Avaya Solution & Interoperability Test Lab

Application Notes for Primas Group LinkScope Customer Experience Power Pack with Avaya Aura® Experience Portal – Issue 1.1

Abstract

These Application Notes describe the configuration steps required to integrate the Primas Group LinkScope Customer Experience Power Pack with Avaya Aura® Communication Manager, Avaya Aura® Application Enablement Services and Avaya Aura® Experience Portal.

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 in Thornton, CO.

1. Introduction

These Application Notes describe the configuration steps required to integrate the Primas Group LinkScope Customer Experience Power Pack (LinkScope) with Avaya Aura® Communication Manager (Communication Manager), Avaya Aura® Application Enablement Services (AES) and Avaya Aura® Experience Portal (Experience Portal).

LinkScope integrates with Communication Manager via TSAPI using AES and it also hosts CCXML and VXML applications that are used by Experience Portal. By the use of Avaya provided APIs, LinkScope provides the following features:

- Basic Screen Pop: Screen Pop to agent desktop when call arrives. Provides basic call information (ANI/DNIS) via Primas Notifier desktop client.
- Enhanced Pop: Repeat caller notification with customizable screen pop window. Includes IVR collected data, caller history and agent scripting.
- WebFQ: Click-to-be-called solution that queues callers into the call center via website. Deploys with customizable html widget that integrates into the LinkScope Server.
- ReconX: Agent desktop re-connect solution. Upon a disconnected call, a popup window provides a clickable option to automatically place an outbound call, verify the previous caller, and reconnect them to the agent.
- FreedomQ: Automated customer call back and queuing solution. Based on configurable hold time thresholds inbound customers are automatically offered the option to receive a callback when undesirable hold-times are met.
- Automated Post Call Survey: Based on call center parameters per caller, such as number of calls, transfers or hold times, customer surveys are automatically triggered.

2. General Test Approach and Test Results

This section describes the interoperability compliance testing used to verify the LinkScope with Avaya products.

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

2.1. Interoperability Compliance Testing

Interoperability compliance testing included feature and serviceability testing. The feature testing focused on the following functionality:

- Basic Pop and Enhanced Pop for incoming ACD Calls.
- Experience Portal successfully running the LinkScope application and all of the call back options.
- The ability of the caller to continue waiting in queue for an agent.
- The ability of the caller to make a call back request.
- LinkScope servicing pending call back requests and running the Callback application via Experience Portal.
- Failure conditions, such as the call back failing due to network problems, and verifying that the call back was rescheduled.

The serviceability testing focused on verifying the ability of the LinkScope to recover from adverse conditions, such as power failures and disconnecting cables to the IP network.

2.2. Test Results

All test cases passed.

2.3. Support

For technical support on LinkScope, contact Primas Group via phone, email, or internet.

- **Phone:** 888-4PRIMAS | 888-477-4627
- **Email:** support@primas.net
- **Web:** www.primas.net/contact.html

3. Reference Configuration

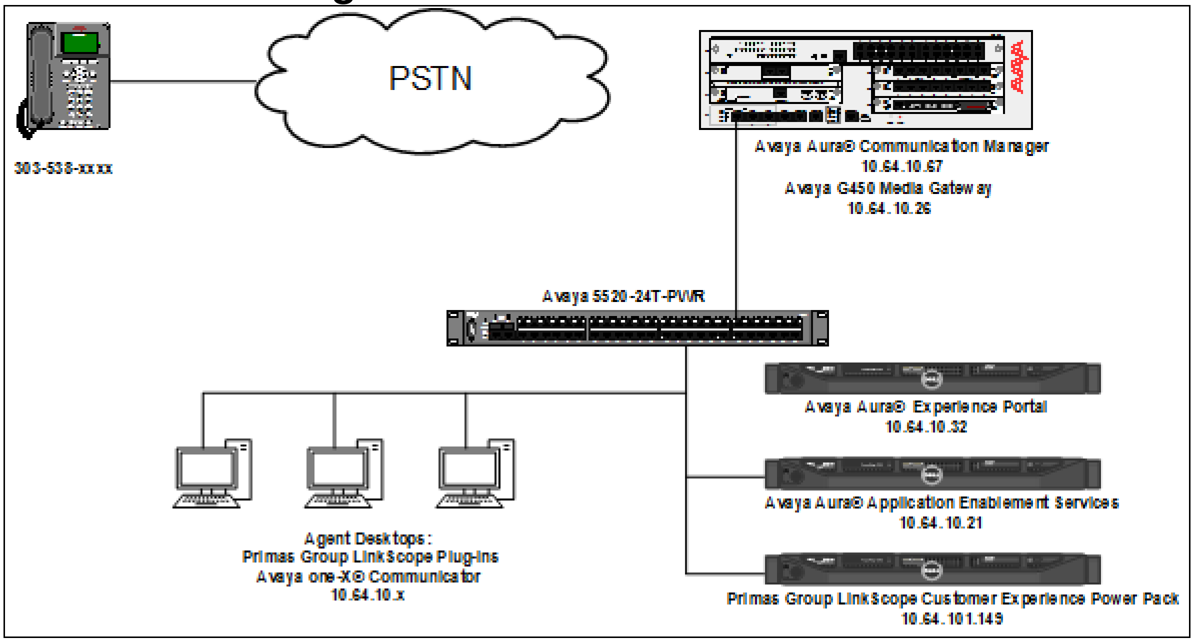
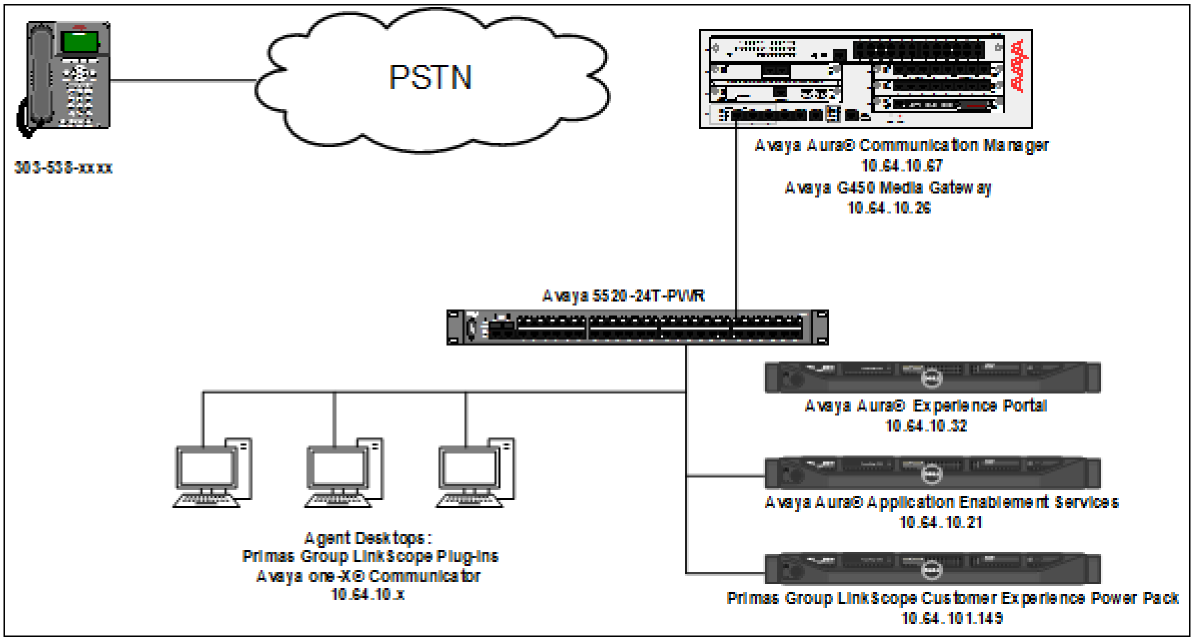

PSTN
303-538-xxxx
Avaya Aura® Communication Manager
10.64.10.67
Avaya G450 Media Gateway
10.64.10.26
Avaya 5520-24T-PWR
Avaya Aura® Experience Portal
10.64.10.32
Avaya Aura® Application Enablement Services
10.64.10.21
Agent Desktops:
Primas Group LinkScope Plug-ins
Avaya one-X® Communicator
10.64.10.x
Primas Group LinkScope Customer Experience Power Pack
10.64.101.149

Figure 1 illustrates the configuration used for testing. In this configuration, Avaya Aura® Experience Portal interfaces with Avaya Aura® Communication Manager via H.323. Avaya Aura® Communication manager interfaces with Primas Group LinkScope Customer Experience Power Pack via a CTI Link using Avaya Aura® Application Enablement Services. The LinkScope server hosted LinkScope and CCXML/VXML applications supporting the inbound and outbound modules. Agent Desktops were used by call center agents to log in using Avaya one-X® Communicator. LinkScope plug-ins for notifications were installed on Agent Desktops.



PSTN
303-538-xxxx
Avaya Aura® Communication Manager
10.64.10.67
Avaya G450 Media Gateway
10.64.10.26
Avaya 5520-24T-PWR
Avaya Aura® Experience Portal
10.64.10.32
Avaya Aura® Application Enablement Services
10.64.10.21
Agent Desktops:
Primas Group LinkScope Plug-ins
Avaya one-X® Communicator
10.64.10.x
Primas Group LinkScope Customer Experience Power Pack
10.64.101.149

Figure 1: Configuration with Avaya products with Primas Group LinkScope

4. Equipment and Software Validated

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

Equipment	Software
Avaya Aura® Experience Portal	7.0.2
Avaya Aura® Communication Manager running on S8300D server	6.3 SP10
Avaya G450 Media Gateway	31.20.1
Avaya Aura® Application Enablement Services	6.3 SP3
Avaya one-X® Communicator	6.2 SP6
Primas LinkScope Customer Experience Power Pack running on a Windows 2008 R2 Server Virtual Machine	7.1

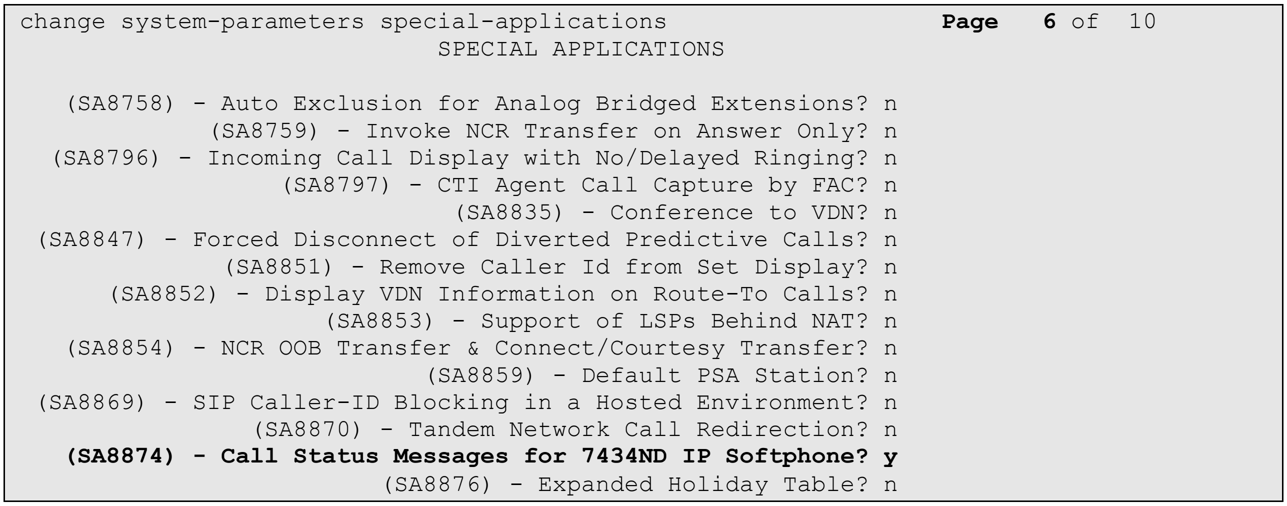
5. Configure Avaya Aura® Communication Manager

This section provides the procedures for configuring Communication Manager via the System Access Terminal (SAT). The procedures include the following areas:

- Administer Special Applications
- Administer H.323 Stations
- Administer Hunt Groups
- Administer Agent IDs
- Administer Call Vectoring
- Administer CTI link

5.1. Administer Special Applications

Using the **change system-parameters special-applications** command, on **Page 6** enable the SA8874 feature. This feature is used for H.323 connections to Experience Portal for supervised transfer or the Application Interface web service for outbound calls.

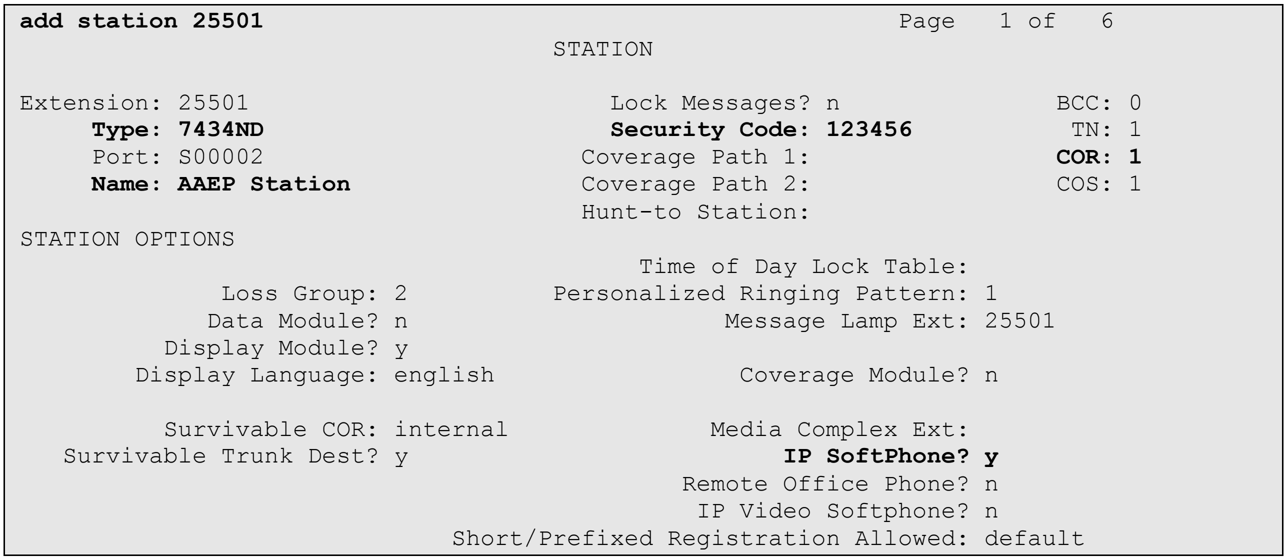


```
change system-parameters special-applications                  Page   6 of  10
                             SPECIAL APPLICATIONS

   (SA8758) - Auto Exclusion for Analog Bridged Extensions? n
             (SA8759) - Invoke NCR Transfer on Answer Only? n
  (SA8796) - Incoming Call Display with No/Delayed Ringing? n
                  (SA8797) - CTI Agent Call Capture by FAC? n
                              (SA8835) - Conference to VDN? n
 (SA8847) - Forced Disconnect of Diverted Predictive Calls? n
              (SA8851) - Remove Caller Id from Set Display? n
       (SA8852) - Display VDN Information on Route-To Calls? n
                     (SA8853) - Support of LSPs Behind NAT? n
   (SA8854) - NCR OOB Transfer & Connect/Courtesy Transfer? n
                            (SA8859) - Default PSA Station? n
 (SA8869) - SIP Caller-ID Blocking in a Hosted Environment? n
                (SA8870) - Tandem Network Call Redirection? n
   (SA8874) - Call Status Messages for 7434ND IP Softphone? y
                          (SA8876) - Expanded Holiday Table? n
```

5.2. Administer H.323 Stations for Avaya Aura® Experience Portal

This section describes the configuration of H.323 stations for Avaya Aura® Experience Portal.

Add an H.323 station for Experience Portal using the **add station** command. In the station form, set the **Type** to **7434ND**, provide a descriptive **Name**, set the **Security Code**, and set the **IP Softphone** field to **y**. The **COR** specified for this station should allow outgoing trunk calls. Repeat this step for each Avaya Aura® Experience Portal station.



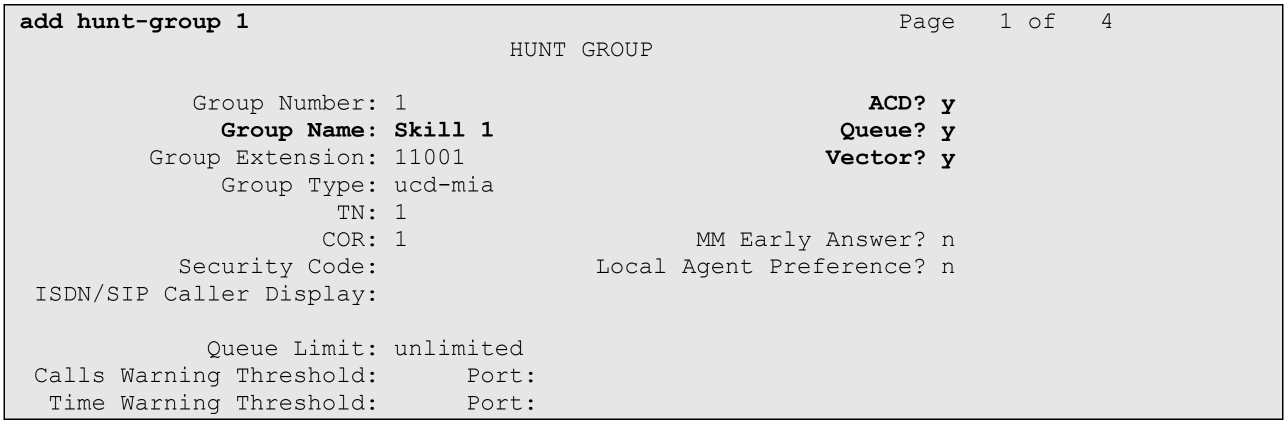
```
add station 25501                                            Page   1 of   6
                                     STATION

Extension: 25501                         Lock Messages? n               BCC: 0
     Type: 7434ND                        Security Code: 123456           TN: 1
     Port: S00002                      Coverage Path 1:                 COR: 1
     Name: AAEP Station                Coverage Path 2:                 COS: 1
                                       Hunt-to Station:
STATION OPTIONS
                                           Time of Day Lock Table:
              Loss Group: 2         Personalized Ringing Pattern: 1
             Data Module? n                     Message Lamp Ext: 25501
          Display Module? y
        Display Language: english                Coverage Module? n

          Survivable COR: internal              Media Complex Ext:
   Survivable Trunk Dest? y                          IP SoftPhone? y
                                              Remote Office Phone? n
                                               IP Video Softphone? n
                              Short/Prefixed Registration Allowed: default
```

Similarly, add stations for call center agents using the same command. Set **Type** according to the phones that are being added.

5.3. Administer Hunt Groups

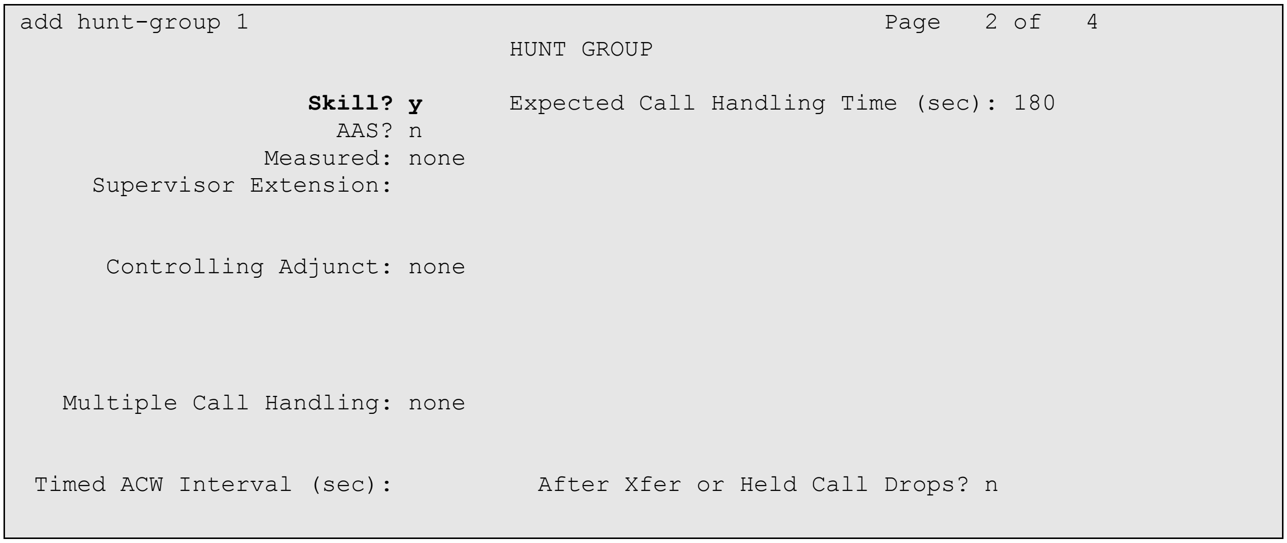
This section provides the Hunt Group configuration for the call center agents and the Experience Portal ports.

For call center agents, using the **add hunt-group** command add a hunt group. Provide a descriptive name and set the **Group Extension** field to a valid extension. Enable the **ACD**, **Queue**, and **Vector** options. This hunt group will be specified in the **Agent LoginIDs** configured in **Section 5.4**.



```
add hunt-group 1                                                Page   1 of   4
                                  HUNT GROUP

            Group Number: 1                                ACD? y
              Group Name: Skill 1                        Queue? y
         Group Extension: 11001                         Vector? y
              Group Type: ucd-mia
                      TN: 1
                     COR: 1                    MM Early Answer? n
           Security Code:               Local Agent Preference? n
 ISDN/SIP Caller Display:

             Queue Limit: unlimited
 Calls Warning Threshold:     Port:
  Time Warning Threshold:     Port:
```

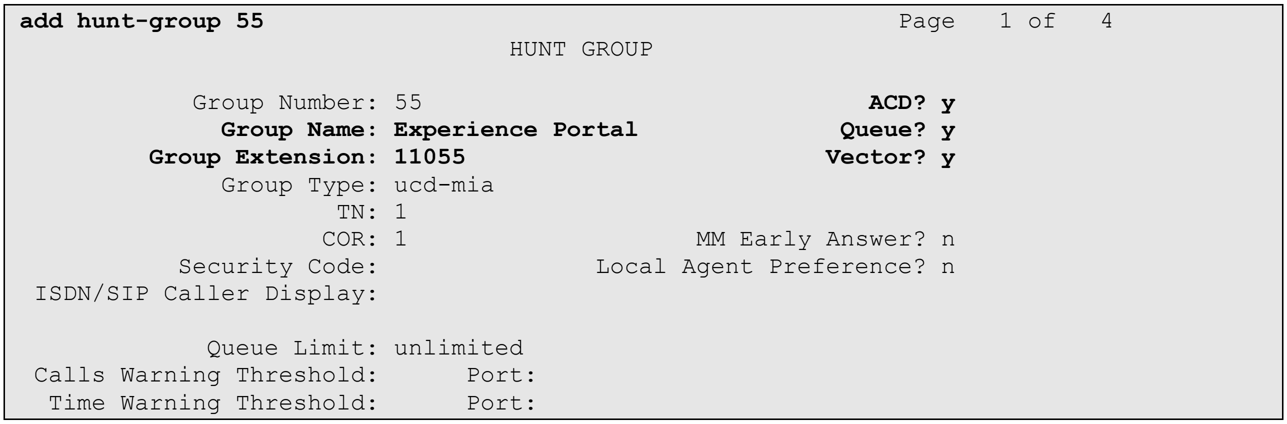
On **Page 2** of the Hunt Group form, enable the **Skill** option.



```
add hunt-group 1                                               Page   2 of   4
                                  HUNT GROUP

                     Skill? y      Expected Call Handling Time (sec): 180
                       AAS? n
                  Measured: none
       Supervisor Extension:


        Controlling Adjunct: none




     Multiple Call Handling: none


 Timed ACW Interval (sec):          After Xfer or Held Call Drops? n
```

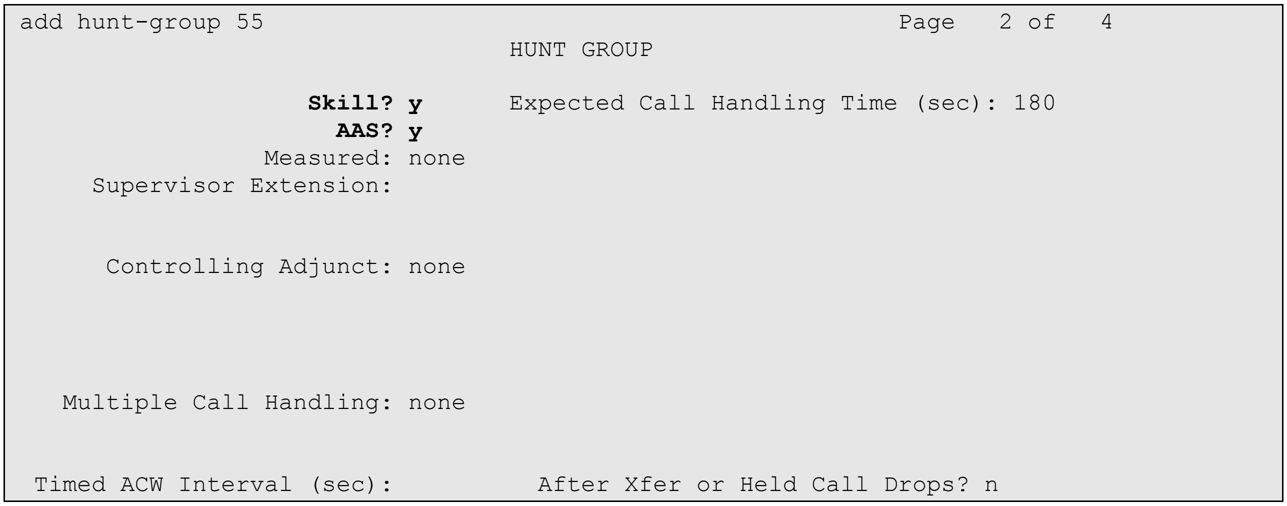
For compliance testing, hunt groups 1 and 2 were created for call center agents.

The Experience Portal ports, configured as H.323 stations, will automatically log into Hunt Group 55 configured below. Provide a descriptive **Group Name** and set the **Group Extension** field to a valid extension. Enable the **ACD**, **Queue**, and **Vector** options. This hunt group will be specified in the **Agent LoginIDs** configured in **Section 5.4**.



```
add hunt-group 55                                            Page   1 of   4
                                  HUNT GROUP

            Group Number: 55                               ACD? y
              Group Name: Experience Portal              Queue? y
         Group Extension: 11055                         Vector? y
              Group Type: ucd-mia
                      TN: 1
                     COR: 1                    MM Early Answer? n
           Security Code:               Local Agent Preference? n
 ISDN/SIP Caller Display:

             Queue Limit: unlimited
 Calls Warning Threshold:      Port:
  Time Warning Threshold:      Port:
```

On **Page 2** of the Hunt Group form, enable the **Skill** and **AAS** options. The **AAS** option will allow the Experience Portal ports to automatically log into the hunt group via the **Agent LoginIDs**.



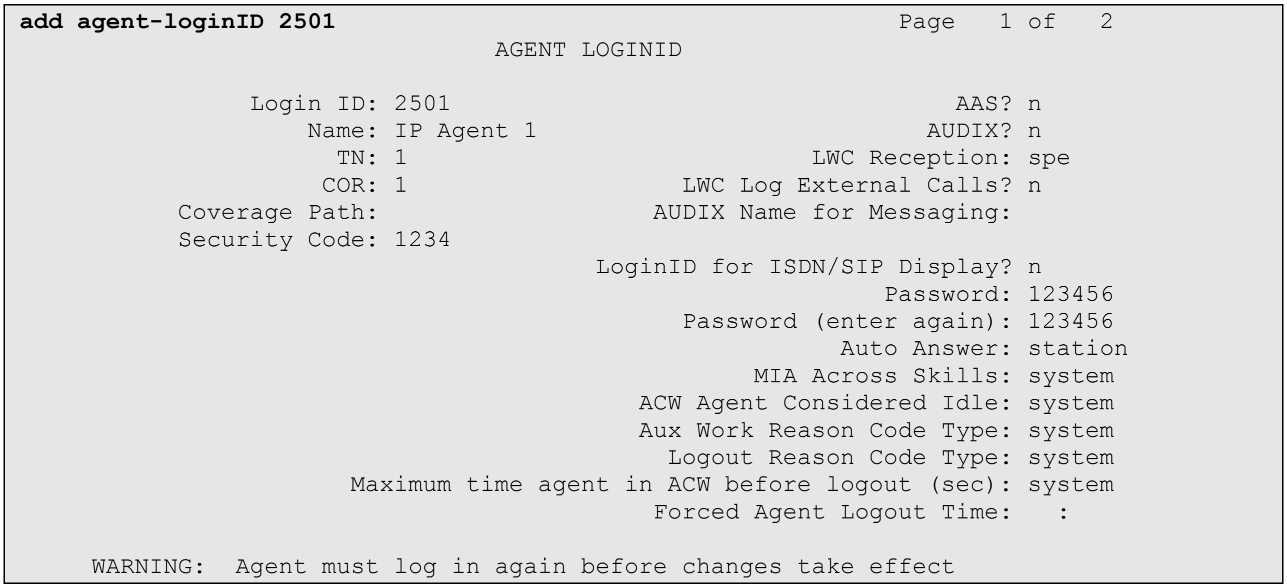
```
add hunt-group 55                                            Page   2 of   4
                                  HUNT GROUP

                    Skill? y      Expected Call Handling Time (sec): 180
                      AAS? y
                 Measured: none
     Supervisor Extension:


      Controlling Adjunct: none




   Multiple Call Handling: none


 Timed ACW Interval (sec):          After Xfer or Held Call Drops? n
```

During the compliance test, hunt groups 1, 2 and 55 were created with extensions 11001, 11002 and 11055, respectively.

5.4. Administer Agent IDs

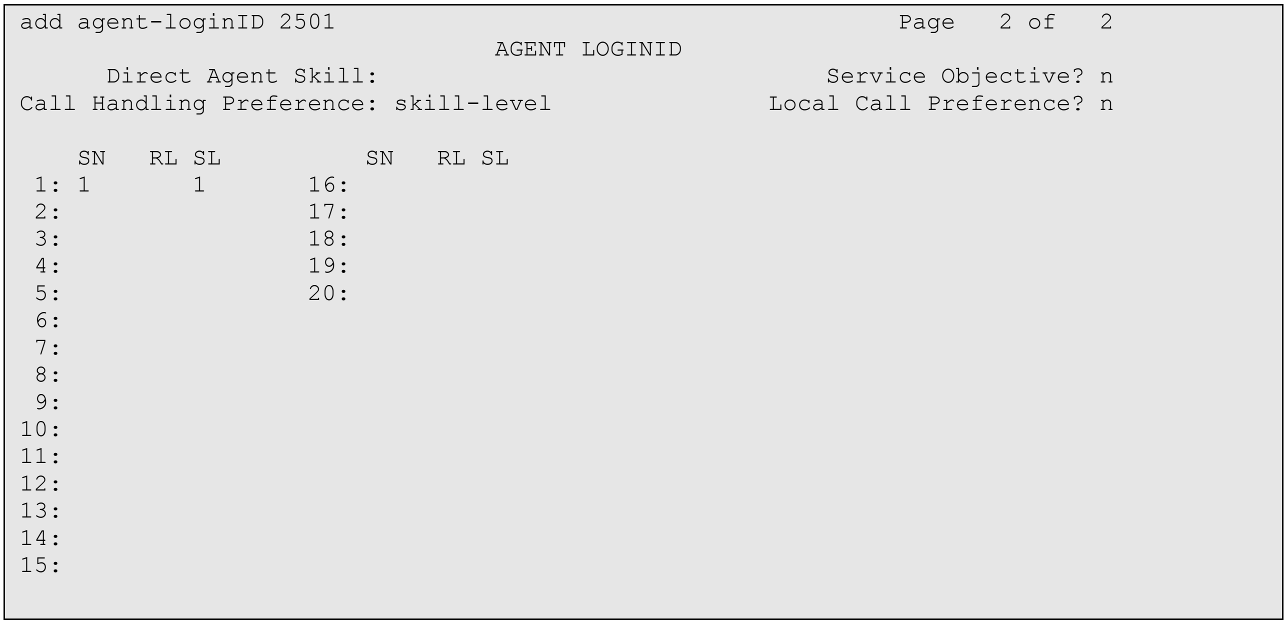
This section provides the Agent Login IDs for the agents and the Avaya Aura® Experience Portal ports.

Add an agent login id using the **add agent-loginID** command for each agent in the call center as shown below.



```
add agent-loginID 2501                                       Page   1 of   2
                                 AGENT LOGINID

                Login ID: 2501                                    AAS? n
                    Name: IP Agent 1                            AUDIX? n
                      TN: 1                             LWC Reception: spe
                     COR: 1                    LWC Log External Calls? n
           Coverage Path:                    AUDIX Name for Messaging:
           Security Code: 1234
                                        LoginID for ISDN/SIP Display? n
                                                            Password: 123456
                                              Password (enter again): 123456
                                                         Auto Answer: station
                                                   MIA Across Skills: system
                                           ACW Agent Considered Idle: system
                                           Aux Work Reason Code Type: system
                                             Logout Reason Code Type: system
                       Maximum time agent in ACW before logout (sec): system
                                            Forced Agent Logout Time:   :

     WARNING:  Agent must log in again before changes take effect
```

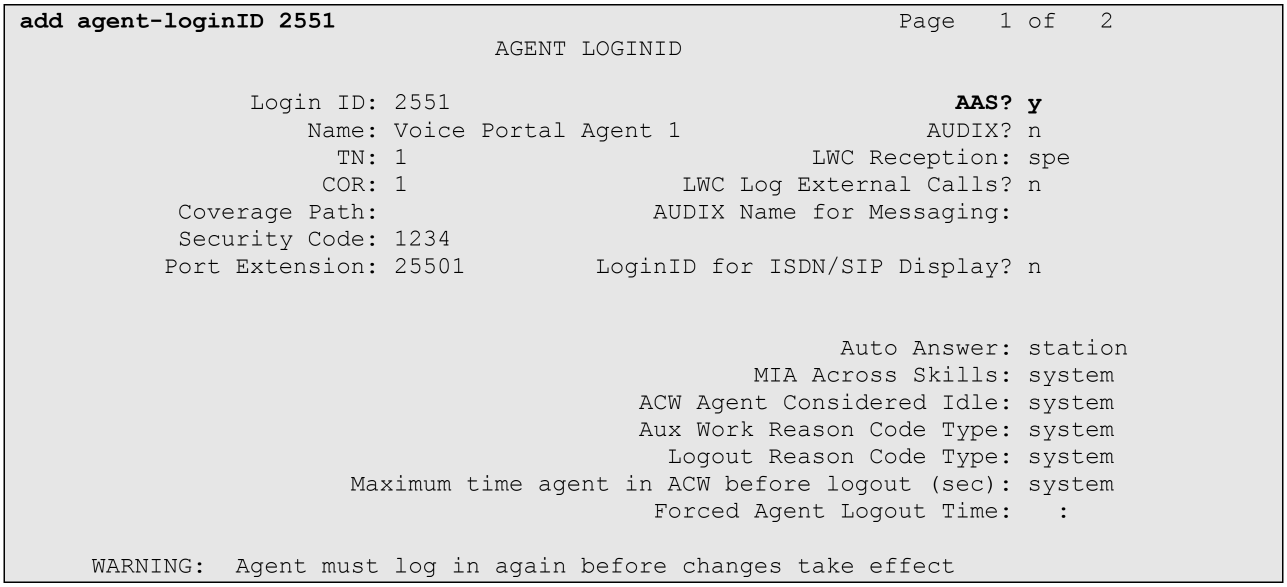
On **Page 2** of the **Agent LoginID** form, set the skill number (**SN**) to hunt group 1, which is the hunt group (skill) that the agents will log into.



```
add agent-loginID 2501                                       Page   2 of   2
                                 AGENT LOGINID
      Direct Agent Skill:                                Service Objective? n
Call Handling Preference: skill-level                Local Call Preference? n

    SN   RL SL           SN   RL SL
 1: 1       1       16:
 2:                 17:
 3:                 18:
 4:                 19:
 5:                 20:
 6:
 7:
 8:
 9:
10:
11:
12:
13:
14:
15:
```

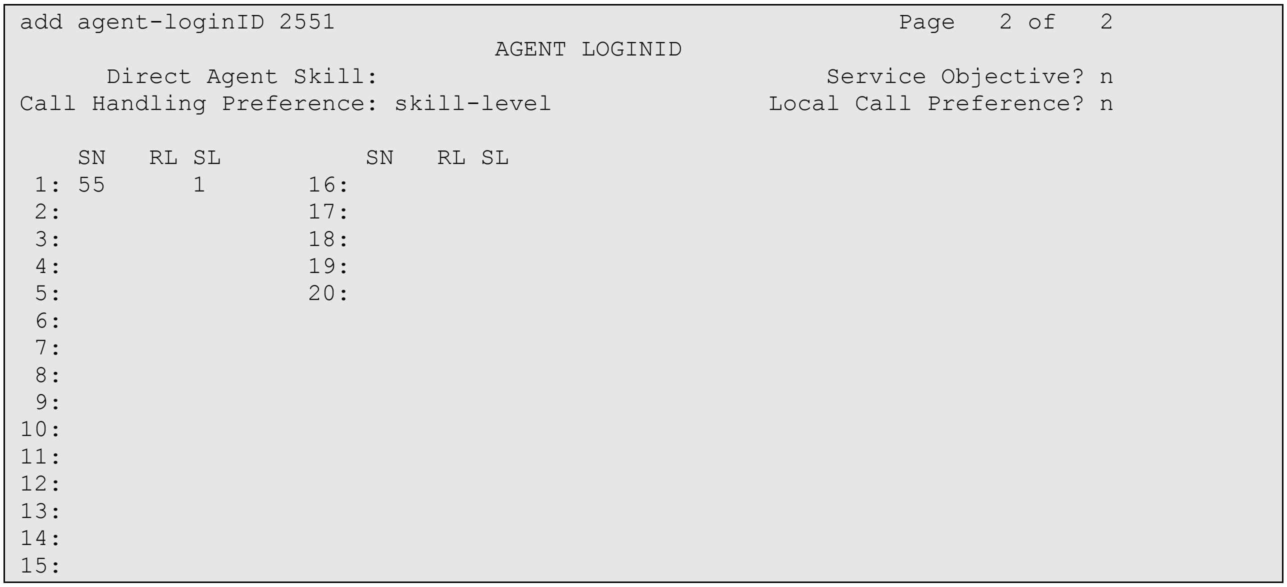
Add an **Agent LoginID** for each Experience Portal port. The **AAS** option is enabled and the **Port Extension** is set to the extension of the H.323 stations corresponding to each Experience

Portal port. Repeat this configuration for each H.323 station corresponding to a Experience Portal port.



```
add agent-loginID 2551                                       Page   1 of   2
                                 AGENT LOGINID

                Login ID: 2551                                    AAS? y
                    Name: Voice Portal Agent 1                  AUDIX? n
                      TN: 1                            LWC Reception: spe
                     COR: 1                   LWC Log External Calls? n
           Coverage Path:                   AUDIX Name for Messaging:
           Security Code: 1234
          Port Extension: 25501        LoginID for ISDN/SIP Display? n


                                                         Auto Answer: station
                                                   MIA Across Skills: system
                                           ACW Agent Considered Idle: system
                                           Aux Work Reason Code Type: system
                                             Logout Reason Code Type: system
                       Maximum time agent in ACW before logout (sec): system
                                            Forced Agent Logout Time:   :

     WARNING:  Agent must log in again before changes take effect
```

On **Page 2** of the **Agent LoginID** form, set the skill number (**SN**) to hunt group 55, which is the hunt group (skill) that the Experience Portal ports will log into.



```
add agent-loginID 2551                                       Page   2 of   2
                                 AGENT LOGINID
      Direct Agent Skill:                               Service Objective? n
Call Handling Preference: skill-level               Local Call Preference? n

    SN   RL SL          SN   RL SL
 1: 55      1       16:
 2:                 17:
 3:                 18:
 4:                 19:
 5:                 20:
 6:
 7:
 8:
 9:
10:
11:
12:
13:
14:
15:
```

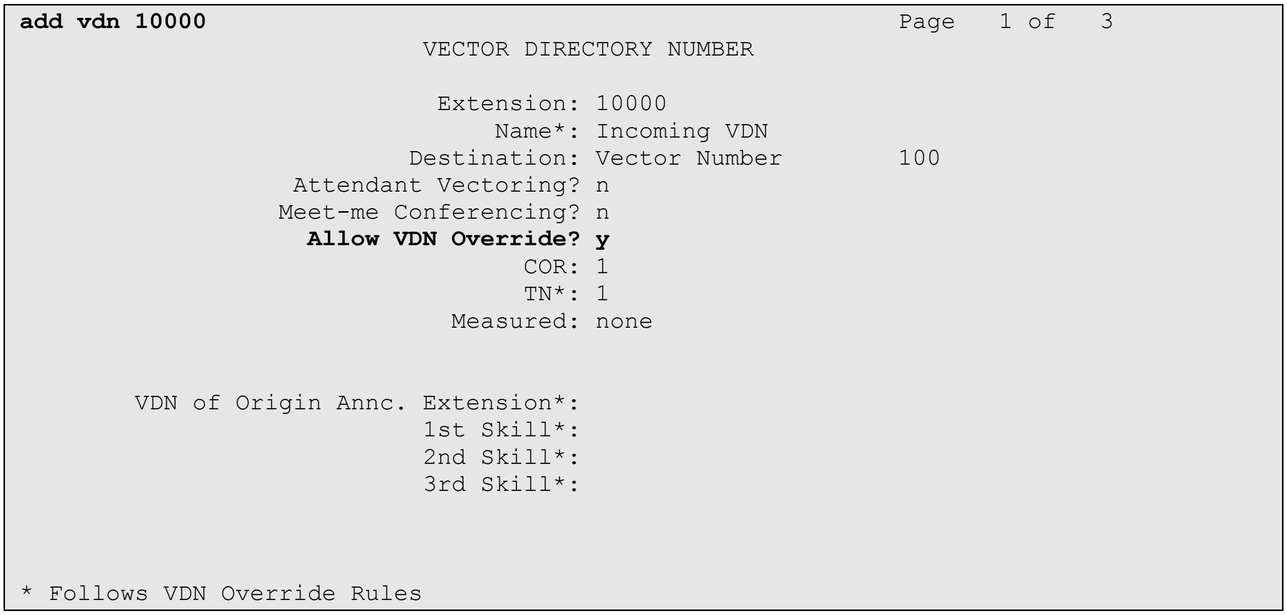
Table below displays the configured stations and associated agents during the compliance test.

Experience Portal		Call Center	
Station	Agent ID	Station	Agent ID
25501	2551	25001	2501
25502	2552	25002	2502
25003	2553	25003	2503
25504	2554		
25505	2555		
25506	2556		
25007	2557		
25008	2558		
25009	2559		
25009	2560		

5.5. Administer Call Vectoring

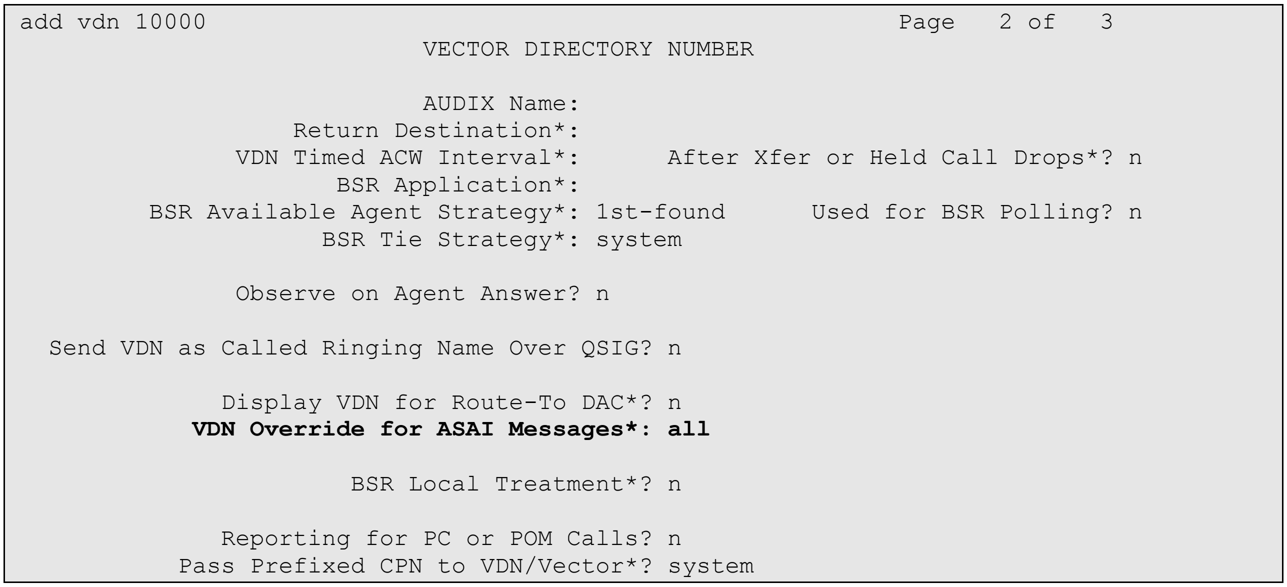
This section describes the procedures for configuring call vectoring for the Primas LinkScope inbound and outbound calls.

Configure the **Vector Directory Number** (VDN) that will handle incoming customer calls. The VDN invokes a vector that will process the call based on its configuration. Using the **add vdn** command, add a vdn. The example below displays configuration for VDN 10000 and vector 100. Note that the **Allow VDN Override** is set to **y.**



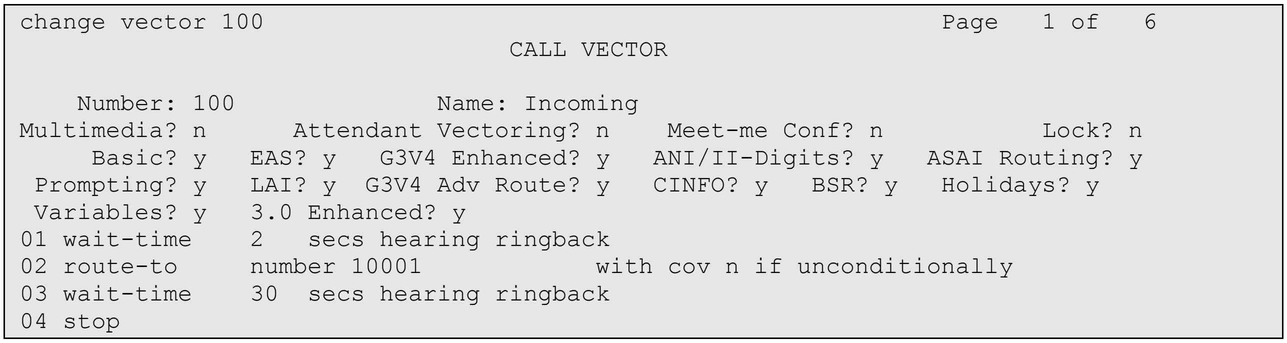
```
add vdn 10000                                                Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                             Extension: 10000
                                 Name*: Incoming VDN
                           Destination: Vector Number        100
                   Attendant Vectoring? n
                  Meet-me Conferencing? n
                    Allow VDN Override? y
                                   COR: 1
                                   TN*: 1
                              Measured: none


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



* Follows VDN Override Rules
```

On **Page 2**, **VDN Override for ASAI Messages*** is set to **all.**



```
add vdn 10000                                                Page   2 of   3
                            VECTOR DIRECTORY NUMBER

                            AUDIX Name:
                   Return Destination*:
               VDN Timed ACW Interval*:      After Xfer or Held Call Drops*? n
                      BSR Application*:
         BSR Available Agent Strategy*: 1st-found      Used for BSR Polling? n
                     BSR Tie Strategy*: system

               Observe on Agent Answer? n

  Send VDN as Called Ringing Name Over QSIG? n

              Display VDN for Route-To DAC*? n
            VDN Override for ASAI Messages*: all

                       BSR Local Treatment*? n

              Reporting for PC or POM Calls? n
           Pass Prefixed CPN to VDN/Vector*? system
```

Below is an example of the vector used by VDN 10000.



```
change vector 100                                               Page   1 of   6
                                  CALL VECTOR

    Number: 100              Name: Incoming
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 route-to     number 10001            with cov n if unconditionally
03 wait-time    30  secs hearing ringback
04 stop
```

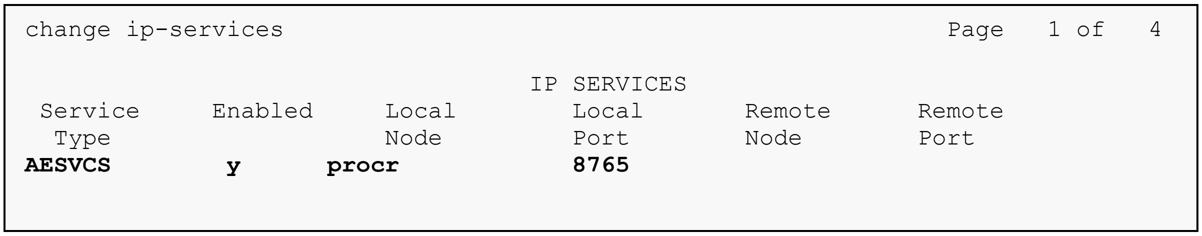
Table below displays the configured VDN/Vector during the compliance test.

VDN/Vector	VDN Override
10000/100	y
10001/1	n
10002/2	n
10003/3	n
10004/4	n
10005/5	y
10006/6	n
10007/7	y
10008/8	y
10009/9	y
10010/10	n
10011/11	y
10012/12	y
10013/13	n
10014/14	n

5.6. Configure AES connection

Use **change ip-services** command to add an entry for AES. On **Page 1**,

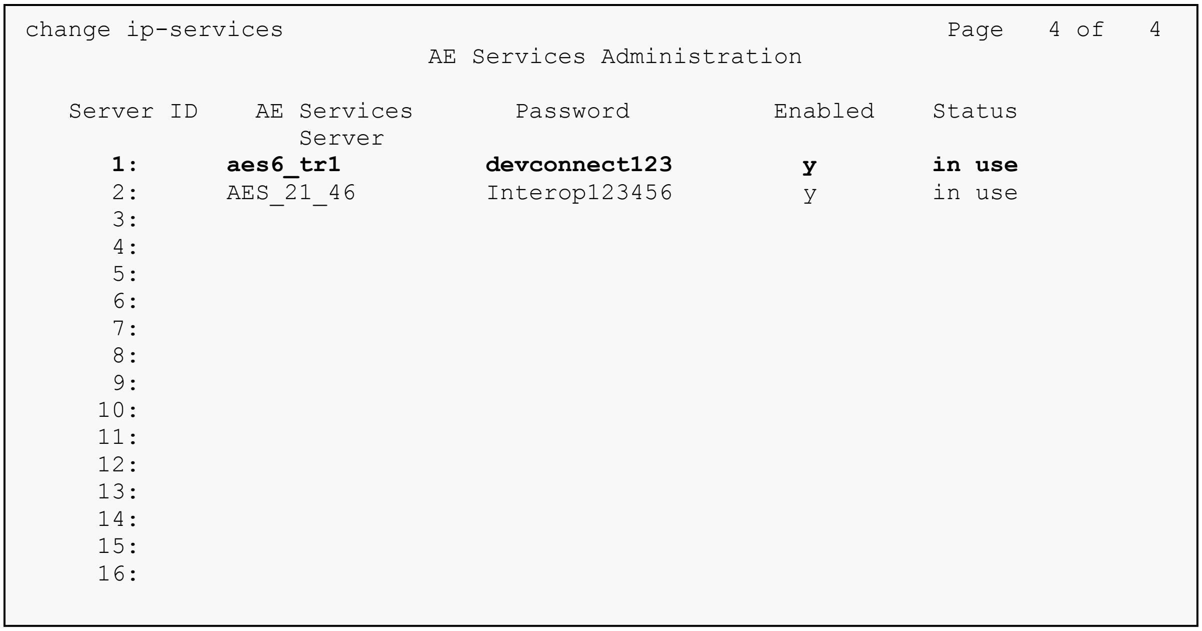
- In the **Service Type** field, type **AESVCS**.
- In the **Enabled** field, type **y**.
- In the **Local Node** field, type the Node name **procr** for the Processor Ethernet Interface.
- In the **Local Port** field, use the default of **8765**.



```
change ip-services                                           Page   1 of   4

                                   IP SERVICES
 Service     Enabled     Local        Local        Remote       Remote
  Type                   Node         Port         Node         Port
AESVCS         y      procr           8765
```

On **Page 4** of the IP Services form, enter the following values:

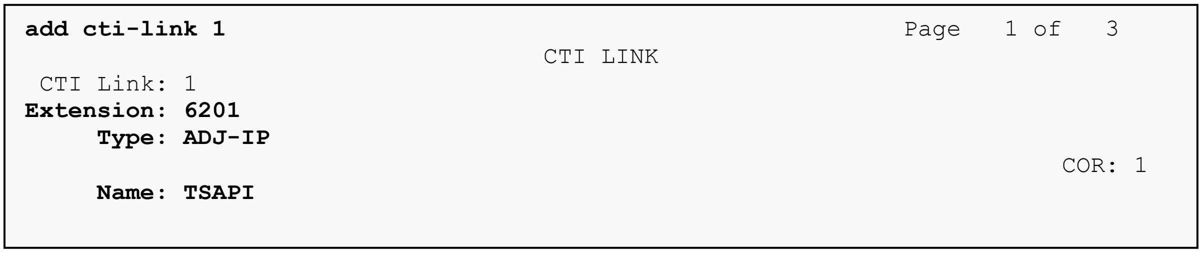
- In the **AE Services Server** field, type the name obtained from the Application Enablement Services server.
- In the **Password** field, type a password to be administered on the Application Enablement Services server.
- In the **Enabled** field, type **y**.



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

   Server ID    AE Services        Password          Enabled    Status
                   Server
      1:      aes6_tr1          devconnect123          y        in use
      2:      AES_21_46         Interop123456          y        in use
      3:
      4:
      5:
      6:
      7:
      8:
      9:
     10:
     11:
     12:
     13:
     14:
     15:
     16:
```

Use **add cti-link *n*** command, where ***n*** is an available CTI link number.

- In the **Extension** field, type **<station extension>**, where **<station extension>** is a valid station extension.
- In the **Type** field, type **ADJ-IP**.
- In the **Name** field, type a descriptive name.



```
add cti-link 1                                               Page   1 of   3
                                    CTI LINK
 CTI Link: 1
Extension: 6201
     Type: ADJ-IP
                                                                        COR: 1

     Name: TSAPI
```

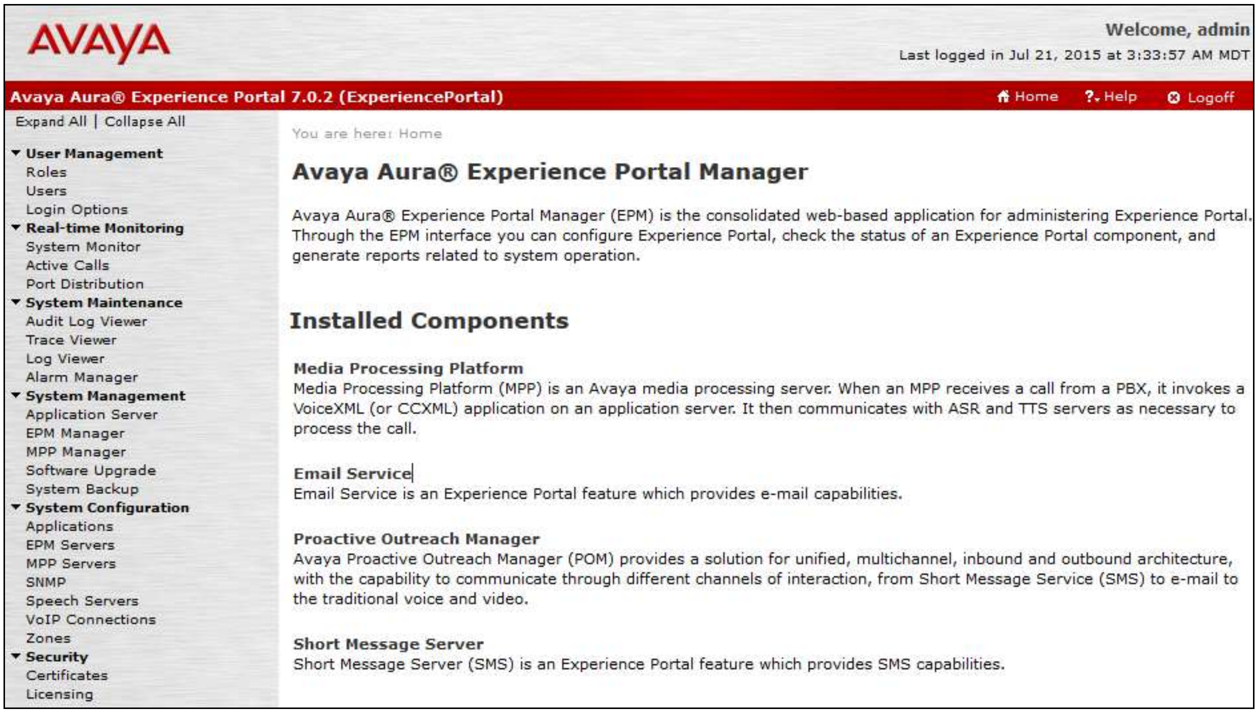
6. Configure Avaya Aura® Experience Portal

This section covers the administration of Avaya Aura® Experience Portal. The following Experience Portal configuration steps will be covered:

- Configuring VoIP Connection
- Configuring Applications
- Configuring Outcall Authentication
- Starting the MPP server

Avaya Aura® Experience Portal is configured via the Experience Portal Management (EPM) web interface. To access the web interface, enter http://<*ip-addr*>/ as the URL in an internet browser, where <*ip-addr*> is the IP address of the EPM. Log in using the Administrator user role. The screen shown below is displayed.

Note: All of the screens in this section are shown after the Experience Portal had been configured. Don't forget to save the screen parameters as you configure Avaya Aura® Experience Portal.



Avaya Aura® Experience Portal Manager

Avaya Aura® Experience Portal Manager (EPM) is the consolidated web-based application for administering Experience Portal. Through the EPM interface you can configure Experience Portal, check the status of an Experience Portal component, and generate reports related to system operation.

Installed Components

Media Processing Platform
Media Processing Platform (MPP) is an Avaya media processing server. When an MPP receives a call from a PBX, it invokes a VoiceXML (or CCXML) application on an application server. It then communicates with ASR and TTS servers as necessary to process the call.

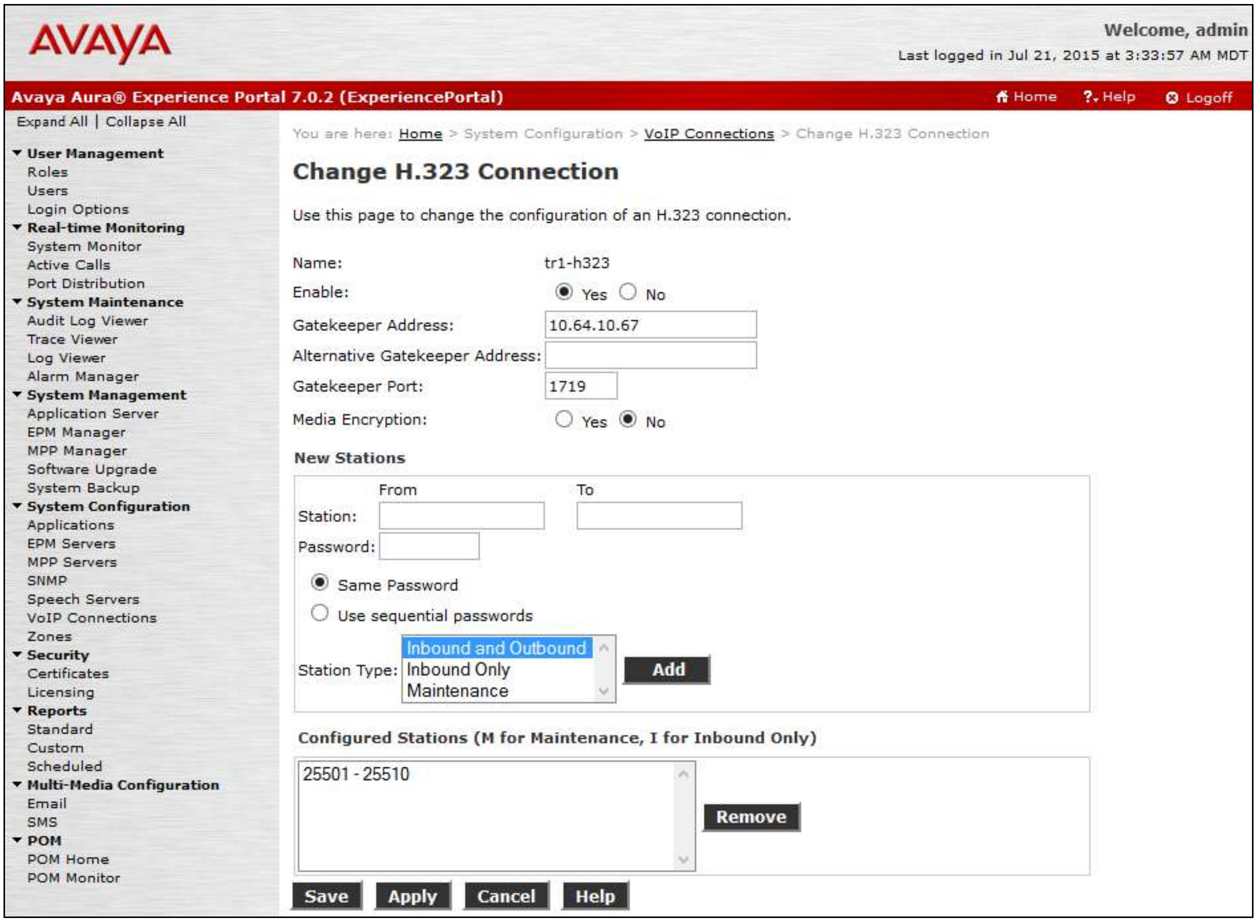
Email Service
Email Service is an Experience Portal feature which provides e-mail capabilities.

Proactive Outreach Manager
Avaya Proactive Outreach Manager (POM) provides a solution for unified, multichannel, inbound and outbound architecture, with the capability to communicate through different channels of interaction, from Short Message Service (SMS) to e-mail to the traditional voice and video.

Short Message Server
Short Message Server (SMS) is an Experience Portal feature which provides SMS capabilities.

6.1. Configure an H.323 VoIP Connection

To configure an H.323 connection, navigate to **System Configuration → VoIP Connections** page and then select the **H.323** tab. In the H.323 tab shown in **VoIP Connections**, set the **Gatekeeper Address** to the IP address of Communication Manager and the **Gatekeeper Port** to **1719**. Next, configure the stations for Experience Portal, which map to the 7434ND stations configured in **Section 5.2**. In addition, set the **Password** for the stations and set the **Station Type** to **Inbound and Outbound**. Below is a screen capture of the configuration during the compliance test.



Change H.323 Connection

Use this page to change the configuration of an H.323 connection.

Name: tr1-h323

Enable: ● Yes ○ No

Gatekeeper Address: 10.64.10.67

Alternative Gatekeeper Address:

Gatekeeper Port: 1719

Media Encryption: ○ Yes ● No

New Stations

Station: From To

Password:

● Same Password

○ Use sequential passwords

Station Type: Inbound and Outbound / Inbound Only / Maintenance

Configured Stations (M for Maintenance, I for Inbound Only)

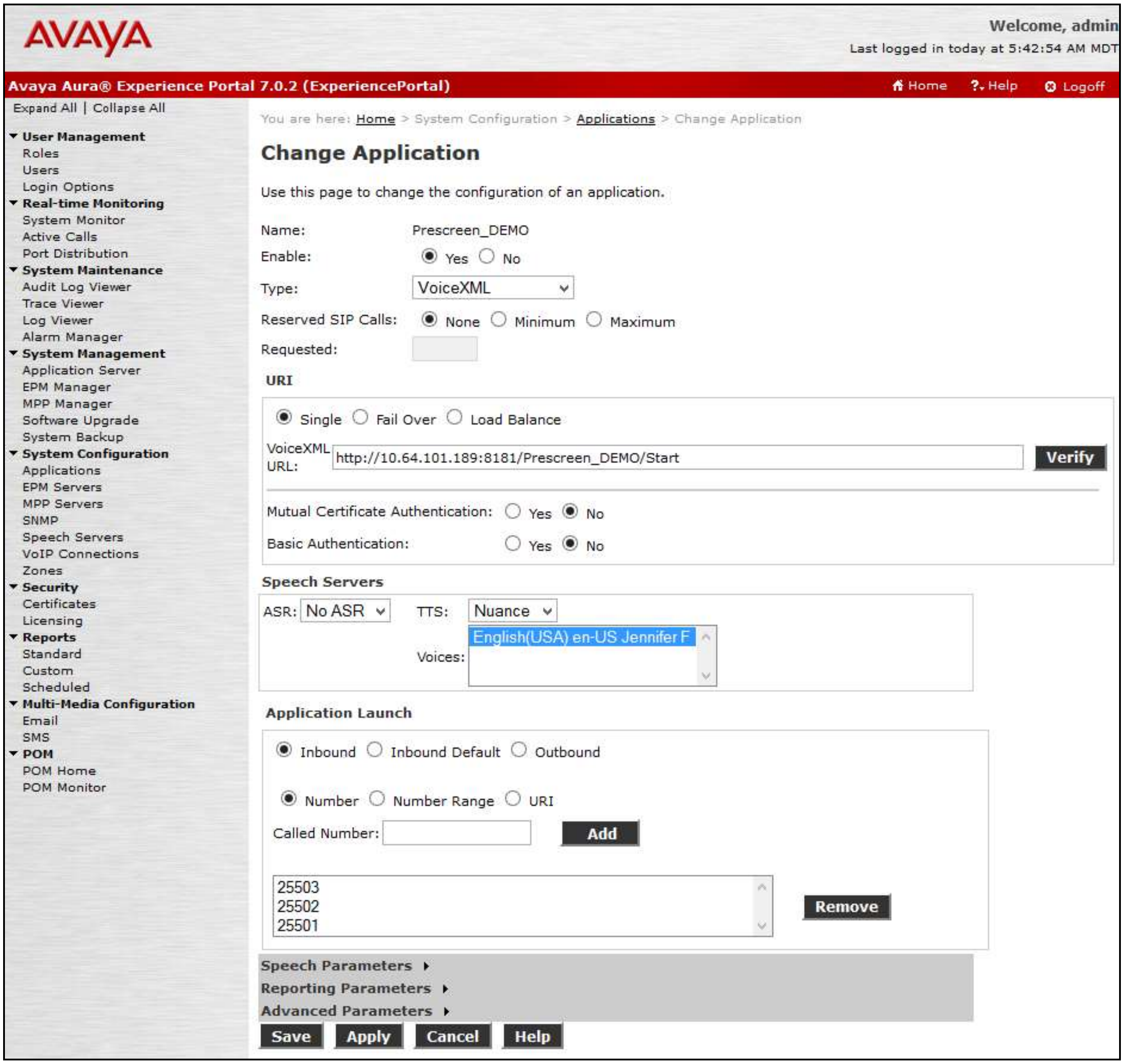
25501 - 25510

6.2. Configure Applications

Two VXML and one CCXML applications are required for the LinkScope Solution. These are deployed to a tomcat server and then referenced by Experience Portal.

To add an application, navigate to **System Configuration → Applications;** on the **Applications** page, select **Add**. Screen captures below display all the three configured applications:

PreScreen Application:



Change Application

Use this page to change the configuration of an application.

Name: Prescreen_DEMO

Enable: ● Yes ○ No

Type: VoiceXML

Reserved SIP Calls: ● None ○ Minimum ○ Maximum

Requested:

URI

● Single ○ Fail Over ○ Load Balance

VoiceXML URL: http://10.64.101.189:8181/Prescreen_DEMO/Start

Mutual Certificate Authentication: ○ Yes ● No

Basic Authentication: ○ Yes ● No

Speech Servers

ASR: No ASR TTS: Nuance

Voices: English(USA) en-US Jennifer F

Application Launch

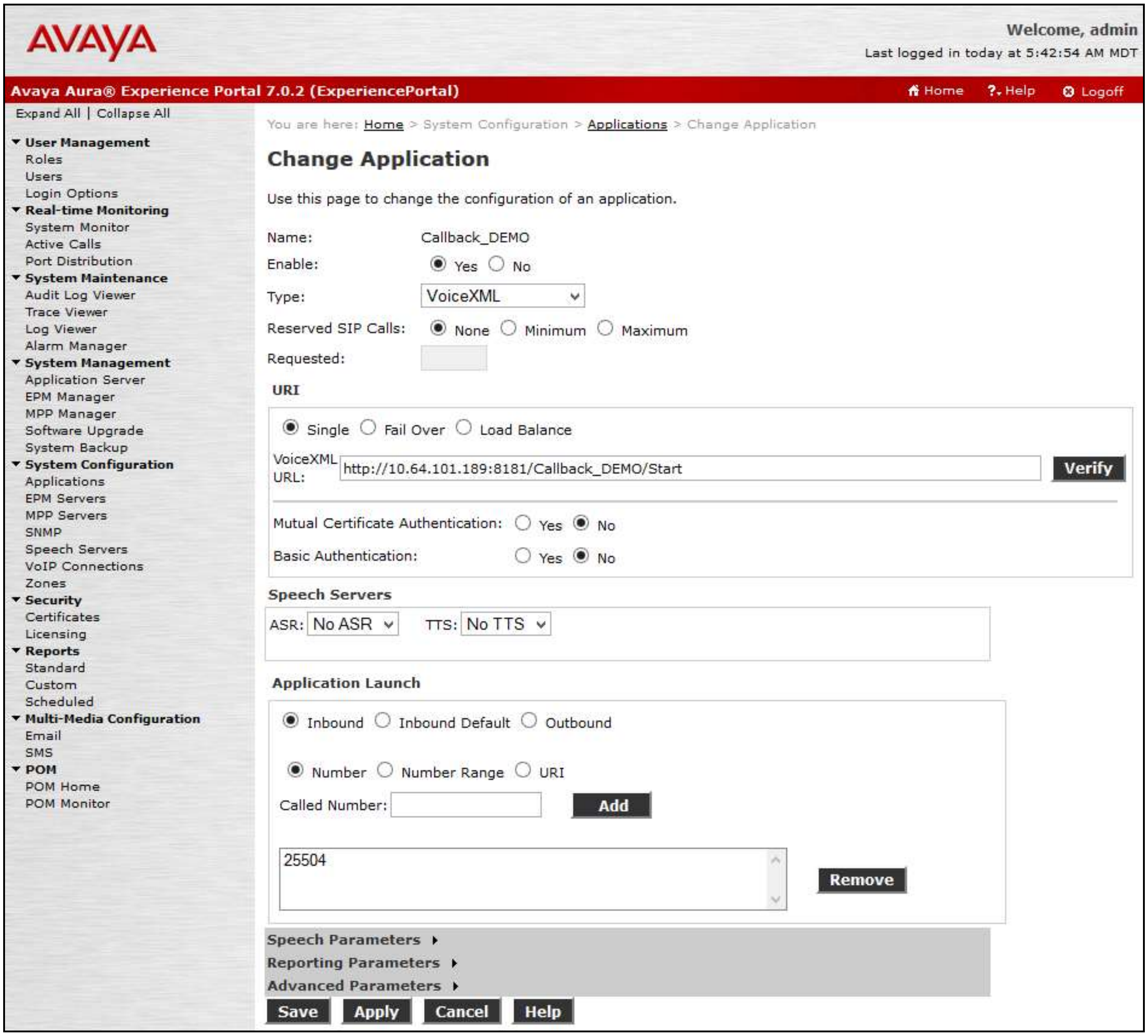
● Inbound ○ Inbound Default ○ Outbound

● Number ○ Number Range ○ URI

Called Number:

25503
25502
25501

Call Back Application:



Change Application

Use this page to change the configuration of an application.

Name: Callback_DEMO

Enable: ● Yes ○ No

Type: VoiceXML

Reserved SIP Calls: ● None ○ Minimum ○ Maximum

Requested:

URI

● Single ○ Fail Over ○ Load Balance

VoiceXML URL: http://10.64.101.189:8181/Callback_DEMO/Start

Mutual Certificate Authentication: ○ Yes ● No

Basic Authentication: ○ Yes ● No

Speech Servers

ASR: No ASR TTS: No TTS

Application Launch

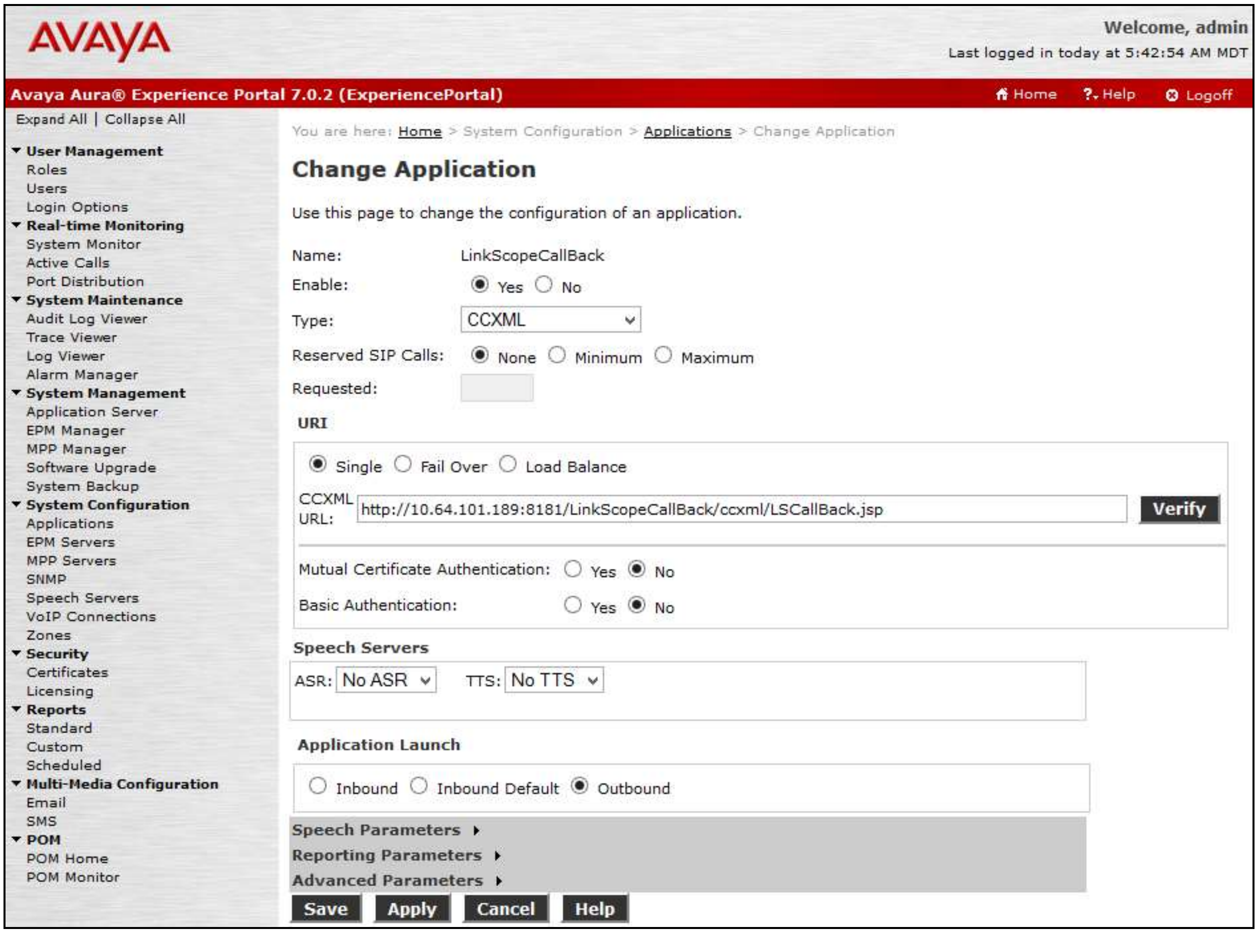
● Inbound ○ Inbound Default ○ Outbound

● Number ○ Number Range ○ URI

Called Number:

25504

LinkScopeCallBack Application:



Change Application

Use this page to change the configuration of an application.

Name: LinkScopeCallBack

Enable: ● Yes ○ No

Type: CCXML

Reserved SIP Calls: ● None ○ Minimum ○ Maximum

Requested:

URI

● Single ○ Fail Over ○ Load Balance

CCXML URL: http://10.64.101.189:8181/LinkScopeCallBack/ccxml/LSCallBack.jsp

Mutual Certificate Authentication: ○ Yes ● No

Basic Authentication: ○ Yes ● No

Speech Servers

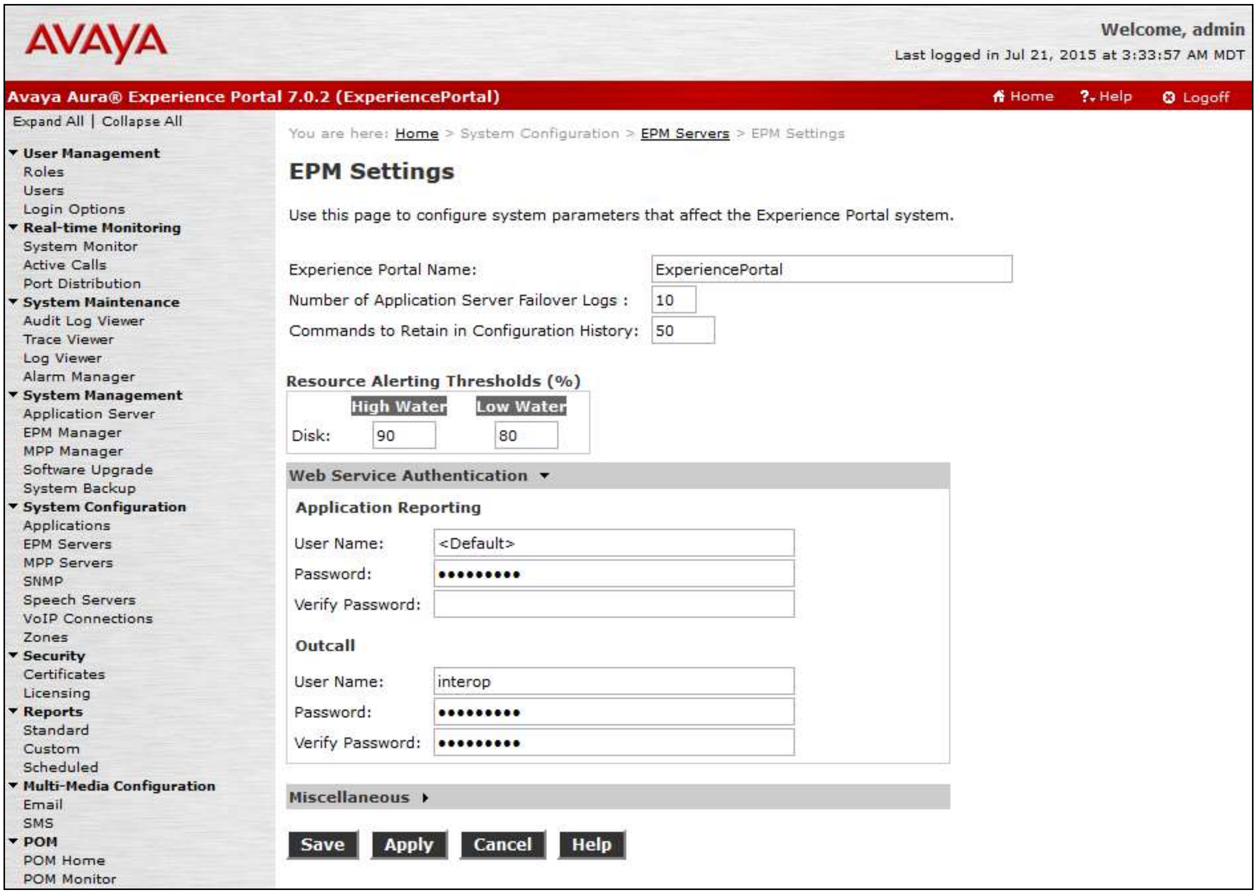
ASR: No ASR TTS: No TTS

Application Launch

○ Inbound ○ Inbound Default ● Outbound

6.3. Configure the Outcall Authentication

Configure the Outcall User Name and Password that will be sent by Primas. Select **System Configuration → EPM Servers** in the left pane. In the resulting page, click on **EPM Settings** to display the page below. Under the **Outcall** section, configure the **User Nam**e and **Password** used by Primas when it makes an outcall request to Experience Portal.



EPM Settings

Use this page to configure system parameters that affect the Experience Portal system.

Experience Portal Name:	ExperiencePortal
Number of Application Server Failover Logs :	10
Commands to Retain in Configuration History:	50

Resource Alerting Thresholds (%)

	High Water	Low Water
Disk:	90	80

Application Reporting

User Name:	<Default>
Password:	•••••••••
Verify Password:	

Outcall

User Name:	interop
Password:	•••••••••
Verify Password:	•••••••••

7. Configure Avaya Aura® Application Enablement Services

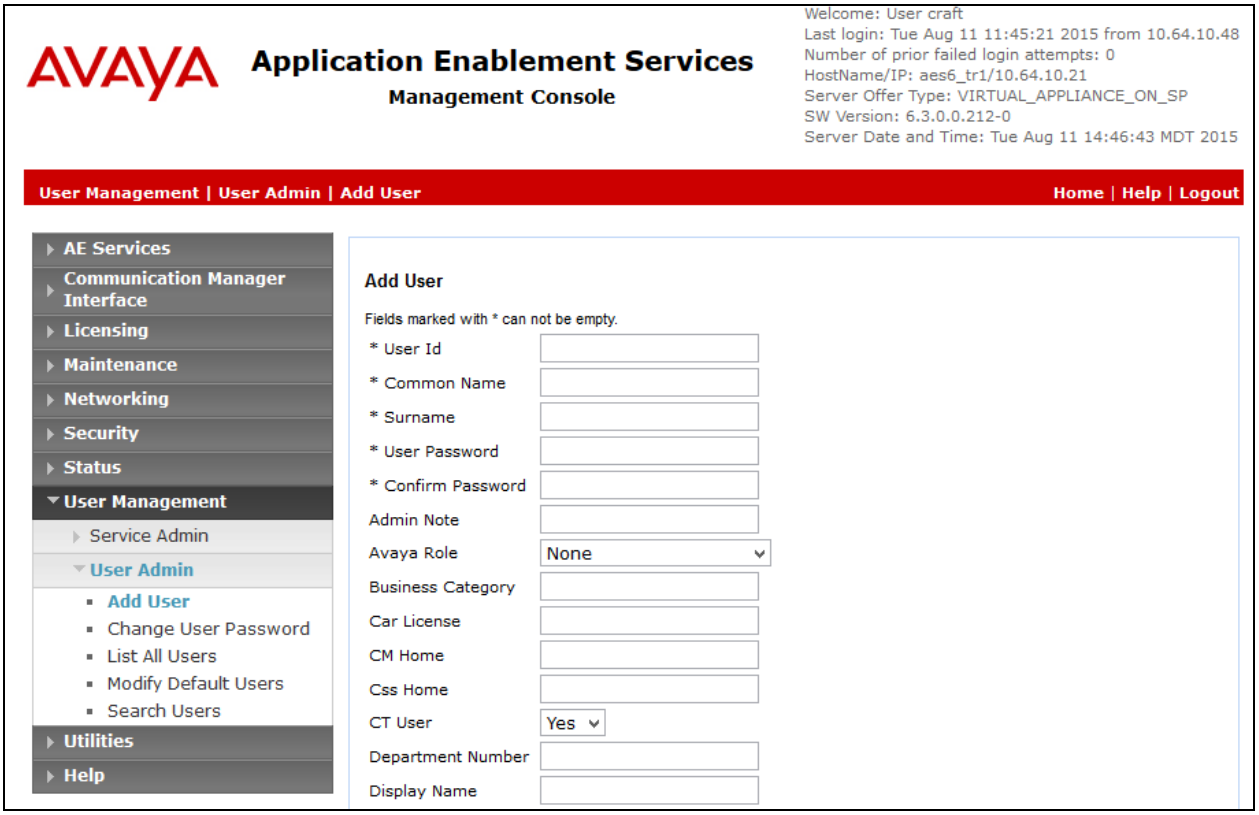
Configuration of Avaya Aura® Application Enablement Services requires a user account be configured for LinkScope.

7.1. Configure User

All administration is performed by web browser, https://<aes-ip-address>/

A user needs to be created for LinkScope to communicate with AES. Navigate to **User Management → User Admin → Add User**.

Fill in **User Id, Common Name, Surname, User Password** and **Confirm Password**. Set the **CT User** to **Yes,** and click **Apply**.



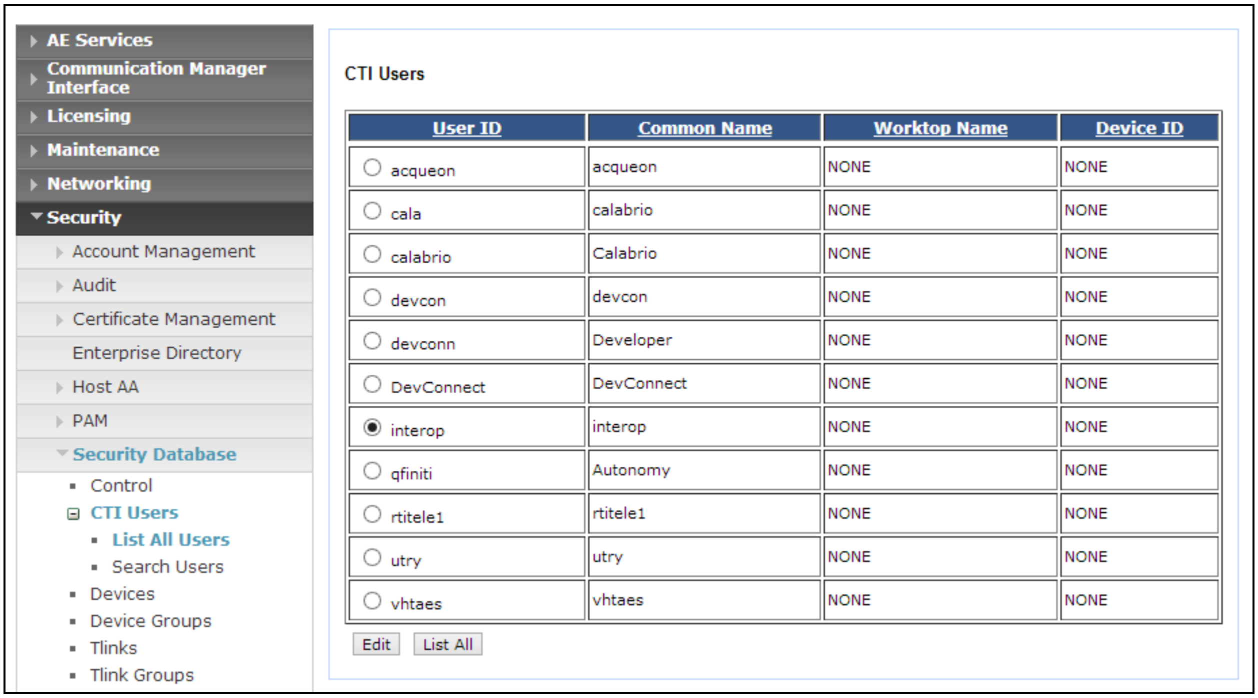
Welcome: User craft
Last login: Tue Aug 11 11:45:21 2015 from 10.64.10.48
Number of prior failed login attempts: 0
HostName/IP: aes6_tr1/10.64.10.21
Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
SW Version: 6.3.0.0.212-0
Server Date and Time: Tue Aug 11 14:46:43 MDT 2015

Add User

Fields marked with * can not be empty.

* User Id	
* Common Name	
* Surname	
* User Password	
* Confirm Password	
Admin Note	
Avaya Role	None
Business Category	
Car License	
CM Home	
Css Home	
CT User	Yes
Department Number	
Display Name	

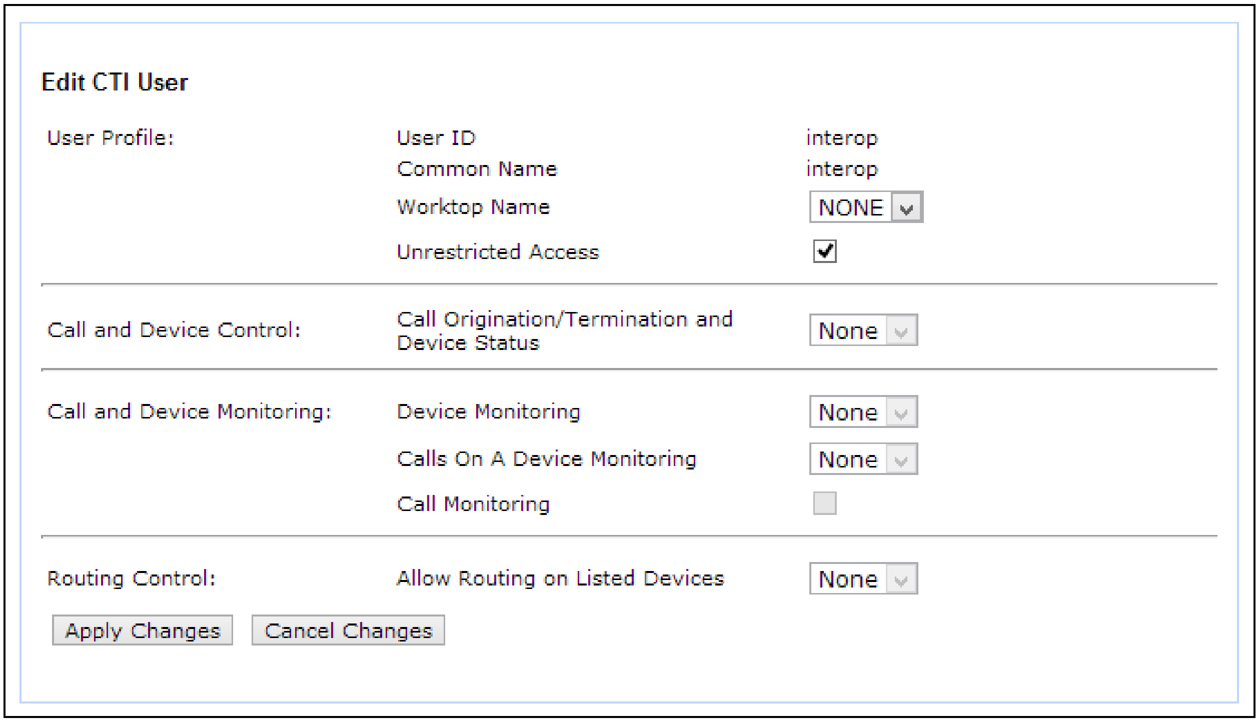
Navigate to **Security → Security Database → CTI Users → List All Users**.



CTI Users

User ID	Common Name	Worktop Name	Device ID
○ acqueon	acqueon	NONE	NONE
○ cala	calabrio	NONE	NONE
○ calabrio	Calabrio	NONE	NONE
○ devcon	devcon	NONE	NONE
○ devconn	Developer	NONE	NONE
○ DevConnect	DevConnect	NONE	NONE
● interop	interop	NONE	NONE
○ qfiniti	Autonomy	NONE	NONE
○ rtitele1	rtitele1	NONE	NONE
○ utry	utry	NONE	NONE
○ vhtaes	vhtaes	NONE	NONE

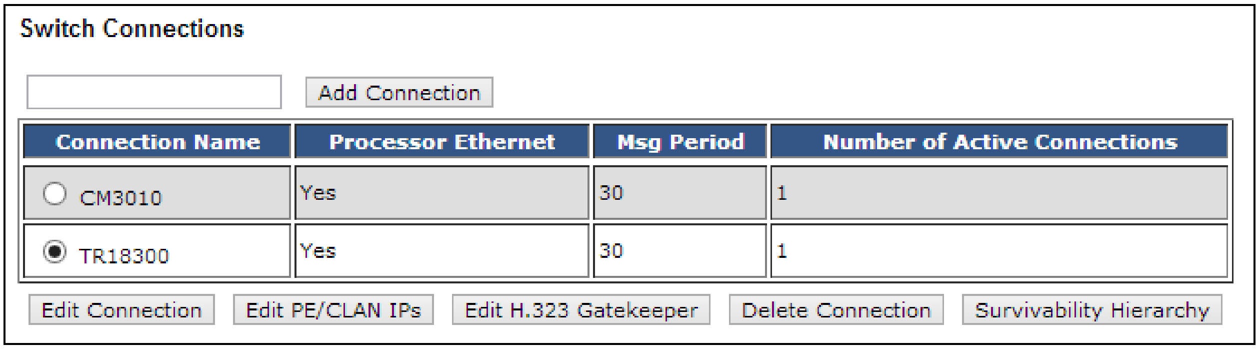
Select the recently added user and click **Edit**. Check the box for **Unrestricted Access** and click **Apply Changes**.


Edit CTI User

User Profile:	User ID	interop
	Common Name	interop
	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

7.2. Configure Communication Manager Switch Connections

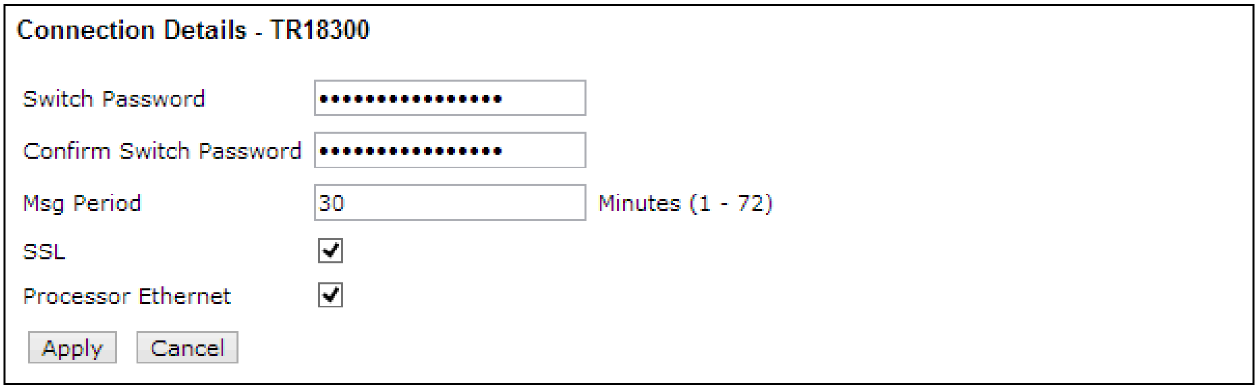
To add links to the Communication Manager, navigate to the **Communication Manager Interface → Switch Connections** page and enter a name for the new switch connection and click the **Add Connection** button. This was previously configured as **TR18300** for this test environment:



Switch Connections

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
○ CM3010	Yes	30	1
● TR18300	Yes	30	1

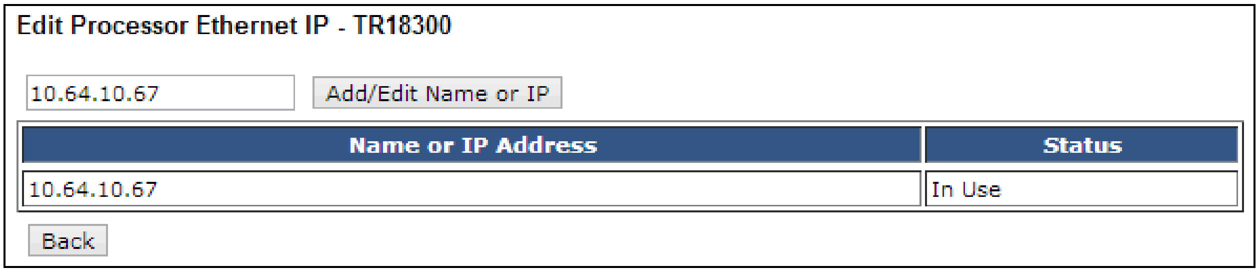
Use the **Edit Connection** button shown above to configure the connection. Enter the **Switch Password** and check the **Processor Ethernet** box if using the **procr** interface, as shown below. This must match the password configured when adding the AESVCS connection in Communication Manager.



Connection Details - TR18300

Switch Password	••••••••••••••••
Confirm Switch Password	••••••••••••••••
Msg Period	30 Minutes (1 - 72)
SSL	☑
Processor Ethernet	☑

Use the **Edit PE/CLAN IPs** button (shown in this section's first screen shot above) to configure the **procr** or **CLAN** IP Address (es) for TSAPI message traffic.

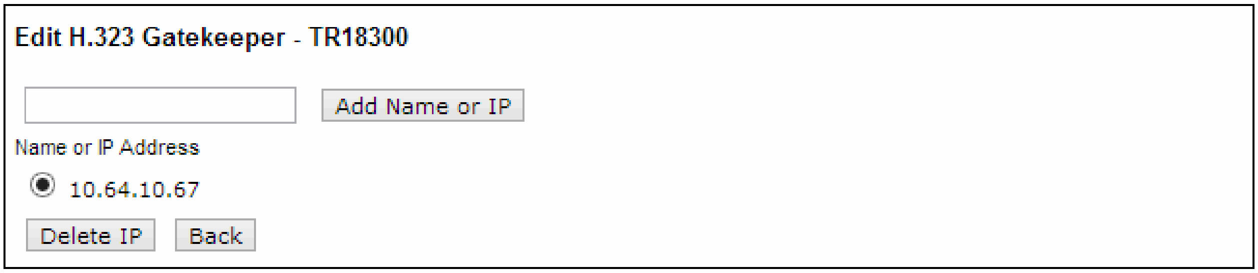


Edit Processor Ethernet IP - TR18300

10.64.10.67

Name or IP Address	Status
10.64.10.67	In Use

Use the **Edit H.323 Gatekeeper** button (shown in this section's first screen capture above) to configure the **procr** or **CLAN** IP Address(es).


Edit H.323 Gatekeeper - TR18300

Name or IP Address

● 10.64.10.67

7.3. Configure TSAPI Link

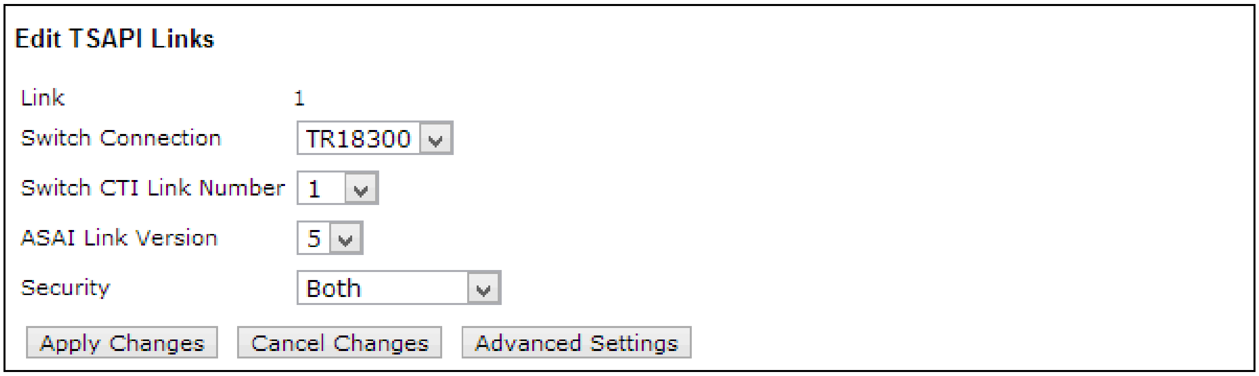
Navigate to the **AE Services → TSAPI → TSAPI Links** page to add the TSAPI CTI Link. Click **Add Link** (not shown).

Select a **Switch Connection** using the drop down menu. Select the **Switch CTI Link Number** using the drop down menu. The **Switch CTI Link Number** must match the number configured in the **cti-link** form for Communication Manager.

Select **Both** in the **Security** selection box. Though **Both** will support both encrypted and unencrypted links, unencrypted link was used during compliance testing.

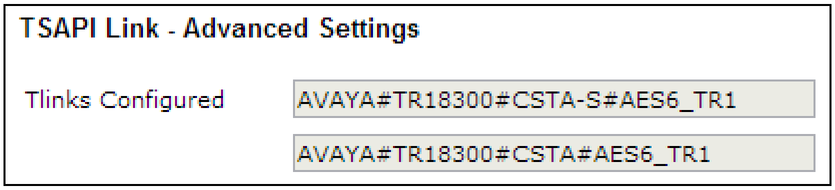
Click **Apply Changes**.

Configuration shown below was previously configured.


Edit TSAPI Links

Link	1
Switch Connection	TR18300
Switch CTI Link Number	1
ASAI Link Version	5
Security	Both

Select **Advanced Settings** and note the Tlinks Configured, it will be used when configuring LinkScope.


TSAPI Link - Advanced Settings

Tlinks Configured

AVAYA#TR18300#CSTA-S#AES6_TR1

AVAYA#TR18300#CSTA#AES6_TR1

8. Configure Primas Group LinkScope Customer Experience Power Pack

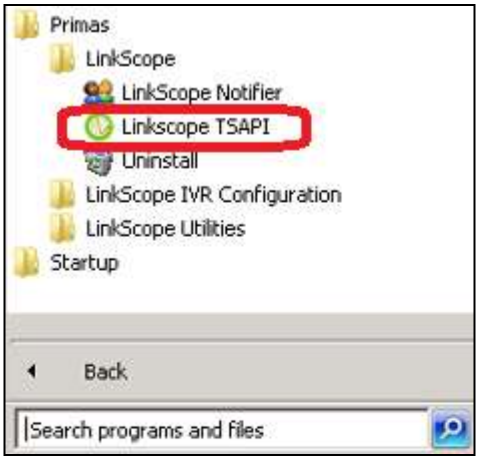
Configuration for LinkScope Customer Experience Power Pack is performed directly on the LinkScope server, which is Windows based. Note that configuration in this section was performed and provided by Primas Group engineer.

The configuration starts with the basic elements of the LinkScope Solution and works its way up to the more complex elements, in the following order:

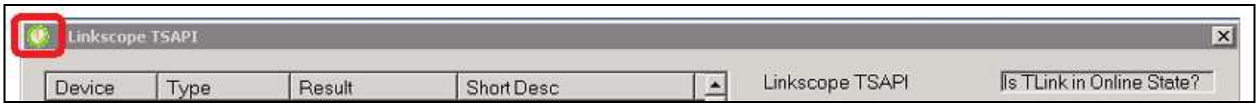
- CTI Link Configuration
- Log on to LinkScope
- Basic Configuration
- Screen Pop Configuration
- Agent Desktop Installation and Configuration of LinkScope Notifier Client
- FreedomQ Configuration
- Experience Pop Configuration
- ReconX
- IVR Application Deployment

8.1. CTI Link Configuration

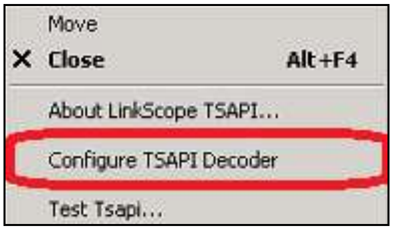
On the LinkScope Server, from the Start menu of the LinkScope Server, select **LinkScope TSAPI**.



From the top left of the LinkScope TSAPI window, right-click the icon.

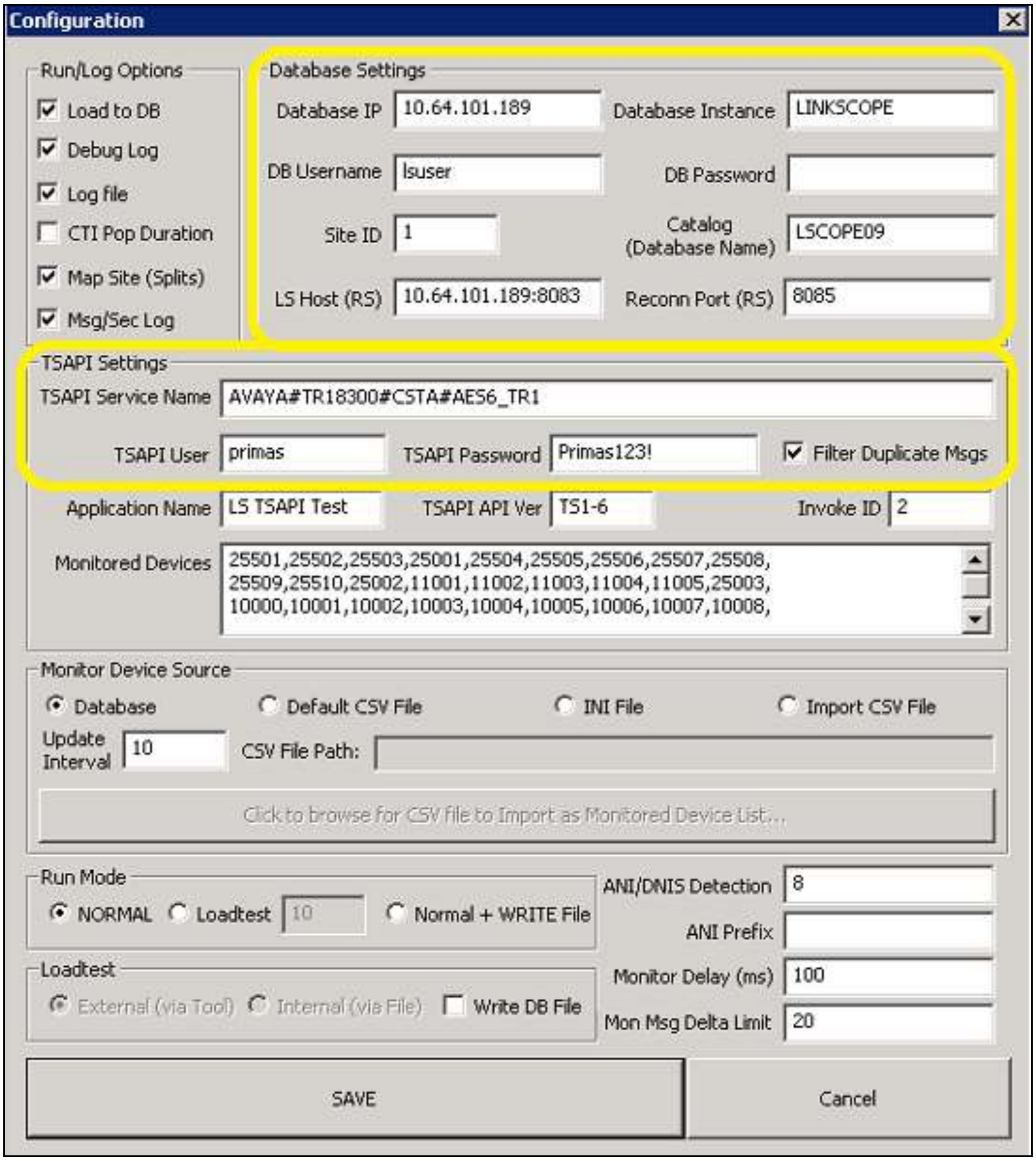


Select **Configure TSAPI Decoder**.



Provide the Database and TSAPI parameters and click **Save**

- Database Settings correspond to the LinkScope Server
- TSAPI Settings correspond to the TSAPI Link on the AES Server.



Configuration

Run/Log Options

☑ Load to DB
☑ Debug Log
☑ Log file
☐ CTI Pop Duration
☑ Map Site (Splits)
☑ Msg/Sec Log

Database Settings

Database IP: 10.64.101.189
Database Instance: LINKSCOPE
DB Username: lsuser
DB Password:
Site ID: 1
Catalog (Database Name): LSCOPE09
LS Host (RS): 10.64.101.189:8083
Reconn Port (RS): 8085

TSAPI Settings

TSAPI Service Name: AVAYA#TR18300#CSTA#AES6_TR1
TSAPI User: primas
TSAPI Password: Primas123!
☑ Filter Duplicate Msgs

Application Name: LS TSAPI Test
TSAPI API Ver: TS1-6
Invoke ID: 2
Monitored Devices: 25501,25502,25503,25001,25504,25505,25506,25507,25508,
25509,25510,25002,11001,11002,11003,11004,11005,25003,
10000,10001,10002,10003,10004,10005,10006,10007,10008,

Monitor Device Source

● Database ○ Default CSV File ○ INI File ○ Import CSV File
Update Interval: 10
CSV File Path:

Click to browse for CSV file to Import as Monitored Device List...

Run Mode

● NORMAL ○ Loadtest 10 ○ Normal + WRITE File

Loadtest

● External (via Tool) ○ Internal (via File) ☐ Write DB File

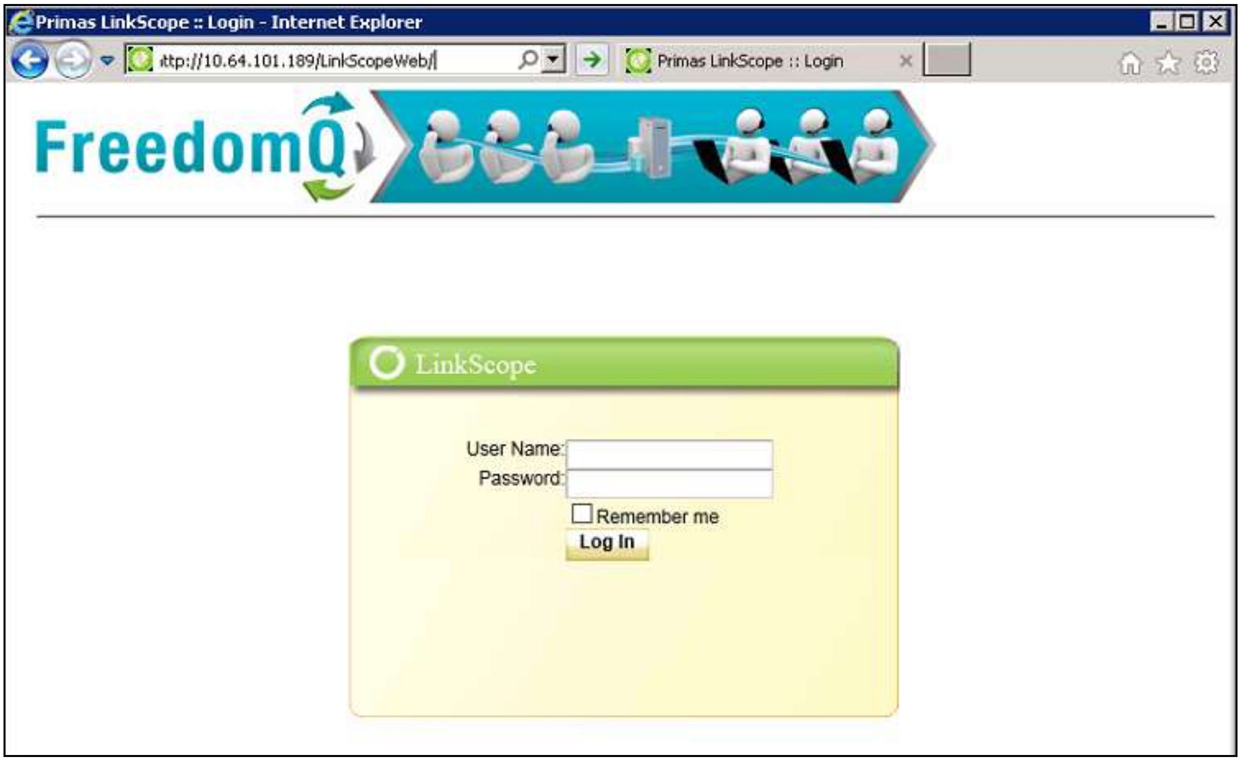
ANI/DNIS Detection: 8
ANI Prefix:
Monitor Delay (ms): 100
Mon Msg Delta Limit: 20

SAVE
Cancel

Close and reopen LinkScope TSAPI in order to Apply Changes and restart the LinkScope TSAPI Service

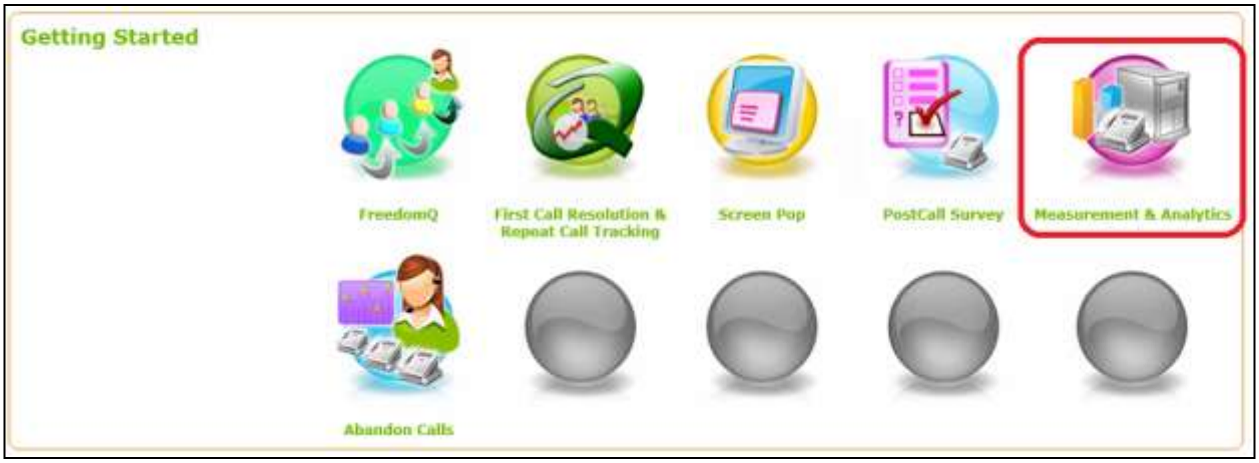
8.2. Log on to LinkScope

Open a browser to the LinkScope home page, http://SERVERIP/LinkScopeWeb/, and log in using appropriate credentials. SERVERIP is the IP Address of LinkScope server.

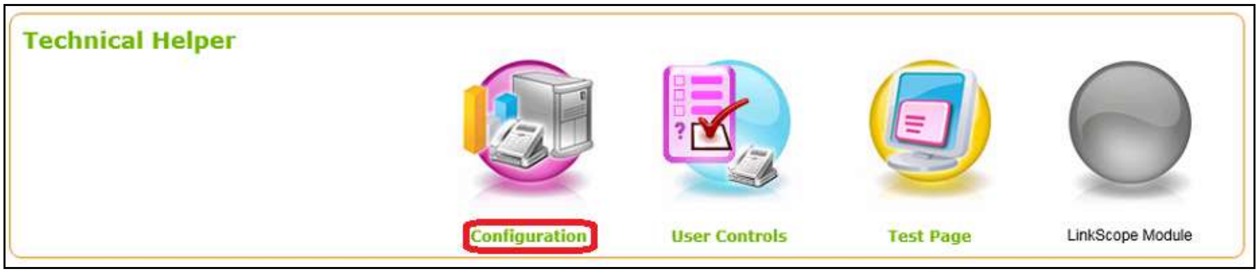

Primas LinkScope :: Login - Internet Explorer
http://10.64.101.189/LinkScopeWeb/
Primas LinkScope :: Login
FreedomQ
LinkScope
User Name:
Password:
☐ Remember me
Log In

8.3. Basic Configuration

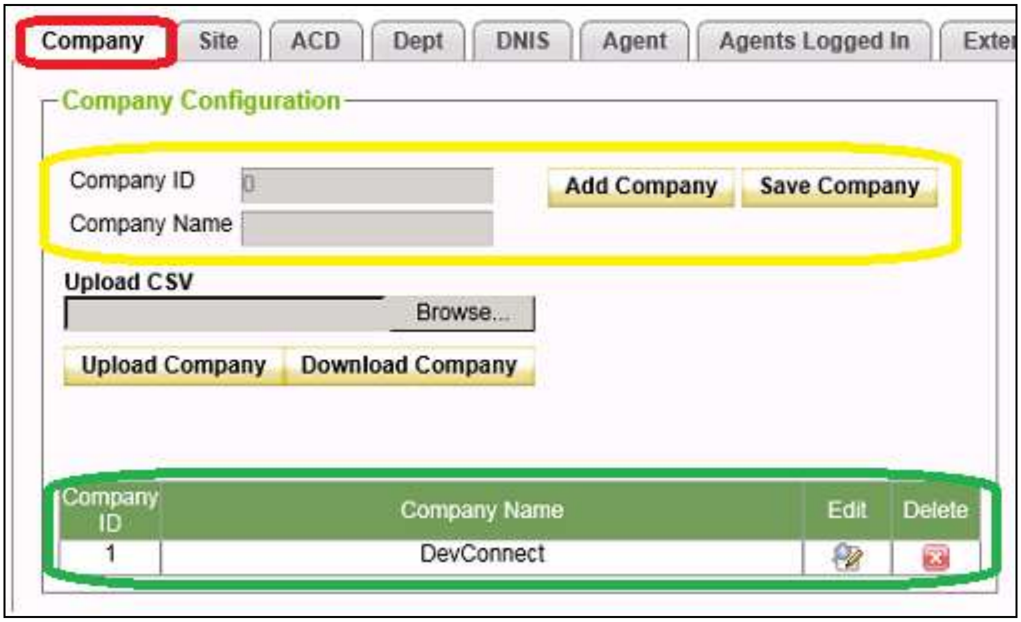
Once logged in, from the **Getting Started** page, select **Measurement & Analytics**.



On the **Technical Helper** page, select **Configuration**.



Select the **Company** tab; enter **Company Name** and click **Add Company**.



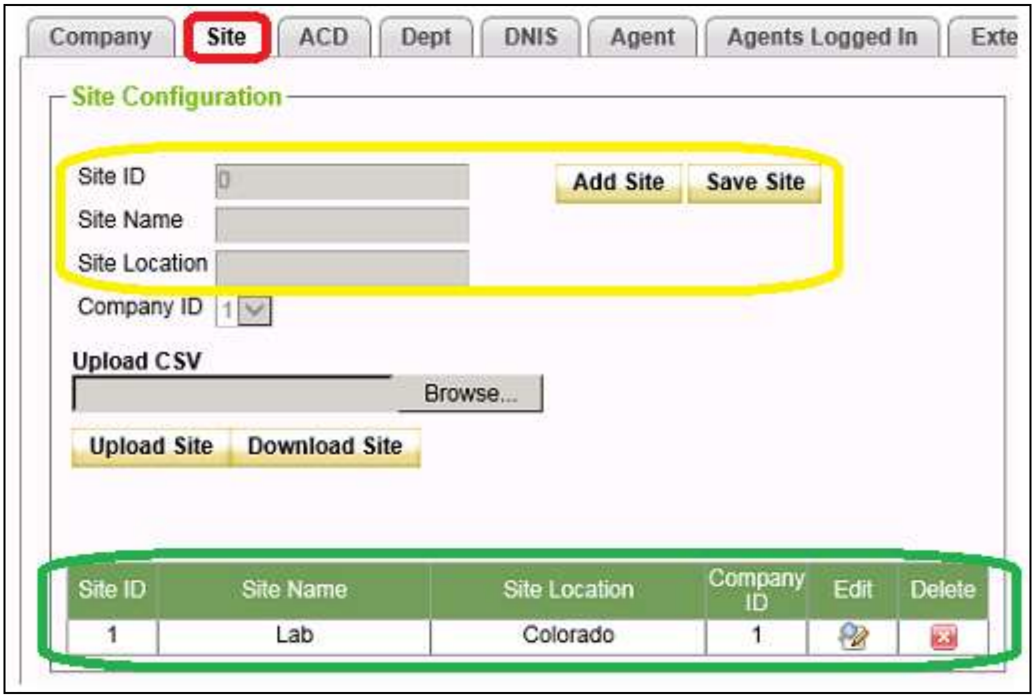
Company Configuration

Company ID: 0

Company Name:

Company ID	Company Name	Edit	Delete
1	DevConnect	✎	☒

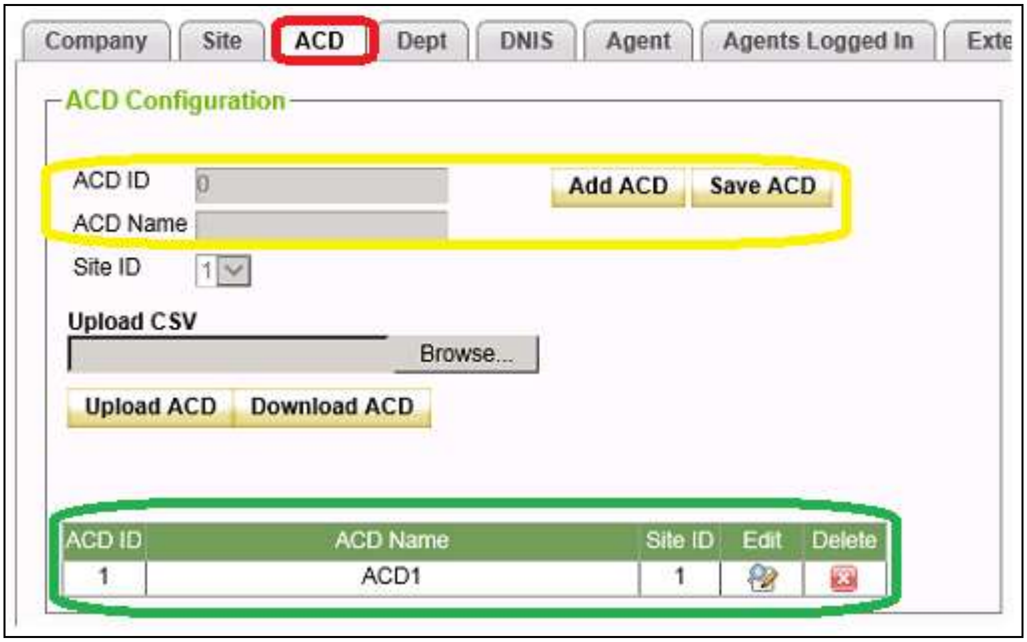
Select the **Site** tab; enter **Site Name** and **Site Location** and click **Add Site**.



Site ID 0
Site Name
Site Location
Company ID 1

Site ID	Site Name	Site Location	Company ID	Edit	Delete
1	Lab	Colorado	1	✎	☒

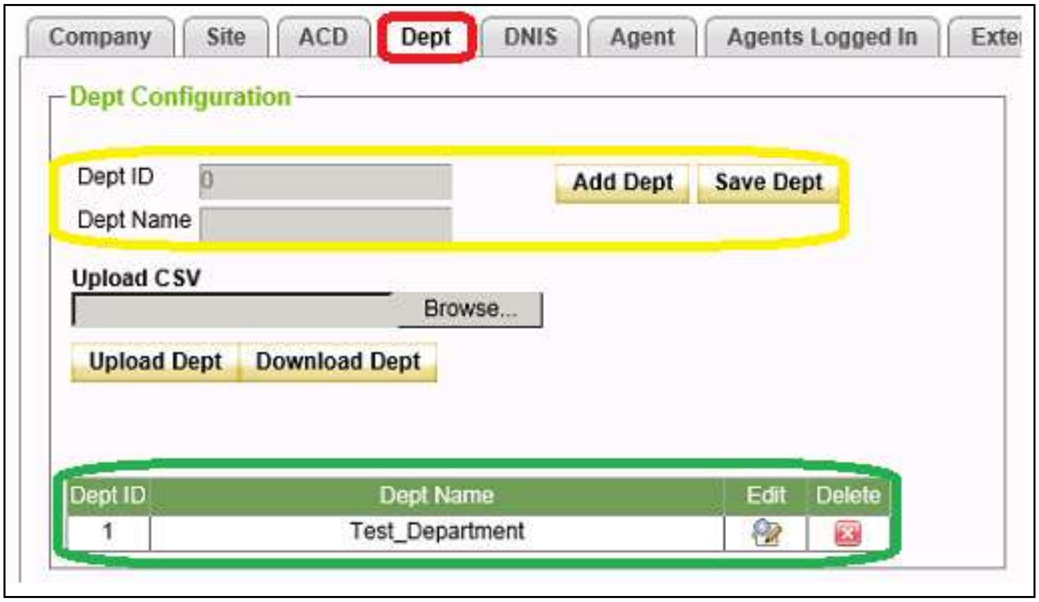
Select the **ACD** tab; enter **ACD Name** and click **Add ACD**.



ACD ID 0
ACD Name
Site ID 1

ACD ID	ACD Name	Site ID	Edit	Delete
1	ACD1	1	✎	☒

Select **Dept** tab; enter **Dept Name** and click **Add Dept**.

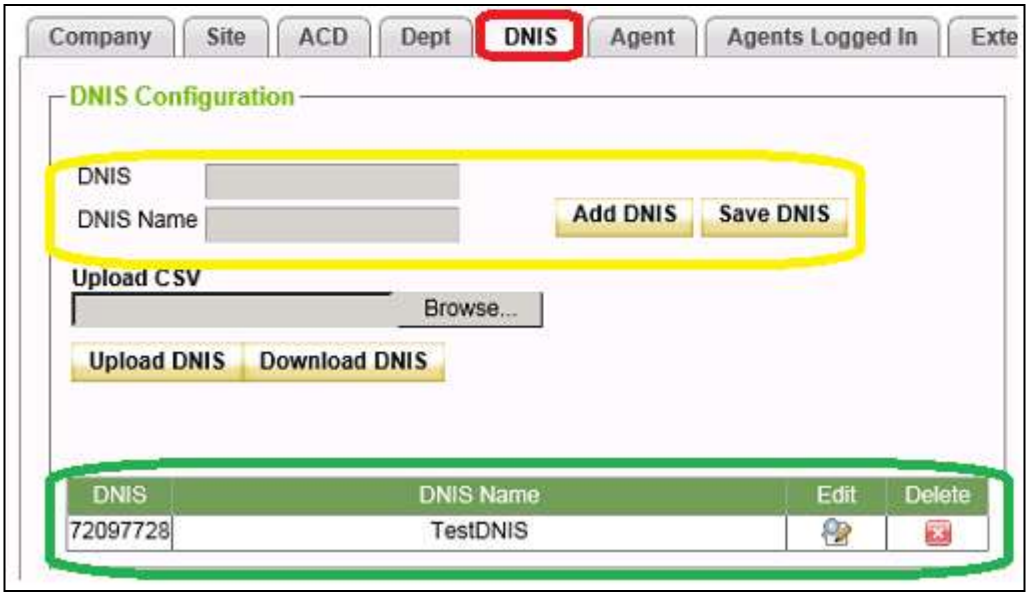


Dept ID: 0

Dept Name:

Dept ID	Dept Name	Edit	Delete
1	Test_Department	✎	☒

Select the **DNIS** tab; enter **DNIS Name** and click **Add DNIS**.

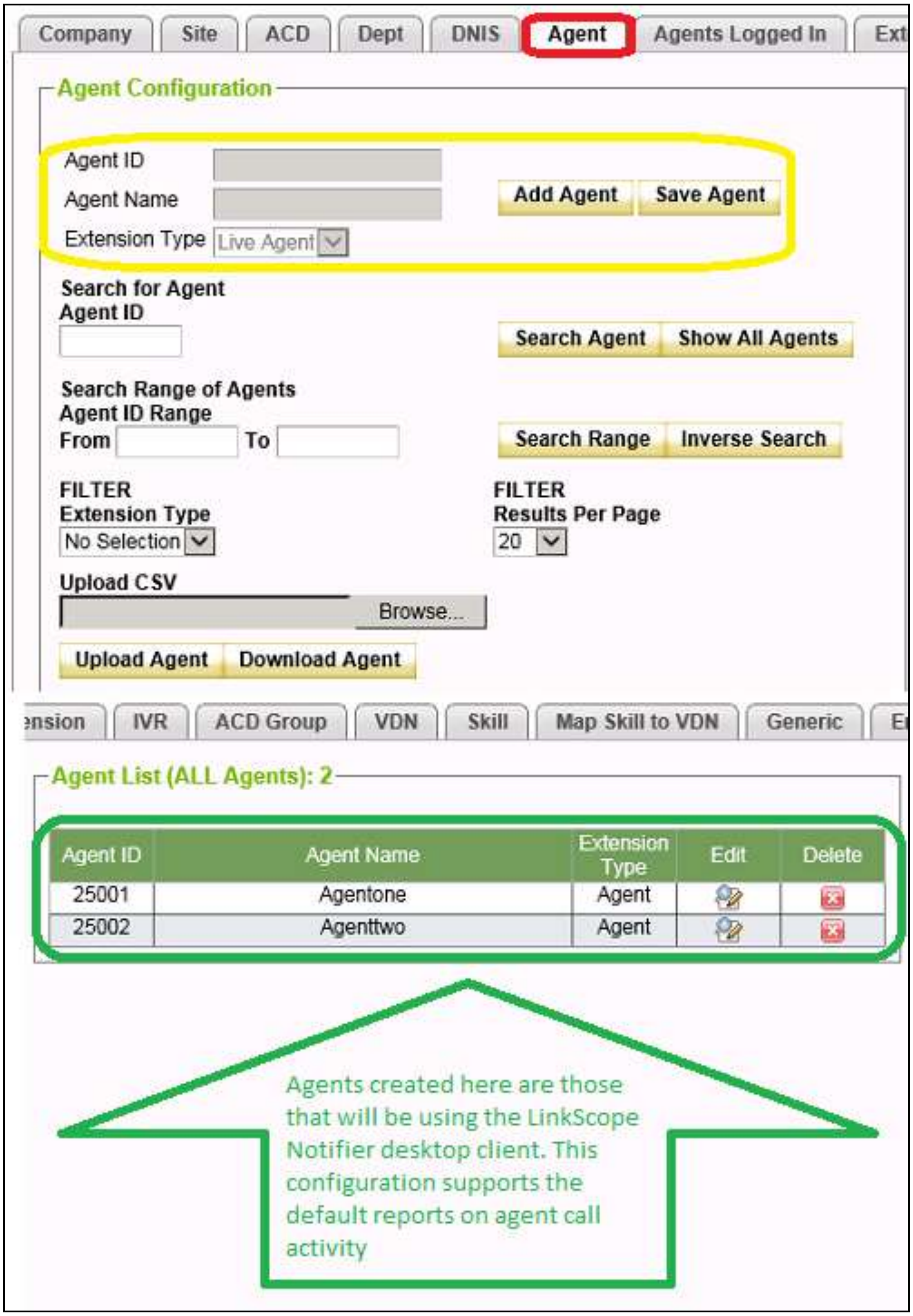


DNIS:

DNIS Name:

DNIS	DNIS Name	Edit	Delete
72097728	TestDNIS	✎	☒

Select the Agent Tab; enter **Agent ID** and **Agent Name**, select **Live Agent** for **Extension type** and click **Add Agent**. Note that Agent IDs are the H.323 Stations that were created for Call Center Agents in **Section 5.2.**



Agent ID

Agent Name

Extension Type: Live Agent

Search for Agent
Agent ID

Search Range of Agents
Agent ID Range
From To

FILTER
Extension Type
No Selection

FILTER
Results Per Page
20

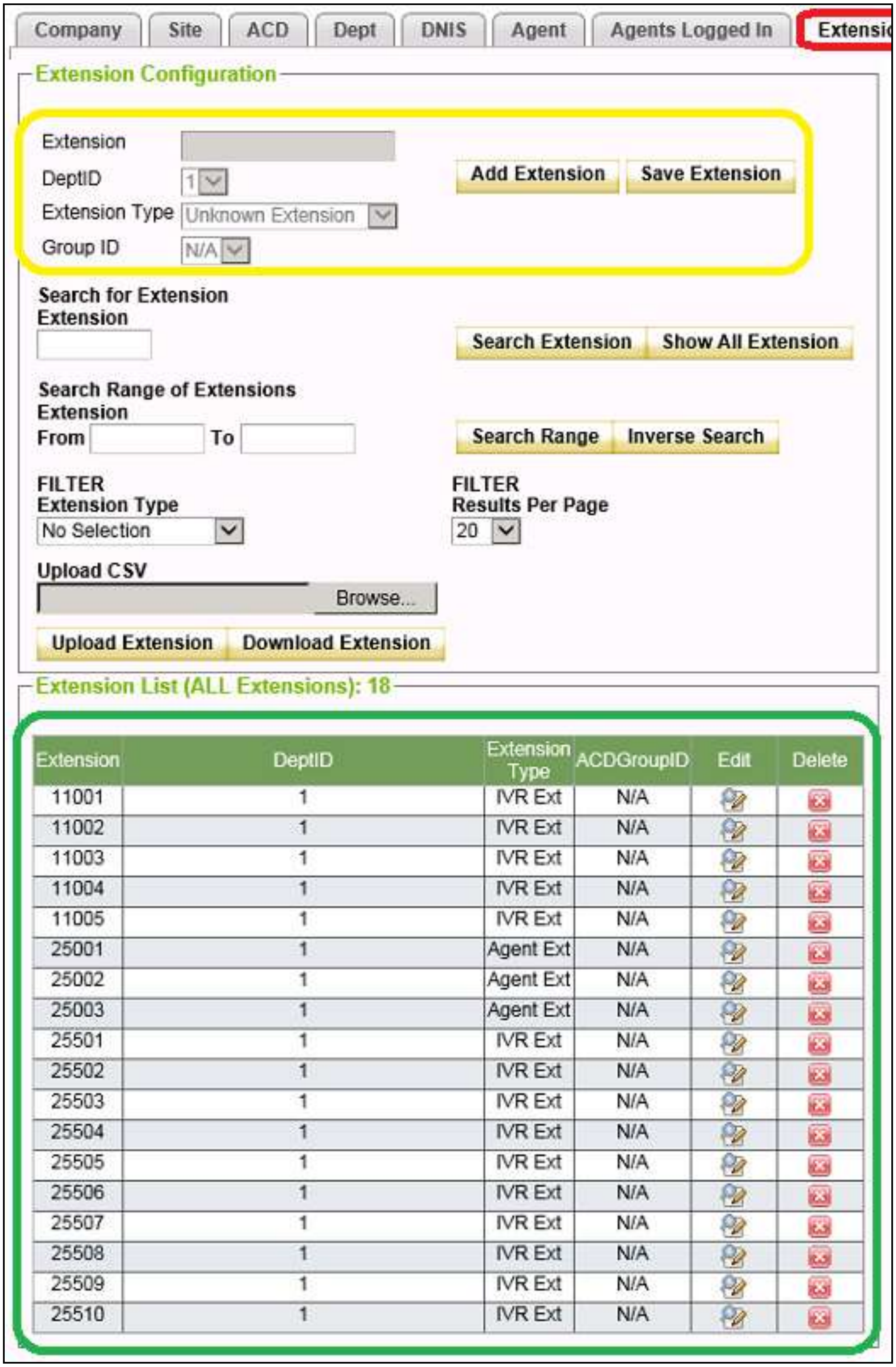
Upload CSV

Agent List (ALL Agents): 2

Agent ID	Agent Name	Extension Type	Edit	Delete
25001	Agentone	Agent	✎	☒
25002	Agenttwo	Agent	✎	☒

Agents created here are those that will be using the LinkScope Notifier desktop client. This configuration supports the default reports on agent call activity

Select the **Extension** tab; **Extension** and click **Add Extension**. Note that these extensions include H.323 stations created for Experience Portal and Call Center Agent, and Hunt Group extensions created in **Section 5.2** and **Section 5.3**, respectively.



Extension Configuration

Extension
DeptID 1
Extension Type Unknown Extension
Group ID N/A

Search for Extension
Extension

Search Range of Extensions
Extension
From To

FILTER
Extension Type
No Selection

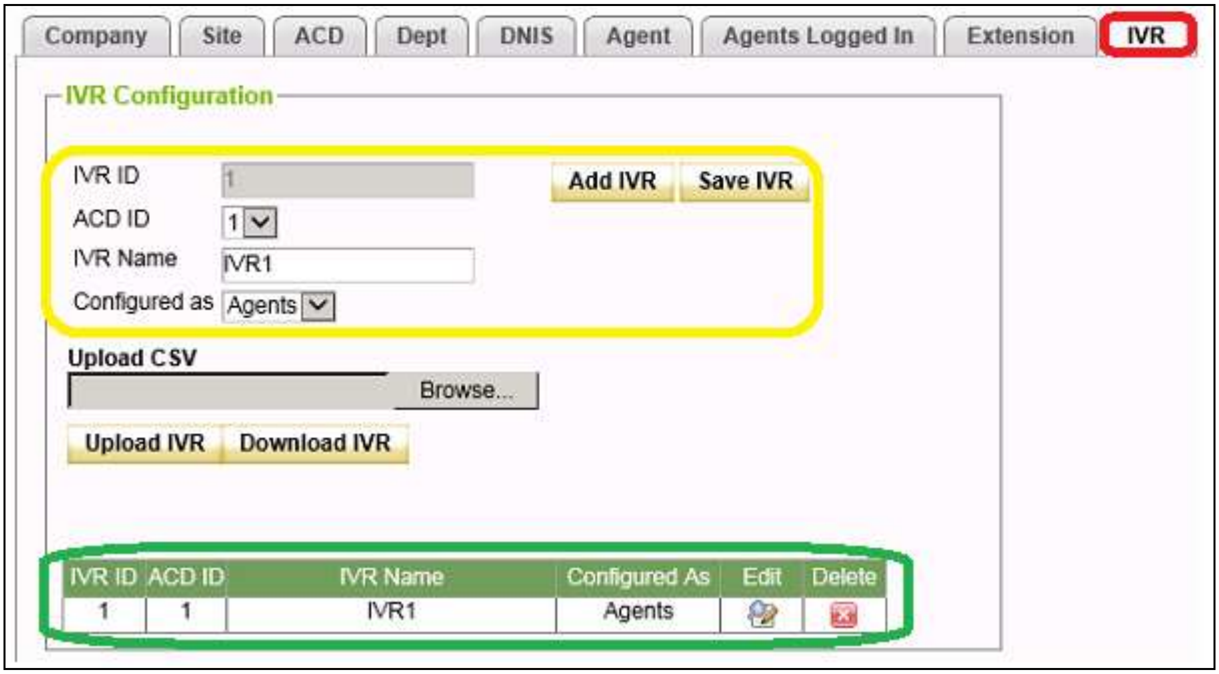
FILTER
Results Per Page
20

Upload CSV

Extension List (ALL Extensions): 18

Extension	DeptID	Extension Type	ACDGroupID	Edit	Delete
11001	1	IVR Ext	N/A	✎	✖
11002	1	IVR Ext	N/A	✎	✖
11003	1	IVR Ext	N/A	✎	✖
11004	1	IVR Ext	N/A	✎	✖
11005	1	IVR Ext	N/A	✎	✖
25001	1	Agent Ext	N/A	✎	✖
25002	1	Agent Ext	N/A	✎	✖
25003	1	Agent Ext	N/A	✎	✖
25501	1	IVR Ext	N/A	✎	✖
25502	1	IVR Ext	N/A	✎	✖
25503	1	IVR Ext	N/A	✎	✖
25504	1	IVR Ext	N/A	✎	✖
25505	1	IVR Ext	N/A	✎	✖
25506	1	IVR Ext	N/A	✎	✖
25507	1	IVR Ext	N/A	✎	✖
25508	1	IVR Ext	N/A	✎	✖
25509	1	IVR Ext	N/A	✎	✖
25510	1	IVR Ext	N/A	✎	✖

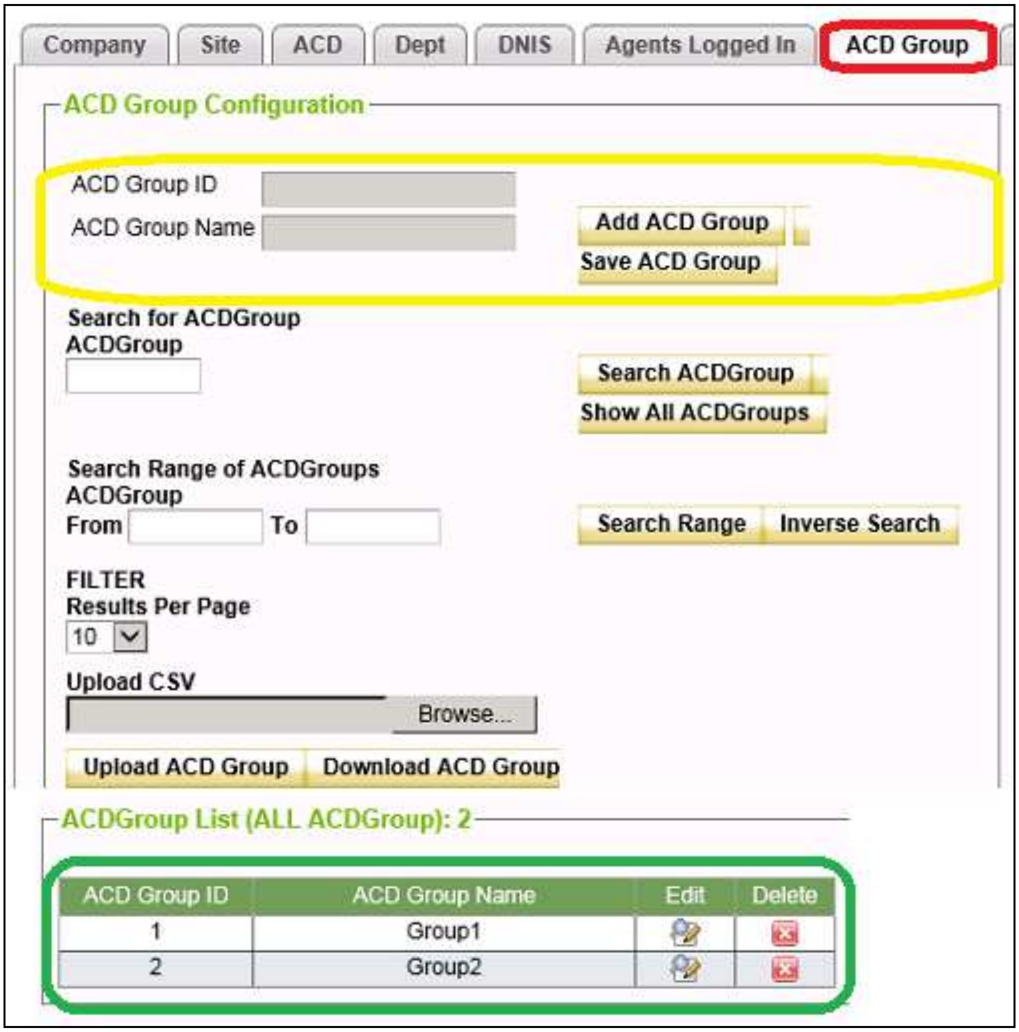
Select the **IVR** tab; enter the **IVR Name**, select **Agents** from the **Configured as** dropdown menu and click **Add IVR**.



IVR ID: 1
ACD ID: 1
IVR Name: IVR1
Configured as: Agents

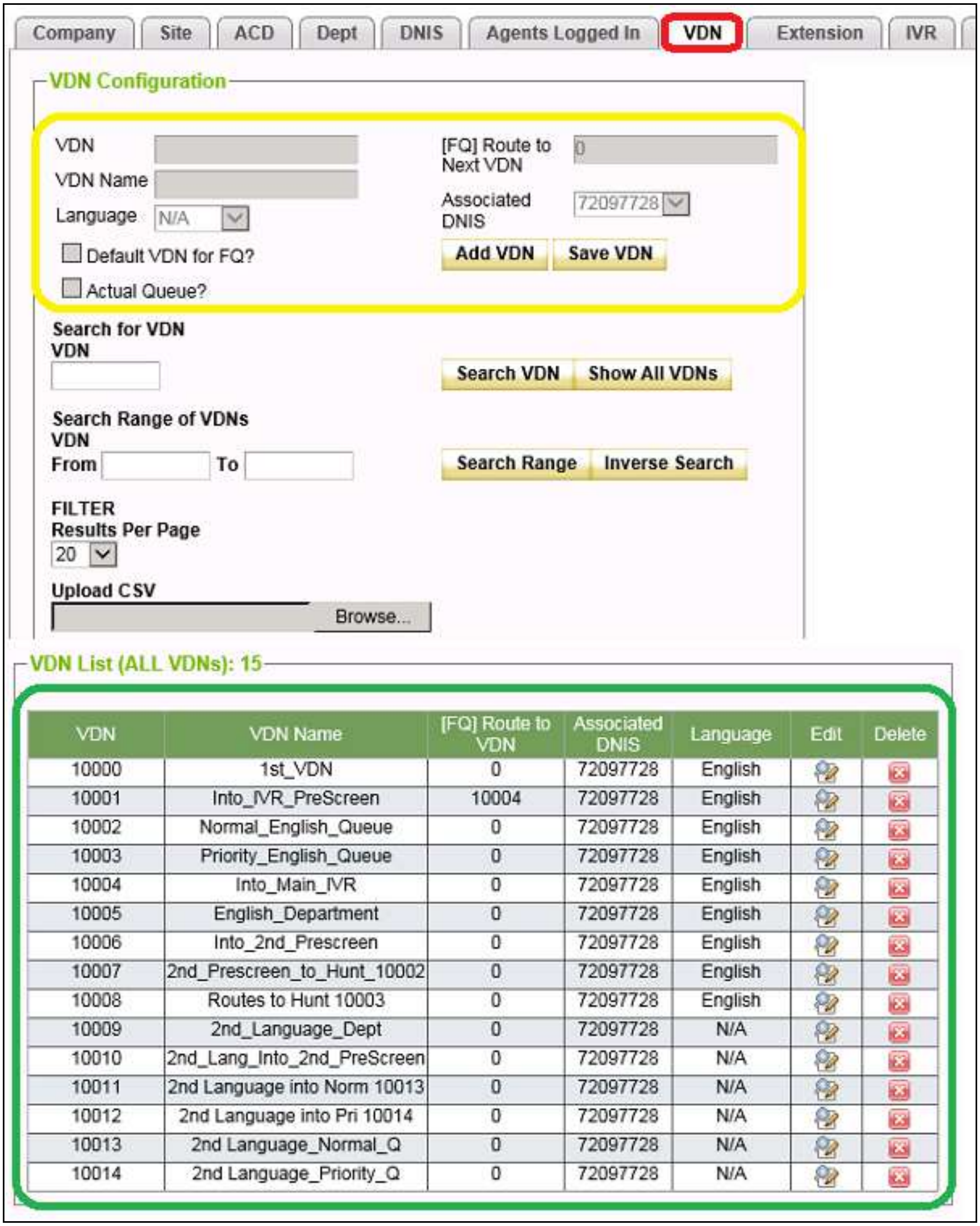
IVR ID	ACD ID	IVR Name	Configured As	Edit	Delete
1	1	IVR1	Agents	✎	☒

Select the **ACD Group** tab, enter **ACD Group ID** and **ACD Group Name**, and click **Add ACD Group**.



ACD Group ID	ACD Group Name	Edit	Delete
1	Group1	✎	☒
2	Group2	✎	☒

Select the **VDN** tab; enter **VDN** and **VDN Name**, and click **Add VDN**. Note these VDNs are the same that were created in **Section 5.5.**



VDN Configuration

VDN

VDN Name

Language N/A

□ Default VDN for FQ?

□ Actual Queue?

[FQ] Route to Next VDN 0

Associated DNIS 72097728

Search for VDN
VDN

Search Range of VDNs
VDN
From To

FILTER
Results Per Page
20

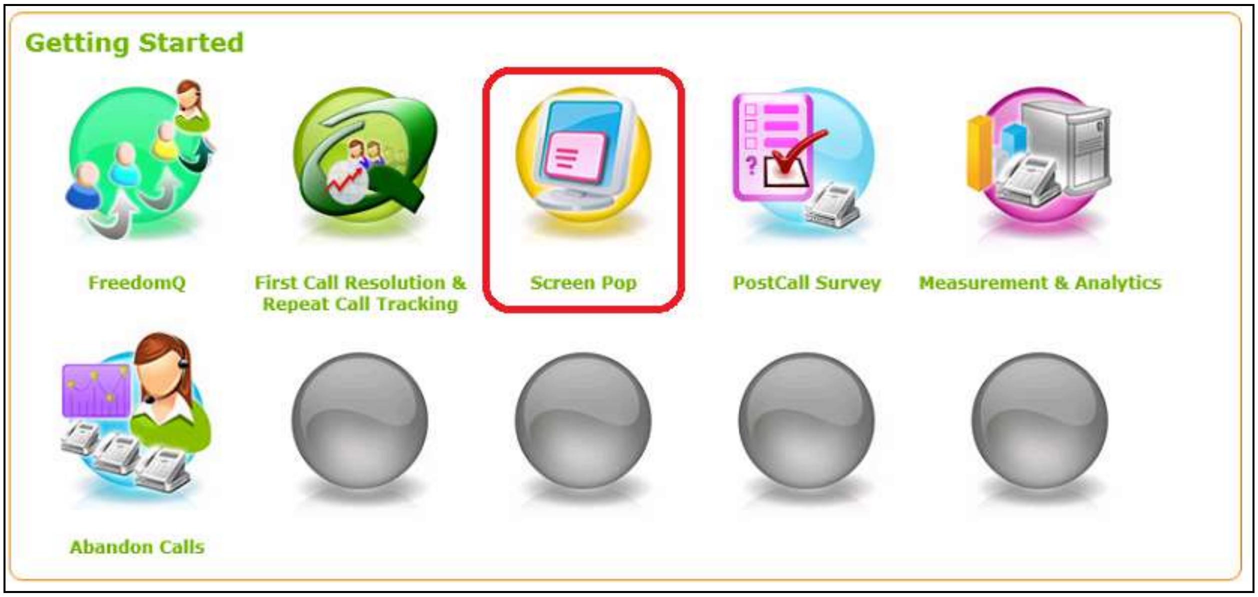
Upload CSV

VDN List (ALL VDNs): 15

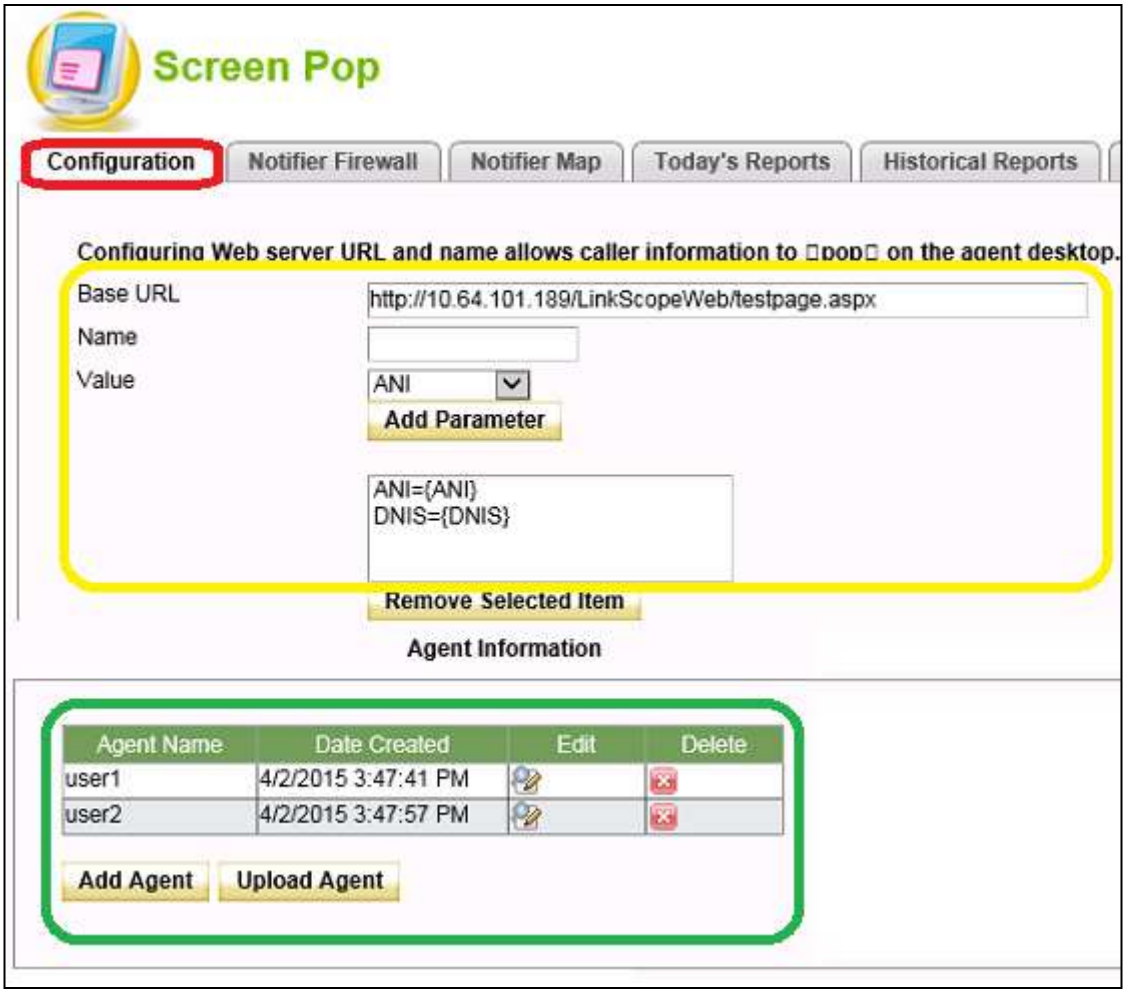
VDN	VDN Name	[FQ] Route to VDN	Associated DNIS	Language	Edit	Delete
10000	1st_VDN	0	72097728	English	✎	☒
10001	Into_IVR_PreScreen	10004	72097728	English	✎	☒
10002	Normal_English_Queue	0	72097728	English	✎	☒
10003	Priority_English_Queue	0	72097728	English	✎	☒
10004	Into_Main_IVR	0	72097728	English	✎	☒
10005	English_Department	0	72097728	English	✎	☒
10006	Into_2nd_Prescreen	0	72097728	English	✎	☒
10007	2nd_Prescreen_to_Hunt_10002	0	72097728	English	✎	☒
10008	Routes to Hunt 10003	0	72097728	English	✎	☒
10009	2nd_Language_Dept	0	72097728	N/A	✎	☒
10010	2nd_Lang_Into_2nd_PreScreen	0	72097728	N/A	✎	☒
10011	2nd Language into Norm 10013	0	72097728	N/A	✎	☒
10012	2nd Language into Pri 10014	0	72097728	N/A	✎	☒
10013	2nd Language_Normal_Q	0	72097728	N/A	✎	☒
10014	2nd Language_Priority_Q	0	72097728	N/A	✎	☒

8.4. Screen Pop Configuration

From the home page click the **Screen Pop** Icon



Set the URL of the desired screen pop page in **Base URL**, add desired parameters and click **Add Parameter**. Create agents, noting the information to be used by agents to log in their Notifier client.



Configuring Web server URL and name allows caller information to pop on the agent desktop.

Base URL: http://10.64.101.189/LinkScopeWeb/testpage.aspx

Name:

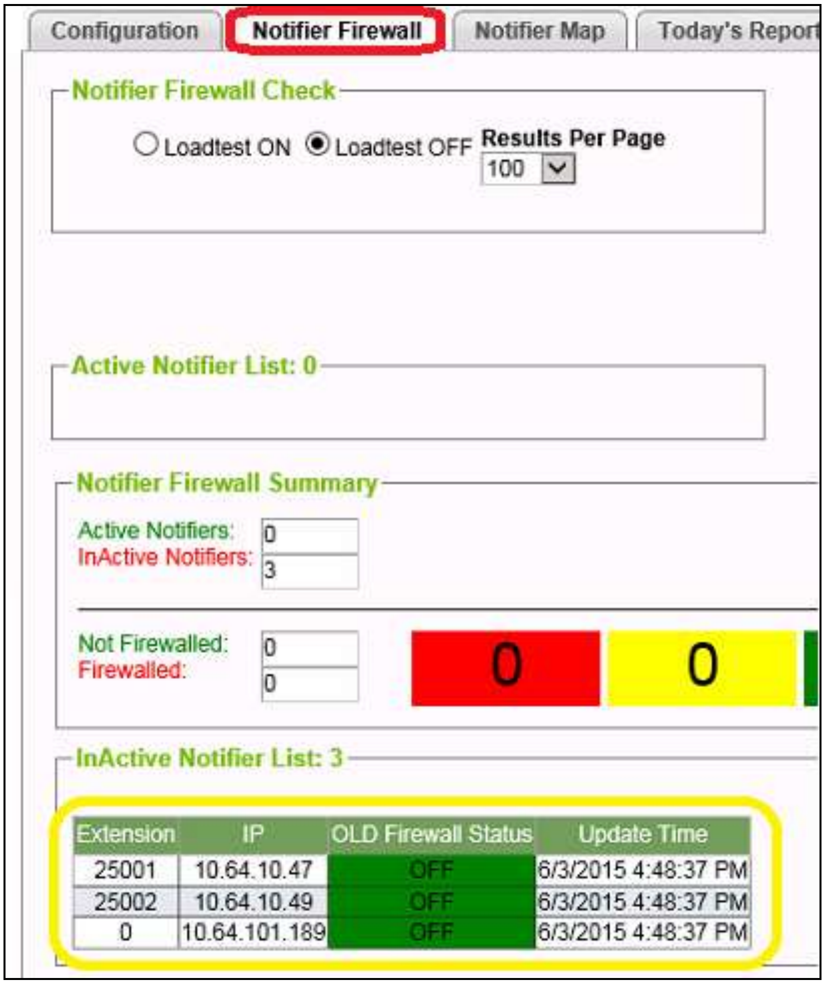
Value: ANI

ANI={ANI}
DNIS={DNIS}

Agent Information

Agent Name	Date Created	Edit	Delete
user1	4/2/2015 3:47:41 PM		☒
user2	4/2/2015 3:47:57 PM		☒

The **Notifier Firewall** tab Assists in identifying firewall issues that will prevent screen pops from reaching agent desktops.



Notifier Firewall Check

○ Loadtest ON ● Loadtest OFF Results Per Page 100

Active Notifier List: 0

Notifier Firewall Summary

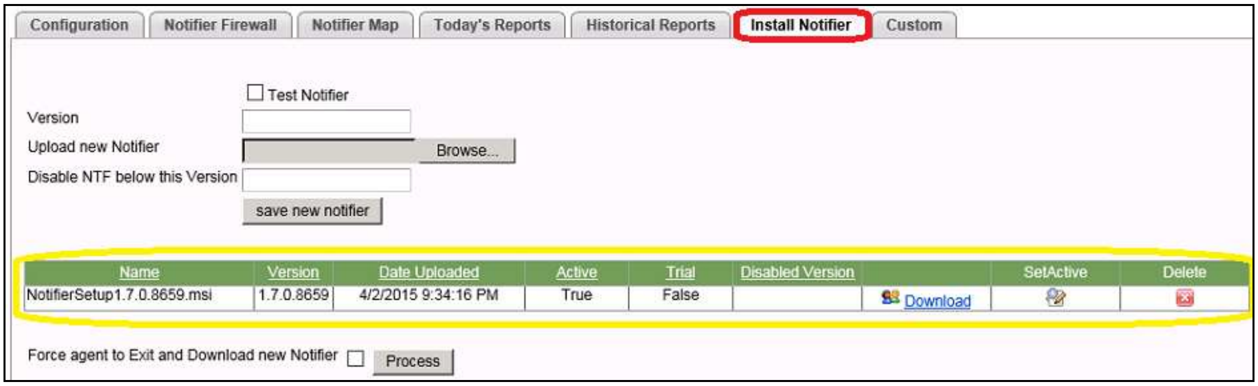
Active Notifiers: 0
InActive Notifiers: 3

Not Firewalled: 0
Firewalled: 0

InActive Notifier List: 3

Extension	IP	OLD Firewall Status	Update Time
25001	10.64.10.47	OFF	6/3/2015 4:48:37 PM
25002	10.64.10.49	OFF	6/3/2015 4:48:37 PM
0	10.64.101.189	OFF	6/3/2015 4:48:37 PM

The **Install Notifier** tab is used to manage, access and distribute the Notifier Screen Pop Client to agent desktops.



□ Test Notifier

Version

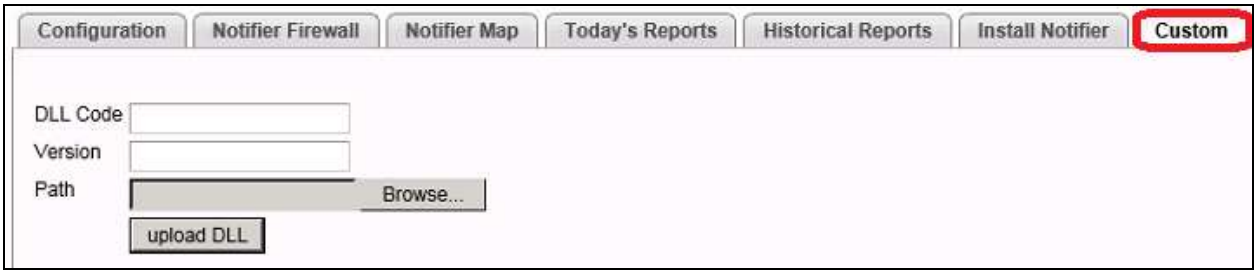
Upload new Notifier

Disable NTF below this Version

Name	Version	Date Uploaded	Active	Trial	Disabled Version		SetActive	Delete
NotifierSetup1.7.0.8659.msi	1.7.0.8659	4/2/2015 9:34:16 PM	True	False		Download	✎	☒

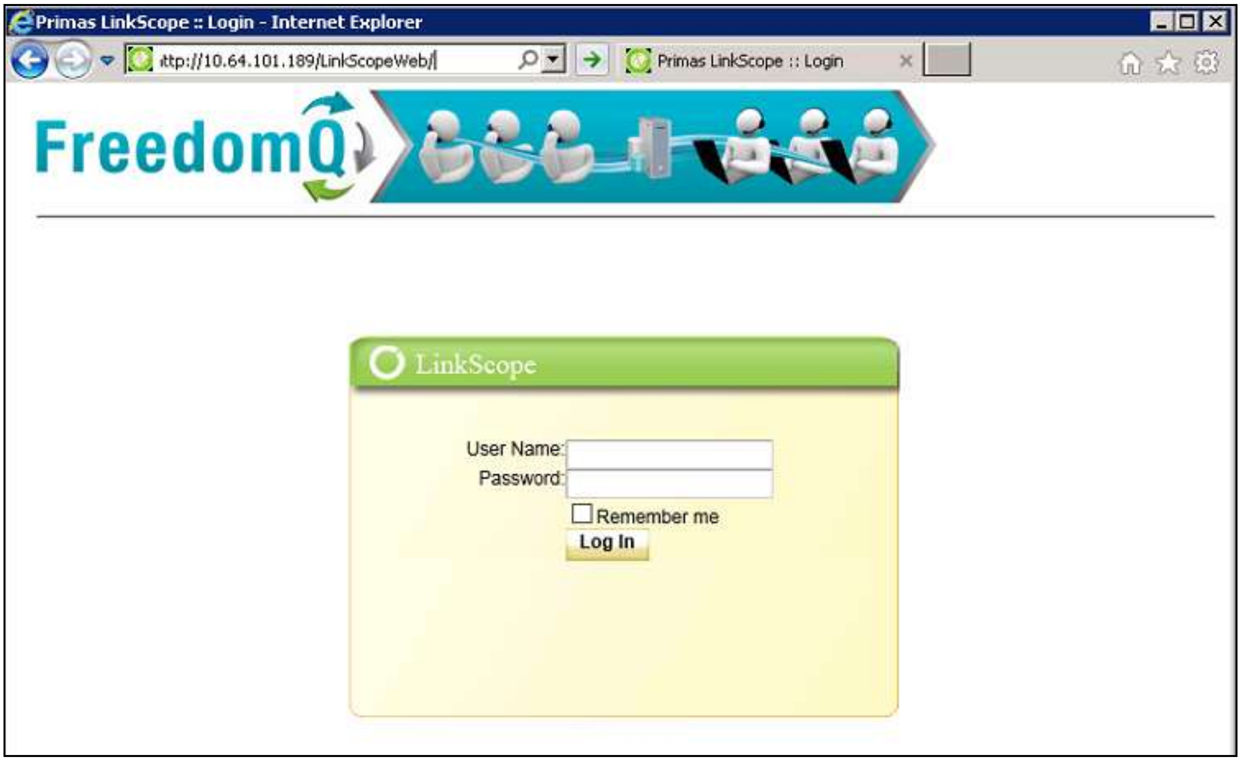
Force agent to Exit and Download new Notifier □

The **Custom** tab can be used to upload and distribute a Custom DLL, used by the Notifier to perform an integrated screen pop



8.5. Agent Desktop Installation and Configuration of LinkScope Notified Client

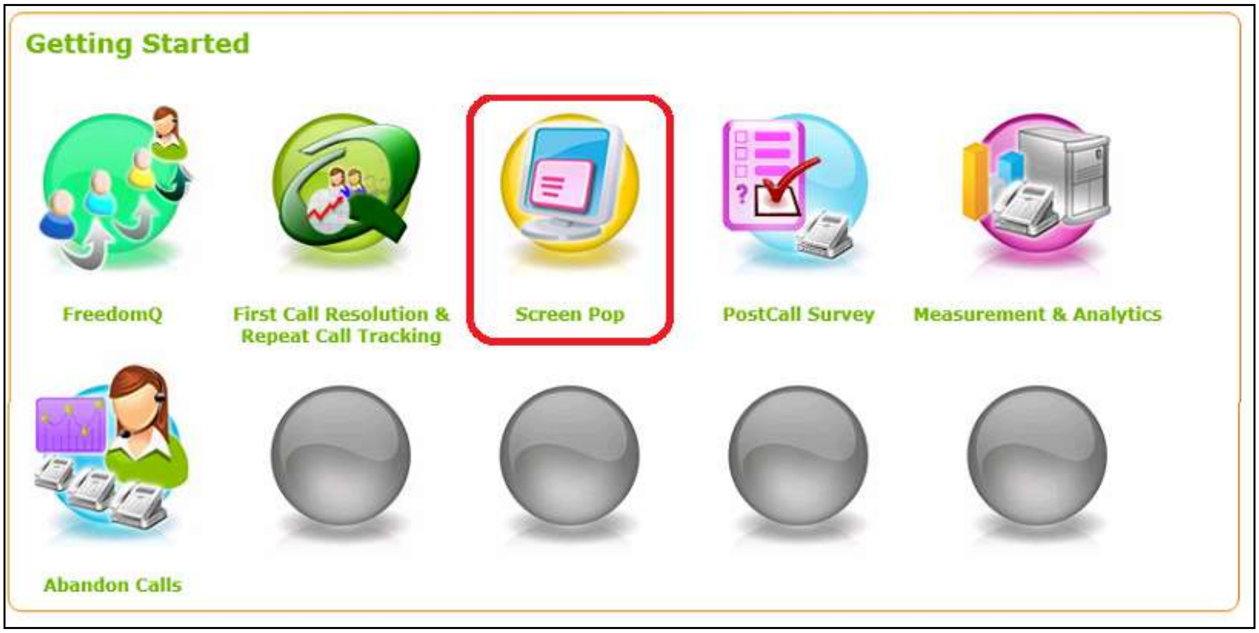
From the Agent Desktop, open a browser to the LinkScope home page and log in http://SERVERIP/LinkScopeWeb/, where SERVERIP is the IP Address of LinkScope server.



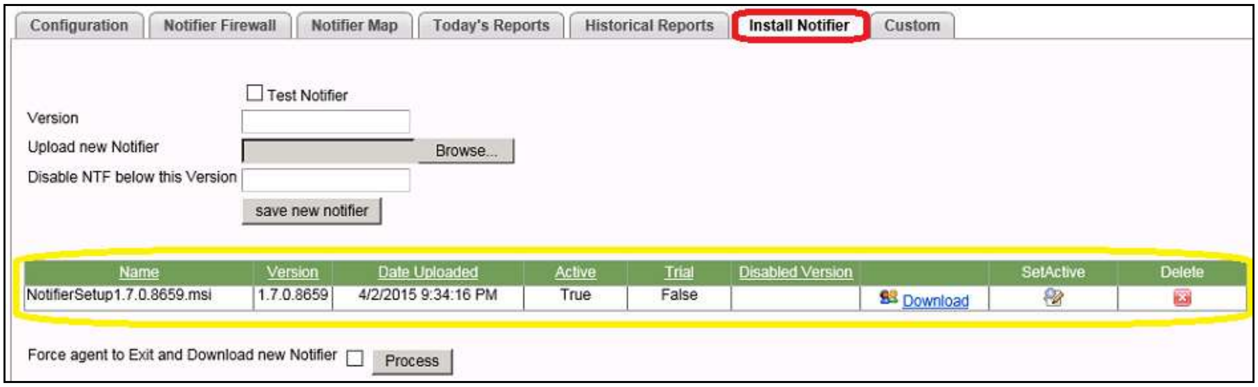
ttp://10.64.101.189/LinkScopeWeb/

Primas LinkScope :: Login - Internet Explorer
Primas LinkScope :: Login
FreedomQ
LinkScope
User Name:
Password:
□ Remember me
Log In

From the home page click the **Screen Pop** Icon



Select the **Install Notifier** tab.



□ Test Notifier

Version

Upload new Notifier Browse...

Disable NTF below this Version

save new notifier

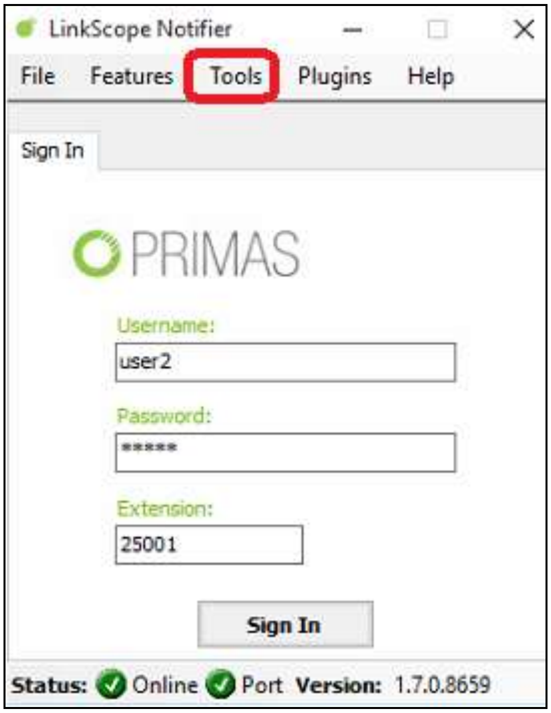
Name	Version	Date Uploaded	Active	Trial	Disabled Version		SetActive	Delete
NotifierSetup1.7.0.8659.msi	1.7.0.8659	4/2/2015 9:34:16 PM	True	False		Download		

Force agent to Exit and Download new Notifier □ Process

Click the **Download** Link, save locally. Run the installation, accepting all defaults until complete.

From **Start Menu** Naviagate to **All Programs → Primas → LinkScope Notifier.**

From the top menu, select **Tools → Options.**

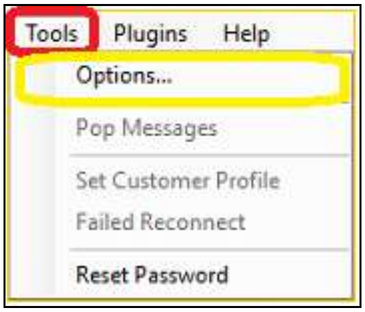


Username: user2

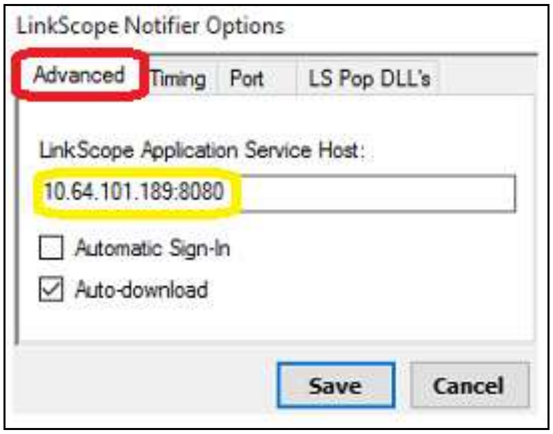
Password: *****

Extension: 25001

Status: Online Port Version: 1.7.0.8659



Select the **Advanced** tab and enter the server IP and port in **LinkScope Application Service Host**.

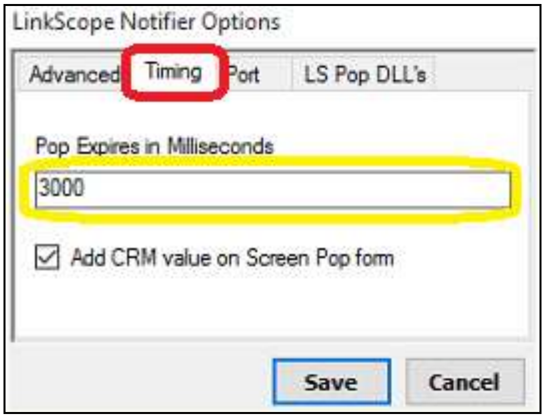


LinkScope Application Service Host: 10.64.101.189:8080

□ Automatic Sign-In

☑ Auto-download

Timing can be left to default or increased for testing purposes.



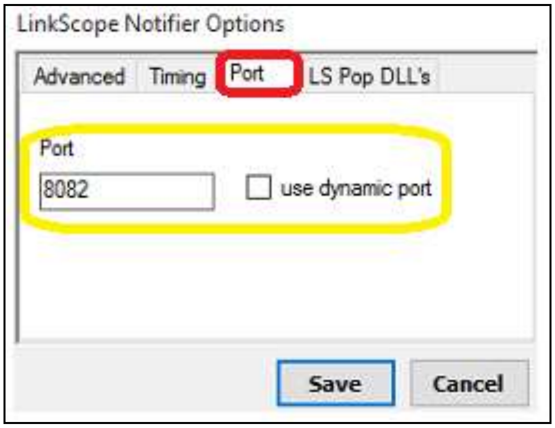
LinkScope Notifier Options

Pop Expires in Milliseconds

3000

☑ Add CRM value on Screen Pop form

Port can be left to default or set to dynamic



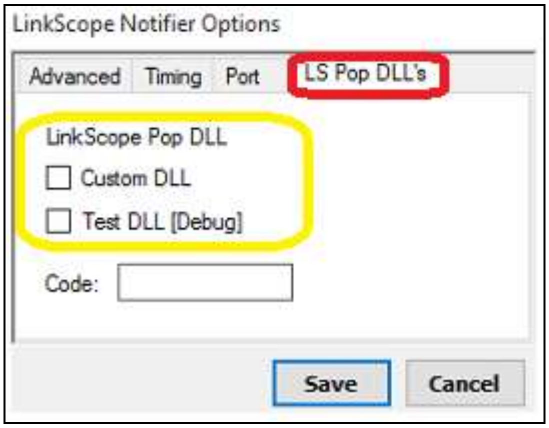
LinkScope Notifier Options

Port

8082

□ use dynamic port

Custom or Test DLLs can be configured (For more information consult the LinkScope Administration Guide)



LinkScope Notifier Options

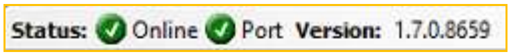
LinkScope Pop DLL

□ Custom DLL

□ Test DLL [Debug]

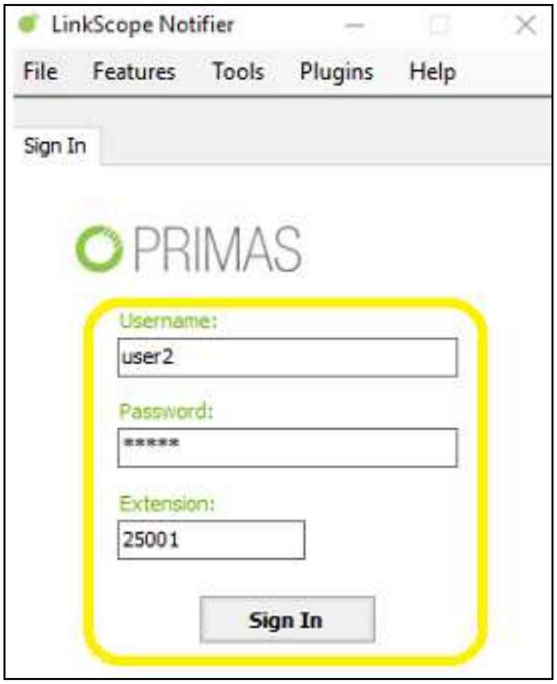
Code:

Status icons indicate that the LinkScope Server is online and that the port is not blocked by a firewall.



Status: ✓ Online ✓ Port Version: 1.7.0.8659

Enter **Username**, **Password** and **Extension**, and click **Sign In.** Note that the Extension is the H.323 station created in **Section 5.2** for Call Center agents.

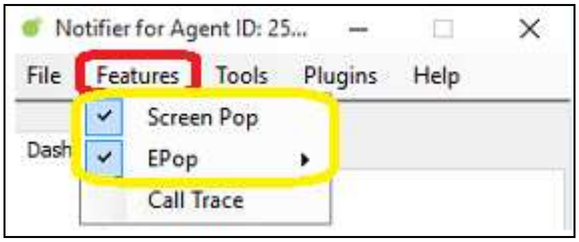


Username: user2

Password: *****

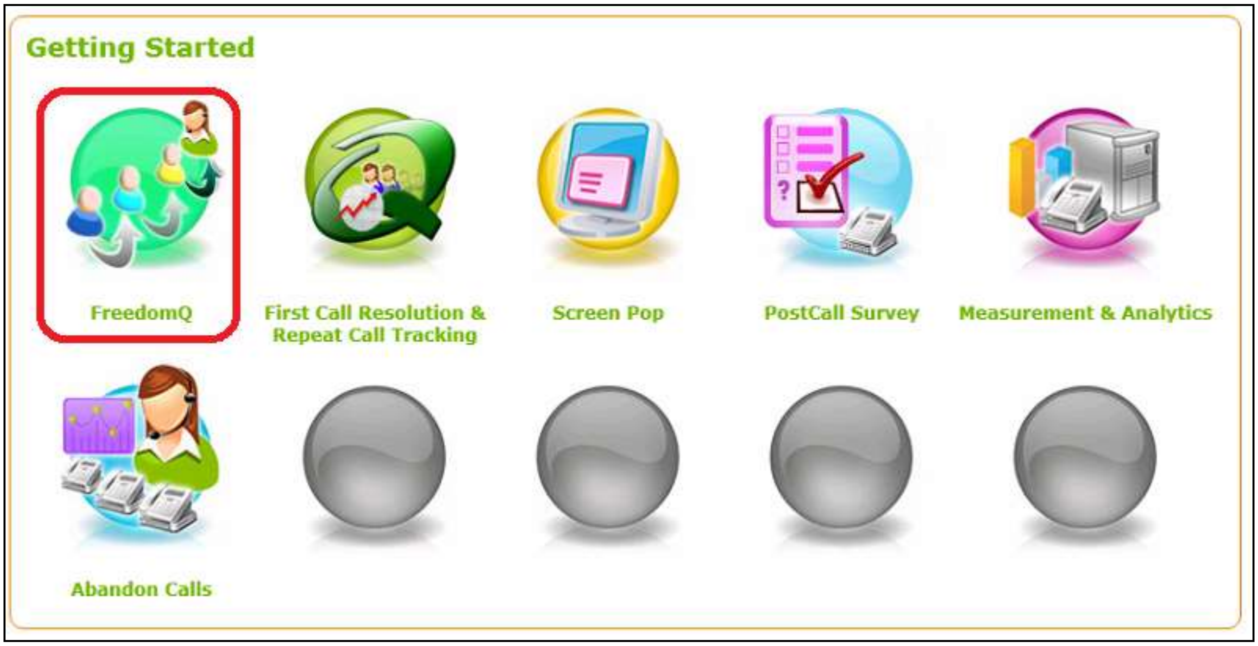
Extension: 25001

Once signed in, use of the **Features** tab allows for the selection of Basic Screen Pop (Screen Pop) or Experience Pop (EPop, Repeat Call Notification with Customizable Agent Script).

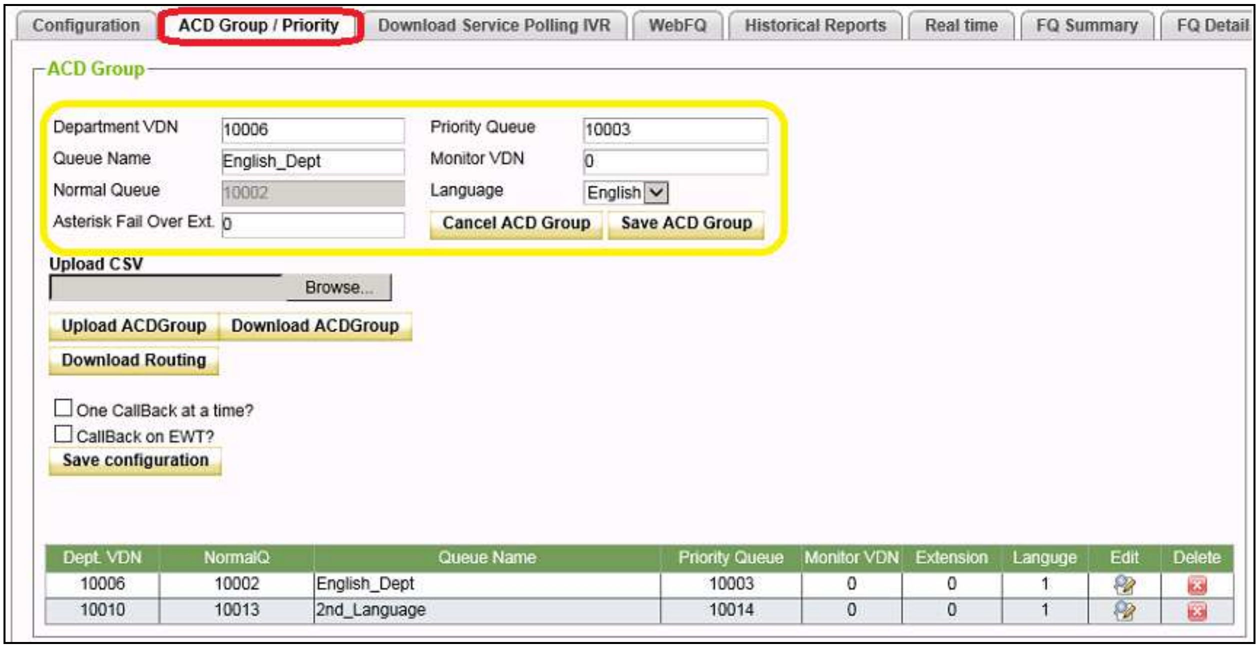


8.6. FreedomQ Configuration

On the LinkScope server, log onto the LinkScope Administration Console, select the FreedomQ icon



Select the **ACD Group / Priority** tab; type in **Department VDN** and **Priority Queue** and click **Save ACD Group**. The VDN and Priority Queue is as configured in Communication Manager.



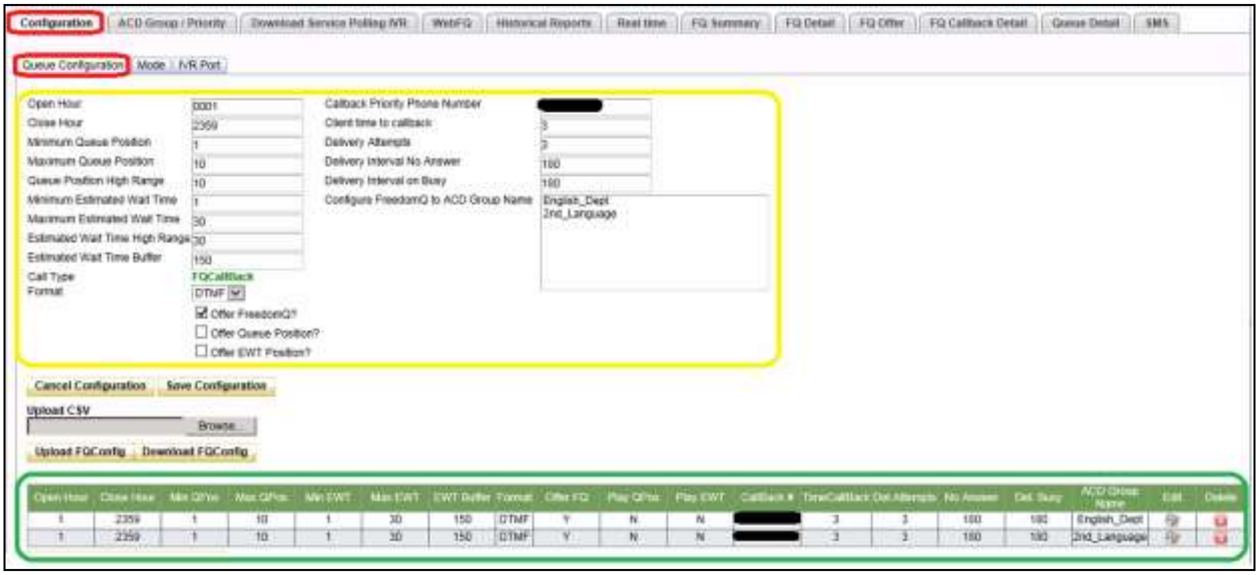
Department VDN	10006	Priority Queue	10003
Queue Name	English_Dept	Monitor VDN	0
Normal Queue	10002	Language	English
Asterisk Fail Over Ext.	0		

☐ One CallBack at a time?

☐ CallBack on EWT?

Dept. VDN	NormalQ	Queue Name	Priority Queue	Monitor VDN	Extension	Languge	Edit	Delete
10006	10002	English_Dept	10003	0	0	1	✎	✖
10010	10013	2nd_Language	10014	0	0	1	✎	✖

Select the **Configuration** tab followed by the **Queue Configuration** tab. For each language and/or department provide the desired FreedomQ performance parameters and click **Save Configuration**.

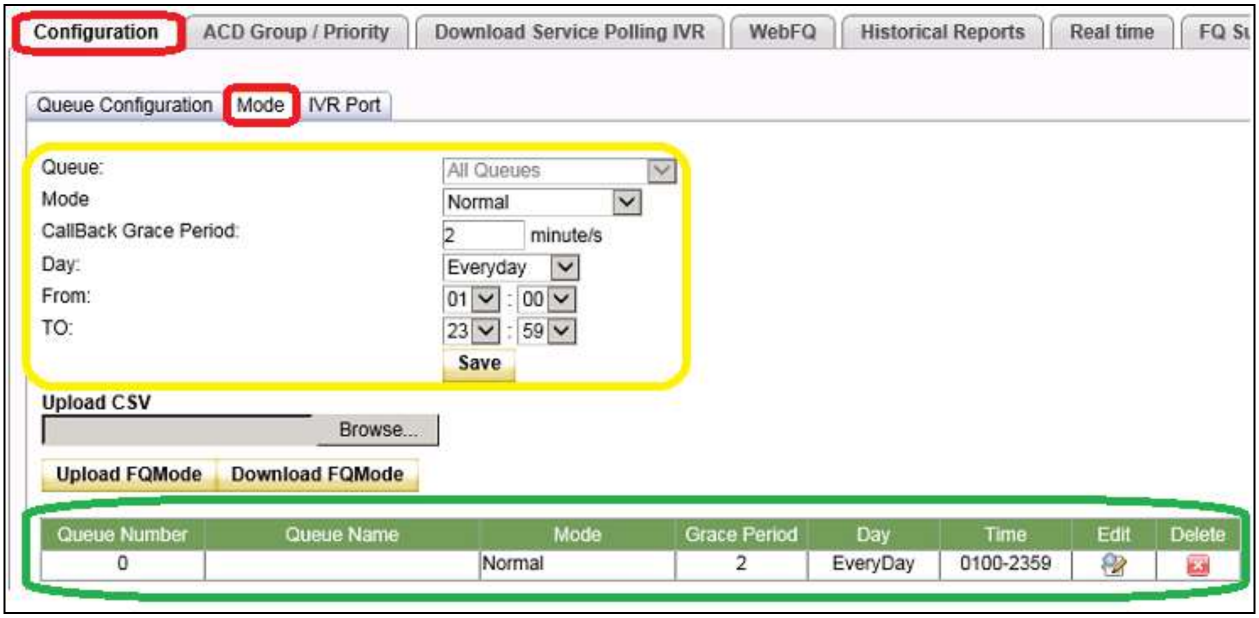


Open Hour	0001	Callback Priority Phone Number	[redacted]
Close Hour	2359	Client time to callback	3
Minimum Queue Position	1	Delivery Attempts	3
Maximum Queue Position	10	Delivery Interval No Answer	180
Queue Position High Range	10	Delivery Interval on Busy	180
Minimum Estimated Wait Time	1	Configure FreedomQ to ACD Group Name	English_Dept 2nd_Language
Maximum Estimated Wait Time	30		
Estimated Wait Time High Range	30		
Estimated Wait Time Buffer	150		
Call Type	FQCallBack		
Format	DTMF		

☑ Offer FreedomQ?
☐ Offer Queue Position?
☐ Offer EWT Position?

Open Hour	Close Hour	Min QPos	Max QPos	Min EWT	Max EWT	EWT Buffer	Format	Offer FQ	Play QPos	Play EWT	CallBack #	TimeCallBack	Del.Attempts	No Answer	Del. Busy	ACD Group Name	Edit	Delete
1	2359	1	10	1	30	150	DTMF	Y	N	N	[redacted]	3	3	180	180	English_Dept		
1	2359	1	10	1	30	150	DTMF	Y	N	N	[redacted]	3	3	180	180	2nd_Language		

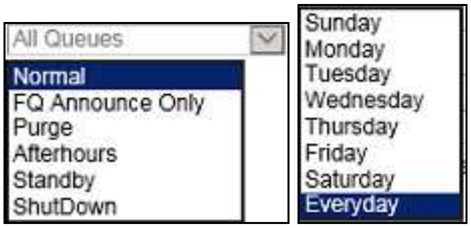
Select the **Mode** tab. Complete parameters as desired and click **Save**.



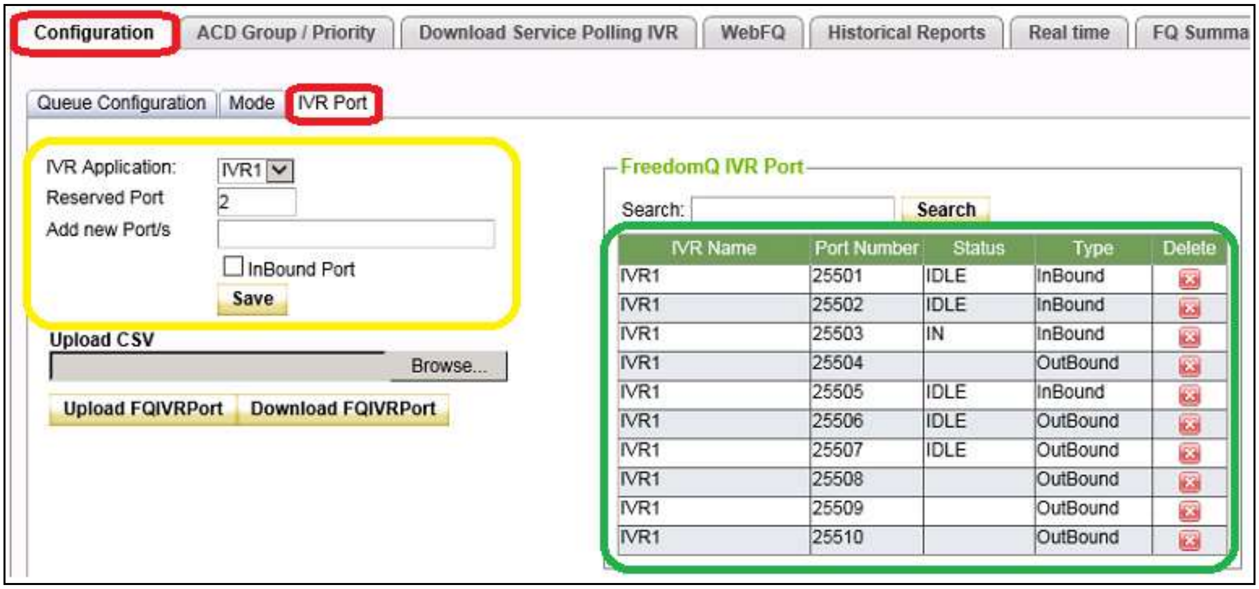
Queue:	All Queues
Mode	Normal
CallBack Grace Period:	2 minute/s
Day:	Everyday
From:	01 : 00
TO:	23 : 59

Queue Number	Queue Name	Mode	Grace Period	Day	Time	Edit	Delete
0		Normal	2	EveryDay	0100-2359		

Examples of Mode Parameters:



Select the **IVR Port** tab, configure inbound/out bound ports and click **Save**.



IVR Application: IVR1

Reserved Port: 2

Add new Port/s:

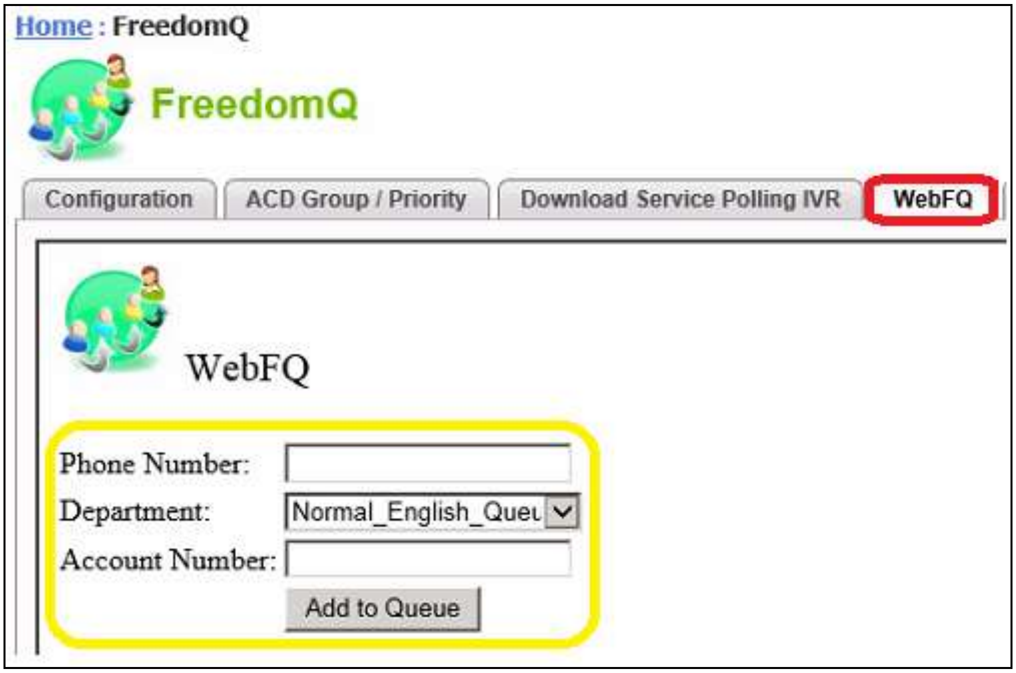
□ InBound Port

Search:

IVR Name	Port Number	Status	Type	Delete
IVR1	25501	IDLE	InBound	☒
IVR1	25502	IDLE	InBound	☒
IVR1	25503	IN	InBound	☒
IVR1	25504		OutBound	☒
IVR1	25505	IDLE	InBound	☒
IVR1	25506	IDLE	OutBound	☒
IVR1	25507	IDLE	OutBound	☒
IVR1	25508		OutBound	☒
IVR1	25509		OutBound	☒
IVR1	25510		OutBound	☒

8.6.1. WebFQ

Continuing from previous section, within FreedomQ Configuration, select the **WebFQ** tab.



Phone Number:

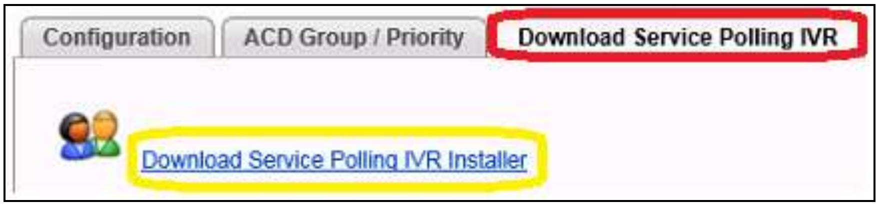
Department: Normal_English_Queu

Account Number:

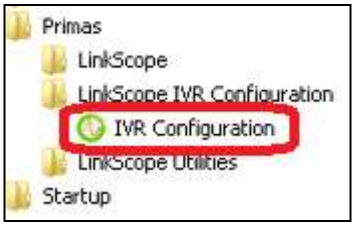
Relying on the FreedomQ configuration that was completed in the previous step, WebFQ adds callers to the language and department queues via the web. The WebFQ code is deployed via the inclusion of an HTML widget on any website. This page allows for the testing of that code in preparation for deployment.

8.6.2. Outbound IVR Polling Service Configuration

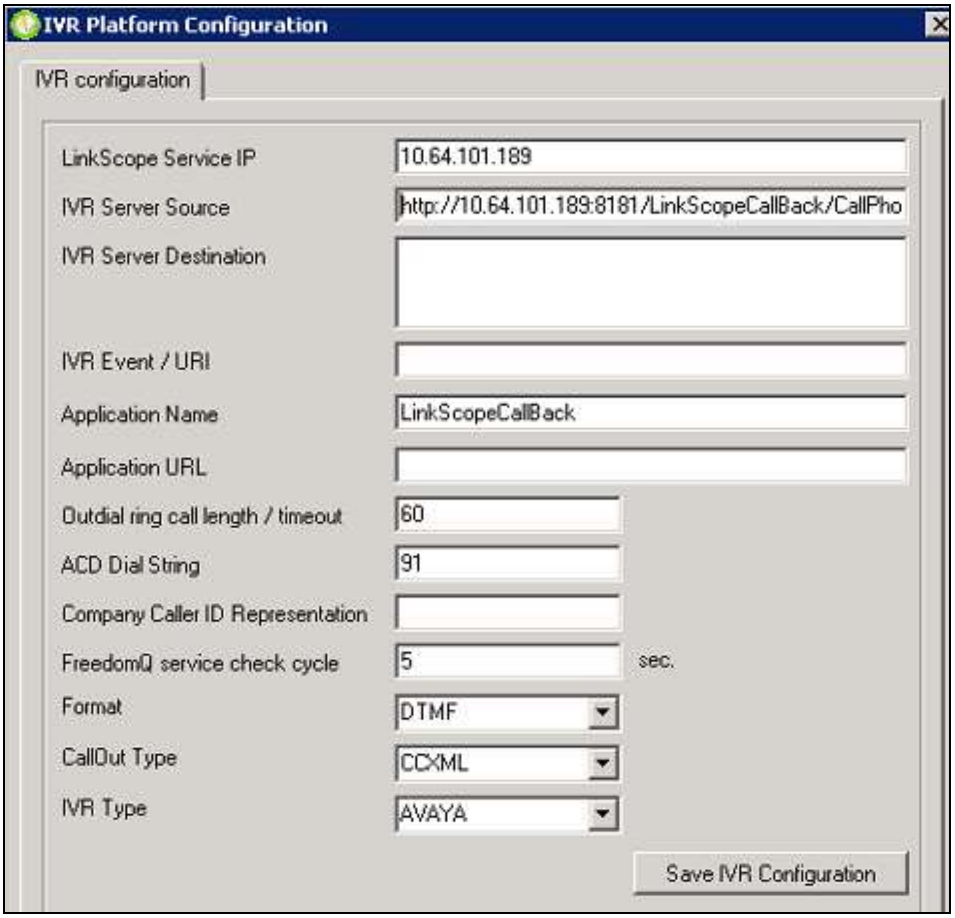
Continuing from previous section, within FreedomQ Configuration, select the **Download Service Polling IVR** tab. Click to download the Installer, execute accepting defaults until installation is complete.


Configuration
ACD Group / Priority
Download Service Polling IVR
Download Service Polling IVR Installer

From the Start menu select **Primas → LinkScope IVR Configuration → IVR Configuration.**



Enter the IVR Configuration and click **Save IVR Configuration.**


IVR Platform Configuration

IVR configuration

LinkScope Service IP	10.64.101.189
IVR Server Source	http://10.64.101.189:8181/LinkScopeCallBack/CallPho
IVR Server Destination	
IVR Event / URI	
Application Name	LinkScopeCallBack
Application URL	
Outdial ring call length / timeout	60
ACD Dial String	91
Company Caller ID Representation	
FreedomQ service check cycle	5 sec.
Format	DTMF
CallOut Type	CCXML
IVR Type	AVAYA

Save IVR Configuration

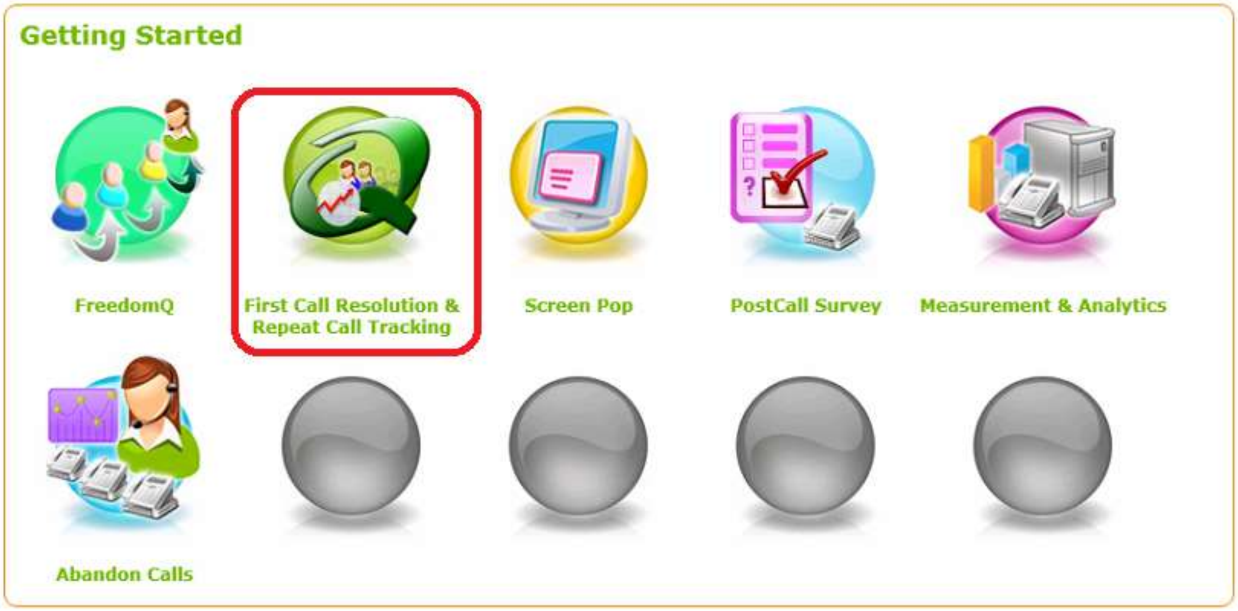
In the above example:

Parameter	Value	Explanation
LinkScope Service IP	10.64.101.189	IP Address of the LinkScope Server
IVR Server Source	http://10.64.101.189:8181/LinkScopeCallBack/CallPhoneServlet?1=1	IP Address must be replaced with Tomcat Server IP
Application Name	LinkScopeCallBack	Exact Name of the Tomcat Deployed Outbound Application

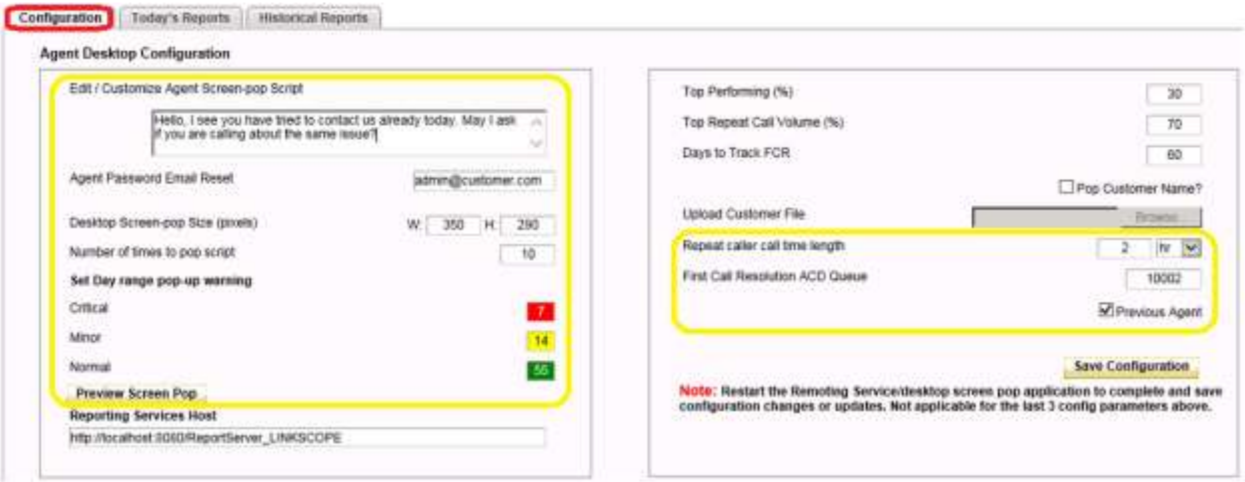
Note: The LinkScope Server will come preconfigured by Primas. This information is included for informational purposes.

8.7. Experience Pop Configuration

On the LinkScope server, while logged into the LinkScope Administration Console, select the **First Call Resolution & Repeat Call Tracking** icon



From the **Configuration** tab, provide Experience Pop window parameters, repeat caller detection and ACD Queue information and click **Save Configuration**.



Agent Desktop Configuration

Edit / Customize Agent Screen-pop Script: Hello, I see you have tried to contact us already today. May I ask if you are calling about the same issue?

Agent Password Email Reset: admin@customer.com

Desktop Screen-pop Size (pixels) W: 350 H: 290

Number of times to pop script: 10

Set Day range pop-up warning

Critical: 7

Minor: 14

Normal: 56

Reporting Services Host: http://localhost:8080/ReportServer_LINKSCOPE

Top Performing (%): 30

Top Repeat Call Volume (%): 70

Days to Track FCR: 60

□ Pop Customer Name?

Upload Customer File

Repeat caller call time length: 2 hr

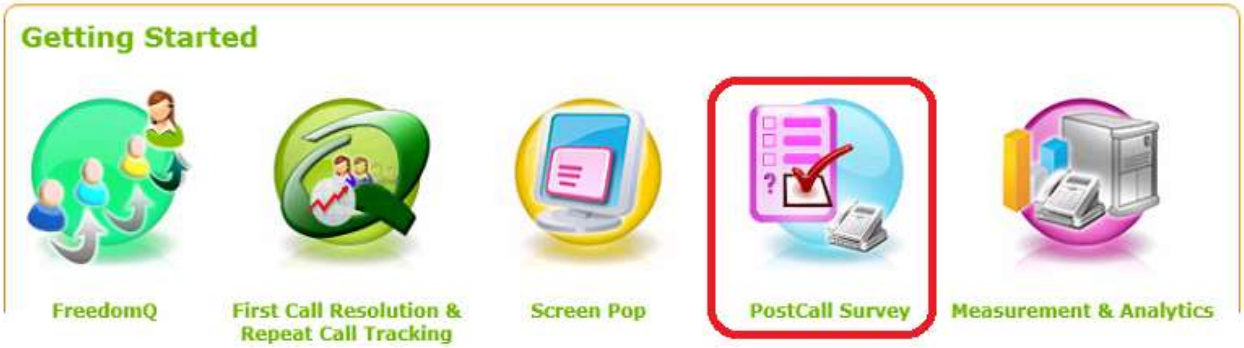
First Call Resolution ACD Queue: 10002

☑ Previous Agent

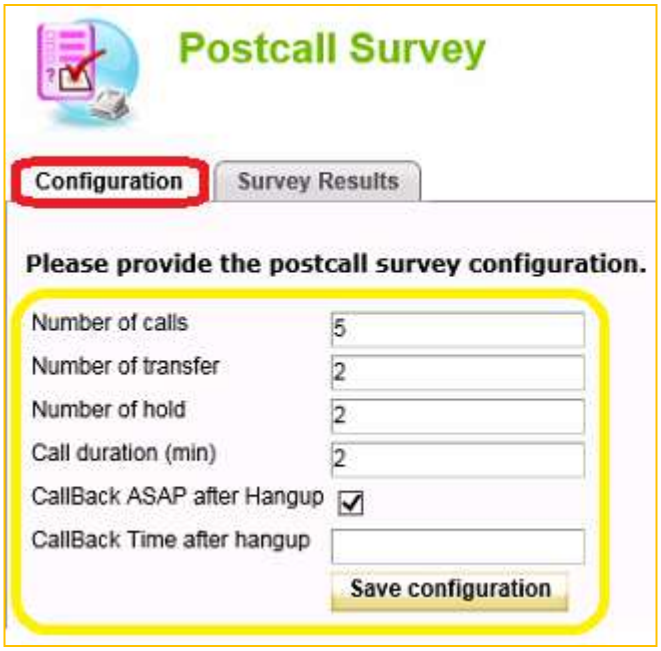
Note: Restart the Remoting Service/desktop screen pop application to complete and save configuration changes or updates. Not applicable for the last 3 config parameters above.

8.7.1. Experience Pop Configuration

From the Main LinkScope administration menu, select **Post Call Survey**.



From the **Configuration** tab, provide desired parameters and click **Save configuration**.



Please provide the postcall survey configuration.

Number of calls	5
Number of transfer	2
Number of hold	2
Call duration (min)	2
CallBack ASAP after Hangup	☑
CallBack Time after hangup	

8.8. ReconX

No Additional configuration is required for ReconX to function. This has been accomplished by:

- Addition of Agent Extensions in LinkScope Basic Configuration
- Configuration of Screen Pop
- Deployment of Notifier to the Agent Desktop
- Configuration of FreedomQ ACD Groups
- Installation and Configuration of the IVR Outbound Polling Service on the LinkScope Server

By default, any call to an agent that disconnects will automatically generate a ReconX pop up window on the agent desktop.

8.9. IVR Application Deployment

Two VXML and one CCXML applications are required for the LinkScope Solution. These are deployed to a tomcat server and then referenced by Experience Portal. The applications are:

Name	Tomcat URL	Type
Pre Screen	http://10.64.101.189:8181/Prescreen_DEMO/Start	VXML (Inbound)
Call Back	http://10.64.101.189:8181/Callback_DEMO/Start	VXML (Outbound)
LinkScope CallBack	http://10.64.101.189:8181/LinkScopeCallBack/CallPhoneServlet?1=1	CCXML

Name	Required?					
	Basic Pop	Enhanced Pop	FreedomQ	WebFQ	Post Call Survey	ReconX
Pre Screen	No	No	Yes	Yes	Yes	Yes
Call Back	No	No	Yes	Yes	Yes	Yes
LinkScope CallBack	No	No	Yes	Yes	Yes	Yes

9. Conclusion

These Application Notes describe the configuration steps required to integrate the Primas Group LinkScope Customer Experience Power Pack application with Avaya Aura® Communication Manager, Avaya Aura® Application Enablement Services and Avaya Aura® Experience Portal. All feature and serviceability test cases were completed successfully.

10. Additional References

This section references the product documentation that is relevant to these Application Notes.

[1] Administering Avaya Aura® Experience Portal, April 2015

[2] Administering Avaya Aura® Communication Manager, Release 6.3, Document 03-300509, Issue 7.0, December 2014

[3] LinkScope Customer Experience Power Pack | Installation Guide V 7.1 May 2015

[4] LinkScope Customer Experience Power Pack | Configuration Guide V 7.1 May 2015

[5] LinkScope Customer Experience Power Pack | Administration Guide V 7.1 May 2015

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 Dev*Connec*t Program at devconnect@avaya.com.