Application Notes for NICE Perform® version 3.5 with Avaya Aura® Session Border Controller, Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services – Issue 1.0

Abstract

These Application Notes describe a compliance-tested configuration consisting of NICE Perform® with Avaya Aura® Session Border Controller, Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services.

NICE Perform® effectively provides a Selective SIP Trunk-Side audio recording solution which leverages the media replication capabilities of Avaya Aura® Session Border Controller. The solution uses CTI events from Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services to identify which media sessions are to be recorded based on a set of user definable business rules.

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 a compliance-tested configuration consisting of NICE Perform® with Avaya Aura® Session Border Controller, Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services.

The purpose of this integration option of Perform is to provide a scalable audio recording solution for enterprises requiring conversations with external parties be recorded for compliance or training purposes. Unlike many recording solutions, the integration with the Session Border Controller enables capture of audio calls at the network ingress/egress point when SIP trunk facilities are used. This approach has the advantage of being less taxing on communication system resources. Similar to TDM Trunk-Side recording solutions, the internal call segments between parties within the enterprise, including consultative legs of conference or transfer calls cannot be captured using the tested method. NICE offers alternative solutions for capturing internal call segments, and the combination of solutions is capable of creating a playback experience which blends recordings from multiple sources into a seamless playback experience. These other solutions were not the focus of, nor included in this compliance test.

In order for the Perform application to be able to identify which sessions to request audio streams for, the Universal Call Identifier (UCID) is extracted from CTI events obtained by monitoring internal devices (stations, ACD hunt groups and VDNs). In the tested configuration, the TSAPI service offered on Application Enablement Services was used for this purpose. All calls originating from within the enterprise have a UCID which is passed in the SIP headers from Communication Manager and Session Manager. For inbound calls, the Session Border Controller was configured with a policy to create a UCID for inbound calls that do not already have one, and to leave the UCID intact for inbound calls that do have this information passed over the public networks.

2. General Test Approach and Test Results

The compliance test focused on the interoperability between NICE Perform® and Avaya Aura® Session Border Controller. Additionally, the interface with Avaya Aura® Application Enablement Services was configured in order to enable the application to subscribe to event notification services for the internal devices. Although other elements were present such as SIP, H.323, Digital and Analog Endpoints, Avaya Aura® Communication Manager, and Avaya Aura® Session Manager, the configuration of these elements was not directly related to the interoperability of the tested solution and are not covered in detail in these notes.

2.1. Interoperability Compliance Testing

The focus of the compliance test was to confirm inbound and outbound calls could be successfully recorded. Additional test conditions were included to verify the functionality of typical call scenarios such as conference and transfer, bridged call appearances, and basic EC500 call scenarios. Serviceability testing included disconnecting Communication Manager and Application Enablement Services as well as Perform from the network, rebooting these servers as well as rebooting the Session Border Controller and Session Manager to confirm that the application was capable of recovering from typical outages.

2.2. Test Results

The objectives of the test were verified. Inbound calls both with, and without UCID being passed over the public networks were successfully recorded demonstrating the effectiveness of the UCID rules on the Session Border Controller policies. Transferred and Conferenced calls were successfully recorded throughout the life of the call with the noted exception below. For serviceability testing, the Perform solution was able to resume recording shortly after service outages.

As is expected with Trunk-Side recording solutions, internal call segments, including the temporary legs of consultative conference and transfer calls resulted in silence as these audio streams do not pass through the Session Border Controller. Calls to desk phones with EC500 activated to alert a mapped external phone (typically a cell phone) were successfully recorded whether picked up on either the desk or cell phone. More complex EC500 scenarios such as handoffs between endpoints were not tested as they are not fully supported by Avaya at this time.

2.3. Support

Technical support for NICE Perform in the Americas can be obtained at:

- Phone: + 1 800 642 3611
- Email: support.americas@nice.com
- Web: www.nice.com/support
- Other Regions: See www.nice.com for information on contacts outside of the Americas.

3. Reference Configuration

The compliance test configuration included a Primary Site consisting of Avaya Aura® Communication Manager, Avaya Aura® Session Manager and Avaya Aura® Application Enablement Services with several SIP, H.323 and TDM endpoints. The Primary Site used SIP trunks for signaling and call routing to and from Communication Manager and Session Manager, as well as a SIP Entity Link between Session Manager and Session Border Controller. A second site was configured with Communication Manager with SIP Trunk facilities to simulate a SIP public network service. All calls to and from the public network routed through Session Border Controller.

The NICE Perform® solution was installed on a single Windows 2003 Server including the Logger, and CLS/Interactions Center servers which are often deployed on multiple servers for scalability and other design considerations.

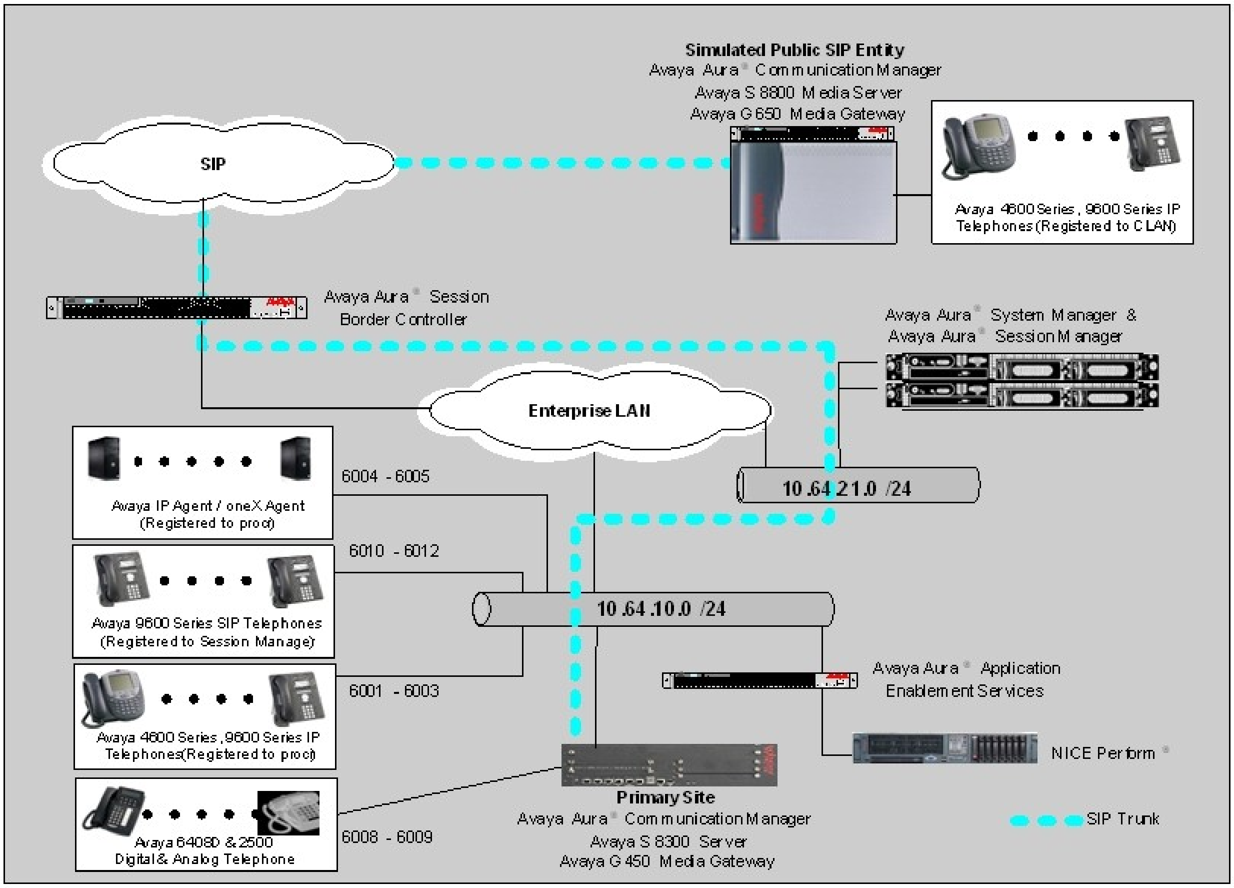

Simulated Public SIP Entity
Avaya Aura® Communication Manager
Avaya S8800 Media Server
Avaya G650 Media Gateway
SIP
Avaya 4600 Series, 9600 Series IP Telephones (Registered to CLAN)
Avaya Aura® Session Border Controller
Avaya Aura® System Manager & Avaya Aura® Session Manager
Enterprise LAN
6004 - 6005
Avaya IP Agent / oneX Agent (Registered to proc)
10.64.21.0 /24
6010 - 6012
Avaya 9600 Series SIP Telephones (Registered to Session Manage)
10.64.10.0 /24
Avaya Aura® Application Enablement Services
6001 - 6003
Avaya 4600 Series, 9600 Series IP Telephones(Registered to proc)
NICE Perform®
Primary Site
Avaya Aura® Communication Manager
Avaya S8300 Server
Avaya G450 Media Gateway
SIP Trunk
Avaya 6408D & 2500 Digital & Analog Telephone
6008 - 6009

Figure 1 – NICE Perform® Compliance Test Configuration

4. Equipment and Software Validated

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

Equipment	Version
Avaya Aura® System Manager On Dell™ PowerEdge™ R610 Server	6.1 (6.1.6.1.1087) Avaya System Platform 6.0.3.1.3
Avaya Aura® Session Manager On HP ProLiant DL360 G7 Server	6.1 (6.1.3.0.613006)
Avaya Aura® Session Border Controller On Avaya S8800 Server	6.0.0.1.5 (E362) Avaya System Platform 6.0.1.0.5
Avaya Aura® Communication Manager On Avaya S8300D Server	R016x.00.1.510.1, Update 19009 (SP3) (Avaya Aura® System Platform: 6.0.3.1.3)
Avaya Aura® Application Enablement Services on S8500B Server	6.1.0 Super Patch 2
Avaya G450 Media Gateway	31.11.1/1
Avaya 9600 Series SIP Phones	SIP 2.6
Avaya 9600 Series H.323 Phones	H.323 3.11
Analog Phone	-
NICE Perform® On HP DL380 G5 Server Microsoft Windows 2003R2 Server	3.5

5. Configure Avaya Aura® Communication Manager

Communication Manager used an existing configuration with SIP trunks to connect to Avaya Aura® Session Manager. Configuration of this aspect of the integration was standard and not directly relevant to the interoperability of NICE Perform®. Therefore, this aspect of the configuration will not be covered in these notes.

The steps necessary to configure Avaya Aura® Application Enablement Services interfaces to Communication Manager are described below.

5.1. Communication Manager Configuration Details

All the configuration changes in this section for Communication Manager are performed through the System Access Terminal (SAT) interface. For more information on configuring Communication Manager, refer to the Avaya product documentation, Reference **[1].**

This section provides the procedures for configuring Communication Manager. The procedures are as follows:

- Verify Feature and License are adequate for the integration
- Administer Processor Ethernet Interface for Application Enablement Services connectivity
- Administer Communication Manager System Features
- Administer Computer Telephony Integration (CTI) Link
- Confirm Station Administration
- Ensure Shared UUI is Passed Over External Trunk Facilities

The detailed administration of contact center entities, such as VDN, Skill, Split, Logical Agents and Station Extensions are assumed to be in place and are not covered in this document.

1. **Verify Feature and License are adequate for the integration**

Applications that use Application Enablement Services TSAPI must have **Computer Telephony Adjunct Links** enabled on Communication Manager. This feature entitlement is provided with each TSAPI license. TSAPI entitlements must be activated in both licenses. If this option is not set to ***y***, contact the Avaya sales team or business partner for a proper license file.

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

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

2. **Administer Processor Ethernet Interface for Application Enablement Services Connectivity**

Enter the **change node-names ip** command. The Application Enablement Services and **procr** node-names need to be defined here.

```
change node-names ip                                            Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
aesserver2          10.64.10.21
default             0.0.0.0
procr               10.64.10.67
procr6              ::
```

On most R6 servers, the Processor Ethernet Interface will already be administered in the ip-interface list. The **display ip-interface procr** command will display the parameters of the Processor Ethernet Interface.

```
display ip-interface procr                                     Page   1 of   2
                                  IP INTERFACES

                  Type: PROCR
                                                       Target socket load: 4800

      Enable Interface? y                           Allow H.323 Endpoints? y
                                                     Allow H.248 Gateways? y
        Network Region: 1                              Gatekeeper Priority: 5

                                 IPV4 PARAMETERS
             Node Name: procr                     IP Address: 10.64.10.67

           Subnet Mask: /24
```

```
display ip-interface procr                                     Page   2 of   2
                                  IP INTERFACES

                 Speed: 100Mbps
                Duplex: Full

                                 IPV6 PARAMETERS
             Node Name: procr6
            IP Address: ::

           Subnet Mask: /64
      Enable Interface? n
```

3. **Administer Processor Ethernet Interface for Application Enablement Services Connectivity (Continued)**

Add an entry for Application Enablement Services as described below:

- Enter the **change ip-services** command.
- In the **Service Type** field, type ***AESVCS***.
- In the **Enabled** field, type ***y***.
- In the **Local Node** field, type the Node name ***procr*** for the Processor Ethernet Interface.
- In the **Local Port** field, use the default of ***8765***.
- Note that in installations using CLAN connectivity, each CLAN interface would require similar configuration, Reference **[2].**

```
change ip-services                                              Page   1 of   4

                                   IP SERVICES
 Service      Enabled     Local        Local        Remote       Remote
  Type                    Node         Port         Node         Port
AESVCS         y      procr            8765
CDR1                  procr            0        MTS              9000
CDR2                  procr            0        RDTT             9001
```

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

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

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

   Server ID    AE Services       Password          Enabled    Status
                   Server
      1:      aesserver2       *                     y        in use
```

Note that the name and password entered for the **AE Services Server** and **Password** fields must match the name and password on the Application Enablement Services server. The administered name for the Application Enablement Services server is created as part of the Application Enablement Services installation, and can be obtained from the Application Enablement Services server by typing ***uname –n*** at the Linux command prompt.

4. Administer Communication Manager System Features

Enter the **change system-parameters features** command and ensure that **Create Universal Call ID (UCID)** is enabled system wide on page 5, and that **Send UCID to ASAI** is set to ***y*** on Page 13. Also, note the **UCID Network Node ID** which will be used later in **Section 8.1, Step 3**. Perform relies on UCID to identify which sessions to record.

```
change system-parameters features                               Page   5 of  19
                        FEATURE-RELATED SYSTEM PARAMETERS

SYSTEM PRINTER PARAMETERS
  Endpoint:              Lines Per Page: 60

SYSTEM-WIDE PARAMETERS
                                     Switch Name:
            Emergency Extension Forwarding (min): 10
          Enable Inter-Gateway Alternate Routing? n
Enable Dial Plan Transparency in Survivable Mode? n
                              COR to Use for DPT: station

MALICIOUS CALL TRACE PARAMETERS
               Apply MCT Warning Tone? n   MCT Voice Recorder Trunk Group:
      Delay Sending RELease (seconds): 0
SEND ALL CALLS OPTIONS
     Send All Calls Applies to: station    Auto Inspect on Send All Calls? n
              Preserve previous AUX Work button states after deactivation? n
UNIVERSAL CALL ID
     Create Universal Call ID (UCID)? y    UCID Network Node ID: 1
```

```
change system-parameters features                               Page  13 of  19
                        FEATURE-RELATED SYSTEM PARAMETERS
 CALL CENTER MISCELLANEOUS
           Callr-info Display Timer (sec): 10
                        Clear Callr-info: next-call
        Allow Ringer-off with Auto-Answer? n

    Reporting for PC Non-Predictive Calls? n


          Interruptible Aux Notification Timer (sec): 3


  ASAI
            Copy ASAI UUI During Conference/Transfer? n
        Call Classification After Answer Supervision? n
                                   Send UCID to ASAI? y
          For ASAI Send DTMF Tone to Call Originator? y
```

5. Administer Computer Telephony Integration (CTI) Link

This section provides the steps required for configuring a CTI Link.

Enter the **add cti-link <link number>** command, where **<link number>** is an available CTI link number.

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

```
add cti-link 1                                                  Page   1 of   3
                                    CTI LINK
 CTI Link: 1
Extension: 6201
     Type: ADJ-IP
                                                                        COR: 1
     Name: AES-10.64.10.21
```

```
add cti-link 1                                                  Page   2 of   3
                                    CTI LINK
FEATURE OPTIONS
      Event Minimization? n        Special Character for Restricted Number? n
      IC Adjunct Routing? n   Send Disconnect Event for Bridged Appearance? n
                                             Two-Digit Aux Work Reason Codes? n
                                                 Block CMS Move Agent Events? n
```

```
add cti-link 1                                                  Page   3 of   3
                                    CTI LINK
Bridged Appearance Origination Restriction? n

            SAC/CF Override: n
```

6. Confirm Station Administration

All SIP stations that will be recorded must have **Type of 3PCC Enabled** set to ***Avaya*** in order for Application Enablement Services to properly send all call events to the application. If this is changed while the endpoint is registered, re-register the endpoint for this setting to completely take effect. Failure to register after changing this setting could result in unpredictable CTI message issues.

```
change station 6010                                                 Page   6 of
6
                                     STATION

SIP FEATURE OPTIONS
         Type of 3PCC Enabled: Avaya
                   SIP Trunk: aar
```

7. **Ensure Shared UUI is Passed Over External Trunk Facilities**

To ensure calls routed to the public network via Session Manager and Session Border Controller contain the UCID generated on Communication Manager, set the **Send UCID?** to ***y***, and **UUI Treatment** to ***shared*** on the third page on the trunk group that is used for routing calls to Session Manager. On the public side Communication Manager, these settings were identical, but the **UUI Treatment** was set to ***service-provider*** and **Send UCID** to ***n*** for some test cases to verify that the Session Border Controller would use the existing UCID, or add a UCID if none was present.

```
change trunk-group 30                                           Page   3 of  22
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                          Maintenance Tests? y



                     Numbering Format: unk-pvt
                                                UUI Treatment: shared
                                              Maximum Size of UUI Contents: 128
                                                 Replace Restricted Numbers? n
                                                Replace Unavailable Numbers? n


                                Modify Tandem Calling Number: no
               Send UCID? y



 Show ANSWERED BY on Display? y
```

6. Configure Avaya Aura® Application Enablement Services

Avaya Aura® Application Enablement Services enables applications to monitor and control telephony resources on Communication Manager. Application Enablement Services receives requests from applications and forwards them to Communication Manager. Conversely, Application Enablement Services receives responses and events from Communication Manager and forwards them to the appropriate applications.

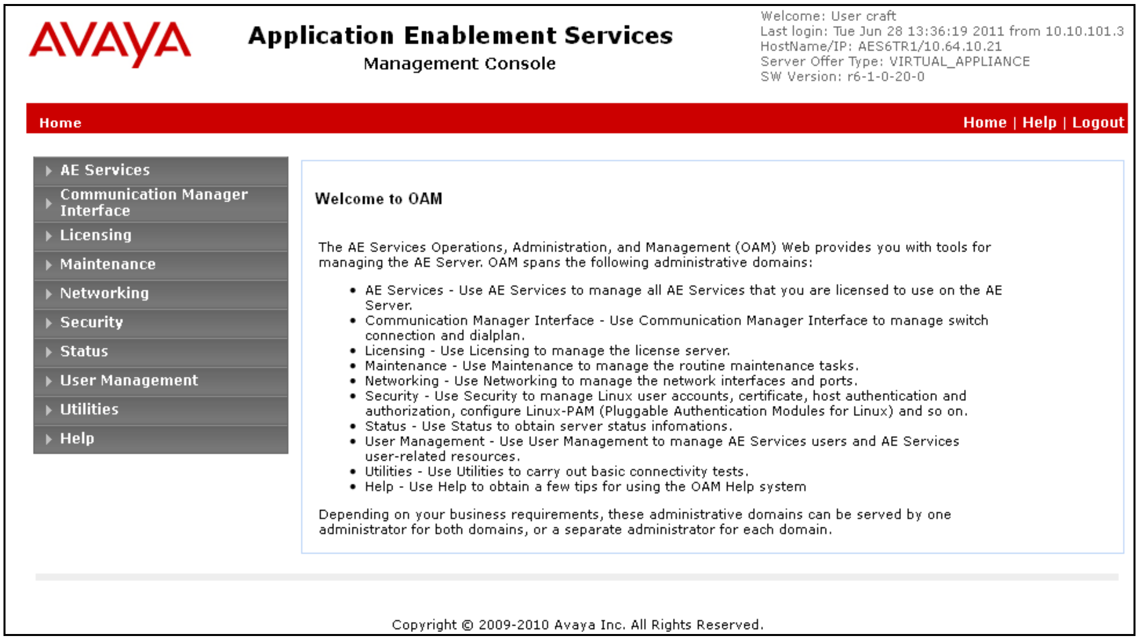
This section assumes that the installation and basic administration of Application Enablement Services has already been performed. For more information on administering Application Enablement Services, refer to the Avaya product documentation, Reference **[2]**.

6.1. Application Enablement Services Configuration Details

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

- Confirm Network Configuration
- Configure Communication Manager Switch Connections
- Verify TSAPI Licensing
- Add TSAPI Links
- Add CTI User
- Enable Unrestricted Access to the Security Database
- Note the T-Link Name

Access the web-based administration interface using **https://<ip-address>** in a browser where **<ip-address>** is the client interface address of the Application Enablement server. Log in using appropriate credentials. The **Welcome to OAM** screen is displayed upon login.



Welcome: User craft
Last login: Tue Jun 28 13:36:19 2011 from 10.10.101.3
HostName/IP: AES6TR1/10.64.10.21
Server Offer Type: VIRTUAL_APPLIANCE
SW Version: r6-1-0-20-0

Welcome to OAM

The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:

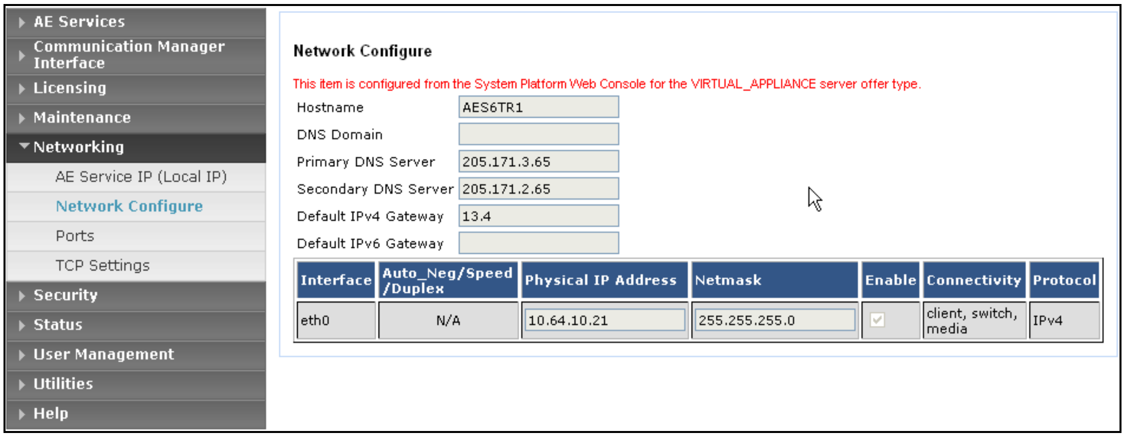
- AE Services - Use AE Services to manage all AE Services that you are licensed to use on the AE Server.
- Communication Manager Interface - Use Communication Manager Interface to manage switch connection and dialplan.
- Licensing - Use Licensing to manage the license server.
- Maintenance - Use Maintenance to manage the routine maintenance tasks.
- Networking - Use Networking to manage the network interfaces and ports.
- Security - Use Security to manage Linux user accounts, certificate, host authentication and authorization, configure Linux-PAM (Pluggable Authentication Modules for Linux) and so on.
- Status - Use Status to obtain server status infomations.
- User Management - Use User Management to manage AE Services users and AE Services user-related resources.
- Utilities - Use Utilities to carry out basic connectivity tests.
- Help - Use Help to obtain a few tips for using the OAM Help system

Depending on your business requirements, these administrative domains can be served by one administrator for both domains, or a separate administrator for each domain.

Copyright © 2009-2010 Avaya Inc. All Rights Reserved.

1. **Confirm Network Configuration**

Select **Networking > Network Configure** and note the client interface IP Address (**eth0** in this example) which will be used later in the application configuration. Application Enablement Services can be configured to use one or multiple NIC interfaces. It is preferable for security and performance reasons to use multiple interfaces and to have these on separate networks. The Communication Manager interface should always be bound to **eth0**.



Network Configure

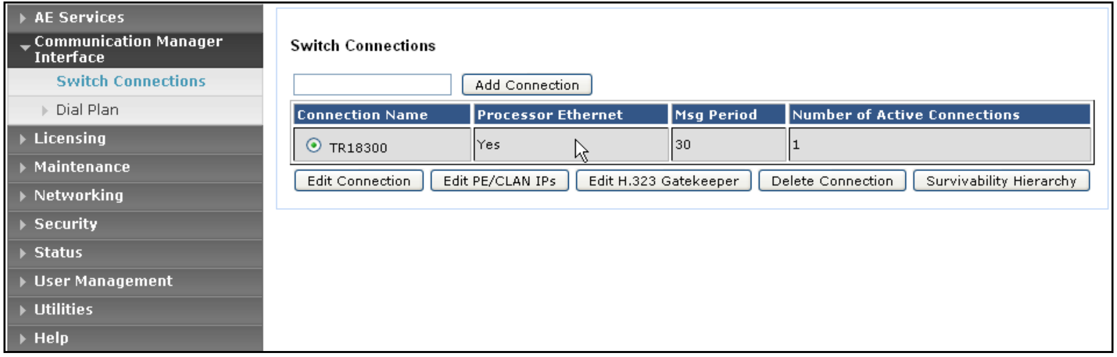
This item is configured from the System Platform Web Console for the VIRTUAL_APPLIANCE server offer type.

Hostname	AES6TR1
DNS Domain	
Primary DNS Server	205.171.3.65
Secondary DNS Server	205.171.2.65
Default IPv4 Gateway	13.4
Default IPv6 Gateway	

Interface	Auto_Neg/Speed /Duplex	Physical IP Address	Netmask	Enable	Connectivity	Protocol
eth0	N/A	10.64.10.21	255.255.255.0	☑	client, switch, media	IPv4

2. **Configure Communication Manager Switch Connections**

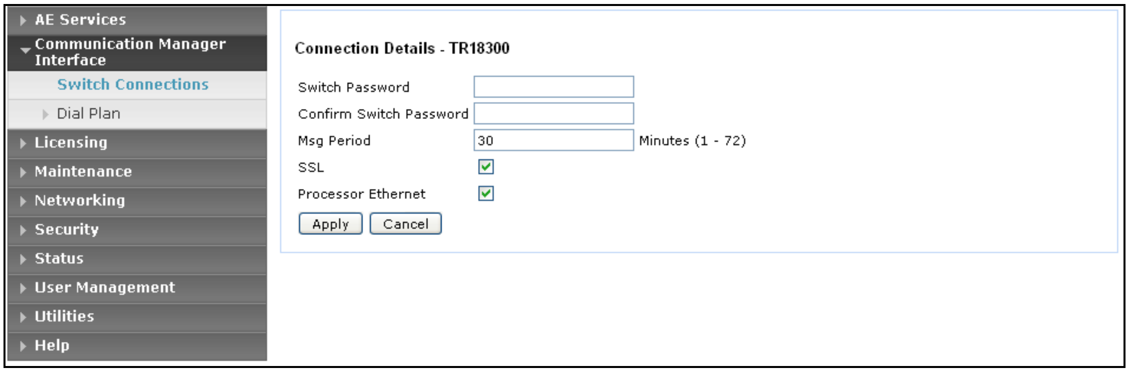
To add links for the Communication Manager, navigate to the **Communication Manager Interface > Switch Connections** page and enter a name for the new switch connection. This was previously configured as **TR18300** for this test environment:



Switch Connections

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

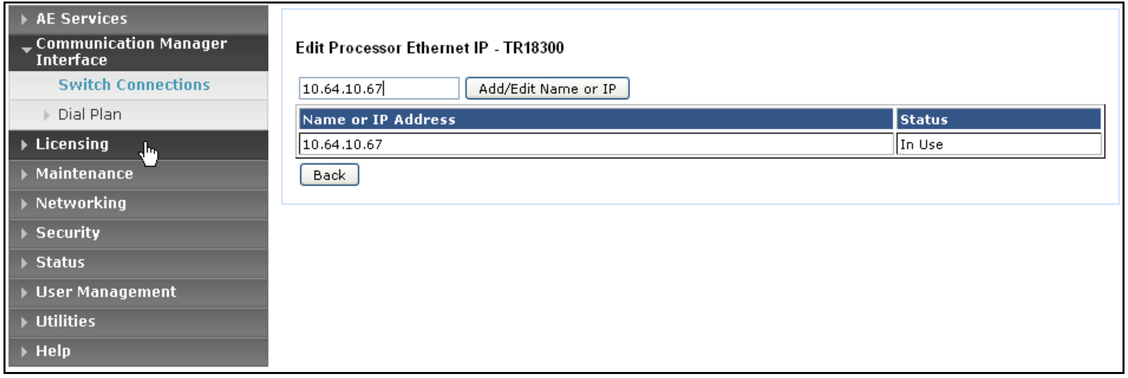
Use the **Edit Connection** button shown above to configure the **Switch Password**. This must match the password configured in **Section 5, Step.2** above. Enter the **Switch Password** and check the **Processor Ethernet** box if using the **procr** interface, as shown below.



Connection Details - TR18300

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

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



Edit Processor Ethernet IP - TR18300

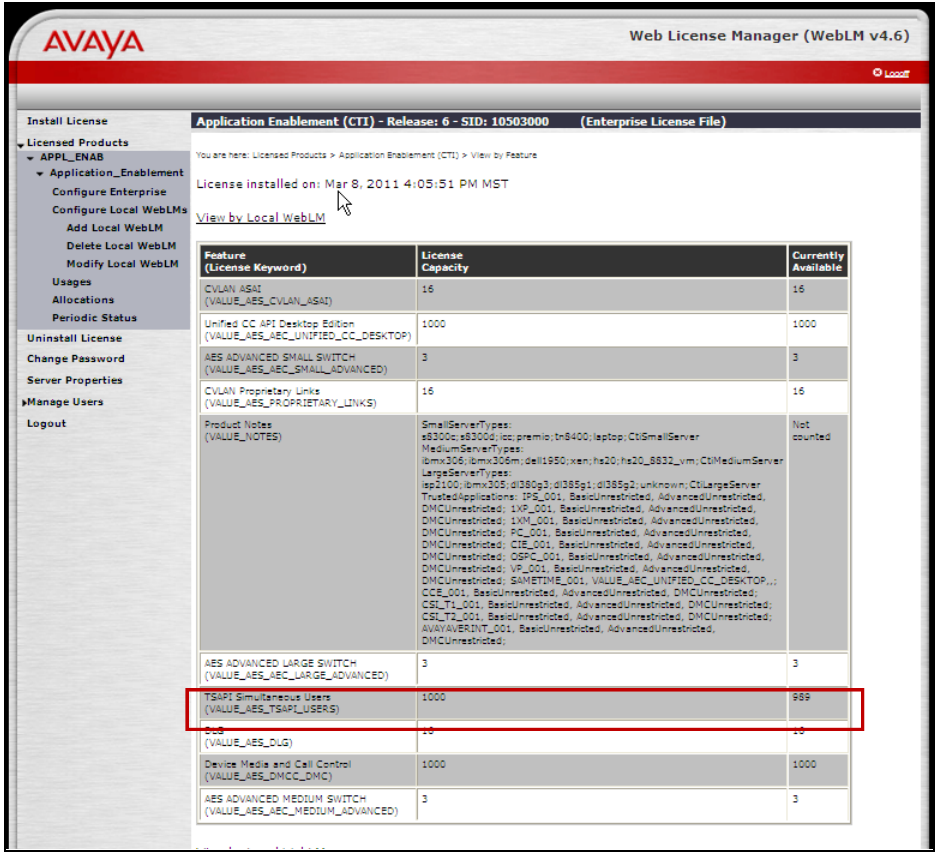
10.64.10.67

Name or IP Address	Status
10.64.10.67	In Use

3. Verify TSAPI Licensing

NICE Perform will consume a **TSAPI** license for each station and ACD Hunt Group that is to be monitored and recorded. If the number of licenses are not adequate for the integration, contact Avaya sales or an authorized reseller.

Navigate to **Licensing > WebLM Server Access** and log in using appropriate credentials. Select **Application_Enablement** under **Licensed Products > APPL_ENAB** to display entitlements and acquired licenses.



Application Enablement (CTI) - Release: 6 - SID: 10503000 (Enterprise License File)

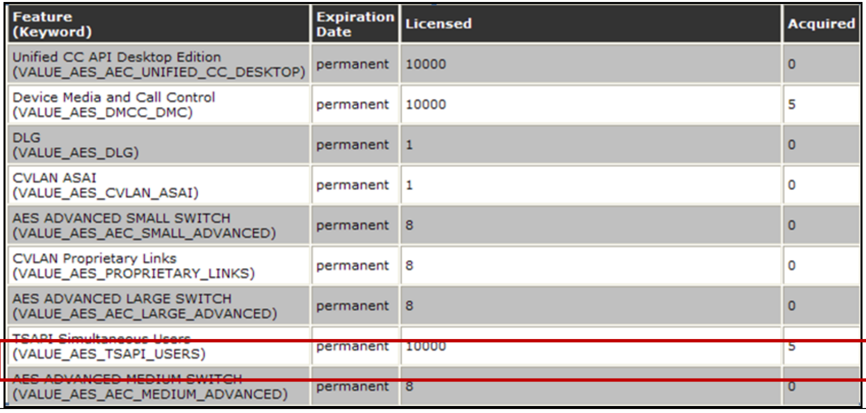
You are here: Licensed Products > Application Enablement (CTI) > View by Feature

License installed on: Mar 8, 2011 4:05:51 PM MST

View by Local WebLM

Feature (License Keyword)	License Capacity	Currently Available
CVLAN ASAI (VALUE_AES_CVLAN_ASAI)	16	16
Unified CC API Desktop Edition (VALUE_AES_AEC_UNIFIED_CC_DESKTOP)	1000	1000
AES ADVANCED SMALL SWITCH (VALUE_AES_AEC_SMALL_ADVANCED)	3	3
CVLAN Proprietary Links (VALUE_AES_PROPRIETARY_LINKS)	16	16
Product Notes (VALUE_NOTES)	SmallServerTypes: s8300c;s8300d;icc;premio;tn8400;laptop;CtiSmallServer MediumServerTypes: ibmx306;ibmx306m;dell1950;xen;hs20;hs20_8832_vm;CtiMediumServer LargeServerTypes: isp2100;ibmx305;dl380g3;dl385g1;dl385g2;unknown;CtiLargeServer TrustedApplications: IPS_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; 1XP_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; 1XM_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; PC_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CIE_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; OSPC_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; VP_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; SAMETIME_001, VALUE_AEC_UNIFIED_CC_DESKTOP,,; CCE_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CSI_T1_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CSI_T2_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; AVAYAVERINT_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted;	Not counted
AES ADVANCED LARGE SWITCH (VALUE_AES_AEC_LARGE_ADVANCED)	3	3
TSAPI Simultaneous Users (VALUE_AES_TSAPI_USERS)	1000	989
DLG (VALUE_AES_DLG)	16	16
Device Media and Call Control (VALUE_AES_DMCC_DMC)	1000	1000
AES ADVANCED MEDIUM SWITCH (VALUE_AES_AEC_MEDIUM_ADVANCED)	3	3

The screenshot below gives a closer look at the license counts.



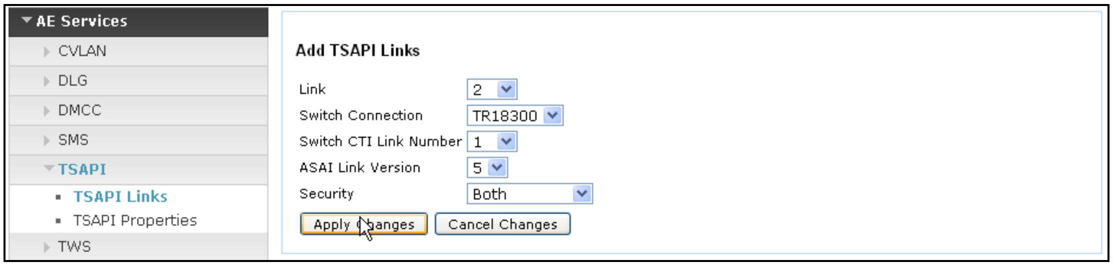
Feature (Keyword)	Expiration Date	Licensed	Acquired
Unified CC API Desktop Edition (VALUE_AES_AEC_UNIFIED_CC_DESKTOP)	permanent	10000	0
Device Media and Call Control (VALUE_AES_DMCC_DMC)	permanent	10000	5
DLG (VALUE_AES_DLG)	permanent	1	0
CVLAN ASAI (VALUE_AES_CVLAN_ASAI)	permanent	1	0
AES ADVANCED SMALL SWITCH (VALUE_AES_AEC_SMALL_ADVANCED)	permanent	8	0
CVLAN Proprietary Links (VALUE_AES_PROPRIETARY_LINKS)	permanent	8	0
AES ADVANCED LARGE SWITCH (VALUE_AES_AEC_LARGE_ADVANCED)	permanent	8	0
TSAPI Simultaneous Users (VALUE_AES_TSAPI_USERS)	permanent	10000	5
AES ADVANCED MEDIUM SWITCH (VALUE_AES_AEC_MEDIUM_ADVANCED)	permanent	8	0

4. Add TSAPI Links

Navigate to the **AE Services > TSAPI > TSAPI Links** page to add the TSAPI CTI Link. Click **Add Link**.

Select an available **Link** and **Switch Connection** using the drop down menus. Select the **Switch CTI Link Number** using the drop down menu. The CTI link number must match the number configured in the **cti-link** form in **Section 5, Step 5**. Click **Apply Changes**.

If the application will use Encrypted Links, select ***Encrypted*** or ***Both*** in the **Security** selection box.



Add TSAPI Links

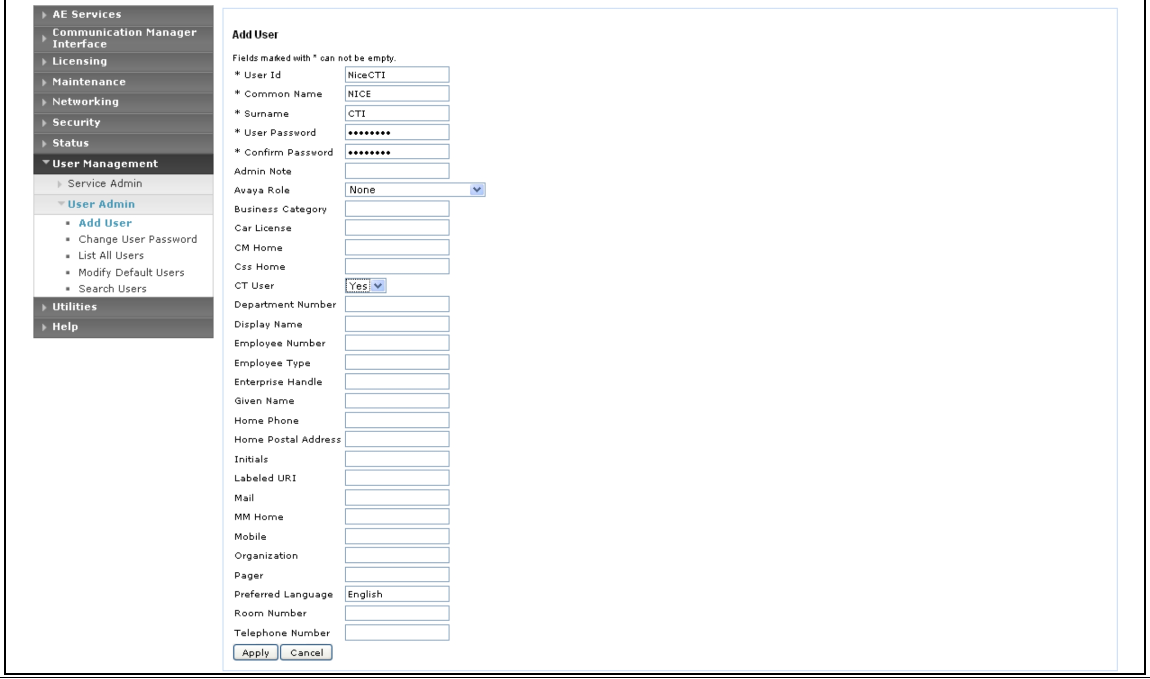
Link: 2
Switch Connection: TR18300
Switch CTI Link Number: 1
ASAI Link Version: 5
Security: Both

5. **Add a CTI User**

Perform requires a CTI user account to access Application Enablement Services. Select **User Management > User Admin > Add User** from the left pane.

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

- In the **User Id** field, type a meaningful user id.
- In the **Common Name** field, type a descriptive name.
- In the **Surname** field, type a descriptive surname.
- In the **User Password** field, type a password for the user.
- In the **Confirm Password** field, re-enter the same password for the user.
- In the **Avaya Role** field, retain the default of ***None.***
- In the **CT User** field, select ***Yes*** from the drop down menu.
- Click **Apply** at the bottom of the screen.



Add User

Fields marked with * can not be empty.

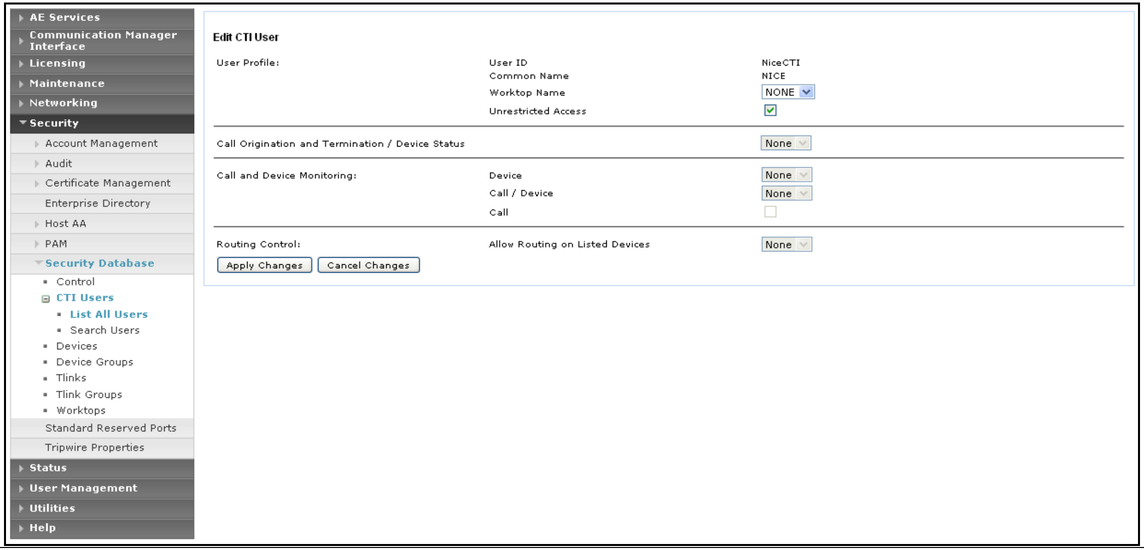
* User Id	NiceCTI
* Common Name	NICE
* Surname	CTI
* User Password	••••••••
* Confirm Password	••••••••
Admin Note	
Avaya Role	None
Business Category	
Car License	
CM Home	
Css Home	
CT User	Yes
Department Number	
Display Name	
Employee Number	
Employee Type	
Enterprise Handle	
Given Name	
Home Phone	
Home Postal Address	
Initials	
Labeled URI	
Mail	
MM Home	
Mobile	
Organization	
Pager	
Preferred Language	English
Room Number	
Telephone Number	

6. **Enable Unrestricted Access to the Security Database**

The Nice user account will require unrestricted Security Database access in order to be able to access any of the Devices (stations) administered to be recorded in the application. This enables a user to administer the agent, vdn and acd devices on the Perform server and not have to duplicate the effort in the Security Database.

To change the security level for the CT User Select **Security > Security Database > CTI Users > List All Users** from the left pane. Choose the CTI user, and click **Edit** (not shown below).

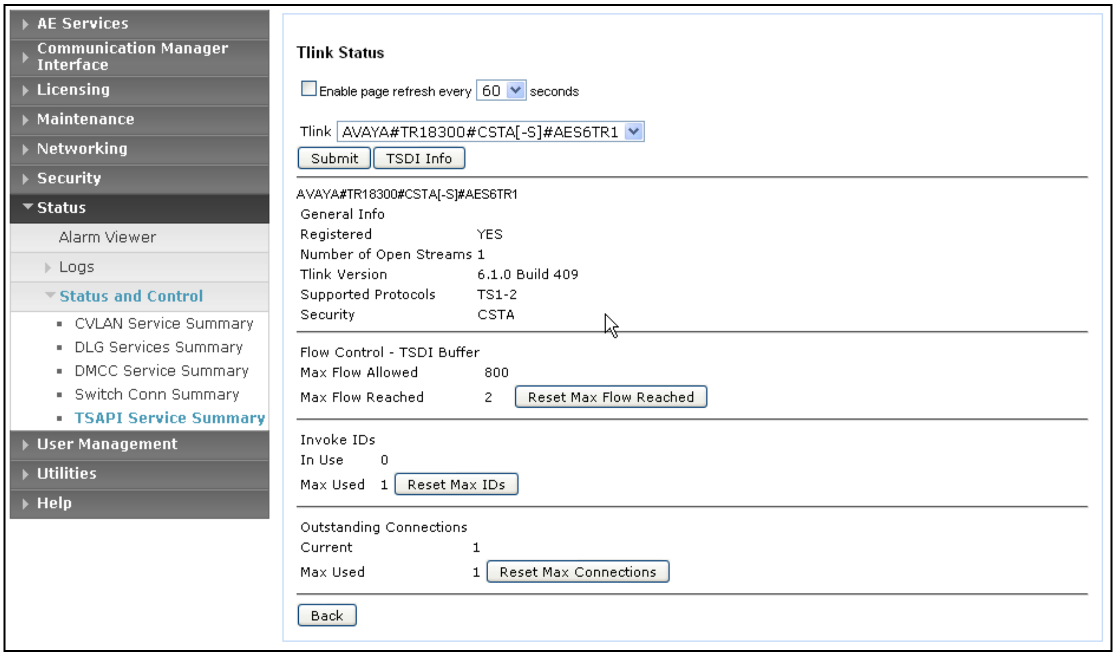
On the **Edit CTI User** page, check the **Unrestricted Access** option and click on **Apply Changes**.



Edit CTI User

User Profile:	User ID	NiceCTI
	Common Name	NICE
	Worktop Name	NONE
	Unrestricted Access	☑
Call Origination and Termination / Device Status		None
Call and Device Monitoring:	Device	None
	Call / Device	None
	Call	□
Routing Control:	Allow Routing on Listed Devices	None

Apply Changes | Cancel Changes

7.	**Note the T-Link Name** This information will be used in the application configuration below. Select **Status > Status and Control > TSAPI Service Summary** from the left pane and select **T-Link Status** (not shown below). Once at the **T-Link Status** screen, this screen shows a select box of the Tlink names. A new Tlink name is automatically generated by the Application Enablement Services server upon creation of a new switch connection. Locate and select the Tlink name associated with the relevant switch connection which would use the name of the switch connection as part of the Tlink name (not shown below). This screen will also provide information on the status of the TLink as shown below: 

Tlink Status

□ Enable page refresh every 60 seconds

Tlink AVAYA#TR18300#CSTA[-S]#AES6TR1

Submit | TSDI Info

AVAYA#TR18300#CSTA[-S]#AES6TR1

```
General Info
Registered                YES
Number of Open Streams    1
Tlink Version             6.1.0 Build 409
Supported Protocols       TS1-2
Security                  CSTA

Flow Control - TSDI Buffer
Max Flow Allowed          800
Max Flow Reached          2    Reset Max Flow Reached

Invoke IDs
In Use      0
Max Used    1  Reset Max IDs

Outstanding Connections
Current                   1
Max Used                  1  Reset Max Connections

Back
```

7. Configure Avaya Aura® Session Manager

The configuration of Session Manager followed standard configuration to establish a SIP Entity Link with Avaya Aura® Session Border Controller for receiving and routing calls from and to the public network. This configuration required nothing special for the NICE Perform® integration and is therefore not covered in this document.

8. Configure Avaya Aura® Session Border Controller

The Avaya Aura® Session Border Controller installation steps include inputs required to properly configure default Public Network and Private Network interfaces and default policies. These steps were performed prior to the testing of the NICE Perform® solution, and had no direct impact on the tested solution. The steps required to configure the interface to permit Perform to send Invites in order to be added to calls, and the associated policies needed are described below.

8.1. Session Border Controller Configuration Details

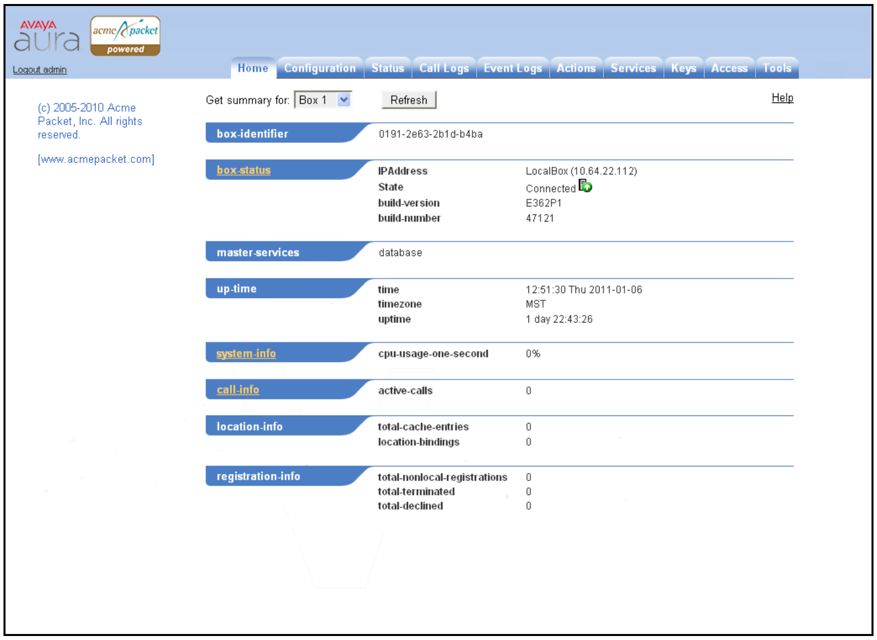
The focus of these notes is to demonstrate the specific configuration steps that pertain to enabling Perform to interact with Session Border Controller. The detailed configuration used in this test is attached in the form of a saved configuration file which can be referred to for specific details about the integration with the Telco provider (in this case, the remote Communication Manager), and Session Manager. Further, this file can be loaded into the Session Border Controller configuration to be used as a starting point for implementations at other locations.

An overview of the configuration tree follows to highlight the specific tasks necessary for the Perform integration. These include:

- Confirm License Capacities
- Enable Third Party Call Control for the Default Session Configuration
- Define UUI creation rules for the Default Session Configuration
- Create a Session Policy and Rule to Handle Perform Session Requests
- Create a SIP Gateway Server

NOTE: In each case, when navigating to a setting page, it is generally necessary to enable the advanced settings view in order to configure the objects necessary for the integration. To do so, click on the Show advanced button at the top of the configuration screen. If the Show basic button is displayed, you are already in advanced mode.

Access the Session Border Controller and log in using appropriate credentials. The configuration interface can be reached via web browser by entering the URL: **https://<ip_address>**.



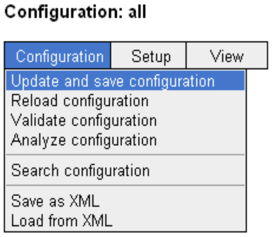
(c) 2005-2010 Acme Packet, Inc. All rights reserved.

[www.acmepacket.com]

Get summary for: Box 1

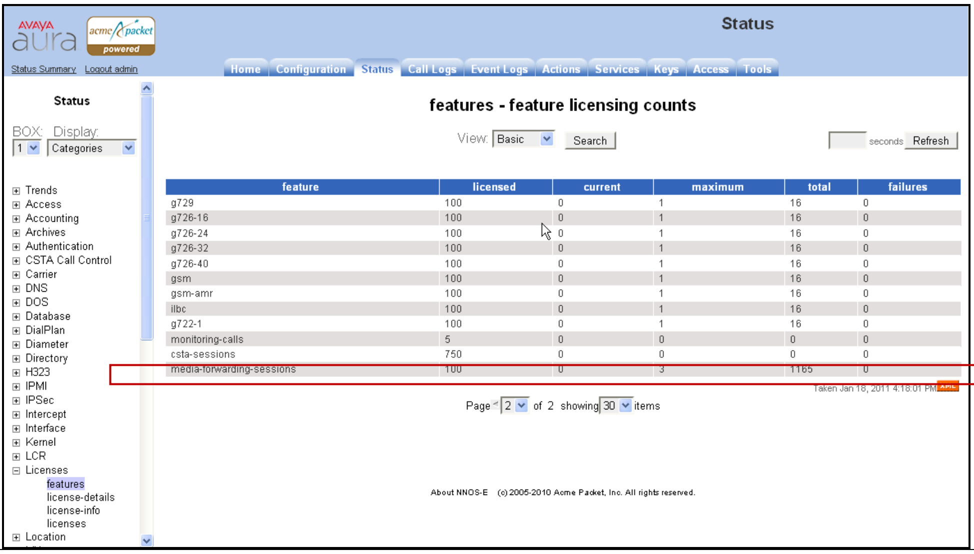
box-identifier	0191-2e63-2b1d-b4ba	
box-status	IPAddress	LocalBox (10.64.22.112)
	State	Connected
	build-version	E362P1
	build-number	47121
master-services	database	
up-time	time	12:51:30 Thu 2011-01-06
	timezone	MST
	uptime	1 day 22:43:26
system-info	cpu-usage-one-second	0%
call-info	active-calls	0
location-info	total-cache-entries	0
	location-bindings	0
registration-info	total-nonlocal-registrations	0
	total-terminated	0
	total-declined	0

Note regarding **Set** and **Save** used throughout this document**:** After setting properties for each object, click Set which is located at the top and bottom of each page, then click on the **Update and save configuration** menu option at the top\left corner of the navigation tree. When prompted, click **yes** to both confirmation dialogs that follow.



1. Confirm License Capacities

Confirm that the license includes an adequate number of **media-forwarding-sessions** to accommodate the maximum number of simultaneous recordings in the configured environment. If additional license entitlements are required, contact your Avaya representative or reseller.



features - feature licensing counts

feature	licensed	current	maximum	total	failures
g729	100	0	1	16	0
g726-16	100	0	1	16	0
g726-24	100	0	1	16	0
g726-32	100	0	1	16	0
g726-40	100	0	1	16	0
gsm	100	0	1	16	0
gsm-amr	100	0	1	16	0
ilbc	100	0	1	16	0
g722-1	100	0	1	16	0
monitoring-calls	5	0	0	0	0
csta-sessions	750	0	0	0	0
media-forwarding-sessions	100	0	3	1165	0

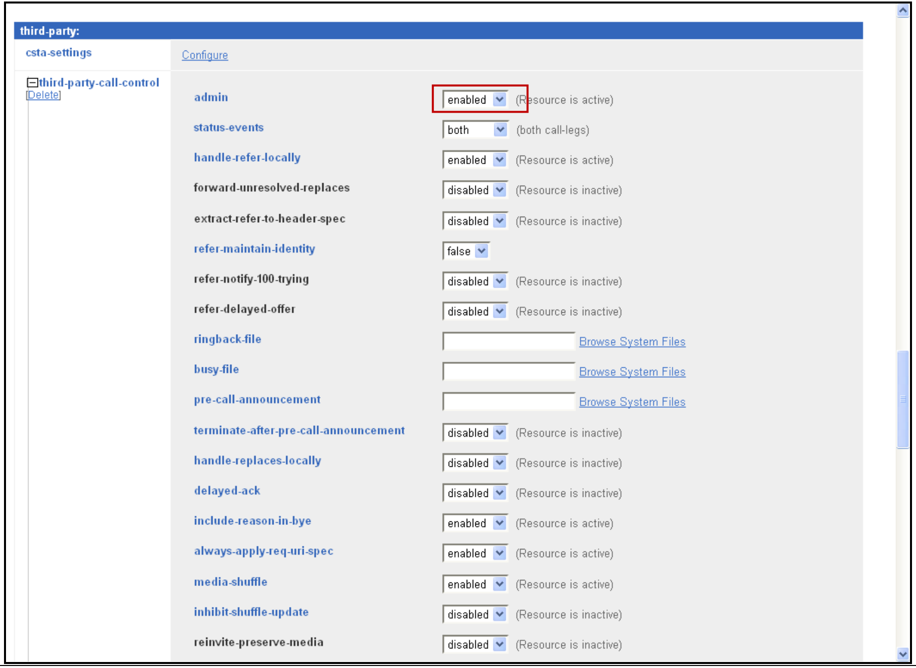
Taken Jan 18, 2011 4:18:01 PM

Page 2 of 2 showing 30 items

About NNOS-E (c) 2005-2010 Acme Packet, Inc. All rights reserved.

2. Enable Third Party Call Control for the Default Session Configuration

Navigate to **vsp\default-session-config** and scroll down to find the **third-party-call-control** property, click on the + icon to expand the properties. Select ***enabled*** on the **admin** property. Set and Save the configuration as described above.

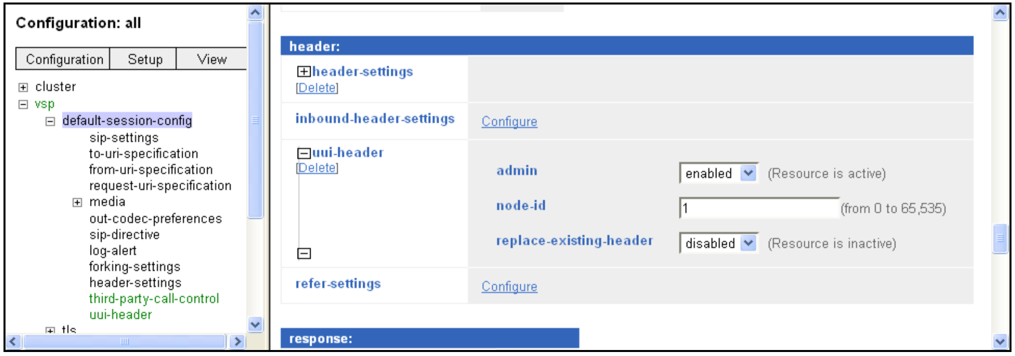


admin	enabled	(Resource is active)
status-events	both	(both call-legs)
handle-refer-locally	enabled	(Resource is active)
forward-unresolved-replaces	disabled	(Resource is inactive)
extract-refer-to-header-spec	disabled	(Resource is inactive)
refer-maintain-identity	false	
refer-notify-100-trying	disabled	(Resource is inactive)
refer-delayed-offer	disabled	(Resource is inactive)
ringback-file		Browse System Files
busy-file		Browse System Files
pre-call-announcement		Browse System Files
terminate-after-pre-call-announcement	disabled	(Resource is inactive)
handle-replaces-locally	disabled	(Resource is inactive)
delayed-ack	disabled	(Resource is inactive)
include-reason-in-bye	enabled	(Resource is active)
always-apply-req-uri-spec	enabled	(Resource is active)
media-shuffle	enabled	(Resource is active)
inhibit-shuffle-update	disabled	(Resource is inactive)
reinvite-preserve-media	disabled	(Resource is inactive)

3. **Define UUI creation rules for the Default Session Configuration**

The Perform integration requires that all sessions passing through the Session Border Controller have a UCID which will be used to identify the specific session for a given call. When calls arrive from the PBX side, they will already have a UCID in the UUI field as shared UUI treatment was set on the trunks from Communication Manager to Session Manager and/or Session Border Controller. When calls arrive from the Telco side, if the header already contains UUI containing a UCID, it will be preserved and passed on to the next hop. If a call from the Telco arrives without UCID, a UCID will be created and Communication Manager will use this UCID.

In the **header** section of the **default-session-config**, click on the + next to **uui header.** Select ***enabled*** for the **admin** property and enter a **node-id**. The node-id can be any integer value, it should match the **UCID Network Node ID** administered in **Section 5, Step 4**. Set and Save the configuration as described above.



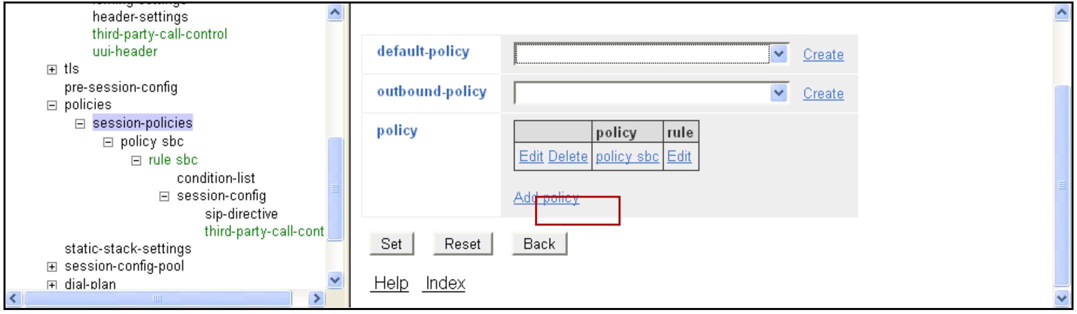
```
Configuration: all
Configuration | Setup | View
⊞ cluster
⊟ vsp
   ⊟ default-session-config
        sip-settings
        to-uri-specification
        from-uri-specification
        request-uri-specification
      ⊞ media
        out-codec-preferences
        sip-directive
        log-alert
        forking-settings
        header-settings
        third-party-call-control
        uui-header
   ⊞ tls
```

```
header:
⊞header-settings [Delete]
inbound-header-settings      Configure
⊟uui-header [Delete]
    admin                     enabled   (Resource is active)
    node-id                   1         (from 0 to 65,535)
    replace-existing-header   disabled  (Resource is inactive)
refer-settings               Configure
response:
```

4. **Create a Session Policy and Rule to Handle Perform Session Requests**

Note: This task requires several steps and spans the next four pages.

Navigate to the **policies\session-policies** property and click on the **Add policy** link. Note that the policy used in the test is already defined in the snapshot below.

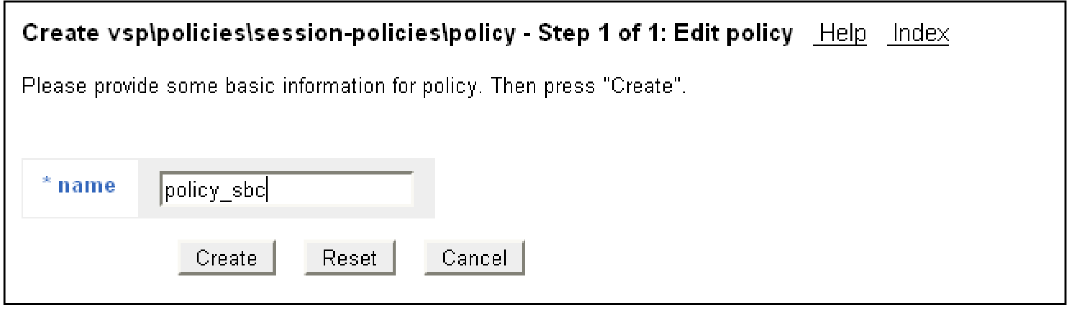


```
   header-settings
   third-party-call-control
   uui-header
⊞ tls
   pre-session-config
⊟ policies
   ⊟ session-policies
      ⊟ policy sbc
         ⊟ rule sbc
              condition-list
            ⊟ session-config
                 sip-directive
                 third-party-call-cont
   static-stack-settings
⊞ session-config-pool
⊞ dial-plan
```

```
default-policy    [          ]  Create
outbound-policy   [          ]  Create
policy                          policy       rule
                  Edit Delete   policy sbc   Edit
                  Add policy
Set   Reset   Back
Help  Index
```

Create a Session Policy and Rule to Handle Perform Session Requests (continued)

The **Add policy** link will prompt for a policy name, **policy_sbc** was used in the test. Click **Create** to create the policy.

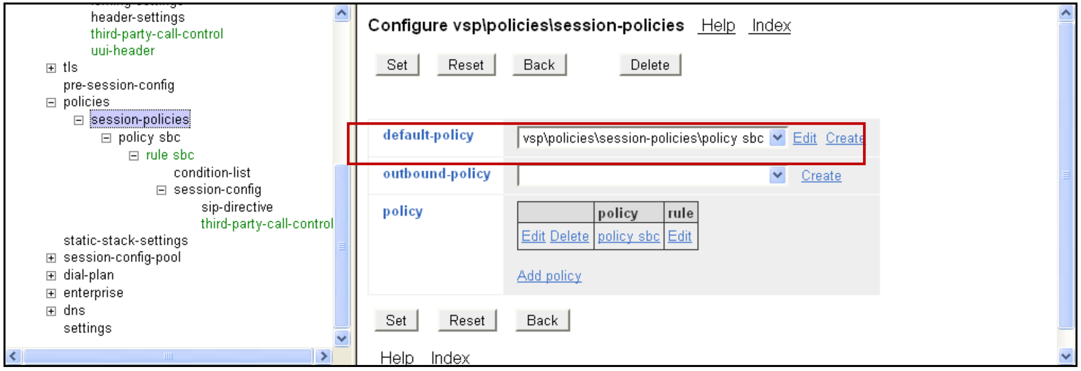


Create vsp\policies\session-policies\policy - Step 1 of 1: Edit policy

Please provide some basic information for policy. Then press "Create".

* name	policy_sbc

Once the policy has been defined, select it from the **default-policy** selection box to assign it to the session-policies property. Click **Set** to confirm the changes.



```
    header-settings
    third-party-call-control
    uui-header
⊞ tls
  pre-session-config
⊟ policies
  ⊟ session-policies
    ⊟ policy sbc
      ⊟ rule sbc
          condition-list
        ⊟ session-config
            sip-directive
            third-party-call-control
  static-stack-settings
⊞ session-config-pool
⊞ dial-plan
⊞ enterprise
⊞ dns
  settings
```

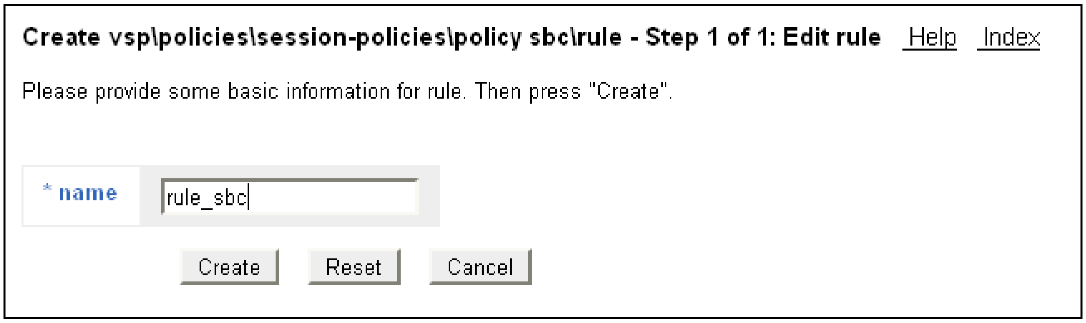
Configure vsp\policies\session-policies

default-policy	vsp\policies\session-policies\policy sbc
outbound-policy	

policy

	policy	rule
Edit Delete	policy sbc	Edit

Next, a rule must be created to instruct how to handle the Perform request. Click on the **Edit** link in the **Rule** column associated with the newly created policy. Assign a rule **name** and click **Create**.



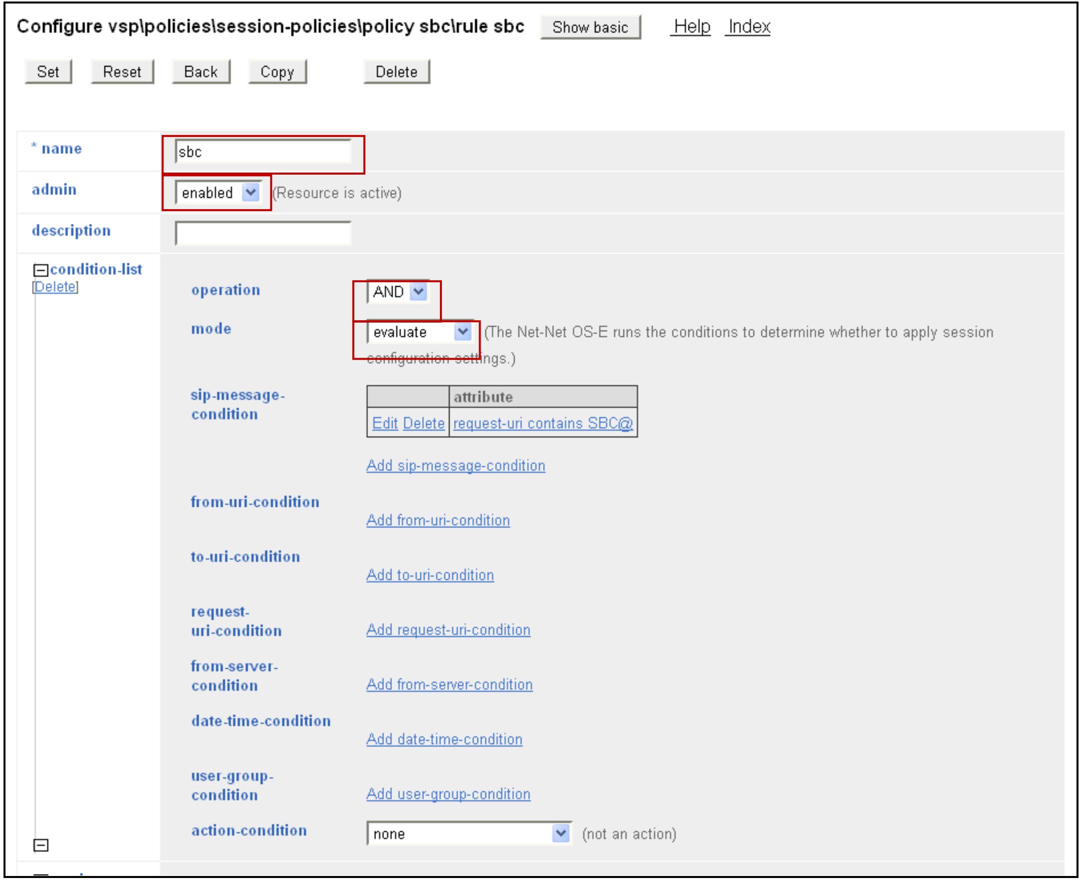
Create vsp\policies\session-policies\policy sbc\rule - Step 1 of 1: Edit rule

Please provide some basic information for rule. Then press "Create".

* name	rule_sbc

Create a Session Policy and Rule to Handle Perform Session Requests (continued)

Click on the **rule_sbc** property in the navigation links (not shown) to configure the properties of the rule. In the test, **sbc** was the name given to the definition, **admin** was ***enabled***, and the **condition-list** object was expanded to define an ***AND* operation** to **evaluate** an attribute that would be contained in the request from Perform (see the next step for the attribute definition).



Configure vsp\policies\session-policies\policy sbc\rule sbc

* name: sbc

admin: enabled (Resource is active)

description:

condition-list [Delete]

operation: AND

mode: evaluate (The Net-Net OS-E runs the conditions to determine whether to apply session configuration settings.)

sip-message-condition:

	attribute
Edit Delete	request-uri contains SBC@

Add sip-message-condition

from-uri-condition: Add from-uri-condition

to-uri-condition: Add to-uri-condition

request-uri-condition: Add request-uri-condition

from-server-condition: Add from-server-condition

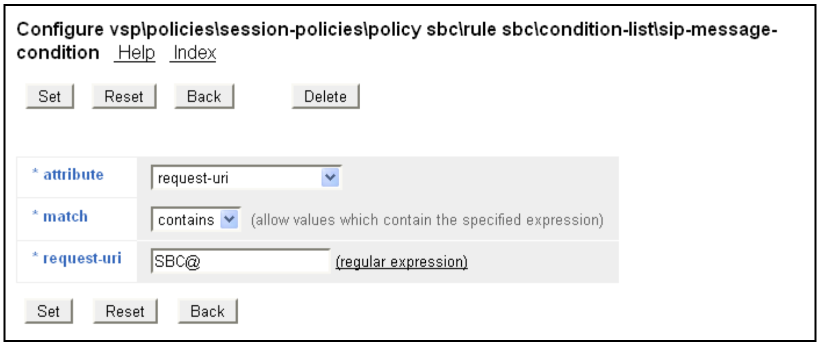
date-time-condition: Add date-time-condition

user-group-condition: Add user-group-condition

action-condition: none (not an action)

Create a Session Policy and Rule to Handle Perform Session Requests (continued)

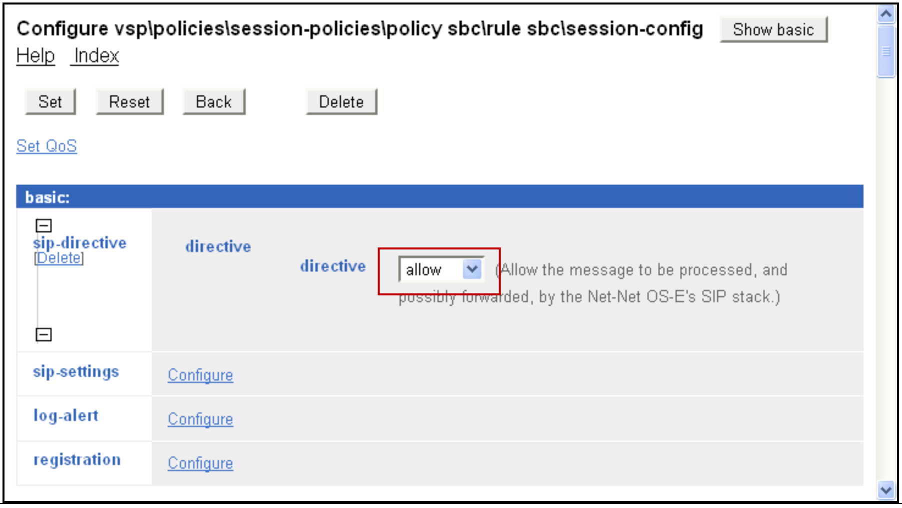
Click on the **Edit** link associated with the **sip-message-condition** property to define the attributes of the condition. Select ***request-uri*** for the **attribute** option, ***contains*** for the **match** option, and enter **SBC@** for the **request-uri** value. Note, the request-uri value must match the Field Mapping entry made on the Perform server (SBC@10.64.22.112 was defined in the Perform configuration in **Section 9.1, Step 1**). Click **Set** to confirm the changes.



Configure vsp\policies\session-policies\policy sbc\rule sbc\condition-list\sip-message-condition

* attribute	request-uri	
* match	contains	(allow values which contain the specified expression)
* request-uri	SBC@	(regular expression)

Next, select the **session-config** property in the navigation panel under the newly created **rule_sbc** property to enable additional properties for the policy. Scroll down to the **basic** settings, click on the + next to **sip-directive** to set the property to ***allow*** message processing. Set and Save the configuration as described above.



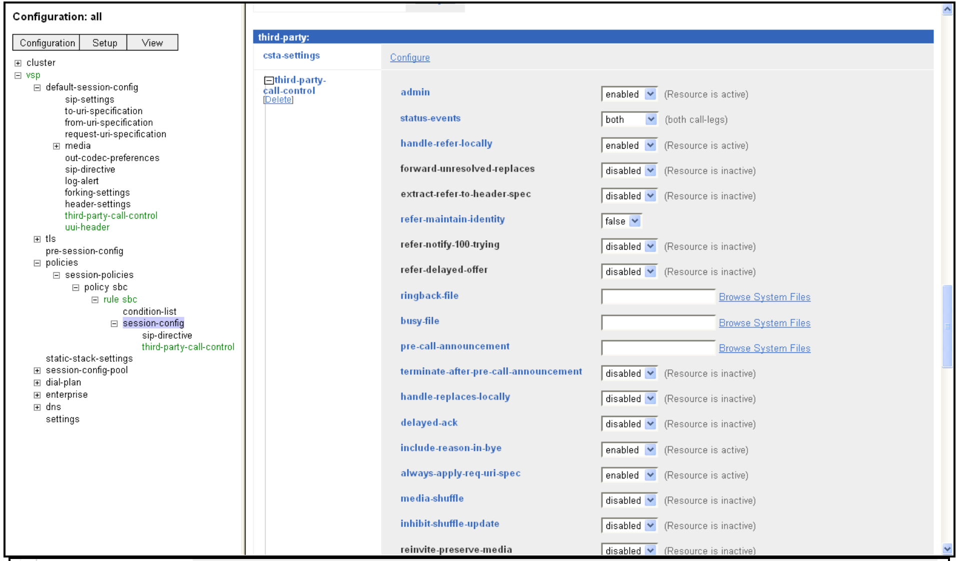
Configure vsp\policies\session-policies\policy sbc\rule sbc\session-config

basic:

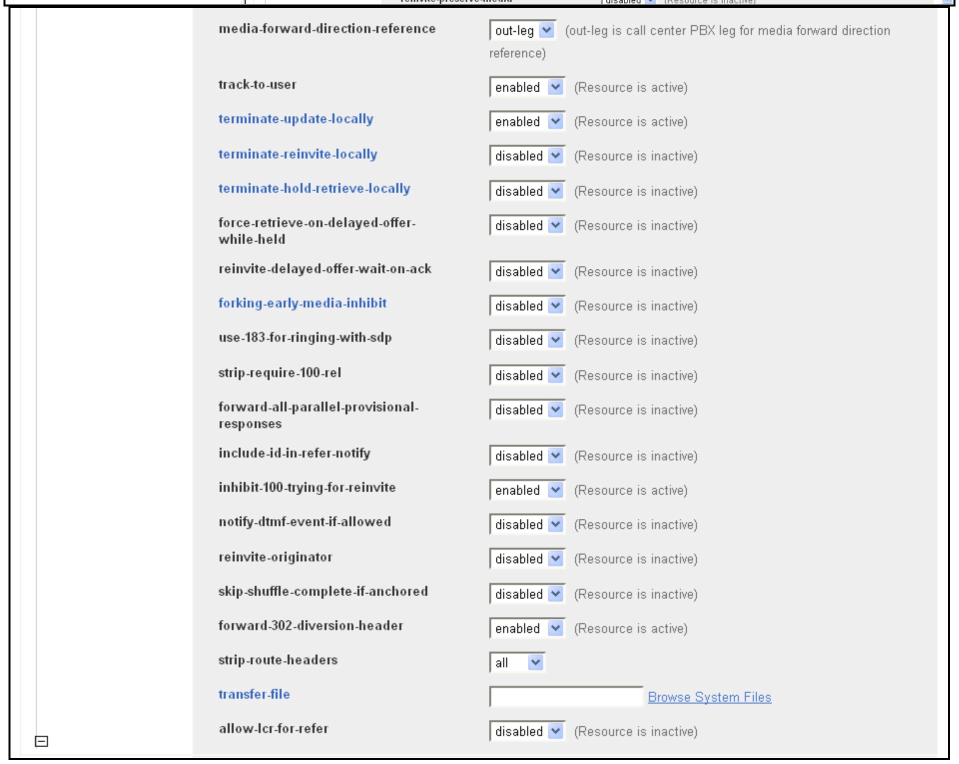
sip-directive [Delete]	directive	
	directive	allow (Allow the message to be processed, and possibly forwarded, by the Net-Net OS-E's SIP stack.)
sip-settings	Configure	
log-alert	Configure	
registration	Configure	

Create a Session Policy and Rule to Handle Perform Session Requests (continued)

Go to the third party heading and match the following settings (which should be default values): Set and Save the configuration as described above.



admin	enabled	(Resource is active)
status-events	both	(both call-legs)
handle-refer-locally	enabled	(Resource is active)
forward-unresolved-replaces	disabled	(Resource is inactive)
extract-refer-to-header-spec	disabled	(Resource is inactive)
refer-maintain-identity	false	
refer-notify-100-trying	disabled	(Resource is inactive)
refer-delayed-offer	disabled	(Resource is inactive)
ringback-file		Browse System Files
busy-file		Browse System Files
pre-call-announcement		Browse System Files
terminate-after-pre-call-announcement	disabled	(Resource is inactive)
handle-replaces-locally	disabled	(Resource is inactive)
delayed-ack	disabled	(Resource is inactive)
include-reason-in-bye	enabled	(Resource is active)
always-apply-req-uri-spec	enabled	(Resource is active)
media-shuffle	disabled	(Resource is inactive)
inhibit-shuffle-update	disabled	(Resource is inactive)
reinvite-preserve-media	disabled	(Resource is inactive)



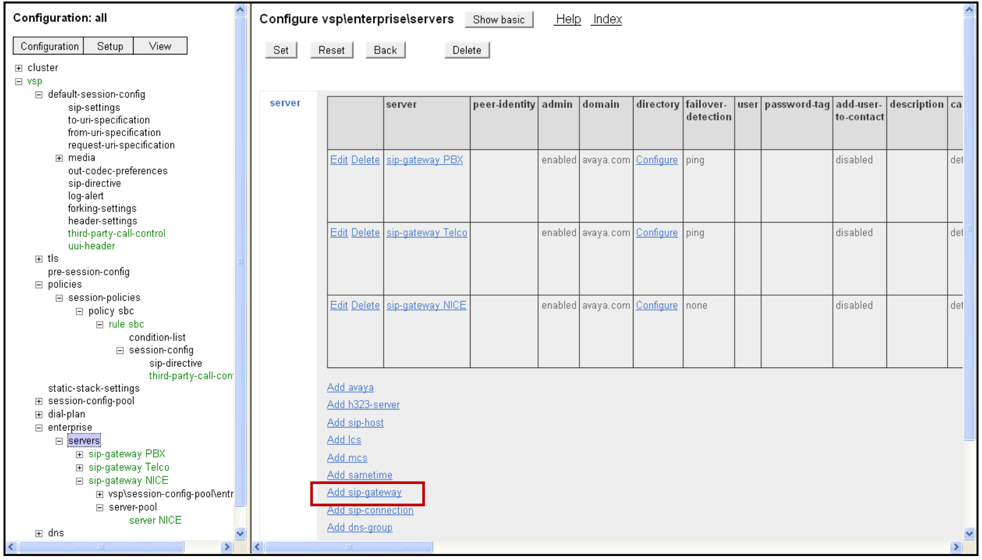
media-forward-direction-reference	out-leg	(out-leg is call center PBX leg for media forward direction reference)
track-to-user	enabled	(Resource is active)
terminate-update-locally	enabled	(Resource is active)
terminate-reinvite-locally	disabled	(Resource is inactive)
terminate-hold-retrieve-locally	disabled	(Resource is inactive)
force-retrieve-on-delayed-offer-while-held	disabled	(Resource is inactive)
reinvite-delayed-offer-wait-on-ack	disabled	(Resource is inactive)
forking-early-media-inhibit	disabled	(Resource is inactive)
use-183-for-ringing-with-sdp	disabled	(Resource is inactive)
strip-require-100-rel	disabled	(Resource is inactive)
forward-all-parallel-provisional-responses	disabled	(Resource is inactive)
include-id-in-refer-notify	disabled	(Resource is inactive)
inhibit-100-trying-for-reinvite	enabled	(Resource is active)
notify-dtmf-event-if-allowed	disabled	(Resource is inactive)
reinvite-originator	disabled	(Resource is inactive)
skip-shuffle-complete-if-anchored	disabled	(Resource is inactive)
forward-302-diversion-header	enabled	(Resource is active)
strip-route-headers	all	
transfer-file		Browse System Files
allow-lcr-for-refer	disabled	(Resource is inactive)

5. Create a SIP Gateway Server

Note: This task requires several steps and spans the next three pages.

By default, the Perform server will appear to be an untrusted entity. By creating a definition for Perform as a SIP Gateway Server, the Session Border Controller will treat messages from this source as trusted and process the messages. Without this step, all requests from Perform would be ignored.

Navigate to the **vsp\enterprise\servers** property on the navigation panel, and select **Add sip-gateway** from the links below the existing PBX and Telco servers. Note that the Perform server definition was previously defined in the snapshot below.

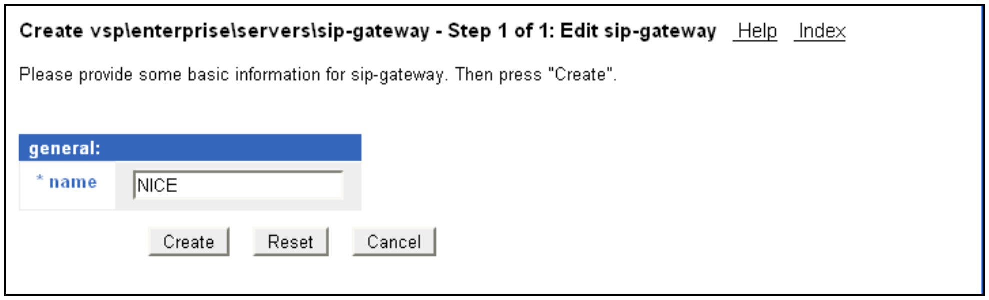


Configure vsp\enterprise\servers

	server	peer-identity	admin	domain	directory	failover-detection	user	password-tag	add-user-to-contact	description	ca
Edit Delete	sip-gateway PBX		enabled	avaya.com	Configure	ping			disabled		de
Edit Delete	sip-gateway Telco		enabled	avaya.com	Configure	ping			disabled		de
Edit Delete	sip-gateway NICE		enabled	avaya.com	Configure	none			disabled		de

Add avaya
Add h323-server
Add sip-host
Add lcs
Add mcs
Add sametime
Add sip-gateway
Add sip-connection
Add dns-group

Enter a name for the Perform server, in the test, **NICE** was used. Click **Create**.



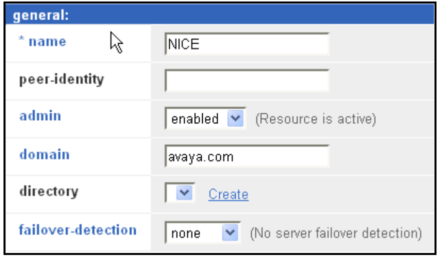
Create vsp\enterprise\servers\sip-gateway - Step 1 of 1: Edit sip-gateway

Please provide some basic information for sip-gateway. Then press "Create".

* name	NICE

Create a NICE SIP Gateway Server (continued)

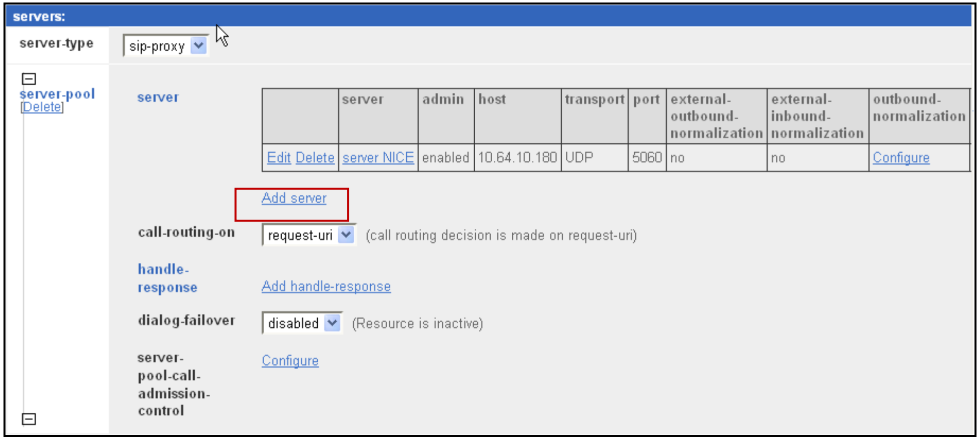
Select the newly created sip-gateway NICE object in the navigation pane, and make the following entries under the **general** settings:



general:

* name	NICE
peer-identity	
admin	enabled (Resource is active)
domain	avaya.com
directory	Create
failover-detection	none (No server failover detection)

In the **servers** section, select the **server-type:** ***sip-proxy*** and expand the **server-pool** object by selecting the + icon. Select the **Add server** link to define the details of the Perform server. Note that the server was previously defined in the snapshot below.



servers:

server-type: sip-proxy

server-pool [Delete]

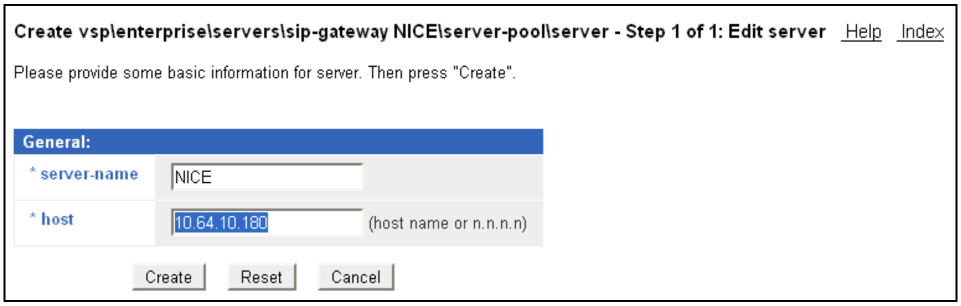
server

	server	admin	host	transport	port	external-outbound-normalization	external-inbound-normalization	outbound-normalization
Edit Delete	server NICE	enabled	10.64.10.180	UDP	5060	no	no	Configure

Add server

call-routing-on	request-uri (call routing decision is made on request-uri)
handle-response	Add handle-response
dialog-failover	disabled (Resource is inactive)
server-pool-call-admission-control	Configure

Enter the **host name** or **IP Address** and a **server-name.** Click **Create** which will return to the screen above.



Create vsp\enterprise\servers\sip-gateway NICE\server-pool\server - Step 1 of 1: Edit server Help Index

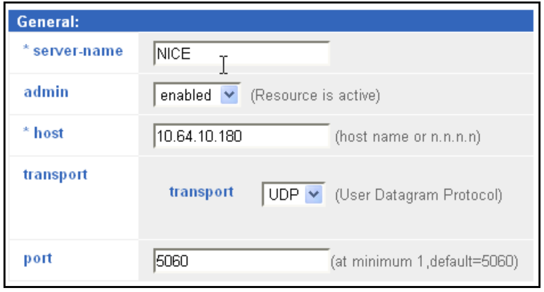
Please provide some basic information for server. Then press "Create".

General:

* server-name	NICE
* host	10.64.10.180 (host name or n.n.n.n)

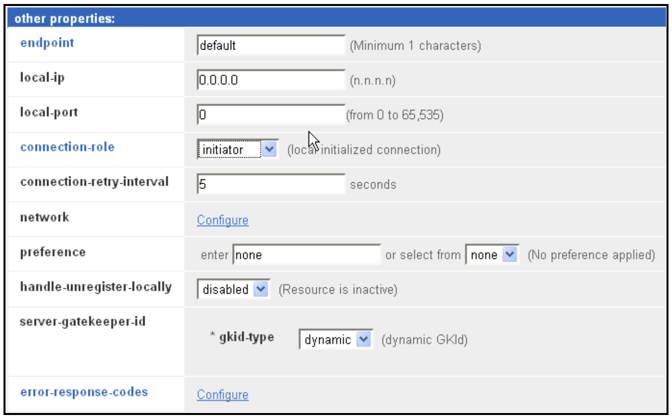
Create a NICE SIP Gateway Server (continued)

Click the **Edit** link for the Perform server to add further details. Accept all defaults, and make the following entries in the **General** and **other properties** sections:



General:

* server-name	NICE
admin	enabled (Resource is active)
* host	10.64.10.180 (host name or n.n.n.n)
transport	transport UDP (User Datagram Protocol)
port	5060 (at minimum 1,default=5060)



other properties:

endpoint	default (Minimum 1 characters)
local-ip	0.0.0.0 (n.n.n.n)
local-port	0 (from 0 to 65,535)
connection-role	initiator (local initialized connection)
connection-retry-interval	5 seconds
network	Configure
preference	enter none or select from none (No preference applied)
handle-unregister-locally	disabled (Resource is inactive)
server-gatekeeper-id	* gkid-type dynamic (dynamic GKId)
error-response-codes	Configure

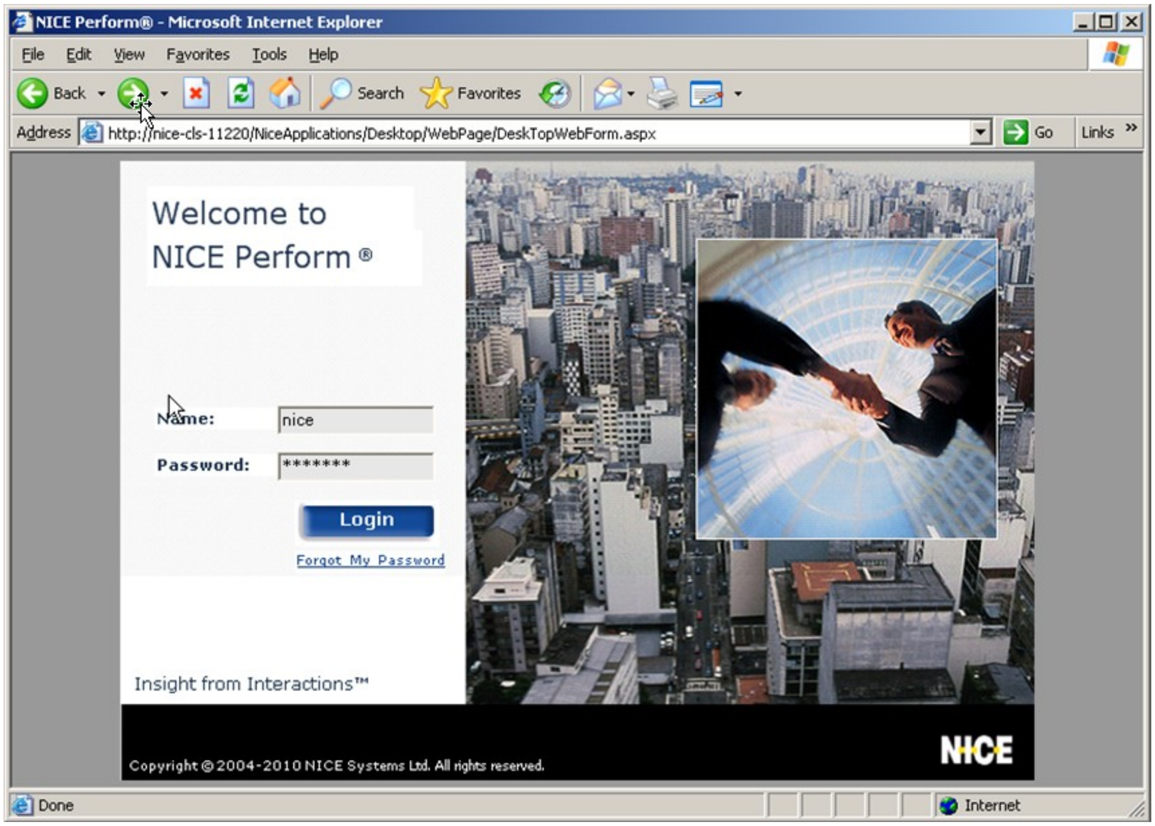
Set and **Save** the configuration as described above. Note: the configuration settings used in this test are displayed in full in **Appendix A** at the end of this document.

9. Configure NICE Perform®

This section provides the steps for configuring the NICE Perform® solution.

9.1. NICE Perform Configuration Details

NICE Perform is configured using a web browser. Enter the URL of the Perform server such as **http://<hostname>/nice** where <hostname> is the ip address or fully qualified domain name of the Perform server. Login using appropriate credentials.


NICE Perform® - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address
Go Links
Welcome to NICE Perform ®
Login
Forgot My Password
Insight from Interactions™
Copyright © 2004-2010 NICE Systems Ltd. All rights reserved.
NICE
Done
Internet

Address: http://nice-cls-11220/NiceApplications/Desktop/WebPage/DeskTopWebForm.aspx

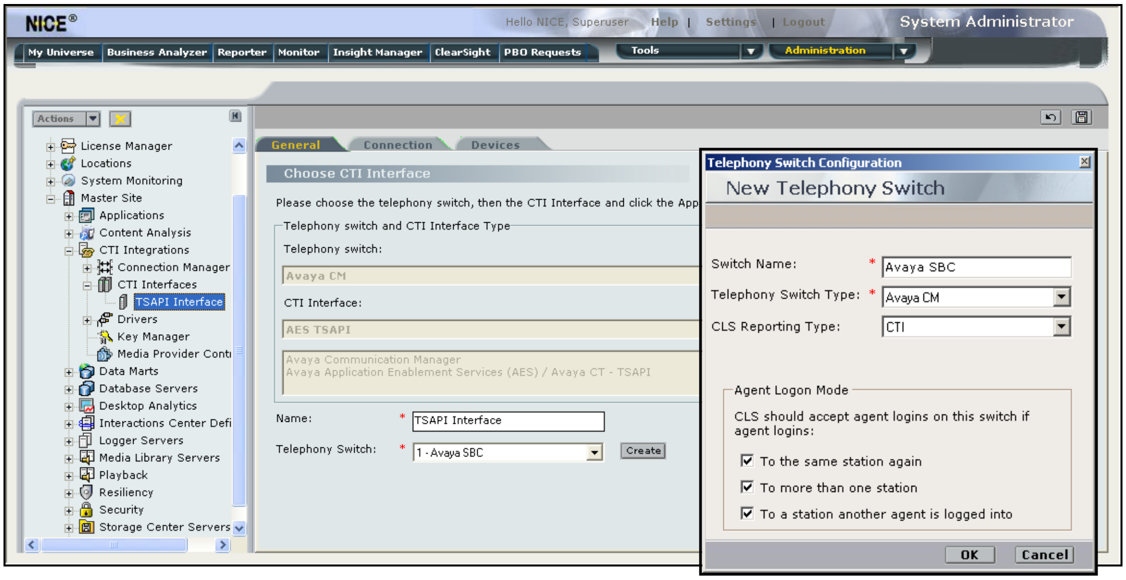
Name: nice

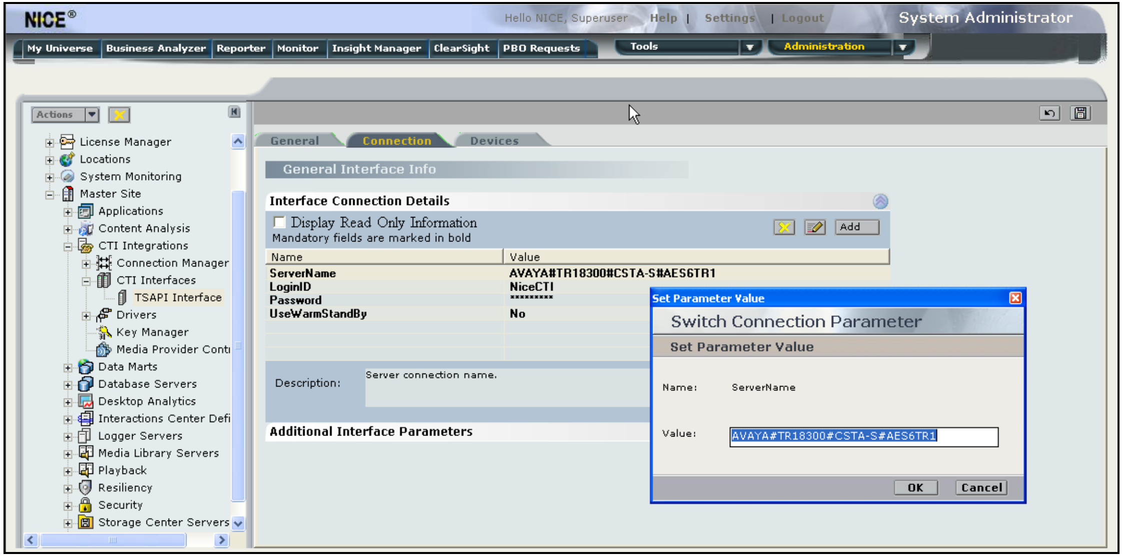
Password: *******

In general, the steps were as follows:

- Configure the Application Enablement Services Interface
- Configure the Logger Channel Mappings

Note that each of these steps requires several subtasks, the illustrations of these subtasks cover several pages to complete each task.

Step	Description
1.	**Configure the Application Enablement Services Interface** Users with System Administration privileges will have the option to select **System Administrator** from the **Accessories** menu. Navigation involves clicking on the objects in the navigation tree on the left panel of the browser window. Navigate to the **Master Site > CTI Integrations > CTI Interfaces > TSAPI Interface** object in the navigation tree and enter a **Name** for the CTI Interface (***TSAPI Interface*** was used in the test. Click **Create** to define the **Telephony Switch,** ***Avaya SBC*** was entered for the **Switch Name**, and ***Avaya CM*** was used for the **Telephony Switch Type**. The **CLS Reporting Type** ***CTI*** was selected and defaults were used for the **Agent Logon Mode**.  NICE Hello NICE, Superuser | Help | Settings | Logout System Administrator My Universe Business Analyzer Reporter Monitor Insight Manager ClearSight PBO Requests Tools Administration Actions License Manager Locations System Monitoring Master Site Applications Content Analysis CTI Integrations Connection Manager CTI Interfaces TSAPI Interface Drivers Key Manager Media Provider Contr Data Marts Database Servers Desktop Analytics Interactions Center Defi Logger Servers Media Library Servers Playback Resiliency Security Storage Center Servers General Connection Devices Choose CTI Interface Telephony Switch Configuration New Telephony Switch Create OK Cancel Please choose the telephony switch, then the CTI Interface and click the App Telephony switch and CTI Interface Type Telephony switch: Avaya CM CTI Interface: AES TSAPI Avaya Communication Manager Avaya Application Enablement Services (AES) / Avaya CT - TSAPI Name: * TSAPI Interface Telephony Switch: * 1 - Avaya SBC Switch Name: * Avaya SBC Telephony Switch Type: * Avaya CM CLS Reporting Type: CTI Agent Logon Mode CLS should accept agent logins on this switch if agent logins: ☑ To the same station again ☑ To more than one station ☑ To a station another agent is logged into

Step	Description
	Configure the Application Enablement Services Interface (continued) Click on the **Connection** tab and click the **Edit** icon for each parameter in the **Interface Connection Details** section. Enter the TLINK name from **Section 6, Step 7** above for the **ServerName** parameter. Similarly, enter the **LoginID** and **Password** as administered in **Section 6, Step 5**. 

Interface Connection Details

☐ Display Read Only Information

Mandatory fields are marked in bold

Name	Value
ServerName	AVAYA#TR18300#CSTA-S#AES6TR1
LoginID	NiceCTI
Password	*********
UseWarmStandBy	No

Description: Server connection name.

Additional Interface Parameters

Set Parameter Value

Switch Connection Parameter

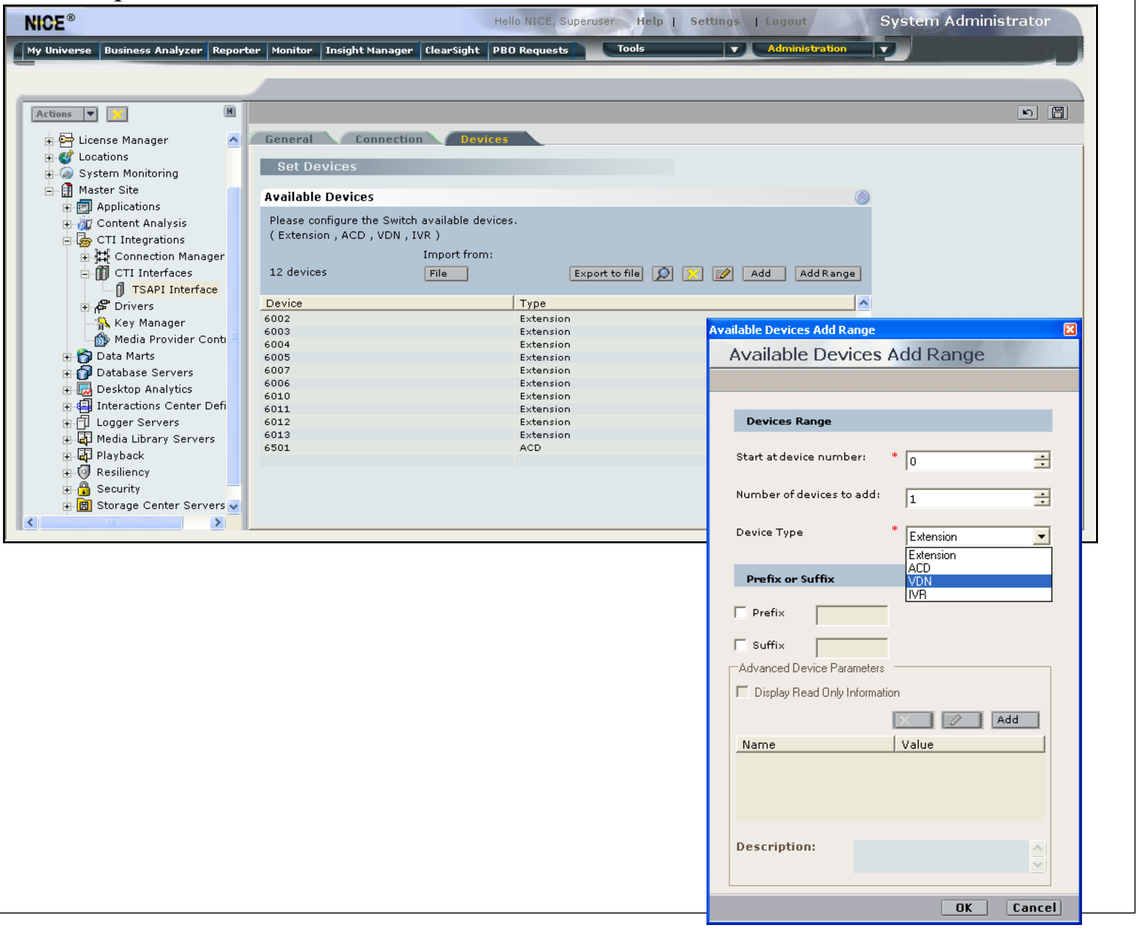
Set Parameter Value

Name: ServerName

Value: AVAYA#TR18300#CSTA-S#AES6TR1

Step	Description
	Configure the Application Enablement Services Interface (continued)

On the **Devices** Tab, create an entry for each Extension, ACD (lead Hunt Group Extension), and VDN that the application will need to monitor in Communication Manager for CTI events. Entry can be simplified if the devices are in a continuous range by using the **Add Range** option, however caution should be excersised with this approach as each invalid device in the range will generate warnings and should be omitted if possible.



Set Devices

Available Devices

Please configure the Switch available devices.
(Extension , ACD , VDN , IVR)

Import from: File

12 devices

Export to file | Add | Add Range

Device	Type
6002	Extension
6003	Extension
6004	Extension
6005	Extension
6007	Extension
6006	Extension
6010	Extension
6011	Extension
6012	Extension
6013	Extension
6501	ACD

Available Devices Add Range

Available Devices Add Range

Devices Range

Start at device number: * 0

Number of devices to add: 1

Device Type * Extension

Extension
ACD
VDN
IVR

Prefix or Suffix

☐ Prefix

☐ Suffix

Advanced Device Parameters

☐ Display Read Only Information

Add

Name	Value

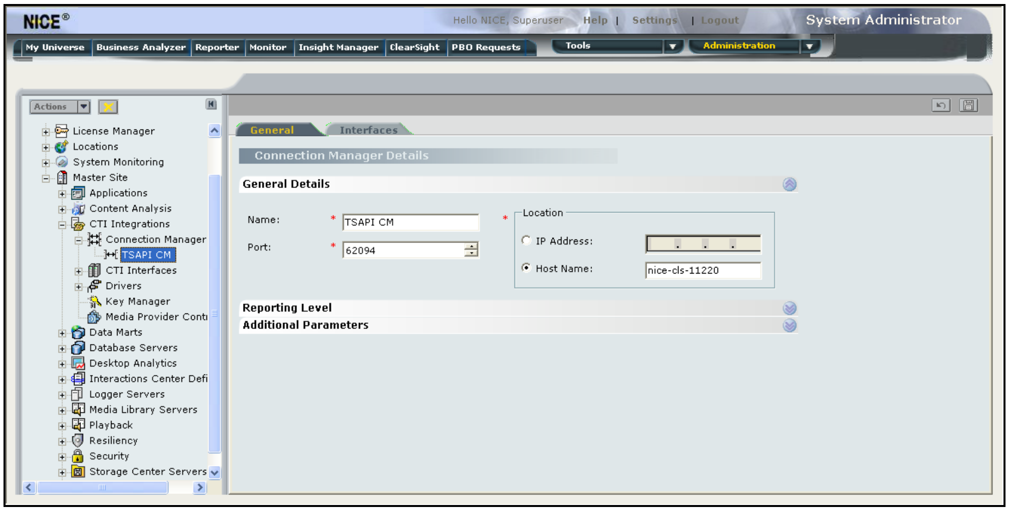
Description:

OK | Cancel

Configure the Application Enablement Services Interface (continued)

The Connection Manager defines how internal modules of the Perform solution will communicate with the CTI Interface module.

Navigate to the **Master Site > CTI Integrations >Connection Manager > TSAPI CM** object in the navigation tree and enter the **Name** and **Port** to use for the connection under the **General Details** section, and enter the **Host Name** of the Perform server in the **Location** section.



Connection Manager Details

General Details

Name: * TSAPI CM

Port: * 62094

Location *

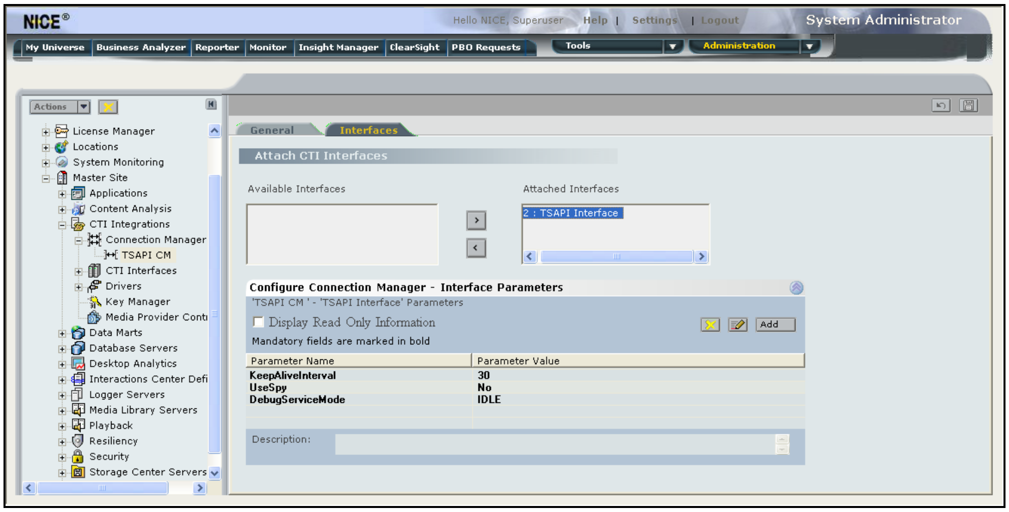
○ IP Address: . . .

● Host Name: nice-cls-11220

Reporting Level

Additional Parameters

On the **Interfaces** tab, highlight the ***TSAPI Interface*** in the **Available Interfaces** column and use the > button to move this interface into the **Attached Interfaces** column. All other settings were defaults.



Attach CTI Interfaces

Available Interfaces

Attached Interfaces: 2 : TSAPI Interface

Configure Connection Manager - Interface Parameters

'TSAPI CM ' - 'TSAPI Interface' Parameters

□ Display Read Only Information

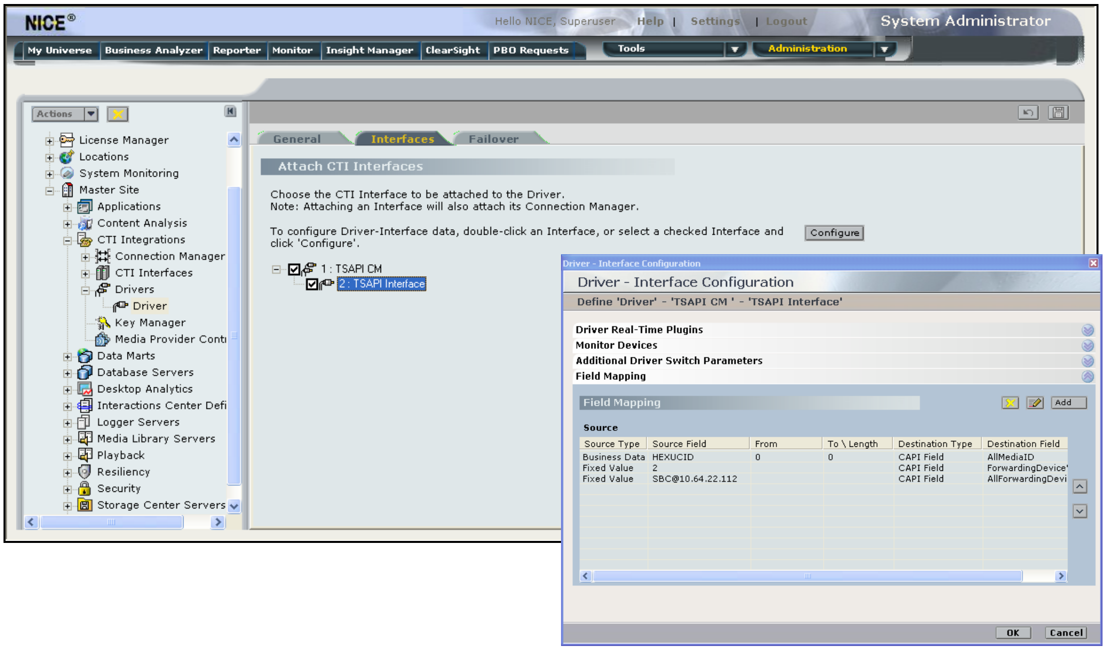
Mandatory fields are marked in bold

Parameter Name	Parameter Value
KeepAliveInterval	30
UseSpy	No
DebugServiceMode	IDLE

Description:

Configure the Application Enablement Services Interface (continued)

Next, navigate to the **Master Site > CTI Integrations > Drivers > Driver** object to link the ***TSAPI Interface***. Click on the **Configure** button to define additional settings in the **Field Mapping** section. These settings are entered using the **Edit** button. The **Business Data (*HEXUCID)***, and **Fixed Value** (*SBC@10.64.22.112)* are settings the driver will use to send SIP Invites to the Session Border Controller.



Attach CTI Interfaces

Choose the CTI Interface to be attached to the Driver.
Note: Attaching an Interface will also attach its Connection Manager.

To configure Driver-Interface data, double-click an Interface, or select a checked Interface and click 'Configure'.

Driver - Interface Configuration

Define 'Driver' - 'TSAPI CM ' - 'TSAPI Interface'

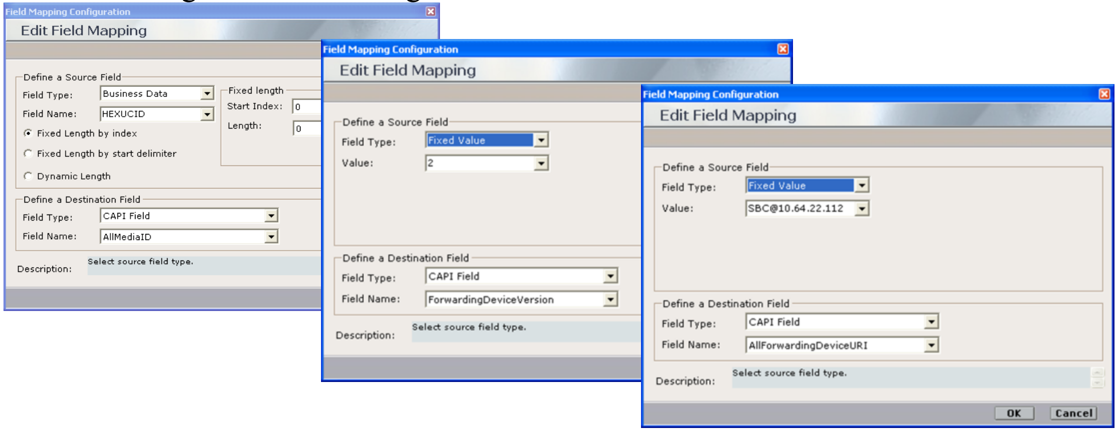
Driver Real-Time Plugins
Monitor Devices
Additional Driver Switch Parameters
Field Mapping

Field Mapping

Source

Source Type	Source Field	From	To \ Length	Destination Type	Destination Field
Business Data	HEXUCID	0	0	CAPI Field	AllMediaID
Fixed Value	2			CAPI Field	ForwardingDevice'
Fixed Value	SBC@10.64.22.112			CAPI Field	AllForwardingDevi

The edit dialogs for these settings are as follows:


Field Mapping Configuration
Field Mapping Configuration
Field Mapping Configuration
OK
Cancel

Edit Field Mapping

Define a Source Field
Field Type: Business Data
Field Name: HEXUCID
● Fixed Length by index
○ Fixed Length by start delimiter
○ Dynamic Length
Fixed length
Start Index: 0
Length: 0
Define a Destination Field
Field Type: CAPI Field
Field Name: AllMediaID
Description: Select source field type.

Edit Field Mapping

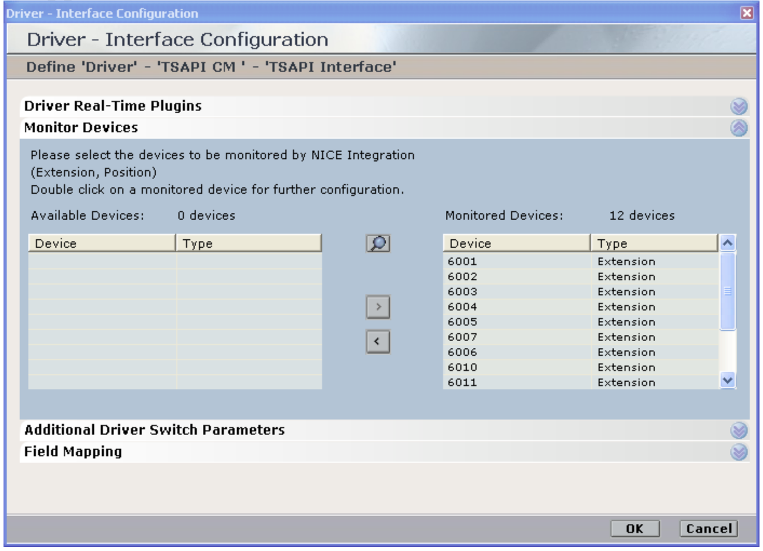
Define a Source Field
Field Type: Fixed Value
Value: 2
Define a Destination Field
Field Type: CAPI Field
Field Name: ForwardingDeviceVersion
Description: Select source field type.

Edit Field Mapping

Define a Source Field
Field Type: Fixed Value
Value: SBC@10.64.22.112
Define a Destination Field
Field Type: CAPI Field
Field Name: AllForwardingDeviceURI
Description: Select source field type.

Configure the Application Enablement Services Interface (continued)

In addition, open the **Monitor Devices** section and move all of the **Available Devices** into the **Monitored Devices** column using the **>** button. This is the last step in configuring the devices the driver will use to request TSAPI Monitors when it starts a connection with Application Enablement Services.



Driver - Interface Configuration

Define 'Driver' - 'TSAPI CM ' - 'TSAPI Interface'

Driver Real-Time Plugins

Monitor Devices

Please select the devices to be monitored by NICE Integration
(Extension, Position)
Double click on a monitored device for further configuration.

Available Devices: 0 devices

Device	Type

Monitored Devices: 12 devices

Device	Type
6001	Extension
6002	Extension
6003	Extension
6004	Extension
6005	Extension
6007	Extension
6006	Extension
6010	Extension
6011	Extension

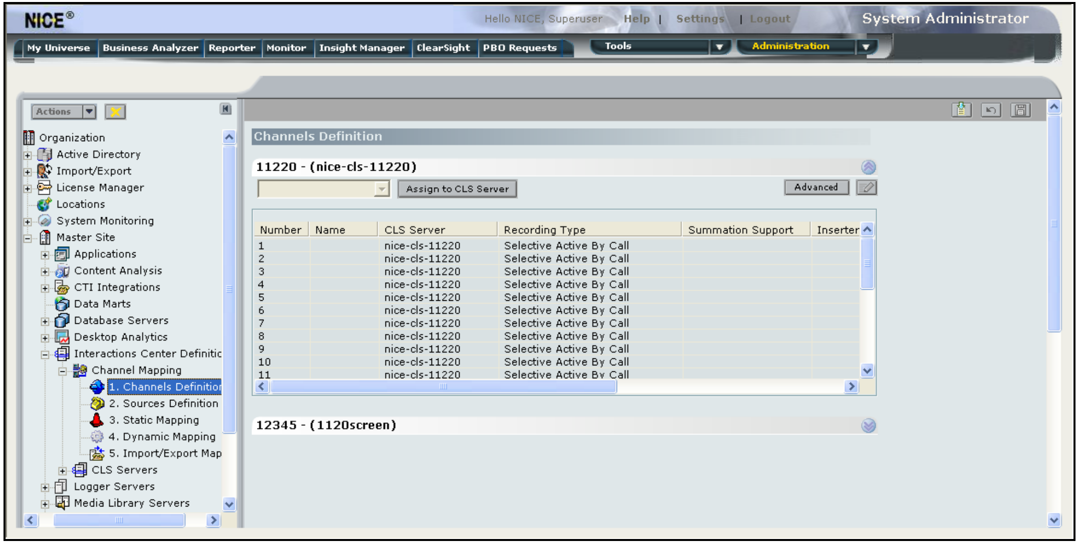
Additional Driver Switch Parameters

Field Mapping

2. **Configure the Logger Channel Mappings**

The Logger is the module that will be responsible for dedicating an available “channel” for each call to be recorded, initiating the Invite to the Session Border Controller, and receiving and storing the RTP media sent from the Session Border Controller.

Navigate to the **Master Site > Interactions Center Definitions > Channel Mapping > Channels Definition** object in the navigation tree. For each channel, click the **Edit** button and set the **Recording Type** to ***Selective Active By Call***. The dialog looks similar to those above, but is not available to illustrate as the system blocks modifying the configuration once the channels are assigned.



Channels Definition

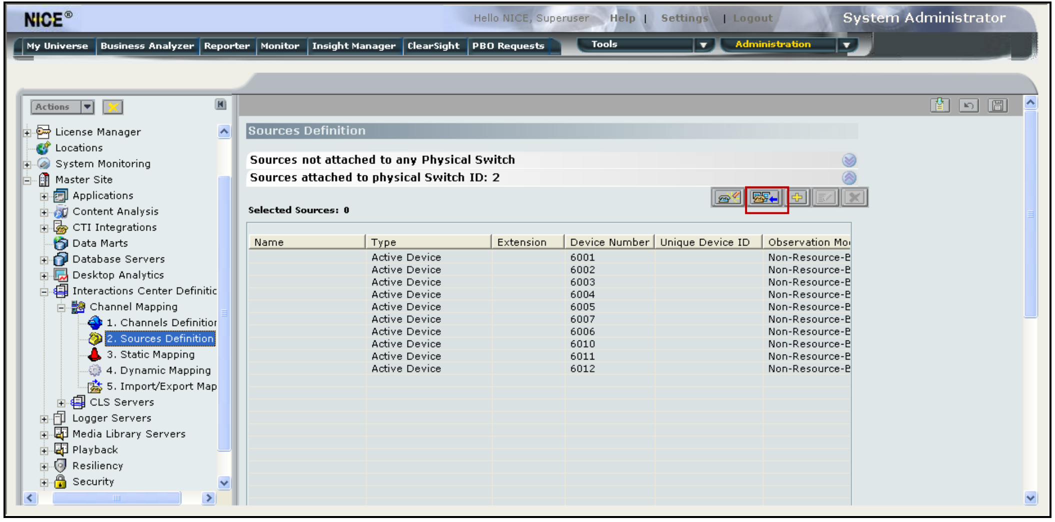
11220 - (nice-cls-11220)

Number	Name	CLS Server	Recording Type	Summation Support	Inserter
1		nice-cls-11220	Selective Active By Call		
2		nice-cls-11220	Selective Active By Call		
3		nice-cls-11220	Selective Active By Call		
4		nice-cls-11220	Selective Active By Call		
5		nice-cls-11220	Selective Active By Call		
6		nice-cls-11220	Selective Active By Call		
7		nice-cls-11220	Selective Active By Call		
8		nice-cls-11220	Selective Active By Call		
9		nice-cls-11220	Selective Active By Call		
10		nice-cls-11220	Selective Active By Call		
11		nice-cls-11220	Selective Active By Call		

12345 - (1120screen)

Configure the Logger Channel Mappings (continued)

In **Sources Definition** create your sources as ***Active Device*** using the **Import Sources from CTI Interface** button under the **Sources attached to physical Switch ID: 1** section and using the wizard to complete the task.



Sources Definition

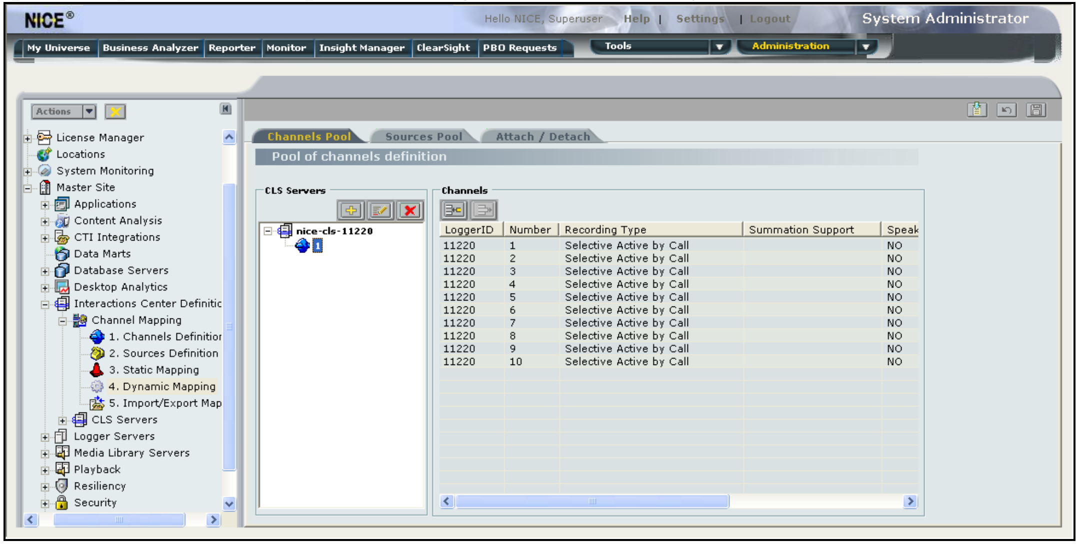
Sources not attached to any Physical Switch

Sources attached to physical Switch ID: 2

Selected Sources: 0

Name	Type	Extension	Device Number	Unique Device ID	Observation Mo
	Active Device		6001		Non-Resource-B
	Active Device		6002		Non-Resource-B
	Active Device		6003		Non-Resource-B
	Active Device		6004		Non-Resource-B
	Active Device		6005		Non-Resource-B
	Active Device		6007		Non-Resource-B
	Active Device		6006		Non-Resource-B
	Active Device		6010		Non-Resource-B
	Active Device		6011		Non-Resource-B
	Active Device		6012		Non-Resource-B

Next, go to **Dynamic Mapping** and define a new channel pool using the button. This snapshot captures the completed configuration of this object.



Pool of channels definition

CLS Servers

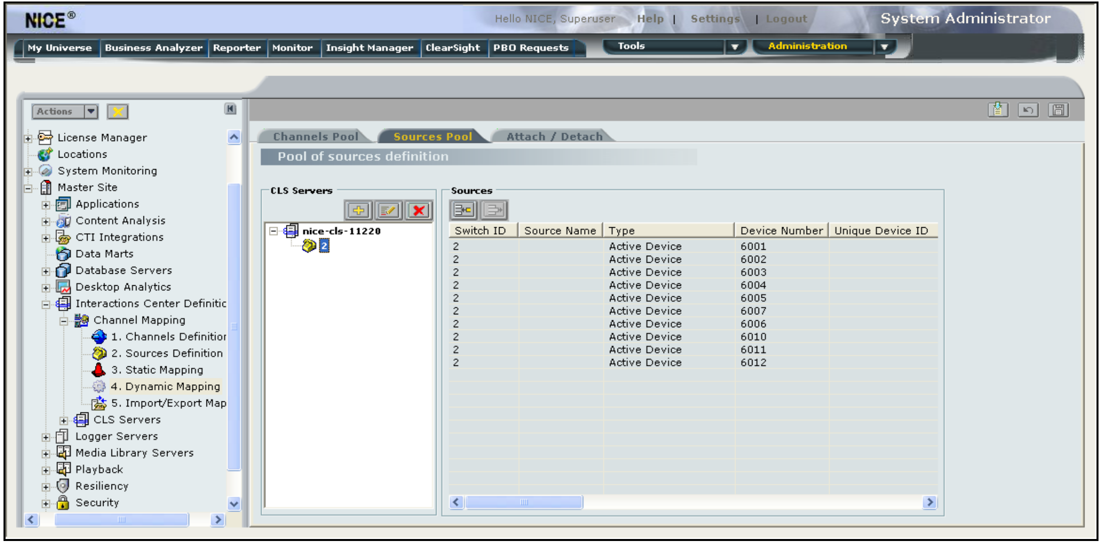
nice-cls-11220

Channels

LoggerID	Number	Recording Type	Summation Support	Speak
11220	1	Selective Active by Call		NO
11220	2	Selective Active by Call		NO
11220	3	Selective Active by Call		NO
11220	4	Selective Active by Call		NO
11220	5	Selective Active by Call		NO
11220	6	Selective Active by Call		NO
11220	7	Selective Active by Call		NO
11220	8	Selective Active by Call		NO
11220	9	Selective Active by Call		NO
11220	10	Selective Active by Call		NO

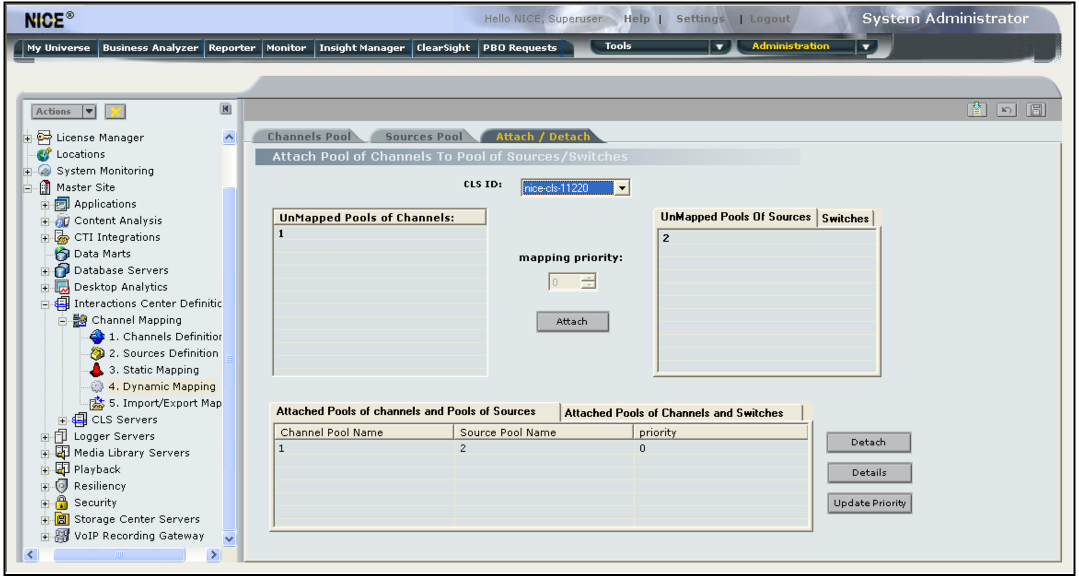
Configure the Logger Channel Mappings (continued)

Click on the **Sources Pool** tab and add your devices to the pool:



Switch ID	Source Name	Type	Device Number	Unique Device ID
2		Active Device	6001	
2		Active Device	6002	
2		Active Device	6003	
2		Active Device	6004	
2		Active Device	6005	
2		Active Device	6007	
2		Active Device	6006	
2		Active Device	6010	
2		Active Device	6011	
2		Active Device	6012	

Finally Go to the **Attach /Detach** tab and attach the pool of channels to the pool of sources. When complete, click Save and Update Configuration buttons on the top right corner of the System Administrator interface.



CLS ID: nice-cls-11220

UnMapped Pools of Channels:
1

mapping priority: 0

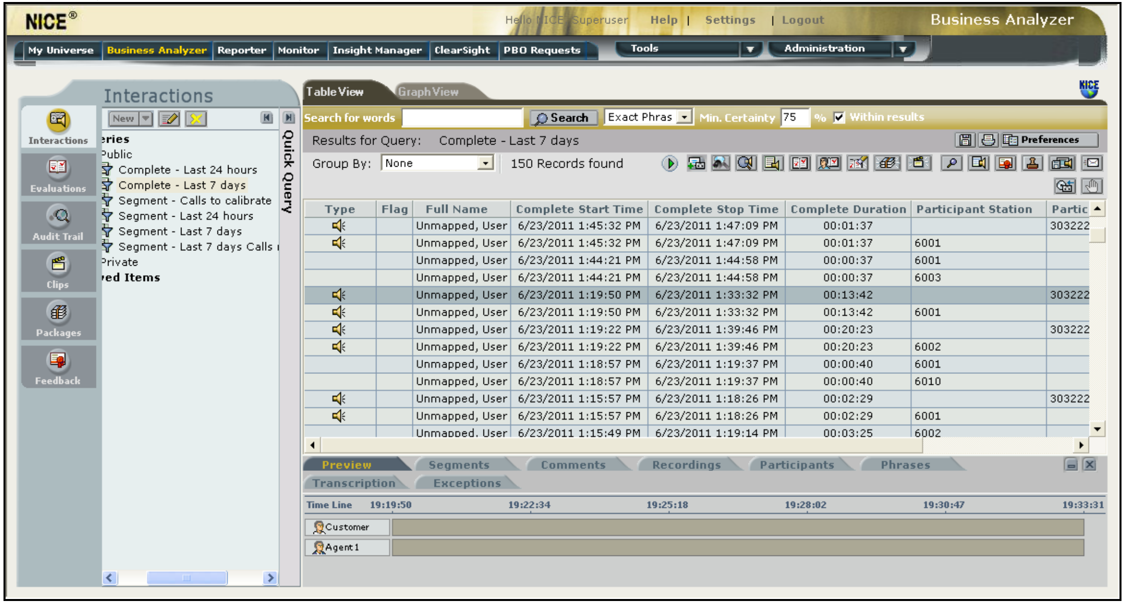
UnMapped Pools Of Sources
2

Attached Pools of channels and Pools of Sources

Channel Pool Name	Source Pool Name	priority
1	2	0

10. Verification Steps

Following each completed test case, the NICE Perform Business Analyzer user application was used to query for the recently completed recordings and initiate a playback.


NICE
Hello NICE, Superuser | Help | Settings | Logout
Business Analyzer
My Universe | Business Analyzer | Reporter | Monitor | Insight Manager | ClearSight | PBO Requests | Tools | Administration
Interactions
Evaluations
Audit Trail
Clips
Packages
Feedback
Quick Query
Table View
Graph View
Search
Exact Phras
Preferences
Preview | Segments | Comments | Recordings | Participants | Phrases
Transcription | Exceptions
Customer
Agent1

Interactions

- eries
- Public
- Complete - Last 24 hours
- Complete - Last 7 days
- Segment - Calls to calibrate
- Segment - Last 24 hours
- Segment - Last 7 days
- Segment - Last 7 days Calls
- Private
- ed Items

Search for words: Exact Phras Min. Certainty 75 % ☑ Within results

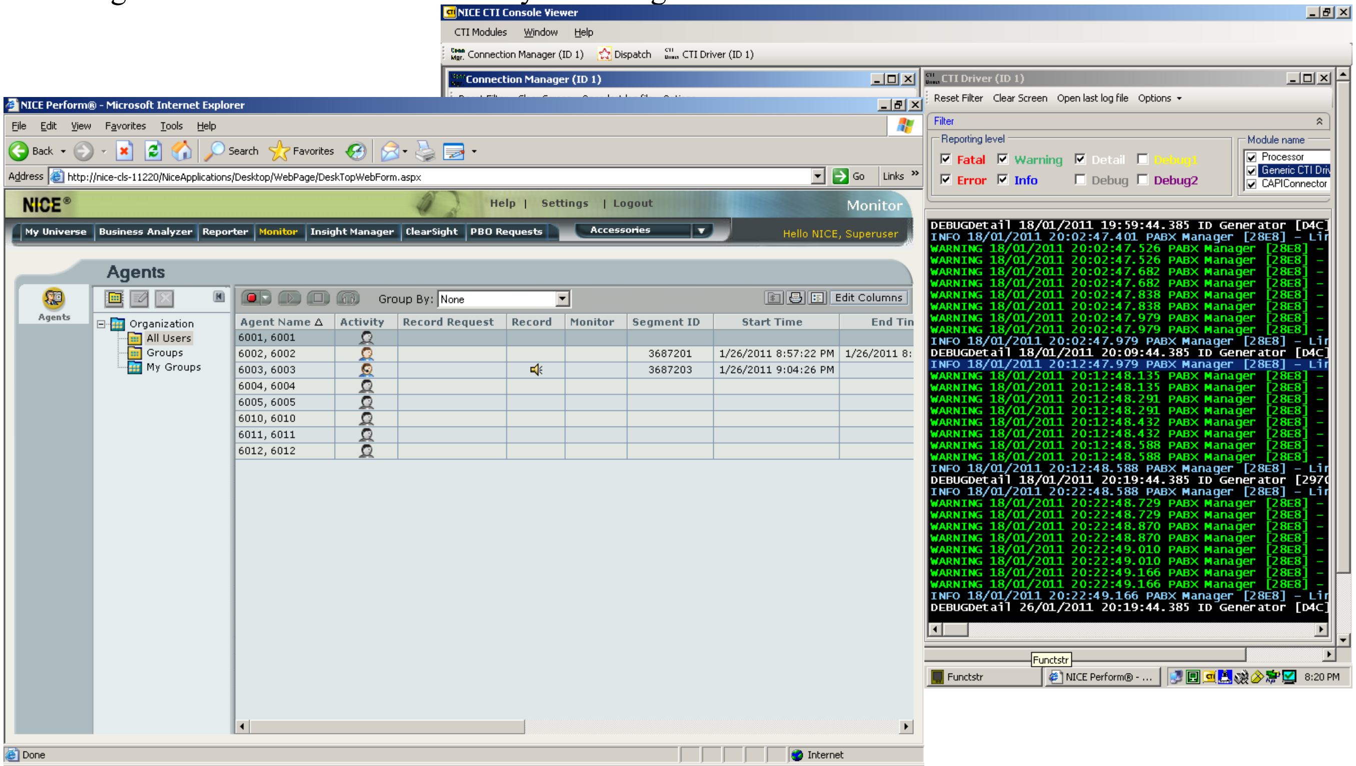
Results for Query: Complete - Last 7 days

Group By: None 150 Records found

Type	Flag	Full Name	Complete Start Time	Complete Stop Time	Complete Duration	Participant Station	Partic
🔈		Unmapped, User	6/23/2011 1:45:32 PM	6/23/2011 1:47:09 PM	00:01:37		303222
🔈		Unmapped, User	6/23/2011 1:45:32 PM	6/23/2011 1:47:09 PM	00:01:37	6001	
		Unmapped, User	6/23/2011 1:44:21 PM	6/23/2011 1:44:58 PM	00:00:37	6001	
		Unmapped, User	6/23/2011 1:44:21 PM	6/23/2011 1:44:58 PM	00:00:37	6003	
🔈		Unmapped, User	6/23/2011 1:19:50 PM	6/23/2011 1:33:32 PM	00:13:42		303222
🔈		Unmapped, User	6/23/2011 1:19:50 PM	6/23/2011 1:33:32 PM	00:13:42	6001	
🔈		Unmapped, User	6/23/2011 1:19:22 PM	6/23/2011 1:39:46 PM	00:20:23		303222
🔈		Unmapped, User	6/23/2011 1:19:22 PM	6/23/2011 1:39:46 PM	00:20:23	6002	
		Unmapped, User	6/23/2011 1:18:57 PM	6/23/2011 1:19:37 PM	00:00:40	6001	
		Unmapped, User	6/23/2011 1:18:57 PM	6/23/2011 1:19:37 PM	00:00:40	6010	
🔈		Unmapped, User	6/23/2011 1:15:57 PM	6/23/2011 1:18:26 PM	00:02:29		303222
🔈		Unmapped, User	6/23/2011 1:15:57 PM	6/23/2011 1:18:26 PM	00:02:29	6001	
		Unmapped, User	6/23/2011 1:15:49 PM	6/23/2011 1:19:14 PM	00:03:25	6002	

Time Line 19:19:50 19:22:34 19:25:18 19:28:02 19:30:47 19:33:31

In addition, the Console Viewer application shown below displays the status of CTI Driver and inter-process communications on the Nice Perform server. The Monitor application will display a recording icon when a call is successfully recording.


NICE CTI Console Viewer
CTI Modules | Window | Help
Connection Manager (ID 1) | Dispatch | CTI Driver (ID 1)
Connection Manager (ID 1)
CTI Driver (ID 1)
Reset Filter | Clear Screen | Open last log file | Options
NICE Perform® - Microsoft Internet Explorer
File | Edit | View | Favorites | Tools | Help
Back | Search | Favorites
Address | Go | Links
NICE
Help | Settings | Logout
Monitor
My Universe | Business Analyzer | Reporter | Monitor | Insight Manager | ClearSight | PBO Requests | Accessories
Hello NICE, Superuser
Agents
Organization
All Users
Groups
My Groups
Edit Columns
Done
Internet
Functstr
NICE Perform® - ...
8:20 PM

Address: http://nice-cls-11220/NiceApplications/Desktop/WebPage/DeskTopWebForm.aspx

Group By: None

Agent Name ∆	Activity	Record Request	Record	Monitor	Segment ID	Start Time	End Tin
6001, 6001							
6002, 6002					3687201	1/26/2011 8:57:22 PM	1/26/2011 8:
6003, 6003			🔈		3687203	1/26/2011 9:04:26 PM	
6004, 6004							
6005, 6005							
6010, 6010							
6011, 6011							
6012, 6012							

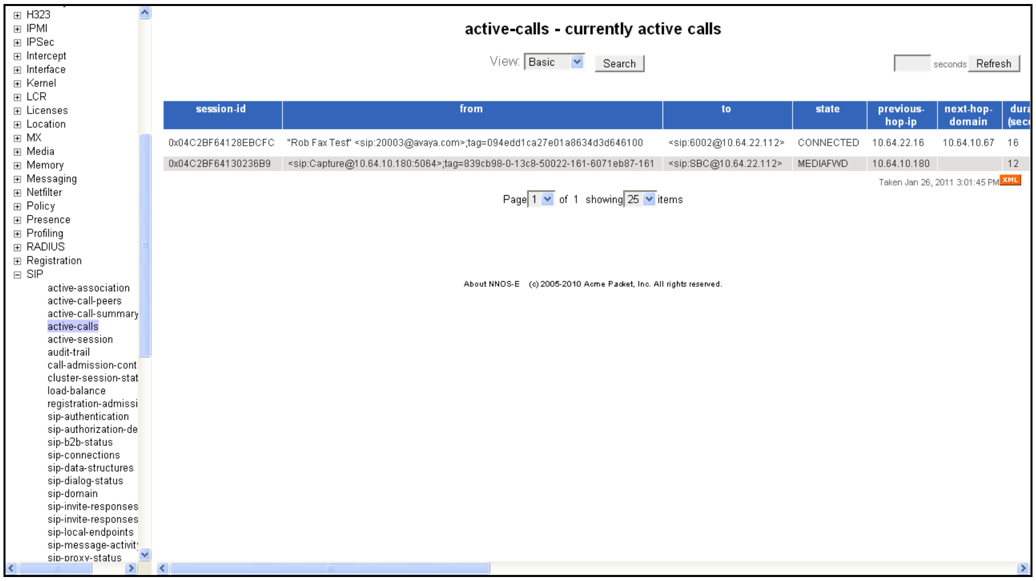
Filter

Reporting level: ☑ Fatal ☑ Warning ☑ Detail □ Debug1 ☑ Error ☑ Info □ Debug □ Debug2

Module name: ☑ Processor ☑ Generic CTI Driv ☑ CAPIConnector

```
DEBUGDetail 18/01/2011 19:59:44.385 ID Generator [D4C]
INFO 18/01/2011 20:02:47.401 PABX Manager [28E8] - Lin
WARNING 18/01/2011 20:02:47.526 PABX Manager [28E8] -
WARNING 18/01/2011 20:02:47.526 PABX Manager [28E8] -
WARNING 18/01/2011 20:02:47.682 PABX Manager [28E8] -
WARNING 18/01/2011 20:02:47.682 PABX Manager [28E8] -
WARNING 18/01/2011 20:02:47.838 PABX Manager [28E8] -
WARNING 18/01/2011 20:02:47.838 PABX Manager [28E8] -
WARNING 18/01/2011 20:02:47.979 PABX Manager [28E8] -
WARNING 18/01/2011 20:02:47.979 PABX Manager [28E8] -
INFO 18/01/2011 20:02:47.979 PABX Manager [28E8] - Lin
DEBUGDetail 18/01/2011 20:09:44.385 ID Generator [D4C]
INFO 18/01/2011 20:12:47.979 PABX Manager [28E8] - Lin
WARNING 18/01/2011 20:12:48.135 PABX Manager [28E8] -
WARNING 18/01/2011 20:12:48.135 PABX Manager [28E8] -
WARNING 18/01/2011 20:12:48.291 PABX Manager [28E8] -
WARNING 18/01/2011 20:12:48.291 PABX Manager [28E8] -
WARNING 18/01/2011 20:12:48.432 PABX Manager [28E8] -
WARNING 18/01/2011 20:12:48.432 PABX Manager [28E8] -
WARNING 18/01/2011 20:12:48.588 PABX Manager [28E8] -
WARNING 18/01/2011 20:12:48.588 PABX Manager [28E8] -
INFO 18/01/2011 20:12:48.588 PABX Manager [28E8] - Lin
DEBUGDetail 18/01/2011 20:19:44.385 ID Generator [297C
INFO 18/01/2011 20:22:48.588 PABX Manager [28E8] - Lin
WARNING 18/01/2011 20:22:48.729 PABX Manager [28E8] -
WARNING 18/01/2011 20:22:48.729 PABX Manager [28E8] -
WARNING 18/01/2011 20:22:48.870 PABX Manager [28E8] -
WARNING 18/01/2011 20:22:48.870 PABX Manager [28E8] -
WARNING 18/01/2011 20:22:49.010 PABX Manager [28E8] -
WARNING 18/01/2011 20:22:49.010 PABX Manager [28E8] -
WARNING 18/01/2011 20:22:49.166 PABX Manager [28E8] -
WARNING 18/01/2011 20:22:49.166 PABX Manager [28E8] -
INFO 18/01/2011 20:22:49.166 PABX Manager [28E8] - Lin
DEBUGDetail 26/01/2011 20:19:44.385 ID Generator [D4C]
```

On the Session Border Controller, the Status tab enables a view of active SIP calls, when the Perform application is successfully recording a call, a MEDIAFWD session will appear in the active call status screen:



active-calls - currently active calls

session-id	from	to	state	previous-hop-ip	next-hop-domain	dura (sec
0x04C2BF64128EBCFC	"Rob Fax Test" <sip:20003@avaya.com>;tag=094edd1ca27e01a8634d3d646100	<sip:6002@10.64.22.112>	CONNECTED	10.64.22.16	10.64.10.67	16
0x04C2BF64130236B9	<sip:Capture@10.64.10.180:5064>;tag=839cb98-0-13c8-50022-161-6071eb87-161	<sip:SBC@10.64.22.112>	MEDIAFWD	10.64.10.180		12

Taken Jan 26, 2011 3:01:45 PM

Page 1 of 1 showing 25 items

About NNOS-E (c) 2005-2010 Acme Packet, Inc. All rights reserved.

11. Conclusion

Nice Perform® successfully demonstrated the ability to record calls that passed through the Avaya Aura® Session Border Controller. Further, the application demonstrated the ability to successfully recover from network and server outages with minimal delay in recovering to full functionality.

12. Additional References

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

Administering Avaya Aura™ Session Manager, Document ID 03-603324, Issue 1, Release 6.1, November, 2010.
Avaya Aura™ Application Enablement Services Administration and Maintenance Guide, Document ID 02-300357, Issue 11, Release 5.2, November, 2009.
Avaya Aura™ SBC System Administration Guide, V6.0
Avaya Aura™ SBC Objects and Properties Reference, V6.0
Administering Avaya Aura™ Communication Manager Server Options, Document ID 03-603479, Issue 2, Release 6.0, June, 2010.
Administering Avaya Aura™ Communication Manager, Document ID 03-300509, Issue 6.0, Release 6.0, June, 2010.

Product information for Nice Perform® may be found in help screens on the Nice Perform® application server and online at http://www.nice.com

Appendix A

Session Border Controller Configuration File Contents

```
#
#  Copyright (c) 2004-2010  Acme Packet Inc.
#  All Rights Reserved.
#
#  File: /cxc/cxc.cfg
#  Date: 16:01:59 Wed 2011-06-05
#
config cluster
 config box 1
  set hostname AuraSBC.avaya.com
  set timezone America/Denver
  set name AuraSBC.avaya.com
  set identifier 00:ca:fe:88:95:64
  config interface eth0
   config ip inside
    set ip-address static 10.64.22.112/24
    config ssh
    return
    config snmp
     set trap-target 10.64.22.111 162
     set trap-filter generic
     set trap-filter dos
     set trap-filter sip
     set trap-filter system
    return
    config web
    return
    config web-service
     set protocol https 8443
     set authentication certificate "vsp\tls\certificate ws-cert"
    return
    config sip
     set udp-port 5060 "" "" any 0
     set tcp-port 5060 "" "" any 0
     set tls-port 5061 "" "" TLS 0 "vsp\tls\certificate aasbc.p12"
    return
    config icmp
    return
    config media-ports
    return
    config routing
     config route Default
      set gateway 10.64.22.1
     return
     config route Static0
      set destination network 192.11.13.4/30
      set gateway 10.64.22.110
     return
     config route Static1
      set admin disabled
     return
     config route Static2
      set admin disabled
     return
     config route Static3
      set admin disabled
     return
     config route Static4
      set admin disabled
     return
     config route Static5
      set admin disabled
     return
     config route Static6
```

```
      set admin disabled
     return
     config route Static7
      set admin disabled
     return
    return
   return
  return
  config interface eth2
   config ip outside
    set ip-address static 10.64.22.113/24
    config sip
     set tcp-port 5060 "" "" any 0
    return
    config media-ports
    return
    config routing
     config route Default
      set admin disabled
     return
     config route external-sip-media-1
      set destination network 10.64.22.0/24
      set gateway 10.64.22.1
     return
    return
   return
  return
  config cli
   set prompt AuraSBC.avaya.com
  return
 return
return

config services
 config event-log
  config file access
   set filter access info
   set count 3
  return
  config file system
   set filter system info
   set count 3
  return
  config file errorlog
   set filter all error
   set count 3
  return
  config file db
   set filter db debug
   set filter dosDatabase info
   set count 3
  return
  config file management
   set filter management info
   set count 3
  return
  config file peer
   set filter sipSvr info
   set count 3
  return
  config file dos
   set filter dos alert
   set filter dosSip alert
   set filter dosTransport alert
   set filter dosUrl alert
   set count 3
  return
  config file krnlsys
   set filter krnlsys debug
   set count 3
  return
 return
return

config master-services
 config database
  set media enabled
 return
return

config vsp
 set admin enabled
 config default-session-config
  config sip-settings
  return
  config to-uri-specification
   set host next-hop
   set port next-hop
   set transport next-hop
  return
  config from-uri-specification
   set host local-ip
   set port local
  return
  config request-uri-specification
   set host next-hop
   set port next-hop
   set transport next-hop
  return
  config media
   set anchor enabled
   config nat-traversal
    set symmetricRTP true
   return
   set rtp-stats enabled
  return
  config out-codec-preferences
   set preference audio pcmu 1
   set preference audio telephone-event 2
   set preference audio any 0
  return
  config sip-directive
   set directive allow
  return
  config log-alert
  return
  config forking-settings
   set outbound-arbiter-rule least-load
  return
  config header-settings
   set blocked-header Remote-Party-ID
   set blocked-header P-Asserted-Identity
  return
  config third-party-call-control
   set admin enabled
  return
  config uui-header
   set admin enabled
   set node-id 1
  return
 return
 config tls
  config default-ca
   set ca-file /cxc/certs/sipca.pem
  return
  config certificate ws-cert
   set certificate-file /cxc/certs/ws.cert
  return
  config certificate aasbc.p12
   set certificate-file /cxc/certs/aasbc.p12
   set passphrase-tag aasbc-cert-tag
  return
 return
 config pre-session-config
  set unregistered-sender-directive discard
 return
 config policies
  config session-policies
   set default-policy vsp\policies\session-policies\policy sbc
   config policy sbc
    config rule sbc
     config condition-list
      set sip-message-condition request-uri contains SBC@
     return
     config session-config
      config sip-directive
       set directive allow
      return
      config third-party-call-control
       set admin enabled
       set media-shuffle disabled
       set media-forward enabled
       set track-to-user enabled
       set terminate-update-locally enabled
      return
     return
    return
   return
  return
 return
 config static-stack-settings
 return
 config session-config-pool
  config entry ToTelco
   config to-uri-specification
    set host next-hop
   return
   config from-uri-specification
    set host local-ip
   return
   config request-uri-specification
    set host next-hop
   return
   config p-asserted-identity-uri-specification
    set host local-ip
   return
  return
  config entry ToPBX
   config to-uri-specification
    set host next-hop-domain
   return
   config request-uri-specification
    set host next-hop-domain
   return
  return
  config entry Discard
   config sip-directive
   return
  return
 return
 config dial-plan
  config source-route FromTelco
   set peer server "vsp\enterprise\servers\sip-gateway PBX"
   set source-match server "vsp\enterprise\servers\sip-gateway Telco"
  return
  config source-route FromPBX
   set peer server "vsp\enterprise\servers\sip-gateway Telco"
```

```
   set source-match server "vsp\enterprise\servers\sip-gateway PBX"
  return
 return
 config enterprise
  config servers
   config sip-gateway PBX
    set domain avaya.com
    set failover-detection ping
    set outbound-session-config-pool-entry vsp\session-config-pool\entry ToPBX
    config server-pool
     config server "Session Manager"
      set host 10.64.21.31
      set transport TCP
     return
    return
   return
   config sip-gateway Telco
    set domain avaya.com
    set failover-detection ping
    set outbound-session-config-pool-entry vsp\session-config-pool\entry ToTelco
    config server-pool
     config server Telco1
      set host 10.64.22.16
      set transport TCP
     return
    return
   return
   config sip-gateway NICE
    set domain avaya.com
    set outbound-session-config-pool-entry vsp\session-config-pool\entry ToPBX
    config server-pool
     config server NICE
      set host 10.64.10.180
     return
    return
   return
  return
 return
 config dns
  config resolver
   config server 205.171.3.65
   return
   config server 205.171.2.65
    set preference 101
   return
  return
 return
 config settings
  set read-header-max 8191
 return
return

config external-services
return

config preferences
 config gui-preferences
 return
return

config access
 config permissions superuser
  set cli advanced
 return
 config permissions read-only
  set config view
  set actions disabled
 return
 config users
```

```
  config user admin
   set password 0x00294af93c871198678ce97c4083c317f8a437765001347649f38ab2aa
   set permissions access\permissions superuser
  return
  config user cust
   set password 0x00bea31439f3abe5ffcc62594dc4af5a772c833cb1ce2ee3c71b60503d
   set permissions access\permissions read-only
  return
  config user init
   set password 0x00b6414a2be8ecc0c7de4623c1ae1661e71f9a1c164549ca781e91e8a6
   set permissions access\permissions superuser
  return
  config user craft
   set password 0x006499848b529b0c6b0cb3b76f54249e9de4a8311cfaebc1c4228c4512
   set permissions access\permissions superuser
  return
  config user dadmin
   set password 0x00781aaf1e367eb73be1a1240fab2c30011f7a80d4814e582268fddfd8
   set permissions access\permissions read-only
  return
 return
return

config features
return
```

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.