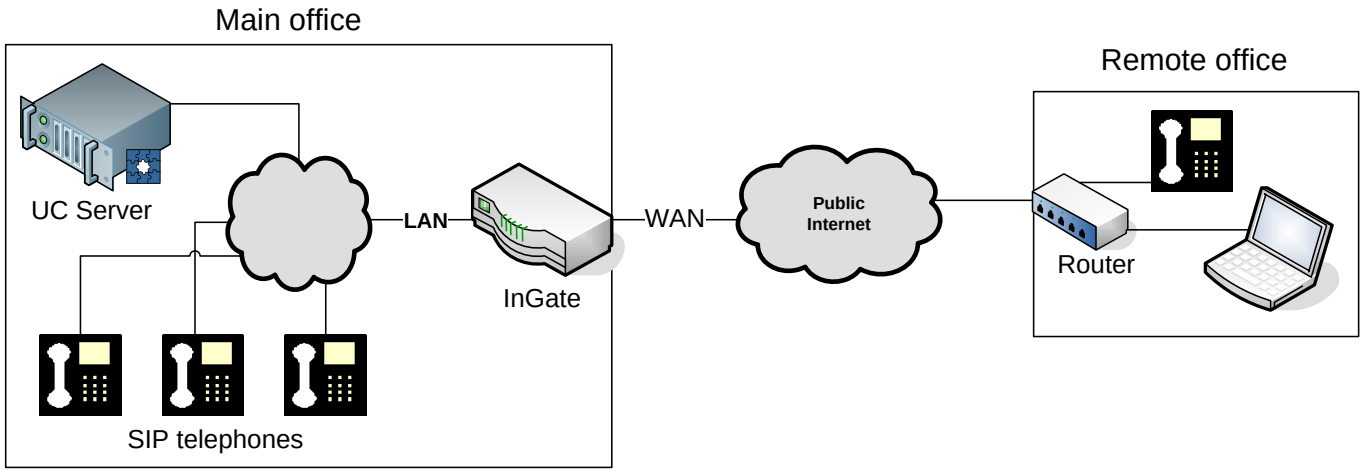
NetVanta Unified Communications Technical Note

Configuring NetVanta Unified Communications for Telecommuters

Overview

The diagram below depicts a typical telecommuter scenario in conjunction with the main office running the NetVanta Unified Communication Server.



SIP telephones operating at remote offices are configured to direct all outbound traffic through the Internet to the Ingate. The Ingate has two network interfaces: one that is connected to the private local area network (LAN) and one that is connected directly to the Internet. The Ingate performs network address translation (NAT) on incoming traffic from remote telephones and redirects it to the UC server, which then handles the calls as though the telephones resided inside the corporate network. Likewise, for outbound calls destined for telecommuter phones, the UC server directs Session Initiation Protocol (SIP) traffic to the Ingate, which performs NAT and redirects the call to the telecommuter telephone on the Internet. This technical note explains how to set up your environment to support this functionality.

NOTE: *An Ingate Remote SIP Connectivity Module license is required to support telecommuter telephones when the phones are behind a NAT.*

NOTE: *SIP telephone configuration instructions in this document pertain only to devices which can be auto-detected and configured and support automatic firmware deployment.*

Telephone Configuration

In order to configure the telephone to be used in a telecommuting environment, you must:

- Configure the telephone so it can place and receive telephone calls normally inside the corporate network.
- Assign the public wide area network (WAN) IP address of the Ingate to the telephone's outbound proxy parameter.

Configuring the Telephone with NetVanta UC Server

Telephones that are to be deployed as telecommuter telephones must first be provisioned locally (inside the corporate network):

1. Connect the telephone to the corporate network.
2. Wait for the telephone to appear as **Not configured** in the **Phones** pane in the UC client.
3. Assign an identity to the phone, such as **1100**.
4. Allow the telephone to reload/reboot.
5. Ensure that the telephone can place and receive calls.

Configuring the Outbound Proxy Parameter on SIP Telephones

After the telephones have been provisioned as per the instructions above in *Configuring the Telephone with NetVanta UC Server*, the phones must then have the outbound proxy parameter set to the public IP address of the Ingate. The Ingate has two network interfaces: one connected to the corporate network (LAN), and one connected to the public Internet (WAN).

To determine the public IP address of the Ingate:

1. Open a Web browser and enter the local IP address for the Ingate.
2. At the top, select **Network**.
3. Select **All Interfaces**.
4. The public IP address is listed under **Directly Connected Networks**. The public IP address will not match the subnet of your local IP addresses. Make a note of the IP address for the network connected directly to the Internet.
5. Close the browser.

You must use the telephone's Web interface to modify the outbound proxy parameter.

To access the Web interface:

1. Open the UC client as a user with administrative privileges.
2. Navigate to the **Phones** pane and locate the telephone provisioned as outlined above in *Configuring the Telephone with NetVanta UC Server*. Make a note of the telephone's IP address.
3. Open a Web browser, and enter the telephone's IP address in the address bar.

The following sections describe how to configure the outbound proxy parameter for several SIP telephones commonly used with the UC server.

Polycom SoundPoint IP Series, SoundStation IP series, and VVX 1500

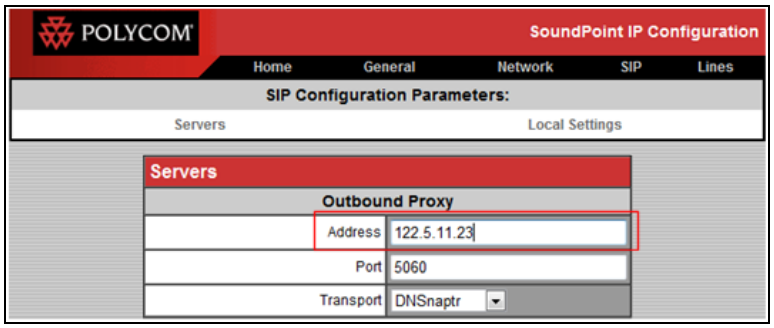
1. When prompted to enter a user name and password, enter the following:

   User: **Polycom**

   Password: **456**

   NOTE: *If you have changed your Polycom administrator password, enter the new password.*

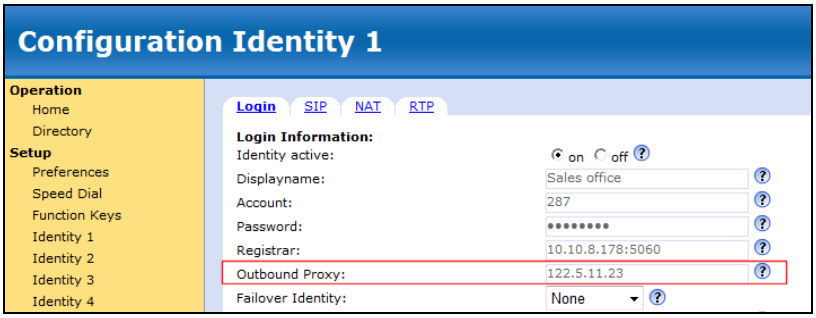
2. From the menu at the top, select **SIP**.
3. Under **Outbound Proxy**, enter the public IP address of the Ingate in the **Address** field.



4. Select **Submit**.
5. Allow the telephone to begin the reboot process. Once it begins the boot cycle you may disconnect the telephone and move it to the remote location.

Snom 300, 320, 360, 370, 820

1. From the menu on the left, select the identity that corresponds to the button number for which the identity was assigned using the UC client. For example, if you assigned Identity 287 to the first button on this Snom telephone, then select **Identity 1**.
2. Enter the public IP address of the Ingate in the **Outbound Proxy** field.



3. Select **Save**. You may now disconnect the telephone and move it to the remote location.

Aastra 9112i, 9133i, 480i, 480iCT, 6751i, 6753i, 6755i, 6757i

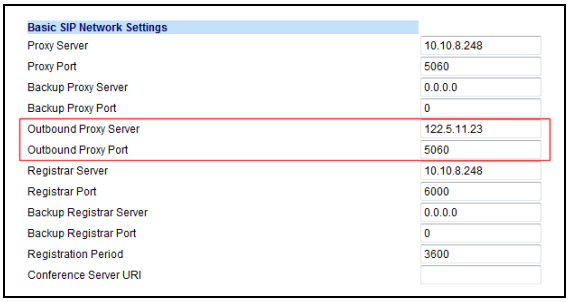
1. Enter the administrator user name and password. The default credentials are:

   User name: **admin**

   Password: **22222**

   NOTE: *If you changed your Aastra administrator password, enter the new password.*

2. From the menu on the left, select **Global SIP.**
3. Under **Basic SIP Network Settings**:
   - Enter the public IP address of the Ingate in the **Outbound Proxy Server** field.
   - Enter **5060** in the **Outbound Proxy Port** field.



4. At the bottom of the page, select **Save Settings.**
5. When prompted to reboot, select **Reboot**.
6. Allow the telephone to begin the reboot process. Once it begins the boot cycle you may disconnect the telephone and move it to the remote location.

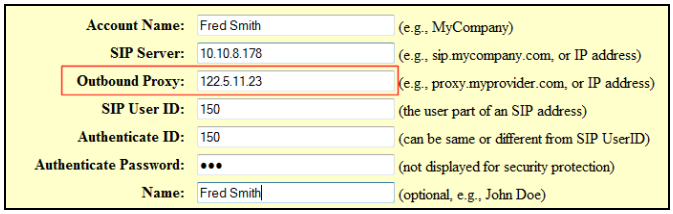
Grandstream Budgetone, GXP, and GXV series

1. Enter the administrator password for the Grandstream.

   Password: **admin**

   NOTE: *If you changed your Grandstream administrator password, enter the new password.*

2. From the menu at the top, select **Account**.
3. Enter the public IP address of the Ingate in the **Outbound Proxy** field.



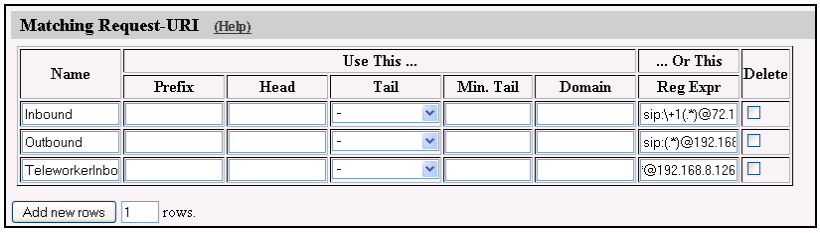
4. At the bottom of the page, select **Update.**
5. Allow the telephone to begin the reboot process. Immediately after it begins the boot cycle, disconnect it and move it to the remote location. If the telephone is allowed to boot up before being moved, the outbound proxy parameter will be overwritten.

Ingate Configuration

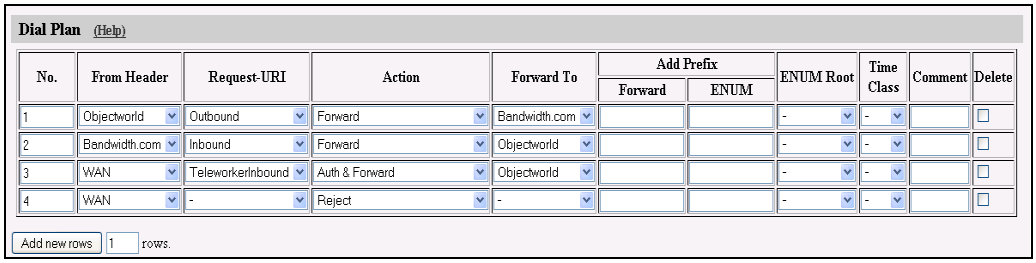
Two sections in the Ingate configuration must be modified in order to enable telecommuter support: the dial plan and the user database.

Modifying the Dial Plan

1. Open a Web browser and enter the local (LAN) IP address for the Ingate.
2. Go to **SIP Traffic** > **Dial Plan**.
3. Add an entry in the **Matching Request – URI** section:
   - Choose a descriptive name. In the figure below, **TeleworkerInbound** is used.
   - Under Reg Expr, enter the LAN IP address of the UC server using this format: **sip:.*@192.168.8.126**.



4. Add an entry in the **Dial Plan** section:
   - Choose a number for the **No.** field that is at least one less than the last **Reject** action. For example if the table has 3 entries, choose 3 for the new number.
   - Choose **WAN** from the **From Header** drop-down menu.
   - Choose the name created in the **Matching Request – URI** section from the **Request – URI** drop-down menu.
   - Choose **Auth & Forward** from the **Action** drop-down menu. This selection ensures that only registered entities are able to have outside calls routed to the UC server and may help prevent toll fraud.



5. Select **Save**, then **Apply** and **Save** the changes.

Modifying the User Database

The entries in the User Database must correspond to the identities assigned to the telecommuter SIP telephones. Before modifying the User Database, you must collect the SIP authentication name and password for each identity.

CAUTION: *To help avoid toll fraud, ensure that the SIP authentication password is complex enough not to be easily guessed.*

***NOTE**: If a SIP authentication name or password is changed in the UC server at any time, then the corresponding entry in the Ingate must also be changed. Failure to update Ingate with the updated SIP authentication information will cause the telecommuter telephones to stop working.*

Collecting SIP Authentication Names and Passwords

1. Open the UC client as a user with administrative privileges.
2. From the **Navigation** menu, select **Identities**
3. Select **View > Display Identities for all User Profiles**.
4. For each identity assigned to a telephone being deployed for a telecommuter:
   - Open the identity
   - Select **SIP Authentication** and make a note of the SIP Authentication name and password.

Modifying the Database

1. Go to **SIP Traffic** > **User Database.**
2. For **rows,** enter the number of identities that corresponds to the number of telecommuter phones being deployed.
3. Select **Add New Rows**.
4. For each identity assigned to a telephone being deployed for a telecommuter, enter the following:

   Username: < the identity assigned to the telecommuter telephone>

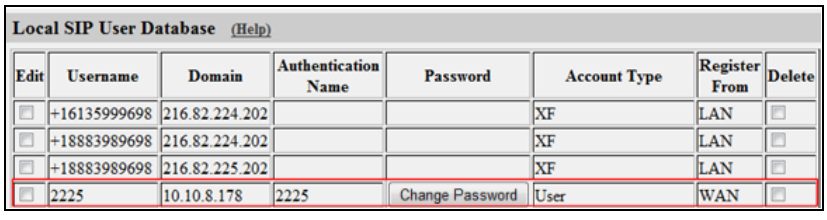
   Domain: < local IP address of the UC server>

   Authentication Name: < SIP authentication name collected in *Collecting SIP Authentication Names and Passwords*>

   Account Type: **User**

   Register From: **WAN**

   Password: Select **Change Password** and enter the password collected in *Collecting SIP Authentication Names and Passwords*.



Local SIP User Database (Help)

Edit	Username	Domain	Authentication Name	Password	Account Type	Register From	Delete
	+16135999698	216.82.224.202			XF	LAN	
	+18883989698	216.82.224.202			XF	LAN	
	+18883989698	216.82.225.202			XF	LAN	
	2225	10.10.8.178	2225	Change Password	User	WAN	

5. Select **Save,** then **Apply** and **Save** the changes.