Avaya Solution & Interoperability Test Lab

Application Notes for TAS ARUTEL Alarm System with Avaya Communication Manager Avaya SIP Enablement Services – Issue 1.0

Abstract

These Application Notes describe the conformance testing of the TAS ARUTEL telephone alarm system with Avaya Communication Manager. These Application Notes contain an extensive description of the configurations for both ARUTEL and Avaya Communication Manager which were used for testing. The testing which was performed tested the major functions of the ARUTEL product.

Information in these Application Notes has been obtained through compliance testing and additional technical discussions. Testing was conducted via the Developer*Connection* Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

The ARUTEL system can react to external alarm stimuli which indicate the existence of an emergency situation by informing affected persons of the situation, and documenting such events.

Alarm situations can be signaled by

- Telephone calls to signal emergency extensions
- Telephone conferences which are established when emergencies occur
- WEB alarm input
- Timed events which generate one-time or repeating alarms
- Optional key pad input from special hardware attached to the ARUTEL system
- Potential-free switch contact closure
- V.24 alarm messages
- Net management system messages

Only the first two alarm methods were tested in this configuration.

Once an alarm is detected by ARUTEL, the actions that it takes depend on how it has been configured. For each alarm detected one or more of the following actions can be taken:

- Presentation of a fixed voice alarm to a predefined list of phone numbers
- Presentation of an ad-hoc voice alarm to a predefined list of phone numbers
- Initiation of a conference to a predefined list of phone number
- Announcement presentation to calling parties containing emergency information.
- Signaling of building management systems via various interfaces
- Sending of text alarm messages via SMS

Only the first four alarms were tested in this configuration.

The ARUTEL allows voice alarms to be configured in a flexible manner, allowing one or more of the following options to be configured for each alarm:

- Alarm initiators can be optionally required to perform authorization via a PIN code
- Alarm recipients can be optionally requested to confirm or reject the ability to respond to an alarm
- Alarm recipients can be optionally requested to input the time that is needed to respond to an alarm

The ARUTEL unit can be interfaced either via an E1/QSIG interface, or via a SIP trunk. The tests described by this application note were done with the ARUTEL SIP trunk: no QSIG tests were performed.

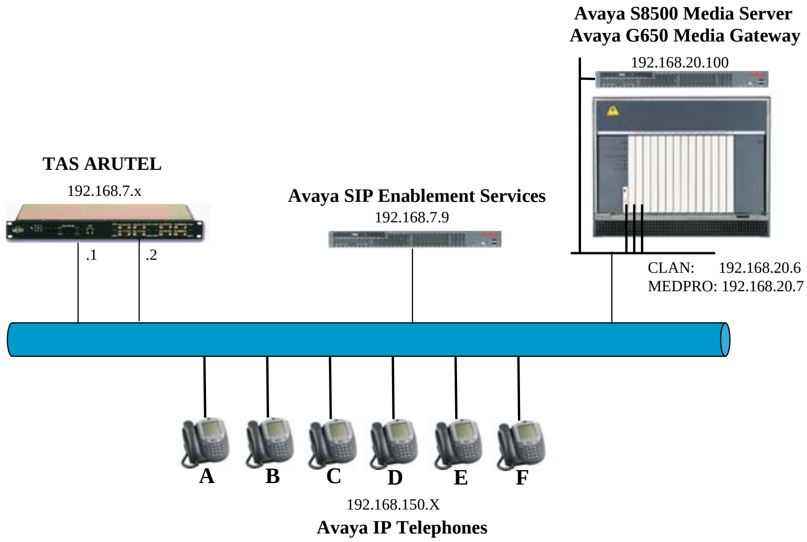


Figure 1: ARUTEL Test Configuration

The TAS ARUTEL alarm system is attached to the Avaya SIP Enablement Server (SES) server via a SIP trunk interface. The ARUTEL can optionally be attached to other devices for sensing and reporting alarms, but these were not tested in these tests and are thus not shown in the diagram.

The ARUTEL unit consists of two components: the Base Unit with the IP address 192.168.7.1, and the EIX interface unit with the IP address 192.168.7.2 which provides connectivity to external PBXs and the base unit.

The following table contains additional information about each of the telephones contained in the above diagram:

Phone	Model	Extension
A	Avaya 4610SW IP	2000114
B	Avaya 4610SW IP	2000115
C	Avaya 4610SW IP	2000115
D	Avaya 4625SW IP	2000152
E	Avaya 4621SW IP	2000135
F	Avaya 4621SW IP	2000134

Table 1: Telephone Configuration

2. Equipment and Software Validated

Hardware/Software Component	Version
Avaya S8500 Media Server with Avaya G650 Media Gateways	Avaya Communication Manager R013x.01.2.632.1 Update: 01.2.632.1-12249
Avaya TN799DP C-LAN interface	HW01/FW017
Avaya TN2302AP IP Media Processor	HW20/FW110
Avaya TN2464CP DS1 Interface	HW01/FW018
Avaya 4610SW IP telephone	H.323 2.4
Avaya 4621SW IP telephone	H.323 2.4
Avaya 4625SW IP telephone	H.323 2.5
Avaya SIP Enablement Services	SES-3.1.0.0-018.0
TAS ARUTEL EIX	6.03b
TAS ARUTEL Linux Server	1.2.02

Table 2: Hardware/Software Component Versions

3. Configuration

3.1. Configure Avaya Communication Manager

The configuration and verification operations illustrated in this section were performed using the Avaya Communication Manager SAT terminal via telnet port 5023.

3.1.1. Verify system-parameters customer-options

Use the **display system-parameters customer** command to verify that Avaya Communication Manager is configured to meet the minimum requirements to support the configuration used for these tests. Those items shown in **bold** indicate required values or minimum capacity requirements. If these are not met in the configuration, please contact an Avaya representative for further assistance.

The value configured for “Maximum Concurrently Registered IP Stations” must be sufficient to support the total number of IP stations used.

Verify that the number of SIP trunks supported by the system is sufficient for the combination of trunks to the TAS ARUTEL and optional SIP endpoints to be supported.

```
display system-parameters customer-options                      Page   2 of  11
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                              USED
                     Maximum Administered H.323 Trunks: 10    0
           Maximum Concurrently Registered IP Stations: 50    10
             Maximum Administered Remote Office Trunks: 0     0
Maximum Concurrently Registered Remote Office Stations: 0     0
              Maximum Concurrently Registered IP eCons: 0     0
  Max Concur Registered Unauthenticated H.323 Stations: 0     0
                  Maximum Video Capable H.323 Stations: 0     0
                   Maximum Video Capable IP Softphones: 0     0
                       Maximum Administered SIP Trunks: 20    20

   Maximum Number of DS1 Boards with Echo Cancellation: 0     0
                             Maximum TN2501 VAL Boards: 1     0
                     Maximum G250/G350/G700 VAL Sources: 0    0
           Maximum TN2602 Boards with 80 VoIP Channels: 0     0
          Maximum TN2602 Boards with 320 VoIP Channels: 0     0
   Maximum Number of Expanded Meet-me Conference Ports: 0     0
```

The “IP Stations” parameter must be set to “y” so that IP stations can be attached.

```
display system-parameters customer-options                      Page   4 of  11
                                OPTIONAL FEATURES

   Emergency Access to Attendant? y                              IP Stations? y
           Enable 'dadmin' Login? y              Internet Protocol (IP) PNC? y
           Enhanced Conferencing? y                       ISDN Feature Plus? n
                  Enhanced EC500? y           ISDN Network Call Redirection? y
    Enterprise Survivable Server? n                         ISDN-BRI Trunks? y
       Enterprise Wide Licensing? n                                ISDN-PRI? y
              ESS Administration? n              Local Survivable Processor? n
          Extended Cvg/Fwd Admin? n                    Malicious Call Trace? n
     External Device Alarm Admin? n                Media Encryption Over IP? n
  Five Port Networks Max Per MCC? n     Mode Code for Centralized Voice Mail? n
                Flexible Billing? n
   Forced Entry of Account Codes? n                Multifrequency Signaling? y
      Global Call Classification? n Multimedia Appl. Server Interface (MASI)? n
             Hospitality (Basic)? y         Multimedia Call Handling (Basic)? n
 Hospitality (G3V3 Enhancements)? n      Multimedia Call Handling (Enhanced)? n
                      IP Trunks? y

           IP Attendant Consoles? n
```

The value configured for "IP Phone" must be sufficient to support the total number of IP stations used.

```
display system-parameters customer-options                      Page  10 of  11
                     MAXIMUM IP REGISTRATIONS BY PRODUCT ID

Product ID  Rel. Limit          Used
IP_API_A       : 0              0
IP_API_B       : 0              0
IP_API_C       : 0              0
IP_Agent       : 1              0
IP_IR_A        : 0              0
IP_Phone       : 12000          10
IP_ROMax       : 12000          0
IP_Soft        : 5              0
IP_eCons       : 0              0
```

3.1.2. Configure Dial Plan

3.1.2.1 Configure Dial Plan Analysis

Use the **change dialplan analysis** command to specify that dialed strings which begin with "6", or "84" are extensions. Include the string "*83" as Dial Access Code, as described in section 3.1.3.3.

```
change dialplan analysis                                        Page   1 of  12
                             DIAL PLAN ANALYSIS TABLE
                                                            Percent Full:    1

      Dialed  Total  Call      Dialed  Total  Call      Dialed  Total  Call
      String  Length Type      String  Length Type      String  Length Type
        2       7    ext
        84      7    ext
        *83     3    dac
```

3.1.2.2 Configure Uniform Dial Plan

Use the **change uniform-dialplan** command to specify that extensions with leading digits of "84", which are allocated to the TAS ARUTEL, are to be processed by Automatic Alternate Routing (aar). The inserted digits are used by aar as the routing pattern selection criteria (see section 3.1.2.3)

```
change uniform-dialplan 1                                       Page   1 of   2
                       UNIFORM DIAL PLAN TABLE
                                                              Percent Full: 0

  Matching         Insert          Node   Matching         Insert          Node
  Pattern   Len Del Digits Net Conv Num    Pattern  Len Del Digits Net Conv Num
  84        7   0    084   aar  n                                       n
```

3.1.2.3 Configure Automatic Alternate Routing

Use the **change aar analysis** command to select a route pattern. The inserted digits specified by the Uniform Dial Plan (see section 3.1.2.2) are used the selection criteria. The "084" string is used to select the route pattern 84 for the ARUTEL (see section 3.1.3.7).

```
change aar analysis 0                                          Page   1 of   2
                             AAR DIGIT ANALYSIS TABLE
                                                          Percent Full:    1

          Dialed           Total     Route    Call   Node  ANI
          String          Min  Max  Pattern   Type   Num   Reqd
    084                    10   10   84       aar          n
```

3.1.3. Configure Interface to SES

3.1.3.1 Specify IP node names

Use the **change node-names ip** command to define the address of the "clan" interface and the Avaya SIP Enablement Services server.

```
change node-names ip                                           Page   1 of   1
                                  IP NODE NAMES
    Name              IP Address          Name              IP Address
clan                192.168.20.6                             .   .   .
default             0 .0 .0 .0                               .   .   .
ipsi                192.168.20.5                             .   .   .
medpro              192.168.20.7                             .   .   .
procr                 .   .   .                              .   .   .
ses2                192.168.7.9                              .   .   .
```

3.1.3.2 Configure Signaling Group for the SIP Trunk Interface to SES

Use the **add signaling-group <x>** command, where <x> is a free signaling group number, to create a signaling group which is to be used to connect to the SES. Accept defaults for parameters, except for those which are highlighted.

Parameter	Usage
Group Type	Enter "sip" to specify a SIP trunk
Transport Method	Enter "tls" to specify that Transport Layer Security should be used to encode data information flow on this signaling group.
Near-end Node Name	Enter "clan" to use the CLAN interface on the S8500
Near-end Listen Port	Enter "5061" to specify the standard TLS listen port
Far-end Node Name	Enter "ses2" to specify the SES server as far-end node name
Far-end Listen Port	Enter "5061" to specify the standard TLS listen port
Far-end Domain	Enter the domain name which is configured for SES, show in Figure 4: System Properties
DTMF over IP	Enter "in-band-g711" to send in-band DTMF signals, as required by the ARUTEL unit.
Direct IP-IP Audio Connections	Enter "n" to specify that direct IP-IP audio connections should not be used. This is essential for compatibility with the ARUTEL
IP Audio Hairpinning	Enter "n" to specify that audio hairpining should not be used

Table 3: Configuration Signaling Group for SIP Interface to SES

```
add signaling-group 83                                          Page   1 of   1
                                SIGNALING GROUP

 Group Number: 83             Group Type: sip
                        Transport Method: tls





   Near-end Node Name: clan                  Far-end Node Name: ses2
 Near-end Listen Port: 5061                Far-end Listen Port: 5061
                                        Far-end Network Region:
       Far-end Domain: ffm.com

                                             Bypass If IP Threshold Exceeded? n

         DTMF over IP: in-band-g711           Direct IP-IP Audio Connections? n
                                                        IP Audio Hairpinning? n
 Session Establishment Timer(min): 120
```

3.1.3.3 Configure Interface to SIP Trunk

Use the **add trunk-group <x>** command, where <x> is a free trunk group number, to create a trunk group which is to be used to connect to the Avaya SES. Accept defaults for parameters, except for those which are highlighted.

Parameter	Usage
Group Type	Specify a type of "sip"
TAC	Set the Trunk Access Code to "*83"
Group Name	Specify "SIP" to identify this trunk. Any identifier can be used.
Service Type	Specify the trunk is used as a "tie" line to another PBX.
Signaling Group	Specify the signaling group which was configured for the sip trunk.
Number of Members	Specify the number of IP connections to be allocated for this trunk

Table 4: Configuration Parameters for Trunk Interface to SIP Trunk

```
add trunk-group 83                                              Page   1 of  21
                                TRUNK GROUP

Group Number: 83                   Group Type: sip           CDR Reports: y
  Group Name: SIP                         COR: 1        TN: 1        TAC: *83
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                          Night Service:
Queue Length: 0
Service Type: tie                   Auth Code? n

                                                       Signaling Group: 83
                                                     Number of Members: 5
```

3.1.3.4 Configure public-unknown-numbering

Use the **change public-unknown-numbering <x>** command, where <x> the leading digit of the extension of the telephones which communicate with the ARUTEL. All of the stations which communicate with the ARUTEL must be included in the public-unknown-numbering table so that the station extensions are properly identified.

Parameter	Usage
Exe Len	Extension length
Ext Code	Extension code
Trk Grp	Trunk group
CPN Prefix	Called party number prefix
Total CPN Len	Total called party number prefix

Table 5: Configuration Parameters for public-unknown-numbering

```
change public-unknown-numbering 2                               Page   1 of   2
                      NUMBERING - PUBLIC/UNKNOWN FORMAT
                                   Total                                   Total
Ext Ext    Trk       CPN            CPN Ext Ext    Trk       CPN            CPN
Len Code   Grp(s)    Prefix         Len Len Code   Grp(s)    Prefix         Len

 7 2000114 83                        7
 7 2000115 83                        7
 7 2000116 83                        7
 7 2000134 83                        7
 7 2000135 83                        7
 7 2000152 83                        7
```

3.1.3.5 Configure Network Region

Use the **change network-region <x>** command, where <x> is the network region used by the SIP trunk. Enter the following parameters:

Parameter	Usage
Location	Use a location of “1”, in this example
Authoritative Domain	Use a domain of “ffm.com”, in this example
Name	Assign a name for identification purposes.
Audio Hairpinning	Specify “n” to enable audio hairpinning.

Table 6: Configuration Parameters for Network Region

```
change ip-network-region 1                                      Page   1 of  19
                               IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain: ffm.com
    Name: FFM
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 3327
DIFFSERV/TOS PARAMETERS                  RTCP Reporting Enabled? y
 Call Control PHB Value: 46      RTCP MONITOR SERVER PARAMETERS
        Audio PHB Value: 46       Use Default Server Parameters? y
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                      RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

3.1.3.6 Configure Codec Set

Use the **change ip-codec-set <x>** command, where <x> is the codec set assigned to the network region used by the SIP trunk. Enter the following parameters:

Parameter	Usage
Audio Codec	Enter "G.711A" to specify the use of the G711 A-Law codec. The ARUTEL also supports the following codecs: "G.729" or "G.723-6.3K". However, these additional codecs were not tested by the tests described by this application note.

Table 7: Configuration Parameters for Trunk Interface to SES

```
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.711A            n         2        20
 2:
 3:
 4:
 5:
 6:
 7:
```

3.1.3.7 Configure Routing Pattern to ARUTEL via SIP Trunk

Use the **change route-pattern** command to specify that the first three digits of the extension number used for this route pattern should be deleted, and trunk group 83 used to route the call. The leading digits “084” were added by the uniform-dialplan entry for this dial pattern, as shown is section 3.1.2.2. All calls to a destination which begins with “84” are routed to the ARUTEL via trunk group 83, the SIP trunk, which is configured in section 3.1.3.3.

Parameter	Usage
Grp No	Specify trunk group “83” which is assigned to the SIP trunk
No. Del Dgts	Specify “3” to delete the three digits which were added via the Uniform Dial Plan (see section 3.1.2.2)

Table 8: Configuration Parameters Routing Pattern to ARUTEL via SIP Trunk

```
change route-pattern 84                                         Page   1 of   3
                    Pattern Number: 84  Pattern Name: ARUTEL
                             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: 83   0                    3                                        n   user
 2:                                                                    n   user
 3:                                                                    n   user
 4:                                                                    n   user
 5:                                                                    n   user
 6:                                                                    n   user

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM  No. Numbering LAR
    0 1 2 3 4 W     Request                                Dgts Format
                                                        Subaddress
 1: y y y y y n  n            rest                                      none
 2: y y y y y n  n            rest                                      none
 3: y y y y y n  n            rest                                      none
 4: y y y y y n  n            rest                                      none
 5: y y y y y n  n            rest                                      none
 6: y y y y y n  n            rest                                      none
```

3.1.4. Configure Telephones

Use the **change station <x>** command to configure telephones to be used for testing.

Parameter	Usage
Type	The model identification of the phone to be used
Name	The name of the user which is to be associated with the phone
Security Code	The security code assigned to the extension. This number must be entered on the phone keypad along with the extension number when logging into the phone.

Table 9: Configuration Parameters IP Telephones

```
change station 2000114                                          Page   1 of   4
                                     STATION

Extension: 2000114                         Lock Messages? n          BCC: 0
     Type: 4610                            Security Code: 4110002     TN: 1
     Port: S00009                        Coverage Path 1:            COR: 1
     Name: ext 2000114                   Coverage Path 2:            COS: 1
                                         Hunt-to Station:

STATION OPTIONS
              Loss Group: 19             Personalized Ringing Pattern: 1
                                                     Message Lamp Ext: 2000114
            Speakerphone: 2-way                   Mute Button Enabled? y
        Display Language: english
 Survivable GK Node Name:
          Survivable COR: internal                  Media Complex Ext:
   Survivable Trunk Dest? y                              IP SoftPhone? n



                                                  Customizable Labels? y
```

3.2. Configure SES

3.2.1. Configure SIP Trunk to TAS ARUTEL

Step 1:
Access the SES Administration web interface, by entering http://<ip-addr>/admin as the URL in an Internet browser, where *<ip-addr>* is the IP address of Avaya SIP Enablement Services.

Log in with the appropriate credentials and then select the *Launch Administration Web Interface* link from the **Interface** screen as shown in Figure 2.

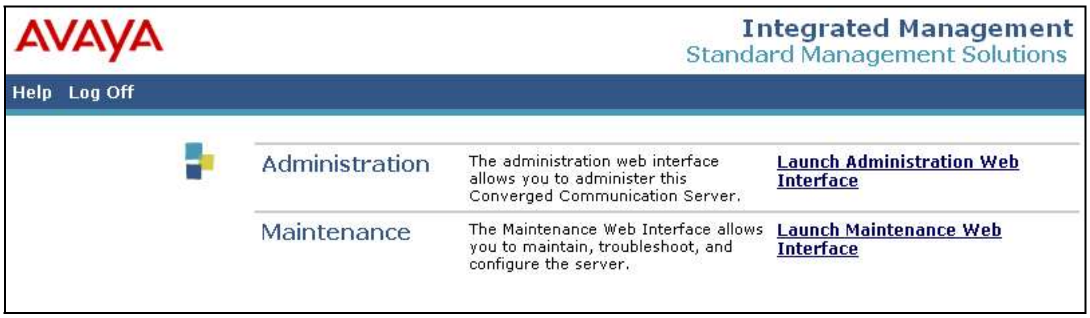


Figure 2 - Avaya SES Main Screen

The Avaya SES Administration Home Screen shown in **Figure 2** will be displayed.

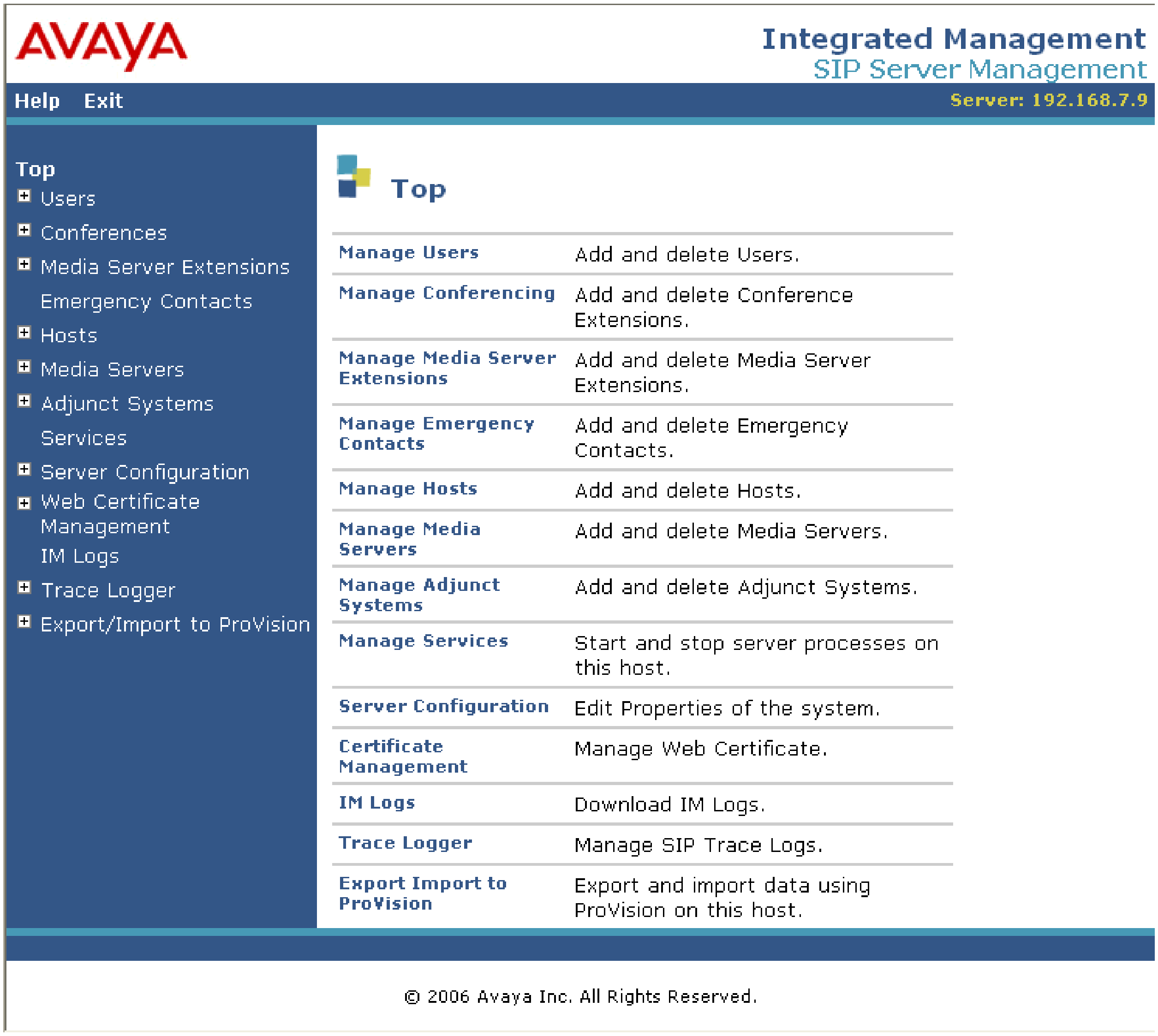


Figure 3: Avaya SES Administration Home Page

Step 2:

From the left pane of the Administration web interface, expand the **Server Configuration** option and select **System Properties**. This screen displays the Avaya SES version and the network properties entered via the installation script during the installation process.

In the **System Properties** screen,

- Enter the SIP domain name assigned to Avaya SIP Enablement Services
- Enter the **License Host** field. This is the host name, the fully qualified domain name, or the IP address of the SIP proxy server that is running the WebLM application and has the associated license file installed.
- After configuring the **System Properties** screen, click the **Update** button.

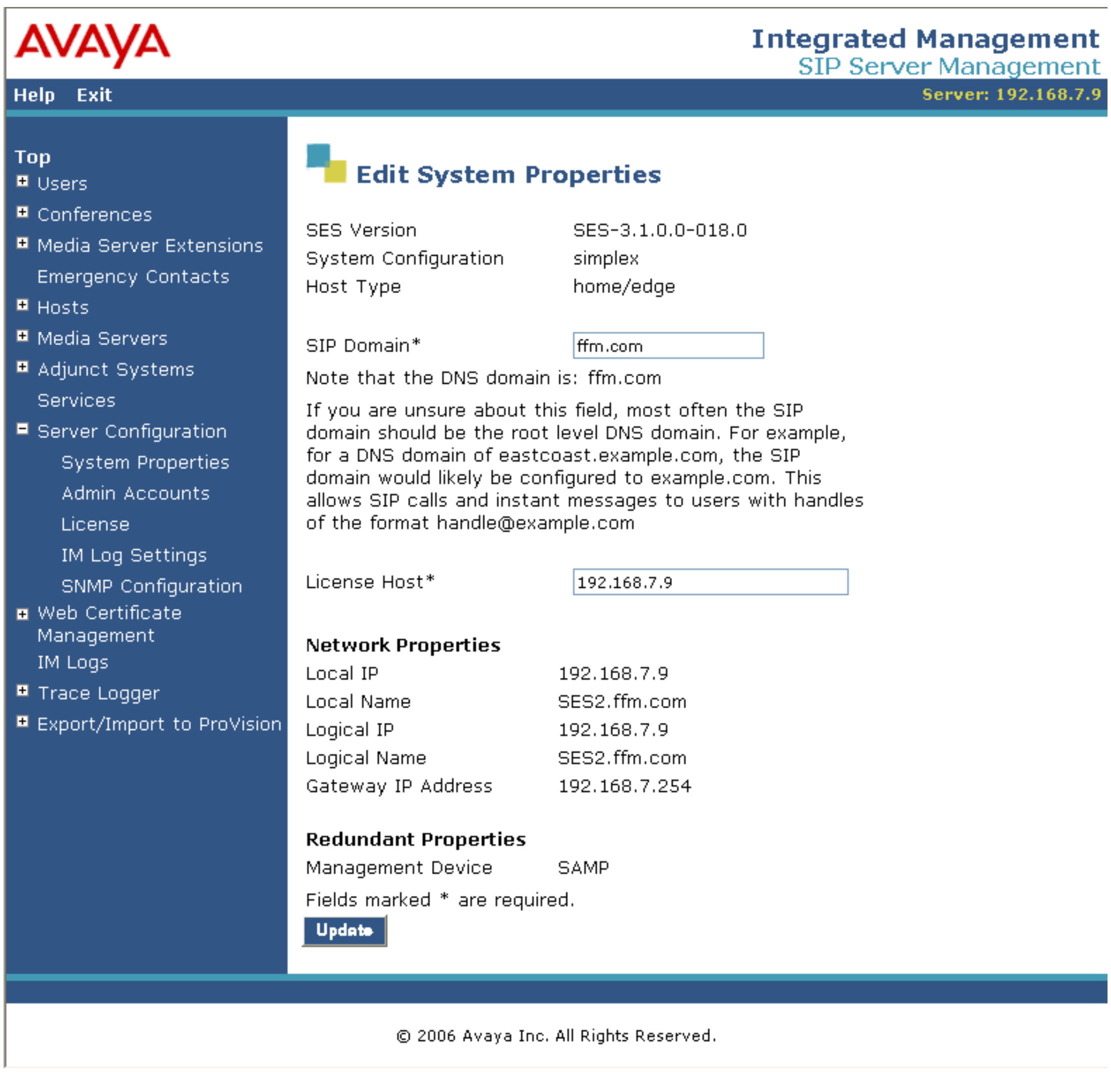


Figure 4: System Properties

Step 3:
After setting up the domain in the **System Properties** screen, create a host computer entry for Avaya SIP Enablement Services. The following example shows the **Edit Host** screen since the host had already been added to the system.

The **Edit Host** screen shown in Figure 5 is accessible by clicking on the **Hosts** link in the left pane and then clicking on the **edit** option under the **Commands** section of the subsequent page, not shown.

- Enter the IP address of this server in the **Host IP Address** field.
- Enter the **DB Password** that was specified while running the install script during the system installation.
- Configure the **Host Type** field. In this example, the host server was configured as a *home/edge* since no additional SES proxy servers exist in the enterprise network.
- The default values for the other fields may be used as shown in Figure 5.
- Click the **Update** button.

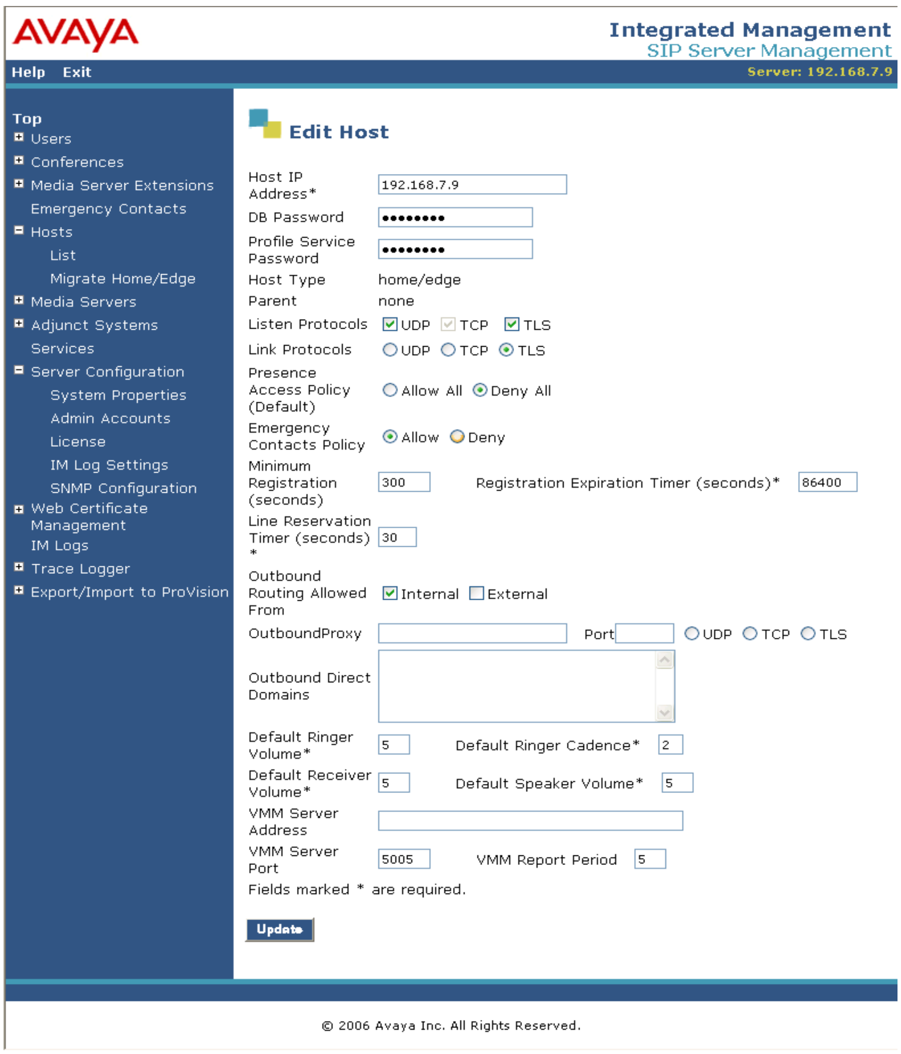


Figure 5: Edit Host

Step 4:
Under the **Media Servers** option in the Administration web interface, select **Add** to add the Avaya Media Server in the enterprise site. This will create the SES side of the SIP trunk previously created in Avaya Communication Manager, not shown.

In the **Add Media Server Interface** screen, enter the following information:

- A descriptive name in the **Media Server Interface Name** field (e.g., S8500).
- Select the home SES server in the **Host** field.
- Select *TLS* (Transport Link Security) for the **SIP Trunk Link Type**. TLS provides encryption at the transport layer. TLS is the only link protocol that is supported for SIP trunking with Avaya Communication Manager.
- Enter the IP address of the Avaya S8500 Media Server in the **SIP Trunk IP Address** field.[1]
- After completing the **Add Media Server** screen, click on the **Add** button.

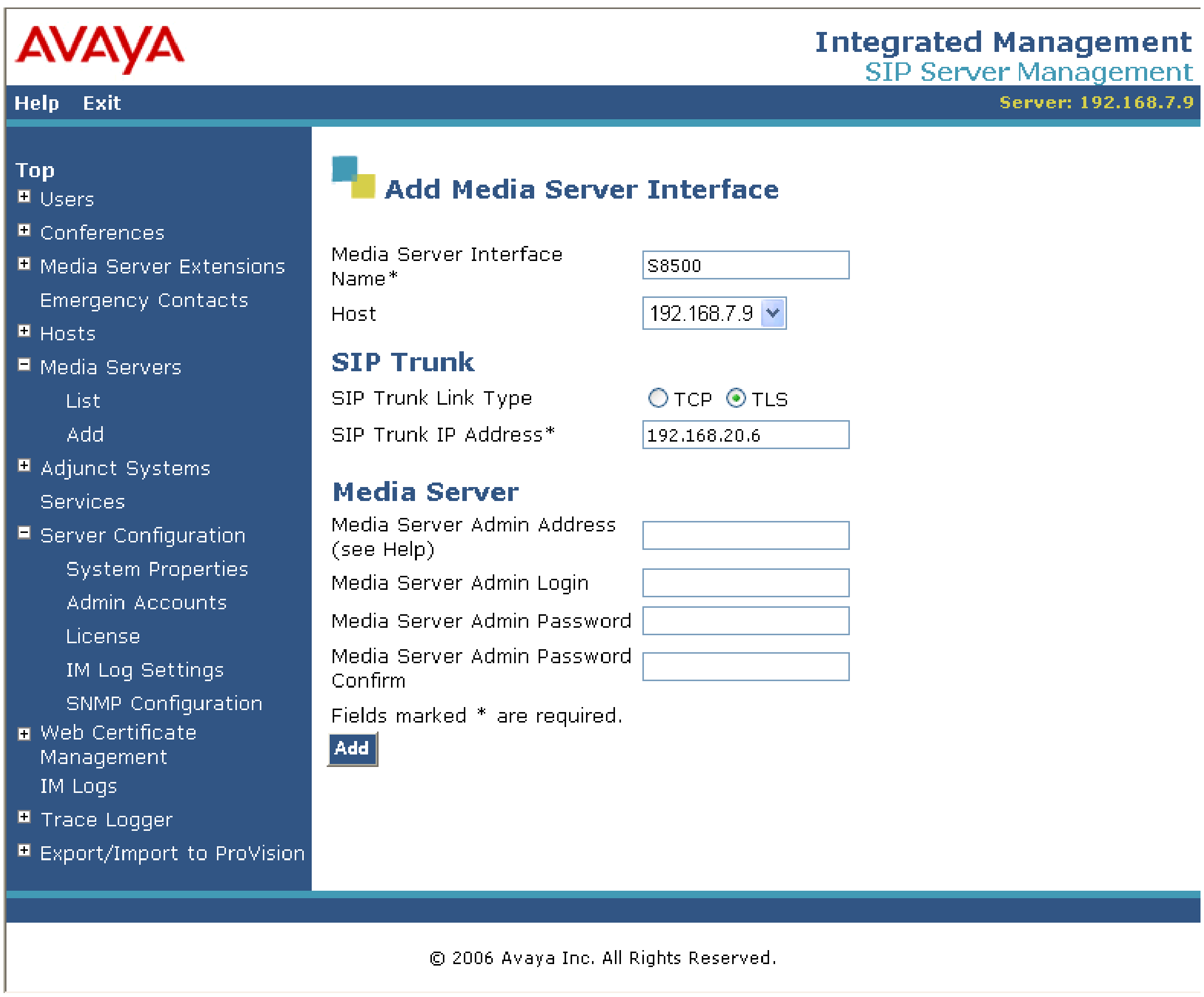


Figure 6: Add Media Server

[1] Depending on the platform of the media server and gateway, this field may be set to the IP address of a C-LAN board.

Step 5:
Incoming calls arriving at Avaya SIP Enablement Services are routed to the appropriate Avaya Communication Manager for termination services. This routing is specified in a **Media Server Address Map** configured on Avaya SIP Enablement Services.

This routing compares the Uniform Resource Identifier (URI) of an incoming INVITE message to the pattern configured in the **Media Server Address Map,** and if there is a match, the call is routed to the designated Avaya Communication Manager. The URI usually takes the form of sip:user@domain, where domain can be a domain name or an IP address. Patterns must be specific enough to uniquely route incoming calls to the proper destination if there are multiple Avaya Communication Managers supported by the Avaya SES.

In this application note only incoming calls from the SIP trunks not attached to Avaya Communication Manager require a media server address map entry.

To configure a **Media Server Address Map**:

- Select **Media Servers** in the left pane of the Administration web interface. This will display the **List Media Servers** screen.
- Click on the **Map** link associated with the appropriate media server to display the **List Media Server Address Map** screen.
- Click on the **Add Map In New Group** link. The screen shown in **Figure 7** is displayed. The Host field displays with the name of the media server to which this map applies.
- Enter a descriptive name in the **Name** field
- Enter the regular expression to be used for the pattern matching in the **Pattern** field.

  In this configuration, the pattern specification (without the double quotes) for DID numbers assigned to the 2* group is: “^sip:2……”. This says URIs beginning with “sip:2” followed by any combination of “6 digits” should be routed to the S8500 media server.

- Click the **Add** button once the form is completed.

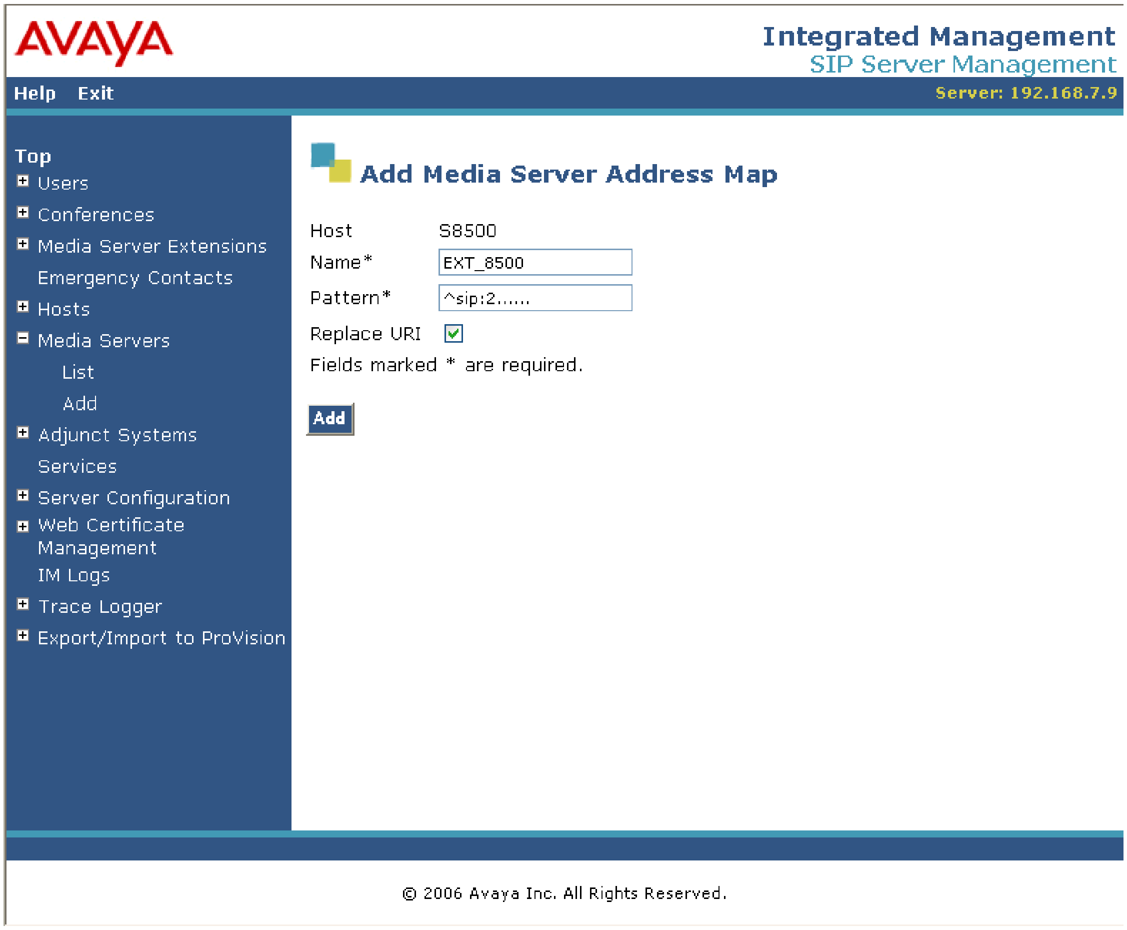


Figure 7: Media Server Address Map

After configuring the media server address map, the **List Media Server Address Map** screen appears as follows:

Figure 8: List Media Server Address Map

Note that after the first **Media Server Address Map** is added, the **Media Server Contact** is created automatically. For the **Media Server Address Map** added in **Figure 7**, the following contact was created:

sip:$(user)@192.168.20.6:5061;transport=tls

The contact specifies the IP address of the Avaya S8500 Media Server CLAN interface and the transport protocol used to send SIP signaling messages. The user in the original request URI is substituted for $(user).

Step 6:
Calls to extensions beginning with "84" are directed by Avaya Communication Manager to use the SIP trunk group and follow subsequent SIP based routing controlled by the Host Address Maps in the Avaya SIP Enablement Services. Similar to the inbound media server address maps, these Host Address Maps also use pattern matching to direct outbound SIP messages to the proper destination (such as ARUTEL in this application note).

In this configuration, the routing rule for the SIP trunk group will be to send all outbound call to extensions beginning with "84" to the ARUTEL SIP trunk. To perform this, the following matching patterns will be created in the Avaya SES (without the double quotes): "^sip:84". This pattern will match on all sip calls starting with leading digits assigned to ARUTEL extensions.

Configuring the host address map for all calls to endpoints attached to the ARUTEL is shown in **Figure** 9.

- Access the **Add Host Address Map** screen by selecting the **Hosts** link in the left pane of the Administration web interface and then clicking on the **Map** link associated with the appropriate host. The **List Host Address Map** screen is displayed.
- From this screen, click the **Add Map In New Group** link to display the **Add Host Address Map** screen shown in
- **Figure** 9.
- Enter a descriptive name for the map, such as "outgoing_ARUTEL".
- Specify an appropriate pattern for the call type. In this example, the pattern used for ARUTEL calls is "^sip:84".
- Leave the **Replace URI** checkbox selected.
- Click the **Add** button.

Additional Host Address Map patterns are added in the same manner.

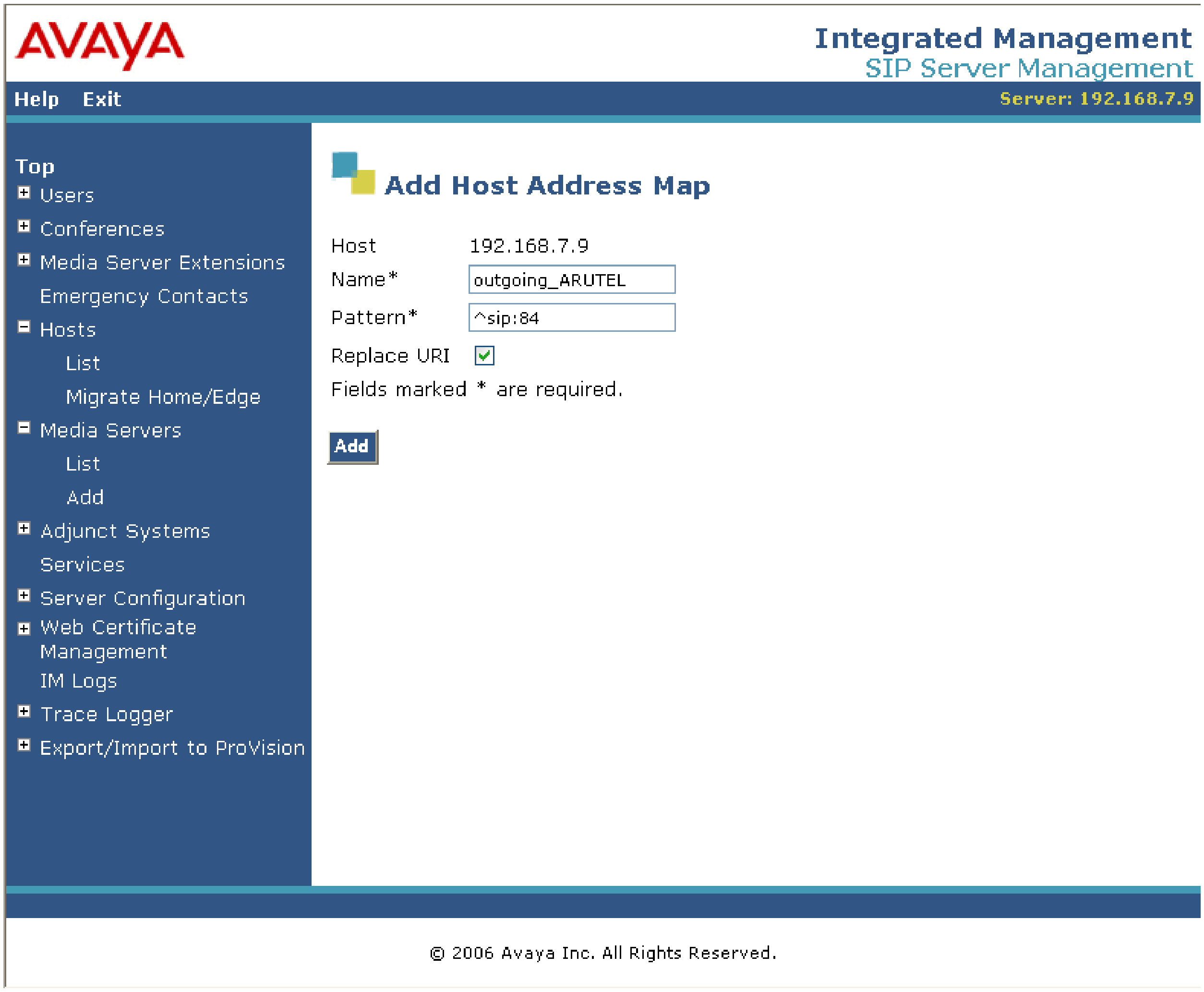


Figure 9: Add Host Address Map

Step 7:
The next step is to enter the contact address for the ARUTEL SIP proxy. In this example, the IP address 192.168.7.2 is used. This information is contained the ARUTEL EIX configuration file described in section 3.3.

To enter the ARUTEL SIP proxy information:

- As described in Step 6, display the **List Host Address Map** screen,
- Click on the **Add Another Contact** link associated with the address map added in
- **Figure** 9 to open the **Add Host Contact** screen. In this screen, the **Contact** field specifies the destination for the call and it is entered as:

sip:$(user)@192.168.7.2:5060;transport=udp

Note: You must replace the IP address (192.168.7.2) with the information assigned to the ARUTEL.

The user part in the original request URI is substituted for the $(user) string before the message is sent to ARUTEL.

- Click the **Add** button when completed.

Step8:
After making changes within the Avaya SES, it is necessary to commit the database changes using the **Update** link that appears when changes are pending. Perform this step by:

- Click the **Update** link that is found in the bottom of the blue navigation bar on the left side of any of the SES Administration screens as shown in Figure 10.

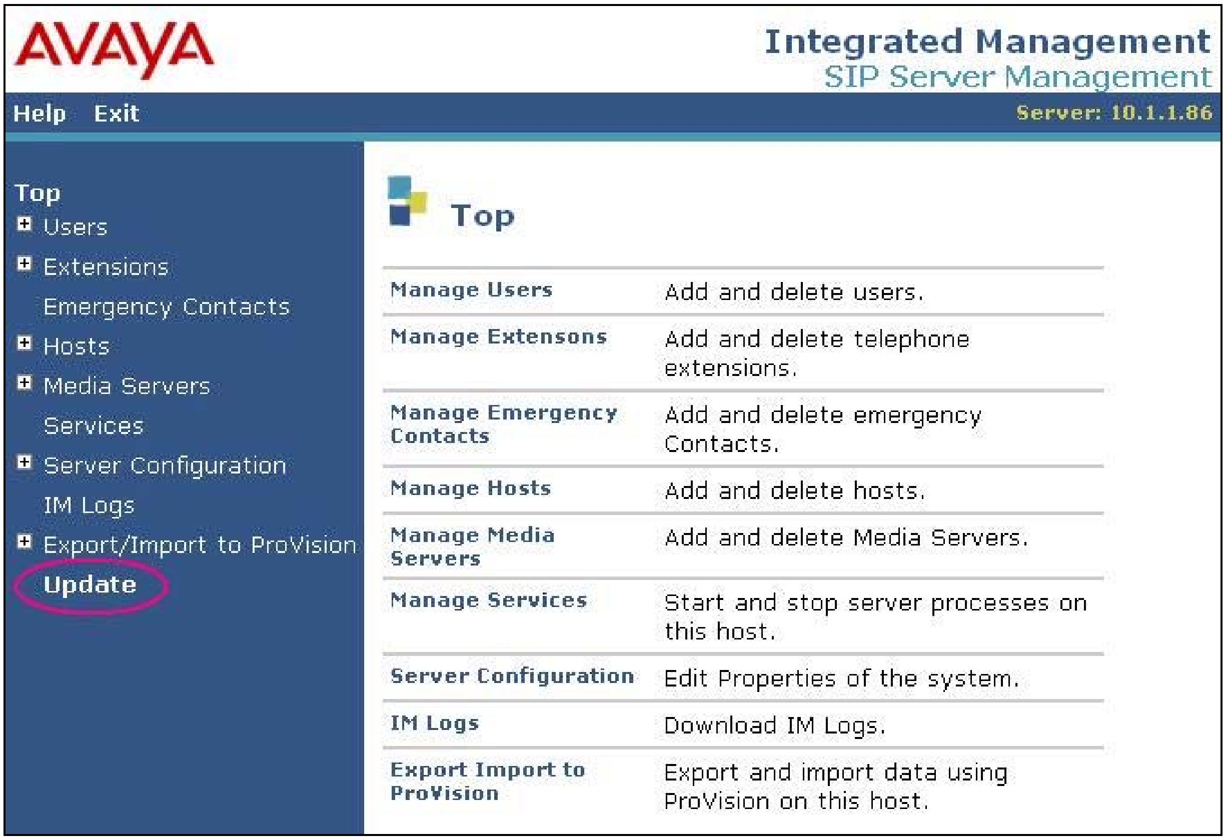


Figure 10: Update Following SES Administrative Changes

Step 9:
The final step to complete the SIP trunk administration on the Avaya SES is to designate the IP address of the ARUTEL SIP Proxy as a trusted host. As a trusted host, the Avaya SES will not issue SIP authentication challenges for incoming requests from the designated IP address.[2]

If multiple SIP proxies are used, the IP address of each SIP proxy must be added as a trusted host.

To configure a trusted host:

- Use a terminal emulator to connect to the Avaya SES IP address (e.g., in this case 192.168.7.9) and login using the administrative login and password.
- Enter the following trustedhost command at the Linux shell prompt:

  trustedhost -a 192.168.7.2 -n 192.168.7.9 -c t-systems_proxy

  The –a argument specifies the address to be trusted; –n specifies the Avaya SES host name; –c adds a comment.

- Use the following trustedhost command to verify the entry is correct:

  trustedhost –L

  Figure 11 illustrates the results of the trustedhost commands.[3]

- Complete the trusted host configuration by returning to the main Avaya SES Administration web page and again clicking on the **Update** link as shown in Figure 10.

  If the **Update** link is not visible, refresh the page by selecting **Top** from the left hand menu. Note this step is required even though the trusted host was configured via the Linux shell.

```
admin@ses> trustedhost -a 192.168.7.2 -n 192.168.7.9 -c ARUTEL
192.168.7.2 is added to trusted host list.
admin@ses> trustedhost -L
Third party trusted hosts.
       Trusted Host       |       CCS Host Name       |         Comment
--------------------------+---------------------------+-------------------------
192.168.7.2               | 192.168.7.9               | ARUTEL
```

Figure 11: Trusted Sites Entry for ARUTEL

---

[2] Note, if the trusted host step is not done, authentication challenges to incoming SIP messages (such as INVITEs and BYEs) will be issued but not responded to. This may cause call setup to fail, active calls be disconnected after timeout periods, and/or SIP protocol errors.

[3] For completeness, the –d argument allows the trust relationship to be deleted. For, example,

trustedhost –d 192.168.7.2 –n 192.168.7.9

removes the trust relationship added above.

3.3. Configure EIX

The ARUTEL configuration information is contained in a flat ASCII file (/config.txt) which can be edited with a text editor. This file is normally preconfigured by TAS prior to shipment of the AURTEL, and normally need not be modified by the customer. The contents of the file are shown here for the sake of documenting the settings which were used for testing.

The format of the parameters in this file is as follows:

<cnfg file> ::= <cnfg lines>
<cnfg lines> ::= <cnfg line> | <cnfg lines> <cnfg line>
<cnfg line> ::= <param line> | <comment line>
<comment line> ::= ; <comment text> CR
<param line> ::= <param text> CR | <param text> ; <comment text> CR
<param text> ::= <param key> <parma modifiers>
<parma modifiers> ::= <param modified> | <parma modifier> <param modifiers>
<parma modifier> ::= <text string>

The usage of the <param key> values within this file is as follows:

Parameter	Usage
N	Dial plan layout
F	Basic flags
I	Network parameters
Z	Access restrictions
f	SIP flags
i	SIP configuration

Table 10: <param key> Value Usage

The ARUTEL configuration parameters used for testing are as follows:

```
;Konfigurationsdatei für Up2 SIP BB EIX3 01006702 Struktur 10
N I00 N0 i49 n30 s12345       ; I00:  international access with “00”
                      ; N0   national access with “0”
                      ; i49  local international code
                      ; n69  local city code
                      ; s12345       subscriber prefix

F UNIFONE                     ; Operation mode
F ATLN_INST                   ; All incoming calls can be routed to alarm system
F ATLN_KARTE          ; All incoming calls can be routed to interal conferences
F K_BNORM                     ; Discard calling number prefix

I i:192.168.7.2 s:255.255.255.0      ;i:     IP address
                      ;s:     netmask
I d0:192.168.7.254            ;Default Router
I B"EIX3_UP3_SIP" L"Avaya"    ;B:     Comm card name
                      ;L:     SNMP Location name

Z0 I0.0.0.0 M0.0.0.0          ;I:     IP address with external access
                      ;M:     Mask for IP address with external access

f FROM_USE_CLI        ;The SIP „From“ Header is set to alternate extension

f CONTACT_USE_CLI             ;The SIP „Contact“ Header is set to alternate extension

i G20                 ;UDP Packe tsize

iSU tas               ;SIP account name for proxy registration
iSD ffm.com                   ;SIP Domain
iAU tas               ;SIP Authorization user name
iAP tas               ;SIP Passwd
iSP 192.168.7.9               ;SIP Proxy IP address

; f SIP_ALLOW_FROM_ALL        ; SIP Meldungen werden von allen IP Adressen
                                     ; akzeptiert (ansonsten nur vom PROXY)
; f GW_AUTH           ; Gateway Autorisierung (Proxy muss sich
                      ; beim GW autorisier)
; f GW_NO_REGISTER

;f ISDN_CLD_NUM_INT   ; BTln (ISDN -> SIP) wird in int. Rufnummer
                      ; gewandelt (anonsten wird die Nummer 1:1 als
                      ; Ziel genutzt)
;f ISDN_CLI_NUM_INT   ; ATln (ISDN -> SIP) wird in int. Rufnummer
                      ; gewandelt (nur gültig wenn FROM_USE_CLI)

;f SIP_CLD_NUM_NORM   ; SIP BTln (SIP -> ISDN) normiert
;f SIP_CLI_NUM_NORM   ; SIP ATln (SIP From -> ISDN) wir normiert:
               ; normal: keine führenden Nullen -> subscriber eine Null -> national zwei Nullen -
> international
```

3.4. Configure Browser

The base unit is configured via a web browser. These configuration web pages contain Active-X components, which require that the web browser be configured for this. This is done by selecting "Tools → Options → Security → Trusted Sites" from the web browser. Enter the IP address of the base unit in the list of trusted sites. Click "Add" followed by "OK".

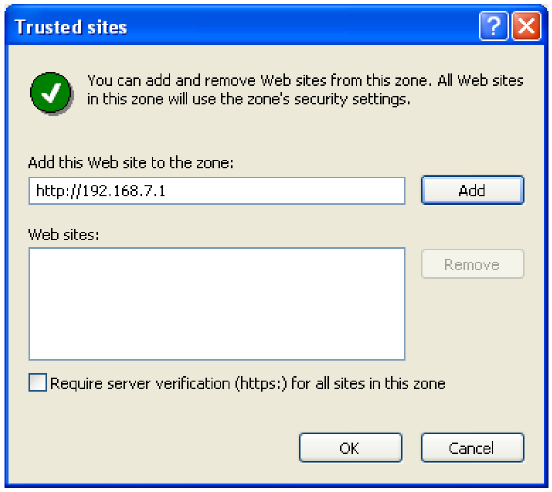


Figure 12: Trusted Sites Entry for ARUTEL

The following menu will appear. Click on the "Custom Level…" button.

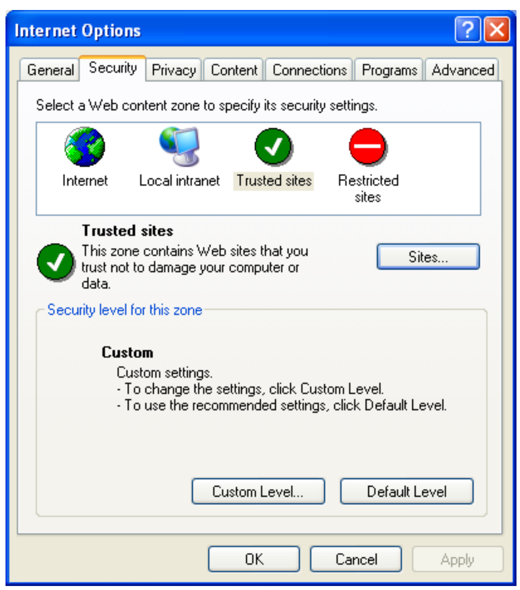


Figure 13: Internet Explorer Security Selection

The "Download unsigned ActiveX controls" and "Initialize and script ActiveX controls not marked as safe" entries must both be set to "Enable".

Click “OK”.

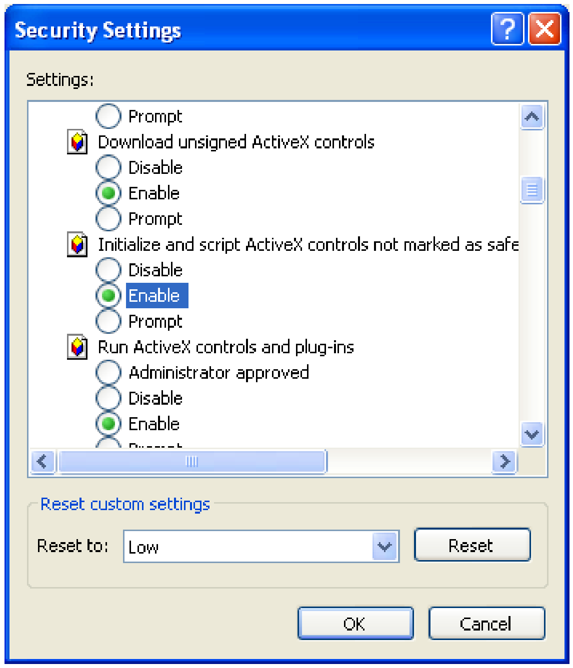


Figure 14: Internet Explorer Security Settings for ARUTEL

3.5. Configure Base Unit

Essential text messages are shown in various menus in this section. These messages are depicted in German are followed by an English translation highlighted in *italics*.

Note that all configuration actions performed with the web-based ARUTEL configuration tool must completed by moving the cursor from the last field which has been changed to another field before the change to that field actually take effect.

3.5.1. Initial System Login

Enter the URL of the ARUTEL base unit in the web browser to select the login screen.

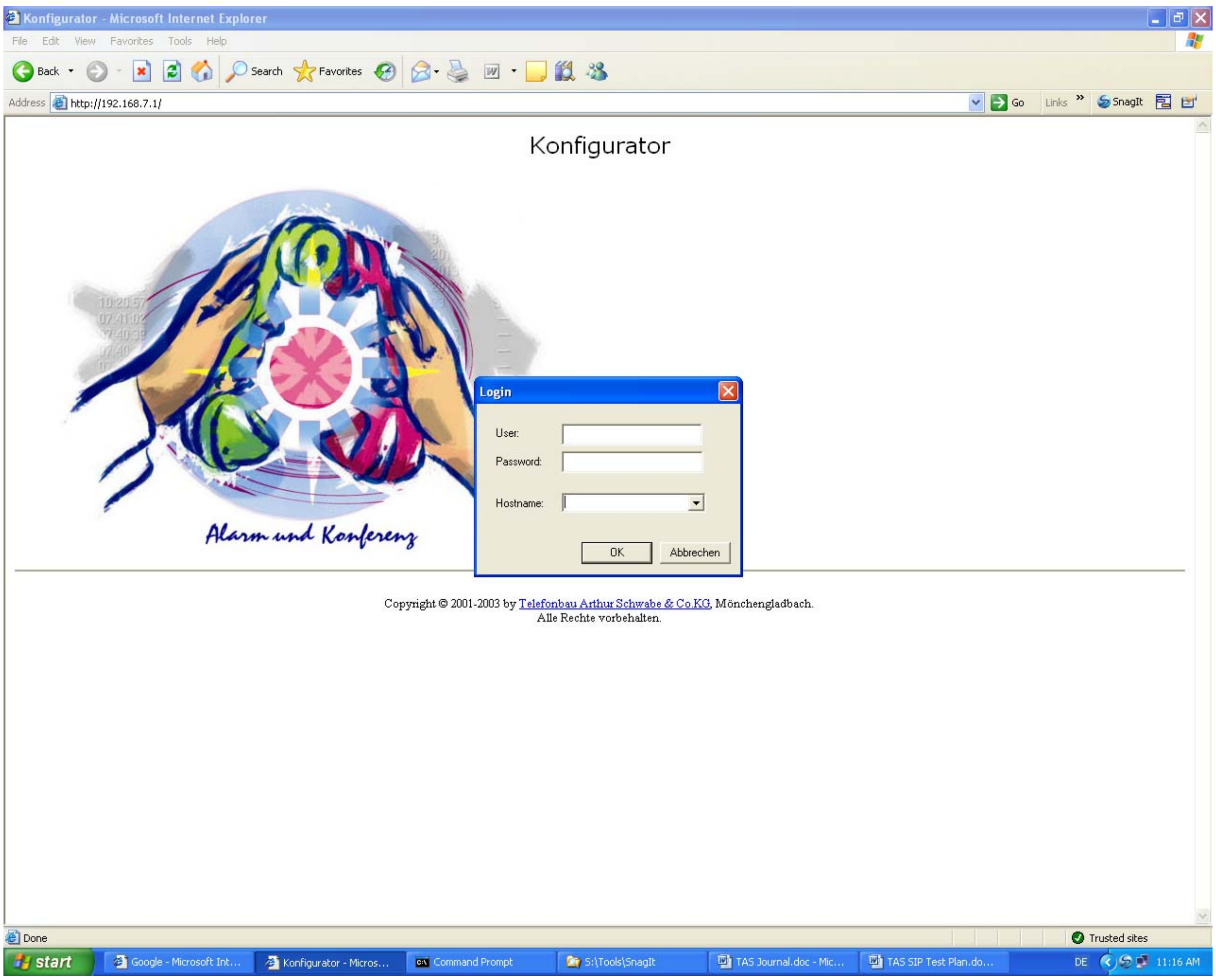


Figure 15: Login Screen for ARUTEL

Enter “up2” for both the default User, Password and the Hostname, and then click “OK”.

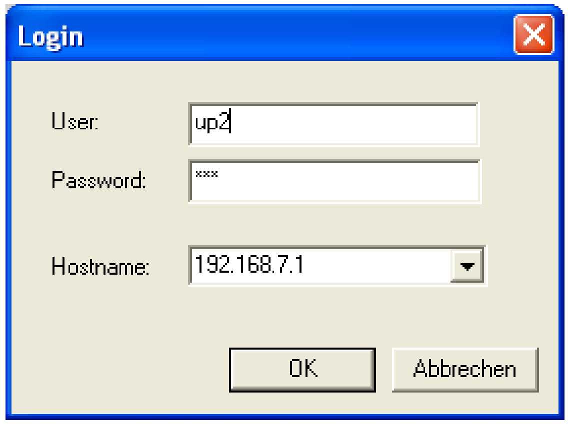


Figure 16: Initial User and Password Settings for ARUTEL

The main configuration screen is then shown:

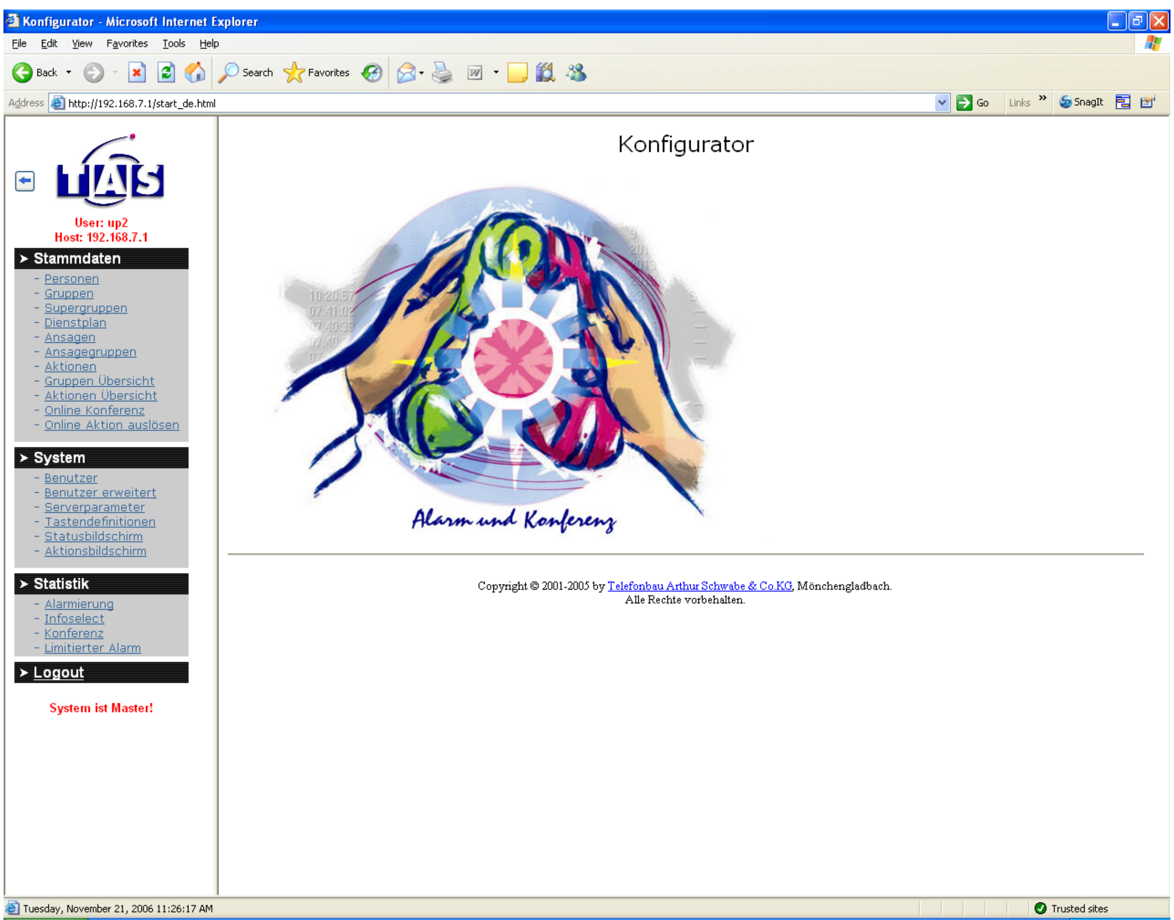


Figure 17: Main Configuration Screen for ARUTEL

3.5.2. Create Announcements

Announcements to be used by ARUTEL can be input via one of the telephone extensions via the following procedure:

1. From the left frame of the main widow, click the "Ansagen" ("*Announcements*") control.
2. The screen content shown below is then displayed.
3. Enter the name of the file which is to be recorded in the "Titel" ("*Title*") field.
4. Enter the number of the phone from which the voice message is to be recorded in the "Rufnummer" ("*Phone Number*") field.
5. Click the "Aufnehmen" ("*Record*") button at the bottom of the screen
6. Answer the selected phone when it rings.
7. Speak the message at the beep and hang up when complete.
8. The message can be replayed by clicking the "Abhören" ("*Playback*") button.

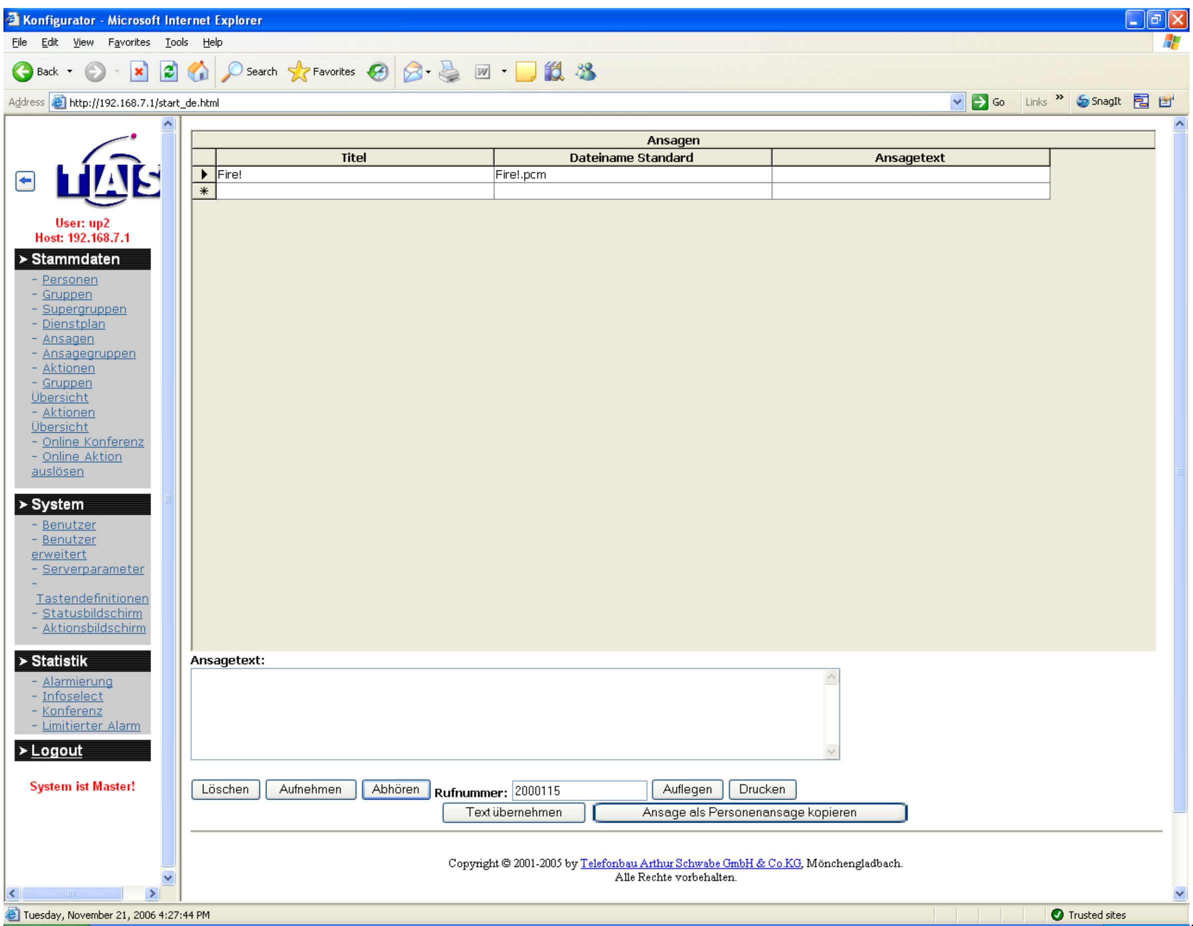


Figure 18: Announcement Configuration Screen

Use this procedure to create the following announcements:

Name	Content
Fire!	“The building is on fire, leave immediately!”
InfoMessage	“Hello, have a nice day”
SpeakMessageNow	“Please speak your message now”
FireAlarmInitiated	“The fire alarm has been initiated”
EnterPinAndSpeakMessage	“Please enter your PIN and speak your message”
PinPositive	“Positive PIN entered”
PinNegative	“Negative PIN entered”
InvalidPin	“Invalid PIN entered”
FireEnterPin	“The building is on fire, please entry your PIN”
WelcomeToConference	“Welcome to the conference”
ConferenceEnd	“The conference has ended”
EnterReactionTime	“Please enter your two digit reaction time in minutes”
ThanksForReactionDigits	“Thank you for entering your reaction time”

Table 11: Voice Messages Used for Testing

3.5.3. Allocate Users

Create the phone numbers for individual users of the system. Click the "Personen" ("*Persons*") control in the left frame. Enter the information described in the following table in fields of this menu, as shown in the screen following the table.

Field	Usage
Name	User name
1. Rufnummer	User's primary extension
2. Rufnummer	User's secondary extension
Dtmf Pin positiv	PIN code entered by accept message
Dtmf Pin negativ	PIN code entered by reject message

Table 12: ARUTEL User Configuration Fields

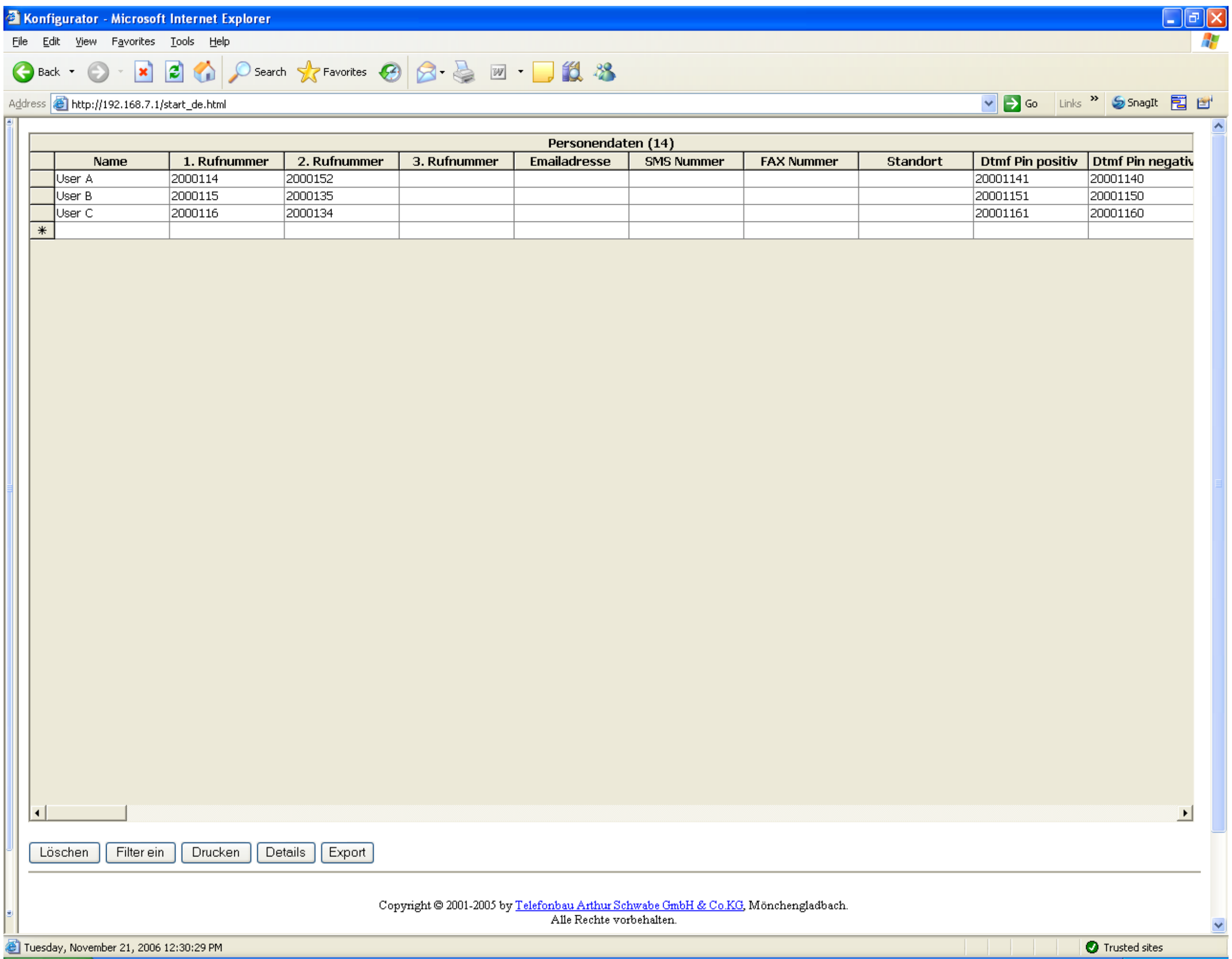


Figure 19: User Allocation Screen

3.5.4. Allocate Groups

Create groups of users. Select the "Gruppen" ("*Groups*") control from the left frame. For each group to be created, enter the name of the group in the "Titel" ("*Title*") field, and select that field with the cursor. Then enter the names of the users to be allocated to that group in the "Name" column. Allocate "Group A" with the following users:

- User A
- User B
- User C

Allocate "Group B" with the following users:

- User A

When the user name is entered in the "Name" field, the remaining fields to the right of this field are populated automatically.

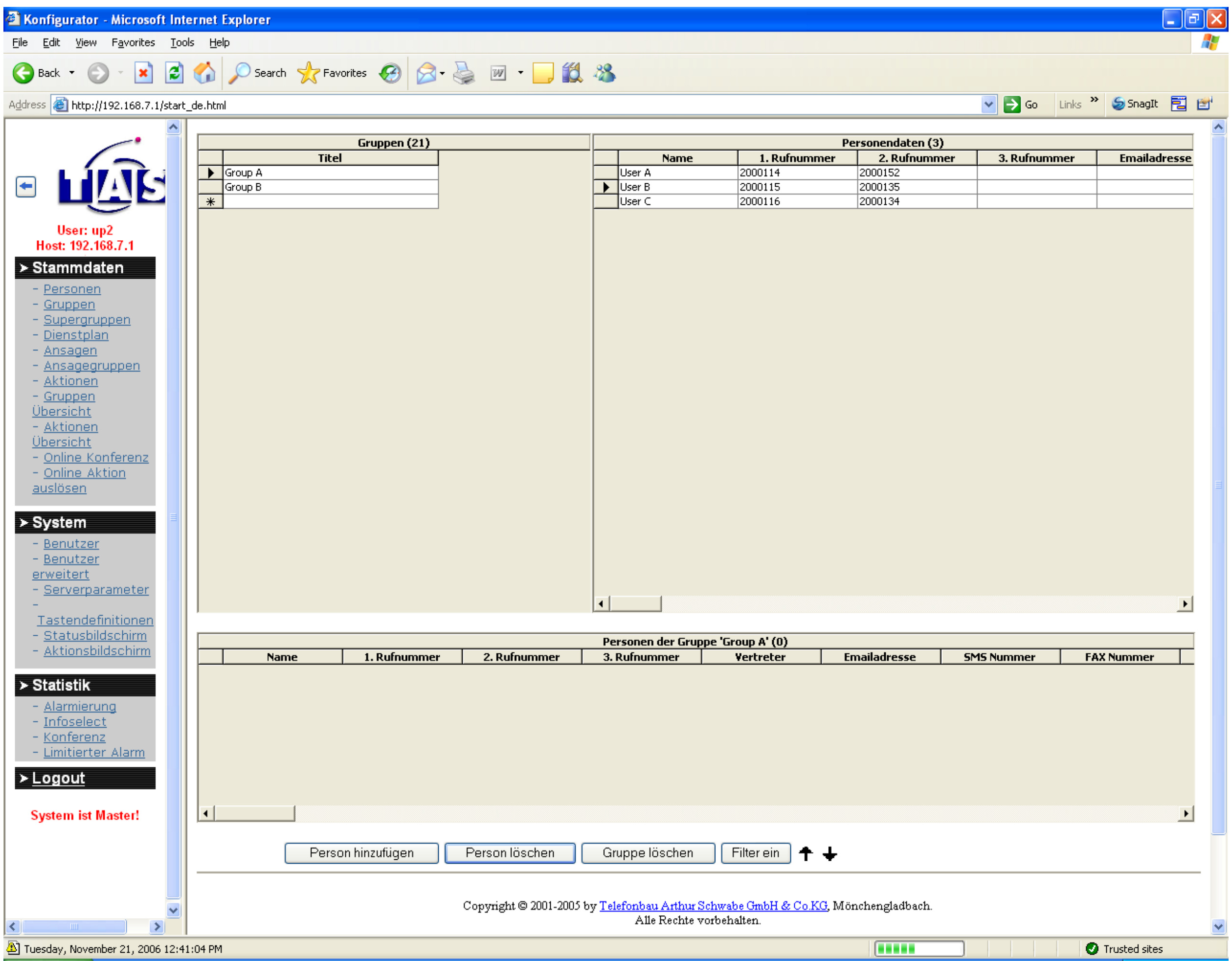
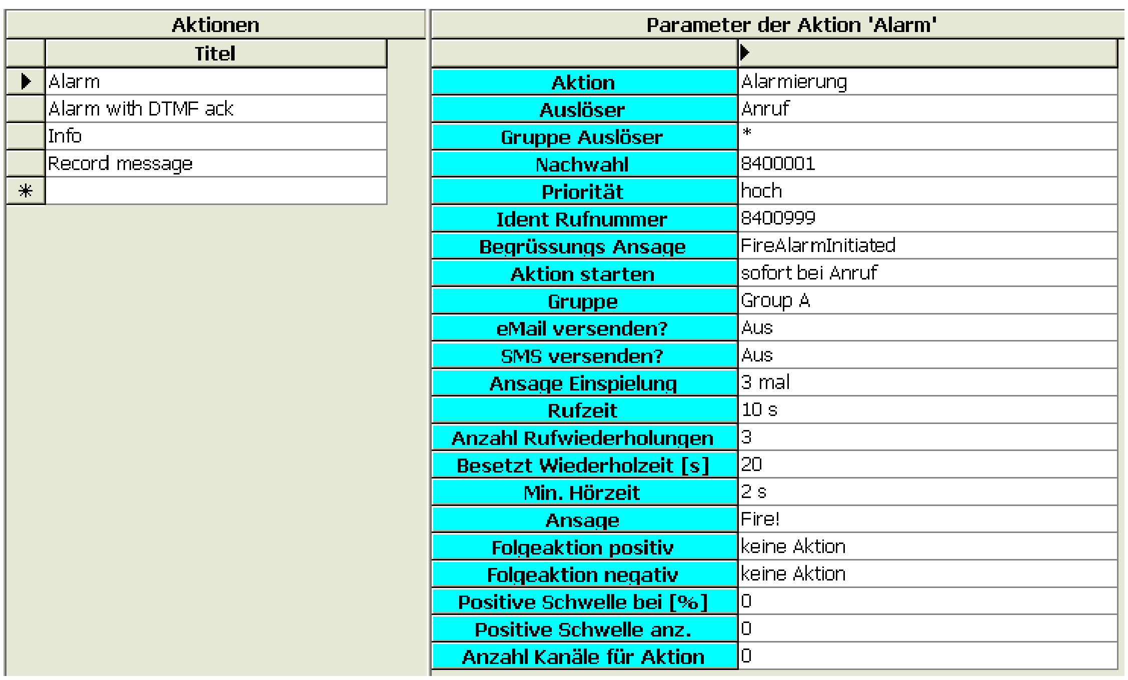


Figure 20: Group Allocation Screen

3.5.5. Create an Alarm with Predefined Message Content

Create an alarm which is played to a group of users when initiated by calling a specified number.

1. Select the “Aktionen” (“*Actions*”) control from the left frame of the main menu. When the “Aktionen” menu appears, enter the information as show in the following steps.
2. From the “Aktionen” menu, create the action “Alarm”, and set the parameters as shown in the following steps.
3. Set the “Aktion” field to “Alarmierung” (“*Alarm*”)
4. Set the “Auslöser” (“*Trigger*”) field to “Anruf” to initiate upon call.
5. Set the “Nachwahl” (“*Extension*”) field to “8400001” to set the number which triggers this action.
6. Set the “Begrüssungs Ansage” (“*Greeting message*”) to “FireAlarmInitiated”, to inform the caller that the alarm has been initiated.
7. Set the group of extensions which are to be called with the message in the “Gruppe” (“*Group*”) field.
8. Set the “Ansage Einspielung” (“*Repeat count*”) field to 3, to repeat the alarm message 3 times.



Aktionen
Titel
Alarm
Alarm with DTMF ack
Info
Record message

Parameter der Aktion 'Alarm'	
Aktion	Alarmierung
Auslöser	Anruf
Gruppe Auslöser	*
Nachwahl	8400001
Priorität	hoch
Ident Rufnummer	8400999
Begrüssungs Ansage	FireAlarmInitiated
Aktion starten	sofort bei Anruf
Gruppe	Group A
eMail versenden?	Aus
SMS versenden?	Aus
Ansage Einspielung	3 mal
Rufzeit	10 s
Anzahl Rufwiederholungen	3
Besetzt Wiederholzeit [s]	20
Min. Hörzeit	2 s
Ansage	Fire!
Folgeaktion positiv	keine Aktion
Folgeaktion negativ	keine Aktion
Positive Schwelle bei [%]	0
Positive Schwelle anz.	0
Anzahl Kanäle für Aktion	0

Figure 21: Parameters for Predefined Alarm

3.5.6. Create an Ad-Hoc Alarm

Create an alarm action which allows a caller to record a message which is played to a group of users.

1. Select the "Aktionen" ("*Actions*") control from the left frame of the main menu. When the "Aktionen" menu appears, enter the information as show in the following steps.
2. From the "Aktionen" menu, create the action "AdHocAlarm", and set the parameters as shown in the following steps.
3. Set the "Aktion" field to "Ad hoc Alarmierung" ("*Ad hoc alarm*")
4. Set the "Auslöser" ("*Trigger*") field to "Anruf" ("*Call*") to initiate upon call.
5. Set the "Nachwahl" field to "8400050" to set the number which triggers this action.
6. Set the "Begrüssungs Ansage" ("*Greeting*") to "SpeakMessageNow", to play the recorded message which requests the caller to speak the message which is to be propagated.
7. Set the group of extensions which are to be called with the message in the "Gruppe" ("*Group*") field.

Aktionen

	Titel
	Alarm
	Alarm with DTMF ack
	Info
	Record message
▶	AdHocAlarm
*	

Parameter der Aktion 'AdHocAlarm'

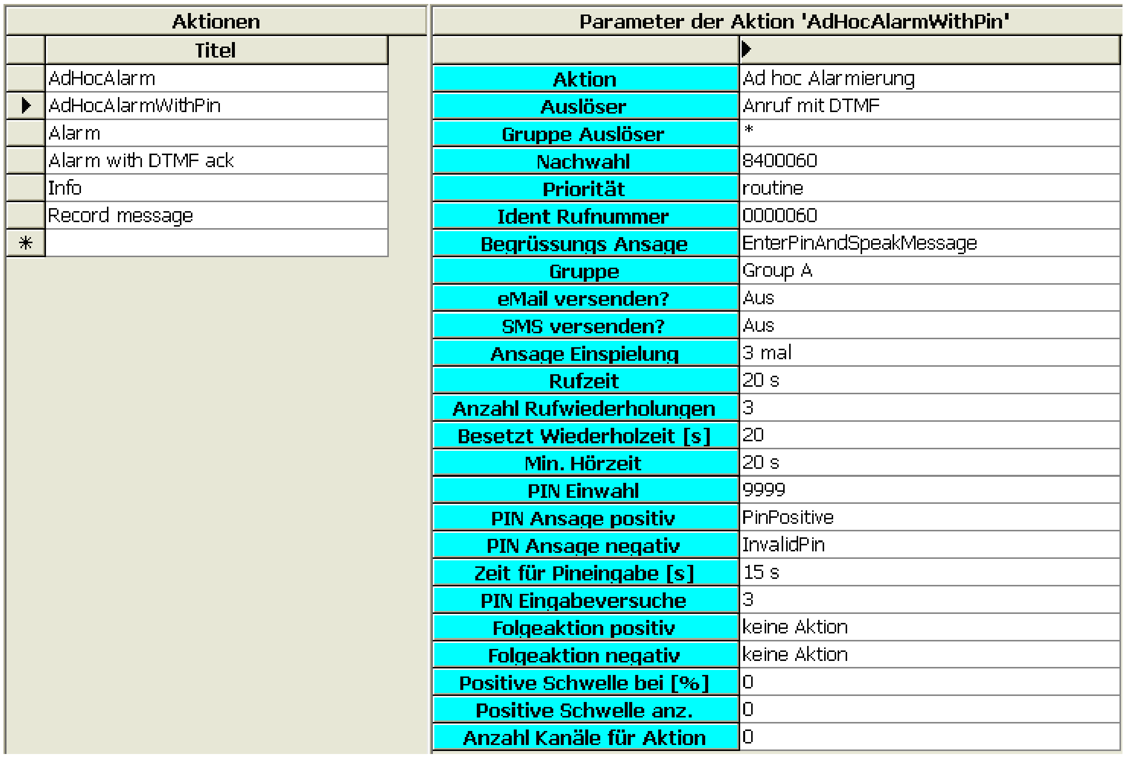
Aktion	Ad hoc Alarmierung
Auslöser	Anruf
Gruppe Auslöser	*
Nachwahl	8400050
Priorität	routine
Ident Rufnummer	8400050
Begrüssungs Ansage	SpeakMessageNow
Gruppe	Group A
eMail versenden?	Aus
SMS versenden?	Aus
Ansage Einspielung	3 mal
Rufzeit	15 s
Anzahl Rufwiederholungen	2
Besetzt Wiederholzeit [s]	0
Min. Hörzeit	max
Folgeaktion positiv	keine Aktion
Folgeaktion negativ	keine Aktion
Positive Schwelle bei [%]	0
Positive Schwelle anz.	0
Anzahl Kanäle für Aktion	0

Figure 22: Parameters for Ad Hoc Alarm

3.5.7. Create an Ad-Hoc Alarm with PIN Authorization

Create an alarm action which allows a caller to record a message which is played to a group of users after authorization with the caller's PIN code.

1. Select the "Aktionen" ("*Actions*") control from the left frame of the main menu. When the "Aktionen" menu appears, enter the information as show in the following steps.
2. From the "Aktionen" menu, create the action "AdHocAlarmWithPin", and set the parameters as shown in the following steps.
3. Set the "Aktion" field to "Ad hoc Alarmierung" ("*Ad hoc alarm*")
4. Set the "Auslöser" ("*Trigger*") field to "Anruf mit DTMF" ("*Call with DTMF*") to initiate upon call.
5. Set the "Nachwahl" field to "8400060" to set the number which triggers this action.
6. Set the "Begrüssungs Ansage" ("*Greeting*") to "EnterPinAndSpeakMessage", to play the recorded message which requests the caller to enter the PIN code and speak the message which is to be propagated.
7. Set the group of extensions which are to be called with the message in the "Gruppe" ("*Group*") field.



Aktionen
Titel
AdHocAlarm
AdHocAlarmWithPin
Alarm
Alarm with DTMF ack
Info
Record message

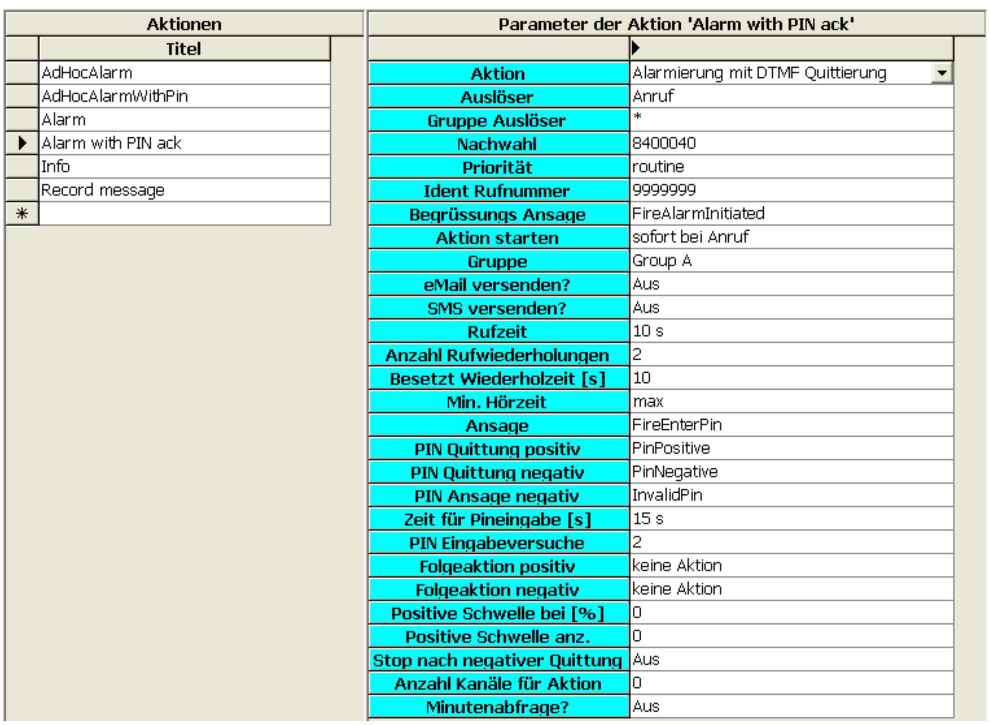
Parameter der Aktion 'AdHocAlarmWithPin'	
Aktion	Ad hoc Alarmierung
Auslöser	Anruf mit DTMF
Gruppe Auslöser	*
Nachwahl	8400060
Priorität	routine
Ident Rufnummer	0000060
Begrüssungs Ansage	EnterPinAndSpeakMessage
Gruppe	Group A
eMail versenden?	Aus
SMS versenden?	Aus
Ansage Einspielung	3 mal
Rufzeit	20 s
Anzahl Rufwiederholungen	3
Besetzt Wiederholzeit [s]	20
Min. Hörzeit	20 s
PIN Einwahl	9999
PIN Ansage positiv	PinPositive
PIN Ansage negativ	InvalidPin
Zeit für Pineingabe [s]	15 s
PIN Eingabeversuche	3
Folgeaktion positiv	keine Aktion
Folgeaktion negativ	keine Aktion
Positive Schwelle bei [%]	0
Positive Schwelle anz.	0
Anzahl Kanäle für Aktion	0

Figure 23: Parameters for Ad Hoc Alarm with PIN

3.5.8. Create Alarm with Confirmation

Create an alarm that can be accepted or rejected by called parties via a positive or negative PIN code. The caller initiates a fixed alarm message which is played to a group of users, each of whom can accept or reject the message.

1. Select the “Aktionen” (“*Actions*”) control from the left frame of the main menu. When the “Aktionen” menu appears, enter the information as show in the following steps.
2. From the “Aktionen” menu, create the action “Alarm with PIN ack”, and set the parameters as shown in the following steps.
3. Set the “Aktion” field to “Alarmiering mit DTMF Quitterung” (“*Alarm with confirmation*”)
4. Set the “Auslöser” (“*Trigger*”) field to “Anruf” (“*Call*”) to initiate upon call.
5. Set the “Nachwahl” field to “8400040” to set the number which triggers this action.
6. Set the “Begrüssungs Ansage” (“*Greeting*”) to “FireAlarmInitiated”, to play the recorded message which informs the caller that the alarm has been initiated.
7. Set the group of extensions which are to be called with the message in the “Gruppe” field.
8. Set the “PIN Quittung positiv” (“*Positive PIN*”) field to “PinPositive” to confirm acceptance to the called party with an audio message.
9. Set the “PIN Quittung negativ” (“*Negative PIN*”) field to “PinNegative” to confirm rejection to the called party with an audio message.
10. Set the “PIN Ansage negativ” (“*Invalid PIN message*”) field to “InvalidPin” to inform the called party that the PIN which was input was neither the positive nor the negative PIN.



Aktionen
Titel
AdHocAlarm
AdHocAlarmWithPin
Alarm
Alarm with PIN ack
Info
Record message

Parameter der Aktion 'Alarm with PIN ack'	
Aktion	Alarmierung mit DTMF Quittierung
Auslöser	Anruf
Gruppe Auslöser	*
Nachwahl	8400040
Priorität	routine
Ident Rufnummer	9999999
Begrüssungs Ansage	FireAlarmInitiated
Aktion starten	sofort bei Anruf
Gruppe	Group A
eMail versenden?	Aus
SMS versenden?	Aus
Rufzeit	10 s
Anzahl Rufwiederholungen	2
Besetzt Wiederholzeit [s]	10
Min. Hörzeit	max
Ansage	FireEnterPin
PIN Quittung positiv	PinPositive
PIN Quittung negativ	PinNegative
PIN Ansage negativ	InvalidPin
Zeit für Pineingabe [s]	15 s
PIN Eingabeversuche	2
Folgeaktion positiv	keine Aktion
Folgeaktion negativ	keine Aktion
Positive Schwelle bei [%]	0
Positive Schwelle anz.	0
Stop nach negativer Quittung	Aus
Anzahl Kanäle für Aktion	0
Minutenabfrage?	Aus

Figure 24: Parameters for Ad Hoc Alarm with PIN

3.5.9. Create Alarm with Reaction Time Input

Create an alarm to which the called party can enter the time required before response to the alarm can begin.

1. Select the “Aktionen” (“*Actions*”) control from the left frame of the main menu. When the “Aktionen” menu appears, enter the information as show in the following steps.
2. From the “Aktionen” menu, create the action “AlarmWithPinAndResponseQuery”, and set the parameters as shown in the following steps.
3. Set the “Aktion” field to “Alarmiering mit DTMF Quitterung” (“*Alarm with DTMF confirmation*”)
4. Set the “Auslöser” field to “Anruf” to initiate upon call.
5. Set the “Nachwahl” (“*Extension*”) field to “8400041” to set the number which triggers this action.
6. Set the “Begrüssungs Ansage” (“*Greeting*”) to “FireAlarmInitiated”, to play the recorded message which informs the caller that the alarm has been initiated.
7. Set the group of extensions which are to be called with the message in the “Gruppe” field.
8. Set the “PIN Quittung positiv” (“*PIN positive*”) field to “PinPositive” to confirm acceptance to the called party with an audio message.
9. Set the “PIN Quittung negativ” (“*PIN negative*”) field to “PinNegative” to confirm rejection to the called party with an audio message.
10. Set the “PIN Ansage negativ” (“*PIN invalid*”) field to “InvalidPin” to inform the called party that the PIN which was input was neither the positive nor the negative PIN.
11. Set the “Stop nach negativer Quittung” (“*Stop after negative confirmation*”) field to “Ein” (“*On*”) to not request a reaction if the message is rejected by the called party.
12. Set the “Minutenabfrage?” (“*Reaction time query?*”) field to “Ein” (“*On*”)to request that the called party enter a reaction time in minutes.

Aktionen
Titel
AdHocAlarm
AdHocAlarmWithPin
AdhocConference
Alarm
Alarm with PIN ack
Info
Record message
AlarmWithPinAndResponseQuery

Parameter der Aktion 'AlarmWithPinAndResponseQuery'	
Aktion	Alarmierung mit DTMF Quittierung
Auslöser	Anruf
Gruppe Auslöser	*
Nachwahl	8400041
Priorität	routine
Ident Rufnummer	9999999
Begrüssungs Ansage	FireAlarmInitiated
Aktion starten	sofort bei Anruf
Gruppe	Group A
eMail versenden?	Aus
SMS versenden?	Aus
Rufzeit	10 s
Anzahl Rufwiederholungen	2
Besetzt Wiederholzeit [s]	10
Min. Hörzeit	max
Ansage	FireEnterPin
PIN Quittung positiv	PinPositive
PIN Quittung negativ	PinNegative
PIN Ansage negativ	InvalidPin
Zeit für Pineingabe [s]	15 s
PIN Eingabeversuche	2
Folgeaktion positiv	keine Aktion
Folgeaktion negativ	keine Aktion
Positive Schwelle bei [%]	0
Positive Schwelle anz.	0
Stop nach negativer Quittung	Ein
Anzahl Kanäle für Aktion	0
Minutenabfrage?	Ein

Figure 25: Parameters for Alarm with PIN and Response Query

The message requesting and the number of digits to be entered by the called party are specified as shown below.

1. Select the "Serverparameter" ("*Server parameter*") control from the left frame of the main menu.
2. When the "Servereinstellungen" ("*Server settings*") menu appears, enter the information as show in the following step in the "Globale Einstellungen" *("Global settings*") form at the bottom of the menu.
3. Set the "Start Minutenabfrage" ("*Start minutes enquiry*") field to "EnterReactionTime" to specify the message which requests the reaction time in minutes.
4. Set the "Ende Minutenabfrage" ("*End minutes enquiry*") field to "ThanksForReactionDigits" to specify the message which acknowledges the input digits by the called party.
5. Set the "Anzahl Ziffern für" ("*Digit Count*") field to "2" to specify a two digit minute delay time.
6. Click the "Speichern" ("*Save*") button to save these settings.

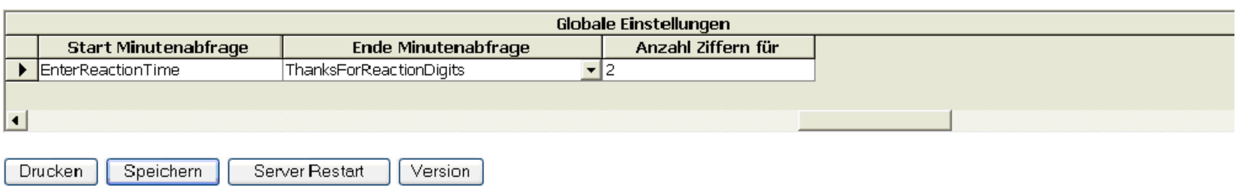


Figure 26: Parameters Global Settings

3.5.10. Create Conference with Participation of Initiator

Create an emergency conference which is to be initiated when a specific number is dialed, at which time the members are called and added to a conference which includes the initiator of this action.

1. Select the "Aktionen" ("*Actions*") control from the left frame of the main menu. When the "Aktionen" menu appears, enter the information as show in the following steps.
2. From the "Aktionen" menu, create the action "Emergency Conference", and set the parameters as shown in the following steps.
3. Set the "Aktion" field to "Konference mit Auslöser and Einwahl" ("*Conference with initiator by call*")
4. Set the "Auslöser" ("*Trigger*") field to "Anruf" ("*Call*") to initiate upon call.
5. Set the "Nachwahl" ("*Extension*") field to "8400070" to set the number which triggers this action.
6. Set the "Ident Rufnummer" ("*Caller ID number*") field to "8400070" to set the number which is shown to the caller.
7. Set the "Begrüssungs Ansage" ("*Greeting*") to "WelcomeToConference", to play the recorded message which informs the calling party that a conference has been initiated.
8. Set the group of extensions which are to be called with the message in the "Gruppe" field.
9. Set the "Begrüssungs Ansage" to "WelcomeToConference", to play the recorded message which informs the called parties that a conference has been initiated.
10. Set the "Konferenz Schlussansage" ("*Conference termination message*") field to "ConferenceEnd" to specify the message to be played when the conference has ended.

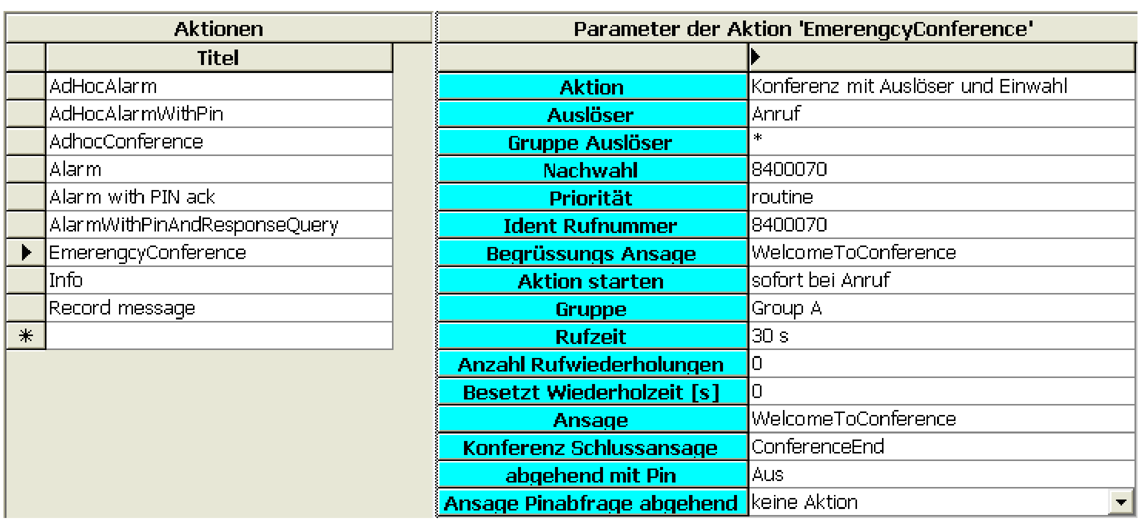


Figure 27: Parameters Emergency Conference

3.5.11. Create Conference Initiated by the Boss

Create an emergency conference which is to be initiated when specific number is dialed, at which time the members are called and added to a conference which includes the initiator of this action. When the initiator of the conference goes on-hook, all calls are terminated.

1. Select the “Aktionen” (“*Actions*”) control from the left frame of the main menu. When the “Aktionen” menu appears, enter the information as show in the following steps.
2. From the “Aktionen” menu, create the action “Emergency Conference”, and set the parameters as shown in the following steps.
3. Set the “Aktion” (“*Action*”) field to “Chefkonferenz” (“*Boss conference*”)
4. Set the “Auslöser” (“*Trigger*”) field to “Anruf” (“*Call*”) to initiate upon call.
5. Set the “Nachwahl” field to “8400071” to set the number which triggers this action.
6. Set the “Ident Rufnummer” (“*Caller ID*”) field to “8400070” to set the number which is shown to the caller.
7. Set the “Begrüssungs Ansage” (“*Greeting*”) to “WelcomeToConference”, to play the recorded message which informs the calling party that a conference has been initiated..
8. Set the group of extensions which are to be called with the message in the “Gruppe” (“*Group*”) field.
9. Set the “Begrüssungs Ansage” to “WelcomeToConference”, to play the recorded message which informs the called parties that a conference has been initiated..
10. Set the “Konferenz Schlussansage” (“*Conference termination message*”) field to “ConferenceEnd” to specify the message to be played when the conference has ended.

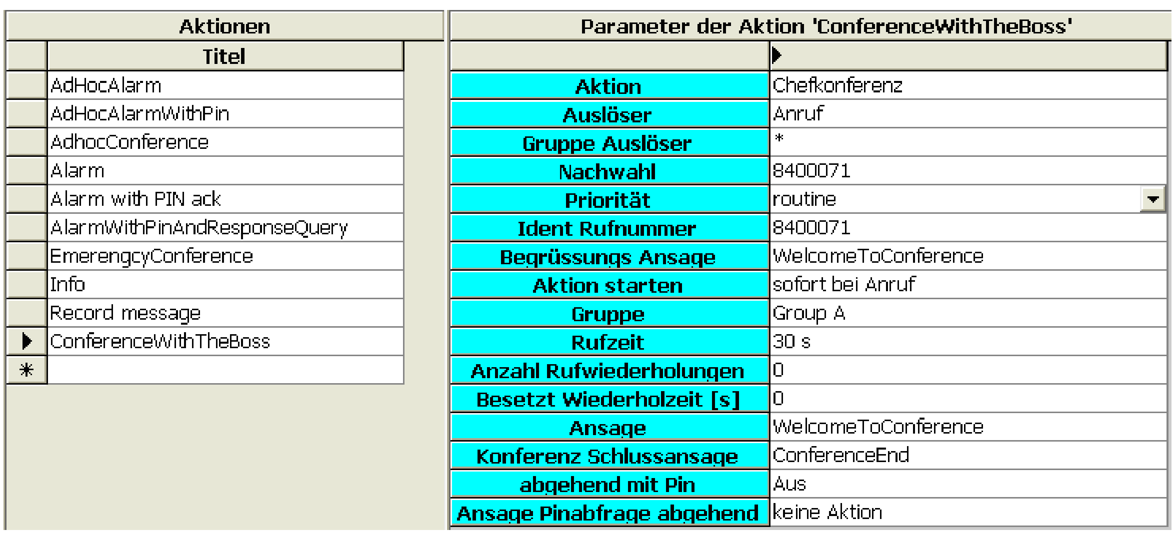


Figure 28: Parameters Emergency Boss Conference

4. Interoperability Compliance Testing

The objective of the compliance testing performed on the TAS ARUTEL product was to verify that it is compatible with Avaya Communication Manager. This includes verifying that the essential ARUTEL features function properly when used with Avaya Communication Manager, and that Avaya Communication Manager features are not hindered by the interaction with ARUTEL. Furthermore, ARUTEL's robustness was verified.

4.1. General Test Approach

The test method employed can be described as follows:

- Avaya Communication Manager was configured to support various local IP telephones.
- The individual features of the ARUTEL were tested by manually making calls to the unit and manually answering and verifying the voice message content of the resulting calls generated by the unit.
- ARUTEL's robustness was tested by verifying its ability to recover from interruptions to its external connections including:
  - The LAN connection between the ARUTEL and the network
  - The LAN connection between the ASC CTI Controller and the network
- ARUTEL's robustness was further tested by verifying the ability to recover from power interruptions to the following components:
  - The ARUTEL server
  - The Avaya Communication Server to which the ARUTEL is attached.

All testing was performed manually. The tests were all functional in nature, and no performance testing was done.

4.2. Test Results

The following capabilities of the ARUTEL were tested for proper interoperation with Avaya Communication Manager:

- Alarm with predefined message content
- Ad-hoc alarm
- Ad-hoc alarm with PIN authorization
- Alarm with confirmation
- Alarm with reaction time input
- Conference with participation of initiator
- Conference initiated by the boss

All tests which were performed produced the expected result.

5. Verification Steps

The following steps can be performed to verify the correct installation and configuration of ARUTEL:

- Verify that the Avaya SES and ARUTEL systems can ping each other
- Verify that the various telephones can call each other
- Verify that it is possible to generate an alarm from the ARUTEL which produces a voice message on an Avaya telephone.

6. Support

Support for ARUTEL is available at:

TAS Gmbh & C. KG
Langmaar 25
41238 Mönchengladbach
Phone: +49 2166 858 0
Fax: +49 2166 858 150
Email: info@tas.de
http://www.tas.de

7. References

[1] "Feature Description and Implementation for Avaya Communication Manager", 555-245-205, Issue 3, June 2005
[2] "Administrator Guide for Avaya Communication Manager", 03-300509, Issue 1, June 2005
[3] "Installing and Administering SIP Enablement Services R3.1.1", 03-600768, Issue 2.0, August 2006
[4] "SIP Support in Release 3.1 of Avaya Communication Manager", 555-245-206, Issue 6, February 2006

8. Conclusion

These Application Notes describe the conformance testing of the TAS ARUTEL alarm system with Avaya Communication Manager and Avaya SES. The various features of the ARUTEL unit which involve its telephone interface were tested. A detailed description of the configuration required for both the Avaya and the TAS equipment is documented within these Application Notes. The ARUTEL passed all of the tests performed, which included both functional and robustness tests.

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 Developer*Connection* Program at devconnect@avaya.com.