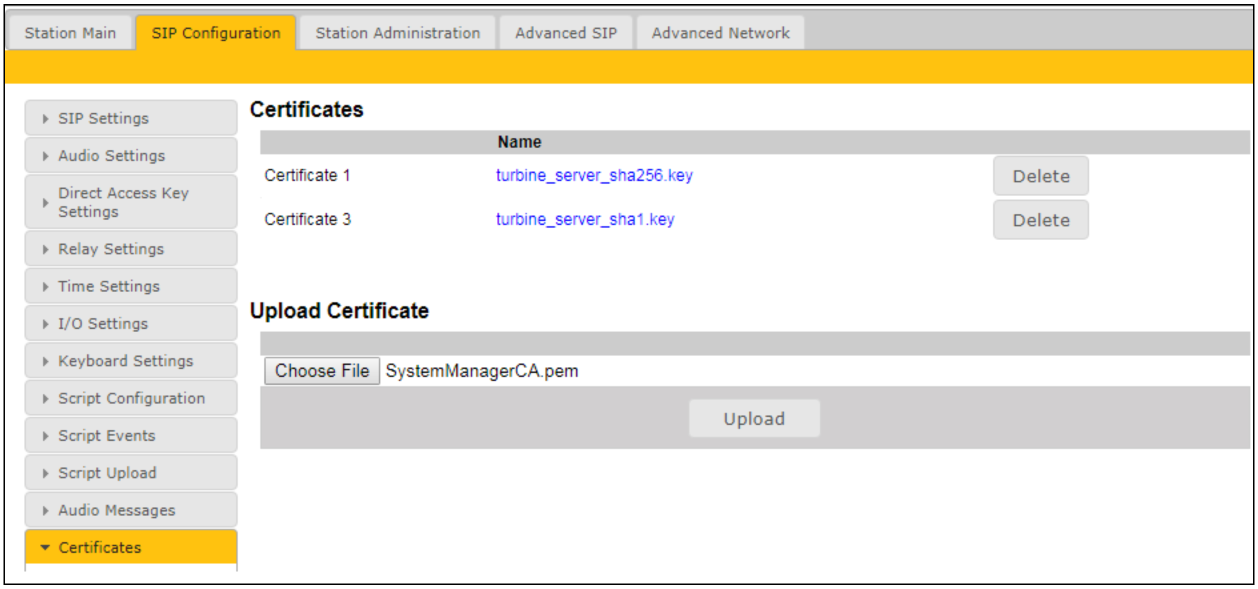
6.1. Launch Web Interface

Access the Turbine web interface, enter **http://<ipaddress>** in an Internet browser window, where **<ipaddress>** is the IP address of Turbine. Log in with the appropriate credentials. The **IP-StationWeb** screen is shown.

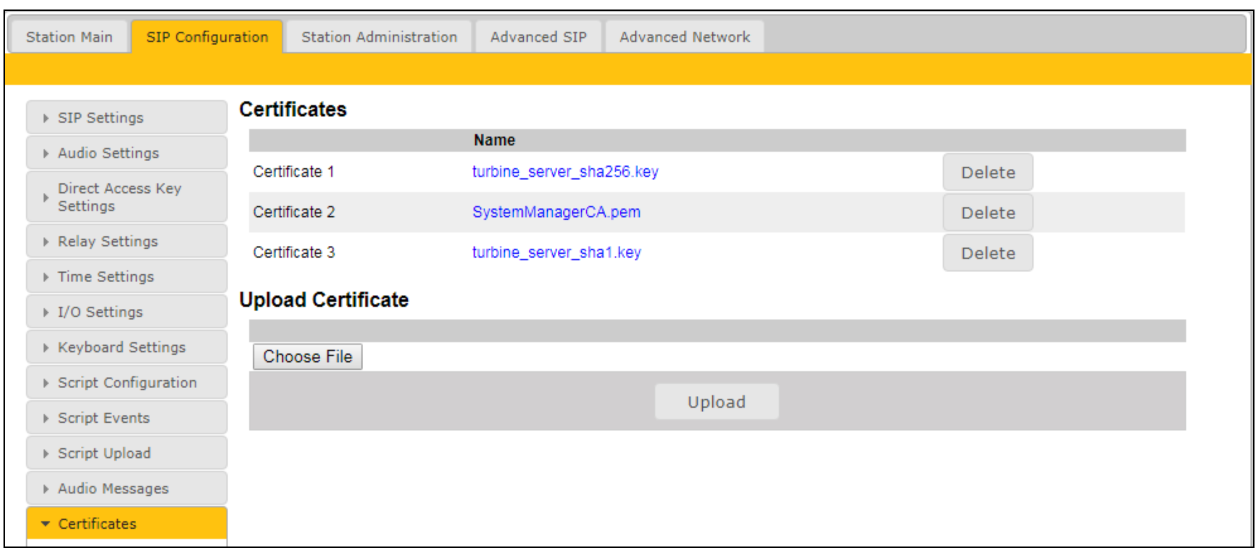


6.2. Add Session Manager root Certificate

Select **SIP Configuration** tab and from the left hand menu select **Certificates**. The Turbine certificates are listed. Click on the **Choose file** and browse to the location of the root certificate .pem file. When selected, click on the **Upload** button.

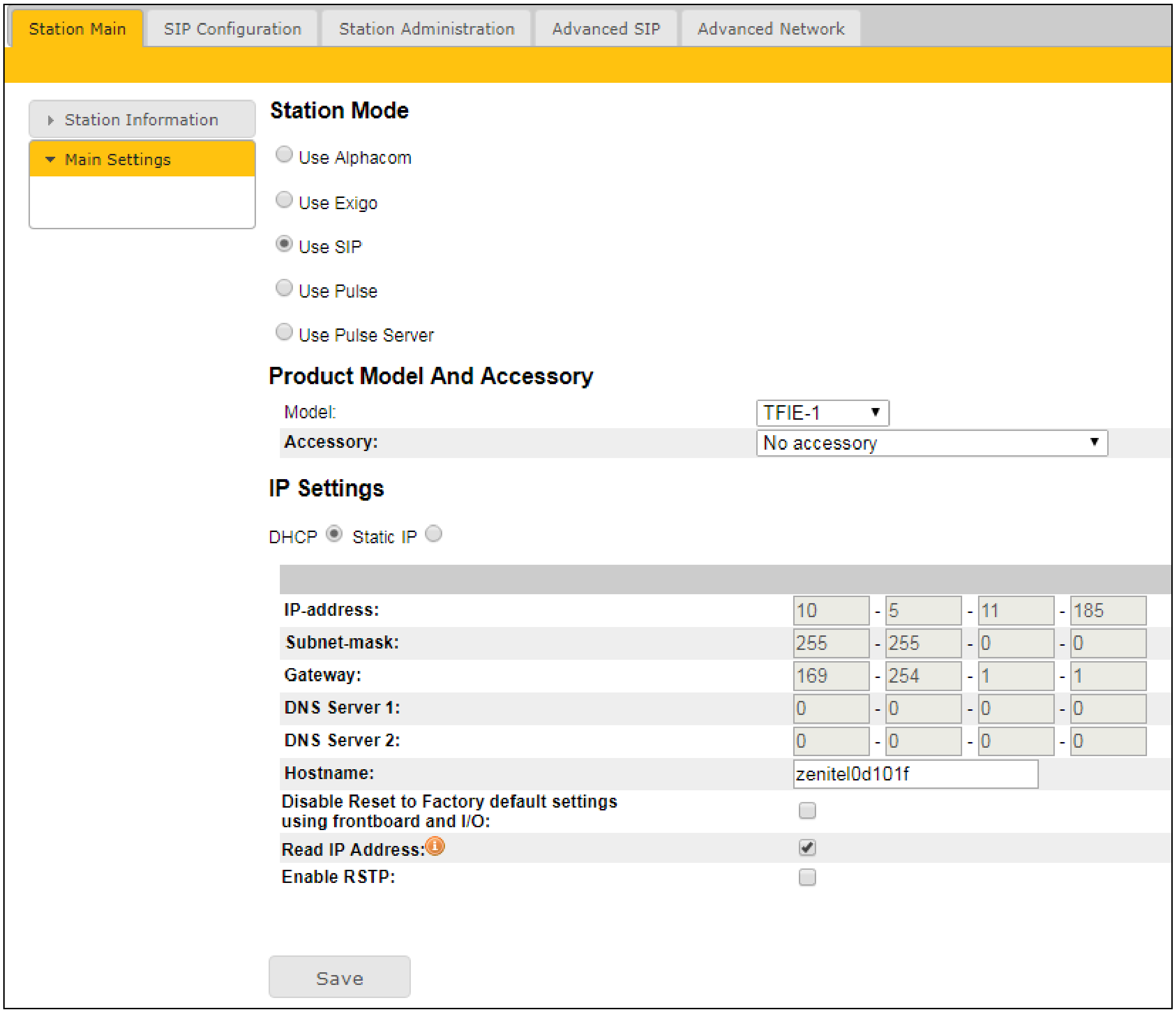


The root certificate is uploaded and is shown in the list.



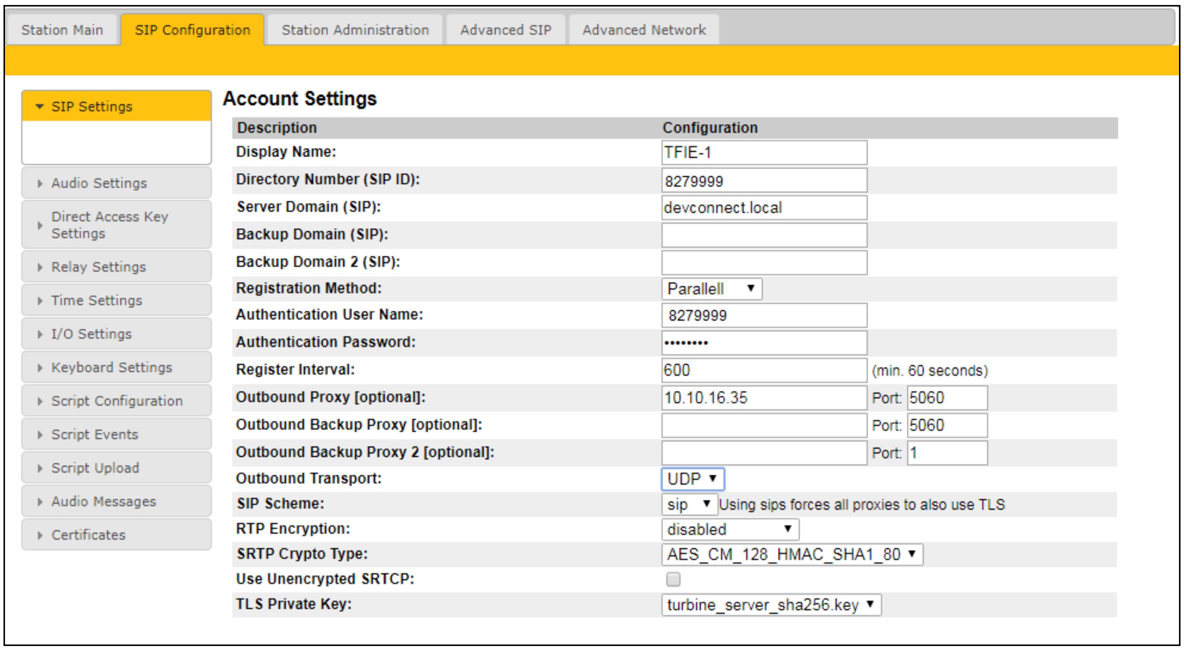
6.3. Administer SIP Settings

Select **Main Settings** from the left menu and select **Use SIP**. From the **Model:** drop down menu choose **TCIS 1-3,TCIS 4-5, TCIV-3/TCIV6, TFIE 1-2** or **Mini (TMIS-1)** depending on the model tested. click **Save** when done. A screen will appear (not shown) to confirm the setting, click Apply and Turbine will reboot.

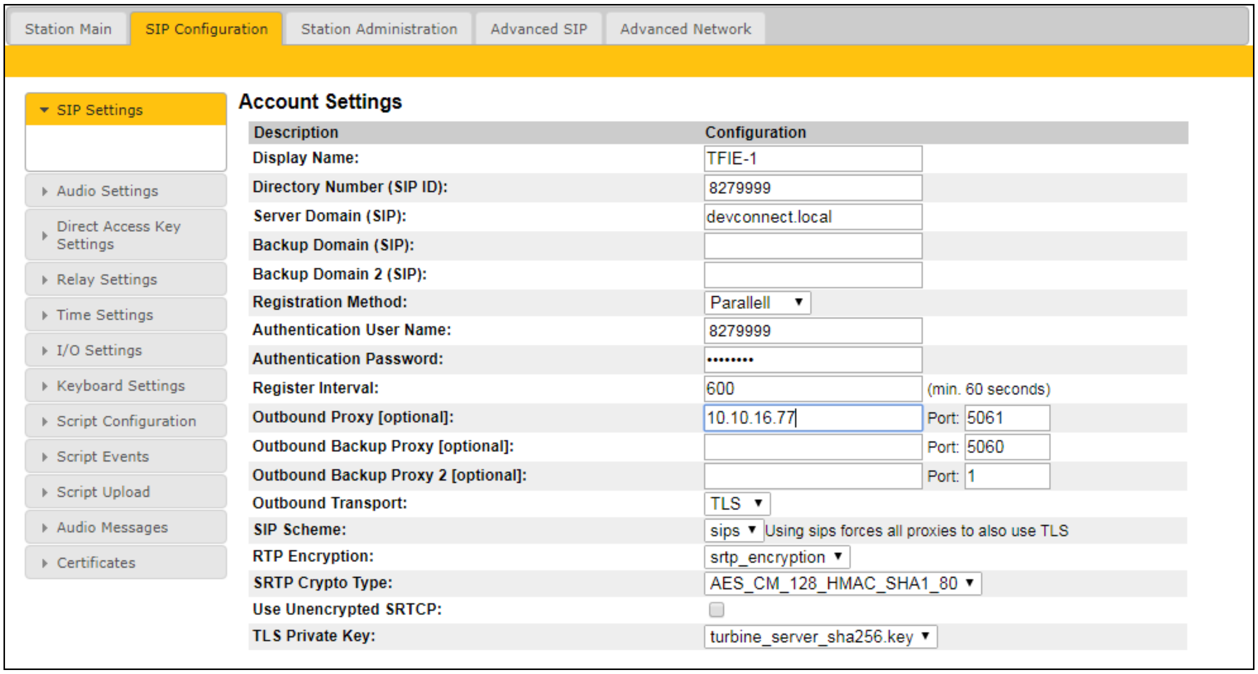


Click on **SIP Configuration → SIP Settings** and configure the following in the **Account Settings** section:

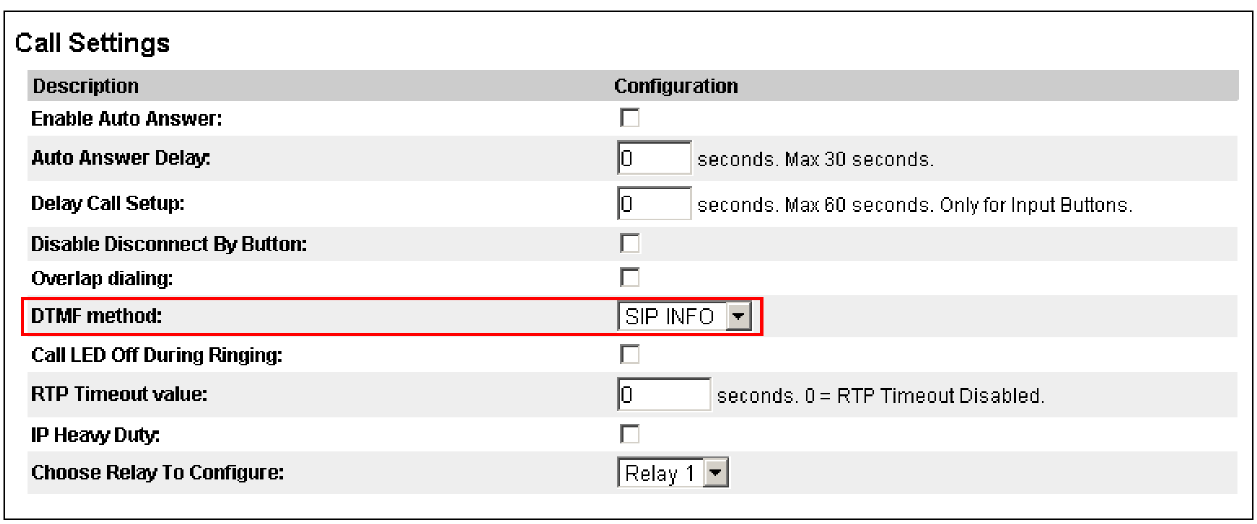
- **Display name**: Enter the desired name.
- **Directory Number (SIP ID)**: Enter a user extension administered from **Section 5.2**.
- **Server Domain (SIP)**: Enter the Domain of Session Manager.
- **Authentication User Name**: Enter a user extension administered from **Section 5.2**.
- **Authentication Password**: Enter the **Communication Profile Password** from **Section 5.2**.
- **Outbound Proxy (optional)**: Enter the IP address of Session Manager and **5060** as the **Port** for UDP/TCP**.**



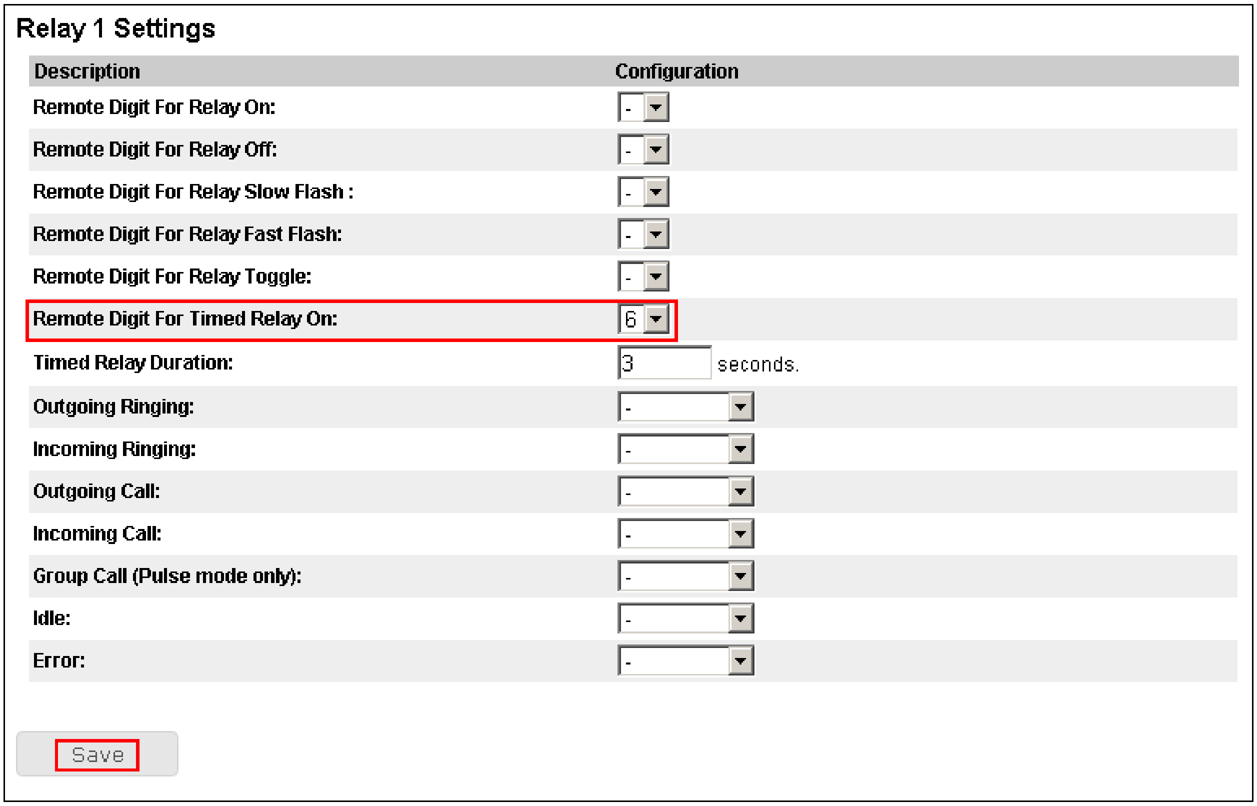
- **Outbound Proxy (optional)**: Enter the IP address of Session Manager and **5061** as the **Port** for TLS
- **SIP Scheme**: Choose **sips** from the drop down.
- **RTP Encryption**: Select **srtp_encryption** from the drop down.



In the **Call Settings** section, configure as required the **DTMF Method** as **SIP INFO** or RFC 2833 (not shown), this allows DTMF tones to be either sent in-band or using SIP INFO messaging. Configure other options as required.

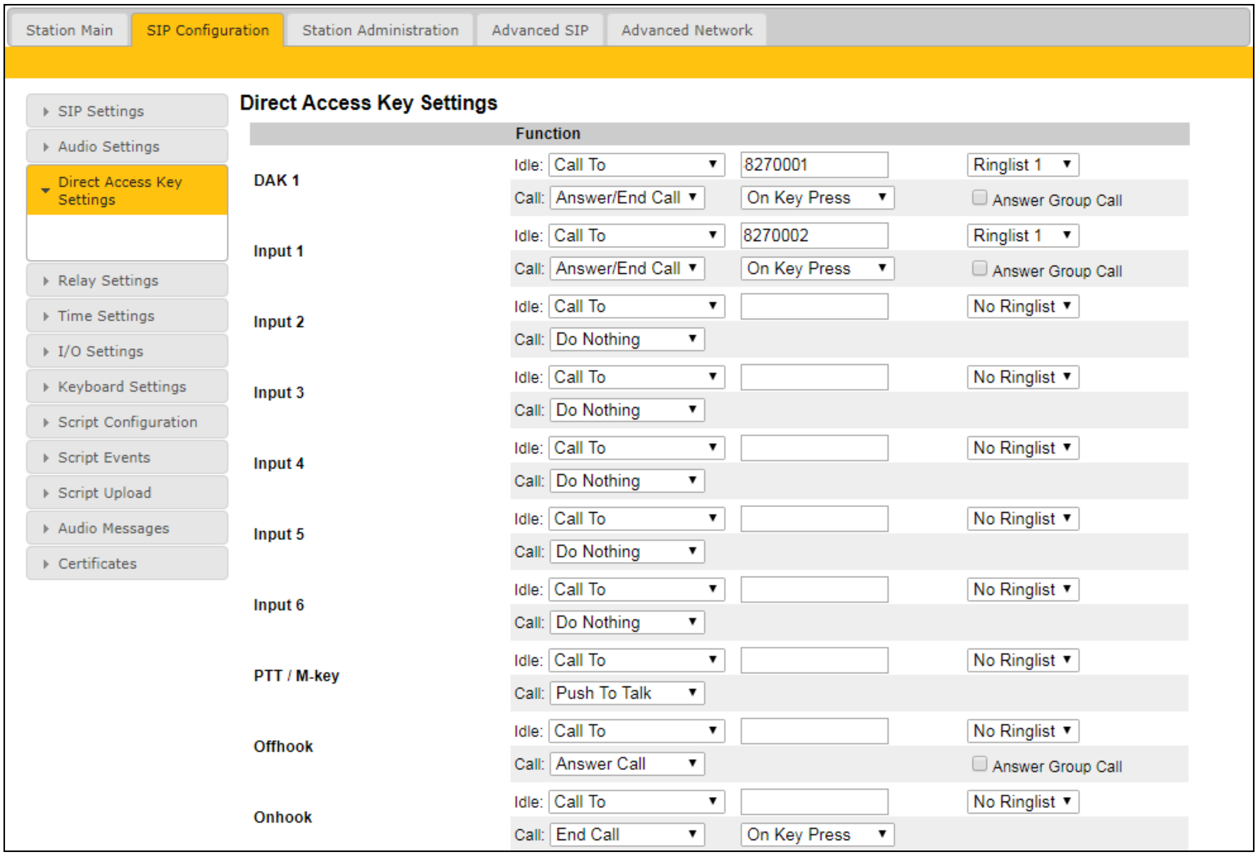


In the **Relay 1 Settings** section select a digit from the drop down box for **Remote Digit for Timed Relay On**. When this digit is pushed by a called party, the relay in the Turbine will be energized. Retain the default values for the remaining fields. Click **Save** when done. A screen will appear (not shown) to confirm the setting, click Reboot and Turbine will reboot.



6.4. Configure Direct Access Key

Select **SIP Configuration → Direct Access Key Settings** from the left menu and select **DAK 1** to configure it. In the **Idle** field select **Call To** from the drop down and enter the extension to be called when the **DAK 1** key is pushed. In the **Call** field select **Answer/End Call** and **On Key Press**.

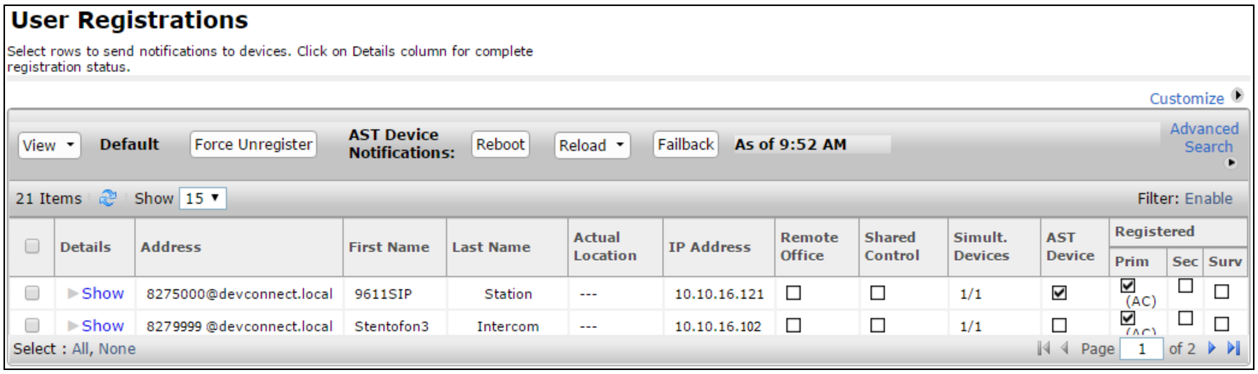


7. Verification Steps

This section provides the tests that can be performed to verify correct configuration of Session Manager and Turbine.

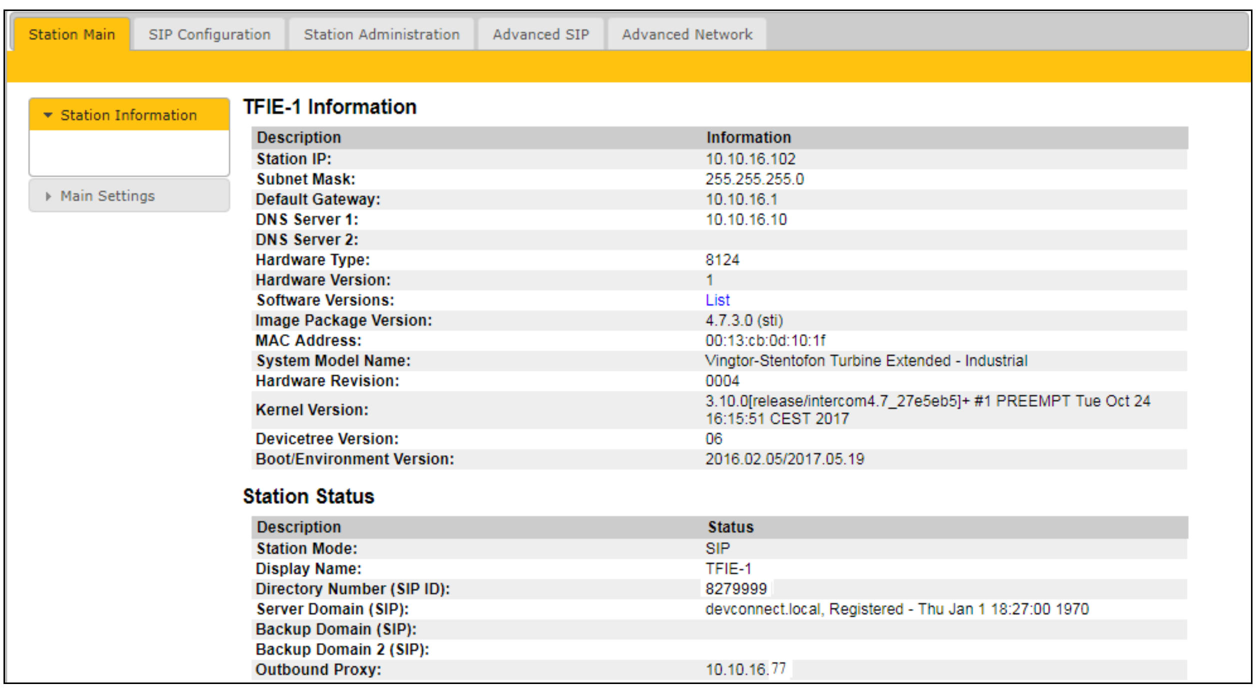
7.1. Verify Avaya Aura® Session SIP Endpoint Registration

From the System Manager web interface, click **Session Manager → System Status → User Registrations.** Verify that Turbine endpoints are successfully registered as shown below.



7.2. Verify Turbine SIP Registration

From the Turbine web interface, select **Information** from the left menu. Verify that the **Registration state** shows **Registered**. Place a call to another endpoint to verify basic call operation.



7.3. Verify Successful Calls

Place a call to and from the Turbine endpoint. Verify 2-way audio is heard and validate call terminates successfully.

8. Conclusion

These Application Notes describe the configuration steps required for configuring Zenitel Turbine IP Intercom Substation to interoperate with Avaya Aura® Session Manager and Avaya Aura® Communication Manager. All feature and serviceability tests were completed successfully with observations made in **Section 2.2**.

9. Additional References

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

The following Avaya product documentation can be found at http://support.avaya.com.

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

[2] *Administering Avaya Aura® Communication Manager Release 7.1,8 May 2017* Document ID 03-300509

[3] *Avaya Aura® Communication Manager Feature Description and Implementation Release 7.1 8 May 2017*, Document ID 555-245-205

[4] *Administering Avaya Aura® System Manager 7.1.1, October 2017*

The Zenitel Turbine documentation can be found at http://www.zenitel.com.

[5] *A100K11013-Pulse-Getting-Started.pdf.*

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.