6AOSCG0015-29A
March 2011

Configuration Guide

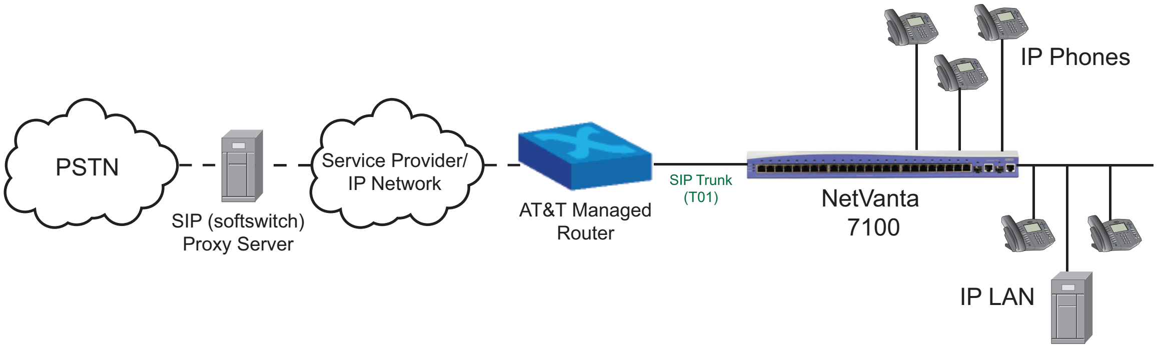
Configuring the NetVanta 7100 for AT&T's IP Flexible Reach Service

This configuration guide describes how to configure the NetVanta 7100 for use with AT&T's IP Flexible Reach Service Managed Internet Service (MIS)/Private Network Transport (PNT), including AT&T Business in a Box (BiB). This guide contains information about how to configure Session Initiation Protocol (SIP) trunk, fax, and user settings on the NetVanta 7100 using the Web-based graphical user interface (GUI) and the ADTRAN Operating System (AOS) command line interface (CLI).

This guide consists of the following sections:

Overview

ADTRAN's NetVanta 7100 Internet Protocol (IP) private branch exchange (PBX) supports SIP trunks delivered from AT&T's IP Flexible Reach Service (MIS/PNT), including AT&T BiB. The following sections of this document explain the application and configuration implementation of SIP trunking terminating directly into the NetVanta 7100 IP PBX.



SIP Trunking Overview

SIP is the industry standard ASCII-based peer-to-peer signaling protocol responsible for the initiation and management of IP voice communication sessions. SIP is designed to control call setup and tear down between IP endpoint devices. The basic function of SIP is to locate endpoints, signal a desire to communicate, establish sessions, and tear down sessions between endpoints. The current version of SIP (2.0) is defined in RFC 3261.

SIP trunking is a packet-based voice service that routes calls over an IP network to an IP-compatible PBX or voice switch using SIP signaling to place and receive calls. The typical SIP trunk service provider offers extensive cost savings, compared to conventional trunk services. The IP connection to the provider carries all traffic, such as local, long distance, and toll free calls, video, email, Internet, data, and other media over a single circuit. Calls into public switched telephone network (PSTN) are also handled by the SIP service provider by passing the calls off to a media gateway that connects to the PSTN for users not using Voice over Internet Protocol (VoIP) service.

Hardware and Software Requirements and Limitations

AOS firmware version A2.07.00.SC.E was used to test AT&T’s IP Flexible Reach Service MIS/PNT, including BiB.

When configuring the SIP trunk for IP Flexible Reach over MIS/PNT, the administrator must use the CLI to add a secondary SIP server during the SIP trunk configuration step.

The NetVanta 7100 does not anchor Realtime Transport Protocol (RTP) when calls are forwarded from the IP phone or when forwarded from within the NetVanta 7100 user account.

The NetVanta 7100 supports user-initiated conferences, but does not include a conference server. The NetVanta Business Communications Server can be attached to any NetVanta 7100 adding additional functionality including meet me conference capability, a visual auto attendant, fax server, and unified messaging.

Since the NetVanta 7100 will be deployed behind an AT&T managed router, no quality of service (QoS) or shaping configuration will be present on the NetVanta 7100. All QoS and/or shaping should be done in the wide area network (WAN) router. If the NetVanta 7100 is used to terminate the WAN, refer to the *Configuring Quality of Service (QoS) in AOS* configuration guide (ADTRAN's Knowledge Base article 2219).

Emergency 911/E911 Services Limitations and Restrictions

Although AT&T provides 911/E911 calling capabilities, AT&T does not warrant or represent that the equipment and software (e.g., IP PBX) reviewed in this customer configuration guide will properly operate with AT&T IP Flexible Reach to complete 911/E911 calls. Therefore, it is the customer's responsibility to ensure proper operation with their equipment/software vendor.

While AT&T IP Flexible Reach services support E911/911 calling capabilities under certain Calling Plans, there are circumstances when 911/E911 service may not be available, as stated in the Service Guide for AT&T IP Flexible Reach found at http://new.serviceguide.att.com. Such circumstances include, but are not limited to, relocation of the end user's customer premises equipment (CPE), use of a non-native or virtual telephone number, failure in the broadband connection, loss of electrical power, and delays that may occur in updating the customer's location in the automatic location information database. Please review the AT&T IP Flexible Reach Service Guide in detail to understand the limitations and restrictions.

> NOTE *N11 (including 911) calls are not supported unless AT&T IP Flexible Reach Local Service is ordered.*

IP Phones and Third Party Vendors Supported

An up-to-date list of supported IP phones can be found at the NetVanta 7100 product page on the ADTRAN website.

ADTRAN Phones - IP706, IP712, IP SoftPhone
Software version tested: 1.3.13

Polycom Phones - IP301, IP321/331, IP430, IP450, IP501, IP550, IP560, IP601, IP650, IP670, IP6xx Expansion Modules, IP5000, IP6000, VVX1500
Application version tested: 3.1.3
Boot version tested: 4.1.2

> NOTE *IP phone software is automatically upgraded to the latest version by the NetVanta 7100.*

RSI - CDR/Call Accounting

SIP Print - Call Recording

Incendonet - Speech Recognition

Lifesize - Video Conference

Multitech - Fax Server

Configuring the NetVanta 7100 for AT&T SIP Trunking Service

To configure the NetVanta 7100 for AT&T SIP trunk and fax settings using the GUI, follow these steps:

- Access the GUI
- Enable SIP privacy
- Configure a new coder-decoder (CODEC) list
- Enable detection of inbound fax calls
- Create a SIP trunk account
- Configure a trunk group
- Add reject template PSTN trunk groups
- Restrict SIP traffic
- Add a SIP identity to a voice user
- Enable modem passthrough and T.38 on an analog user
- Save the configuration

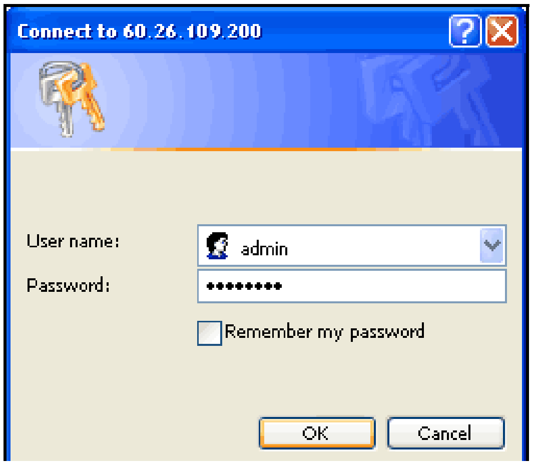
Accessing the GUI

To access the GUI, follow these steps:

1. Open a new Web page in your Internet browser.
2. Enter your AOS product's IP address in the Internet browser's address field in the following form: **http://**<*ip address*>**/admin**. For example:

   http://60.26.109.200/admin

3. At the prompt, enter your user name and password and select **OK**.



Connect to 60.26.109.200

User name: admin

Password: ••••••••

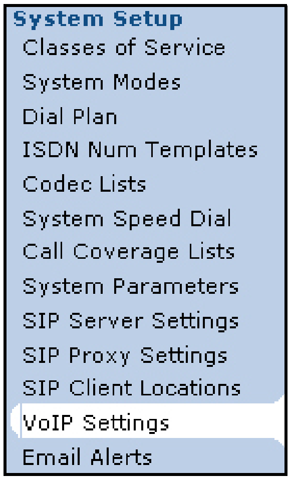
*The default user name is **admin** and the default password is **password**.*

Enabling SIP Privacy

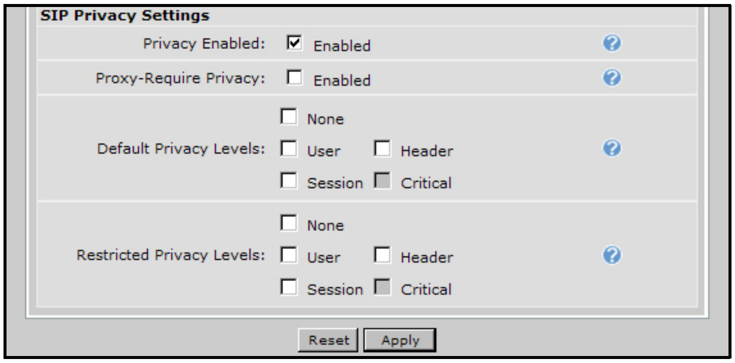
SIP privacy specifies that outbound calls include SIP privacy headers and inbound calls are filtered based on privacy settings.

To configure SIP privacy using the GUI, follow these steps:

1. Navigate to **Voice** > **System Setup** > **VoIP Settings** to access the **VoIP Settings** menu.



2. In the **SIP Settings** tab under **SIP Privacy Settings**, select the check box next to **Privacy Enabled** and select **Apply**.



SIP Privacy Settings

Privacy Enabled:	☑ Enabled
Proxy-Require Privacy:	□ Enabled
Default Privacy Levels:	□ None □ User □ Header □ Session □ Critical
Restricted Privacy Levels:	□ None □ User □ Header □ Session □ Critical

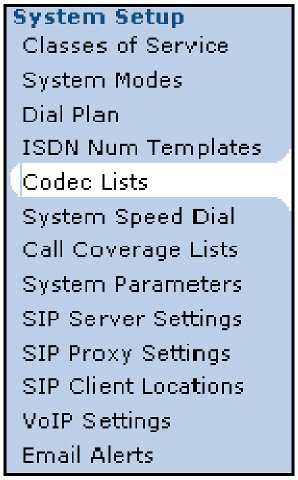
Configuring a CODEC List

Voice CODEC lists are lists of CODECs arranged in preferred order with the first listed CODEC being the most preferred for call negotiation. Order is important when creating a CODEC list. The interface attempts to use the first CODEC in the list to negotiate a call. If the first CODEC negotiation is unsuccessful, the interface uses the second CODEC in the list and so on. If this process is unsuccessful, the call will fail.

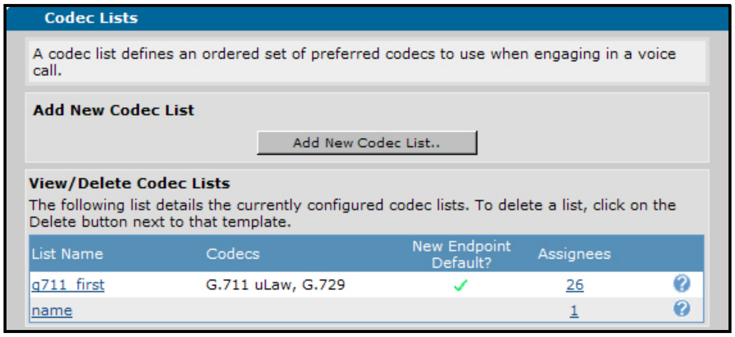
The primary reason to create and assign voice CODEC lists is to save time. CODEC lists are created, listing CODECs in the order of preference, and then lists are applied to interfaces. Configuring a CODEC list allows the list to be applied to multiple interfaces, such as Media Gateway Control Protocol (MGCP) interfaces, voice trunks, voice accounts, and voice users without having to define the order of CODECs individually. The order of preference is used primarily to conserve bandwidth on WAN-based interfaces.

To configure a CODEC list using the GUI, follow these steps:

1. Navigate to **Voice > System Setup > Codec Lists** to access the **Codec Lists** menu.



2. Select the **Add New Codec List** button. The **Add New Codec List** menu will appear.



Codec Lists

A codec list defines an ordered set of preferred codecs to use when engaging in a voice call.

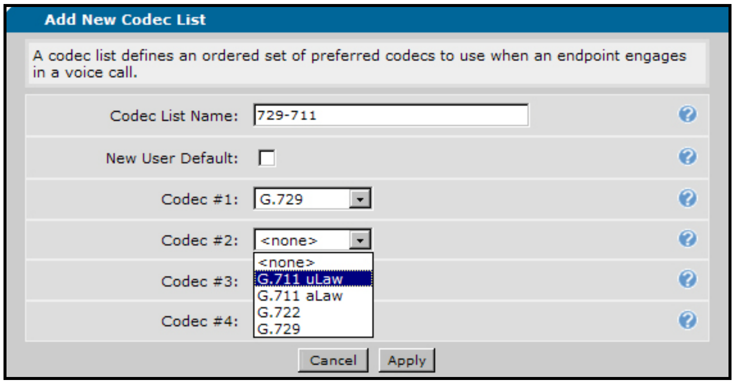
Add New Codec List

View/Delete Codec Lists

The following list details the currently configured codec lists. To delete a list, click on the Delete button next to that template.

List Name	Codecs	New Endpoint Default?	Assignees	
g711_first	G.711 uLaw, G.729	✓	26	?
name			1	?

3. In the **Codec List Name** field, enter a descriptive name for the CODEC list.



Add New Codec List

A codec list defines an ordered set of preferred codecs to use when an endpoint engages in a voice call.

Codec List Name: 729-711

New User Default: □

Codec #1: G.729

Codec #2: <none>

Codec #3:

Codec #4:

4. Using the **Codec #1** drop-down menu, select the **G.729** CODEC.
5. Using the **Codec #2** drop-down menu, select the **G.711 uLaw** CODEC.
6. Select the **Apply** button to apply the changes to the system configuration.

Enabling Inbound Fax Call Detection

Inbound fax call detection provides modem passthrough on gateway calls inbound from a VoIP network. Modem passthrough allows modem and fax calls to maintain a connection without altering the signal with voice improvement settings, such as echo cancellation and VAD.

Inbound fax call detection can only be configured using the CLI. For more information on enabling inbound fax call detection, refer to *Enabling Inbound Fax Call Detection on page 21*.

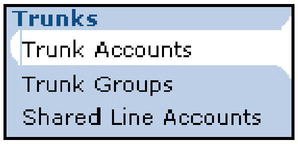
Creating a SIP Trunk Account

The SIP trunk is where all IP information and SIP messaging to the SIP network are configured.

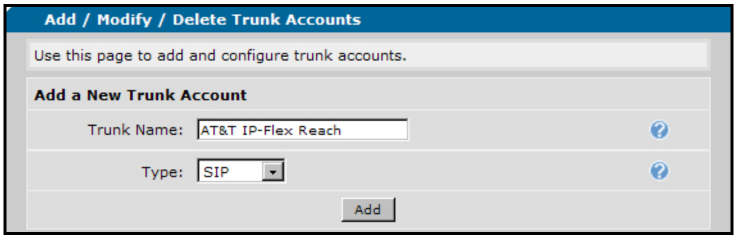
> NOTE
>
> *In A2.07.00.SC.E, a secondary SIP server must be configured using the CLI. Refer to Creating a SIP Trunk Account on page 22 for more information on configuring a secondary SIP server.*

To configure a SIP trunk account using the GUI, follow these steps:

1. Navigate to **Voice** > **Trunks** > **Trunk Accounts** to access the trunk accounts menu.



2. In the **Add a New Trunk Account** section, enter the desired name for the SIP trunk in the **Trunk Name** field. Select **SIP** as the trunk type using the **Type** drop-down menu.



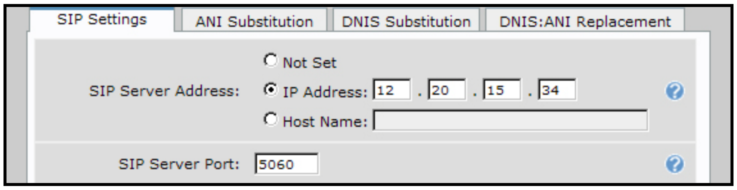
Use this page to add and configure trunk accounts.

Add a New Trunk Account

Trunk Name: AT&T IP-Flex Reach

Type: SIP

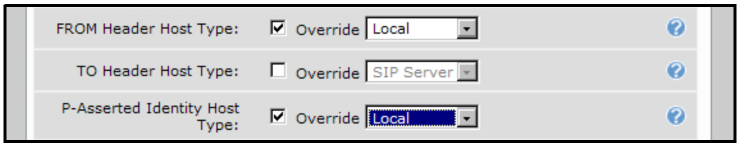
3. Select **Add** to create the new trunk account. The **Edit SIP Trunk** menu will appear.
4. On the **SIP Settings** tab, enter the **SIP Server Address** using either the specific host name with the fully qualified domain name (FQDN) or the IP address on which the trunks will terminate and the appropriate port (port **5060**).



SIP Server Address: ○ Not Set
● IP Address: 12 . 20 . 15 . 34
○ Host Name:

SIP Server Port: 5060

5. Enable the **FROM Header Host Type** using the **Override** check box, and select **Local** using the drop-down menu.

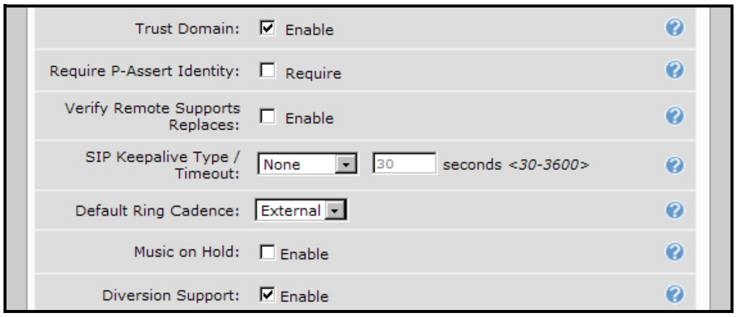


FROM Header Host Type: ☑ Override Local

TO Header Host Type: □ Override SIP Server

P-Asserted Identity Host Type: ☑ Override Local

6. Enable the **P-Asserted Identity Host Type** using the **Override** check box, and select **Local** using the drop-down menu.
7. Enable **Trust Domain** and **Diversion Support** by selecting the **Enable** check boxes.



Trust Domain: ☑ Enable

Require P-Assert Identity: □ Require

Verify Remote Supports Replaces: □ Enable

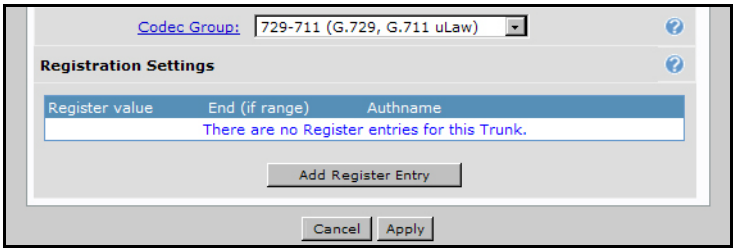
SIP Keepalive Type / Timeout: None 30 seconds *<30-3600>*

Default Ring Cadence: External

Music on Hold: □ Enable

Diversion Support: ☑ Enable

8. Select the new CODEC group for use on this SIP trunk using the **Codec Group** drop-down menu and select **Apply** to apply the configuration settings.



Codec Group: 729-711 (G.729, G.711 uLaw)

Registration Settings

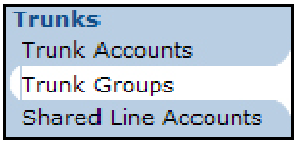
Register value	End (if range)	Authname
There are no Register entries for this Trunk.		

Configuring Trunk Groups

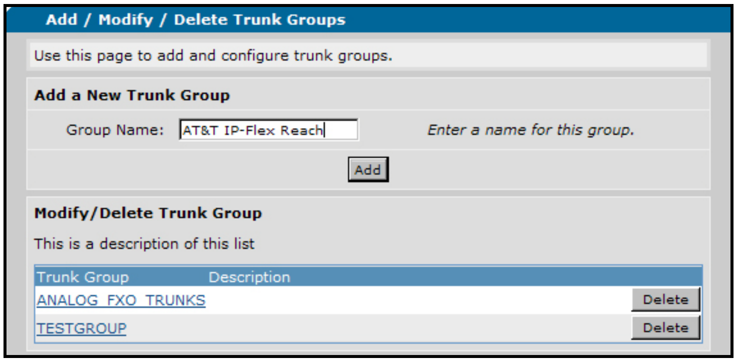
Trunk groups comprise one or more trunk accounts. They are used to assign outbound call capabilities (local calls, long distance calls, etc.). A cost is assigned to each attribute in the outbound call template and is used to select lowest cost route when multiple trunk groups are present on the NetVanta 7100. Use this section to create a trunk group, add the trunk account members to the group, and define the outbound call templates and costs.

To configure trunk groups using the GUI, follow these steps:

1. Navigate to **Voice** > **Trunks** > **Trunk Groups** to access the **Trunk Groups** menu.



2. In the **Add a New Trunk Group** section, enter a name for the trunk group in the **Group Name** field.



Add / Modify / Delete Trunk Groups

Use this page to add and configure trunk groups.

Add a New Trunk Group

Group Name: AT&T IP-Flex Reach

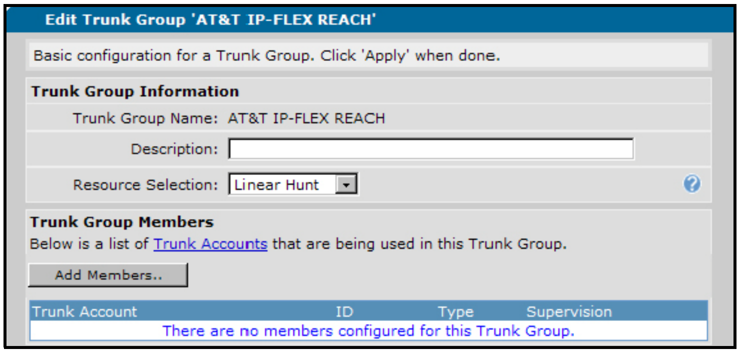
Enter a name for this group.

Modify/Delete Trunk Group

This is a description of this list

Trunk Group	Description	
ANALOG_FXO_TRUNKS		Delete
TESTGROUP		Delete

3. Select the **Add** button to add the new trunk group and access the **Edit Trunk Group** menu.
4. In the **Edit Trunk Group** menu, select the **Add Members** button to add members to the trunk group. The **Add Members to Trunk Group** menu will appear.



Edit Trunk Group 'AT&T IP-FLEX REACH'

Basic configuration for a Trunk Group. Click 'Apply' when done.

Trunk Group Information

Trunk Group Name: AT&T IP-FLEX REACH

Description:

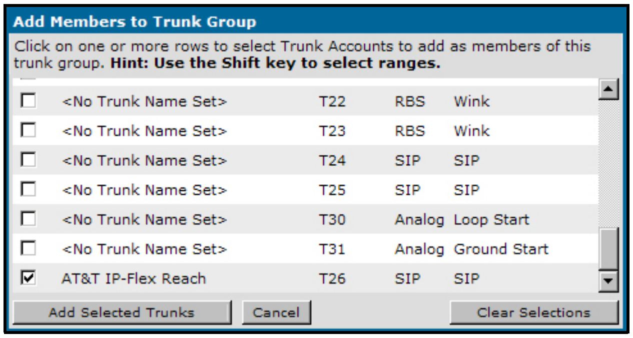
Resource Selection: Linear Hunt

Trunk Group Members

Below is a list of Trunk Accounts that are being used in this Trunk Group.

Trunk Account	ID	Type	Supervision
There are no members configured for this Trunk Group.			

5. Select the check box beside the name you entered for the AT&T IP Flex Reach SIP trunk account.



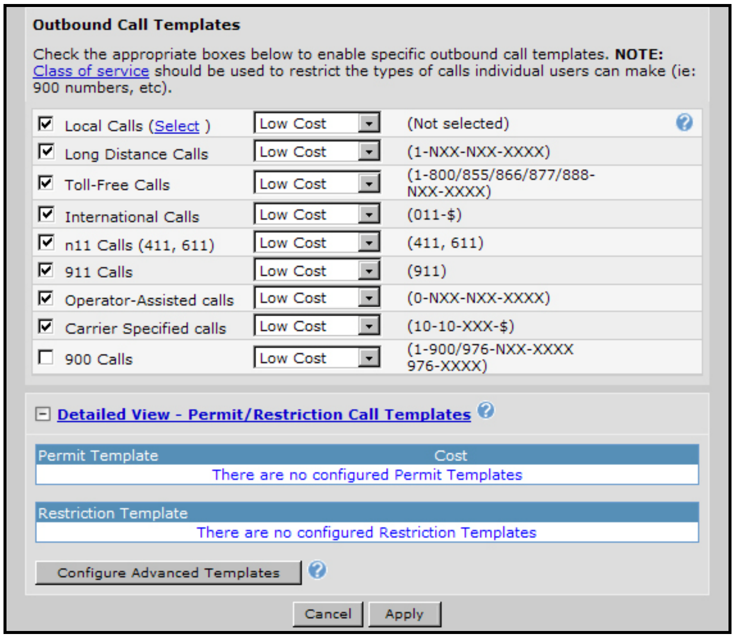
Add Members to Trunk Group

Click on one or more rows to select Trunk Accounts to add as members of this trunk group. **Hint: Use the Shift key to select ranges.**

☐	<No Trunk Name Set>	T22	RBS	Wink
☐	<No Trunk Name Set>	T23	RBS	Wink
☐	<No Trunk Name Set>	T24	SIP	SIP
☐	<No Trunk Name Set>	T25	SIP	SIP
☐	<No Trunk Name Set>	T30	Analog	Loop Start
☐	<No Trunk Name Set>	T31	Analog	Ground Start
☑	AT&T IP-Flex Reach	T26	SIP	SIP

6. Select **Add Selected Trunks** to add the selected trunk account to the trunk group and return to the **Edit Trunk Group** menu.

7. In the **Edit Trunk Group** menu under **Outbound Call Template** section, select the check boxes to enable the desired outbound call templates. Outbound call templates assign the types of calls that are permitted to be routed out the associated trunk.



Outbound Call Templates

Check the appropriate boxes below to enable specific outbound call templates. **NOTE:** Class of service should be used to restrict the types of calls individual users can make (ie: 900 numbers, etc).

☑ Local Calls (Select)	Low Cost	(Not selected)
☑ Long Distance Calls	Low Cost	(1-NXX-NXX-XXXX)
☑ Toll-Free Calls	Low Cost	(1-800/855/866/877/888-NXX-XXXX)
☑ International Calls	Low Cost	(011-$)
☑ n11 Calls (411, 611)	Low Cost	(411, 611)
☑ 911 Calls	Low Cost	(911)
☑ Operator-Assisted calls	Low Cost	(0-NXX-NXX-XXXX)
☑ Carrier Specified calls	Low Cost	(10-10-XXX-$)
☐ 900 Calls	Low Cost	(1-900/976-NXX-XXXX 976-XXXX)

⊟ Detailed View - Permit/Restriction Call Templates

Permit Template	Cost
There are no configured Permit Templates	

Restriction Template
There are no configured Restriction Templates

8. Select a cost for each enabled outbound call template using the associated drop-down menu. This option is used if a call is accepted by several trunks. The call will be routed to the trunk with the lowest cost value. **Low Cost** is an acceptable default.

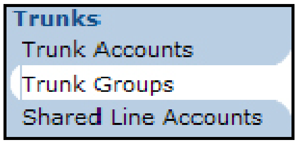
9. Select **Apply** at the bottom of the menu to accept the new settings and return to the **Trunk Groups** menu.

Adding Reject Templates to PSTN Trunk Groups

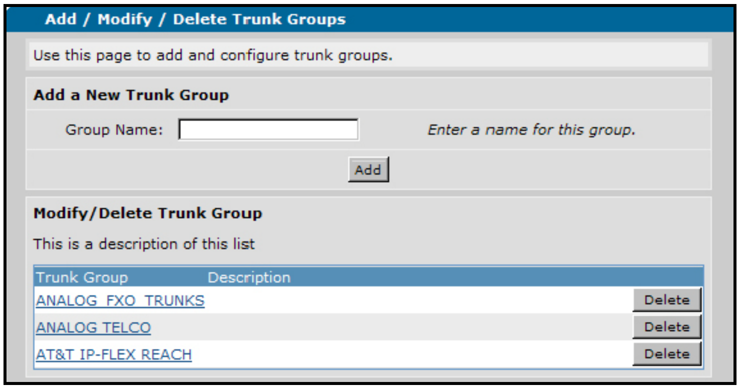
Reject templates are used on trunk groups to prevent calls to specific numbers from being routed out the specified trunks. If trunk groups for failover or PSTN connectivity are present in the NetVanta 7100 configuration, reject templates must be added for all telephone numbers supplied with the SIP trunk.

To add reject templates to a PSTN trunk group using the GUI, follow these steps:

1. Navigate to **Voice > Trunks > Trunk Groups** to access the **Trunk Groups** menu.



2. Select the trunk group associated with the PSTN connection. The **Edit Trunk Group** menu will appear.



Add / Modify / Delete Trunk Groups

Use this page to add and configure trunk groups.

Add a New Trunk Group

Group Name: *Enter a name for this group.*

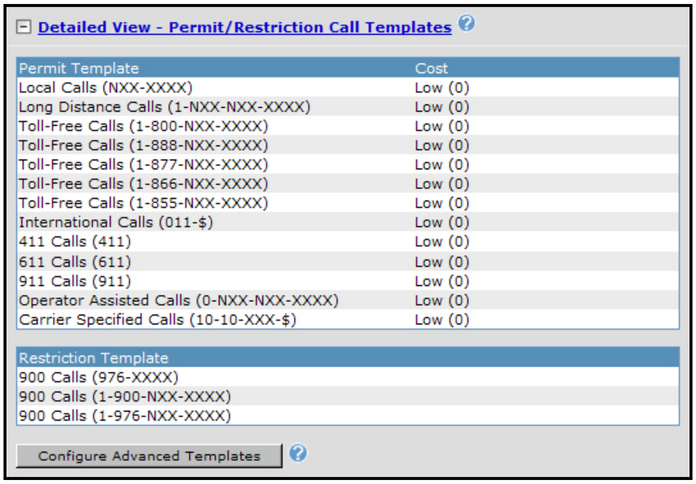
Modify/Delete Trunk Group

This is a description of this list

Trunk Group	Description	
ANALOG_FXO_TRUNKS		Delete
ANALOG TELCO		Delete
AT&T IP-FLEX REACH		Delete

3. In the **Edit Trunk Group** menu, select **Detailed View - Permit/Restriction Call Templates** to expand this section.

4. Select the **Configure Advanced Templates** button to access the **Advanced Permit/Restriction Templates** menu.

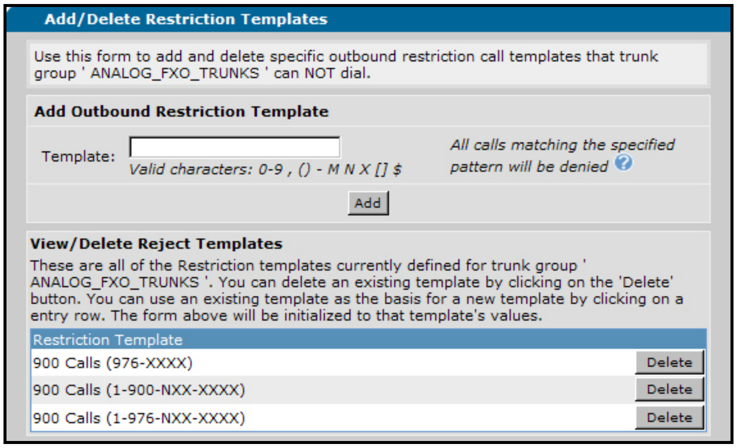


Detailed View - Permit/Restriction Call Templates

Permit Template	Cost
Local Calls (NXX-XXXX)	Low (0)
Long Distance Calls (1-NXX-NXX-XXXX)	Low (0)
Toll-Free Calls (1-800-NXX-XXXX)	Low (0)
Toll-Free Calls (1-888-NXX-XXXX)	Low (0)
Toll-Free Calls (1-877-NXX-XXXX)	Low (0)
Toll-Free Calls (1-866-NXX-XXXX)	Low (0)
Toll-Free Calls (1-855-NXX-XXXX)	Low (0)
International Calls (011-$)	Low (0)
411 Calls (411)	Low (0)
611 Calls (611)	Low (0)
911 Calls (911)	Low (0)
Operator Assisted Calls (0-NXX-NXX-XXXX)	Low (0)
Carrier Specified Calls (10-10-XXX-$)	Low (0)

Restriction Template
900 Calls (976-XXXX)
900 Calls (1-900-NXX-XXXX)
900 Calls (1-976-NXX-XXXX)

5. In the **Add/Delete Restriction Templates** section, enter an assigned SIP telephone number in the **Template** field, and select the **Add** button to add the outbound restriction call template.



Add/Delete Restriction Templates

Use this form to add and delete specific outbound restriction call templates that trunk group ' ANALOG_FXO_TRUNKS ' can NOT dial.

Add Outbound Restriction Template

Template: *Valid characters: 0-9 , () - M N X [] $* *All calls matching the specified pattern will be denied*

View/Delete Reject Templates

These are all of the Restriction templates currently defined for trunk group ' ANALOG_FXO_TRUNKS '. You can delete an existing template by clicking on the 'Delete' button. You can use an existing template as the basis for a new template by clicking on a entry row. The form above will be initialized to that template's values.

Restriction Template	
900 Calls (976-XXXX)	Delete
900 Calls (1-900-NXX-XXXX)	Delete
900 Calls (1-976-NXX-XXXX)	Delete

6. Repeat Step 5 for all telephone numbers supplied with the SIP trunk. Alternatively, wildcards can be used to include all assigned SIP telephone numbers. The template pattern may be a specific number but may also contain wildcards to match several AS-DIALED numbers. The available wildcards are:

   0-9 = Match exact digit only.
   M = Any digit 1 to 8.
   X = Any single digit (0 to 9).
   N = Any digit 2 to 9.
   [123] = Any digit contained in the bracketed list.

> NOTE *Do not use dashes, commas, spaces, etc., inside the brackets. Commas are implied between numbers in the brackets.*

The special characters **( )**, **-**, **+** are always ignored.

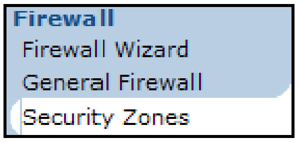
Examples: 1) 555-81XX matches 555-8100 to 555-8199.
2) 555-812[012] matches 555-8120 to 555-8122.
3) NXX-XXXX matches 7-digit local.
4) 1-NXX-NXX-XXXX matches long distance calls in North America.

Restricting SIP Traffic

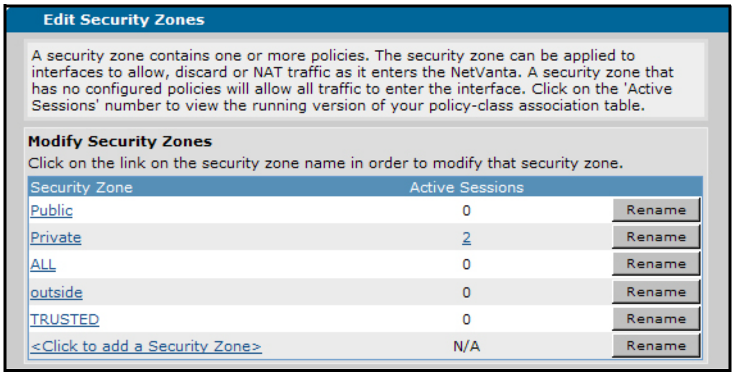
For security purposes, ADTRAN recommends restricting inbound SIP traffic to only allow AT&T's specified SIP server or IP border element. Once configured, you can change the firewall configuration using either the GUI or the CLI. These changes are made to allow SIP traffic only from the trusted SIP server or IP border element.

To restrict SIP traffic using the GUI, follow these steps:

1. Navigate to **Data > Firewall > Security Zones** to access the **Edit Security Zones** menu.



2. In the **Edit Security Zones** menu, select **Public**.



Edit Security Zones

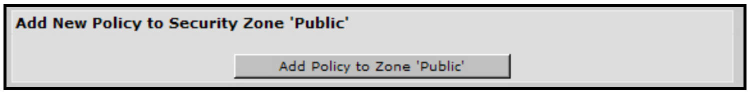
A security zone contains one or more policies. The security zone can be applied to interfaces to allow, discard or NAT traffic as it enters the NetVanta. A security zone that has no configured policies will allow all traffic to enter the interface. Click on the 'Active Sessions' number to view the running version of your policy-class association table.

Modify Security Zones

Click on the link on the security zone name in order to modify that security zone.

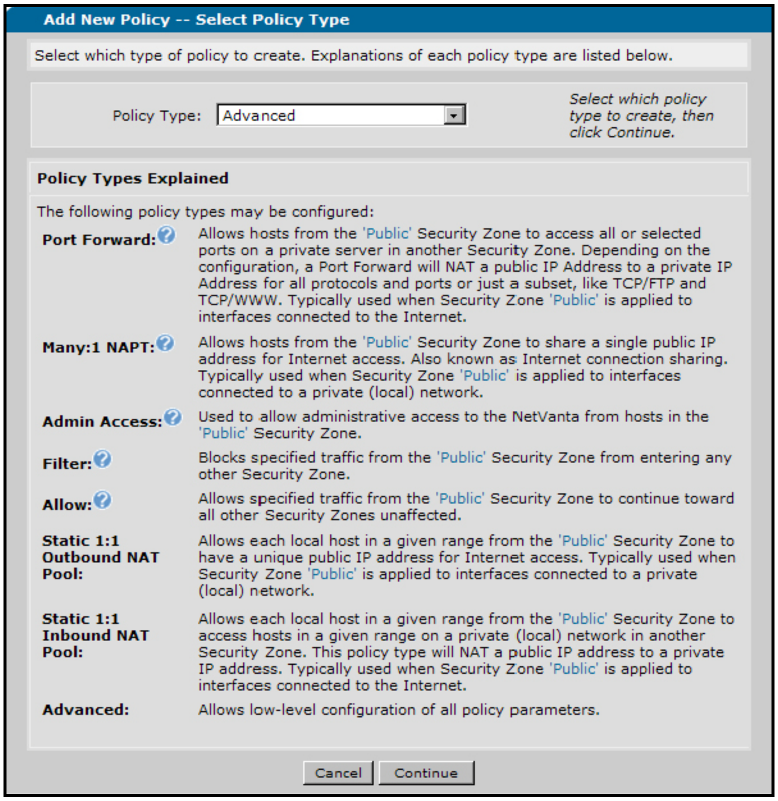
Security Zone	Active Sessions	
Public	0	Rename
Private	2	Rename
ALL	0	Rename
outside	0	Rename
TRUSTED	0	Rename
<Click to add a Security Zone>	N/A	Rename

3. In the **Add New Policy to Security Zone 'Public'** section, select the **Add Policy to Zone 'Public'** button. The **Add New Policy -- Select Policy Type** menu will appear.



Add New Policy to Security Zone 'Public'

4. Select **Advanced** from the **Policy Type** drop-down menu and select the **Continue** button.



Add New Policy -- Select Policy Type

Select which type of policy to create. Explanations of each policy type are listed below.

Policy Type: Advanced

Select which policy type to create, then click Continue.

Policy Types Explained

The following policy types may be configured:

Port Forward: Allows hosts from the 'Public' Security Zone to access all or selected ports on a private server in another Security Zone. Depending on the configuration, a Port Forward will NAT a public IP Address to a private IP Address for all protocols and ports or just a subset, like TCP/FTP and TCP/WWW. Typically used when Security Zone 'Public' is applied to interfaces connected to the Internet.

Many:1 NAPT: Allows hosts from the 'Public' Security Zone to share a single public IP address for Internet access. Also known as Internet connection sharing. Typically used when Security Zone 'Public' is applied to interfaces connected to a private (local) network.

Admin Access: Used to allow administrative access to the NetVanta from hosts in the 'Public' Security Zone.

Filter: Blocks specified traffic from the 'Public' Security Zone from entering any other Security Zone.

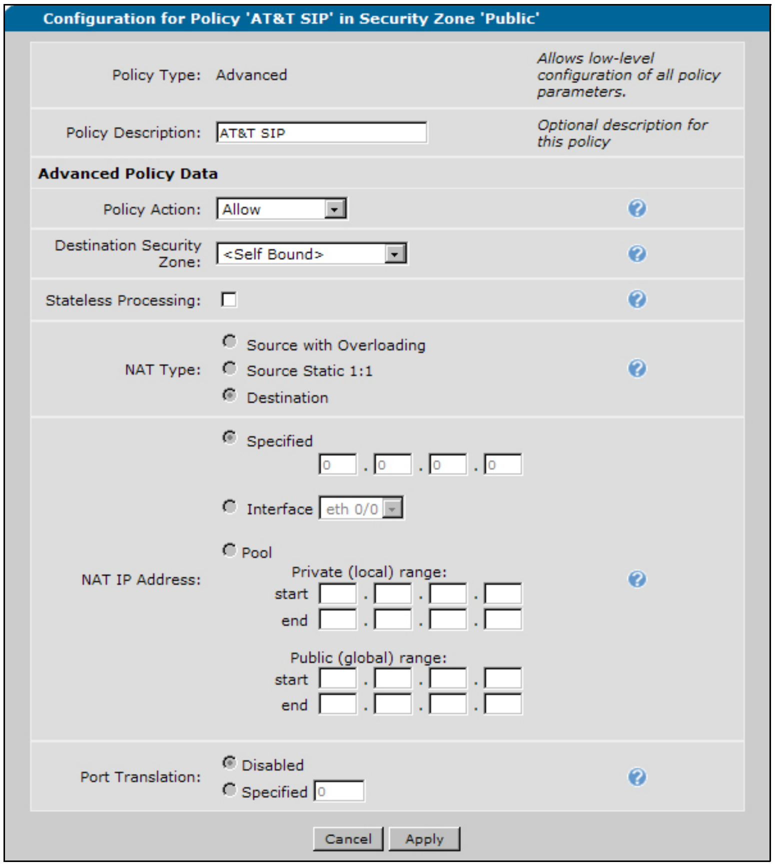
Allow: Allows specified traffic from the 'Public' Security Zone to continue toward all other Security Zones unaffected.

Static 1:1 Outbound NAT Pool: Allows each local host in a given range from the 'Public' Security Zone to have a unique public IP address for Internet access. Typically used when Security Zone 'Public' is applied to interfaces connected to a private (local) network.

Static 1:1 Inbound NAT Pool: Allows each local host in a given range from the 'Public' Security Zone to access hosts in a given range on a private (local) network in another Security Zone. This policy type will NAT a public IP address to a private IP address. Typically used when Security Zone 'Public' is applied to interfaces connected to the Internet.

Advanced: Allows low-level configuration of all policy parameters.

5. Enter a description of the policy in the **Policy Description** field, for example **AT&T SIP**.



Configuration for Policy 'AT&T SIP' in Security Zone 'Public'

Policy Type: Advanced — *Allows low-level configuration of all policy parameters.*

Policy Description: AT&T SIP — *Optional description for this policy*

Advanced Policy Data

Policy Action: Allow

Destination Security Zone: <Self Bound>

Stateless Processing: □

NAT Type:
○ Source with Overloading
○ Source Static 1:1
● Destination

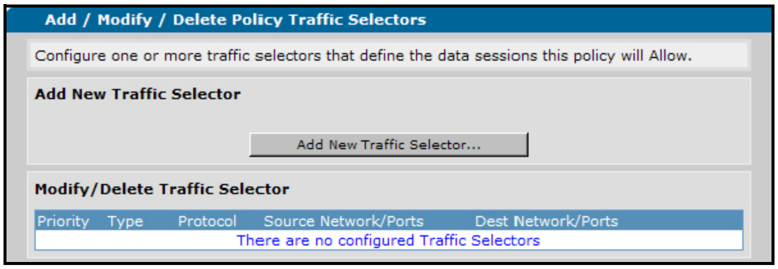
NAT IP Address:
● Specified 0 . 0 . 0 . 0
○ Interface eth 0/0
○ Pool
Private (local) range:
start . . .
end . . .
Public (global) range:
start . . .
end . . .

Port Translation:
● Disabled
○ Specified 0

6. Select **Allow** using the **Policy Action** drop-down menu.

7. Select **<Self Bound>** using the **Destination Security Zone** drop-down menu, and select the **Apply** button. The **Add/Modify/Delete Policy Traffic Selectors** menu will appear.

8. In the **Add/Modify/Delete Policy Traffic Selectors** menu, select the **Add New Traffic Selector** button to configure the IP addresses of the trusted SIP servers. The **Add New Custom Policy Entry** menu will appear.



Add / Modify / Delete Policy Traffic Selectors

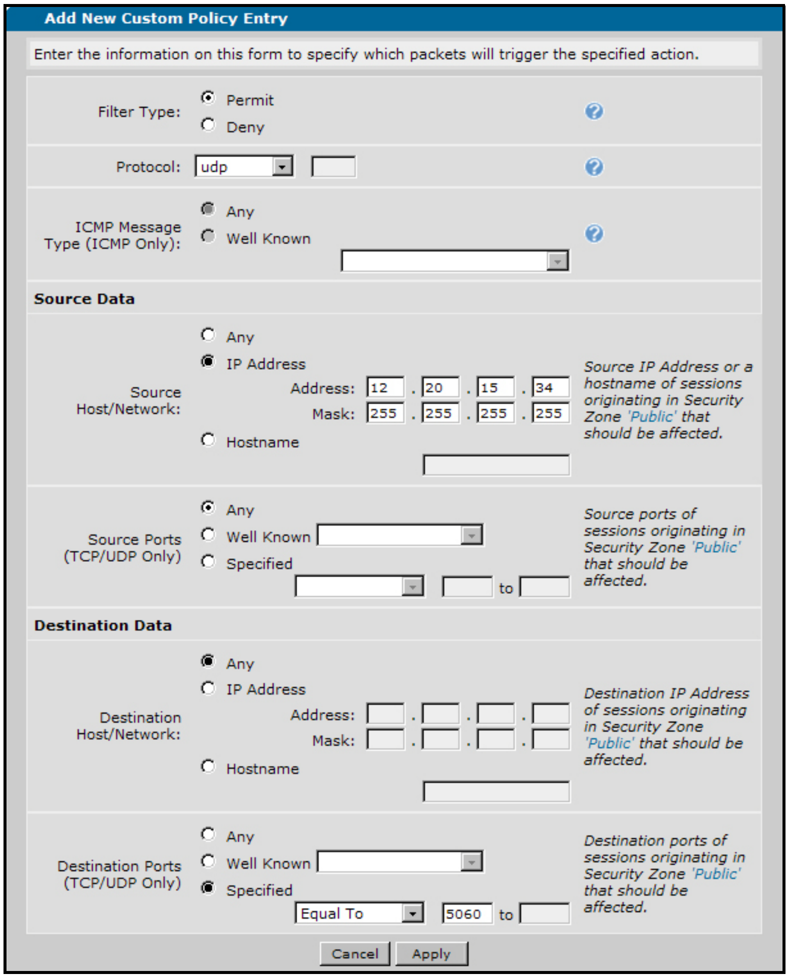
Configure one or more traffic selectors that define the data sessions this policy will Allow.

Add New Traffic Selector

Modify/Delete Traffic Selector

Priority	Type	Protocol	Source Network/Ports	Dest Network/Ports
There are no configured Traffic Selectors				

9. Next to **Filter Type**, select the **Permit** check box, and select **UDP** in the **Protocol** drop-down menu.



Add New Custom Policy Entry

Enter the information on this form to specify which packets will trigger the specified action.

Filter Type: ● Permit ○ Deny

Protocol: udp

ICMP Message Type (ICMP Only): ● Any ○ Well Known

Source Data

Source Host/Network: ○ Any ● IP Address ○ Hostname
Address: 12 . 20 . 15 . 34
Mask: 255 . 255 . 255 . 255

Source IP Address or a hostname of sessions originating in Security Zone 'Public' that should be affected.

Source Ports (TCP/UDP Only): ● Any ○ Well Known ○ Specified

Source ports of sessions originating in Security Zone 'Public' that should be affected.

Destination Data

Destination Host/Network: ● Any ○ IP Address ○ Hostname

Destination IP Address of sessions originating in Security Zone 'Public' that should be affected.

Destination Ports (TCP/UDP Only): ○ Any ○ Well Known ● Specified
Equal To 5060 to

Destination ports of sessions originating in Security Zone 'Public' that should be affected.

10. In the **Source Host/Network** section under **Source Data**, select the **IP Address** check box. In the **Address** field, enter the IP address of the SIP server or IP border element from which SIP traffic will be originating in the **Address** field, and enter a host netmask in the **Mask** field.

11. Under **Destination Data** in the **Destination Ports (TCP/UDP Only)** section, select the **Specified** check box. Select **Equal To** using the drop-down menu and enter **5060** in the adjacent field.

12. Select **Apply**. The **Configuration for Policy 'AT&T SIP' in Security Zone 'Public'** menu will appear.

13. To add a second SIP server IP address or IP border element for MIS/PNT, repeat Steps 8 to 11 with the appropriate IP address. All other settings will remain the same.

14. Select **Apply** in the **Configuration for Policy 'AT&T SIP' in Security Zone 'Public'** menu to accept the changes.

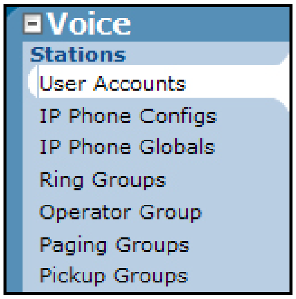
Adding a SIP Identity to a Voice User

Publicly routable PSTN numbers can be associated with specific SIP or analog users, ring groups consisting of multiple users, or auto attendants on the NetVanta 7100.

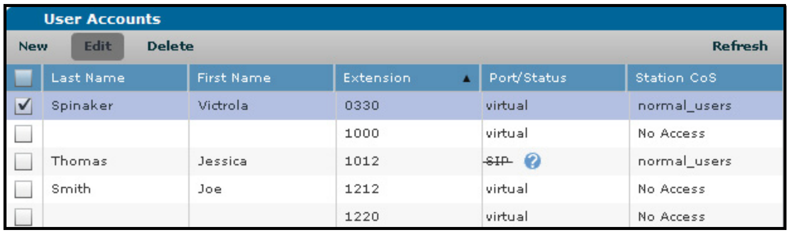
SIP identities play two roles: they provide public phone number association to private extensions for inbound calls, and they are used as the caller ID number when calling out the associated SIP trunk.

To add a SIP identity to a voice user using the GUI, follow these steps:

1. Navigate to **Voice** > **Stations** > **User Accounts** to access the **User Accounts** menu.



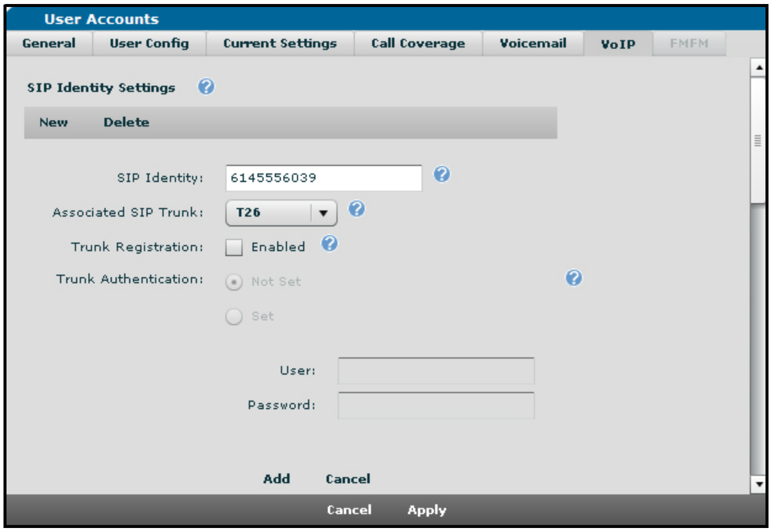
2. Select a voice user to which you would like to add a SIP identity (a check mark will appear in the check box next to the account name), and select **Edit**.



☐	Last Name	First Name	Extension ▲	Port/Status	Station CoS
☑	Spinaker	Victrola	0330	virtual	normal_users
☐			1000	virtual	No Access
☐	Thomas	Jessica	1012	~~SIP~~ ?	normal_users
☐	Smith	Joe	1212	virtual	No Access
☐			1220	virtual	No Access

3. In the menu that appears, select the **VoIP** tab.

4. Under **SIP Identity Settings**, select **New**. This will expand the window, allowing you to configure a new SIP identity. The number of digits used in the SIP identity can vary depending on how the network presents the dialed number in the SIP INVITE.



SIP Identity Settings

SIP Identity: 6145556039

Associated SIP Trunk: T26

Trunk Registration: ☐ Enabled

Trunk Authentication: ● Not Set ○ Set

User:

Password:

5. In the **SIP Identity** field, enter the public phone number you would like to associate with the user.
6. Using the **Associated SIP Trunk** drop-down menu, select the SIP trunk associated with AT&T's IP Flexible Reach Service, and select **Add**. To determine the SIP trunk associated with AT&T's IP Flexible Reach Service, navigate to **Voice > Trunks > Trunk Accounts**. The SIP trunk ID is located in the **Modify/Delete Trunk Account** section in the **ID** column, adjacent to the name of the SIP trunk created in *Creating a SIP Trunk Account on page 7*.
7. Select **Apply** at the bottom of the window to apply the settings. Now any call to this public phone number will ring this user's phone. Also, any call from the user out the AT&T SIP trunk will automatically use this public phone number as the caller ID.

Enabling G.711 Modem Passthrough and T.38 Fax on an Analog User

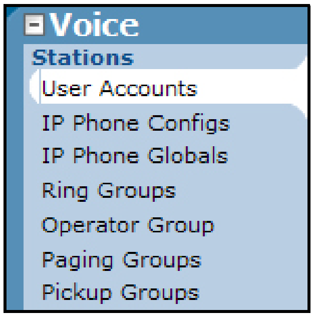
The NetVanta 7100 supports modems and fax through G.711 passthrough and T.38 options. Modem passthrough and T.38 can be enabled on the accounts associated with foreign exchange station (FXS) ports and virtual users.

Modem passthrough switches the fax tone detection to passthrough mode. The passthrough mode allows modem and fax calls to maintain a connection without altering the signals of the voice transmissions, maintaining voice transmission improvement settings like echo cancellation and voice activity detection (VAD).

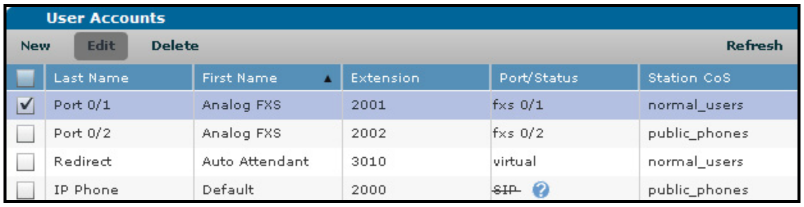
T.38 protocol provides techniques for correcting network delays and managing missing or delayed packets during the transition from time division multiplexing (TDM) transmission to Fax over Internet Protocol (FoIP) (or vice versa). The T.38 protocol achieves this purpose by modifying the protocol commands and responses on the TDM transmission side, keeping IP network delays from failing the transaction, and using fax-aware buffer-management techniques to correct missing or delayed packets.

To configure G.711 modem passthrough and T.38 fax on an analog user account using the GUI, follow these steps:

1. Navigate to **Voice** > **Stations** > **User Accounts**.



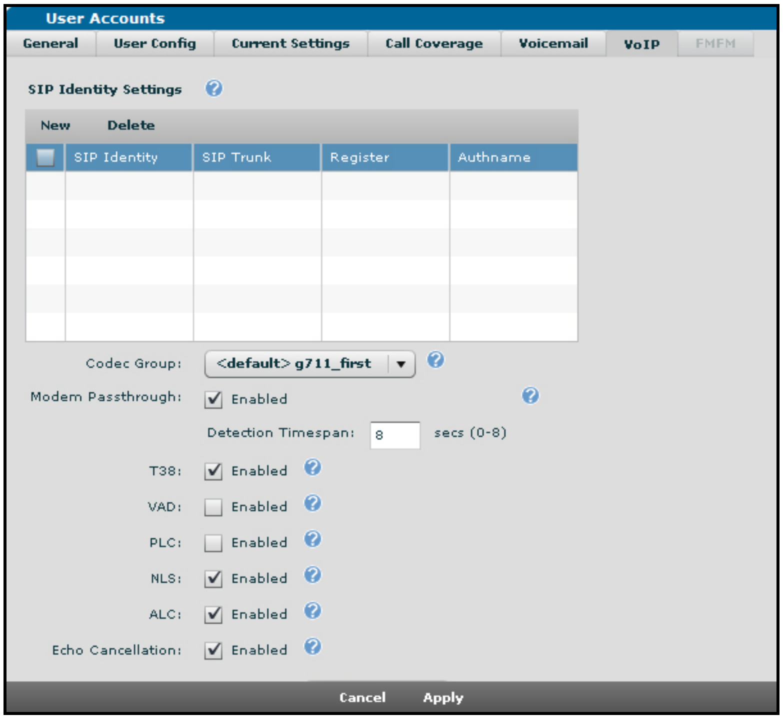
2. Select the account associated with the FXS port connected to the fax machine (a check mark will appear in the check box next to the account name), and select **Edit**.



□	Last Name	First Name ▲	Extension	Port/Status	Station CoS
☑	Port 0/1	Analog FXS	2001	fxs 0/1	normal_users
□	Port 0/2	Analog FXS	2002	fxs 0/2	public_phones
□	Redirect	Auto Attendant	3010	virtual	normal_users
□	IP Phone	Default	2000	~~SIP~~	public_phones

3. In the new menu that appears, select the **VoIP** tab.

4. To configure G.711 modem passthrough only, select the **Enabled** check box next to **Modem Passthrough** and select **Apply**.
To configure T.38 support, select the **Enabled** check boxes next to **Modem Passthrough** and **T38** and select **Apply**.



□	SIP Identity	SIP Trunk	Register	Authname

Codec Group: <default> g711_first

Modem Passthrough: ☑ Enabled

Detection Timespan: 8 secs (0-8)

T38: ☑ Enabled

VAD: □ Enabled

PLC: □ Enabled

NLS: ☑ Enabled

ALC: ☑ Enabled

Echo Cancellation: ☑ Enabled

Saving the Configuration

Changes made to the NetVanta 7100 will take effect immediately, but do not persist after the unit is rebooted unless they are saved. The configuration can be saved by selecting the **Save** link at the top right in the GUI.

Configuring the NetVanta 7100 for AT&T SIP Trunk and Fax in the CLI

To configure the NetVanta 7100 for AT&T SIP trunk and fax settings using the CLI, follow these steps:

- Access the CLI
- Enable SIP privacy
- Configure a new coder-decoder (CODEC) list
- Enable detection of inbound fax calls
- Create a SIP trunk account
- Configure a trunk group
- Add reject template PSTN trunk groups
- Restrict SIP Traffic
- Add a SIP identity to a voice user
- Enable modem passthrough and T.38 on an analog user
- Save the configuration

Accessing the CLI

To access the CLI on your AOS unit, follow these steps:

1. Boot up the unit.
2. Telnet to the unit (**telnet** <*ip address*>). For example:

   ```
   telnet 208.61.209.1.
   ```

> NOTE *If during the unit's setup process you have changed the default IP address (**10.10.10.1**), use the configured IP address.*

3. Enter your user name and password at the prompt.

> NOTE *The AOS default user name is **admin** and the default password is **password**. If your product no longer has the default user name and password, contact your system administrator for the appropriate user name and password.*

4. Enter the Enable mode by entering **enable** at the prompt as follows:

   ```
   >enable
   ```

5. Enter your Enable mode password at the prompt.
6. Enter the unit's Global Configuration mode as follows:

   ```
   #configure terminal
   (config)#
   ```

Enable SIP Privacy

SIP privacy specifies that outbound calls include SIP privacy headers and inbound calls are filtered based on privacy settings.

Use the **ip sip privacy** command from the Global Configuration mode to enable SIP privacy.

```
(config)#ip sip privacy
```

Configuring a CODEC List

Voice CODEC lists are lists of CODECs arranged in preferred order with the first listed CODEC being the most preferred for call negotiation. Order is important when creating a CODEC list. The interface attempts to use the first CODEC in the list to negotiate a call. If the first CODEC negotiation is unsuccessful, the interface uses the second CODEC in the list and so on. If this process is unsuccessful, the call will fail.

The primary reason to create and assign voice CODEC lists is to save time. CODEC lists are created, listing CODECs in the order of preference, and then lists are applied to interfaces. Configuring a CODEC list allows the list to be applied to multiple interfaces, such as MGCP interfaces, voice trunks, voice accounts, and voice users without having to define the order of CODECs individually. The order of preference is used primarily to conserve bandwidth on WAN-based interfaces.

To configure a CODEC list using the CLI, follow these steps:

1. From the Global Configuration mode, use the **voice codec-list** command to create a new CODEC list and enter the Voice CODEC List Configuration mode:

   ```
   (config)#voice codec-list <name>
   ```

   The <*name*> variable specifies the CODEC list name.
2. In the Voice CODEC List Configuration mode, use the **codec g729** command to assign the G.729 CODEC (8000 bps) as the primary CODEC for negotiation:

   ```
   (config-codec)#codec g729
   ```
3. In the Voice CODEC List Configuration mode, use the **codec g711ulaw** command to assign the G.711 Mu-Law CODEC (64000 bps) as the secondary CODEC for negotiation:

   ```
   (config-codec)#codec g711ulaw
   ```

Enabling Inbound Fax Call Detection

Inbound fax call detection provides modem passthrough on gateway calls inbound from a VoIP network. Modem passthrough allows modem and fax calls to maintain a connection without altering the signal with voice improvement settings, such as echo cancellation and VAD.

Use the **voice modem-passthrough-mode inbound** command from the Global Configuration mode to enable modem passthrough on gateway calls inbound from a VoIP network.

```
(config)#voice modem-passthrough-mode inbound
```

Creating a SIP Trunk Account

The SIP trunk is where all IP information and SIP messaging configurations to the SIP network are configured.

To configure a SIP trunk account using the CLI, follow these steps:

1. From the Global Configuration mode, use the **voice trunk type sip** command to create a new SIP trunk account and enter the Voice SIP Trunk Configuration mode:

   (config)#**voice trunk** <*Txx*> **type sip**

   The <*Txx*> variable specifies the trunk's two-digit identifier in the format Txx (for example, **T26**).

   The **sip** parameter configures this trunk for use with SIP.

2. From the Voice SIP Trunk Configuration mode, use the **description** command to identify the trunk with a description:

   (config-Txx)#**description** <*text*>

   The <*text*> variable identifies the trunk using up to 80 alphanumeric characters.

3. From the Voice SIP Trunk Configuration mode, use the **sip-server primary** command to define the primary name or IP address of the SIP server to which the trunk will send call-related SIP messages:

   (config-Txx)#**sip-server primary** <*value*>

   The <*value*> variable specifies the FQDN or IP address of the SIP proxy server. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

4. From the Voice SIP Trunk Configuration mode, use the **sip-server secondary** command to define the secondary name or IP address of the SIP server to which the trunk will send call-related SIP messages:

   (config-Txx)#**sip-server secondary** <*value*>

   The <*value*> variable specifies the FQDN or IP address of the SIP proxy server. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

5. From the Voice SIP Trunk Configuration mode, use the **codec-group** command to assign a CODEC list to the SIP trunk:

   (config-Txx)#**codec-group** <*name*>

   The <*name*> specifies the CODEC list to be used for the trunk. The CODEC list used should be the CODEC list created in *Configuring a CODEC List on page 21*.

6. From the Voice SIP Trunk Configuration mode, use the **trust-domain** command to add security measures for users' identity and privacy by connecting the trunk to a trusted domain. Using a trusted domain adds another level of privacy from participating service providers:

   (config-Txx)#**trust-domain**

7. From the Voice SIP Trunk Configuration mode, use the **diversion-supported** command to apply a SIP Diversion header to redirected calls on the trunk:

   (config-Txx)#**diversion-supported**

8. From the Voice SIP Trunk Configuration mode, use the **grammar from host local** command to set the FROM header format to use a local IP:

   ```
   (config-Txx)#grammar from host local
   ```

9. From the Voice SIP Trunk Configuration mode, use the **grammar p-asserted-identity host local** command to set the p-asserted-identity header host format to use a local IP for constructing the header:

   ```
   (config-Txx)#grammar p-asserted-identity host local
   ```

Configuring Trunk Groups

Trunk groups comprise one or more trunk accounts. They are used to assign outbound call capabilities (local calls, long distance calls, etc.). A cost is assigned to each attribute in the outbound call template and is used to select lowest cost route when multiple trunk groups are present on the NetVanta 7100. Use this section to create a trunk group, add the trunk account members to the group, and define the outbound call templates and costs.

To configure a trunk group using the CLI, follow these steps:

1. From the Global Configuration mode, use the **voice grouped-trunk** command to create a new trunk group and enter the Voice Trunk Group Configuration mode:

   ```
   (config)#voice grouped-trunk <trunk group>
   ```

   The <*trunk group*> variable specifies the name of the newtrunk group.

2. From the Voice Trunk Group Configuration mode, use the **trunk** command to add the SIP trunk account to the trunk group:

   ```
   (config-TRUNKGROUP)#trunk <Txx>
   ```

   The <*Txx*> variable specifies the trunk's two-digit identifier in the format Txx. The trunk used should be the SIP trunk account created in *Creating a SIP Trunk Account on page 22*.

3. From the Voice Trunk Group Configuration mode, enter the outbound call templates and their costs. Valid cost range is **0** to **499**.

   You can enter an exact phone number, or you can use wildcards to help define rejected numbers. The available wildcards for this command are:

   0-9 = Match exact digit only.
   M = Any digit 1 to 8.
   X = Any single digit (0 to 9).
   N = Any digit 2 to 9.
   [123] = Any digit contained in the bracketed list.

> NOTE *Do not use dashes, commas, spaces, etc., inside the brackets. Commas are implied between numbers in the brackets.*

The special characters **( )**, **-**, **+** are always ignored.

Examples: 1) 555-81XX matches 555-8100 to 555-8199.
2) 555-812[012] matches 555-8120 to 555-8122.
3) NXX-XXXX matches 7-digit local.
4) 1-NXX-NXX-XXXX matches long distance calls in North America.

Enter the desired outbound call templates as follows:

```
(config-TRUNKGROUP)#accept NXX-NXX-XXXX cost 0
(config-TRUNKGROUP)#accept 1-NXX-NXX-XXXX cost 0
(config-TRUNKGROUP)#accept NXX-NXX-XXXX cost 0
(config-TRUNKGROUP)#accept 1-NXX-NXX-XXXX cost 0
(config-TRUNKGROUP)#accept 1-800-NXX-XXXX cost 0
(config-TRUNKGROUP)#accept 1-888-NXX-XXXX cost 0
(config-TRUNKGROUP)#accept 1-877-NXX-XXXX cost 0
(config-TRUNKGROUP)#accept 1-866-NXX-XXXX cost 0
(config-TRUNKGROUP)#accept 1-855-NXX-XXXX cost 0
(config-TRUNKGROUP)#accept 011-$ cost 0
(config-TRUNKGROUP)#accept 411 cost 0
(config-TRUNKGROUP)#accept 611 cost 0
(config-TRUNKGROUP)#accept 911 cost 0
(config-TRUNKGROUP)#accept 0-NXX-NXX-XXXX cost 0
(config-TRUNKGROUP)#accept 10-10-XXX-$ cost 0
(config-TRUNKGROUP)#accept 511 cost 0
```

Adding Reject Templates to PSTN Trunk Groups

Reject templates are used on trunk groups to prevent calls to specific numbers from being routed out the specified trunks. If trunk groups for failover or PSTN connectivity are present in the NetVanta 7100 configuration, reject templates must be added for all telephone numbers supplied with the SIP trunk.

To configure reject templates for a PSTN trunk group using the CLI, follow these steps:

1. From the Global Configuration mode, use the **voice grouped-trunk** command to enter the Voice Trunk Configuration mode for the trunk group associated with the PSTN connections:

   ```
   (config)#voice grouped-trunk <trunk group>
   ```

   The *<trunk group>* variable specifies the name of the trunk group. The trunk group should be the one associated with PSTN connections.

2. From the Voice Trunk Configuration mode, use the reject command to prevent calls to all SIP phone numbers supplied with the SIP trunk:

   ```
   (config-TRUNKGROUP)#reject <pattern>
   ```

   The *<pattern>* variable specifies the reject numbers for the trunks. You can enter an exact phone number, or you can use wildcards to help define rejected numbers. The available wildcards for this command are:

   0-9 = Match exact digit only.
   M = Any digit 1 to 8.
   X = Any single digit (0 to 9).

N = Any digit 2 to 9.
[123] = Any digit contained in the bracketed list.

> NOTE *Do not use dashes, commas, spaces, etc., inside the brackets. Commas are implied between numbers in the brackets.*

The special characters **( )**, **-**, **+** are always ignored.

Examples: 1) 555-81XX matches 555-8100 to 555-8199.
2) 555-812[012] matches 555-8120 to 555-8122.
3) NXX-XXXX matches 7-digit local.
4) 1-NXX-NXX-XXXX matches long distance calls in North America.

Restricting SIP Traffic

For security purposes, ADTRAN recommends restricting inbound SIP traffic to only allow AT&T's specified SIP server or IP border element. Once configured, you can change the firewall configuration using either the GUI or the CLI. These changes are made to allow SIP traffic only from the trusted SIP server or IP border element.

To restrict SIP traffic using the CLI, follow these steps:

1. From the Global Configuration mode, use the **ip access-list extended** command to create an extended access control list (ACL) that will be used to allow only SIP traffic from AT&T and enter the Extended ACL Configuration mode:

   ```
   (config)#ip access-list extended <name>
   ```

   The *<name>* variable specifies the name for the ACL.

2. From the Extended ACL Configuration mode, use the **permit** command to configure the ACL to permit only User Datagram Protocol (UDP) traffic from AT&T SIP servers on port 5060. If you are using IP Flexible Reach over MIS/PNT, both the primary and secondary SIP server or IP border element IP addresses must be entered.

   ```
   (config-ext-nacl)#permit udp host <ip address> any eq 5060
   ```

   The **host** *<ip address>* parameter specifies a single host IP address. The IP address should be expressed in dotted decimal notation (for example, **10.10.10.1**). The IP address used should be the IP address of an AT&T SIP server or IP border element.

3. From the Extended ACL Configuration mode, use the following command to enter the Access Control Policy (ACP) Configuration mode for the **Public** ACP:

   ```
   (config-ext-nacl)#ip policy-class Public
   ```

4. From the **Public** ACP Configuration mode, use the allow list command to allow traffic from the ACL configured in Step 1 to enter the NetVanta 7100.

   ```
   (config-policy-class)#allow list <acl name> self
   ```

   The *<acl name>* variable specifies the ACL against which to check traffic before allowing packets to enter the interface. The ACL should be the ACL configured in Step 1.

Adding a SIP Identity to a Voice User

Publicly routable PSTN numbers can be associated with specific SIP or analog users, ring groups consisting of multiple users, or auto attendants on the NetVanta 7100.

SIP identities play two roles: they provide public phone number association to private extensions for inbound calls, and they are used as the caller ID number when calling out the associated SIP trunk.

To add a SIP identity to a voice user using the CLI, follow these steps:

1. From the Global Configuration mode, enter the **voice user** command followed by the desired user's extension:

   (config)#**voice user** *<extension>*

   The <*extension*> variable specifies the user's extension.

2. From the Voice User Account Configuration mode, use the **sip-identity** command to configure the SIP identity for the user and specify the associated SIP trunk through which to register the user:

   (config-extension)#**sip-identity** *<station> <Txx>*

   The <*station*> variable specifies the station to be used for the SIP identity. This variable should correspond to the desired PSTN number.

   The <*Txx*> variable specifies the SIP trunk through which to register the station. The trunk is specified in the format Txx (e.g., **T26**). This trunk used should be the SIP trunk created in *Creating a SIP Trunk Account on page 22*.

Configuring G.711 Modem Passthrough and T.38 Fax on an Analog User

The NetVanta 7100 supports modems and fax through G.711 passthrough and T.38 options. Modem passthrough and T.38 can be enabled on the accounts associated with FXS ports and virtual users.

Modem passthrough switches the fax tone detection to passthrough mode. The passthrough mode allows modem and fax calls to maintain a connection without altering the signals of the voice transmissions, maintaining voice transmission improvement settings like echo cancellation and voice activity detection.

T.38 protocol provides techniques for correcting network delays and managing missing or delayed packets during the transition from TDM transmission to FoIP (or vice versa). The T.38 protocol achieves this purpose by modifying the protocol commands and responses on the TDM transmission side, keeping IP network delays from failing the transaction, and using fax-aware buffer-management techniques to correct missing or delayed packets.

To configure G.711 modem passthrough and T.38 fax on an analog user account using the CLI, follow these steps:

1. From the Global Configuration mode, enter the **voice user** command followed by the desired user's extension:

   (config)#**voice user** *<extension>*

   The <*extension*> variable specifies the user's extension.

2. To enable only G.711 modem passthrough without T.38, enter the following at the Voice User Account Configuration mode prompt.

   ```
   (config-extension)#modem-passthrough
   ```

3. To enable both modem passthrough and T.38, enter the following at the Voice User Account Configuration mode prompt.

   ```
   (config-extension)#modem-passthrough
   (config-extension)#t38
   ```

Saving the Configuration

Changes made to the NetVanta 7100 will take effect immediately, but do not persist after the unit is rebooted unless they are saved. The configuration can be saved in the CLI using the **write memory** command issued at the Enable mode prompt.

Troubleshooting

AT&T field technicians and engineers can contact ADTRAN Technical Support for assistance.

AT&T customers requesting support on the NetVanta 7100 from ADTRAN must have a valid maintenance contract through ADTRAN Custom Extended Services (ACES). Please have your ADTRAN ACES contract number or product serial number available when contacting ADTRAN Technical Support for assistance.

Phone Support: 888-423-8726

Email Support: support@adtran.com

Web Support: www.adtran.com/support

Technical support during normal hours (7:00 a.m. to 7:00 p.m. Central Standard Time) will receive a same-day phone response.

After-hours technical support (7:00 p.m. to 7:00 a.m. Central Standard Time) will receive a best-effort phone response for service-affecting emergencies only. The equipment must have been performing in the network prior to the failure that prompted the call for support. Installation of new hardware and configuration changes to existing hardware are not supported after hours.

What to Provide Technical Support

When contacting ADTRAN Technical Support, it is important to have the following information available for the Technical Support Engineer (TSE):

1. Description of the setup
2. Copy of the NetVanta 7100 configuration
3. Results of the following **show** commands:
   a. show voice user sip
   b. **show sip user-registration**

4. Screen capture of the following **debug** commands taken when the issue is experienced:
   a. **debug voice verbose**
   b. **debug sip stack messages**
   c. **debug isdn l2-formatted** (when the issue involves a primary rate interface (PRI))
   d. **debug interface fxo** (when the issue involves analog trunks)

The ADTRAN TSE may request additional debug or other information based on what is indicated from these results.

Troubleshooting Commands

All AOS commands can be found in the *AOS Command Reference Guide* (ADTRAN's Knowledge Base article 2219).

See Table 1 below for a list of some common commands used by the TSE when troubleshooting the NetVanta 7100.

Table 1. Common Troubleshooting Commands

Command	Description
show voice user sip	Shows SIP user's first and last name, extension, media access control (MAC) address, IP address and physical port if MAC and Address Resolution Protocol (ARP) tables are populated.
show sip user-registration	Lists all registered SIP users.
show media-gateway summary active	Displays resources assigned to active RTP sessions.
show running-config voice [**grouped-trunk** *<name>* | **ring-group** *<name>* | **trunk** *<Txx>* | **user** *<number* | *name* | *last name>*]	Displays running voice configurations. The **grouped-trunk** *<name>* parameter displays voice trunk group configurations for the specified trunk. The **ring-group** *<name>* parameter displays ring group configurations for the specified ring group. The **trunk** *<Txx>* parameter displays voice trunk configurations for the specified trunk. The trunk is specified in the format Txx (e.g., **T01**). The **user** *<number* | *name* | *last name>* parameter displays voice user configurations for the specified number, first name, or last name.
debug voice switchboard call	Activates debug messages for calls switched through the NetVanta 7100. The **call** parameter isolates debug output to call details.
debug sip stack messages	Displays all SIP messages sent to and from the NetVanta 7100.
debug isdn l2-formatted	Displays Layer 2 formatted PRI signaling information.
debug interface [**fxo** | **fxs**]	Display's foreign exchange office (FXO) or foreign exchange station (FXS) state and signaling information.

See Table 2 below for some of the common debug commands for IP phones:

Table 2. IP Phone Debug Commands

Command	Description
debug ip dhcp-server	Shows Dynamic Host Configuration Protocol (DHCP) server information when a phone is attempting to retrieve an IP address.
debug ip ftp-server	Displays NetVanta 7100 File Transfer Protocol (FTP) server information when an IP phone is downloading its configuration.
debug ip tftp server events	Displays NetVanta 7100 Trivial File Transfer Protocol (TFTP) server information when an IP phone is downloading its configuration.
debug sip user-registration	Provides SIP trunk-registration event information when an IP phone registers with the NetVanta 7100.