ADTRAN

6AOSCG0037-29C
March 2013

Configuration Guide

Simple Remote Phones for the NetVanta 7000 Series

This configuration guide outlines the steps necessary to operate simple remote phones with a NetVanta 7000 Series product. The guide includes an overview of the simple remote phone function and outlines the steps necessary to configure the IP phones and the ADTRAN Operating System (AOS) device to receive and route calls. Troubleshooting information and additional documentation resources are provided at the end of this guide.

This guide consists of the following sections:

Simple Remote Phone Overview

Prior to the release of AOS R10.3.1 for the NetVanta 7000 Series product, supporting a remote phone at the customer location required the remote phone to be installed behind a SIP aware firewall or virtual private network (VPN) capable device. While this solution is recommended for certain applications, (especially applications requiring added security and PC connectivity behind remote phones), another option is now available. Since the release of AOS R10.3.1, the Simple Remote Phones feature of the NetVanta 7000 Series allows remote phones to be located behind a non-SIP aware firewall and does not require VPN. This feature enables customers with less complex needs to have a solution for their remote employees. The remote phone is configured to contact the NetVanta 7000 Series product (deployed as an IP PBX) through its wide area network (WAN) interface connected to the Internet. Once installed behind a remote user network, the IP phone acquires a local IP address and attempts to register with the NetVanta 7000 Series unit using SIP signaling. Once registered, the phone can make and receive calls remotely.

Typically, the system would use the IP address and port number specified in the Contact header of SIP packets to determine how to route the SIP traffic. However, if the remote phone is located behind a non-SIP aware firewall, the Contact header information cannot be used because it reflects the private IP address and port of the phone. Instead of using the Contact header IP address and port number, the back-to-back user agent (B2BUA) must send SIP messages to the Layer 3 source IP address and port number. For Realtime Transport Protocol (RTP) packets, the B2BUA must anchor the media and relay packets to the Layer 3 source IP address and port number rather than using the IP address and port specified in the Session Description Protocol (SDP). When the system receives any SIP message for a voice user configured for source IP address and port routing, the system sends all subsequent SIP messages to the Layer 3 IP address and port number from which the request was received.

Additional information available online at ADTRAN's Support Community, https://supportforums.adtran.com. Specific resources are listed in *Additional Resources on page 29*.

Hardware and Software Requirements and Limitations

The simple remote phone feature is available on AOS products as outlined in the *AOS Feature Matrix*, available online at ADTRAN's Support Community, https://supportforums.adtran.com.

The NetVanta 7060 will not support the simple remote phone feature as discussed in this configuration guide as a standalone solution. It must be used in conjunction with another ADTRAN router running the session border controller (SBC) feature pack firmware. Contact your ADTRAN reseller for more information.

Simple remote phones must use User Datagram Protocol (UDP) for SIP messaging.

Some advanced features of the NetVanta 7000 Series product will not function in conjunction with simple remote phones. These limitations include:

- Paging groups (handsfree auto answer and overhead paging are both supported)
- Shared line accounts and shared call appearances (SLA/SCA)
- SIP over Transmission Control Protocol (TCP)
- Status groups (busy lamp fields)

NOTE *Do NOT enable media anchoring globally on the NetVanta 7000 Series or it will adversely affect system resources. Media anchoring should only be enabled on a per SIP user basis.*

Toll Fraud Liability

Be advised that certain security risks are inherent in the use of any telecommunications or networking equipment, including but not limited to, toll fraud, Denial of Service (DoS) attacks, loss or theft of data, and the unauthorized or illegal use of said equipment. Ultimately, the responsibility for securing your telecommunication and networking equipment rests with you, and you are encouraged to review documentation regarding available security measures, their configuration and implementation, and to test such features as is necessary for your network. Refer to *Security Best Practices for AOS Products* and *NetVanta 7000 Series Security Guide* for suggested practices. Many other documents are available online at ADTRAN's Support Community, https://supportforums.adtran.com

Configuration Introduction

Successful configuration of simple remote phones requires four main tasks. The first task is to configure the NetVanta 7000 Series unit with the appropriate SIP server settings, and then configure the firewall. This is accomplished through the AOS graphical user interface (GUI). The second task, setting the expire times by configuring header manipulation rules (HMR), can only be accomplished through the AOS command line interface (CLI). The third task requires altering the IP phone configuration files, using a text editor, to specify the SIP port and then replacing it on the IP phones. The fourth and final task is to configure the boot server address either through DHCP options or manually on the IP phone.

It is necessary to perform all the steps in each section for each task and do so in the order presented in this document. The configuration steps for these tasks are explained in *Table 1*.

Table 1. Simple Remote Phones Configuration Tasks

Task	Method	Description
Task 1: Configuring Simple Remote Phones through the GUI on page 4	GUI Configuration	Update the system configuration.
Task 2: Specifying Registration Expire Times through the AOS CLI on page 13	CLI Configuration	Update the registration expire times.
Task 3: Altering the IP Phone Configuration Files on page 17	IP Phone Configuration	Update the phone configuration with correct port number.
Task 4: Configure the Boot Server Address for the IP Phone on page 18	Remote DHCP Server or manually through IP Phone Configuration	Configure Option 66 or 157 on the remote DHCP server or manually enter the boot server IPv4 Address on the IP phones.

Task 1: Configuring Simple Remote Phones through the GUI

There are several SIP settings that must be configured on the NetVanta 7000 Series unit to allow simple remote phones to successfully operate in a network. The simplest method for making these changes in the configuration is through the AOS GUI. In this section, you will access the GUI of the NetVanta 7000 Series unit and make changes to the configuration through several menus. Each section provides the menu navigation and appropriate settings. Due to the complexity of this feature, not all options are explained for all menus, only those pertaining to this specific feature. Additionally, an example configuration is provided using CLI commands in the *Configuration Example on page 19*.

To configure simple remote phones using the GUI on an AOS product, follow these steps:

1. Modify the IP phone global settings.
2. Specify the SIP server for IP phones.
3. Configure SIP server settings.
4. Enable remote phone mode for each SIP user.
5. Configure firewall settings.

Accessing the GUI

AOS products ship with a user-friendly GUI that can be used to perform many basic management and configuration functions on the AOS product. To access the GUI and begin configuring this feature, follow these steps:

1. Open a new web page in your Internet browser.
2. Enter your AOS product's IP address in the browser's address field in the format **http://**<*ip address*>**/admin**, for example:

   http://10.10.10.1/admin
3. At the prompt, enter your user name and password and select **OK**.

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

Step 1: Modify the IP Phone Global Settings

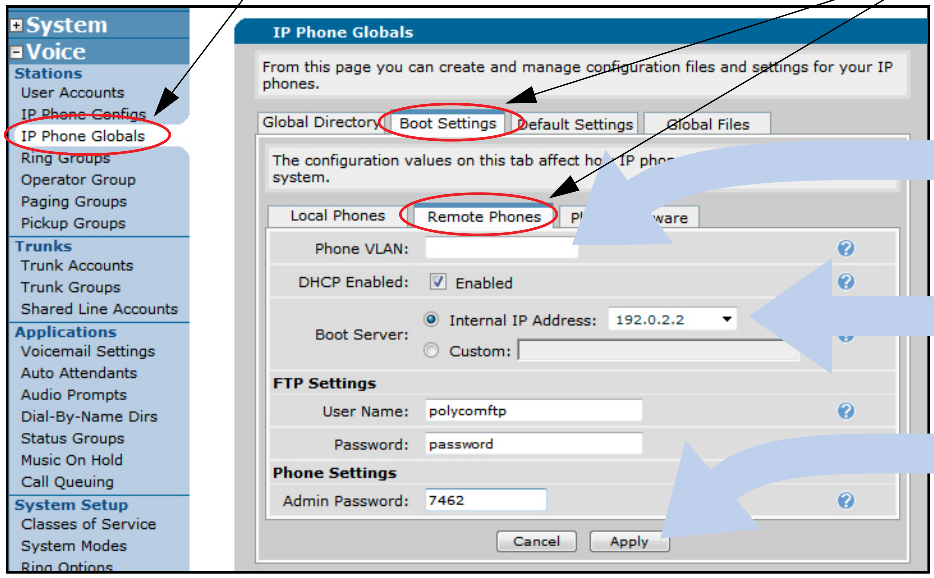
The external or WAN IPv4 address of the NetVanta 7000 Series unit must be specified in the global settings for remote phones in order for the IP phones to successfully locate the boot server and download the correct updated configuration files. This is configured from the **IP Phone Globals** menu.

1. Navigate to **Voice** > **Stations** > **IP Phone Globals**.
2. Select the **Boot Settings** tab and the **Remote Phones** tab.
3. Be sure to clear the information (if there are any default settings) in the **Phone VLAN** field.
4. Select the IPv4 address of the NetVanta 7000 Series unit that corresponds to the WAN interface from the **Boot Server** drop-down menu.

5. Select **Apply** at the bottom of the menu to accept the changes.

Select **IP Phone Globals** from the **Voice** > **Stations** menu.

Select **Boot Settings** and then **Remote Phones** to make changes to the boot settings for remote phones.



From this page you can create and manage configuration files and settings for your IP phones.

The configuration values on this tab affect ho IP phon system.

Phone VLAN:

DHCP Enabled: ☑ Enabled

Boot Server: ● Internal IP Address: 192.0.2.2 ○ Custom:

FTP Settings

User Name: polycomftp

Password: password

Phone Settings

Admin Password: 7462

Leave the **Phone VLAN** field blank. If there is a default setting in this field, remove it.

From the drop-down menu, select the IPv4 address for the WAN interface as the boot server.

Select **Apply** to accept the changes.

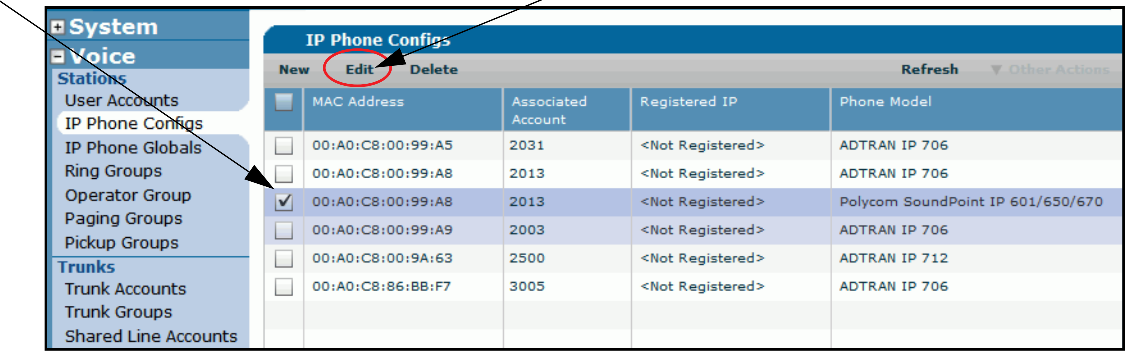
Step 2: Specify the SIP Server IPv4 Address for IP Phones

The external or WAN IPv4 address of the NetVanta 7000 Series unit must be specified in the IP phone's configuration in order for the IP phones to successfully locate the SIP server. This is configured from the **IP Phone Configs** menu.

1. Navigate to **Voice** > **Stations** > **IP Phone Configs**.
2. Select the check box next to the MAC Address of the IP phone you are configuring as a simple remote phone. Select **Edit** from the menu options.

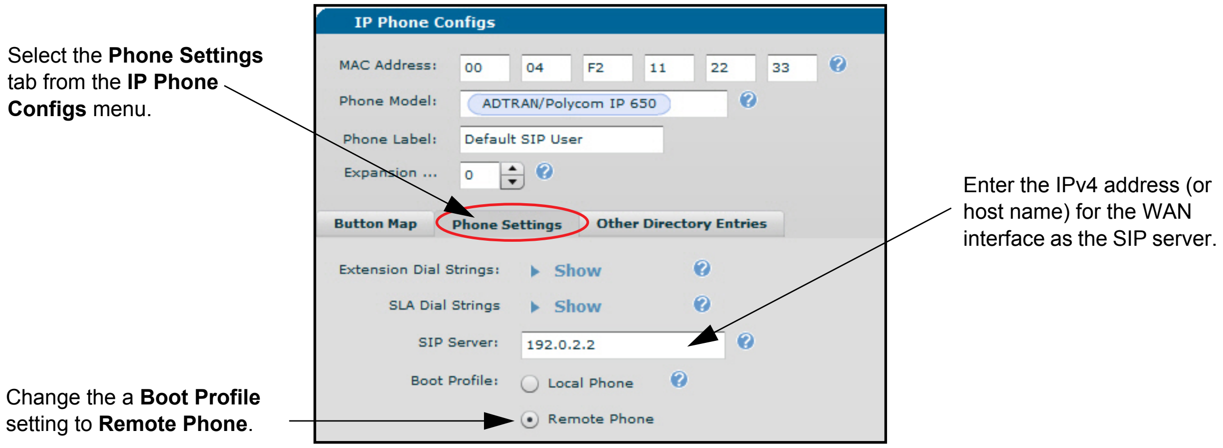
Select the check box next to the IP phone to be configured as a remote phone.

Select **Edit** to make changes to the IP phone configuration.



	MAC Address	Associated Account	Registered IP	Phone Model
□	00:A0:C8:00:99:A5	2031	<Not Registered>	ADTRAN IP 706
□	00:A0:C8:00:99:A8	2013	<Not Registered>	ADTRAN IP 706
☑	00:A0:C8:00:99:A8	2013	<Not Registered>	Polycom SoundPoint IP 601/650/670
□	00:A0:C8:00:99:A9	2003	<Not Registered>	ADTRAN IP 706
□	00:A0:C8:00:9A:63	2500	<Not Registered>	ADTRAN IP 712
□	00:A0:C8:86:BB:F7	3005	<Not Registered>	ADTRAN IP 706

3. Select the **Phone Settings** tab.
4. Enter the IPv4 address (or host name) in the **SIP Server** field. This should be the WAN IPv4 address of the NetVanta 7000 Series unit through which the IP phone will be connecting.
5. For the **Boot Profile,** select **Remote Phone** using the radio button.



MAC Address: 00 04 F2 11 22 33

Phone Model: ADTRAN/Polycom IP 650

Phone Label: Default SIP User

Expansion ...: 0

Extension Dial Strings: ▸ Show

SLA Dial Strings ▸ Show

SIP Server: 192.0.2.2

Boot Profile: ○ Local Phone ● Remote Phone

Select the **Phone Settings** tab from the **IP Phone Configs** menu.

Enter the IPv4 address (or host name) for the WAN interface as the SIP server.

Change the a **Boot Profile** setting to **Remote Phone**.

6. Select **Apply** at the bottom of the menu to accept the changes. You may have to scroll down the menu to find this option.

Step 2: Configuring the SIP Server Settings

SIP INVITE authentication must be enabled from the **Local SIP Server Configuration** menu. From this same GUI menu, you will also add a non-standard port for SIP traffic destined for remote phones.

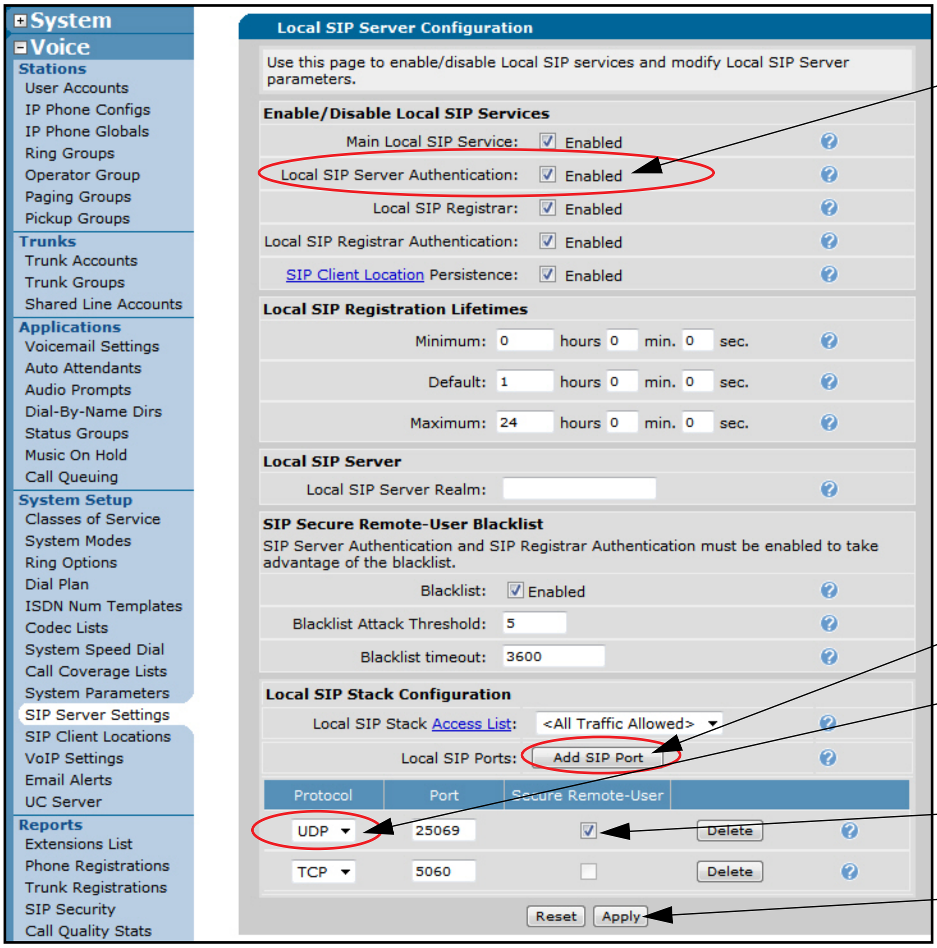
Use the following steps to enable SIP INVITE authentication and add a UDP SIP port:

1. Navigate to **Voice** > **System Setup** > **SIP Server Settings**.
2. Select the check box next to **Local SIP Server Authentication** to enable SIP INVITE authentication.
3. In the **Local SIP Stack Configuration** section, select **Add SIP Port** from **Local SIP Ports**.
4. Select **UDP** for the new **Protocol/Port**, and enter a non-standard port, such as **25069**. Select the check box under **Secure Remote-User** to enable security for this port. The **Secure Remote-User** functionality is not available on TCP ports.

> NOTE
>
> *For enhanced security on AOS R10.3.0 and later, ADTRAN recommends using a non-standard port (other than 5060) for SIP traffic destined for remote phones. The examples in this configuration guide use UDP port **25069**. You can use a port number appropriate for your network, but be sure to use the same port number in Step 4: Configuring Firewall Permissions on page 9 and Task 3: Altering the IP Phone Configuration Files on page 17. The valid port range is **0** to **65535**.*

Selecting **Secure Remote-User** for UDP ports allows SIP traffic only from configured remote voice users, causing SIP traffic from unconfigured remote voice users to be dropped. The system monitors the secure ports for REGISTER and INVITE attempts from remote voice users that fail to authenticate and logs them in the blacklist according to the settings under the **SIP Secure Remote-User Blacklist** section on this same GUI menu. The blacklisted table can be viewed from the **Reports** > **SIP Security** and is shown in *Troubleshooting on page 23*.

5. You can modify or delete this port, but no changes will occur until you select **Apply**.



Local SIP Server Configuration

Use this page to enable/disable Local SIP services and modify Local SIP Server parameters.

Enable/Disable Local SIP Services

Main Local SIP Service: ☑ Enabled

Local SIP Server Authentication: ☑ Enabled

Local SIP Registrar: ☑ Enabled

Local SIP Registrar Authentication: ☑ Enabled

SIP Client Location Persistence: ☑ Enabled

Local SIP Registration Lifetimes

Minimum: 0 hours 0 min. 0 sec.

Default: 1 hours 0 min. 0 sec.

Maximum: 24 hours 0 min. 0 sec.

Local SIP Server

Local SIP Server Realm:

SIP Secure Remote-User Blacklist

SIP Server Authentication and SIP Registrar Authentication must be enabled to take advantage of the blacklist.

Blacklist: ☑ Enabled

Blacklist Attack Threshold: 5

Blacklist timeout: 3600

Local SIP Stack Configuration

Local SIP Stack Access List: <All Traffic Allowed>

Local SIP Ports: Add SIP Port

Protocol	Port	Secure Remote-User	
UDP	25069	☑	Delete
TCP	5060	□	Delete

Reset Apply

Select the check box to enable **Local SIP Server Authentication**.

Select **Add SIP Port**.

Select **UDP** from the drop-down menu and enter a non-standard port number.

Select **Secure Remote User** to enable security.

Select **Apply** to accept the changes.

6. Select **Apply** to save the settings.

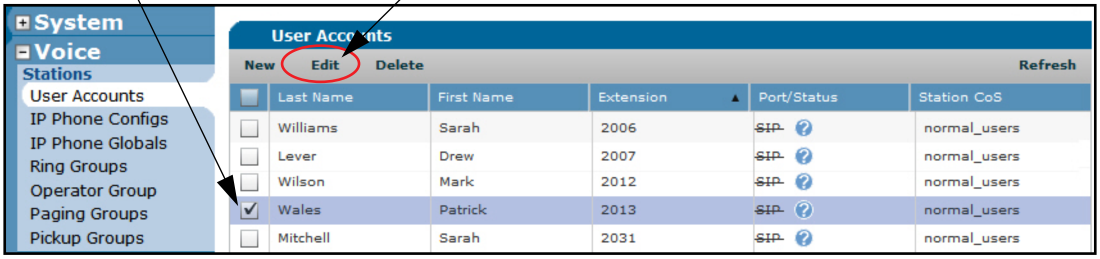
Step 3: Configuring Each Voice User for Remote Phone Mode

Voice user accounts are used to define phone users that are registered to the NetVanta 7000 Series unit. Each remote phone must have a corresponding voice user account. The configuration in this step describes how to enable remote phone mode for each user account. The user accounts should already exist on your NetVanta 7000 Series unit according to the instructions provided in *Configuring User Accounts on the NetVanta 7000 Series* available online at ADTRAN's Support Community, https://supportforums.adtran.com. Repeat this step for each remote phone and user you are configuring as simple remote phone. Users who are not configured as Simple Remote Phone users will not be able to access the unit on the secure UDP port(s).

1. Navigate to **Voice** > **Stations** > **User Accounts**.
2. Select the check box next to the voice user account for which to enable remote phone mode.
3. Select **Edit** to access the **User Account** menu.

Select the check box next to the user to be configured as a remote phone.

Select **Edit** to make changes to the user account.



User Accounts

New | Edit | Delete | Refresh

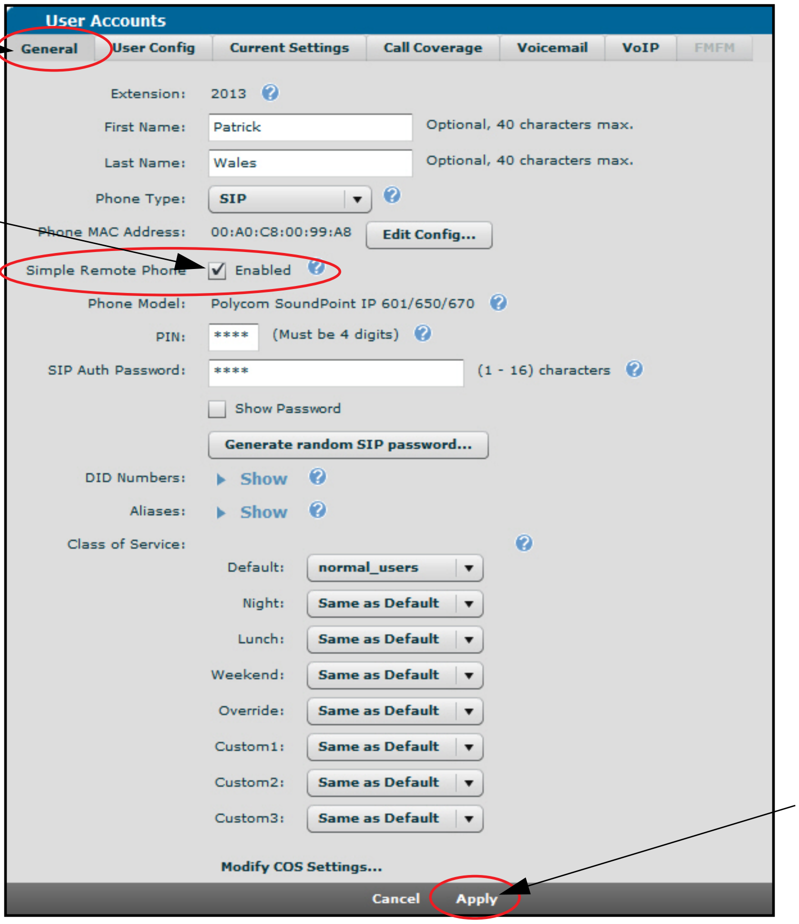
□	Last Name	First Name	Extension ▲	Port/Status	Station CoS
□	Williams	Sarah	2006	~~SIP~~	normal_users
□	Lever	Drew	2007	~~SIP~~	normal_users
□	Wilson	Mark	2012	~~SIP~~	normal_users
☑	Wales	Patrick	2013	~~SIP~~	normal_users
□	Mitchell	Sarah	2031	~~SIP~~	normal_users

4. From the **General** tab, select the check box next to **Simple Remote Phone** from the **General** tab.

Select the General tab.

Select the check box to enable **Simple Remote Phone** mode.

Select **Apply** to accept the changes.



User Accounts

Extension: 2013

First Name: Patrick Optional, 40 characters max.

Last Name: Wales Optional, 40 characters max.

Phone Type: SIP ▾

Phone MAC Address: 00:A0:C8:00:99:A8 Edit Config...

Simple Remote Phone ☑ Enabled

Phone Model: Polycom SoundPoint IP 601/650/670

PIN: **** (Must be 4 digits)

SIP Auth Password: **** (1 - 16) characters

□ Show Password

Generate random SIP password...

DID Numbers: ▸ Show

Aliases: ▸ Show

Class of Service:

Default: normal_users ▾

Night: Same as Default ▾

Lunch: Same as Default ▾

Weekend: Same as Default ▾

Override: Same as Default ▾

Custom1: Same as Default ▾

Custom2: Same as Default ▾

Custom3: Same as Default ▾

Modify COS Settings...

Cancel Apply

5. Select **Apply** to accept the changes.

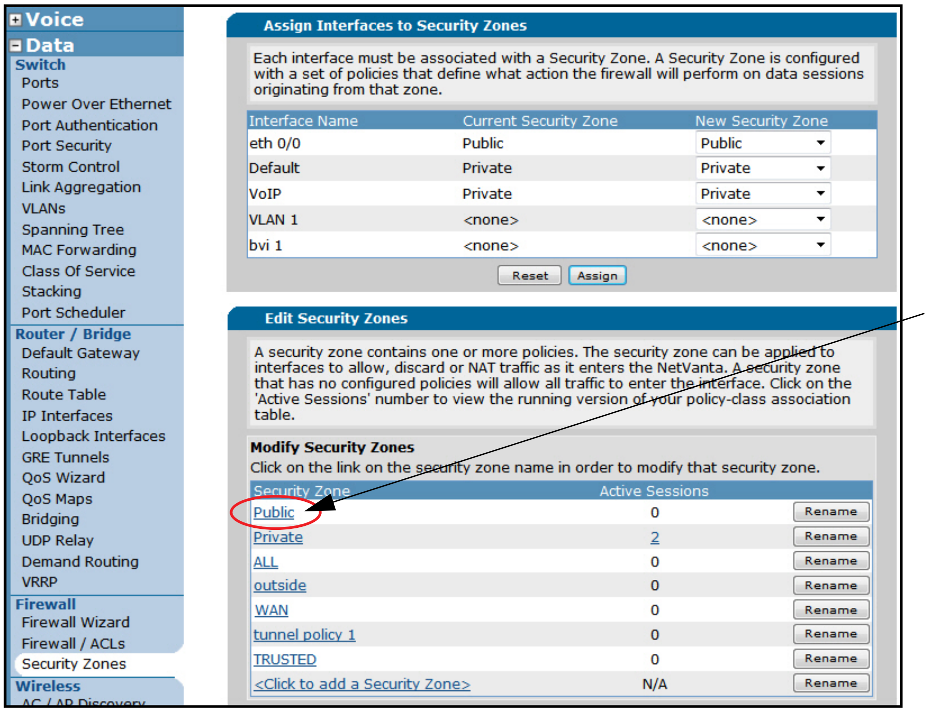
Step 4: Configuring Firewall Permissions

Modifications to the firewall settings are necessary to ensure that the remote phones operate properly. These modifications allow SIP and FTP traffic into the public security zone with certain limitations. In the most common scenario, it is necessary to configure the firewall to allow SIP traffic with the UDP port destination specified earlier in *Step 2: Configuring the SIP Server Settings on page 6*. This is accomplished by adding a policy to the public security zone that allows this specific traffic through the firewall. Allowing FTP traffic through the firewall is not necessary if the IP phones are configured prior to deployment outside the LAN. If the IP phones were configured locally, you can skip the steps to allow FTP traffic through the firewall.

> *Additional configuration settings are required to fully configure the firewall and depend upon the particular needs of each customer. For additional information on firewall configuration, refer to the AOS Command Reference Guide and the configuration guide, Configuring IPv4 Firewall in AOS, both available online at ADTRAN's Support Community, https://supportforums.adtran.com.*

In the following example, two firewall policies are configured in the public security zone. One policy is configured to allow any UDP traffic that is destined for port **25069**. Another policy is configured to allow FTP access through the firewall.

1. Proper security precautions should be taken in regards to allowing SIP traffic and FTP access to the NetVanta unit from outside sources. Refer to the *NetVanta 7000 Series Security Guide* available online at https://supportforums.adtran.com for specific recommendations.
2. Navigate to **Data** >**Firewall** > **Security Zones**.
3. Select the **Public** security zone from the list under **Edit Security Zones**.



Assign Interfaces to Security Zones

Each interface must be associated with a Security Zone. A Security Zone is configured with a set of policies that define what action the firewall will perform on data sessions originating from that zone.

Interface Name	Current Security Zone	New Security Zone
eth 0/0	Public	Public
Default	Private	Private
VoIP	Private	Private
VLAN 1	<none>	<none>
bvi 1	<none>	<none>

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.

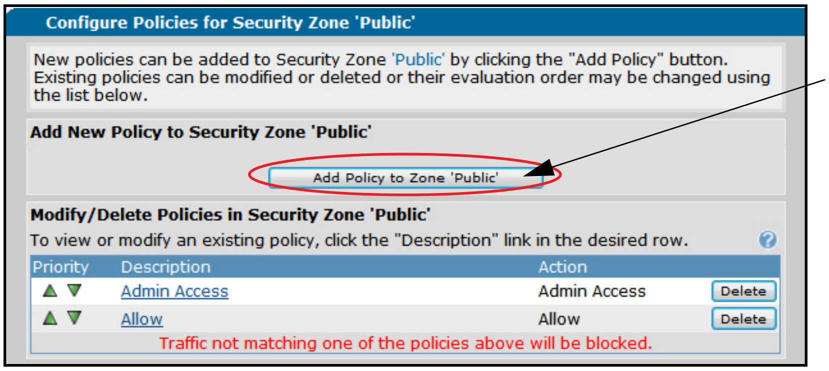
Modify Security Zones

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
WAN	0	Rename
tunnel policy 1	0	Rename
TRUSTED	0	Rename
<Click to add a Security Zone>	N/A	Rename

Select the **Public** security zone to add a new policy.

4. Create a policy to allow the SIP traffic for the specified UDP port. Select **Add Policy to Zone 'Public'**.



Configure Policies for Security Zone 'Public'

New policies can be added to Security Zone 'Public' by clicking the "Add Policy" button. Existing policies can be modified or deleted or their evaluation order may be changed using the list below.

Add New Policy to Security Zone 'Public'

Modify/Delete Policies in Security Zone 'Public'

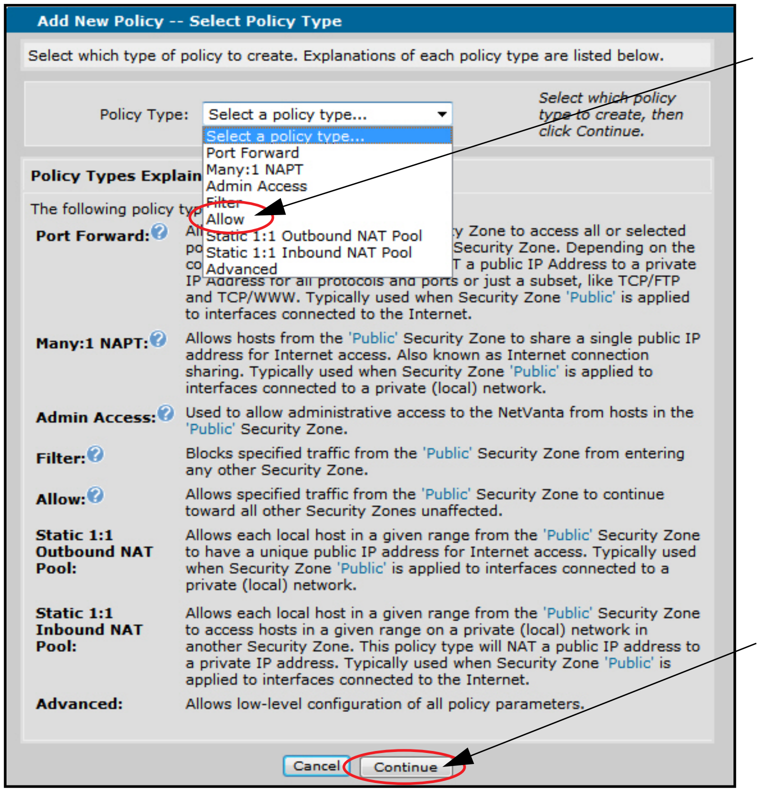
To view or modify an existing policy, click the "Description" link in the desired row.

Priority	Description	Action	
▲ ▼	Admin Access	Admin Access	Delete
▲ ▼	Allow	Allow	Delete

Traffic not matching one of the policies above will be blocked.

Select **Add Policy to Zone 'Public'** to open the **Add New Policy** menu.

5. Select **Allow** from the **Policy Type** drop-down menu and select **Continue**.



Add New Policy -- Select Policy Type

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

Policy Type: Select a policy type...

Select which policy type to create, then click Continue.

Policy Types Explain

The following policy typ

Port Forward: Al y Zone to access all or selected po Security Zone. Depending on the co T 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.

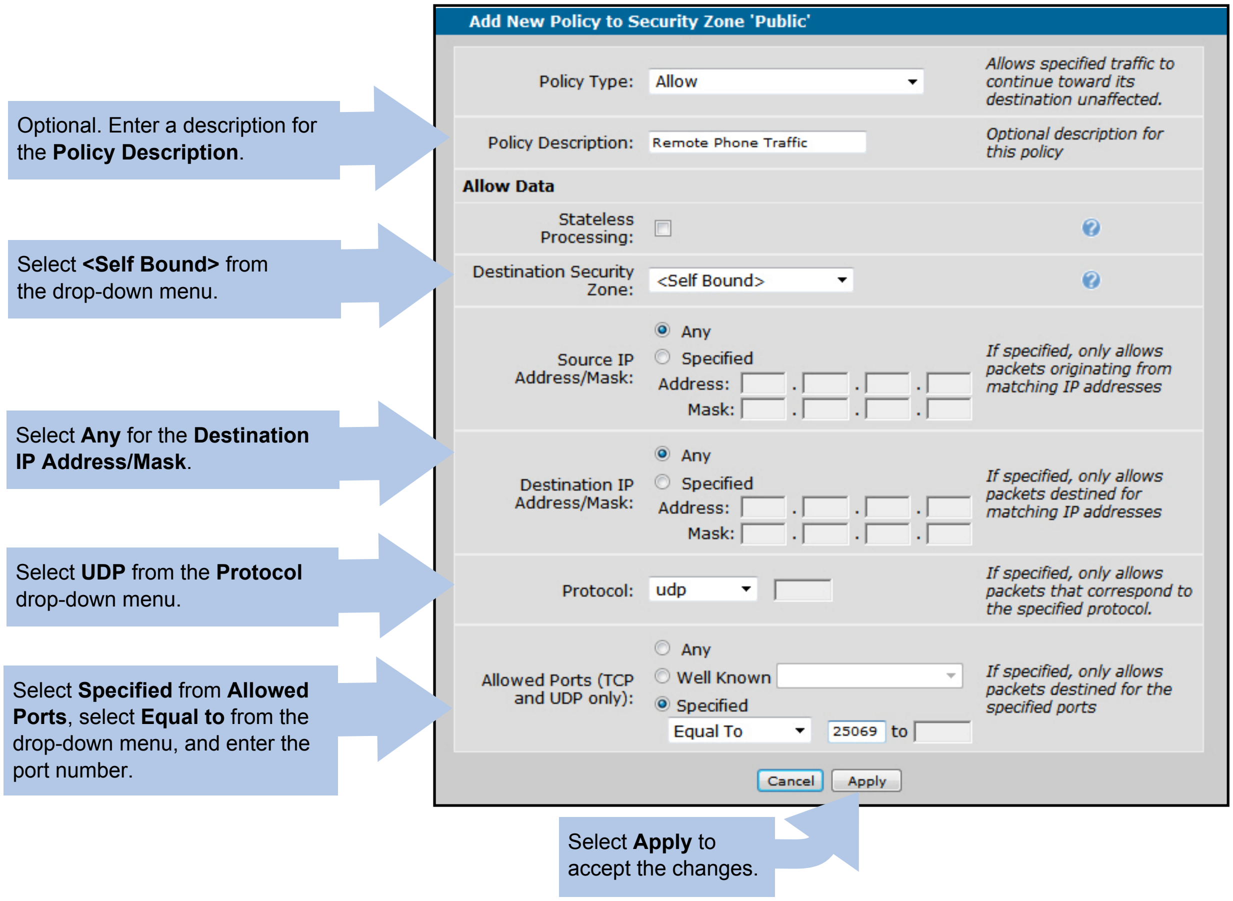
Select **Allow** from the **Policy Type** drop-down menu.

Select **Continue** to configure the new policy.

6. Optional. From the **Add New Policy to Security Zone 'Public'** menu, enter a **Policy Description**, such as **Remote Phone Traffic**.

7. Select **<Self Bound>** as the **Destination Security Zone**.

8. Select **Any** for the **Destination IP Address/Mask**. Select **UDP** for the **Protocol**, which allows only traffic that corresponds to the UDP protocol. From **Allowed Ports (TCP and UDP only)**, select **Specified** and choose **Equal To** from the drop-down menu. Enter the port number in the field that follows. For this example we've used **25069**. This port number should match the one used in *Step 2: Configuring the SIP Server Settings on page 6*. TCP traffic is not allowed through the secure ports.



Add New Policy to Security Zone 'Public'

Policy Type: Allow — *Allows specified traffic to continue toward its destination unaffected.*

Policy Description: Remote Phone Traffic — *Optional description for this policy*

Allow Data

Stateless Processing: □

Destination Security Zone: <Self Bound>

Source IP Address/Mask: ● Any ○ Specified Address: . . . Mask: . . . — *If specified, only allows packets originating from matching IP addresses*

Destination IP Address/Mask: ● Any ○ Specified Address: . . . Mask: . . . — *If specified, only allows packets destined for matching IP addresses*

Protocol: udp — *If specified, only allows packets that correspond to the specified protocol.*

Allowed Ports (TCP and UDP only): ○ Any ○ Well Known ● Specified Equal To 25069 to — *If specified, only allows packets destined for the specified ports*

Optional. Enter a description for the **Policy Description**.

Select **<Self Bound>** from the drop-down menu.

Select **Any** for the **Destination IP Address/Mask**.

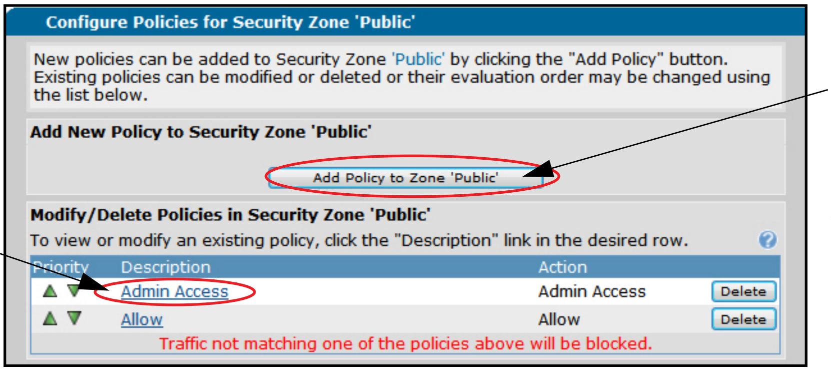
Select **UDP** from the **Protocol** drop-down menu.

Select **Specified** from **Allowed Ports**, select **Equal to** from the drop-down menu, and enter the port number.

Select **Apply** to accept the changes.

9. Select **Apply** to accept the changes.

10. Next, create a policy to allow FTP access. (This step is optional if IP phones were configured prior to deployment outside the LAN.) If an **Admin Access** policy already exists, select it to modify its settings, then skip to Step 12. If an **Admin Access** policy does not already exist, select **Add Policy to Zone 'Public'** to create a new policy and open the **Add New Policy** menu.



Configure Policies for Security Zone 'Public'

New policies can be added to Security Zone 'Public' by clicking the "Add Policy" button. Existing policies can be modified or deleted or their evaluation order may be changed using the list below.

Add New Policy to Security Zone 'Public'

Modify/Delete Policies in Security Zone 'Public'

To view or modify an existing policy, click the "Description" link in the desired row.

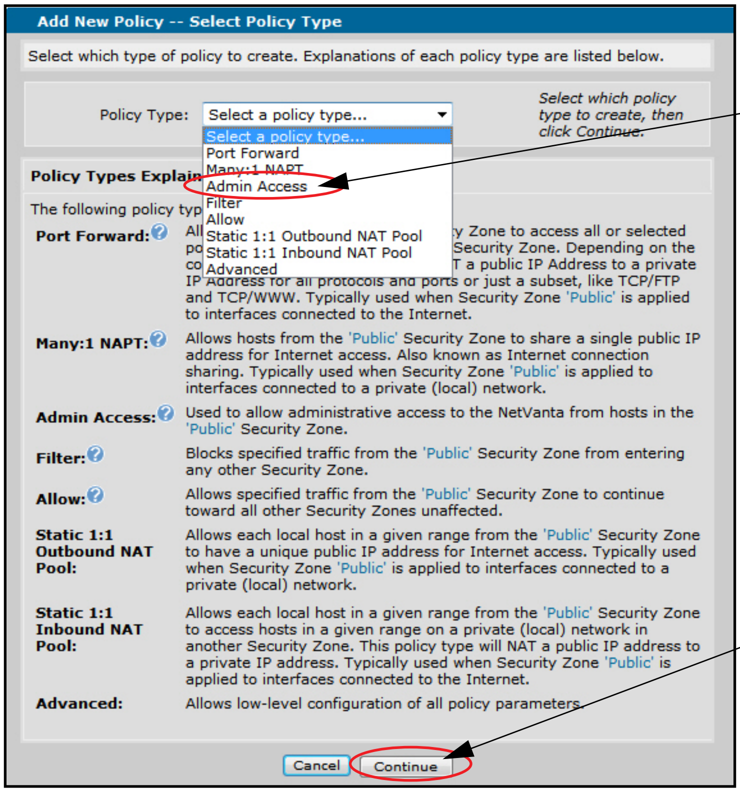
Priority	Description	Action	
▲ ▼	Admin Access	Admin Access	Delete
▲ ▼	Allow	Allow	Delete

Traffic not matching one of the policies above will be blocked.

Select the **Admin Access** policy to edit it.

If an **Admin Access** policy does not exist, select **Add Policy to Zone 'Public'** to open the **Add New Policy** menu.

11. Select **Admin Access** from the **Policy Type** drop-down menu and select **Continue**.



Add New Policy -- Select Policy Type

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

Policy Type: Select a policy type...

Select which policy type to create, then click Continue.

Policy Types Explain

The following policy typ

Port Forward: All y Zone to access all or selected po Security Zone. Depending on the co T 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.

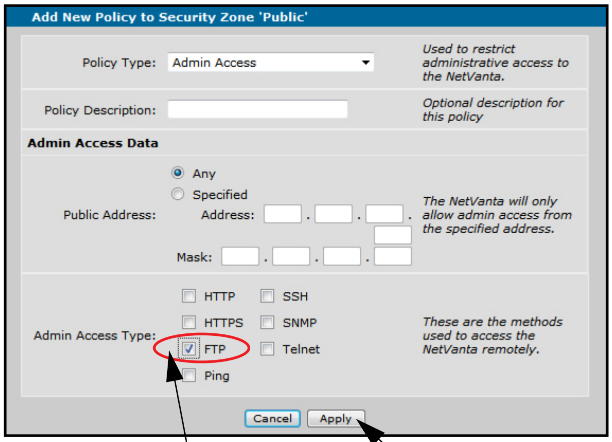
Advanced: Allows low-level configuration of all policy parameters.

Select **Admin Access** from the **Policy Type** drop-down menu.

Select **Continue** to configure the new policy.

12. Select the check box next to **FTP** for the **Admin Access Type** and select **Apply**.

Add a New Policy for Admin Access OR **Edit an Existing Admin Access Policy**



Add New Policy to Security Zone 'Public'

Policy Type: Admin Access ▾ — *Used to restrict administrative access to the NetVanta.*

Policy Description: — *Optional description for this policy*

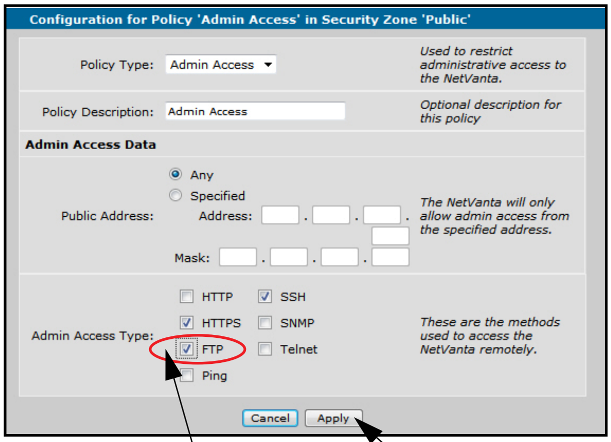
Admin Access Data

Public Address: ● Any ○ Specified Address: . . . Mask: . . . — *The NetVanta will only allow admin access from the specified address.*

Admin Access Type: □ HTTP □ SSH □ HTTPS □ SNMP ☑ FTP □ Telnet □ Ping — *These are the methods used to access the NetVanta remotely.*

Select **FTP** for the **Admin Access Type**.

Select **Apply**.



Configuration for Policy 'Admin Access' in Security Zone 'Public'

Policy Type: Admin Access ▾ — *Used to restrict administrative access to the NetVanta.*

Policy Description: Admin Access — *Optional description for this policy*

Admin Access Data

Public Address: ● Any ○ Specified Address: . . . Mask: . . . — *The NetVanta will only allow admin access from the specified address.*

Admin Access Type: □ HTTP ☑ SSH ☑ HTTPS □ SNMP ☑ FTP □ Telnet □ Ping — *These are the methods used to access the NetVanta remotely.*

Select **FTP** for the **Admin Access Type**.

Select **Apply**.

13. Select **Apply** to accept the changes. Once you have saved the changes, you can log out of the GUI.

Task 2: Specifying Registration Expire Times through the AOS CLI

At the present time, this task is limited to configuration through the CLI.

During registration, the user agent (UA) attempts to register for a specified amount of time. If the UA does not re-register before the expiration time, the registration expires.

If a softphone is being used as a simple remote phone, you should set the softphone's maximum registration request to a time less than your firewall's UDP session timeout (for example, 55 seconds). For all other phones, you must create an HMR to adjust the expiration times. Refer to the configuration guide, *Manipulating SIP Headers and Messages in AOS*, available online at https://supportforums.adtran.com, for more information about configuring HMR. The following section outlines the basic configuration steps necessary to enable the HMR feature necessary for Simple Remote Phones.

Accessing the CLI

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

1. Telnet to the unit (**telnet** <*ip address*>), for example:

   telnet 10.10.10.1.

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

2. 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.*

3. Enable your unit by entering **enable** at the prompt as follows:

```
>enable
```

4. If configured, enter your Enable mode password at the prompt.

> NOTE *The default Enable mode password is **password**. If your product no longer has the default Enable password, contact your system administrator for the appropriate password.*

5. Enter the unit's Global Configuration mode as follows:

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

Configuring HMR to Adjust Expiration Times

The following steps configure an HMR rule set to adjust the expiration times.

1. Create an HMR rule set. An HMR rule set is a named collection of one or more sequenced message rules. When a rule set is applied to a message, all matching message rules are processed in sequence.

   To create an HMR rule set and enter the rule set's configuration mode, enter the **hmr rule-set** <*name*> command from the Global Configuration mode. The <*name*> parameter is the name given to the HMR rule set. Names must be unique for each rule set you configure.

   To create the HMR rule set, and enter its configuration mode, enter the command as follows:

```
(config)#hmr rule-set REMOTE_PHONE_TWEAKS
Configuring new HMR rule set REMOTE_PHONE_TWEAKS
(config-rule-set-REMOTE_PHONE_TWEAKS)
```

2. Create HMR message rules for the rule set. A message rule is a collection of one or more header commands that determine the types of SIP headers to act upon and the action to be taken. When a message rule is applied to a SIP message, all matching header commands are processed.

   Each message rule is named and can be configured to apply to SIP responses. To create an HMR message rule and enter the rule's configuration mode, enter the **message-rule** <*name*> **message-type response** command from the rule set's configuration mode. The <*name*> parameter specifies the name of the message rule. Message rule names must be unique within the HMR rule set. The optional **message-type response** parameter specifies that the rule is applied to SIP response messages. Entering the command from the HMR Rule Set Configuration mode prompt as follows creates a message rule named **CHANGE_EXPIRES_TIME** that applies to SIP response messages and enters the rule's configuration mode:

```
(config-rule-set-REMOTE_PHONE_TWEAKS)#message-rule CHANGE_EXPIRES_TIME
        message-type response
Configuring new HMR message rule CHANGE_EXPIRES_TIME
```

3. Specify the HMR message rule's matching header action(s). HMR message rules are used to match specified SIP headers in a SIP message using the **match header** <*header*> **match-value** <*pattern*> command from the HMR Message Rule Configuration mode. The **match** commands allow you to specify conditions that must be true in order for the message rule to be processed. If a **match header** command is present in the message rule's configuration, the message rule is processed only if the header match resolves as true. Multiple **match header** commands can be present, but all of them must resolve as true for the message rule to be processed. The <*header*> parameter of the command indicates the SIP header to be used for matching. The optional **match-value** <*pattern*> parameter specifies the pattern to be used for matching. The <*pattern*> parameter can be entered as a regular expression or a text string, and can reference variable names. For more information about using regular expressions, refer to *Manipulating SIP Headers and Messages in AOS*, online at https://supportforums.adtran.com.

   To specify that the HMR rule matches SIP headers based on a specific header and a specified pattern, enter the commands from the HMR Message Rule Configuration mode as follows:

   ```
   (config-msg-rule-CHANGE_EXPIRES_TIME)#match header sip-status-line match-value /200/
   (config-msg-rule-CHANGE_EXPIRES_TIME)#match header from match-value /5\d{3}/
   (config-msg-rule-CHANGE_EXPIRES_TIME)#match header CSeq match-value /REGISTER/i
   ```

4. Specify the action the HMR message rule uses to modify the existing SIP headers. Use the **modify header** <*header*> **position first-match [match-value** <*pattern*>**] new-value** <*pattern*> command from the HMR Message Rule Configuration mode. The <*header*> parameter specifies the SIP header type that you want to modify in the SIP message. The **position first-match** keyword specifies the first matching header in the SIP message. The optional **match-value** <*pattern*> parameter specifies the pattern to use for matching and filters the SIP headers. The <*pattern*> parameter can be entered as a regular expression or a text string. If both the match pattern and SIP header are specified, the indicated header is modified if it contains the match pattern. If only the header type is specified, the SIP header is modified unconditionally. The **new-value** <*pattern*> parameter specifies the value to be assigned to the header, and it can include buffers captured with the optional **match-value** parameter.

   To modify a SIP header in the SIP message, enter the command from the HMR Message Rule Configuration mode as follows:

   ```
   (config-msg-rule-CHANGE_EXPIRES_TIME)#modify header expires position first-match
           new-value /55/
   (config-msg-rule-CHANGE_EXPIRES_TIME)#modify header contact position first-match
           match-value /(;expires=)\d+/i new-value /\155/
   ```

5. Create an HMR policy. The HMR policy is a named collection of one or more rule sets, and the policy is used to apply the rule sets to specific SIP traffic. Create the HMR policy using the **hmr policy** <*name*> command from the Global Configuration mode. The <*name*> parameter is a unique name given to the policy. To create the HMR policy **SIP_GLOBAL_OUT**, enter the command as follows:

   ```
   (config)#hmr policy SIP_GLOBAL_OUT
   Configuring new HMR policy SIP_GLOBAL_OUT
   (config-policy-SIP_GLOBAL_OUT)
   ```

6. Apply the HMR rule sets to an HMR policy. After creating the HMR policy in the Global Configuration mode, you must then apply the relevant rule sets to the policy. Rule sets are added to the policy using the **rule-set** <*name*> command from the HMR Policy Configuration mode. The <*name*> parameter is

the name of the previously created rule set that you want to apply to the policy. Multiple rule sets can be added to a single policy. When multiple rule sets are applied to a message, the results of each rule set are applied before the next rule set is evaluated and applied.

To add a rule set to an HMR policy, enter the **rule-set** command from the HMR Policy Configuration mode as follows:

```
(config-policy-SIP_GLOBAL_OUT)#rule-set REMOTE_PHONE_TWEAKS
```

7. Apply the HMR policy to all outbound SIP traffic. To apply an HMR policy to all outbound SIP traffic, enter the **ip sip hmr** *<policy name>* **out** command from the Global Configuration mode prompt. The *<policy name>* parameter specifies the HMR policy you are applying. In addition, you must specify that the policy is applied to outgoing SIP traffic on the device by using the **out** keyword.

   To add the HMR policy **SIP_GLOBAL_OUT** to the AOS unit for all outbound SIP traffic, enter the command as follows:

   ```
   (config)#ip sip hmr SIP_GLOBAL_OUT out
   ```

The following is a full example for configuring HMR to adjust expiration times:

```
(config)#hmr rule-set REMOTE_PHONE_TWEAKS
Configuring new HMR rule set REMOTE_PHONE_TWEAKS
(config-rule-set-REMOTE_PHONE_TWEAKS)#message-rule CHANGE_EXPIRES_TIME
        message-type response
Configuring new HMR message rule CHANGE_EXPIRES_TIME
(config-msg-rule-CHANGE_EXPIRES_TIME)#match header sip-status-line match-value /200/
(config-msg-rule-CHANGE_EXPIRES_TIME)#match header from match-value /5\d{3}/
(config-msg-rule-CHANGE_EXPIRES_TIME)#match header CSeq match-value /REGISTER/i
(config-msg-rule-CHANGE_EXPIRES_TIME)#modify header expires position first-match
        new-value /55/
(config-msg-rule-CHANGE_EXPIRES_TIME)#modify header contact position first-match
        match-value /(;expires=)\d+/i new-value /\155/
(config)#hmr policy SIP_GLOBAL_OUT
Configuring new HMR policy SIP_GLOBAL_OUT
(config-policy-SIP_GLOBAL_OUT)#rule-set REMOTE_PHONE_TWEAKS
(config)#ip sip hmr SIP_GLOBAL_OUT out
```

NOTE

AOS automatically creates sequence numbers at the end of certain commands when configuring HMR. The output from a ***show run*** *command issued after HMR configuration will display these sequence numbers.*

Task 3: Altering the IP Phone Configuration Files

Each IP phone has a configuration file that contains the SIP registration information. This SIP information must be altered to reflect the SIP port the remote phone should use to access the NetVanta 7000 Series unit. The configuration file must be downloaded through FTP from the NetVanta 7000 Series unit and altered using a text editor. Once the file is altered, save it to the NetVanta 7000 Series unit for the IP phone to download and update its configuration. The following instructions explain how to perform these steps.

> *The NetVanta 7000 Series unit includes an FTP server that is enabled by default. If you are accessing an existing installed unit and are uncertain whether the FTP server is enabled, use the* ***ip ftp server*** *command to enable it. Through the GUI, navigate to* ***System*** *>* ***IP Services*** *and check that* ***FTP Server*** *is enabled.*

1. Using your preferred FTP client, connect to the NetVanta 7000 Series unit with its IPv4 address. When prompted, enter the username and password.
2. Locate the appropriate configuration file for your IP phone type and download it. Depending on the brand of IP phone, this file will have one of the following naming schemes:
   - For ADTRAN IP phones (IP 700 Series), the filename is **adtran_*mac*.txt** where ***mac*** is the unique MAC address for the IP phone. This file is located in the ADTRAN directory on CompactFlash.
   - For Polycom IP phones, the filename is ***extension-mac*.cfg** where the ***extension*** is the extension number for the phone on the PBX and the ***mac*** is the unique MAC address for the IP phone. This file is located in the Polycom directory on CompactFlash.
3. Open the downloaded configuration file in a text editor and add the following information (depending on the IP phone type):
   - For ADTRAN IP phones, add the following two lines to the end of the configuration file, changing ***XXXXX*** to the SIP port number:

     ```
     RegServer.0.Port.1 XXXXX
     ProxyServer.0.Port.1 XXXXX
     ```

   - For Polycom IP phones, add the following command within the **<reg/>** section of the file, changing the ***XXXXX*** to the SIP port number:

     ```
     reg.1.server.1.port="XXXXX"
     ```

> *For enhanced security on AOS R10.3.0 and later, ADTRAN recommends using a non-standard port (other than 5060) for SIP traffic destined for remote phones. The examples in this configuration guide use UDP port* ***25069****. You can use a port number appropriate for your network, but be sure to use the same port number in Step 2: Configuring the SIP Server Settings on page 6 and Step 4: Configuring Firewall Permissions on page 9 as you use in this step.*

4. Save the configuration file and replace it on the NetVanta 7000 Series unit through FTP.
5. Reboot the IP phone to allow it to download the new configuration file and apply the changes.

Task 4: Configure the Boot Server Address for the IP Phone

Each IP phone must be able to locate the boot server. The boot server IPv4 address is provided either using the default DHCP options (option 66 for Polycom phones or option 157 for ADTRAN IP phones), or manually entering the IPv4 address in the IP phone menus. Instructions for each method is provided in this section. Select the applicable method for your situation.

Using DHCP Options 66 or 157

The default method for obtaining a boot server IPv4 addresses for both ADTRAN and Polycom IP phones is to use DHCP options. ADTRAN IP phones use DHCP option 157, and Polycom IP phones use DHCP option 66. If you plan to use this method, you must configure the remote router or server acting as the DHCP server for the remote phone with the appropriate DHCP option for your phone type. Below are example strings to use in either case:

- Option 66 for Polycom Phones, example String: **ftp://polycomftp:password@192.0.2.2/polycom**
- Option 157 for ADTRAN IP Phones, example String: **TftpServers=0.0.0.0,FtpServers=192.0.2.2:/ADTRAN,FtpLogin=polycomftp,FtpPassword=password,Layer2Tagging=True,VlanID=2**

NOTE *The default FTP username is **polycomftp** and the default FTP password is **password**. If this has been changed, contact your system administrator to obtain the proper FTP credentials. ADTRAN recommends changing the default passwords, especially if opening the firewall to FTP access.*

Manually Providing the IPv4 Address

The IPv4 address of the boot server can be manually entered through the phone menus if you don not plan to use the DHCP options described above. Use the following instructions for your specific IP phone model to complete this task.

ADTRAN IP Phones

This method is only supported on ADTRAN IP phones with R2 firmware (2.0.0) or later, and is not supported on version 1.3.16 and earlier. R2 firmware added the ability to configure FTP server settings. To check the firmware version on your ADTRAN IP phone, navigate to **Menu** > **1. Phone Status** > **4. Firmware Version**. If your firmware needs to be upgraded, refer to *Upgrading IP 700 Series Phone Firmware* available online at https://supportforums.adtran.com.

1. Press the **Menu** button.
2. Select **2**. **Phone Settings** and **6**. **Network**.
3. Enter the password. If the phone has been previously configured, enter **456**. If the phone is new and has never been confirgured, enter **1234**. After entering the password, press **Ok**.
4. Select **7. Server Menu**. Edit the server type by selecting **1. Server Type** and select **FTP**. Press **Ok**.
5. Once you are returned to the **Server Menu**, select **2. Address** to enter the WAN IPv4 address of the NetVanta 7000 Series with a **/ADTRAN** path (for example, **192.0.2.2/ADTRAN**).When entering the server address use the **Aa1** softkey to switch between alpha and numeric characters. Use the ***** (asterisk)

key to enter the decimals for the IPv4 address. Use the # (pound) key to enter the /. Press **Ok** after entering the address path.

6. Select **3. Login**, enter the FTP username, and press **Ok.** Select **4. Password** to enter the FTP password, and then press **Ok**. Both of these entries are the FTP username and password used on the NetVanta 7000 Series unit. The default username is **polycomftp** and password is **password**.

> *ADTRAN recommends changing the default passwords, especially if opening the firewall to FTP access.*

7. After entering this information, select **Exit** until you return to the main phone menu.

Polycom IP Phones

1. Press the **Menu** button.
2. Select **Settings** and **Advanced**.
3. Enter the password **456**.
4. Select **Admin Settings** > **Network Configuration > Server Menu**.
5. Select the **Server Type**, and set the type to **FTP**.
6. Select the **Server Address**. Enter the WAN IPv4 address of the NetVanta 7000 Series with a **/polycom** path (for example, **198.165.1.4/polycom**). When entering the server address use the **1/A/a** softkey to switch between alpha and numeric characters. Use the ***** (asterisk) to enter the decimals for the IPv4 address. Use the # (pound) key to enter the /.
7. Edit the **Server User** and **Server Password** to enter the FTP username and password used on the NetVanta 7000 Series unit. The default username is **polycomftp** and password is **password**.

> *ADTRAN recommends changing the default passwords, especially if opening the firewall to FTP access.*

8. After entering this information press the **Back** softkey twice, and select **Save Config** to preserve these changes.

This concludes the configuration steps necessary for the Simple Remote Phones feature.

Configuration Example

The following example enables a NetVanta 7000 Series unit to receive SIP registrations from remote phones that are located behind a non-SIP aware router. It uses HMR to modify the registration expiration times to keep the firewall sessions established on the remote non-SIP aware router. Two SIP users are created, one for extension **5555** and one for extension **5777**. Both SIP users have remote phone mode enabled, and authentication is required to register with NetVanta 7000 Series unit.

The Ethernet 0/0 (eth 0/0) port is connected to the public Internet and uses the IPv4 address of **192.0.2.2**. The firewall is configured with IPv4 ACLs to allow UDP SIP traffic on port 25069. The remote phones were configured manually or by a remote DHCP server to register to the public IPv4 address of the NetVanta 7000 Series unit (192.0.2.2) on UDP port 25069.

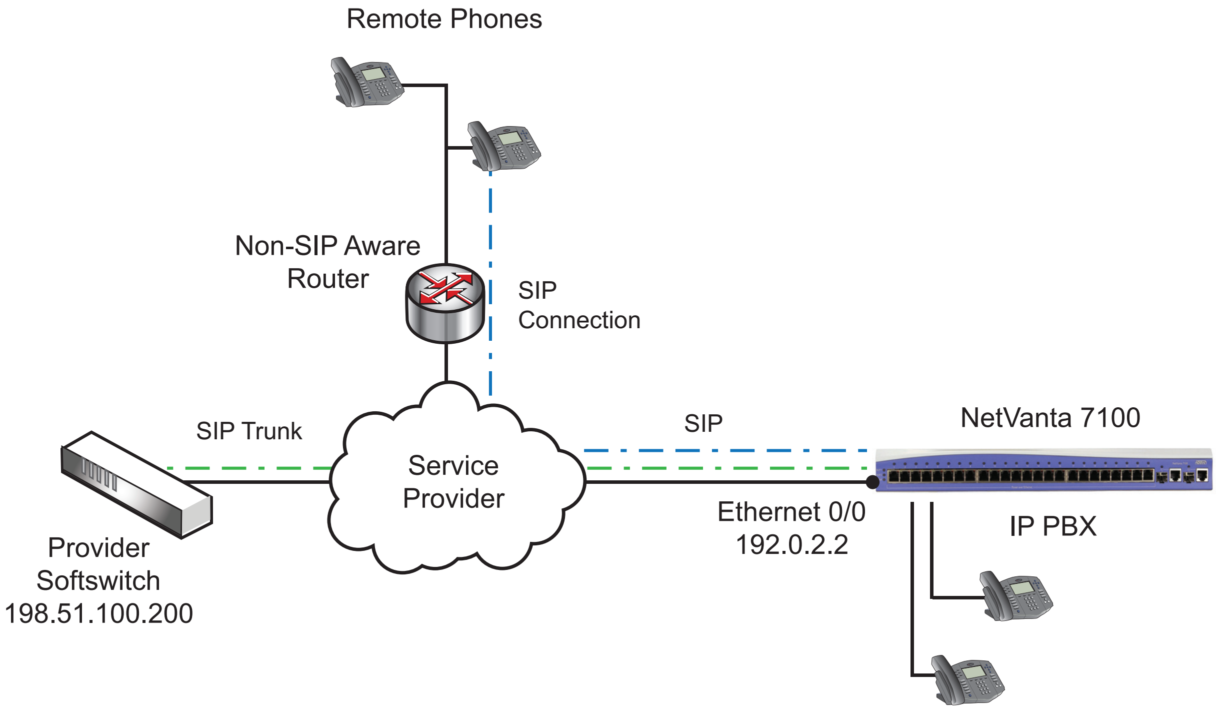


Figure 1. Simple Remote Phones Example with a NetVanta 7100

> NOTE *The configuration parameters entered in this example are sample configurations only, and only pertain to the configuration of simple remote phones. This application should be configured in a manner consistent with the needs of your particular network. CLI prompts have been removed from the configuration example to provide a method of copying and pasting configurations directly from this configuration guide into the CLI. This configuration should not be copied without first making the necessary adjustments to ensure it will function properly in your network.*

> NOTE *AOS automatically creates sequence numbers (i.e., 10 and 20) at the end of certain commands when configuring HMR. The output below shows these sequence numbers, but they are not required to be entered with the commands.*

```
!
ip sip udp 25069
!
ip sip authenticate
!
hmr rule-set REMOTE_PHONE_TWEAKS
  message-rule CHANGE_EXPIRES_TIME message-type response 10
```

```
    match header sip-status-line match-value /200/
    match header from match-value /5\d{3}/
    match header CSeq match-value /REGISTER/i
    modify header Expires position first-match new-value /55/ 10
    modify header contact position first-match match-value /(;expires=)\d+/i new-value /\155/ 20
!
hmr policy SIP_GLOBAL_OUT
  rule-set REMOTE_PHONE_TWEAKS 10
!
ip sip hmr SIP_GLOBAL_OUT out
!
voice user 5555
  remote-phone
!
voice user 5777
  remote-phone
!
ip access-list extended ADMIN
 remark “Admin Access”
 permit tcp any  any eq https
 permit tcp any  any eq ssh
!
ip access-list standard MATCH_ALL
 remark “All Traffic”
 permit any
!
ip access-list extended REMOTE_PHONES
 remark “Remote Phone Traffic”
 permit udp any any eq 25069
!
ip access-list extended SIP
 remark “SIP Traffic”
 permit udp host 198.51.100.200 any eq 5060
!
ip policy-class PRIVATE
 allow list MATCH_ALL self
 nat source list MATCH_ALL interface ethernet 0/0 overload
!
ip policy-class PUBLIC
 allow list SIP self
 allow list REMOTE_PHONES self
 allow list ADMIN self
!
end
```

Configuration Command Summary

The following table summarizes the commands used to configure simple remote phone in AOS products, using the CLI. This table is provided for reference for configurations using the CLI only and may not be presented in the same order as the GUI steps.

Table 2. AOS CLI Command Summary

Step	Command	Description
Step 1	Enable SIP on a non-standard UDP port.	
	(config)#**ip sip udp** *<port>*	Enables SIP on a UDP port (other than 5060).
Step 2	Enable SIP call authentication.	
	(config)#**ip sip authenticate**	Enable SIP INVITE authentication.
Step 3	Specify registration expire times by setting softphone expire times according to the softphone being used or creating HMR for physical phones.	
	(config)#**hmr rule-set** *<name>*	Creates an HMR rule set and enters the rule set's configuration mode.
	(config-rule-set-set1)#**message-rule** *<name>* **message-type response**	Creates a message rule for the rule set and specifies the message type to which the rule applies.
	(config-msg-rule-rule1)#**match header** *<header>* **match-value** *<pattern>*	Specifies that the message rule match the specified SIP header and specifies a pattern used for matching. Patterns can be a regular expression or text string.
	(config-msg-rule-rule1)#**modify header** *<header>* **position first-match match-value** *<pattern>* **new-value** *<pattern>*	Specifies that the message rule modifies the specified header, in which position the specified header resides, and the **match-value** parameter specifies a pattern used for matching. Patterns can be a regular expression, text string, or variable. The **new-value** parameter specifies the new value to assign to the header, which can also be a regular expression or text string.
	(config)#**hmr policy** *<name>*	Creates an HMR policy and enters the policy's configuration mode.
	(config-policy-MYPOLICY1)#**rule-set** *<name>*	Applies a rule set to an HMR policy.
	(config)#**ip sip hmr** *<policy name>* **out**	Applies an HMR policy to all outgoing SIP traffic.

Table 2. AOS CLI Command Summary *(Continued)*

Step	Command	Description
Step 4	Enable remote phone mode for each SIP user.	
	(config)#**voice user** <*extension*>	Enters the Voice User Account Configuration mode.
	(config-extension)#**remote-phone**	Enables remote phone mode for this user.
Step 5	Configure firewall settings to allow SIP traffic (destined for the UDP port specified in **Step 1**) into the public interface.	
	(config)#**ip access-list extended** <*name*>	Creates an extended IPv4 ACL and enters the Extended IPv4 ACL Configuration mode.
	(config-ext-nacl)#**remark** <*"remark"*>	Associates a descriptive tag with an IPv4 ACL. Tags can be up to 80 alphanumeric characters enclosed in quotation marks.
	(config-ext-nacl)#**permit udp host** <*ipv4 address*> **any eq** <*port*>	Permits UDP packets originating from a specific IP address, with **any** destination IPv4 address and a port equal to the **eq** <*port*>. The **host** <*ipv4 address*> parameter specifies a single host address. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**). The <*port*> specifies the port number. Range is **0** to **65535**.
Step 6	Apply the ACL to the policy class.	
	(config)#**ip policy-class** <*ipv4 acp name*>	Create an ACP and enter the ACP configuration mode.
	(config-policy-class)#**allow list** <*ipv4 acp name*> **self**	Specify an ACL to determine which packets are allowed to enter the interface to which the ACP is assigned, and create a firewall association in the firewall.

Troubleshooting

There are several methods available to assist in troubleshooting your configuration settings and parameters. Both the GUI and CLI offer assistance. This section provides many of those available to you and how to access them.

Show Commands

The following **show** commands can be used to display specific portions of the configuration. These commands are all entered from the Enable mode.

The **show run voice user [**<*number*>**] [verbose**] command displays voice user information. The optional <*number*> parameter specifies which voice user information is displayed, and the optional **verbose** keyword indicates all information for voice users is displayed. The following is sample output from this command:

```
#show run voice user
Building configuration...
!
!
voice user 5001
  connect sip
  sip authentication password "fRiaxoecrOus9Iup"
  remote-phone
!
voice user 8002
  connect sip
  sip-authentication password "BIUT5iuSiejoaTHo"
!
end
```

The **show sip user-registration** command displays SIP server registration information. The following is sample output from this command:

```
#show sip user-registration
EXT.        TYPE                                    IP ADDRESS          PORT        EXP
----------  --------------------------------------  ------------------  ---------   --------
5001        Adtran-SIP-IP712/v2.2.0T3               10.17.125.225       1046        25
8002        Adtran-SIP-IP712/v2.2.0T3               10.10.10.2          5060        3419
Total phones registered: 2
```

SIP Security Statistics for Remote Users

To display SIP secuirty statististics regarding remote users, such as dropped requests and suspect and blacklist entries, enter the **show sip secure remote-user** [**blacklist** | **dropped-requests**] command. Including the optional **blacklist** parameter displays only SIP security blacklisted entries. Including the optional **dropped-requests** parameter displays dropped SIP requests on secure ports. The following is sample output from this command:

```
#show sip secure remote-user

Dropped SIP Request Information:

Port     Protocol     Registers     Invites       Other Requests
-------  ------------ ------------- ----------    ----------------------
2112     UDP           0            33                                 0

Number of secure ports: 1

Suspect Entries:
10.10.23.2 : 16348 / UDP
   User/Agent: 2565551234/Adtran-SIP-IP706/v2.4.0.3
   Timeout (seconds): 600
```

```
Total suspect entries: 1

Blacklisted Entries:
10.10.19.1 : 32768 / UDP
   User/Agent: 2565556789/Adtran-SIP-IP706/v2.4.0.3
   Timeout (seconds): 3600
Total blacklisted entries: 1

* Port, protocol, and User/Agent values taken from first suspect SIP message
```

These statistics display the number of dropped SIP requests and the type, such as registers and invites, that were encountered on the configured secure port. **Other Requests** include ACK, CANCEL, OPTIONS, SUBSCRIBE, NOTIFY, PUBLISH, INFO, REFER, MESSAGE, and UPDATE requests. The output also displays the number of suspect entries with summary information which includes the IPv4 address and voice user attemping a call. Once the number of failed attempts from an IPv4 address, regardless of its source port, exceeds the blacklist attack threshold, a blacklist entry is recorded and the IPv4 address is removed from the suspect list.

A maximum number of 100 combined entries can be stored in the suspect and blacklist entry tables. If the maximum number is exceeded, the oldest entries from the suspect list are removed as needed to make room for new blacklist entries, and no new suspect entries are added. When there are no suspect entries left to sacrifice for space, no more blacklists entries will be added until blacklist entries are removed either manually (using the **clear sip secure remote-user blacklist** command) or through timeouts.

Clear Commands

To clear SIP security remote user statistics, enter the **clear sip secure remote-user [blacklist | blacklist** *<ipv4 address>* **| dropped-requests**] command. If you do not specify the IPv4 address for the blacklist item to clear, all blacklist items are cleared. The following example displays the results of the **show sip secure remote-user** command once blacklist items are cleared:

```
#clear sip secure remote-user blacklist
#show sip secure remote-user

Dropped SIP Request Information:

Port    Protocol    Registers    Invites       Other Requests
------  ----------- ------------ ----------    ---------------------
2112    UDP         0            33                                0

Number of secure ports: 1
There are no suspect entries reported.
There are no blacklisted entries reported.
```

Debug Commands

The **debug sip stack messages** command activates debug messages associated with SIP stack events. Debug messages are displayed in real time. Use the **no** form of this command to disable the debug messages.

> *Turning on a large amount of debug information can adversely affect the performance of your unit.*

```
#debug sip stack message
18:35:35.311 SIP.STACK MSG    Rx: UDP src=10.17.125.225:1046 dst=10.17.125.213:5060
18:35:35.312 SIP.STACK MSG      REGISTER sip:10.17.125.213 SIP/2.0
18:35:35.312 SIP.STACK MSG      Via: SIP/2.0/UDP 192.168.2.8;branch=z9hG4bK860fdff897075D95
18:35:35.312 SIP.STACK MSG      From: "5001" <sip:5001@10.17.125.213>;tag=D798FD35-CE6BB98
18:35:35.312 SIP.STACK MSG      To: <sip:5001@10.17.125.213>
18:35:35.313 SIP.STACK MSG      CSeq: 357 REGISTER
18:35:35.313 SIP.STACK MSG      Call-ID: 34798381-9342341b-79e412be@192.168.2.8
18:35:35.314 SIP.STACK MSG      Contact: <sip:5001@192.168.2.8>;methods="INVITE, ACK, BYE,
    CANCEL, OPTIONS, INFO, MESSAGE, SUBSCRIBE, NOTIFY, PRACK, UPDATE, REFER"
18:35:35.315 SIP.STACK MSG      Authorization: Digest username="5001", realm="192.168.2.213",
    nonce="44ee20831d39", uri="sip:10.17.125.213", response="d4001619a9af0b36e7e5f89565b542c6",
    algorithm=MD5
18:35:35.315 SIP.STACK MSG      Max-Forwards: 70
18:35:35.315 SIP.STACK MSG      Expires: 55
18:35:35.316 SIP.STACK MSG      Content-Length: 0
18:35:35.316 SIP.STACK MSG
18:35:35.322 SIP.STACK MSG    Tx: UDP src=10.17.125.213:5060 dst=10.17.125.225:1046
18:35:35.322 SIP.STACK MSG      SIP/2.0 200 OK
18:35:35.322 SIP.STACK MSG      From: "5001"<sip:5001@10.17.125.213>;tag=D798FD35-CE6BB98
18:35:35.323 SIP.STACK MSG      To: <sip:5001@10.17.125.213>;
    tag=4518a18-7f000001-13c4-29ba-4ecb051e-29ba
18:35:35.323 SIP.STACK MSG      Call-ID: 34798381-9342341b-79e412be@192.168.2.8
18:35:35.323 SIP.STACK MSG      CSeq: 357 REGISTER
18:35:35.324 SIP.STACK MSG      Contact: <sip:5001@192.168.2.8>;methods="INVITE, ACK, BYE,
    CANCEL, OPTIONS, INFO, MESSAGE, SUBSCRIBE, NOTIFY, PRACK, UPDATE, REFER"
18:35:35.324 SIP.STACK MSG      Expires: 55
18:35:35.324 SIP.STACK MSG      Via: SIP/2.0/UDP 192.168.2.8; received=10.17.125.225;
    branch=z9hG4bK860fdff897075D95
18:35:35.325 SIP.STACK MSG      Supported: 100rel,replaces
18:35:35.325 SIP.STACK MSG      Allow: ACK, BYE, CANCEL, INFO, INVITE, NOTIFY, OPTIONS,
    PRACK, REFER, REGISTER
18:35:35.325 SIP.STACK MSG      User-Agent: ADTRAN_NetVanta_7100
18:35:35.326 SIP.STACK MSG      Content-Length: 0
```

The **debug sip secure remote-user** command activates debug messages associated with SIP security remote user events. Debug messages are displayed in real time. Use the **no** form of this command to disable the debug messages. The following is a portion of the sample output displayed while debug messages for SIP security for remote users is enabled:

```
#debug sip secure remote-user
10:05:26.224 SIP.REMOTE-SECURITY Source IP 10.10.23.2 has failed 4 of 5 authentication attempts
10:05:26.276 SIP.STACK MSG    Rx: UDP src=10.10.23.2:2112 dst=10.17.220.104:2112
10:05:26.277 SIP.STACK MSG       ACK sip:2565556674@10.17.220.104:2112 SIP/2.0
10:05:26.277 SIP.STACK MSG       Max-Forwards: 70
10:05:26.277 SIP.STACK MSG       Content-Length: 0
10:05:26.278 SIP.STACK MSG       Via: SIP/2.0/UDP 10.10.23.2:2112;branch=z9hG4bK074b144b7
10:05:26.278 SIP.STACK MSG       Call-ID: 46ae9a82b800b24835b7f4cb13cca524@10.10.23.2
10:05:26.278 SIP.STACK MSG       From: 2565551234
    <sip:2565551234@10.17.220.104:2112>;tag=033a263449c0a29
10:05:26.278 SIP.STACK MSG       To: 2565556674
    <sip:2565556674@10.17.220.104:2112>;tag=5cef930-7f000001-13c4-13793-e966789b-13793
10:05:26.279 SIP.STACK MSG       CSeq: 3784849 ACK
10:05:26.279 SIP.STACK MSG       User-Agent: Adtran-SIP-IP706/v2.4.0.3
10:05:26.280 SIP.STACK MSG
10:05:26.318 SIP.STACK MSG    Rx: UDP src=10.10.23.2:2112 dst=10.17.220.104:2112
10:05:26.318 SIP.STACK MSG       INVITE sip:2565556674@10.17.220.104:2112 SIP/2.0
10:05:26.318 SIP.STACK MSG       Max-Forwards: 70
10:05:26.319 SIP.STACK MSG       Content-Length: 331
10:05:26.319 SIP.STACK MSG       Via: SIP/2.0/UDP 10.10.23.2:2112;branch=z9hG4bK75e4e3c2b
10:05:26.319 SIP.STACK MSG       Call-ID: 46ae9a82b800b24835b7f4cb13cca524@10.10.23.2
10:05:26.320 SIP.STACK MSG       From: 2565551234
    <sip:2565551234@10.17.220.104:2112>;tag=033a263449c0a29
10:05:26.320 SIP.STACK MSG       To: 2565556674 <sip:2565556674@10.17.220.104:2112>
10:05:26.320 SIP.STACK MSG       CSeq: 3784850 INVITE
10:05:26.321 SIP.STACK MSG       Supported: 100rel
10:05:26.321 SIP.STACK MSG       Supported: timer
10:05:26.321 SIP.STACK MSG       Allow: INVITE, ACK, CANCEL, BYE, NOTIFY, REFER, OPTIONS,
    UPDATE, PRACK, SUBSCRIBE, MESSAGE, INFO
10:05:26.322 SIP.STACK MSG       Content-Type: application/sdp
10:05:26.322 SIP.STACK MSG       Supported: replaces
10:05:26.322 SIP.STACK MSG       Authorization:Digest
    response="0b01e2101eabc0013bb5fa676895d90a",username="2565551234",realm="10.17.220.104"
    ,nonce="5cef93055c23",uri="sip:2565556674@10.17.220.104:2112"
10:05:26.323 SIP.STACK MSG       Contact: 2565551234
    <sip:2565551234@10.10.23.2:2112;transport=udp>
10:05:26.323 SIP.STACK MSG       User-Agent: Adtran-SIP-IP706/v2.4.0.3
10:05:26.323 SIP.STACK MSG
10:05:26.324 SIP.STACK MSG       v=0
10:05:26.324 SIP.STACK MSG       o=MxSIP 0 0 IN IP4 10.10.23.2
10:05:26.324 SIP.STACK MSG       s=SIP Call
10:05:26.324 SIP.STACK MSG       c=IN IP4 10.10.23.2
10:05:26.325 SIP.STACK MSG       t=0 0
```

```
10:05:26.325 SIP.STACK MSG        m=audio 3000 RTP/AVP 9 0 8 18 113 101
10:05:26.326 SIP.STACK MSG        a=rtpmap:9 G722/8000
10:05:26.326 SIP.STACK MSG        a=rtpmap:0 PCMU/8000
10:05:26.326 SIP.STACK MSG        a=rtpmap:8 PCMA/8000
10:05:26.326 SIP.STACK MSG        a=rtpmap:18 G729/8000
10:05:26.327 SIP.STACK MSG        a=rtpmap:113 L16/16000
10:05:26.327 SIP.STACK MSG        a=rtpmap:101 telephone-event/8000
10:05:26.327 SIP.STACK MSG        a=silenceSupp:off - - - -
10:05:26.328 SIP.STACK MSG        a=fmtp:101 0-15
10:05:26.328 SIP.STACK MSG        a=ptime:20
10:05:26.328 SIP.STACK MSG        a=sendrecv
10:05:26.329 SIP.STACK MSG
10:05:26.334 SIP.STACK MSG      Tx: UDP src=10.17.220.104:2112 dst=10.10.23.2:2112
10:05:26.335 SIP.STACK MSG        SIP/2.0 401 Unauthorized
10:05:26.335 SIP.STACK MSG        From: 2565551234
    <sip:2565551234@10.17.220.104:2112>;tag=033a263449c0a29
10:05:26.335 SIP.STACK MSG        To: 2565556674
    <sip:2565556674@10.17.220.104:2112>;tag=5cefb30-7f000001-13c4-13793-b6083b99-13793
10:05:26.336 SIP.STACK MSG        Call-ID: 46ae9a82b800b24835b7f4cb13cca524@10.10.23.2
10:05:26.336 SIP.STACK MSG        CSeq: 3784850 INVITE
10:05:26.337 SIP.STACK MSG        WWW-Authenticate: Digest
    realm="10.17.220.104",nonce="5cefb3055c47"
10:05:26.337 SIP.STACK MSG        Via: SIP/2.0/UDP 10.10.23.2:2112;branch=z9hG4bK75e4e3c2b
10:05:26.337 SIP.STACK MSG        Supported: 100rel,replaces
10:05:26.338 SIP.STACK MSG        Allow: ACK, BYE, CANCEL, INFO, INVITE, NOTIFY, OPTIONS,
    PRACK, REFER, REGISTER
10:05:26.338 SIP.STACK MSG        User-Agent: ADTRAN_NetVanta_7100/SIP6.016.D.E
10:05:26.338 SIP.STACK MSG        Content-Length: 0
10:05:26.338 SIP.STACK MSG
2013.03.01 10:05:26 SIP.REMOTE-SECURITY SIP traffic from 10.10.23.2 has been blacklisted
```

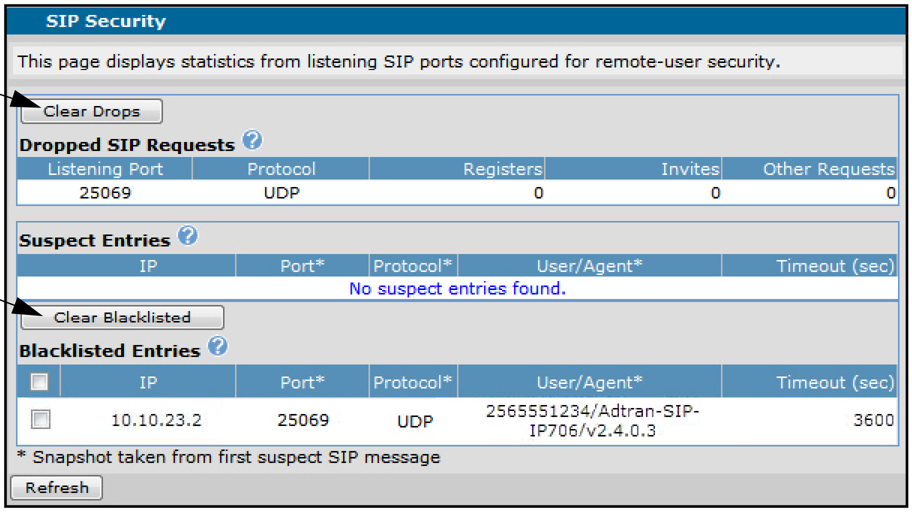
GUI Troubleshooting Tools

To view statistics from listening SIP ports configured for remote user security, navigate to **Voice** > **Reports** > **SIP Security**. From this GUI menu, you can view suspect and blacklisted entries, as well as clear entries from the tables.

This table displays source information from remote voice users that have failed to authenticate a SIP REGISTER and/or INVITE request. These entries have attempted to register or place a call and have exceeded the blacklist attack threshold. An entry remains blacklisted until the configured blacklist timeout expires or the entry is manually cleared. The system polls the blacklist every 60 seconds to check for IPv4 addresses that have cleared from the blacklist. Rebooting the system clears all entries from the blacklist.

Select to manually clear entries from the **Dropped SIP Requests** table.

Select to manually clear entries from the **Blacklisted Entries** table.



SIP Security

This page displays statistics from listening SIP ports configured for remote-user security.

Dropped SIP Requests

Listening Port	Protocol	Registers	Invites	Other Requests
25069	UDP	0	0	0

Suspect Entries

IP	Port*	Protocol*	User/Agent*	Timeout (sec)
No suspect entries found.				

Blacklisted Entries

□	IP	Port*	Protocol*	User/Agent*	Timeout (sec)
□	10.10.23.2	25069	UDP	2565551234/Adtran-SIP-IP706/v2.4.0.3	3600

* Snapshot taken from first suspect SIP message

Additional Resources

There are additional resources available to aid in configuring your ADTRAN unit. Many of the topics discussed in this guide, such as configuring HMR policies and IPv4 firewall, are complex and require thorough understanding. The documents listed below are available online at ADTRAN's Support Community at https://supportforums.adtran.com.

- *Configuring the Firewall IPv4 in AOS*
- *Configuring Media Anchoring in AOS*
- *Configuring User Accounts on the NetVanta 7000 Series*
- *Manipulating SIP Headers and Messages in AOS*
- *NetVanta 7000 Series Security Guide*
- *Security Best Practices for AOS Products*
- *Source and ANI Based Routing in AOS Voice Products*
- *Understanding the Firewall Menu in the AOS Web Interface*