



## **Avaya Solution & Interoperability Test Lab**

---

# **Application Notes for IPC Alliance 15.03 with Avaya Aura® Communication Manager 6.3 and Avaya Aura® Session Manager 6.3 using SIP Trunks – Issue 1.0**

### **Abstract**

These Application Notes describe the configuration steps required for IPC Alliance 15.03 to interoperate with Avaya Aura® Communication Manager 6.3 and Avaya Aura® Session Manager 6.3 using SIP trunks.

IPC Alliance is a trading communication solution. In the compliance testing, IPC Alliance used SIP trunks to Avaya Aura® Session Manager, for turrent users on IPC to reach users on Avaya Aura® Communication Manager and on the PSTN.

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 IPC Alliance 15.03 to interoperate with Avaya Aura® Communication Manager 6.3 and Avaya Aura® Session Manager 6.3 using SIP trunks.

IPC Alliance is a trading communication solution. In the compliance testing, IPC Alliance 15.03 used SIP trunks to Avaya Aura® Session Manager, for turret users on IPC to reach users on Avaya Aura® Communication Manager and on the PSTN.

## 2. General Test Approach and Test Results

The feature test cases were performed manually. Calls were manually established among IPC turret users with Avaya SIP, Avaya H.323, and/or PSTN users. Call controls were performed from the various users to verify the call scenarios.

The serviceability test cases were performed manually by disconnecting and reconnecting the LAN connection to the IPC ESS server.

### 2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing included basic call, display, G.711, codec negotiation, media shuffling, hold/reconnect, DTMF, call forwarding unconditional/ring-no-answer/busy, blind/attended transfer, and conference.

The serviceability testing focused on verifying the ability of IPC Alliance to recover from adverse conditions, such as disconnecting/reconnecting the LAN connection to IPC Alliance 15.03

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.

### 2.2. Test Results

All test cases were executed and verified.

### 2.3. Support

Technical support on IPC Alliance can be obtained through the following:

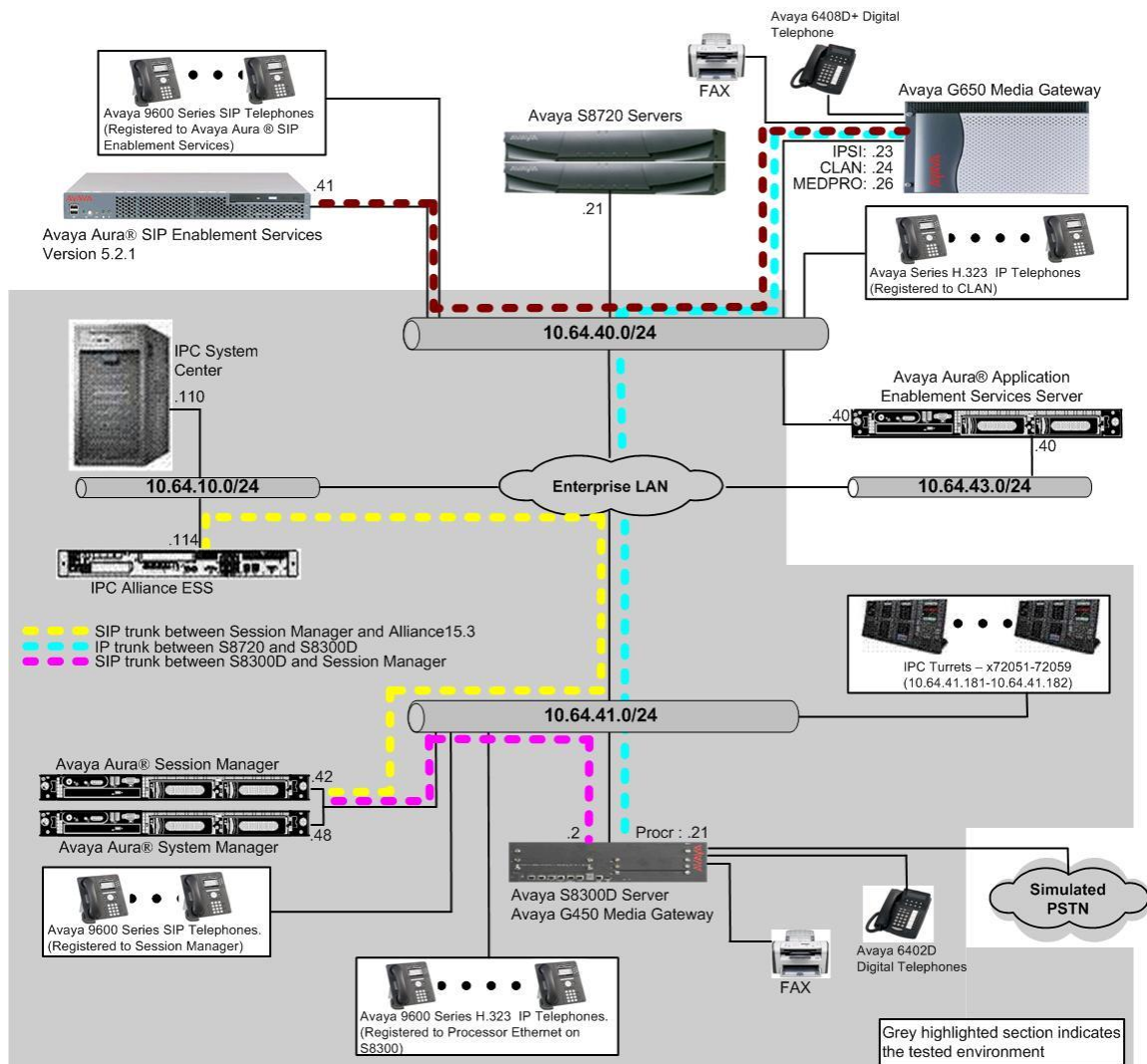
- **Phone:** (800) NEEDIPC, (203) 339-7800
- **Email:** [systems.support@ipc.com](mailto:systems.support@ipc.com)

### 3. Reference Configuration

As shown in the test configuration below, IPC Alliance 15.03 at the Remote Site consists of the Enterprise SIP Server (ESS), Alliance MX, System Center, and Turrets. SIP trunks are used from IPC Alliance to Avaya Aura® Session Manager, to reach users on Avaya Aura® Communication Manager and on the PSTN. In the compliance testing, the “avaya.com” domain was used for Avaya site, and “ipc.com” was used on IPC site.

A five digit Uniform Dial Plan (UDP) was used to facilitate dialing between the Central and Remote sites. Unique extension ranges were associated with Avaya Aura® Communication Manager users at the Central site (720xx), and IPC turret users at the Remote site (332xx).

The configuration of Avaya Aura® Session Manager is performed via the web interface of Avaya Aura® System Manager. The detailed administration of basic connectivity between Avaya Aura® Communication Manager, Avaya Aura® System Manager, and Avaya Aura® Session Manager is not the focus of these Application Notes and will not be described.



**Figure 1: Test Configuration of IPC Alliance system**

## 4. Equipment and Software Validated

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

| Equipment  | Software  |
|--|---|
| Avaya Aura® Communication Manager on Avaya S8300D Server   | R016x.03.0.124.0-21172  |
| Avaya Aura® Session Manager  | 6.3.5.0.635005  |
| Avaya Aura® System Manager   | 6.3.5.5.2017  |
| Avaya 9620 IP Telephone (H.323)  | 3.1   |
| Avaya 9630 IP Telephone (SIP)  | 2.6.4   |
| Avaya A175 Desktop Video Device (SIP)  | Hardware - 2.0  |
| IPC Alliance 15.03 <ul style="list-style-type: none"><li>• Alliance MX</li><li>• System Center<ul style="list-style-type: none"><li>○ SIPX Line Card</li></ul></li><li>• Turrets</li><li>• Enterprise SIP Server</li></ul> | 15.03.00.23<br>15.03.00.23<br>15.03.00.23<br>15.03.00.23<br>15.03.00.22<br>2.01.00-03 |

## 5. Configure Avaya Aura® Communication Manager

This section provides the procedures for configuring Communication Manager. The procedures include the following areas:

- Verify Communication Manager license
- Administer system parameters features
- Administer SIP trunk group
- Administer SIP signaling group
- Administer IP network region
- Administer IP codec set
- Administer route pattern
- Administer private numbering
- Administer uniform dial plan
- Administer AAR analysis
- Administer ISDN trunk group
- Administer tandem calling party number

In the compliance testing, the same set of codec set, network region, trunk group, and signaling group were used for the Avaya SIP and IPC turret users, which enabled IPC turret users to use the same digits dialing as Avaya SIP users, to reach other users on Communication Manager and on the PSTN.

### 5.1. Verify Communication Manager License

Log into the System Access Terminal (SAT) to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the “display system-parameters customer-options” command. Navigate to **Page 2**, and verify that there is sufficient remaining capacity for SIP trunks by comparing the **Maximum Administered SIP Trunks** field value with the corresponding value in the **USED** column.

The license file installed on the system controls the maximum permitted. If there is insufficient capacity, contact an authorized Avaya sales representative to make the appropriate changes.

|  |      |              |
|--|------|--------------|
| display system-parameters customer-options                   |      | Page 2 of 11 |
| OPTIONAL FEATURES  |      |              |
| IP PORT CAPACITIES   | USED |              |
| Maximum Administered H.323 Trunks: 4000                      | 27   |              |
| Maximum Concurrently Registered IP Stations: 2400            | 2    |              |
| Maximum Administered Remote Office Trunks: 4000              | 0    |              |
| Maximum Concurrently Registered Remote Office Stations: 2400 | 0    |              |
| Maximum Concurrently Registered IP eCons: 68                 | 0    |              |
| Max Concur Registered Unauthenticated H.323 Stations: 100    | 0    |              |
| Maximum Video Capable Stations: 2400                         | 2    |              |
| Maximum Video Capable IP Softphones: 2400                    | 2    |              |
| Maximum Administered SIP Trunks: 4000                        | 65   |              |
| Maximum Administered Ad-hoc Video Conferencing Ports: 4000   | 0    |              |
| Maximum Number of DS1 Boards with Echo Cancellation: 80      | 0    |              |

## 5.2. Administer System Parameters Features

Use the “change system-parameters features” command to allow for trunk-to-trunk transfers.

This feature is needed to be able to transfer an incoming call from IPC back out to IPC (incoming trunk to outgoing trunk), and to transfer an outgoing call to IPC to another outgoing call to IPC (outgoing trunk to outgoing trunk). For ease of interoperability testing, the **Trunk-to-Trunk Transfer** field was set to “all” to enable all trunk-to-trunk transfers on a system wide basis. Note that this feature poses significant security risk, and must be used with caution. For alternatives, the trunk-to-trunk feature can be implemented on the Class Of Restriction or Class Of Service levels. Refer to [1] for more details.

```
change system-parameters features                               Page 1 of 20
      FEATURE-RELATED SYSTEM PARAMETERS
      Self Station Display Enabled? n
      Trunk-to-Trunk Transfer: all
      Automatic Callback with Called Party Queuing? n
      Automatic Callback - No Answer Timeout Interval (rings): 3
      Call Park Timeout Interval (minutes): 10
      Off-Premises Tone Detect Timeout Interval (seconds): 20
      AAR/ARS Dial Tone Required? y

      Music (or Silence) on Transferred Trunk Calls? no
      DID/Tie/ISDN/SIP Intercept Treatment: attendant
      Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred
      Automatic Circuit Assurance (ACA) Enabled? n
```

## 5.3. Administer SIP Trunk Group

Use the “change trunk-group n” command, where “n” is the existing SIP trunk group number used to reach Session Manager, in this case “92”.

For **Group Name**, update as desired to reflect the same trunk group used to reach Session Manager and IPC. For **Number of Members**, enter sufficient number for simultaneous calls to Avaya SIP and IPC users. Note that a call between an Avaya SIP user and an IPC user uses two SIP trunks, whereas a call between an Avaya non-SIP user and an IPC user uses one SIP trunk. Make a note of the **Signaling Group** number.

```
change trunk-group 92                                         Page 1 of 21
      TRUNK GROUP

      Group Number: 92
      Group Name: SM 41 42
      Direction: two-way
      Dial Access? n
      Queue Length: 0
      Service Type: tie

      Group Type: sip
      COR: 1
      Outgoing Display? y
      Auth Code? n

      CDR Reports: n
      TN: 1
      TAC: 1092
      Night Service:

      Member Assignment Method: auto
      Signaling Group: 92
      Number of Members: 10
```

Navigate to **Page 3**, and enter “private” for **Numbering Format**.

|                                  |                                 |
|----------------------------------|---------------------------------|
| change trunk-group 92            | Page 3 of 21                    |
| TRUNK FEATURES                   |                                 |
| ACA Assignment? n                | Measured: none                  |
|                                  | Maintenance Tests? y            |
| Numbering Format: private        |                                 |
|                                  | UUI Treatment: service-provider |
|                                  | Replace Restricted Numbers? n   |
|                                  | Replace Unavailable Numbers? n  |
| Modify Tandem Calling Number: no |                                 |
| Show ANSWERED BY on Display? y   |                                 |
| DSN Term? n                      | SIP ANAT Supported? n           |

Navigate to **Page 4**, and enter “101” for **Telephone Event Payload Type**, as required by IPC.

|   |                        |
|---|------------------------|
| change trunk-group 92   | Page 4 of 21           |
| PROTOCOL VARIATIONS   |                        |
|   | Mark Users as Phone? y |
| Prepend '+' to Calling/Alerting/Diverting/Connected Number? n |                        |
| Send Transferring Party Information? y                        |                        |
| Network Call Redirection? y                                   |                        |
| Build Refer-To URI of REFER From Contact For NCR? n           |                        |
| Send Diversion Header? n                                      |                        |
| Support Request History? y                                    |                        |
| Telephone Event Payload Type: 101                             |                        |
| Convert 180 to 183 for Early Media? n                         |                        |
| Always Use re-INVITE for Display Updates? n                   |                        |
| Identity for Calling Party Display: P-Asserted-Identity       |                        |
| Block Sending Calling Party Location in INVITE? n             |                        |
| Accept Redirect to Blank User Destination? n                  |                        |
| Enable Q-SIP? n   |                        |



## 5.4. Administer SIP Signaling Group

Use the “change signaling-group n” command, where “n” is the existing SIP signaling group number used by the SIP trunk group from **Section 5.3**.

For **DTMF over IP**, enter “rtp-payload”. For **Direct IP-IP Audio Connections**, enter “y”. Make a note of the **Far-end Network Region** number.. Also note the values of **Near-end Listen Port** and **Far-end Listen Port**, which will be used later.

```
change signaling-group 92                                     Page 1 of 2
SIGNALING GROUP
Group Number: 92      Group Type: sip
IMS Enabled? n      Transport Method: tls
Q-SIP? n
IP Video? y      Priority Video? y      Enforce SIPS URI for SRTP? y
Peer Detection Enabled? y      Peer Server: SM
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n

Near-end Node Name: procr      Far-end Node Name: SM-1
Near-end Listen Port: 5061      Far-end Listen Port: 5061
Far-end Network Region: 1
Far-end Secondary Node Name:

Far-end Domain:
Incoming Dialog Loopbacks: eliminate      Bypass If IP Threshold Exceeded? n
DTMF over IP: rtp-payload      RFC 3389 Comfort Noise? n
Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3      IP Audio Hairpinning? n
Enable Layer 3 Test? y      Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n      Alternate Route Timer(sec): 6
```

## 5.5. Administer IP Network Region

Use the “change ip-network-region n” command, where “n” is the existing far-end network region number used by the SIP signaling group from **Section 0**.

For **Name**, update as desired to reflect the same network region used to reach IPC. Enter “yes” for **Intra-region IP-IP Direct Audio** and **Inter-region IP-IP Direct Audio**, as shown below. In the compliance testing, the same network region was used for all Avaya users. Make a note of the **Codec Set** number.

```
change ip-network-region 1                                     Page 1 of 20
IP NETWORK REGION
Region: 1
Location: 1      Authoritative Domain: avaya.com
Name:      Stub Network Region: n
MEDIA PARAMETERS      Intra-region IP-IP Direct Audio: yes
Codec Set: 1      Inter-region IP-IP Direct Audio: yes
UDP Port Min: 16390      IP Audio Hairpinning? n
UDP Port Max: 16999
DIFFSERV/TOS PARAMETERS
Call Control PHB Value: 46
Audio PHB Value: 46
```

```

Video PHB Value: 26
802.1P/Q PARAMETERS
Call Control 802.1p Priority: 6
Audio 802.1p Priority: 6
Video 802.1p Priority: 5
H.323 IP ENDPOINTS
H.323 Link Bounce Recovery? y
Idle Traffic Interval (sec): 20
Keep-Alive Interval (sec): 5
Keep-Alive Count: 5
AUDIO RESOURCE RESERVATION PARAMETERS
RSVP Enabled? n

```

## 5.6. Administer IP Codec Set

Use the “change ip-codec-set n” command, where “n” is the existing codec set number used by the IP network region from **Section 5.5**. Update the audio codec types in the **Audio Codec** fields as necessary.

In the compliance testing, the same codec set was used for all Avaya users.

```

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:
3:
4:
5:
6:
7:

```

## 5.7. Administer Route Pattern

Use the “change route-pattern n” command, where “n” is the existing route pattern number to reach Session Manager, in this case “92”. For **Pattern Name**, update as desired to reflect the same route pattern used to reach Session Manager and IPC.

```

change route-pattern 92
Page 1 of 3

Pattern Number: 92
Pattern Name: no IMS SIP trk
SCCAN? n      Secure SIP? n

Grp FRL NPA Pfx Hop Toll No.  Inserted      DCS/ IXC
No      Mrk Lmt List Del  Digits      QSIG
Dgts      Intw
1: 92    0                                n  user
2:                                n  user
3:                                n  user
4:                                n  user

BCC VALUE  TSC  CA-TSC      ITC BCIE Service/Feature PARM  No.  Numbering LAR
0 1 2 M 4 W      Request      Dgts Format
Subaddress
1: y y y y y n  n      rest      none

```

## 5.8. Administer Private Numbering

Use the “change private-numbering 0” command, to define the calling party number to send to IPC. Add an entry for the trunk group defined in **Section 5.3**. In the example shown below, all calls originating from a 5-digit extension beginning with 720 and routed to trunk group 92 will result in a 5-digit calling number. The calling party number will be in the SIP “From” header.

|                            |          |            |                |           |                        |
|----------------------------|----------|------------|----------------|-----------|------------------------|
| change private-numbering 0 |          |            |                |           | Page 1 of 2            |
| NUMBERING - PRIVATE FORMAT |          |            |                |           |                        |
| Ext Len                    | Ext Code | Trk Grp(s) | Private Prefix | Total Len |                        |
| 5                          | 720      | 92         |                | 5         | Total Administered: 12 |
| 5                          | 720      | 11         |                | 5         | Maximum Entries: 540   |

## 5.9. Administer Uniform Dial Plan

This section provides a sample AAR routing used for routing calls with dialed digits 332xx to IPC. Note that other methods of routing may be used. Use the “change uniform-dialplan 0” command, and add an entry to specify the use of AAR for routing digits 332xx, as shown below.

|                           |     |     |               |          |             |
|---------------------------|-----|-----|---------------|----------|-------------|
| change uniform-dialplan 0 |     |     |               |          | Page 1 of 2 |
| UNIFORM DIAL PLAN TABLE   |     |     |               |          |             |
| Percent Full: 0           |     |     |               |          |             |
| Matching Pattern          | Len | Del | Insert Digits | Net Conv | Node Num    |
| 332                       | 5   | 0   | aar           | n        |             |
| 333                       | 5   | 0   | aar           | n        |             |

## 5.10. Administer AAR Analysis

Use the “change aar analysis 3” command, and add an entry to route calls to 332xx. In the example shown below, calls with digits 332xx will be routed using route pattern “92”. Set the **Call Type** to “unku”, to prevent “+” being added as a prefix.

|                          |           |           |               |           |          |         |             |
|--------------------------|-----------|-----------|---------------|-----------|----------|---------|-------------|
| change aar analysis 3    |           |           |               |           |          |         | Page 1 of 2 |
| AAR DIGIT ANALYSIS TABLE |           |           |               |           |          |         |             |
| Location: all            |           |           |               |           |          |         |             |
| Percent Full: 1          |           |           |               |           |          |         |             |
| Dialed String            | Total Min | Total Max | Route Pattern | Call Type | Node Num | ANI Req |             |
| 332                      | 5         | 5         | 92            | unku      |          | n       |             |
| 333                      | 5         | 5         | 9             | aar       |          | n       |             |

## 5.11. Administer ISDN Trunk Group

Use the “change trunk-group n” command, where “n” is the existing ISDN trunk group number used to reach the PSTN, in this case “80”. Navigate to **Page 3**.

For **Modify Tandem Calling Number**, enter “tandem-cpn-form” to allow for the calling party number from IPC to be modified. By enabling this feature, the calling party number will be sent to PSTN when call is coming from IPC side via a SIP trunk.

|   |  |  |                                |      |    |
|---|--|--|--------------------------------|------|----|
| change trunk-group 80                   |  |  | Page                           | 3 of | 21 |
| TRUNK FEATURES                          |  |  |                                |      |    |
| ACA Assignment? n                       |  | Measured: none                                     | Wideband Support? n            |      |    |
|   |  | Internal Alert? n                                  | Maintenance Tests? y           |      |    |
|   |  | Data Restriction? n                                | NCA-TSC Trunk Member:          |      |    |
|   |  | Send Name: y                                       | Send Calling Number: y         |      |    |
| Used for DCS? n                         |  |  | Send EMU Visitor CPN? y        |      |    |
| Suppress # Outpulsing? n                |  | Format: private                                    |                                |      |    |
| Outgoing Channel ID Encoding: preferred |  | UII IE Treatment: service-provider                 |                                |      |    |
|   |  |  | Replace Restricted Numbers? n  |      |    |
|   |  |  | Replace Unavailable Numbers? n |      |    |
|   |  |  | Send Connected Number: y       |      |    |
| Network Call Redirection: none          |  |  | Hold/Unhold Notifications? n   |      |    |
| Send UII IE? y                          |  | Modify Tandem Calling Number: tandem-cpn-form      |                                |      |    |
| Send UCID? n                            |  |  |                                |      |    |
| Send Codeset 6/7 LAI IE? y              |  | Dsl Echo Cancellation? n                           |                                |      |    |
| Apply Local Ringback? n                 |  | US NI Delayed Calling Name Update? n               |                                |      |    |
| Show ANSWERED BY on Display? y          |  | Invoke ID for USNI Calling Name: variable          |                                |      |    |
|   |  | Network (Japan) Needs Connect Before Disconnect? n |                                |      |    |
| DSN Term? n                             |  |  |                                |      |    |

## 5.12. Administer Tandem Calling Party Number

Use the “change tandem-calling-party-num” command, to define the calling party number to send to the PSTN for tandem calls from IPC turret users.

In the example shown below, all calls originating from a 5-digit extension beginning with 3 and routed to trunk group 80 will result in a 10-digit calling number. For **Number Format**, use an applicable format, in this case “pub-unk”.

|                                 |                |          |          |                |          |
|---------------------------------|----------------|----------|----------|----------------|----------|
| change tandem-calling-party-num |                |          | Page     | 1 of           | 8        |
| CALLING PARTY NUMBER CONVERSION |                |          |          |                |          |
| FOR TANDEM CALLS                |                |          |          |                |          |
|                                 |                | Incoming | Outgoing | Natl           | Outgoing |
| Any                             | Any CPN        | Number   | Trunk    | Intl           | Number   |
| Len                             | Len CPN Prefix | Format   | Group(s) | Del Pfx Insert | Format   |
| 5                               | 33             |          | 80       | 5 7209772879   | pub-unk  |

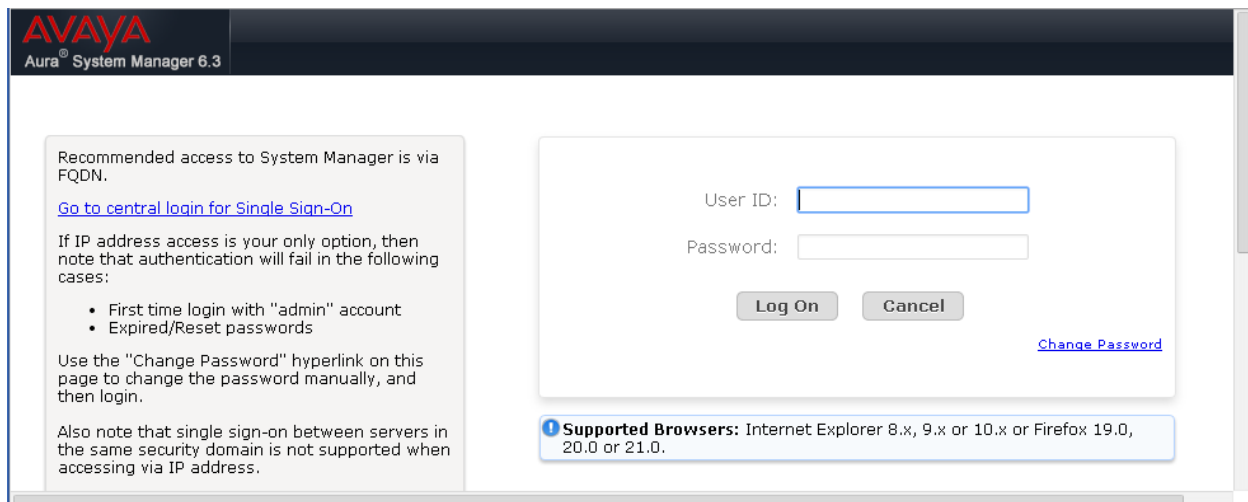
## 6. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Avaya Aura® Session Manager. The procedures include the following areas:

- Launch System Manager
- Administer locations
- Administer adaptations
- Administer SIP entities
- Administer entity links
- Administer routing policies
- Administer dial patterns

### 6.1. Launch System Manager

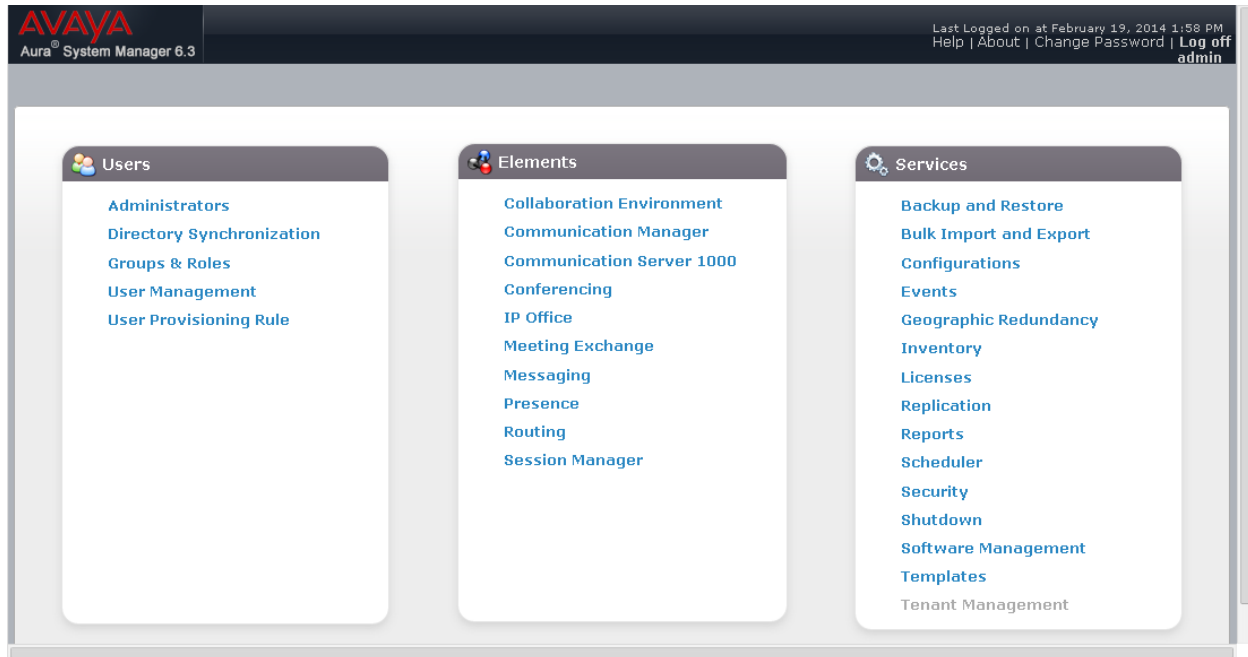
Access the System Manager web interface by using the URL “https://ip-address” in an Internet browser window, where “ip-address” is the IP address of the System Manager server. Log in using the appropriate credentials.



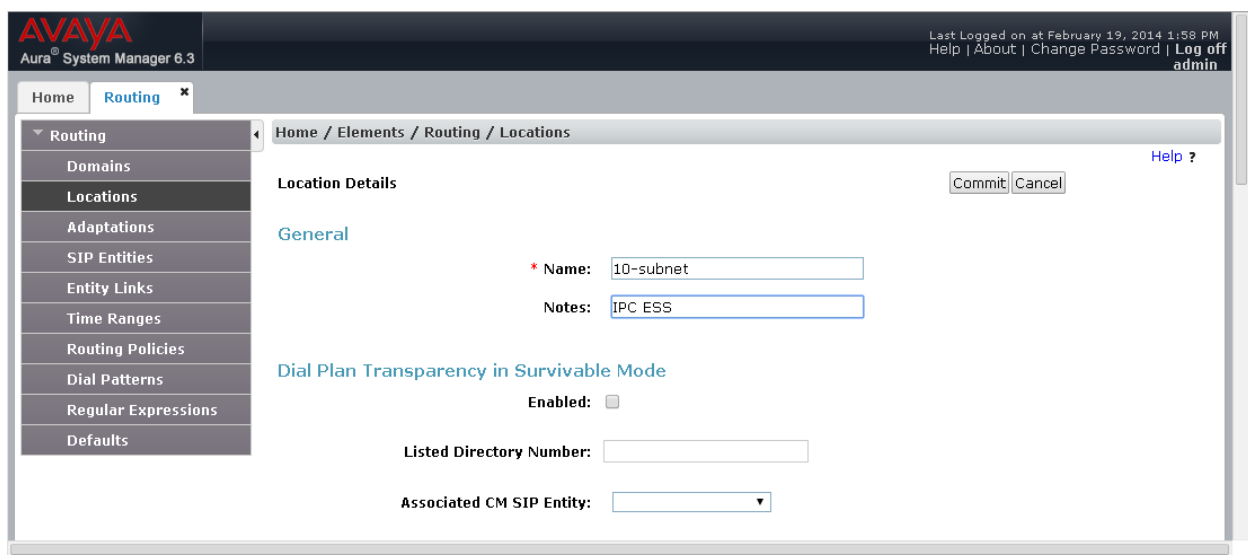
The screenshot shows the Avaya Aura System Manager 6.3 login interface. The header features the Avaya logo and the text "Aura® System Manager 6.3". The main content area is divided into two sections. On the left, a grey box contains instructions: "Recommended access to System Manager is via FQDN." followed by a link "Go to central login for Single Sign-On". Below this, it states "If IP address access is your only option, then note that authentication will fail in the following cases:" and lists two bullet points: "First time login with 'admin' account" and "Expired/Reset passwords". It then advises to use the "Change Password" hyperlink to change the password manually. At the bottom of this box, it notes that single sign-on between servers in the same security domain is not supported when accessing via IP address. On the right, a white box contains the login form with fields for "User ID:" and "Password:", "Log On" and "Cancel" buttons, and a "Change Password" link. At the bottom of the page, a blue box lists "Supported Browsers: Internet Explorer 8.x, 9.x or 10.x or Firefox 19.0, 20.0 or 21.0."

## 6.2. Administer Locations

In the subsequent screen, select **Elements** → **Routing**. Select **Routing** → **Locations** from the left pane, and click **New** in the subsequent screen (not shown) to add a new location for IPC.



The **Location Details** screen is displayed. In the **General** sub-section, enter a descriptive **Name** and optional **Notes**. In the **Location Pattern** sub-section (not shown), click **Add** and enter the applicable **IP Address Pattern**. Retain the default values in the remaining fields.



### 6.3. Administer Adaptations

Select **Routing** → **Adaptations** from the left pane, and click **New** in the subsequent screen (not shown) to add a new adaptation for IPC.

The **Adaptation Details** screen is displayed. In the **General** sub-section, enter a descriptive **Adaptation name**. For **Module name**, select “DigitConversionAdapter”. For Module Parameter Type, select “Name-Value Parameter”.

For **Name-Value Parameter**, enter “iodstd” for Name and “avaya.com” for Value. On the second line, enter “odstd” for Name and “ipc.com” for Value. “avaya.com” is the Avaya side domain, and “ipc.com” is IPC side domain. This will set the source and destination domains for all incoming and outgoing calls for IPC.

AVAYA  
Aura® System Manager 6.3

Last Logged on at February 19, 2014 1:58 PM  
Help | About | Change Password | Log off  
admin

Home Routing

Home / Elements / Routing / Adaptations

Adaptation Details

Commit Cancel

General

\* Adaptation Name: IPC Domain Conversion

Module Name: DigitConversionAdapter

Module Parameter Type: Name-Value Parameter

Add Remove

|                          | Name   | Value     |
|--------------------------|--------|-----------|
| <input type="checkbox"/> | iodstd | avaya.com |
| <input type="checkbox"/> | odstd  | ipc.com   |

Select : All, None

## 6.4. Administer SIP Entities

Select **Routing** → **SIP Entities** from the left pane, and click **New** in the subsequent screen (not shown) to add a new SIP entity for IPC.

The **SIP Entity Details** screen is displayed. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **FQDN or IP Address:** The IP address of the IPC ESS server.
- **Type:** “Other”
- **Adaptation:** Select the IPC adaptation name from **Section 6.3**.
- **Time Zone:** Select the applicable time zone.

AVAYA  
Aura® System Manager 6.3

Last Logged on at February 19, 2014 1:58 PM  
Help | About | Change Password | Log off admin

Home Routing

Home / Elements / Routing / SIP Entities

SIP Entity Details

General

\* Name: IPC Alliance 15.3

\* FQDN or IP Address: 10.64.10.114

Type: Other

Notes: ESS on Alliance system

Adaptation: IPC Domain Conversion

Location:

Time Zone: America/Denver

\* SIP Timer B/F (in seconds): 4

Credential name:

Call Detail Recording: both

CommProfile Type Preference:

Loop Detection

Loop Detection Mode: Off

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration



## 6.5. Administer Entity Links

Select **Routing** → **Entity Links** from the left pane, and click **New** in the subsequent screen (not shown) to add a new entity link for IPC.

The **Entity Links** screen is displayed. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **SIP Entity 1:** The Session Manager entity name.
- **Protocol:** The signaling group transport method.
- **Port:** The signaling group listen port number.
- **SIP Entity 2:** The IPC entity name from **Section 6.4**.
- **Port:** The signaling group listen port number.

AVAYA  
Aura® System Manager 6.3

Last Logged on at February 19, 2014 1:58 PM  
Help | About | Change Password | Log off admin

Home Routing

Routing  
Domains  
Locations  
Adaptations  
SIP Entities  
Entity Links  
Time Ranges  
Routing Policies  
Dial Patterns  
Regular Expressions  
Defaults

Home / Elements / Routing / Entity Links

Entity Links

Commit Cancel

1 Item Filter: Enable

| <input type="checkbox"/> | Name                  | SIP Entity 1 | Protocol | Port   | SIP Entity 2        | DNS Override             | Port   | Connection Policy |
|--------------------------|-----------------------|--------------|----------|--------|---------------------|--------------------------|--------|-------------------|
| <input type="checkbox"/> | * SM63_IPC Alliance 1 | * SM63       | TCP      | * 5060 | * IPC Alliance 15.3 | <input type="checkbox"/> | * 5060 | trusted           |

Select : All, None

Commit Cancel

## 6.6. Administer Routing Policies

Select **Routing** → **Routing Policies** from the left pane, and click **New** in the subsequent screen (not shown) to add a new routing policy for IPC.

The **Routing Policy Details** screen is displayed. In the **General** sub-section, enter a descriptive **Name**.

In the **SIP Entity as Destination** sub-section, click **Select** and select the IPC entity name from **Section 6.4** in the listing (not shown).

Retain the default values in the remaining fields.

AVAYA  
Aura® System Manager 6.3

Last Logged on at February 19, 2014 1:58 PM  
Help | About | Change Password | Log off admin

Home Routing

Home / Elements / Routing / Routing Policies

Routing Policy Details

Commit Cancel

General

\* Name: Route2Alliance153

Disabled: ☐

\* Retries: 0

Notes:

SIP Entity as Destination

Select

| Name              | FQDN or IP Address | Type  | Notes                          |
|-------------------|--------------------|-------|--------------------------------|
| IPC Alliance 15.3 | 10.64.10.114       | Other | This is ESS on Alliance system |

Time of Day

Add Remove View Gaps/Overlaps

1 Item Filter: Enable

| Ranking | Name | Mon                                 | Tue                                 | Wed                                 | Thu                                 | Fri                                 | Sat                                 | Sun                                 | Start Time | End Time | Notes |
|---------|------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|------------|----------|-------|
| 0       | 24/7 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | 00:00      | 23:59    |       |

Select : All, None

## 6.7. Administer Dial Patterns

Select **Routing** → **Dial Patterns** from the left pane, and click **New** in the subsequent screen (not shown) to add a new dial pattern to reach IPC turret users.

The **Dial Pattern Details** screen is displayed. In the **General** sub-section, enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Pattern:** Enter a dial pattern to match.
- **Min:** The minimum number of digits to be matched.
- **Max:** The maximum number of digits to be matched.
- **SIP Domain:** During the compliance test, “all” was selected for the sip domain.
- **Notes:** Any desired description.

In the **Originating Locations and Routing Policies** sub-section, click **Add** and create a new policy for reaching IPC turret users. In the compliance testing, the policy allowed for call origination from all locations, as shown below. Retain the default values in the remaining fields.

**AVAYA**  
Aura® System Manager 6.3

Last Logged on at February 19, 2014 1:58 PM  
Help | About | Change Password | Log off admin

Home Routing

Home / Elements / Routing / Dial Patterns

**Dial Pattern Details** [Commit] [Cancel] [Help ?]

**General**

\* Pattern: 332

\* Min: 5

\* Max: 5

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: -ALL-

Notes: Alliance via SI

**Originating Locations and Routing Policies**

[Add] [Remove]

1 Item [Filter: Enable]

| <input type="checkbox"/> | Originating Location Name | Originating Location Notes | Routing Policy Name | Rank | Routing Policy Disabled  | Routing Policy Destination | Routing Policy Notes |
|--------------------------|---------------------------|----------------------------|---------------------|------|--------------------------|----------------------------|----------------------|
| <input type="checkbox"/> | -ALL-                     |                            | Route2Alliance153   |      | <input type="checkbox"/> | IPC Alliance 15.3          |                      |

Select : All, None

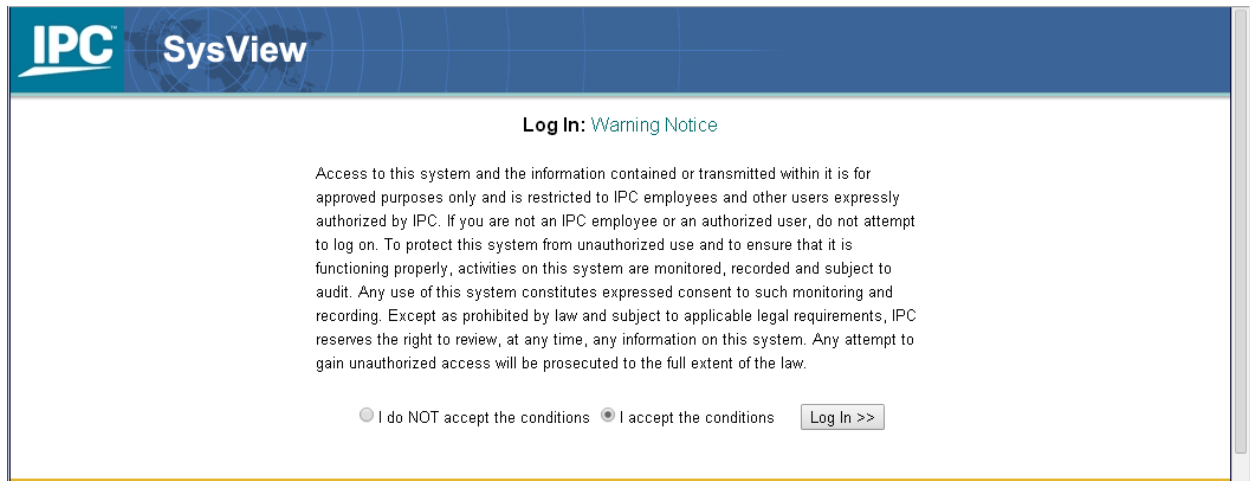
## 7. Configure IPC Alliance 15.03

This section provides the procedures for configuring IPC Alliance 15.03. The procedures include the following areas:

- Configure Route Plan
- Configure SIP Proxy
- Administer Trusted Host
- Configure SIP Trunk

### 7.1. Configure Route Plan

Access the **IPC System Center** web interface by using the URL <https://ip-address/webadmin> in an Internet browser window, where “ip-address” is the IP address of the System Center. Select “I accept the condition”, and Log in using the appropriate credentials.



The screenshot shows the IPC SysView login interface. At the top, there is a blue header with the 'IPC' logo and 'SysView' text. Below the header, the page is titled 'Log In: Warning Notice'. A paragraph of text explains the system's security and usage policies. At the bottom, there are two radio buttons for accepting or declining the conditions, and a 'Log In >>' button.

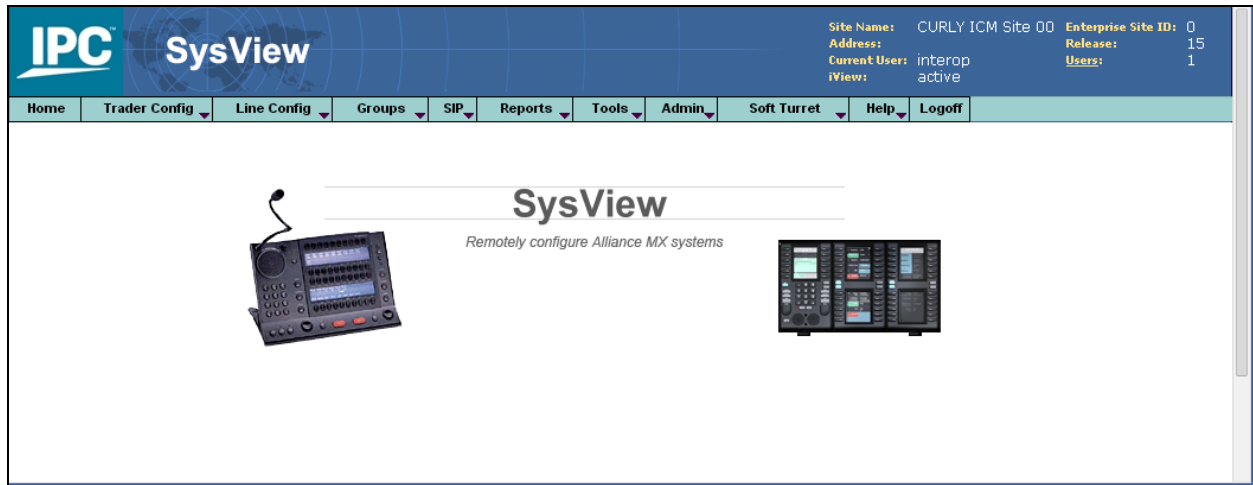
**IPC SysView**

**Log In: Warning Notice**

Access to this system and the information contained or transmitted within it is for approved purposes only and is restricted to IPC employees and other users expressly authorized by IPC. If you are not an IPC employee or an authorized user, do not attempt to log on. To protect this system from unauthorized use and to ensure that it is functioning properly, activities on this system are monitored, recorded and subject to audit. Any use of this system constitutes expressed consent to such monitoring and recording. Except as prohibited by law and subject to applicable legal requirements, IPC reserves the right to review, at any time, any information on this system. Any attempt to gain unauthorized access will be prosecuted to the full extent of the law.

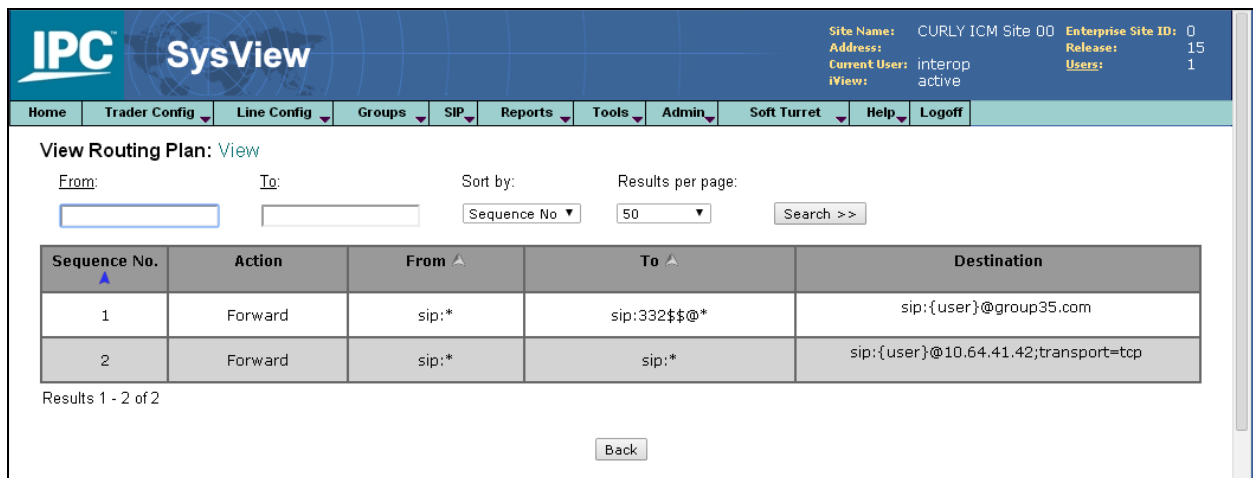
☐ I do NOT accept the conditions ☒ I accept the conditions

On the **SysView** page, navigate to **SIP → Routing Plan → View Routing Plan** to view what is used during the compliance test.



The entry with **Sequence Number 1** was used for routing of inbound calls to IPC. Note that the Destination URL contains the internal default value for the SIP trunk card, in this case “group35.com”. The entry with **Sequence Number 2** was used for routing of outbound calls to Session Manager.

To create a new routing plan, redirect the path to **SIP → Routing Plan → Add Routing Plan**.



## 7.2. Configure SIP Proxy

On the SysView page, navigate to **SIP → SIP Server → Configuration** to create a new server configuration. Enter a domain that will be used on the IPC side. Provide SIP ports for TCP/UDP and TLS. During the test TCP was used.

The screenshot shows the IPC SysView interface. The top navigation bar includes links for Home, Trader Config, Line Config, Groups, SIP, Reports, Tools, Admin, Soft Turret, Help, and Logoff. The right side of the header displays system information: Site Name (CURLY ICM Site 00), Address, Current User (interop), iView (active), Enterprise Site ID (0), Release (15), and Users (1). The main content area is titled 'Edit Configuration: Enter Details' and features a 'Proxy Server' configuration form. This form includes sections for Domains List (with a text input containing 'ipc.com'), SIP Ports (with TCP/UDP Port set to 5060 and TLS Port set to 5061), Security Parameters (with Domain and Realm both set to 'sip:ipc.com' and 'ipc.com' respectively), TLS Certificate (with Certificate File and Trusted CA File paths), and License Server (with IP or FQDN set to '10.64.10.110').

| Proxy Server                    |  |
|---------------------------------|--|
| Domains List:                   | <input type="text" value="ipc.com"/>   |
|                                 |  |
|                                 |  |
|                                 |  |
|                                 |  |
| SIP Ports:                      | TCP/UDP Port: <input type="text" value="5060"/>  |
|                                 | TLS Port: <input type="text" value="5061"/>  |
| Security Parameters:            | Domain: <input type="text" value="sip:ipc.com"/>   |
|                                 | Realm: <input type="text" value="ipc.com"/>  |
| TLS Certificate:                | Certificate File: <input type="text" value="/usr/local/SipProxy/config/localhost.key-cert.pem"/> |
|                                 | Trusted CA File: <input type="text" value="/usr/local/SipProxy/config/SipStackCACert.pem"/>      |
| License Server:<br>(IP or FQDN) | <input type="text" value="10.64.10.110"/>  |

### 7.3. Administer Trusted Host

From the Linux shell of the ESS server, navigate to the `/usr/local/SipProxy/` directory, and issue the command shown below with the “-add” option to add Session Manager as a trusted host. Note that 10.64.41.42 is the IP address of the signaling interface for Session Manager.

```
[ipadmin@esshost ~]$ cd /usr/local/SipProxy
[ipadmin@esshost SipProxy]$ ./trusted_hosts.pl -add=10.64.41.42
```

The same command can be used with the “-view” option to make certain Session Manager is displayed as a trusted host.

```
[ipadmin@esshost ~]$ cd /usr/local/SipProxy
[ipadmin@esshost SipProxy]$ ./trusted_hosts.pl -view
ip_address      last_modified
10.64.41.42     2014-01-23 16:05:53
```

### 7.4. Configure SIP Trunk

On the **SysView** page, navigate to **SIP → SIP Trunk Parameters** and select the “Edit SIP Config” button.

The screenshot shows the SysView interface with the 'Edit SIP Config' page selected. The page has a navigation bar with 'Home', 'Trader Config', 'Line Config', 'Groups', 'SIP', 'Reports', 'Tools', 'Admin', 'Soft Turret', 'Help', and 'Logoff'. The 'SIP' menu is expanded, showing 'Edit SIP Config' and 'Enter Details'. The main content area has two sections: '1. Enter Search Criteria' with a 'DDI Groups' dropdown set to '-- All --', and '2. Choose Display Format' with 'Sort by: DDI Group ID' and 'Display 50 results per page'. At the bottom are 'Back', 'Reset', and 'Edit SIP Config >>' buttons.

On the **Select SIP Config to Edit** page, select the relevant SIP “DDI Group ID”, in this case “35” and click on the “Edit Selected” button.

The screenshot shows the SysView interface with the 'Select SIP Config to Edit' page selected. The page has a navigation bar with 'Home', 'Trader Config', 'Line Config', 'Groups', 'SIP', 'Reports', 'Tools', 'Admin', 'Soft Turret', 'Help', and 'Logoff'. The 'SIP' menu is expanded, showing 'Select SIP Config to Edit' and 'Change Search'. The main content area shows 'Search Results for: --All--' and 'Results 1 - 1 of 1'. A table displays the results:

| Select                | DDI Group ID | Outbound URI | Transport Type | User Name |
|-----------------------|--------------|--------------|----------------|-----------|
| <input type="radio"/> | 35           | avaya.com    | TCP            | ipc       |

At the bottom are 'Back' and 'Edit Selected >>' buttons.

On the **Edit SIP Config Details** page, provide Outbound URI.

IPC SysView

Site Name: CURLY ICM Site 00 Enterprise Site ID: 0  
Address: Release: 15  
Current User: interop Users: 1  
iView: active

Home Trader Config Line Config Groups SIP Reports Tools Admin Soft Turret Help Logoff

**Edit SIP Config: Edit SIP Config Details**

[Back to Search Results](#)

Advanced...

**1. Enter Details**

DDI Group ID: 35

Outbound URI: avaya.com

User Name: ipc

Password: ...

Confirm Password: ...

Back Reset Save Edits >>

## 8. Configure IPC Alliance MX

This section provides the procedures for configuring IPC Alliance MX. The procedures include the following areas:

- Launch Iview
- Administer wire groups

The configuration of Alliance MX is typically performed by IPC installation technicians. The procedural steps are presented in these Application Notes for informational purposes.

### 8.1. Launch Iview

From the Alliance MX console (or System Center console), right-click and select **Windows** → **Command Tool** from the pop-up boxes.

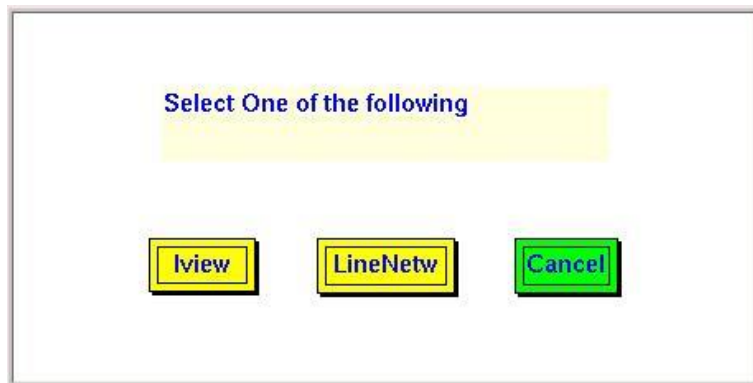




The **cmdtool** screen is displayed. Enter “iview &”, as shown below.

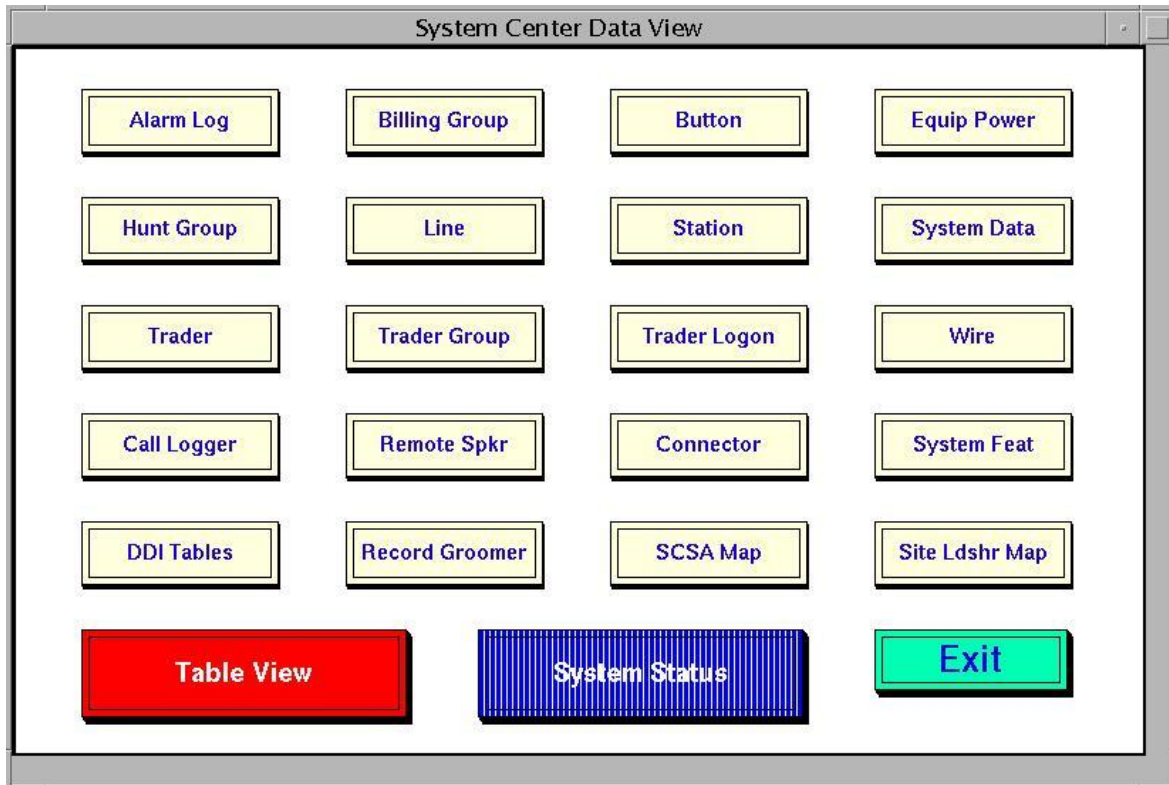


In the pop-up box shown below, click **Iview**.

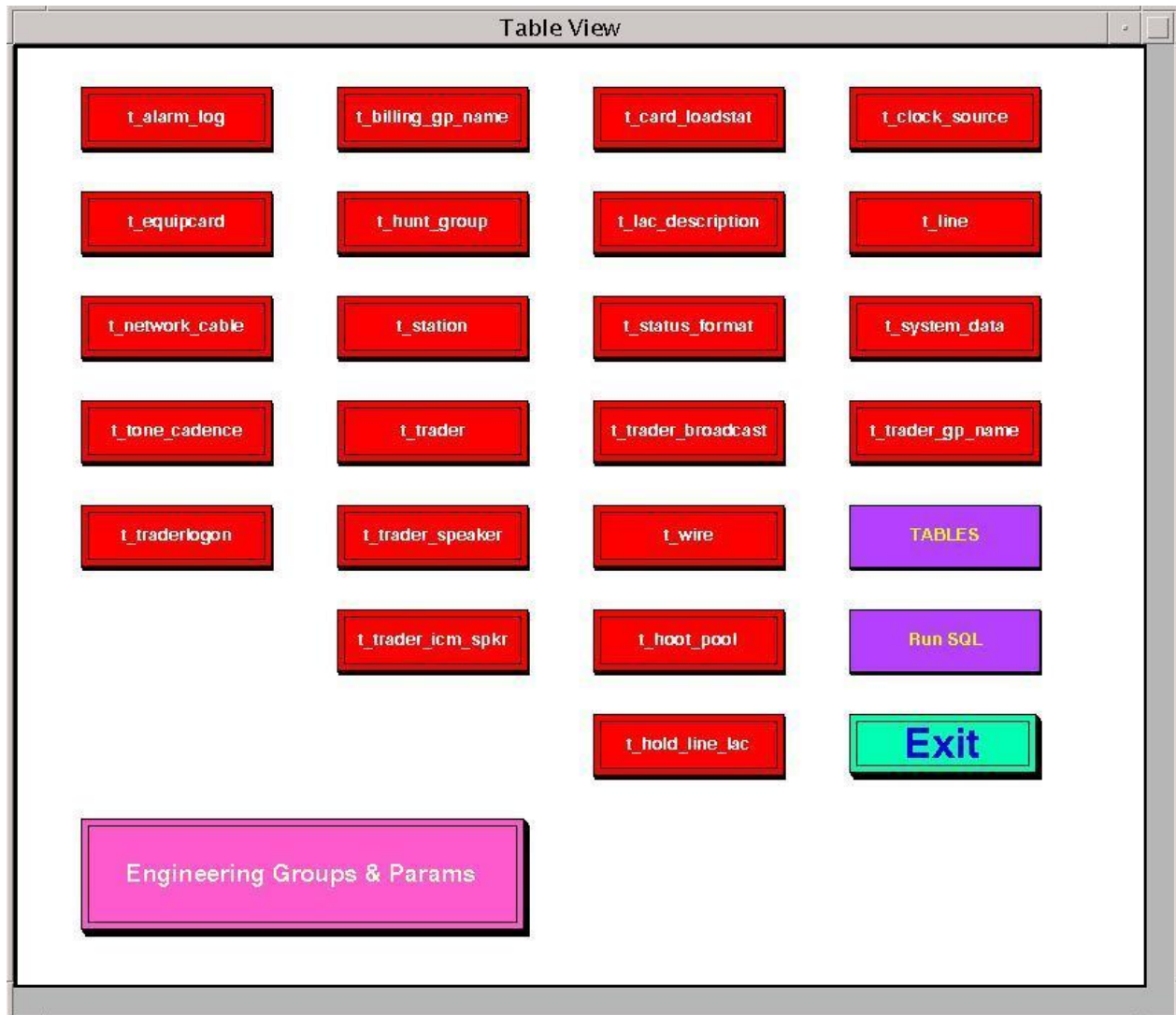


## 8.2. Administer Wire Groups

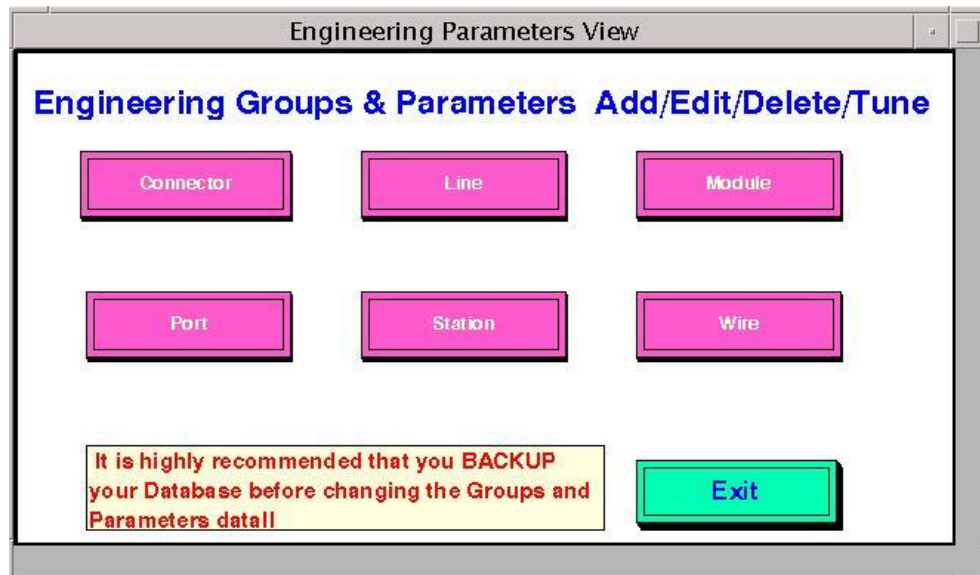
The **System Center Data View** screen is displayed. Click **Table View**.



The **Table View** screen is displayed. Click **Engineering Groups & Params**.



The **Engineering Parameters View** screen is displayed next. Click **Wire**.



The **Wire Groups & Parameters Menu** screen is displayed. In the **Wire Groups** sub-section, scroll down and select “SIP”. Click **Edit**.



The **p\_Wire Edit Group** screen is displayed next. Scroll down the screen as necessary to locate the entry with **Param ID** of “365”. Click on the corresponding **New Param Value** field, and enter “2” to denote Avaya as the PBX provider. Locate the entry with **Param ID** of “370”. Click on the corresponding **New Param Value** field, and enter “4” to enable Forward Switching. Scroll down the screen as necessary to locate the entry with **Param ID** of “661”. Click on the corresponding **New Param Value** field, and enter “1” to activate detection for G729. Locate the entry with **Param ID** of “666”. Click on the corresponding **New Param Value** field, and enter “1” to enable SIP Provisional Acknowledgement (PRACK). Locate the entry with **Param ID** of “668”. Click on the corresponding **New Param Value** field, and enter “0” to disable SIP Remote Party ID (RPI).

After the configuration changes, reboot the SIP trunk card or perform a system load

|     | D           | E         | F         | G                | H                                       | I          | J        | K        | L |
|-----|-------------|-----------|-----------|------------------|---|------------|----------|----------|---|
| 1   | Param Value | Param Min | Param Max | Param Name       | Param Description                       | Param Type | Param Id | Group Id |   |
| 71  | 47          | 0         | 32767     | DSP_VTHRESH_LVL8 | Volume Threshold Level 8                | number     | 137      | 27       |   |
| 72  | 16423       | 1         | 32767     | DSP_VBALANCE     | DSP Volume Balance                      | number     | 138      | 27       |   |
| 73  | 32767       | 1         | 32767     | DSP_TERM_ATTEN   | DSP TERM threshold                      | number     | 141      | 27       |   |
| 74  | 0           | -5        | 5         | TERM_SHIFT       | gain/loss into ipc network              | number     | 362      | 27       |   |
| 75  | 0           | -5        | 5         | PERIPH_SHIFT     | gain/loss into public network           | number     | 363      | 27       |   |
| 76  | 6           | 0         | 32        | INTERDIGIT_TO    | interdigit timeout for enbloc signaling | number     | 364      | 27       |   |
| 77  | 2           | 1         | 7         | PBX_PROVIDER     | 7/DEF,AVYA,NRTL,ERISN,MITL,SMNS,CS21    | enum       | 365      | 27       |   |
| 78  | 6           | 1         | 15        | MAX_DIVERTS      | Max Number of Diverts per Call          | number     | 369      | 27       |   |
| 79  | 4           | 0         | 4         | FS_ENABLE        | 0-4/Off, Imm&Busy, RNA, All, Always FS  | number     | 370      | 27       |   |
| 80  | 200         | 200       | 10000     | FS_DELAY         | Time(msec) to Wait B4 Forward Switching | number     | 371      | 27       |   |
| 81  | 1           | 1         | 5         | LN_RECORDS       | 1-5/NONE,MX_PBX,MWI,DISC,All            | number     | 375      | 27       |   |
| 82  | 16          | -32767    | 32767     | VPKT_CONTROL     | Voice Pkt Control                       | number     | 642      | 27       |   |
| 83  | 10          | -32767    | 32767     | VPKT_PERIOD      | Voice Pkt Period in samples             | number     | 643      | 27       |   |
| 84  | 12825       | -32767    | 32767     | VPKT_JITTERDEPTH | Voice Pkt Jitter Depth in samples       | number     | 644      | 27       |   |
| 85  | 0           | -32767    | 32767     | VPKT_JITTERCTRL  | Voice Pkt Jitter Control                | number     | 645      | 27       |   |
| 86  | 0           | -32767    | 32767     | VPKT_SPARE1      | Voice Pkt spare1                        | number     | 646      | 27       |   |
| 87  | 1400        | 0         | 3000      | INTRUSION_FREQ   | Intrusion frequency, Hz                 | number     | 647      | 27       |   |
| 88  | 350         | 0         | 3000      | DIALTONELO_FREQ  | Dialtone LO frequency, Hz               | number     | 648      | 27       |   |
| 89  | 440         | 0         | 3000      | DIALTONEHI_FREQ  | Dialtone HI frequency, Hz               | number     | 649      | 27       |   |
| 90  | 480         | 0         | 3000      | BUSYTONELO_FREQ  | Busytone LO frequency, Hz               | number     | 650      | 27       |   |
| 91  | 620         | 0         | 3000      | BUSYTONEHI_FREQ  | Busytone HI frequency, Hz               | number     | 651      | 27       |   |
| 92  | 440         | 0         | 3000      | RINGBACKLO_FREQ  | Ringback LO frequency, Hz               | number     | 652      | 27       |   |
| 93  | 480         | 0         | 3000      | RINGBACKHI_FREQ  | Ringback HI frequency, Hz               | number     | 653      | 27       |   |
| 94  | 480         | 0         | 3000      | ERRTONELO_FREQ   | Error tone LO frequency, Hz             | number     | 654      | 27       |   |
| 95  | 620         | 0         | 3000      | ERRTONEHI_FREQ   | Error tone HI frequency, Hz             | number     | 655      | 27       |   |
| 96  | 1209        | 0         | 3000      | SPLSHTONELO_FREQ | Splash tone LO frequency, Hz            | number     | 656      | 27       |   |
| 97  | 1477        | 0         | 3000      | SPLSHTONEHI_FREQ | Splash tone HI frequency, Hz            | number     | 657      | 27       |   |
| 98  | 1400        | 0         | 3000      | RECWARNTONE_FREQ | Record warning frequency, Hz            | number     | 658      | 27       |   |
| 99  | 0           | 0         | 10000     | MRD_Ringback_Ton | Ringback Tone Duration (msec)           | number     | 659      | 27       |   |
| 100 | 1           | 0         | 1         | VAD              | Voice Activity Detection                | number     | 661      | 27       |   |
| 101 | 0           | 0         | 1         | MWI_Subscribe    | Send MWI Subscribe, Off = 0, On = 1     | number     | 663      | 27       |   |
| 102 | 0           | 0         | 1         | SIP_Divert       | HistoryInfo = 0, CCDiversion = 1        | number     | 664      | 27       |   |
| 103 | 1           | 0         | 1         | SIP_PRACK        | Enable SIP Provisional ACK              | number     | 666      | 27       |   |
| 104 | 1           | 0         | 1         | SIP_PA1          | Enable SIP P-Asserted Identity          | number     | 667      | 27       |   |
| 105 | 0           | 0         | 1         | SIP_RPID         | Enable SIP Remote Party ID              | number     | 668      | 27       |   |
| 106 | 0           | 0         | 1         | AEC_Enable       | Enable AEC Control Filter               | number     | 669      | 27       |   |
| 107 | 0           | -3        | 3         | AEC_Control      | AEC Aggression level                    | number     | 670      | 27       |   |
| 108 | 0           | 0         | 1         | AEC_NR_Filter    | Enable AEC Noise Reduction              | number     | 671      | 27       |   |

## 9. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Avaya Aura® Session Manager and IPC Alliance MX.

### 9.1. Verify Avaya Aura® Session Manager

From the System Manager home page (not shown), select **Session Manager** → **System Status** → **SIP Entity Monitoring** from the left pane to display the **SIP Entity Link Monitoring Status Summary** screen. Double click on the IPC entity name from **Section 6.4**.

Session Manager Administration

Communication Profile Editor

Network Configuration

Device and Location Configuration

Application Configuration

System Status

SIP Entity Monitoring

Managed Bandwidth Usage

Security Module Status

SIP Firewall Status

Registration Summary

User Registrations

Session Counts

System Tools

Performance

### SIP Entity Link Monitoring Status Summary

This page provides a summary of Session Manager SIP entity link monitoring status.

#### SIP Entities Status for All Monitoring Session Manager Instances

Run Monitor

1 Items | Refresh Filter: Enable

| <input type="checkbox"/> | Session Manager      | Type | Monitored Entities |              |    |               |      |       |
|--------------------------|----------------------|------|--------------------|--------------|----|---------------|------|-------|
|                          |                      |      | Down               | Partially Up | Up | Not Monitored | Deny | Total |
| <input type="checkbox"/> | <a href="#">SM63</a> | Core | 2                  | 0            | 7  | 0             | 2    | 11    |
| <input type="checkbox"/> |                      |      |                    |              |    |               |      |       |
| <input type="checkbox"/> |                      |      |                    |              |    |               |      |       |
| <input type="checkbox"/> |                      |      |                    |              |    |               |      |       |
| <input type="checkbox"/> |                      |      |                    |              |    |               |      |       |

Select: All, None

#### All Monitored SIP Entities

Run Monitor

11 Items | Refresh Filter: Enable

| <input type="checkbox"/> | SIP Entity Name                   |
|--------------------------|-----------------------------------|
| <input type="checkbox"/> | <a href="#">IPC Uniqy V1</a>      |
| <input type="checkbox"/> | <a href="#">IPC Uniqy V2</a>      |
| <input type="checkbox"/> | <a href="#">S8300D-G430-601</a>   |
| <input type="checkbox"/> | <a href="#">S8720-G650-521</a>    |
| <input type="checkbox"/> | <a href="#">ModularMessaging</a>  |
| <input type="checkbox"/> | <a href="#">IPC Alliance 15.3</a> |

The **SIP Entity, Entity Link Connection Status** screen is displayed. Verify that **Conn. Status** and **Link Status** are “Up”, as shown below.

Aura® System Manager 6.3

Last Logged on at February 27, 2014 11:28 AM  
[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

[Home](#)
[Session Manager](#)

Session Manager
Dashboard
Session Manager Administration
Communication Profile Editor
Network Configuration
Device and Location Configuration
Application Configuration
System Status
SIP Entity Monitoring
Managed Bandwidth Usage
Security Module Status
SIP Firewall Status
Registration Summary
User Registrations
Session Counts
System Tools
Performance

Home / Elements / Session Manager / System Status / SIP Entity Monitoring

## SIP Entity, Entity Link Connection Status

This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.

**All Entity Links to SIP Entity: IPC Alliance 15.3**

Status Details for the selected Session Manager:

Summary View

| 2 Items                                    | Refresh                | Filter: Enable |        |       |              |  |             |
|--|------------------------|----------------|--------|-------|--------------|--|-------------|
| Session Manager                            | SIP Entity Resolved IP | Port           | Proto. | Deny  | Conn. Status | Reason Code                              | Link Status |
| <input type="radio"/> <a href="#">SM63</a> | 10.64.10.114           | 5060           | UDP    | FALSE | UP           | 200 Options received from a non-SIPX UAC | UP          |
| <input type="radio"/> <a href="#">SM63</a> | 10.64.10.114           | 5060           | TCP    | FALSE | UP           | 200 Options received from a non-SIPX UAC | UP          |
|  |                        |                |        |       |              |  |             |



## 9.2. Verify IPC Alliance 15.03

From the SysView web interface, select **SIP → Update ESS with SIP Trunk Info → View SIP Cards Group**. Verify that there is an entry that corresponds to SIP card number. Verify that the **Status** is “Online”, as shown below.

The screenshot shows the IPC SysView web interface. The top navigation bar includes links for Home, Trader Config, Line Config, Groups, SIP, Reports, Tools, Admin, Soft Turret, Help, and Logoff. The right side of the header displays system information: Site Name (CURLY ICM Site 00), Address, Current User (interop), iView (active), Enterprise Site ID (0), Release (15), and Users (1). The main content area is titled 'View SIP Card Groups: View'. It features search filters for IP Address and Domain Name, a 'Sort by' dropdown (set to IP), and a 'Results per page' dropdown (set to 50). A 'Search >>' button is present. Below the filters is a table with the following data:

| IP           | Domain      | Status |
|--------------|-------------|--------|
| 10.64.10.116 | group35.com | Online |

Below the table, it indicates 'Results 1 - 1 of 1'. At the bottom of the results area are 'Back' and 'Refresh' buttons.

## 10. Conclusion

These Application Notes describe the configuration steps required for IPC Alliance MX 15.03 to successfully interoperate with Avaya Aura® Session Manager 6.3 using SIP trunks. All feature and serviceability test cases were completed.

## 11. Additional References

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

- [1] *Administering Avaya Aura® Communication Manager*, Release 6.3, October 2013, Issue 9, Document Number 03-300509
- [2] *Administering Avaya Aura® Session Manager*, Release 6.3, October 2013, Issue 3, Document Number 03-603324
- [3] *Administering Avaya Aura® System Manager*, Release 6.3, October 2013, Issue 3

The following document was provided by IPC

- [4] *IPC PATCH 15.03.00.06g Install Guide*, Revision Number 7, April 2011, available upon request to IPC Support.
- [5] *Nexus Suite 2.0 SP1 Patch11 or Higher Deployment Guide*, Part Number B02200161, Revision Number 01, available upon request to IPC Support.

---

**©2014 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](mailto:devconnect@avaya.com).