

# Allworx<sup>®</sup> System Administration Guide



## Table of Contents

<b>1</b>	<b>Introduction</b> .....	<b>1</b>
1.1	Who Should Read This Guide.....	1
1.2	What this Guide Is and What It Is Not.....	1
1.3	Allworx Family of Servers.....	1
<b>2</b>	<b>Accessing Web Administration</b> .....	<b>2</b>
<b>3</b>	<b>Configuring a New Allworx Server</b> .....	<b>3</b>
<b>4</b>	<b>Upgrading Server Software</b> .....	<b>4</b>
4.1	Step 1: Copy Files to the Update Area.....	4
4.1.1	Alternative 1: Automatic Download from the Web.....	4
4.1.2	Alternative 2: Manually Installing Files Using FTP.....	5
4.2	Step 2: Activate the Update.....	5
<b>5</b>	<b>Network Configuration</b> .....	<b>6</b>
5.1	Network Mode: Standard Router.....	7
5.2	Network Mode: LAN Host.....	8
5.3	Network Mode: NAT/Firewall.....	9
5.4	Network Mode: NAT/Firewall with DMZ.....	11
5.5	Network Mode: NAT/Firewall with Stealth DMZ.....	12
5.6	Example 1: Secure Firewall.....	12
5.7	Example 2: Secure Firewall with 3 <sup>rd</sup> Party Email Server.....	13
<b>6</b>	<b>Adding Handsets</b> .....	<b>14</b>
6.1	SIP Phones.....	14
6.1.1	Plug-and-Play.....	14
6.1.2	Manual Add.....	14
6.2	Analog Phones.....	16
6.3	Testing Phones.....	16
<b>7</b>	<b>SIP Proxies and SIP Gateways</b> .....	<b>17</b>
7.1	Introduction.....	17
7.2	Configuration.....	17
7.2.1	Details about SIP Proxies.....	18
7.2.2	Details about SIP Gateways.....	20
7.3	Enterprise Dialing Feature.....	20
7.3.1	Allworx Enterprise Client.....	20
7.3.2	Central Hub / Enterprise Server.....	20
7.3.3	Steps on How to Setup Enterprise Dialing.....	21
<b>8</b>	<b>Remote Allworx Server Multi-Site Calling</b> .....	<b>22</b>
8.1	Introduction.....	22
8.2	Quality of Service Between Sites.....	22
8.3	Limiting Total Number of Calls Between Sites.....	22
8.4	Defining Remote Allworx Sites.....	22
<b>9</b>	<b>Configuring Allworx IP Phones</b> .....	<b>24</b>
9.1	Introduction.....	24
9.2	Why Multiple Call Appearances is Useful.....	24
9.3	View Configuration.....	25
9.4	Programmable Function Keys (PFK's).....	25
9.4.1	Busy Lamp Field (BLF) PFK Type.....	25
9.4.2	Call Appearance PFK Type.....	26
9.4.3	Call Monitor PFK Type.....	26
9.4.4	Function PFK Type.....	26
9.4.5	Line Appearance PFK Type.....	26

9.4.6	Not Used PFK Type .....	27
9.4.7	Parking Orbit PFK Type .....	27
9.4.8	Queue Appearance PFK Type .....	27
9.4.9	Speed Dial PFK Type.....	27
9.4.10	Configuration Example: Busy Receptionist.....	27
9.5	Call Assistant Appearances .....	27
9.6	Phone Options .....	28
9.6.1	Description of Specific Options .....	28
9.7	Configuration Templates .....	31
9.7.1	Default Templates .....	31
9.7.2	Viewing a Template's Configuration.....	31
9.7.3	Creating a New Template .....	31
9.7.4	Applying a Template to a Phone's Configuration .....	32
9.7.5	Deleting a New Template.....	32
9.7.6	Changing a Template's Configuration.....	32
<b>10</b>	<b>Digital Lines.....</b>	<b>33</b>
10.1	Introduction .....	33
10.1.1	PRI Support.....	33
10.1.2	Data Support.....	33
10.1.3	Restrictions .....	33
10.2	Configuration.....	34
10.2.1	Information on Specific Parameters .....	34
<b>11</b>	<b>Dialing Rules and Service Groups .....</b>	<b>37</b>
11.1	Background Information.....	37
11.1.1	Dialing Rules .....	37
11.1.2	Home Area Code .....	37
11.1.3	Service Groups .....	37
11.1.4	Exceptions.....	38
11.2	North American Numbering Plan Administration (NANPA).....	38
11.3	Defining Service Groups .....	39
11.4	Configuring Home Area Code And All Other Area Codes.....	39
11.5	Interaction Between Service Groups and Handset Outside Line Restrictions .....	40
<b>12</b>	<b>Unified Messaging .....</b>	<b>41</b>
12.1	Access Mechanisms .....	41
12.1.1	Forwarding Messages via Message Aliases .....	41
12.1.2	Common Mistake in Forwarding Messages .....	41
12.1.3	POP3 Client .....	41
12.2	Access Examples.....	42
12.2.1	Example 1 .....	42
12.2.2	Example 2 .....	42
12.2.3	Example 3 .....	43
12.2.4	Example 4 .....	43
<b>13</b>	<b>Backing up and Restoring Data.....</b>	<b>44</b>
13.1	How to Create a Backup .....	44
13.1.1	OfficeSafe Application on the PC .....	44
13.1.2	Configuring Backups on the Allworx Server .....	45
13.1.3	Additional Backup Options .....	46
13.2	How to Restore Data.....	46
13.3	Server to Server Backup and Restore .....	48
13.4	Exporting and Importing Backup Files .....	48

13.4.1	Export Backup Files .....	48
13.4.2	Import Backup Files .....	49
<b>14</b>	<b>Remote IP Phone .....</b>	<b>51</b>
14.1	General Network Configuration Requirements .....	51
14.2	Allworx Server Behind 3 <sup>rd</sup> Party NAT Firewall .....	51
14.3	Remote Allworx IP Phone .....	52
14.3.1	Configuration.....	52
14.3.2	Remote Phone Behind a Third Party Firewall .....	52
14.3.3	Limitations .....	53
14.4	Remote 3 <sup>rd</sup> Party IP Phones.....	55
<b>15</b>	<b>Call Routing.....</b>	<b>56</b>
15.1	Call Routing Concepts .....	56
15.1.1	Introduction .....	56
15.1.2	Connection Attempt.....	56
15.1.3	Finally Clause.....	56
15.1.4	Primary Route, On-Busy Route, and Call Route .....	56
15.1.5	CallerID Dependant Call Routes .....	57
15.1.6	Presence .....	57
15.1.7	User Extensions and System Extensions .....	57
15.1.8	Concept Summary .....	57
15.2	View and Change a Call Route .....	57
15.3	Changing a User's Presence Setting .....	59
15.3.1	Changing Presence Via an Allworx IP Phone .....	59
15.3.2	Changing Presence Via Any Phone .....	59
15.3.3	Changing Presence Via the User Intranet Web Site .....	59
15.3.4	Changing Presence Via the Administrative Web Page .....	59
15.4	Outside Line Call Routing .....	60
15.5	Example Call Route Configurations .....	60
15.5.1	Example 1: Ring 1 Phone, Then Voicemail.....	60
15.5.2	Example 2: Ring 1 <sup>st</sup> Phone, Then ring 2 <sup>nd</sup> Phone, Then Voicemail.....	61
15.5.3	Example 3: CO Line Rings 2 Phones, Then ring 3 <sup>rd</sup> Phone, Then Voicemail .....	61
<b>16</b>	<b>Key System Behavior .....</b>	<b>62</b>
16.1	Example Configuration.....	62
<b>17</b>	<b>Direct Inward Dialing (DID).....</b>	<b>63</b>
17.1	Create a DID Block .....	63
17.2	Configure a Call Routing Plan for the DID Block.....	63
17.3	Create the DID Lines .....	64
<b>18</b>	<b>Web, FTP, and CIFS .....</b>	<b>66</b>
18.1	Web Sites.....	66
18.1.1	Internal Administration Web Site .....	66
18.1.2	Internal System Info Web Site.....	66
18.1.3	Internal Custom System Web Site .....	66
18.1.4	Internal Custom User Web Site.....	66
18.1.5	External Custom Web Site .....	67
18.2	Internal FTP Site .....	67
18.3	External FTP Site .....	67
18.4	Internal CIFS File Server (Allworx 10x only) .....	67
<b>19</b>	<b>Auto Attendant .....</b>	<b>68</b>
19.1	Configuring the Auto Attendant.....	68
19.2	How to Assign the Auto Attendant to an Outside Line .....	70

19.3	How to Record the Auto Attendant Greetings .....	71
<b>20</b>	<b>Call Queues .....</b>	<b>73</b>
20.1	Configuring a Queue .....	73
20.1.1	Managing Custom Queue Message Content .....	74
20.2	Servicing a Queue with an Allworx IP Phone .....	74
20.2.1	Configuring the Phone .....	74
20.2.2	Agent Phone Configuration Example .....	75
20.2.3	Logging in and out of the Queue .....	76
20.3	Servicing a Queue with a Non-Allworx IP Phone .....	76
20.4	Configuring Calls To Route To the Queue .....	76
20.4.1	Example 1: Call Routing To Auto Attendant and Then Call Queue .....	77
20.4.2	Example 2: Call Routing Directly to Call Queue .....	77
20.4.3	Example 3: Call Routing To AA, Live Answer Option, and then Call Queue .....	77
<b>21</b>	<b>Call Monitors .....</b>	<b>78</b>
21.1	Difference between Call Monitors and Call Queues .....	78
21.2	Configuring a Call Monitor .....	78
21.2.1	Modify Call Monitor Description .....	78
21.2.2	Setup Call Monitor into Call Route .....	78
21.3	Call Monitor with an Allworx IP Phone .....	79
21.3.1	Configuring the Phone .....	79
21.4	Configuring Calls to Route to the Call Monitor .....	79
21.4.1	Example 1: Call Routing to Auto Attendant and then Call Monitor .....	80
21.4.2	Example 2: Call Routing to Call Monitor and then Transfer to a Call Queue .....	80
<b>22</b>	<b>Parking Orbits .....</b>	<b>81</b>
22.1	Configuring Parking Orbits for Allworx IP Phones .....	81
<b>23</b>	<b>Zoned Paging and Overhead Paging .....</b>	<b>83</b>
23.1	Paging Amplifier and Door Release Relay .....	83
23.2	Paging Zone Names .....	83
23.3	Paging Zone Operation on the Handsets .....	84
<b>24</b>	<b>Abbreviations .....</b>	<b>85</b>

## 1 Introduction

### 1.1 Who Should Read This Guide

This guide is to be read by people who will be installing and maintaining the Allworx server. The technical background of the administrator is assumed to be greater than that of the system's end users. This is not an end user document. The reader is expected to have a sufficient computer networking and basic telephony background.

### 1.2 What this Guide Is and What It Is Not

The Allworx server web administration interface is designed to be easy to navigate and use. It has built in descriptions, help, and tips on many of its pages. This manual is not a duplication of that information, but is to be used in concert with that. This manual is intended to describe only those features or administration mechanics that are more complex and difficult to understand. Therefore, not all the features or all the parameters of each feature are discussed here. Again, this guide discusses only those features and parameters that require additional explanation beyond what is on the web pages.

This manual is not a tutorial on basic computer networking or telephone systems. Other sources may need to be consulted to supply that information.

### 1.3 Allworx Family of Servers

The award-winning Allworx family of servers now includes the Allworx 6x, Allworx 10x, and Allworx 24x server products. The Allworx 6x is available in two configurations: one with a removable flash drive and another with an external USB 2.0 hard drive. The removable flash drive configuration is considered the standard base configuration. The three servers in the Allworx family differ in features and capabilities. This guide explains these differences. The table below depicts which Allworx server offers which capabilities.

	Allworx 6x Standard	Allworx 6x With USB Drive	Allworx 10x	Allworx 24x
Call Assistant PC Application Support	✓	✓	✓	✓
3-Way Conferencing with Analog Phones			✓	
N-Way Conferencing	1 Node	1 Node		4 Nodes
Door Relay Activation and Paging Amplifier Control	✓	✓		✓
FXO/FXS Support for G.729A	✓	✓		✓
Text to Speech			✓	
CIFS File Server			✓	
Allworx Communications Center (Group Calendaring)		✓	✓	✓
External Inbound Email Support		✓	✓	✓
Outbound Email Support	✓	✓	✓	✓
Total number of users supported	30 max	30 max	100 max	100 max

## 2 Accessing Web Administration

The administrative interface to the Allworx server is accessed using a web browser via the LAN interface of the product at TCP port 8080. Assuming the network settings are set to their factory defaults, the steps to connect to this interface are:

1. Plug your PC into the server's LAN port. On the Allworx 10x, which has four switched LAN ports, any port can be used.
2. Set up the PC's network interface to obtain an IP address automatically (using DHCP).
3. Verify that the PC has an IP address on the 192.168.2.x network. You may need to release and renew the PC's IP address to get an address from the server.
4. Open your browser and enter the URL of `http://192.168.2.254:8080`.
5. When the "Welcome to Allworx" page appears, login using the default password of "admin".

### 3 Configuring a New Allworx Server

Log into the Allworx server web administration page. When the **Home** page appears, click on the **Install Checklist** link (on the left hand side) to bring up a new window containing steps necessary to set up a new system. Each brief step description is followed by a link to get to the appropriate administrative web page to execute the step. These steps are ordered to aid in a successful configuration. Most of the web pages to execute each step contain all the descriptions and help necessary to carry out the step. Use this guide to supplement the information on the web pages when necessary.



## 4 Upgrading Server Software

The software on the Allworx server is upgradeable. Before performing an upgrade, be aware that:

- It is highly recommended that you perform an OfficeSafe backup prior to performing the upgrade (see *Backup and Restoring Data*).
- An upgrade will require a reboot of the server. So, the system should be idle (no phone or data users) when this is done, or a disconnection and/or disruption of data may occur.

To upgrade the software on the server, go to the **Maintenance / Update** web administration page. (In most cases the web administration pages can be viewed with various web browsers, but for this task it is recommended that you use the Microsoft Internet Explorer browser.) You will see a screen area like this:

**Update**

**Current version:** 6.2.0.8  
**Build Date:** Aug 28 2006, 19:56:06

Two steps are required for installing an Allworx software update:

**1) Copy Files To Update Area**

The files for the software update must first be copied to the Allworx. To copy files, you may [download from the web](#), or you may use an FTP program to transfer files from an Allworx Software Release CD. Use the FTP program to connect to **192.168.7.254** (any username/password, then cd to 'update' and use binary transfer mode). The FTP program must be running on a PC connected to the Allworx LAN.

**TIP**  
Copying files from the web may take several minutes depending on the speed of your network connection. Before downloading from the web, you may wish to [check the web](#) now to see if a new software version is available.

**2) Activate the Update**

After the files have been copied to the update area, they must be activated. Click on the "Activate Update" button to perform this step.

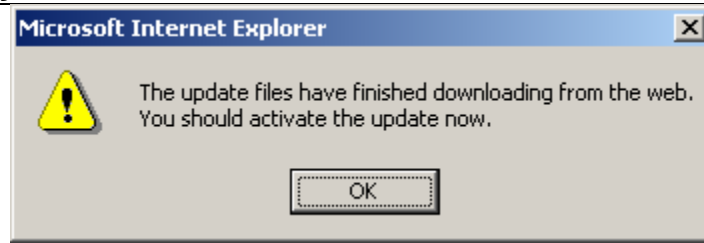
As you can see, there are two steps involved: copying the files to the update area and activating the update.

### 4.1 Step 1: Copy Files to the Update Area

The copy step allows two alternatives: letting the sever download the software update files from the web or manually copying update files that you already have to an FTP window. Let's look at each of these alternatives in more detail.

#### 4.1.1 Alternative 1: Automatic Download from the Web

When you click on the **download from the web** link, the server makes a connection to a web site on the Internet that has the software and begins to download it to the server. Of course, if your server cannot get to the Internet, this will fail. So, make sure that your Internet connectivity is working. Depending on the performance of your Internet connection, this will take awhile (as of this writing, the download is about 32M bytes). After the download is complete, the web browser will pop up a window like this:



You must continue with the Activate step to complete the software update.

If you do not get this dialog, do not activate the update. You should reboot the server and use alternative 2 described in the next section.

If this step doesn't seem to work, check the **Reports / System Events** page for any error information.

If the download took a long time to complete, your browser's connection to the server web administration may time out. If this happens, you will be asked to login again.

## 4.1.2 Alternative 2: Manually Installing Files Using FTP

Instead of having the server download the software update files from the web, you may already have the files on a CD or your PC's hard drive. Ensure that you have these following files that constitute a complete release:

Product/File	Allworx 6x	Allworx 10x	Allworx 24x
Upgrade.dat	x	x	x
Oisapp	x	x	x
InstallFiles.arc	x	x	x
InstallFiles.ini	x	x	x
NewFlash.sre	x	x	x
Oisapp.sym		x	

Now you need to transfer them to the server. To do this, click on the **FTP window** link or enter the following URL into your browser:

- **ftp://192.168.2.254/update** (assuming factory default settings)

Using Windows Explorer, copy or drag the files from your PC (CD or hard drive) to the FTP window. This will cause the files to be transferred to the server.

After all the files have been copied, continue with the Activate step to complete the software update.

### Note


If you have problems FTP'ing files using a browser, it is acceptable to FTP files to the server via a command line tool such as Microsoft's FTP client available from a Command Prompt window.

## 4.2 Step 2: Activate the Update

Once you have copied the software update files to the server, you are ready to update the server's software. Click the **Activate Update** button. This will cause the server to internally validate and install the files and then reboot. The web administration will guide you as you wait for the update to be performed.

## 5 Network Configuration

The Allworx server provides powerful and flexible network infrastructure capability. Much of this flexibility is configured by setting the **Network Mode** parameter on the **Network / Configuration** page. This page shows different parameter sets depending on the **Network Mode** setting. If the **Network Mode** is set to the factory default value of NAT/Firewall with DMZ, the page will be similar to the one shown below.


Home > Network > Configuration

About

Phone System

Business

**Network**

Configuration

Static Routes

VPN

Servers

Reports

Maintenance

Need help?

Install Checklist

[Logout]

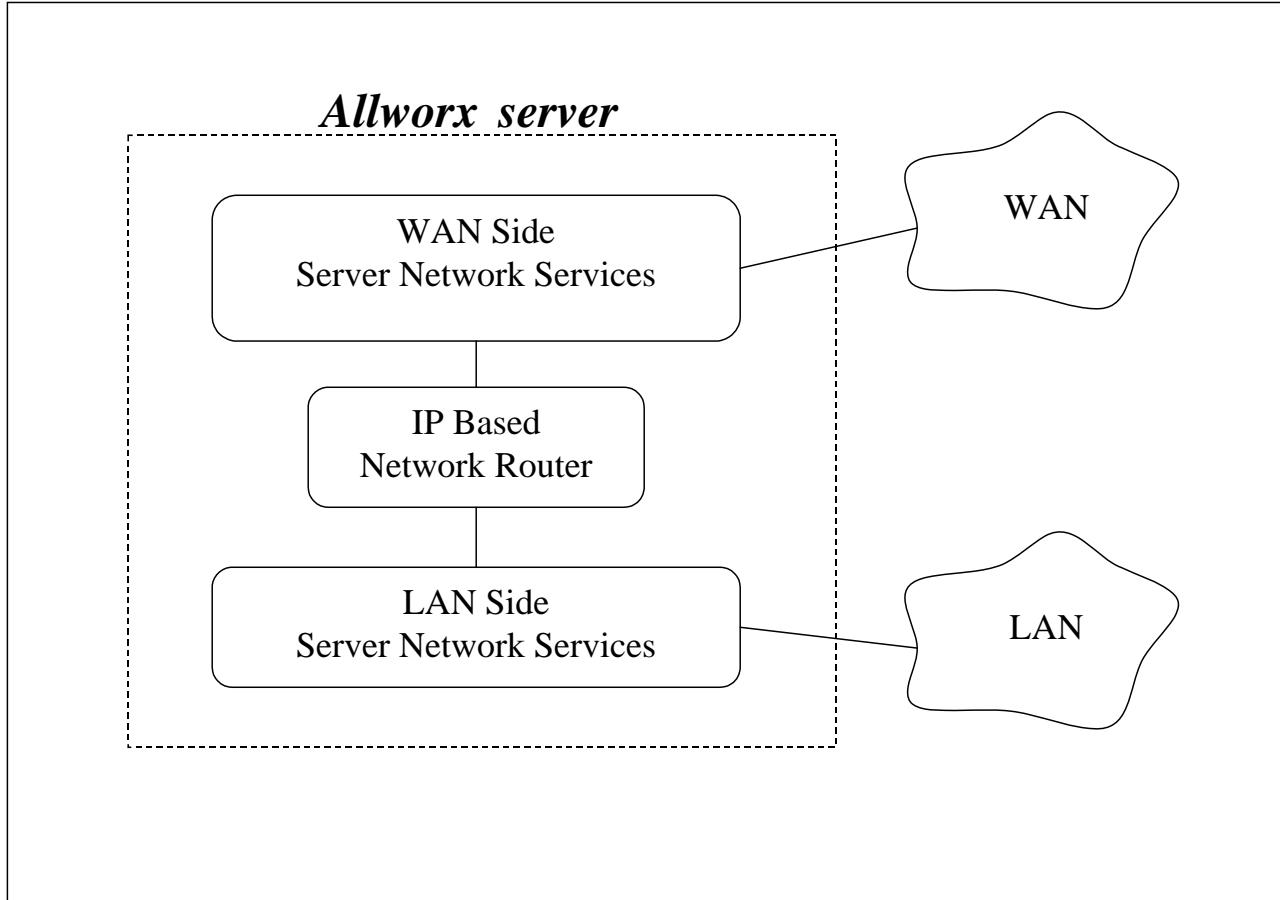
### Configuration

	Current Value	Action
Network Mode	NAT/Firewall with DMZ	
LAN IP Address	192.168.2.254	
LAN Subnet Mask	255.255.255.0	
WAN Settings Method	Static	
WAN IP Address	192.168.1.1	
WAN IP Subnet Mask	255.255.255.0	
Gateway	192.168.1.254	<a href="#">Modify</a>
PPPoE Username		
PPPoE Service Name		
PPPoE MTU	1492	
<b>LAN Addresses and Ports exposed through Firewall</b>		
DNS Server (53)	enabled	
DNS Client (4069)	enabled	
FTP (20,21)	disabled	
HTTP (80)	enabled	
POP3 (110)	enabled	
Communications Center (1112,2112,2113)	disabled	
PPTP (1723)	enabled	
Remote Allworx Handsets (2088,8081)	enabled	
SIP (5060)	enabled	
SMTP (25)	enabled	
SNTP Client (4068)	enabled	
Host Name	allworx	
Domain Name (DNS)	allworx.inscitek.com	

Each of the possible network mode parameter values is described below.

## 5.1 Network Mode: Standard Router

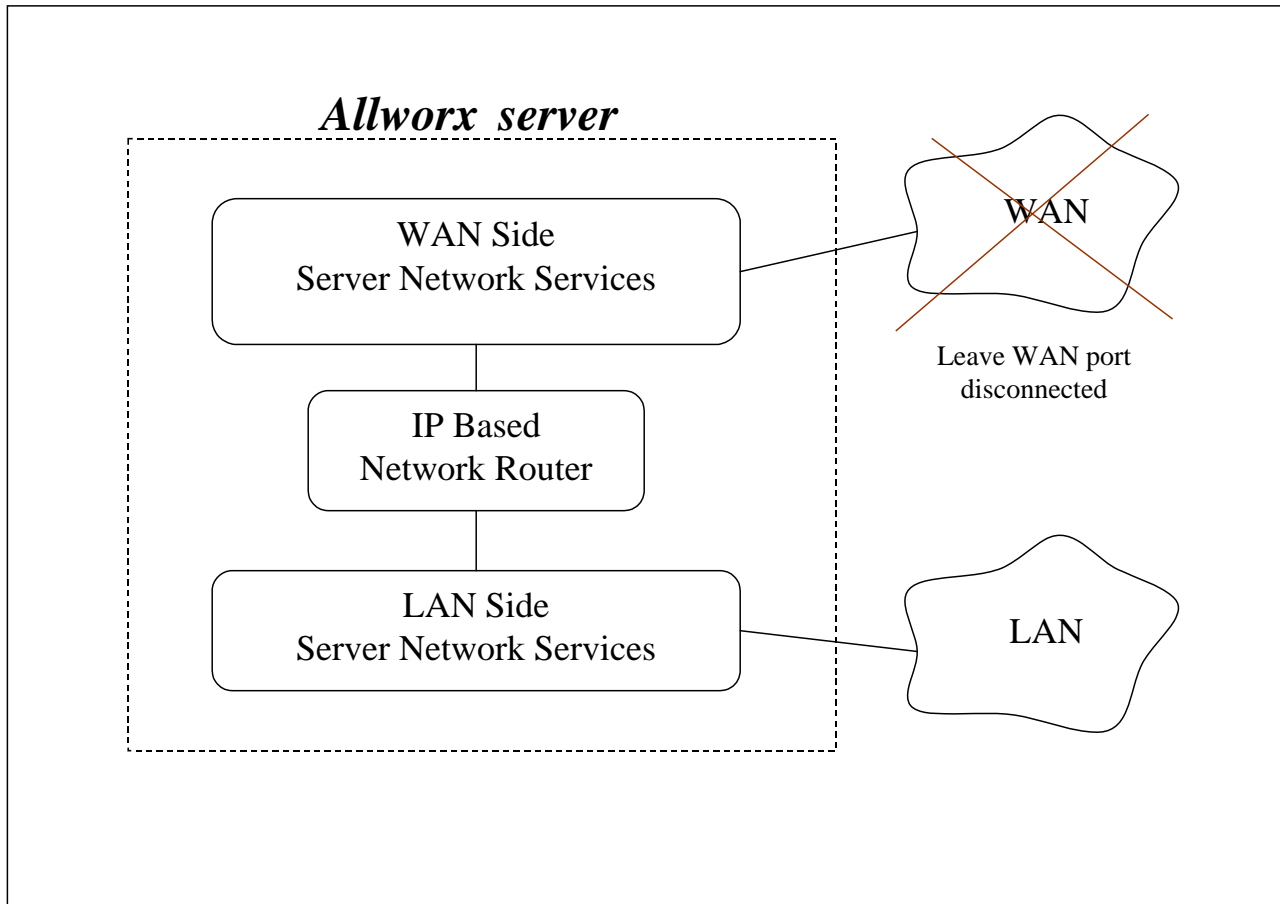
When the network mode is set to Standard Router, the logical network capability is as shown in the diagram below:



The server acts like an ordinary two port router with the server routing packets between the LAN and WAN interfaces. No NAT or firewall functionality is enabled. All LAN hosts are “visible” on the WAN. If the DHCP server is enabled (see the **Servers / DHCP Server** page), then the DHCP server will send its LAN IP address as the DHCP router (gateway) option so that LAN clients will know to use the Allworx server as the router to the WAN. WAN hosts wanting to connect to LAN hosts will need to be configured with a network route using the Allworx server’s WAN address as a gateway to the LAN.

## 5.2 Network Mode: LAN Host

When the network mode is set to LAN Host, the logical network capability is as shown in the diagram below:



This mode is designed to be used when the Allworx server is deployed as a peer (instead of as a router or firewall) on the local area network.

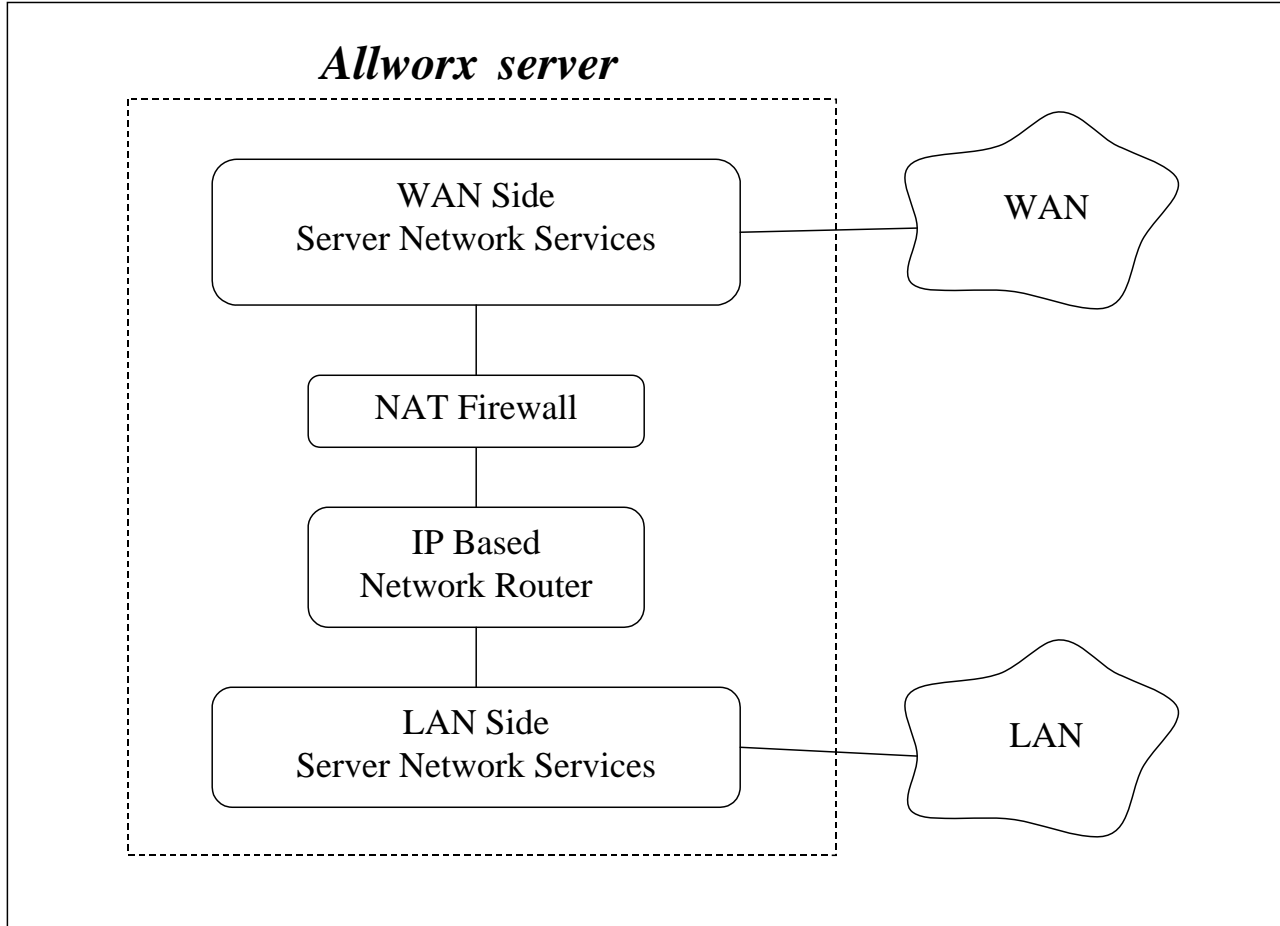
This mode is the same as Standard Router except that when the DHCP server is enabled, it will pass out the configured **Gateway** address (set on the **Network / Configuration / Modify** page) as the DHCP router (gateway) option instead of giving out the Allworx server's LAN address.

When in this mode, it is recommended that the WAN network port not be connected (i.e. no network cable should be plugged in). Even though no network is plugged in, a WAN IP address and subnet mask must be assigned. A subnet number that is distinct from the LAN subnet number must be used when assigning the WAN IP address. Furthermore, a completely unused subnet number should be used to avoid any routing conflicts.

The WAN services (like FTP and HTTP) are still available via the LAN if the proper routes are configured on your network.

### 5.3 Network Mode: NAT/Firewall

When the network mode is set to NAT/Firewall, the logical network capability is as shown in the diagram below:



This mode's default setting permits only outbound connections from the LAN to the WAN; all WAN initiated connections are denied. In addition, all packets are subject to network address translation (NAT) such that no LAN addresses are "visible" on the WAN, yet have access to the WAN. These features reduce the ability of WAN hosts to attack LAN hosts.

WAN access to specific LAN network services can be allowed by exposing those specific LAN ports through the firewall. This configuration is made in the **Firewall** section of the **Network / Configuration / Modify** page.

**Firewall**

LAN Addresses exposed through firewall:

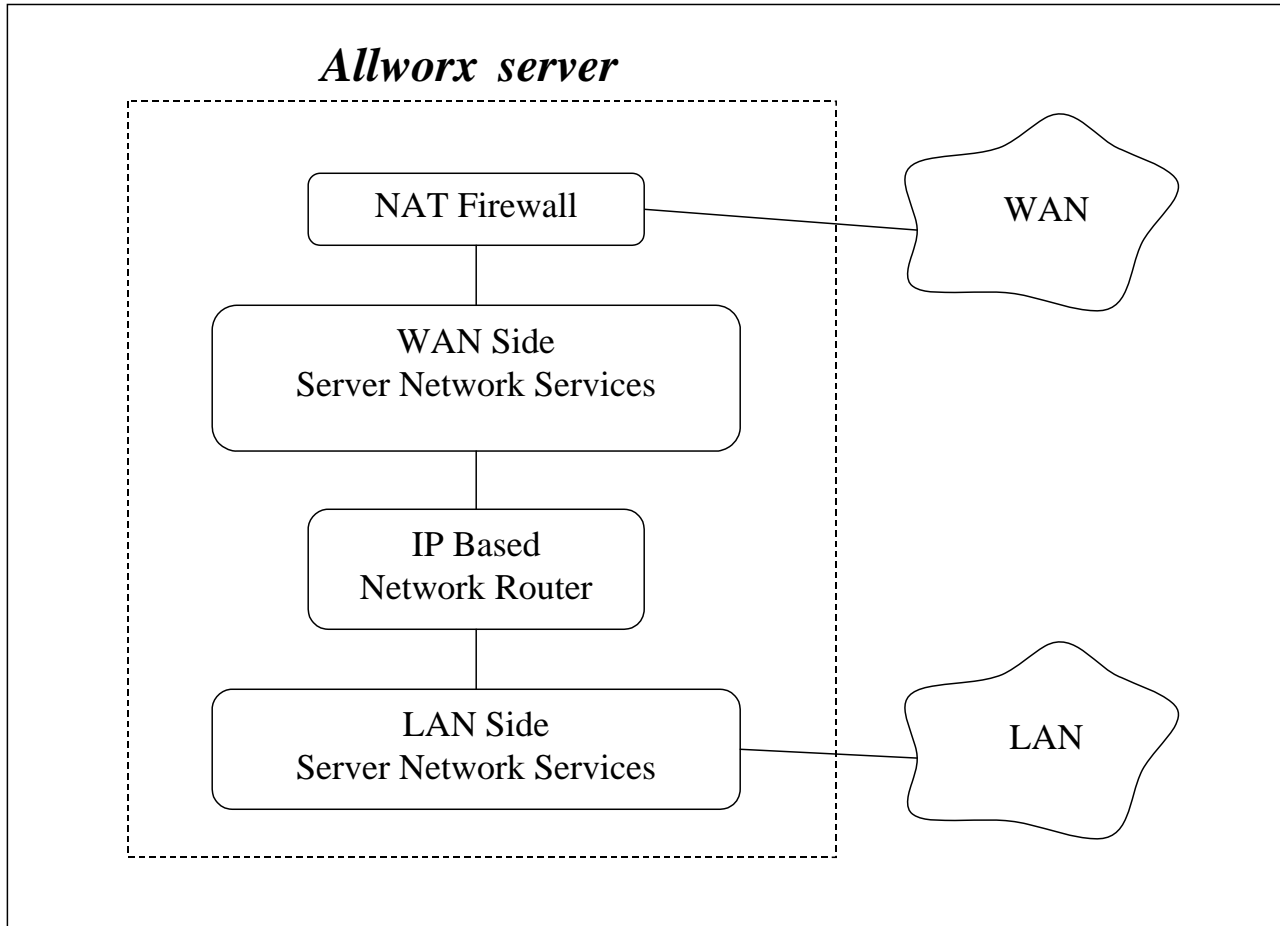
WAN Port #	Protocol	IP Address	Local Port #
<input type="text"/>	TCP ▾	<input type="text"/>	<input type="text"/>
<input type="text"/>	TCP ▾	<input type="text"/>	<input type="text"/>
<input type="text"/>	TCP ▾	<input type="text"/>	<input type="text"/>
<input type="text"/>	TCP ▾	<input type="text"/>	<input type="text"/>
<input type="text"/>	TCP ▾	<input type="text"/>	<input type="text"/>
<input type="text"/>	TCP ▾	<input type="text"/>	<input type="text"/>
<input type="text"/>	TCP ▾	<input type="text"/>	<input type="text"/>
<input type="text"/>	TCP ▾	<input type="text"/>	<input type="text"/>
<input type="text"/>	TCP ▾	<input type="text"/>	<input type="text"/>
<input type="text"/>	TCP ▾	<input type="text"/>	<input type="text"/>
<input type="text"/>	TCP ▾	<input type="text"/>	<input type="text"/>

For example, a web server at port 80 is on a PC at 192.168.101.9. This is on the LAN. To permit access to this web server from the WAN at port 5000, create a new entry in the above table where the **WAN Port #** is 5000, the **Protocol** is TCP, the **IP Address** is 192.168.101.9, and the **Local Port #** is 80.

Due to security requirements, the Allworx server's LAN IP address is not permitted as an **IP Address** in the table above. The server's VPN feature can be used to access Allworx LAN network services from the WAN.

## 5.4 Network Mode: NAT/Firewall with DMZ

When the network mode is set to NAT/Firewall with DMZ, the logical network capability is as shown in the diagram below:



Turning on the DMZ moves the WAN network services behind the firewall. This means that even the Allworx WAN services (POP, SMTP, FTP, HTTP, etc.) are not available by hosts on the WAN. Making some of these services available can be done in the **Firewall** section of the **Network / Configuration / Modify** page.



**Firewall**

**LAN Addresses exposed through firewall:**

WAN Port #	Protocol	IP Address	Local Port #
<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>

**Allworx Services (ports) exposed through DMZ:**

- DNS Server (53)
- DNS Client (4069)
- FTP (20,21)
- HTTP (80)
- POP3 (110)
- PPTP (1723)
- Communications Center (1112,2112,2113)
- Remote Allworx Handsets (2088,8081)
- SIP (5060)
- SMTP (25)
- SNTP Client (4068)

Notice the checkboxes for specific Allworx services. They are convenience shortcuts to filling in the form above them.

## 5.5 Network Mode: NAT/Firewall with Stealth DMZ

This mode is the same as NAT/Firewall with DMZ except that all ICMP services (echo, redirect, etc) are turned off. This makes it more difficult for attacks from the WAN to probe the server. It also makes it more difficult for the administrator to troubleshoot any network connectivity problems (since ping and traceroute won't work).

## 5.6 Example 1: Secure Firewall

Requirements:

The Allworx server will be used as the router between a LAN and the Internet. Protecting the LAN from the Internet is a requirement. The server will be used as the local email server with email being sent to it from the WAN and LAN. The server will be the LAN timeserver. All other WAN services will be denied.

Configuration:

1. Set the **Network Mode** to NAT/Firewall with Stealth DMZ. Setting it to stealth mode will reduce the ability of Internet attacks to recognize the existence of the Allworx server and its offered services.
2. In the Firewall section of the **Network / Configuration / Modify** page, change the Allworx Services (ports) exposed through DMZ so that only SMTP, DNS, and SNTP are checked. SMTP is required to receive email from the Internet for local users. DNS is required so the email server can resolve

outbound mail addresses. SMTP is required to get accurate time from an Internet time server (configured on the Maintenance / Time page).

## **5.7 Example 2: Secure Firewall with 3<sup>rd</sup> Party Email Server**

### Requirements:

The requirements are identical to *Example 1* except that instead of using the Allworx server as the email server, another host (at 192.168.101.12) on the LAN will be used as the email server.

### Configuration:

The configuration is identical to the previous example except for the following changes:

1. Uncheck the SMTP service from the list of exposed Allworx services.
2. In the Firewall section of the Network / Configuration / Modify page, add an entry to LAN Addresses exposed through firewall where:
  - WAN Port # is 25.
  - Protocol is TCP.
  - IP Address is set to the LAN email server, 192.168.101.12
  - Local Port # is 25.

## 6 Adding Handsets

### 6.1 SIP Phones

#### 6.1.1 Plug-and-Play

Some SIP phones are plug-and-play, which means that they will automatically register with the server when they boot up on the network. The following phones are capable of this:

- Allworx IP phones including the 9102 and 9112
- Cisco models 7905 and 7912 running SIP software versions 1.01 or greater
- Cisco models 7940 and 7960 running SIP software versions POS3-06-3-00 or greater

The means of configuring these phones varies depending on the DHCP configuration on their LAN:

1. If the phone is getting its IP address from the Allworx server's DHCP server, the phone needs no manual configuration.
2. If the phone is getting its IP address from a non-Allworx server's DHCP server and the DHCP server sends the phone the Allworx server's IP address as the TFTP boot server (option #66), the phone needs no manual configuration.
3. If the phone is getting its IP address from a non-Allworx server's DHCP server and the DHCP server doesn't send option #66 to the phone, then the Allworx server's IP address needs to be manually set on the phone as its boot server. See the Allworx IP Phone User's Guide for more information.
4. If the DHCP server is sending the wrong (or no) option #66 IP address:
  - For Allworx IP phones, the manual setting on the phone will override the value sent by the DHCP server.
  - For Cisco phones, the alternate TFTP server should be set on the phone to override the value sent by the DHCP server.
5. If there is no DHCP server, then the phone needs to be manually configured with a static IP address, a netmask, a gateway and an Allworx server's IP address as its boot server.

*TIP: If you are having trouble getting a phone configured, restore it to factory defaults and reapply the desired settings.*

When an Allworx IP phone is booted on the network, the Allworx server will automatically prompt you to upgrade its software when it has a newer version available.

When a plug-and-play phone is registered with the server, it will appear on the **Phone System / Handsets** page in the **SIP Handsets** section. It will show the correct model and the MAC address will be displayed in the **Identification** column.

*TIP: Note that a Cisco 7960 will be recognized as a 7940 and will have to be changed to 7960 via the **Phone System / Handsets** page by clicking on the **Modify** link next to the phone entry.*

#### 6.1.2 Manual Add

The Allworx server supports the manual adding of SIP phones to the system. This may be done when the SIP phone to be added is not a plug-and-play phone or you want to configure the phone without actually plugging it into the network (For example, to pre-configure the server before an installation at the customer site).

To manually add a SIP phone, click on the **New SIP Handset** link in the **SIP Handsets** section of the **Phone System / Handsets** page.

### SIP Handset

Owner	{none}	▼
Extension	---	▼ (optional, see TIP)
Caller ID Number	user owner's extension	▼
Caller ID Name	<input type="text"/>	
Description	<input type="text"/>	

**TIP**

If an *Owner* other than 'admin' is selected the handset will automatically be added to the owner's *In Office* call route.

If an *Extension* is selected, the extension will be created with a call route to ring this handset. This is typically used in the case of a conference room or lab phone that does not require an owner.

---

### Handset Configuration

Model	Allworx 9112	▼
Login ID	<input type="text"/>	
Password	<input type="text"/>	
<input checked="" type="checkbox"/>	Phone will download configuration file from Allworx	
MAC Address	<input type="text"/>	
SIP Protocol Port	5060	<input type="text"/>

Select the phone model and fill in the required fields.

#### 6.1.2.1 Plug-and-Play Phones

If the phone is one of the supported plug-and-play types, then follow these steps:

1. Change the **Model** to the appropriate selection for the phone that is to be configured.
2. Enter a **Login ID** and **Password** for the phone to use to authenticate with the server. Note that the Login ID must be unique; cannot use the same Login ID on multiple phones.
3. Enter the correct MAC Address for the phone. Note if this is not correct, then when the phone is booted on the network, the server will have a duplicate entry for this phone because it will plug-and-play register itself with the system using the correct MAC address.
4. Enter the other parameters as necessary.
5. Click the **Add** button to add the new handset to server.

#### 6.1.2.2 Other/Generic Phones

If the phone is not an Allworx IP phone or one of the recognized Cisco phone types, then follow these steps:

1. Change the **Model** to Generic SIP.
2. Enter a Login ID and Password for the phone to use to authenticate with the server. Note that the Login ID must be unique; cannot use the same Login ID on multiple phones.
3. Click the **Add** button to add the new handset to server.
4. Configure the phone (following its particular configuration instructions) with the **User ID** (shown on the updated **Phone System / Handsets** page), **Login ID**, and **Password**.

When the phone is registered with the server, its entry on the **Handsets** page will indicate that by showing an expiration date and time.

## **6.2 Analog Phones**

Plug the phone into one of the server's FXS phone ports reserved for Inside Phone Extensions. It is a good idea to plug the first phone into the highest numbered port, and then working backwards towards the lowest numbered FXS port. Lift the phone receiver so that the phone is "off hook." Click the **Scan For New Handsets** link on the **Phone System / Handsets** page in the **Analog Handsets** section. Your phone will now appear in the **Analog Handsets** section of the page. Hang up the phone receiver.

## **6.3 Testing Phones**

Below are some suggested steps for verifying that a phone is set up correctly:

1. Dial 400 for auto attendant.
2. Enter '#7'. The auto attendant will play back information about the phone configuration.
3. Hang up. The phone will ring back.

If any of these steps fail, check:

- Physical wiring between phone and server
- Network settings
- Phone and server configuration

## 7 SIP Proxies and SIP Gateways

Note that this is an optional feature that requires a feature key. The necessary key is referred to as the *Internet Call Access Feature Key*.

### 7.1 Introduction

The Allworx server products support connectivity to external SIP compliant devices such as SIP proxy servers and SIP gateways. The Allworx products make an administrative distinction between four specific classes of SIP devices based on their typical functional use scenarios and how they interact with the Allworx system:

- **SIP Proxy** – An external SIP server that typically requires registration/authentication and is logically treated as an external service for routing calls. For example, when you desire to place calls through an Internet Telephony Service Provider (ITSP), you need to define a new SIP proxy to communicate with that external service. Typically, you reach SIP proxies through the Internet or through wide area network (WAN). A key distinction of a **SIP Proxy** in Allworx terms is that it is a device or server that the Allworx server will *register* with.
- **SIP Gateway** – Allworx defines a SIP Gateway to be a SIP compatible device that extends the connectivity of the Allworx PBX. For example, you might configure a SIP gateway to attach a FXO, FXS or T1 expander gateway. Typically SIP gateways are local devices that you implicitly trust and have them connected via an Ethernet interface directly to the same LAN that the Allworx server is connected to. SIP Gateways are expected to *register* with the Allworx server.
- **SIP Handsets** – A SIP compatible handset (telephone) that registers with the Allworx server. Attachment and configuration of SIP handsets is discussed in another section and does not require the advanced optional feature key needed for accessing SIP Gateways and Proxies. See **Adding Handsets** section for information about connecting to Allworx IP phones or other 3<sup>rd</sup> party SIP handsets.
- **Remote Allworx** – A remote peer system that is another Allworx system. The remote system does not have to be the same model as the local Allworx system, but typically they should be running the same version of software, if possible.

SIP Gateways and SIP proxies are distinctly defined, but are configured in a very similar manner. Both types of devices are added to the system through the **Phone System / Outside Lines** page.

### 7.2 Configuration

Configuration of SIP Proxies and Gateways is very straight forward, although there are several possible customization parameters to help deal with different types of devices that may either not be fully compliant with the SIP standards or comply with an older version of the standard.

For example, to define a new SIP Proxy connection on the Allworx server so it can access an Internet Telephony Service Provider (ITSP) to provide support for dialing and receiving outside calls you need to go to the **Phone System / Outside Lines** page. In the **SIP Proxies** section, you will see a list of all the SIP Proxies you have already configured. To configure a new SIP Proxy, click the **Add a New SIP Proxy** link that will present a page of many parameters that need to be defined for the ITSP service.

The technique for creating a new gateway is very similar to the Proxy method except that you consult the **SIP Gateways** section of the **Phone System / Outside Lines** page and use the **Add New SIP Gateway** to define a new gateway. Once either a SIP Proxy or a SIP Gateway is defined on the **Outside Lines** page, you can use their respective **Modify** link to make adjustments to their configurations. One particular thing to note about the **Modify** page is that it actually presents the opportunity to make adjustments to parameter choices

that are not presented on the creation page. These additional parameters in the **Advanced Settings** section should only have to be adjusted if the associated device or service is not fully compliant in some way with the current edition of the SIP standards.

## **7.2.1 Details about SIP Proxies**

Here is some additional information on particular parameters for SIP proxies.

**Description:** This field is the friendly name of the SIP Proxy and can be any text useful to the System Administrator. For example, you may want to enter the name of the ITSP this proxy relates to.

**User ID:** The ITSP or the Administrator of the SIP proxy service you are connecting to typically assigns this value. This ID is usually a phone number.

**SIP Server:** This is the DNS name or IP address of the proxy service you are connecting to. This is obtained from the ITSP. A port number can be selected here which is almost always 5060, but it should be verified with the service provider (ITSP).

**Outbound Proxy:** This is the DNS name or IP address of the outbound redirect server if different than the above SIP server. In many cases this is not required, but some service providers differentiate between inbound and outbound calls.

**SIP Registration Required:** If your SIP proxy server requires a SIP registration, check the box indicating this and fill in the Login ID and Password assigned by the ITSP. If the ITSP uses a registrar server that is different than the SIP proxy server, enter the DNS name or IP address of this server in the **Registrar** name field.

**Caller ID Name:** The assigned Caller ID passed outbound when calls are placed towards the SIP proxy. Some ITSP's may ignore this or refuse calls if set.

**Caller ID Number:** The assigned Caller ID Number passed outbound when calls are placed towards the SIP proxy. Some ITSP's may ignore this or refuse calls if set.

**Maximum Active Calls:** The Allworx server will use this number to limit the total number of the incoming and outgoing active calls with this SIP Proxy. This is useful for controlling the network bandwidth used, since it is assumed by Allworx that the SIP proxy is not a LAN local service.

**Number of Line Appearances:** This field defines the number of Line Appearances you would like defined for this Proxy so that Allworx will create a virtual set of phone lines that mimic real physical analog phone lines on this service. This is a feature unique to Allworx and allows ITSP services to be used in a conventional key system manner. Typically this number matches the maximum number of active calls limit set above, but it can be less. Note: Set a value of zero if Line Appearance functionality is not required.

**Send Digits as Dialed:** Specifies that outbound numbers should always be sent exactly as dialed on the handset placing the call. In most cases, you want the number converted into NANPA dialing form, so this box is not typically checked. However, in some cases, the service provider or proxy may be doing the conversion automatically so you may want to defeat the Allworx server's conversion mechanism.

**Digits Sent:** This is the number of dialed DTMF digits to be sent to the ITSP when making a call. If the number specified is less than the number dialed, the trailing digits are the ones sent. The default value is typical.

**Proxy is an Enterprise Server:** This is an advanced feature that allows interfacing to external SIP proxy services that actually have dial plan knowledge of your local site, but in most cases this feature is not used. See the **Enterprise Dialing Feature** section later in this chapter for more information.

**Default Auto Attendant:** Select the auto-attendant that should be used when inbound calls from this Proxy are routed to an Auto Attendant.

**Call Routing:** This selection determines how calls received from this proxy are routed inbound to the Allworx server. This is identical to the manner how all outside lines are configured including analog phone lines and digital lines.

## 7.2.1.1 Advanced Settings

The specifics of what values to enter for each of the Advanced Settings parameters vary with different ITSP's. Consult with your ITSP for this information.

**DTMF Payload:** This value is used as the "assumed" DTMF payload for inbound calls that do not include the RFC 2833 DTMF negotiation. Typically this is set to 96 or 101.

**Pad DTMF RTP Packets:** DTMF RTP packets are typically smaller than 64 bytes. Some switches and routers will discard any UDP packets shorter than 64 bytes. When this box is checked the Allworx will pad the DTMF packet by expanding the RTP header to make the packet at least 64 bytes long. Typically this checkbox is not checked.

**Enable Early Media:** Some service providers send audio before an outbound call has been answered (using 183 Session Progress in SIP). This can be used to relay announcements (e.g. "Your call can not be completed as dialed) or remote ring back tones. When this checkbox is checked, the Allworx will present the audio to the caller when received. When this checkbox is not checked, the Allworx will ignore the early audio and generate a ring back tone internally. Typically this checkbox is checked.

**Supports Symmetric Response Routing:** Some service providers assist the remote end in NAT traversal by supporting RFC 3581 "Symmetric Response Routing". When this checkbox is checked, a remote handset behind a NAT firewall will assume the service provider can correctly detect the audio port to send traffic to. When this checkbox is not checked, the handset needs to be port-forwarded through the NAT firewall, or must use the Allworx for proxying of audio traffic (see **Servers / VoIP Server**). Typically this checkbox is not checked.

**Supports SIP REFER:** This selects the method of transferring calls between multiple remote end-points through the service provider. When this checkbox is checked, SIP REFER is sent to the service provider to allow them to connect the two end-points within their network without intervention by the Allworx. When this checkbox is not checked, the Allworx will act as a proxy between the two remote ends of the calls. Typically this checkbox is checked.

**Supports SIP Redirect:** This selects the method of redirecting inbound calls that are forwarded back to the service provider without being answered (e.g. all calls are forwarded to a cell phone). If this checkbox is checked, a SIP 300 redirect message is sent. If this checkbox is not checked, the Allworx will negotiate the call setup for the service provider. Typically this checkbox is not checked.

**Obtain DID number from [source]:** This defines the SIP header to extract the DID number from for inbound calls from the service provider that are routed to a DID block,. Typically this is set to [SIP To: header field].

**Use [source] in Request URI of outbound calls:** This defines the "username" parameter of the SIP Request URI for outbound calls to the service provider. Most service providers expect to have the requested number or ID [dialed number] in this field, but some require the registered account information [address of record]. Typically this is set to [dialed number].



## 7.2.2 Details about SIP Gateways

Many parameters associated with SIP Gateways are the same as their counterpart under SIP proxies. In particular, all the **Advanced Settings** are identical. See the SIP Proxy section above for more information about the common fields. Parameter information specific to SIP Gateways is detailed here.

**Gateway uses SIP Registration:** This parameter selection requires the definition of the Login ID and Password the gateway will use to register with Allworx, assuming the gateway supports SIP registration. This is the desired configuration to use especially if the gateway uses DHCP to obtain its IP address so that the Allworx always knows how to contact the gateway for outbound calls.

**Gateway uses Static IP Address:** This parameter selection is used when the gateway does not support registration or when you do not wish to authenticate the gateway. Contacting the gateway through this mechanism requires the gateway to have a static IP address. DNS names are not allowed for security reasons.

**Prefix String:** This parameter defines DTMF digits to be prepended to the dialed number string when placing outbound calls through the gateway (e.g. "9" for dialing through another SIP PBX).

## 7.3 Enterprise Dialing Feature

Allworx supports multi-site configurations using remote phones and remote servers. Remote phones are adequate for individual remote users that need access to the phone services of the office. Remote servers provide independent phone services per site, but with point-to-point dialing between users at the sites via the Internet. The **Remote Servers** functionality is referred to as **Site-to-Site** Calling. See the **Remote Server Multi-site Calling** section for more information.

While the Remote Servers functionality is fully integrated and easy to configure, since the remote servers need to be configured in a full mesh fashion; each site must know about all other sites. While this works well for small installations, more than ten sites can become more difficult to administer.

The Enterprise Dialing feature in Allworx is designed to address this by allowing a third party SIP server to be the "central hub" for all calls between sites. This provides a centralized "phone book" and administrative service for the entire VoIP network. Note that the required centralized server functionality referred to in this section is not an application currently available from Allworx. The Allworx servers themselves are designed to be able to integrate with such an enterprise level infrastructure, but not to host the Enterprise Server functionality itself. Such SIP Proxy Enterprise Servers are available from other providers.

### 7.3.1 Allworx Enterprise Client

Each Allworx server can be configured as an "enterprise client" and direct inter-office calls to the "central hub." A SIP Proxy is created for the central hub, with the call routing set to "Proxy is an enterprise server." The "Enterprise Dialing" rule (**Phone System / Dial Plan** web page) is set to a service group that contains just the SIP Proxy entry for the central hub server. The number of digits to collect/send is set to cover the entire enterprise.

The Allworx dial plan uses an '8' prefix to indicate that the dialed number is to be forwarded to the Enterprise Server. For example, dialing 81234 will send a SIP INVITE with a URI of "<sip:1234@centralHubServer>" to the Enterprise Server.

### 7.3.2 Central Hub / Enterprise Server

The central hub is a SIP proxy server that accepts incoming INVITEs from the Allworx servers, determines the final destination for the request, and forwards the request to the destination Allworx. It maintains an active

list of Enterprise extensions and their mappings to extensions at each site. For example, an enterprise with 4-digit dialing might have the following information in its databases.

Site Account Name	Account Password	Current address	Site Description
allworx1	*****	66.64.219.38:5060	New York City office
allworx2	*****	64.129.42.33:5060	Atlanta office
allworx3	*****	129.116.21.193:5060	San Diego office

The current address is the IP Address and SIP Protocol port of the Allworx server. This can be static or updated through periodic SIP Registration. The Enterprise extensions could be configured as follows:

Enterprise Extension	User	User Extension	Site
1234	John Doe	108	allworx1
1452	Larry Tate	111	allworx1
4689	Fred Jones	108	allworx2
5999	Jane Smith	177	allworx3

For example, John Doe in New York City dials 84689 to reach Fred Jones. The SIP INVITE is sent to the central hub with a URI of "< sip:4689@centralHubAddress>". The Central Hub validates the sender's credentials and looks up 4689 in its databases. It composes an INVITE with a URI of "< sip:108@64.129.42.33:5060>" and sends it to allworx2. Fred Jones answers the phone and the call is established.

Shortly after, John Doe dials 81452 to reach Larry Tate. The SIP INVITE is sent to the central hub with a URI of "< sip:1452@centralHubAddress>". The Central Hub validates the sender's credentials and looks up 1452 in its databases. The recipient is on the same server as the sender (allworx1), so the hub responds with a 300 Redirect with a Contact header URI of "< sip:111@66.64.219.38:5060>." The Allworx server (allworx1) then initiates a call to extension 111. Larry Tate answers the phone and the call is established.

### 7.3.3 Steps on How to Setup Enterprise Dialing

1. Go to the **Phone System / Outside Lines** page.
2. Either **Add New SIP Proxy** or, if it exists, **Modify SIP Proxy** that is the target for the "Central Hub"
3. Check "**Proxy is an Enterprise Server**" under **Call Route** to indicate the SIP Server is an Enterprise central server.
4. Click **Update** button to save settings.

Note that the steps for configuring and maintaining the SIP centralized server are well beyond the scope of this document. If you wish to deploy such an arrangement across sites, it will require detailed knowledge about use and administration of SIP proxy servers. Contact Allworx customer support for an application note with additional helpful administration.

## 8 Remote Allworx Server Multi-Site Calling

Note that this is an optional feature that requires a feature key. The necessary key is referred to as the *Internet Call Access Feature Key* and is the same key that enables SIP Proxy and SIP Gateway functionality described in the previous chapter.

### 8.1 Introduction

The Allworx server products support VoIP calling between servers connected in a peer-to-peer manner. These peer Allworx servers are typically located at different sites. For example, a small business with three office locations may have a dedicated Allworx server at each location where each site is configured to be able to place VoIP calls to each of the two other sites without using conventional circuit switched voice trunks. In addition to these sites each with their own Allworx server, additional site(s) can be serviced via individual remote phones that are each associated with a specific site's Allworx server. See the **Remote IP Phone** section for more details on configuring remote IP phones that are not associated with a local Allworx server.

### 8.2 Quality of Service Between Sites

To take advantage of multi-site calling it is important to take into consideration the quality of the network data connection that spans between each set of sites that will be calling each other. The quality of the data connection will have a direct impact on the observed voice quality between the sites. While the raw bandwidth requirements are not particularly cumbersome for each call that is setup, limiting the number of calls to within the bandwidth available is important to enforce. Additionally, and perhaps more importantly having a good understanding of the typical packet latency and loss rates are also key to accurately accessing the voice quality one would expect to observe on a day to day basis.

The best arrangement to have is to use a managed data service from a quality service provider to be able to deliver a guaranteed level of service according to an agreed upon Service Level Agreement (SLA). Barring that, many *best effort* services, such as an ordinary Internet access service delivered to each site will likely provide acceptable voice quality a majority of the time – but the performance can vary widely depending on many different factors which are beyond the scope of this document. If you are unfamiliar with such considerations, Allworx suggests you read the *Allworx VoIP Tutorial* white paper available on [www.allworx.com](http://www.allworx.com) as a starting point for your investigation into such topics.

### 8.3 Limiting Total Number of Calls Between Sites

It is important to limit the maximum number of allowed calls that will simultaneously exist between the local site and all other sites. This limit is set on the **Servers / VoIP Server** web page under the parameter **Maximum Active Remote Calls**. The default value is eight, but you should select a value based on the total amount of bandwidth you are willing to dedicate to voice calls. See the Allworx VoIP Tutorial white paper available on [www.allworx.com](http://www.allworx.com) for some tips about computing a reasonable value for this parameter.

### 8.4 Defining Remote Allworx Sites

It is actually quite straightforward to configure site-to-site connectivity. For each pair of sites you wish to be able to have communicate with each other, you simply need to define a remote site on each system to point to its symmetrical peer. To define the peer go to **Phone System / Outside Lines** and under the **Remote Allworx** section of the page select **Add New Remote Allworx**. Once each remote site is defined, you can use the associated **Modify** link to adjust any settings as needed. Here is a description of each required parameter to define a pair of sites:

**Description:** A friendly administrative name for the remote site.

**Login ID:** The assigned login name used to register with the remote site. For security purposes this should be kept relatively secret. The peer site must also specify this same login name for the two Allworx servers to successfully identify each other.

**Password:** The assigned password used to register with the remote site. For security purposes this should be kept secret and not easily guessed. The peer site must also specify the same password for the two Allworx servers to successfully authenticate with each other.

**Remote IP Address:** The public static IP address of the remote site. This is required so that the local Allworx server knows how to contact the peer remote server.

**Remote Extension Range:** This is the dialing prefix this local site uses to reach its peer site. The last three digits of the 7-digit dialed number is always the 3 digit extension of the user you wish to reach at that remote site. Many times administrators configure speed dial or PFK buttons on the phones to map to the 4 digit prefix of commonly dialed sites.

## 9 Configuring Allworx IP Phones

### 9.1 Introduction

To configure Allworx IP phones, go to the **SIP Handsets** section of the **Phone System / Handsets** page.

SIP Handsets <a href="#">add new SIP Handset</a>					
Handset	Line	Owner	Caller ID	Identification	Action
Allworx 9112	<a href="#">View Configuration</a>	<a href="#">Add</a>	<a href="#">Call Appearance</a>	<a href="#">Reboot Phone</a>	<a href="#">Replace Phone</a>
User 1	1	User1	User 1	MAC: 00-0A-DD-81-00-B2 User ID: 5100 Login ID: 5100 192.168.2.2:5060 (expires: SEP 12, 2005 04:54 PM)	<a href="#">Modify</a> <a href="#">Delete</a> <a href="#">Ring</a>

This shows a list of all Allworx IP phones known by the Allworx server. As you can see, a number of functions are available by clicking handset specific links.

#### Phone Functions:

- **View Configuration** – This allows you to view and modify the phone configuration. This is detailed in another section of this document.
- **Add Call Appearance** – This allows you to create another call appearance for this phone. Multiple call appearances allow a single phone to handle calls for multiple extensions (or users).
- **Reboot Phone** – Reboot the phone. The reboot will occur after a short delay on an idle phone. If the phone is in-use, the reboot will wait until the phone is idle.
- **Replace Phone** – This allows the phone to be replaced by another while automatically transferring all the configuration parameters and settings to the new phone. This is typically used when replacing a defective handset with a new one.
- **Modify** – This allows for the modification of handset call appearance parameters.
- **Delete** – Delete the phone (so the server no longer knows about it).
- **Ring** – Ring the phone. This is useful to verify connectivity.

The phones must be rebooted before any configuration changes will take affect. This can be done remotely using the **Reboot** Phone link described above or manually from the station.

## 9.2 Why Multiple Call Appearances is Useful

Adding Call Appearances to a station can be very helpful. Why this is helpful is probably best explained through an example. However, before getting into an example it is important to make a distinction between having multiple Call Appearances on a phone station and having multiple Programmable Feature Keys (PFK) on the same station assigned to the same Call Appearance. Adding call appearances to a station in effect defines another logical address that can be mapped into a call route uniquely. However, adding multiple instances of the same Call Appearance to a station allows the station to take multiple calls to the same logical address.

#### Example: Administrative Assistant

The office administrative assistant, Susan Bell, wants to be able to optionally answer the phones of two executives: Tom Brown and Joe Andrews. Here are the steps to accomplish this:

1. The assistant will already have one Call Appearance on her phone for her own calls. New Call Appearances will be added for each executive. The first new Call Appearance description could be

changed from “Susan Bell (L2)” to “Susan Bell (Tom)”. The second description could be changed similarly.

2. The call routes for the executives would be set to ring their own handset and the assistant’s handset in parallel. However, by setting it to ring the Call Appearance on Susan’s phone that is designated for that executive, she’ll know who the call is for and can answer accordingly (“Good morning, Tom Brown’s office...”).

Note that the procedures in this example could be applied to other scenarios like one person answering calls to “sales” as well as “support”. By sending each of those calls to distinct Call Appearances, the answering person can greet the caller appropriately.

## 9.3 View Configuration

The phone configuration parameters are available by clicking on the **View Configuration** link of a specific handset from the **Handsets** page. Once viewing the specific configuration of a particular handset you should be on the **Phone System / Handsets / View Configuration** page. In addition to the summary information about the handset you are viewing including its available call appearances, there are the following set of areas the handset settings can be manipulated in:

- Programmable Feature Keys
- Call Assistant Appearances
- Template Options
- Phone Options

Each one of the above topics will be examined in the sections below.

## 9.4 Programmable Function Keys (PFK’s)

Look at the **Programmable Function Keys** section on the **View Configuration** page of a particular handset. This section is used to show and modify the configuration of the individual PFK’s on a particular handset. To change the configuration, click the **Modify** link.

For each PFK in the phone station there is a numbered row corresponding to the individual PFK. The System Administrator has the ability to set the function for the particular PFK by clicking the drop down arrow and choosing one of the available functions. Each function is detailed in the following sections, but here is a list of the types supported:

- Busy Lamp Field (BLF)
- Call Appearance
- Call Monitor
- Function Feature Key
- Line Appearance
- Not Used
- Parking Orbit
- Queue Appearance
- Speed Dial

### 9.4.1 Busy Lamp Field (BLF) PFK Type

A Busy Lamp Field PFK is used to monitor and dial another phone. The other phone is specified when setting up the BLF function. When the PFK is pressed, the behavior of this function is dependent upon the **Station Mode** selection.

- When **Station Mode** is set to **PBX Behavior**, the extension of the owner of the designated phone is dialed.
- When **Station Mode** is set to **Key System Behavior**, an intercom connection is made to the designated phone.

Note: The Station Mode is selected under the **Phone Options** page of each handset's **View Configuration** page.

## **9.4.2 Call Appearance PFK Type**

The PFK can be mapped to one of the phone's Call Appearances. This allows calls to be placed or received. Additional notes:

- Recall that a phone can have multiple Call Appearances. This allows for each call appearance to be distinctly used in call routing and for those calls to be managed independently and concurrently on the same phone.
- Mapping more than one PFK to the same Call Appearance allows multiple calls to that call appearance to be active at the same time. The Call Appearance won't appear busy to the call route (see Call Routing) until all the PFK's defined for that call appearance are in use. This is akin to call waiting except the PFK's are used to alert and select a new call.

## **9.4.3 Call Monitor PFK Type**

The PFK is mapped to one of the 10 Call Monitors in the system. A Call Monitor allows live call answering of any outside line or call route that is mapped through the associated call monitor.

## **9.4.4 Function PFK Type**

The PFK can be set to perform one of a specified set of functions:

- **Centrex Flash** – Sends a flash signal out the analog CO line. This is ignored if not connected to an analog CO line.
- **Headset** – Turns the headset (if one is plugged in) on and off. If a headset is plugged in and the handset is off-hook, then this button toggles the audio between the headset and the handset. Note if a headset PFK isn't defined, the phone's speaker button will be used to operate the headset.
- **Personal Speed Dial** – Dials a Personal Speed Dial Number that is programmed directly on the phone. The mapping of Personal Speed Dial PFK's and Personal Speed Dial Numbers defined in the handset is as follows. Starting with the uppermost PFK on the phone, count each Personal Speed Dial PFK beginning with 0. This number determines which handset defined Personal Speed Dial Number the PFK dials.
- **Redial** – Redials the last dialed number. Unless the Enable Line Appearance(s) Use of Dial Plan phone option is enabled, only Call Appearance (not Line Appearance) dialed calls can be redialed.

## **9.4.5 Line Appearance PFK Type**

The PFK monitors the status of an outside line, answers incoming calls on that line, and also selects the line for outbound calls. The line is specified when setting up this function for this PFK. For outside lines to be available for selection, they must be enabled on the **Phone System / Outside Lines / Modify** page by checking the **Enable Line Appearance** checkbox. Any number dialed on a Line Appearance bypasses dialing rules, service groups, call history, and the handset's **Outside Line Connection** parameters (**Phone System / Handsets / Modify Handset**).

Unique Allworx Functionality

Allworx has enhanced key-system capabilities relative to SIP devices and Digital Lines. Any SIP proxy, SIP gateway, or Digital Line (T1) bearer channel can be made available as Line Appearance selections when they are enabled on their respective configuration pages. Through this manner, the Allworx system can present a common key-system use model to all external voice circuit facilities including VoIP trunks going to an ITSP.

## **9.4.6 Not Used PFK Type**

No action. This function is selected when the PFK should be disabled.

## **9.4.7 Parking Orbit PFK Type**

The PFK can be mapped to one of the 9 Parking Orbits. When calls are parked they are sent into a Parking Orbit 701 through 709. A PFK can be setup to answer a call in any one of the 9 Parking Orbits.

## **9.4.8 Queue Appearance PFK Type**

The PFK automatically monitors the status of a Call Queue and answers calls that are in the queue. See *Call Queues* for more information on configuring phones for this use.

## **9.4.9 Speed Dial PFK Type**

The PFK automatically dials an extension. The extension is specified when setting up the Speed Dial function for this PFK.

## **9.4.10 Configuration Example: Busy Receptionist**

### Requirements:

Susan works as a receptionist at a busy office. She gets many phone calls each hour. She wants to be able to answer each call while minimizing the possibility of any caller getting a busy signal.

### Phone Configuration:

She has one Call Appearance defined on her phone. She sets up 8 of her phone's PFK's to map to her phone's Call Appearance. (She wants to use the remaining PFK's for other functions).

### Discussion:

When the first phone call comes in, her phone will ring and the first of the Call Appearance PFK's will blink green. While talking with the first caller, a second call comes in. Her phone rings again and the second Call Appearance PFK blinks green. She puts the first caller on hold by pressing the Hold button on her phone and picks up the second caller by pressing the second Call Appearance PFK. She continues to put callers on hold and answer new calls just as described. She terminates calls by switching to another Call Appearance PFK.

## **9.5 Call Assistant Appearances**

The Call Assistant Appearance requires the Call Assistant software application and the Call Assistant Feature Key to be installed.

The Call Assistant Appearance settings extend the number of the features available in Programmable Function Keys by creating virtual keys within the Call Assistant software application. The additional virtual appearances are available only when the Call Assistant application is connected to an Allworx IP phone. However, when connected, this has the practical implication of having many additional PFK's, for these features, beyond the physical keys available on the actual phone.

Call Assistant Appearances has the following PFK features available:



- Call Appearance
- Line Appearance
- Queue Appearance
- Call Monitor

See the above section on PFK Function Selections for details on each of these features. The handset will ring when any of these appearances ring; see the Call Assistant software documentation for further details. Enable the above feature by check the appropriate field and modify the parameters, if needed.

Look at the **Call Assistant Appearance** section on the **View Configuration** page of a particular handset. This section is used to show and modify the specific additional appearances defined for a particular handset when a user has connected to this handset with their Call Assistant application. To modify the configuration, click the **Modify** link. These options work identically to the corresponding appearance types described in the previous section on physical PFK buttons.

## 9.6 Phone Options

Look at the **Phone Options** section on the **View Configuration** page of a particular handset. This section is used to show and modify the phone options for a particular handset. To change the configuration, click the **Modify** link. Many of these options are easily understood from the web page. However, some of the more complicated ones will be described next.

### 9.6.1 Description of Specific Options

**Station Mode Selection** – This selection can be set to **PBX Behavior** or **Key System Behavior**. This selection is used to change the way two areas of a phone behaves:

- It affects how some of the PFK functions work. These changes will be specified below when the functions are described.
- It affects how the Hold button on a handset works. When in Key System mode, the Hold button performs a system wide call park operation that allows the call to be picked up by any handset. When in PBX mode or the active call is on a Call Appearance PFK, the Hold button performs a station based hold operation that is exclusive to the handset.

**Call History Size** – Specifies the number of calls the station will keep in call history. If you specify a value of zero, the phone will not maintain a Call History to help preserve the handset user's privacy.

**Clock Mode** – This specifies whether the phone station should display its idle screen clock in 12 hour or 24 hour format. There is an option also to disable the clock display if the phone is not synchronized to network time or for some reason the handset user does not wish the time to be displayed.

**Codec Preference Order** – Sets the preferred codec order in the phone. The codec is the method of encoding/decoding the audio sent to and received by the phone. The two possible codec's are G.711 and G.729A. G.711 preserves voice quality, but takes more bandwidth. G.729A takes less bandwidth, but reduces voice quality. Note that this only sets the preferred codec order. Not all codec's are supported for all call types (for example, accessing the server auto attendant requires G.711). To maintain operability, the phone will use whichever codec is required to support the call. This means that your preferred codec won't always be the one used.

**Daylight Savings Time** – Specifies the daylight savings time rule the handset uses to compute its local time. Typically you will want to use the **Use Current Server Setting** option if the telephone station is local to the same timezone that the server is in. However, for remote phones, you may want to force a different daylight savings time observance based on the locale the phone is physically located.

**Hold Reminder Mode** – This parameter specifies how the phone operates relative to a hold reminder. Hold reminder is a feature to remind the handset user that they have left a phone on hold:

- **No Reminder** – Never remind the user
- **On Hook** – Beep when ever the phone is put on-hook with call(s) on hold
- **Timer** – Beep after the call has been on-hold for the specified period of time
- **On Hook and Timer** – Beep after the call has been on-hold for the specified period of time or if the handset is placed on hook.

**Jitter Buffer Size** – Jitter is a variation in network audio packet latency experienced by the phone, resulting in a reduction in audio quality. The phone uses a jitter buffer to maximize the audio quality when jitter occurs. This configuration parameter can be used to alter the size of the jitter buffer.

**Message Waiting Indication** – This parameter indicates how the phone should display indication of a voice mail message waiting for the user who is the owner of this handset. If the station has no owner, then this setting has no meaning. The possible settings are:

- **Visual** – The red LED indicator on the Messages button is illuminated.
- **Stutter Dial Tone** – The station emits a stutter when a dial tone is started for each call.
- **Both** – The station does both of the above.

**Off Hook Digits Dialed** – Enables the phone to automatically dial some digits whenever the phone is taken off hook.

- An example of this is a service phone placed at a locked door or loading dock where all dialing is disabled and you want the phone to automatically dial a predefined number when it is taken off hook.
- Another example might be to have the phone automatically dial '9' (or '8' + PIN Code) to get an outside line. Note that these digits will always be dialed when the phone is taken off hook, so this might interfere with other uses of the phone. For example, if the phone is configured to automatically dial '9', the user will not be able to use PBX features that don't start with '9' (Call Park, Call Forwarding, etc.).

**Paging Mode** – Specifies the conditions under which pages are heard on this handset. The choices are:

- Pages Always Accepted
- Pages Never Accepted
- Pages Only Accepted when the station is on-hook

**Paging Zones** – Sets the list of paging zones that the phone will participate in. For example, if the sales team uses zone 3 for pages to the entire team, then this option on the team member's phones must be set to include zone 3. The paging zones setup can also be modified via **Phone System / Paging**.

**Redial Memory** – Sets the length of time the redial memory persists in the phone station. This setting is useful to adjust to maintain privacy on phones that are used in shared areas.

**RTP Media Range (Port to Port)** – This parameter specifies the range of UDP ports used for Real Time Packet communications. Using a maximum range of values makes the phone the most secured from snooping and denial of service activities. However, when remote phones are placed behind 3<sup>rd</sup> party firewalls, under certain conditions the UDP port range may need to be greatly restricted so that mapping rules can be created for each phone behind the firewall. See the chapter on Remote Phone Configuration for more information about conditions where you might need to reconfigure this port range.

**SIP NAT Keep-alive Interval** – Some NAT firewalls will automatically timeout connections. If a remote phone is behind such a firewall, then this setting allows a keep-alive packet to be sent from the phone to the

Allworx server at the frequency specified. When set to an interval more frequent than the firewall timeout, this will prevent the firewall from timing out the connection.

**SIP Port** – This is the UDP port number used for the SIP protocol by the phone station. Typically the default value of 5060 is always used unless there are special circumstances where the phone is placed behind a 3<sup>rd</sup> party firewall and a different mapping is desired.

**Time Zone** - Specifies the time zone rule the handset uses to compute its local time. Typically you will want to use the **Use Current Server Setting** option if the telephone station is local to the same timezone that the server is in. However, for remote phones, you may want to force a different time zone observance based on the locale the phone is physically located.

#### Checkbox parameters

**Enable Audible Dialing** – When enabled, DTMF are heard on the handset or speaker when dialing the phone station. When disabled, dialing operations are silent.

**Enable Auto On Hold** – When one call is active on the phone and another call comes in (with a free Call/Line Appearance PFK), if the PFK for the new call is pressed, the first call is automatically put on hold instead of terminated.

**Enable Auto Retrieve Calls** – When the phone is on the hook and a call is on hold, then when the phone is taken off hook, the call on hold is automatically retrieved. When this is not enabled, the phone gets an open line (if available) when taken off hook.

**Enable Call Timer Display** – When disabled prevents the phone from displaying any call duration timers.

**Enable Caller ID Display** – When disabled prevents the phone from displaying any caller ID information during calls.

**Enable Configuration Menu** – When disabled, this prevents the phone station operator from accessing the station configuration menu. This is useful for securing phones located in common areas.

**Enable DTMF Payout** – When disabled, DTMF digits are not allowed to be sent during an active call.

**Enable Intercom Auto Answer** – When disabled, incoming intercom calls must be manually answered like a regular phone call. Otherwise, intercom calls automatically answer with a live microphone after the alerting tone.

**Enable Keypad Dialing** – If not enabled, the keypad cannot be used to initiate or transfer a call. This does not prevent the keypad from functioning during an active call. It prevents the use of the keypad to initiate any functions directly with the Allworx server (for example: dial number, Call Park, etc.).

**Enable Line Appearance(s) Use of Dial Plan** – If not enabled, the phone number dialed when a Line Appearance PFK is selected is not displayed by the phone, is not recorded in the phone's call history, and is not available for redial. A reason for disabling this is if the CO lines on the system do not follow the North American Numbering Plan (including if the lines connects to another PBX). The use of this feature requires the server's dial plan to be configured (see **Dialing Rules and Service Groups**).

**Enable Off Hook Ringing** – Normally the phone audibly rings anytime there is an active incoming call. However, when this checkbox is disabled, the phone station will not audibly ring if you are already in an active call. The appearance LED indicators and the display operation are not affected.

**Enable On Hook Dialing** – On hook dialing means that the handset doesn't have to be picked up (nor the speakerphone button hit) before dialing a number on the keypad. When the phone is on hook and a digit is dialed on the keypad, the phone will automatically go into speakerphone mode.

**Enable Visual Ringing** – When checked the visual indicator on the phone lights anytime the phone has an incoming call. When disabled, only audible ringing is heard assuming that is enabled.

## 9.7 Configuration Templates

Configuring many phones can be time consuming and error prone. To improve this, the Allworx server provides templates that store a phone configuration. The system provides a factory default template for each phone type. However, the System Administrator can create his/her own unique templates as well.

A list of all the templates known by the system is in the **Handset Configuration Templates** section of the **Phone System / Handsets** page.

Handset Configuration Templates		
Model	Description	Action
Allworx 9112	9112 (Factory - Key)	<a href="#">View</a> <a href="#">Activate</a>
Allworx 9112	9112 (Factory - PBX) <b>[ACTIVE]</b>	<a href="#">View</a>
Allworx 9102	9102 (Factory) <b>[ACTIVE]</b>	<a href="#">View</a>

### 9.7.1 Default Templates

The current default template for each phone type is listed as **[ACTIVE]** in the list of **Handset Configuration Templates**. To make another template the default, click its **Activate** link. The current active templates are used for configuring phones during plug-n-play.

### 9.7.2 Viewing a Template's Configuration

To view a template's phone configuration, click on the template **Description** in the list of **Handset Configuration Templates**.

### 9.7.3 Creating a New Template

New templates can be created from any phone's configuration. Creating a new template has a few steps:

1. Click **View Configuration** on an existing phone.
2. Change the configuration according to the requirements for the new template.
3. Save the current configuration as a template.

To perform the last step, notice the **Template Options** section of the **View Configuration** page.

Template Options	
<input type="button" value="Save"/>	this handset configuration in a template
<input type="button" value="Apply"/>	the <input type="text" value="orbit test"/> template to this handset configuration.

When you click the **Save** button, a pop-up window prompts you to enter the description for the new configuration. After clicking **OK** in the pop-up window, the template is saved and will now appear in the list of **Handset Configuration Templates**.

### 9.7.4 Applying a Template to a Phone's Configuration

To apply a template to a phone's configuration, follow these steps:

1. Click **View Configuration** on the phone to be changed.
2. Using the **Template Options** section, select the template to be applied from the drop down list.
3. Click the **Apply** button.

### 9.7.5 Deleting a New Template

The factory provided templates cannot be deleted. To delete an administrator created template, click its **Delete** link in the **Handset Configuration Templates** section of the **Phone System / Handsets** page.

### 9.7.6 Changing a Template's Configuration

Templates can be saved, applied, and deleted. To change a template's configuration, a combination of those operations must be used. The template configuration cannot be edited directly. The required steps to change a template are to: delete the template you want to change, edit a phone's configuration that reflects the template you want to change, and then save the template with the original name.

## **10 Digital Lines**

The digital lines feature set is specific to Allworx products that have built in T1 interfaces such as the Allworx 24x. This feature is not available on other Allworx server products.

### **10.1 Introduction**

Allworx refers generically to the integrated T1 interfaces as *Digital Lines*. For example, on the Allworx 24x product there are two T1 Digital Line interfaces. These interfaces are accessed through the connectors labeled T1-A and T1-B respectively. The T1-A interface can operate as a Primary Rate ISDN line and/or as a T1 data line for connectivity to another site or to an Internet Service Provider. That is, the T1-A interface supports both circuit switched voice calls and TCP/IP data. The T1-B interface is dedicated for use as a data connection. The data connection can be used for connectivity to another remote site on a dedicated T1 line or for connectivity to a service provider for Internet access.

#### **10.1.1 PRI Support**

The T1-A interface supports Primary Rate ISDN using the National Standard ISDN format (NI-2), Lucent Custom 4ESS, Lucent Custom 5ESS, and Nortel DMS-100 switch types. The Allworx server ISDN interface is always configured as the “user side” equipment with the intention of hooking to the service provider’s Central Office (CO) “network side” equipment. The Allworx server interfaces have a fully integrated CSU/DSU and are typically intended for direct short haul connection to the service provider’s “smart jack”. Consult the product installation instructions for further information.

Note: When PRI operation is desired it is important to define exactly one PRI D-Channel for the Digital Line and a minimum of one PRI B-Channel. The configuration must match the provisioning defined by the Central Office with a typical configuration having 23 B-channels on slots 1 through 23 and one D-Channel on slot 24.

#### **10.1.2 Data Support**

The T1-A interface and T1-B interface can be configured to carry TCP/IP packets using PPP encapsulation on any combination of slots constituting a full or fractional T1 interface. In fact, even when T1-A is configured for circuit switched PRI operations, extra (non-voice) slots can be used for dedicated data connections as long as the remote end service provider allows such a configuration.

Each T1 interface that has data slots configured on it constitutes a single logical serial channel using HDLC encapsulation of PPP packets per RFC-1662. Even though any combination of slots can be used for data on each Digital Line, only one logical data interface can be defined per T1 line.

To use a Digital Line as the system’s WAN interface (for Internet traffic, inter site, etc.), you must select the **“Use a T1 port as the WAN interface”** option on the **Network / Configuration / Modify** page after you have configured the T1 interfaces as desired. Note that even though Digital Lines can be configured and reconfigured without a system reboot, changes to the Network Configuration settings do require a reboot after updating them.

Note: Since the data support is fully symmetrical it is possible to connect two Allworx server devices back to back between their T1 interfaces either on the same site or across sites using a dedicated T1 line that spans between two sites via the service provider.

#### **10.1.3 Restrictions**

Up through software release 6.2 of the Allworx server software, only one interface may be designated as the logical WAN interface for the system. That is, only the Ethernet WAN port or one of the T1 interfaces may be used for routing TCP/IP traffic. You must pick either Ethernet WAN, T1-A, or T1-B ports to be the data WAN interface for the system even though you may provision multiple interfaces simultaneously. This restriction

will be removed in a future software release such that any combination of Ethernet interfaces or Digital Line interfaces can be used as redundant/simultaneous WAN interfaces.

## 10.2 Configuration

The configuration of the Digital Lines is quite straightforward and most parameter settings are dictated by how the service provider provisions the line that each interface is connected to. It is critically important that the settings entered match the service provider's expected configuration or improper operation will result. Typically, you will want to fully configure the line or lines that are being used before physically making the connections to the service provider's point of demarcation.

### Configuration Hint

When using a Digital Line for circuit switched voice operation, it is typically desired to set all the Digital Line parameters including the functional definition for each time slot on T1 line. Once this configuration has been set, each slot configured to support circuit switch voice calls will appear as a new outside line. That is, each separate slot configured for circuit switched voice calls is logically treated as a separate telephone line. At that point, details of how that line is routed or configured is set under the **Digital Lines** section found on the **Phone System / Outside Lines** configuration page.

### 10.2.1 Information on Specific Parameters

Parameters for each Digital Line are configured on the **Network / Digital Lines / Modify** page for the specific line you wish to configure. It is important to provision Digital Lines that are not going to be used as **Disabled**. The disabled state is the factory default setting for each T1 line.

**Description** – A friendly helpful description for the Digital Line interface. This description is used in all other places this line is referred to, such as in the Outlines Lines view and configuration pages of the phone system.

**Line Mode** – The provisioned operational mode for this interface. Currently only **T1** mode and **Disabled** are available. In the future, additional options may be available such as E1 and J1 for use in international markets outside of North America.

**Line Coding Mode** – Both B8ZS and AMI modes are supported. It is strongly recommended that B8ZS mode be used if the service provider supports it. You must pick the setting that matches the service provider's setting, but lines should be ordered as B8ZS, if the CO switch allows it. Note that in AMI mode, clear channel data service is not available and only a 56K data rate will be available on each slot. Generally speaking a PRI line should always be set to B8ZS mode.

**Framing Mode** – The Allworx server supports both Super Frame (D4) and Extended Super Frame (ESF) modes. You must pick the setting that matches the service provider's configuration, but it is recommended to have the service provider use ESF mode, if available.

**Clock Source** – This setting allows you to specify the Digital Line data clocking source reference for this interface. Network clocking is almost always the desired setting because the service provider will be the source of the timing reference and the Allworx interface will be the slave to that network clock. Internal timing mode indicates that the Allworx device is the source of the clocking time reference. This mode is useful if you are going to hook two devices back to back. In that case, one end needs to provide the clock reference and the other must slave to that master. The exact terminology may vary from device to device. For this setting on Allworx devices, "**Network mode**" means it is the slave and "**Internal Mode**" means it is the clock master.

**Loopback Mode** – This selection allows the interface to be put into a diagnostic mode for testing purposes. Generally speaking you always want to select **Normal Operation**. The use of the test modes is beyond the scope of this document:

- Normal Operation – Transmit and receive lines that connect normally and all loop back features modes are disabled.
- Remote Frames – Incoming data is synchronized and decoded at the frame level. These decoded frames are then reframed locally and sent back out on the transmitted output line.
- Remote Unframed – Incoming data is decoded at the bit level from analog voltages to digital bits and directly sent out as a stream of bits back towards the source on the transmitted output line. No attempt is made to synchronize or verify the data at the frame level.
- Local Unframed – An internal analog loop back is performed on the local interface so that transmit data is immediately looped back to the receive path. This mode is useful for verifying that the physical interface is operating correctly on the Allworx unit. Although not strictly required, it is recommended that **B8ZS**, **ESF**, and **Clock Source Internal** be used for such tests.

**Line Build Out** – These settings determine the pulse shape and transmit power levels used on the analog output of the Digital Line interface. The dB settings are for long haul configurations, while the distance settings are used for short haul configurations. Generally speaking the short haul settings should always be used since Allworx equipment is intended for use with a local smart jack only and not for driving the physical T1 lines on the telephone poles directly. You must pick the length setting that matches the cabled distance between the Allworx server and the service provider's demarcation point. If this setting is improperly configured line errors may be very common or problematic and affect system reliability.

**PRI Switch Type** – Select the Primary ISDN (PRI) switch type that is used by the service provider. Select NONE if this interface is not connected to a PRI based service. Note: If this parameter is improperly configured your telephone service will most likely work, however there will be subtle problems when certain type of conditions occur such as calling cell phones, busy numbers, or during network congestion. Additionally, Caller ID functionality may be affected as well. Take care to find out the correct setting from the service provider and set this parameter accordingly.

**Voice Channel Selection Order** – This parameter determines the order the Allworx PBX will attempt to seize a line for *outgoing* calls within each service group assigned to this Digital Line. You want to set this selection to be the opposite direction that the service provider uses for *incoming* calls. For example, if the service provider hunts incoming calls starting from slot 1 towards higher numbered slots looking for the first available channel for a new incoming call, you will want to configure the PBX for "**Descending Mode**". If the service provider starts at the top and hunts towards lowered numbered slots, select "**Ascending Mode**". This parameter is not critical but having it properly set dramatically lowers the probability for a condition called *glare* where both the PBX and the Central Office attempt to put the same slot into service simultaneously for two unrelated calls.

**Caller ID Name** – Since most PRI lines hook directly into the international SS7 telephone signaling network, it is possible to have parties you call, see any callerID string you desire them to see. For analog phone lines your CO determines this string, but for PRI lines the PBX can determine it. Set the caller ID name field to the value you wish called parties to see when placing outgoing calls on this Digital Line. Note: the service provider may override these settings.

**Caller ID Number** – This number is the phone number presented to called parties for outgoing calls. See name setting above for more information.

**PPP Username** – This is the login account name to use for this Digital Line when the line has one or more slots defined on it for data operation. If authentication is not required, leave this field blank.

**PPP Password** – This is the login account password to use for this Digital Line when the line has one or more slots defined on it for data operation. If authentication is not required, leave this field blank.



**PPP MTU** – This setting determines the Maximum Transmit Unit Size to use when sending IP packets to the remote end. The Allworx firewall will force TCP connections to negotiate a MTU no larger than this value. Typically the default value is 1500. The normal Ethernet maximum will suffice however lower values may be required depending on the service provider. If you are having problems consult your data service provider for advice. If you are unsure of a proper value to use and are having data connectivity problems, a value of 512 will negatively impact performance, but should always work.

**PPP HDLC Fill** – This value is the fill value to use on the data line across all slots when the data connection is idle between HDLC frames. Typically the default value of all 1's will suffice, but a flag fill may be desired in AMI line mode.

**Source IP Address** – This parameter is used to determine the static IP address for the Allworx server end of a data connection. Typically, this is the public IP address associated with your ISP connection. If a value of 0.0.0.0 is entered, the service provider is expected to provide the correct value dynamically during session establishment, if the service provider supports that. Consult your ISP for more information.

**Destination IP Address** – This parameter is used to determine the static IP address associated with the router/gateway at the far end of this Digital Line. A value of 0.0.0.0 can be used to have the service provider assign the proper value, if the service supports that. Consult your ISP for more information.

**Channel Assignments** – On a Digital Line you must specify the desired operating mode for each time slot per the provisioning defined by the service provider or the device you have connected at the other end of the Digital Line. If the proper selections are not made, improper operation will result. Currently the following modes are supported:

- Disabled – Indicates that this time slot is not used on this Digital Line
- PRI B Channel – A bearer channel for ISDN PRI operation that can be used for carrying voice calls. Specifying this mode, in effect, defines a new outside line for the PBX for each slot configured in this mode. A maximum of 23 slots can be configured for this mode.
- PRI D Channel – A data signaling channel for ISDN PRI operation which is used for transporting call control information between the PBX and the Central Office. The Allworx server always operates as “user equipment” on a PRI line. If PRI operation is enabled on this line, exactly one slot must be configured as the PRI D channel. Typically, this will be slot 24.
- 56K Data Channel – Specifies that 56Kbits/sec of bandwidth is provided by this slot for the Digital Line's logical data connection. This mode is typically only used if 64K clear channel service is not available. This is the only mode that should be used for data connections when AMI Line Code mode is selected.
- 64K Data Channel – Specifies that 64Kbits/sec of bandwidth is provided by this slot for the Digital Line's logical data connection. This is used when clear channel data service is available. This mode must not be selected if the Digital Line's AMI Line Code mode is selected.

## 11 Dialing Rules and Service Groups

### 11.1 Background Information

This section describes the procedures the Allworx system follows for placing outbound calls.

#### 11.1.1 Dialing Rules

As a user dials digits on a phone, the system collects the digits one at a time. How does it know when it should wait for more digits (because the user is dialing slowly) or when it should take the digits it has and try to make a call with them? The rules the server follows are called Dialing Rules. Dialing Rules specify to the Allworx server what digit sequences are valid to be dialed out on the public phone network.

Examples:

- When dialing a “local” number, you do not normally dial 1 and the area code. So, the system should collect the first 7 digits dialed and then try to make the call. The server should not be waiting for more digits.
- When you dial a long distance number, you normally dial 1 plus the area code and then the 7 digit local number. The system needs to recognize this case distinctly from the “local” number case and know to collect all 11 digits before trying to make the call.

In addition, some local calling areas require an area code to be dialed without the 1 prefix in order to properly dial some numbers. This implies that these rules may vary depending on the local calling area where the Allworx server is installed.

#### 11.1.2 Home Area Code

Some features of the Allworx server and phones (example: redialing from call history and when mapping numbers to 11-digit form to SIP proxies) require the knowledge of the home area code. Therefore, this information is a required part of the dialing rules to enable those features to operate as expected.

#### 11.1.3 Service Groups

The server can use a variety of services to place outside calls such as: Digital Lines, CO lines, SIP Gateways, and SIP Proxies. Some of these services may be optimum for particular types of calls. For example, your SIP Proxy might be the least expensive way to make long distance calls, however your CO lines are best for local calls.

A Service Group is a collection of services that can be used to place outside calls. The server creates several Service Groups automatically:

- All Digital Lines & CO Lines
- All Digital Lines, CO Lines & SIP Gateways
- All Digital Lines, CO Lines, SIP Gateways, and SIP Proxies
- All SIP Gateways
- All SIP Proxies

Note: The Digital Line Service Group is only available on the Allworx 24x.

Additional Service Groups can be defined by the administrator to customize mappings of dialed numbers to any service or set of services.

## 11.1.4 Exceptions

Dialing Rules and Service Groups are only used for Call Appearance calls, not for Line Appearance calls. This is because Line Appearance calls access the outside line directly.

Only the North American Numbering Plan (NANP) is supported by the server dialing rules. If your Allworx server is located in an area that does not support NANP, then you can gain direct access to an outside line by using a Line Appearance PFK or dialing '9#'.

## 11.2 North American Numbering Plan Administration (NANPA)

The Allworx server routes calls using the Service Group that has been assigned to the *type* of number dialed. When NANPA is enabled or disabled it changes the types of numbers dialed that the system supports.

### Dialing Rules

#### Enable North American Number Plan Administration (NANPA)

The system routes calls using the Service Group that has been assigned to the *type* of number dialed. When NANPA is enabled or disabled it changes the types of numbers dialed that the system supports. The table below displays the types supported based on the NANPA setting.

Type	Number dialed
<b>Area Code / Exchange</b>	xxx-nnnn 9+aaa-xxx-nnnn 9+1+aaa-xxx-nnnn
<b>Emergency</b>	9+911
<b>Phone Services</b> (211,311,411,511,611,711,811)	9+n11
<b>Operator</b>	9+0
<b>Long Distance Services</b>	9+1010...
<b>International Calls</b>	9+011...
<b>Public SIP Directory</b>	8+nnnn (4 digits)
<b>PIN Code</b>	78+nnnnn
<b>Outside Line Seizure</b>	9#

NANPA is typically enabled for installations in North America.

NANPA is typically enabled for installations in North America, and disabled for all other solutions

When NANPA is disabled (unchecked) and if 9 is dialed and "All other numbers" is used for an outside call, the system requires a # after dialing the number to terminate the collection of digits. If # is not pressed the system will time out after 6 seconds and try to route the call based on the number dialed.

## 11.3 Defining Service Groups

### Service Group

A **Service Group** is an ordered list of services (CO Lines, Digital Lines, SIP Gateways, SIP Proxies) the system will use when attempting to make an outside call. Services in a group are tried in order until the outside call can be placed.

Select a service from the list of Services and move it to the Service Group. You can also move services in a group up or down to change the order the system will use.

Description

Services		Service Group
CO Line One (CO) Digital Line 1 - 01 (Digital Line) Digital Line 1 - 02 (Digital Line) Proxy 1 (SIP Proxy) test (SIP Gateway)	<input type="button" value="move -&gt;"/> <input type="button" value="&lt;- move"/>	<input type="button" value="move up"/> <input type="button" value="move down"/>

Enter a **Description** for this service group. Then, move the individual services required for this group into the new Service Group box.

When an outbound call is initiated using the Service Group, the services in the group will be tried in top-down order until an idle service is found. The call will be made using the first idle service in the list. So, the last step in setting up a Service Group is to ensure that the order of the services reflects your preferred priority of use. When one of the services in the group is a SIP proxy, the SIP proxy will continue to be considered idle until its Maximum Active Calls setting has been reached.

## 11.4 Configuring Home Area Code And All Other Area Codes

### Dialing Rules

The Allworx uses the table below to determine how numbers in your region are dialed and which Service Group is used to complete the call. Enter your **Home** Area Code and any area codes that do not require dialing 1 before the area code. If some exchanges inside an area code require dialing 1 while others do not, you need only to enter the area code/exchanges that require dialing 1. You may also enter any area codes or area code/exchanges for which you require a specific Service Group to be used to complete the call.

Area Code	Exchange	Dial Method	Service Group
<input type="text"/>	<input type="text"/>	Area Code dialed	All Digital Lines, CO Lines & SIP Gateways
<b>Home</b> <input type="text"/>		Area Code NOT dialed	All Digital Lines, CO Lines & SIP Gateways
all others		1 + Area Code dialed	All Digital Lines, CO Lines & SIP Gateways

#### NOTE

If the **Home** Area Code has been set, seven digit phone numbers (nnn-nnnn) will be routed using the Service Group selected for the **Home** Area Code. Seven digit numbers will be routed using the "All CO Lines, Digital Lines, Gateways & SIP Proxies" Service Group if the Home Area Code has *not* been set.

## Configuration Steps

1. Enter your Home Area Code and set the Dial Method. Most local calling areas will set the Dial Method to Area Code NOT dialed (i.e. 7-digit dialing). This sets up the dialing rule for local calls.
2. Notice the all others area code entry. Its Dial Method is permanently set to 1 + Area Code dialed. This sets up the dialing rule for most long distance calling.
3. Set up any additional area codes where you must dial the area code, but not a 1 prefix.
4. Choose the desired Service Group for each of the area code entries.
5. If there are any additional area codes with unique Service Group requirements, enter it in an empty Area Code row, select its Dial Method, and choose the Service Group.

If the **Home** Area Code has been set, seven digit phone numbers (nnn-nnnn) will be routed using the Service Group selected for the **Home** Area Code. Seven digit numbers will be routed using the "All CO Lines, SIP Gateways & SIP Proxies" Service Group if the Home Area Code has *not* been set.

## **11.5 Interaction Between Service Groups and Handset Outside Line Restrictions**

As stated above, Service Groups are used to direct the placement of outbound calls to particular services and the service chosen for a particular call is the first idle service in the group. However, a handset can be configured to further restrict its use of any CO Line, Digital Line Bearer Channel, SIP Gateway, or SIP Proxy when placing an outside call. The rule for resolving this is as follows:

1. According to the number dialed, the configured Service Group is found for a particular outbound call.
2. When the first idle service in the group is found, the list of handset restrictions is checked.
3. If the found service is restricted for the handset, then the next idle service is found and the handset check is made again.
4. This continues until a non-restricted idle service is found to place the call.
5. If a non-restricted idle service is not found, then the caller hears a fast busy signal indicating that no available outside lines were found.

## 12 Unified Messaging

The Allworx server supports unified messaging such that a user's voicemail and email messages are combined into one "inbox" in the system. Because voicemail and email are stored together and because voicemail can be accessed as voicemail on the phone or as email on a PC, unified messaging may behave in unexpected ways. Here are some of the important properties of the unified messaging feature:

- Voicemail and email are stored in one inbox on the server. Messages from this inbox can be forwarded to another email account or POP'd to an email client.
- Using a phone, the voicemail messages can be listened to, deleted, etc. When a voicemail message is deleted via a phone, it is deleted from the inbox on the server
- When unified messages are deleted off the server because of a POP or a mail forward, the voicemail is deleted as well, and is no longer available on a phone.

### 12.1 Access Mechanisms

The two main mechanisms to access your voicemail and email messages from the server are:

- Forwarding messages to another email account
- Using a POP3 email client to transfer the messages to your PC.

#### 12.1.1 Forwarding Messages via Message Aliases

Using the server's Message Aliases feature (**Business / Message Aliases** page), you can forward any incoming message (voicemail or email) for a user to an external (non-Allworx server) email account. This is done by entering the user's Allworx login name as the email alias and the external email address in the members list. If you want to save a copy of the message on the Allworx server, also enter the user's login name in the members list.

Note: If you save a copy on the server, eventually the user may exceed his inbox quota on the server. To avoid this, the user's messages must be periodically deleted from the server.

#### 12.1.2 Common Mistake in Forwarding Messages

A common error is assigning the Allworx server's domain name to be that of an existing domain name.

##### Example:

MyCompany pays an Internet hosting service to provide email for all their employees at [user@mycompany.com](mailto:user@mycompany.com). The employees get their email by configuring their email application to POP the email off the hosting service's email server. When the Allworx server is installed, it is given a domain name of mycompany.com.

This creates a problem where the Internet DNS servers are configured such that mail for user@mycompany.com is to be sent to the external hosting service's IP address, but the Allworx DNS server has been configured to think it is responsible for handling email for the same domain name. Then when putting user@mycompany.com in the members list, the Allworx server says "that's me!" and sends the email to himself instead of to the external IP address. The solution is to not use the same domain name for both.

#### 12.1.3 POP3 Client

Using the **POP3 Mail Transfers** section of the **Business / Users / Modify User** page, each Allworx user can be configured so that a POP3 request to transfer email to a POP3 client will work:

- email and voicemail messages
- email messages only

- no messages.

Only the first option will transfer voicemail messages to the PC's email application's inbox.

Each user's PC email application needs to be configured so it can talk to the Allworx server to send and receive messages. The precise details depend on the application, but here is the required server information:

- Enter the IP address of the Allworx server's **LAN TCP/IP Address** (from the **Network / Configuration** page) as the incoming POP3 server address.
- Enter the same address as the outgoing SMTP server address.
- Enter the Allworx login name and password for the user as the POP3 user and password.
- Do not use Secure Password Authentication (SPA).
- Do not use SSL to communicate with the Allworx server.
- Do not use authentication for the outgoing server.

In addition, most popular email applications allow the messages to be left on the server when they are transferred to the PC. When using this feature, the user may eventually exceed his inbox quota on the server. To avoid this, it is recommended that you enable your email application to either delete all the server email after N days or to delete it when it is deleted on the PC.

## 12.2 Access Examples

### 12.2.1 Example 1

#### Requirements:

Tom (login name "tom") does not expect to get email at his Allworx server address, but instead uses an external email account (tom@yahoo.com). His Allworx server voicemail should be sent to the external email account, but should also be available from his phone.

#### Configuration:

Set up an Allworx server Message Alias for Tom to forward all his messages to his external email account as well as keep a copy on the Allworx server. Create a new message alias such that:

- **Email Alias** is set to "tom".
- **Members** is set to "tom" and "tom@yahoo.com".

#### Commentary:

Tom will use his phone to delete old voicemail messages. If any email is sent to his Allworx server account, it will be forwarded to his external account, leaving a copy on the Allworx server. If email accumulates on the server, he will need to periodically connect with a POP email client to delete the old email messages.

### 12.2.2 Example 2

#### Requirements:

Tom is a remote user of the system and does not have a phone. His extension is configured to send all calls directly to his voicemail. He does not want to call in to get his voicemail, but instead wants all email and voicemail messages to be sent directly to his external email account (tom@yahoo.com).

#### Configuration:

Set up an Allworx server Message Alias for Tom to forward all his messages to his external email account. Create a new message alias such that:

- **Email Alias** is set to "tom".

- Members is set to "tom@yahoo.com".

## Commentary:

Tom will get all his email and voicemail messages using his external email account. Since the system will delete the messages off the server as soon as they are forwarded, he does not need to periodically delete anything.

### 12.2.3 Example 3

#### Requirements:

Tom will use the Allworx server for his email. He wants to use his phone to listen to voicemail messages, but does not want them sent to his email account.

#### Configuration:

- Set up Tom's Allworx server **POP3 Mail Transfers** configuration to transfer only email messages.
- Set up Tom's PC email application to POP email off the Allworx server without leaving a copy on the server.

## Commentary:

Tom's email messages will be deleted off the server as soon as they are POP'd to his PC's email application. Voicemail messages will be kept on the server until he deletes them via his phone.

### 12.2.4 Example 4

#### Requirements:

Tom will use the Allworx server for his email. He wants to use his phone to listen to voicemail messages and wants those messages sent to his email account as well.

#### Configuration:

- Set up Tom's Allworx server **POP3 Mail Transfers** configuration to transfer both email and voicemail messages (the default).
- Set up Tom's PC's email application to POP email off the Allworx server while leaving a copy on the server until he deletes the message on his PC.

## Commentary:

Tom will be able to listen to his voicemail messages on his phone or on his PC (via email). If he deletes a voicemail message using his phone, it will not be deleted on his PC. However, if he deletes a voicemail from his PC, it will be deleted from the server, making it no longer available on his phone. He will have to periodically delete messages from his PC so that he doesn't exceed his message quota on the server.



## 13 Backing up and Restoring Data

It is a good idea to back up your Allworx server data. In the event of a server failure, you can restore your data from the backup. You can set up the Allworx OfficeSafe Application to create the backup as frequently as you need. Take a few minutes to assess how much data you would be willing to lose in case you need to restore the system from a backup.

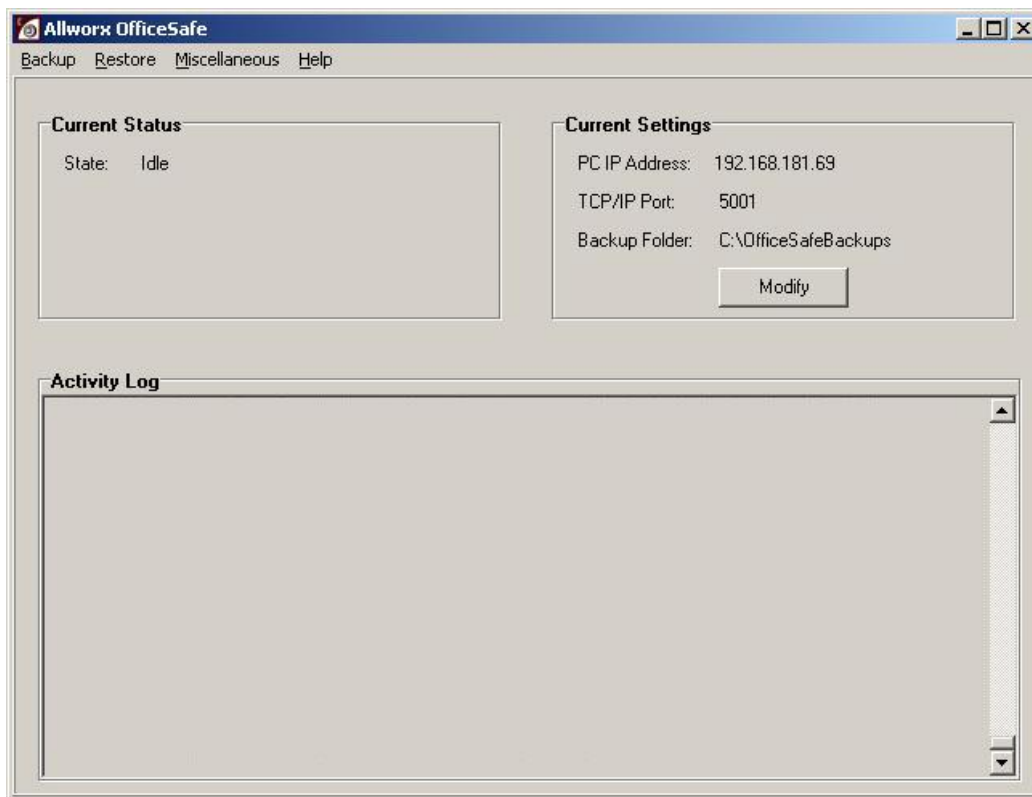
OfficeSafe is optimized for restoring the entire Allworx server disk. It is not possible to restore only a particular file.

### 13.1 How to Create a Backup

Backups are initiated from the Allworx server and require the PC creating the backup to be connected to the server's LAN and running the OfficeSafe application. Parameters for backups are set from both the OfficeSafe application and the Allworx Server since the server needs to be told how and when to contact the PC running OfficeSafe.

#### 13.1.1 OfficeSafe Application on the PC

1. Double-click **OfficeSafe** on your desktop or select **Programs / Allworx / OfficeSafe**.
2. The PC's **Current Settings** are displayed in the main dialog box. The destination of the backups is defaulted to **Backup Folder: C:\OfficeSafeBackups**. Use the **Modify** button to set the Allworx backup destination and port for the backup server connection. The default TCP port should be fine in most cases. If your local network architecture requires a different port number, make sure it is changed on the server as well as in OfficeSafe.



## 13.1.2 Configuring Backups on the Allworx Server

Backups are initiated from the Allworx Server and require a destination PC running the OfficeSafe application. A backup can be initiated either periodically or immediately. The periodic backup cycles include: none, daily, semi-weekly, weekly and month.

**Backup**

Start Time 00 hrs. 00 min.

IP Address (of PC running OfficeSafe)

TCP/IP Port 5001 (of PC running OfficeSafe)

Frequency <NONE>

Mode incremental

**TIP**  
For optimum system performance, the recommended setting for the backup Mode is *incremental*. When set to *incremental*, full backups will automatically be performed when:

- an existing backup is not found on the PC running OfficeSafe
- this is the first backup after the Allworx server software has been upgraded
- this is the first backup after the Allworx server software has been restored
- the OfficeSafe PC application has been configured to force a full backup

Update Start Over Cancel

1. Access **Maintenance / Backup / Modify** and the above page should appear.
2. Set the Backup **Start Time** to have the backup performed automatically at the appointed time of the day.
3. Set the **IP Address** and the **TCP/IP Port** of the PC running OfficeSafe. These values can be obtained from the **OfficeSafe Current Settings** fields.

Note: The IP Address and TCP/IP Port setting must match the OfficeSafe application settings.

4. Select the Backup **Frequency**. The frequency can be set from every day to once a month. More frequent updates mean that, in case of a disk failure, you will lose less data when you restore from the last backup.
5. Set Backup **Mode** to **Full** or **Incremental**.
  - Full: Writes all server data for every backup performed
  - Incremental: Writes only the changes to the server data and merges with previous backup data. This backup mode is helpful to speed the duration of each backup if several gigabytes of data are actually in use on the system being backed up.
6. Click **Update** to save the backup settings and to return to the OfficeSafe screen. A backup will commence at the **Start Time** on each day applicable based on the **Frequency** setting

### Tips about backups:

- Once backup settings have been configured, you can use the **Backup Now** button to initiate an extra backup out of the normal periodic backup period. A dialog prompt is displayed by the server when OfficeSafe Backup process has started.
- Do not exit the OfficeSafe application. The OfficeSafe application must be running on the PC whenever a backup is performed. You can use the *minimize* option in the application to hide it in the system tray. Consult the activity logs to ensure backups are occurring when expected.

- The OfficeSafe application Current Status and Activity Log will give progress during the backup process. When the backup is completed, the Current Status state will be Idle and the Activity Log will display “Saving backup completed successfully.”
- Incremental backups only update an existing backup image. If you wish to archive multiple backups in a rolling backup history window, full backups are required.

### 13.1.3 Additional Backup Options

The follow options are available from the OfficeSafe application under **Backup Options**:

- **Override Allworx Server Backup Mode** is used to force a full backup when the server is set to incremental for one of the following conditions:
  - After  $N$  days since the last full backup, where  $N$  is selectable
  - After every  $N$  incremental backups, where  $N$  is selectable
  - Never (default)
- **Retain Old Backups** is used to set the number of old full backups to retain. The default is zero to conserve disk space on the PC, but you may want to maintain at least two complete backups.

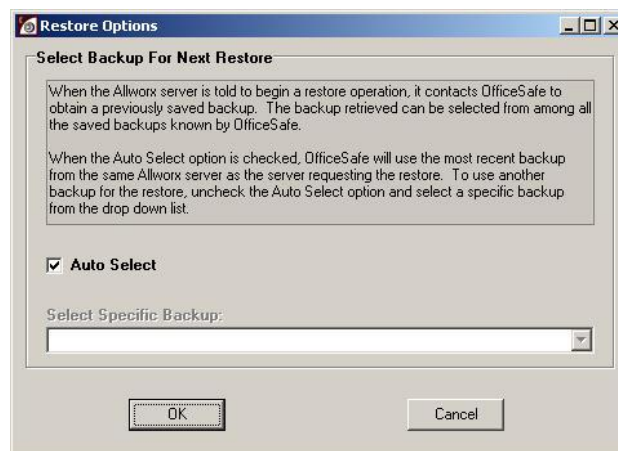
## 13.2 How to Restore Data

You must restore the data while the Allworx server is in Safe Mode. When in Safe Mode, the server will always use the factory default IP address (192.168.2.254) with DHCP enabled. In order to avoid IP address conflicts on the network, it is recommended that all the LAN connections be unplugged and to plug in only the OfficeSafe PC used for configuring the restore.

Restores are initiated from the Allworx server in Safe Mode and require the PC providing the backup to be connected to the server’s LAN and running the OfficeSafe application.

### Step to Restore

1. From the OfficeSafe Application, a restore will use the most recent backup by default. Select **Restore Option** under **Restore** to select the backup to restore. If **Auto Select** is enabled (the Default setting), then the most resent backup will be used. Disable **Auto Select** and click on the drop-down list to select any available backup.



2. On the Allworx server side, you need to restart the server system into Safe Mode. This can be done via the web administration page of the server or by forcing the system into Safe Mode via the front panel of the unit. The method used to force entry into Safe Mode via the front panel varies by product model.

Consult the installation or troubleshooting guides for your specific product model for more details. The procedure for restarting into Safe Mode from the server application is the same for all product models and is accessed via the **Maintenance -> Restart** page on the web administration interface.

- Select **Enter Safe Mode after restart**.
- Click **Restart**.
- Type "**SAFEMODE**" into the pop-up browser window.
- The Allworx server will power down and then power back up in Safe Mode.

### Restart

To restart the Allworx, select an option from the list then click on "Restart".

Normal restart

Restart with factory defaults restored

Enter Safe Mode after restart

3. Once the system powers up into Safe Mode you will be able to access the Safe Mode web page and you should see a screen similar to the following screen.

The Allworx is currently in **Safe Mode**. [Open System Events Window](#)

**Status:**

**OfficeSafe**

IP Address of OfficeSafe PC:

Port #:

**Disk Operations**

If you have just installed a new or empty *Primary Disk*, you must *Format* it before you *Update* the software. Alternatively, you can *Restore from OfficeSafe*.

If you have just installed a new *Mirror Disk*, you should *Mount* the disks now. The mirroring will be performed during the mount. **NOTE:** Make sure you have installed the disks correctly. The *Primary Disk* (the disk that will be copied) **MUST** be installed on left side as you look at the front of the server. The *Mirror Disk* must be installed to the right of the *Primary Disk*.

**Reboot Operations**

The *Reboot in Normal Mode* options have been disabled because the disk (s) have not been mounted. You must first *Mount* the disk(s) before you can boot the Allworx in Normal Mode.

Reboot in Normal Mode

Reboot in Normal Mode with Factory Defaults restored

Reboot in Normal Mode with Factory Defaults restored AND all user settings and files erased

Reboot in Safe Mode

**Software Update**

Two steps are required for updating the software:

1. **Copy Files To Allworx**

The files for the software update must first be copied to the server. To copy update files to the server, you may drag and drop the update files from an Allworx Software Release CD using an [FTP window](#) as the destination.

2. **Activate the Update**

After the files have been copied to the server, they must be activated. Select the "Update" button below to perform this step.

(disk(s) must be mounted first!)

**NOTE:** If the FTP Window fails to open, you can FTP the files directly to the Allworx system. FTP to address **192.168.2.254**. Change to directory 'update'. Make sure FTP is set to perform 'binary' transfers. See the Allworx System Administration manual for more information.

4. In the **OfficeSafe** section of the screen, enter the **IP Address of OfficeSafe PC** that is plugged into the server's LAN port.
5. Select the **Restore from OfficeSafe** button. Important Note: The PC that will provide the restore image must be running OfficeSafe.
6. Select **Accept** on the Confirm Restore Request dialog box to begin the restore.
7. Depending on the size of the backup data (and the performance of your network and OfficeSafe PC), it may take several minutes or perhaps over an hour for the backup to be restored if there are several gigabytes of data to recover. You will see a "**Restore was successful**" message in the Status pane on the Safe Mode page when the operation completes.
8. Select "**Reboot in Normal Mode**" and click the **Reboot** button. CAUTION: Do NOT select "Reboot the Allworx server in Normal Mode with Factory Defaults restored". This will cause your restored settings to be lost during the reboot. If you do this by accident, you will want to start the entire restore operation over again.
9. When the Allworx server has restarted, reconnect your LAN devices and log in to the server.
10. Verify that the data has been restored successfully.

## **13.3 Server to Server Backup and Restore**

Backup and restore can be performed from one server to another. This allows a standard backup image to be loaded onto multiple servers or replicate an existing server. Using the procedure described above, simply perform a backup from one server and then use this backup to perform a restore onto a different server.

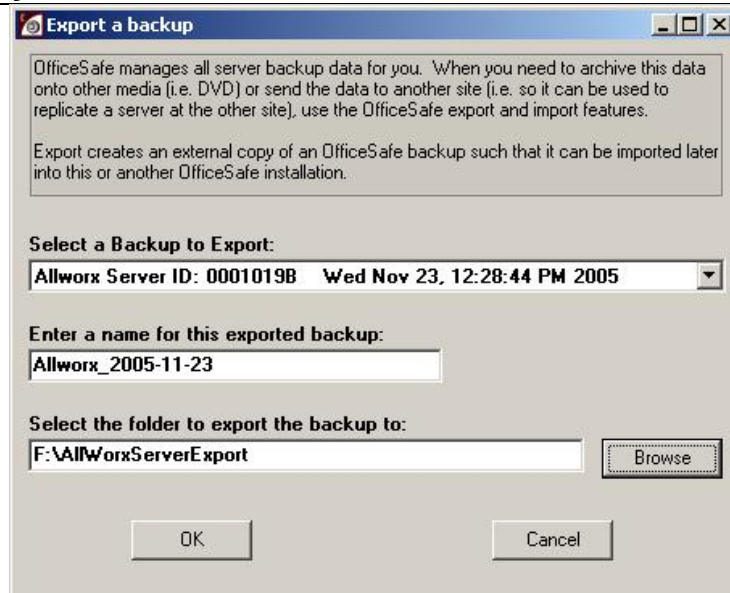
## **13.4 Exporting and Importing Backup Files**

OfficeSafe manages all server backup data for you. When you need to archive this data onto other media (i.e. DVD), store in a network location, or send the data to another site (i.e. so it can be used to replicate a server at the other site), use the OfficeSafe export and import features.

### **13.4.1 Export Backup Files**

Export creates an external copy of an OfficeSafe backup such that it can be imported later into this or another OfficeSafe installation.

1. Select **Export Backup** under **Backup**



2. Select the backup to export
3. Enter then name for this exported backup: <Export Name>
4. Select the export folder: <Export Folder>
5. Select **OK** to start the export operation.

The full path of the export destination will be <Export Folder>\<Export Name>; in the above example the destination will be *F:\AllWorxServerExport\Allworx\_2005-11-23*. The combination of export name and folder location must be unique for each export operation.

## 13.4.2 Import Backup Files

Import transfers a previously exported backup into this OfficeSafe installation so that it can be used to restore a local Allworx server.

1. Select **Import Backup** under **Backup**



2. Select the folder to import the backup from. Note: If the export is in its original location, then the full path will be the export name appended to the export folder (in the above export example this would be F:\AllWorxServerEXport\AllWorx\_2005-11-23)
3. Select **OK** to start the export
4. When the import is completed, it will be ready to use for restores.

## 14 Remote IP Phone

A remote IP phone is one where the phone's Local Area Network (LAN) is not the same as the Allworx server's LAN. An example of this scenario is where the Allworx server is set up at the company's main office, but an employee wants to be able to have an office phone at home so that calls to/from that phone work just as though the employee was at the company's main office.

### 14.1 General Network Configuration Requirements

In support of remote IP phone usage, several remote phone's and Allworx server network configurations are possible:

1. The Allworx server can be directly connected to the Internet via its WAN port. However, the WAN cannot be in "Use PPPoE" mode.
2. The Allworx server can be behind a single 3<sup>rd</sup> party NAT firewall. This requires a specific server and firewall configuration that is described below.
3. The remote phone can be directly connected to the Internet.
4. The remote phone can be behind a single 3<sup>rd</sup> party NAT firewall.

Note: *Allworx cannot guarantee proper operation of 3<sup>rd</sup> party networking products. However, Allworx expects this to work with typical firewalls and tests against several brands. Some NAT/Firewall configuration may be required.*

### 14.2 Allworx Server Behind 3<sup>rd</sup> Party NAT Firewall

To support remote IP phones and SIP Proxy usage when the Allworx server itself is behind a single 3<sup>rd</sup> party NAT firewall, the server's Network Mode must be in LAN Host Mode. This can be set on the **Network / Configuration / Modify** page.

When set to LAN Host Mode, the page contains a **Public IP Address** section as shown below:

**Public IP Address**

If you are using a third party NAT Firewall to map a Public IP Address to the Allworx LAN IP Address, then enter that address here, otherwise leave this field blank.

**Public IP Address**

**NOTE**  
The Public IP Address is used by Allworx VoIP services to encode the proper IP Addresses when communicating with remote SIP services or devices (such as IP Phones) when a third party NAT Firewall is between the Allworx and the Internet.

Most third party NAT Firewalls require specific access rules to enable this functionality. Refer to your firewall documentation to map the ports shown in the table below from the Public IP Address to the Allworx LAN IP Address:

Port(s)	Protocol
2088	UDP
5060	UDP
8081	TCP
15000-15511	UDP



As instructed on the page, enter the firewall's public internet IP address in the **Public IP Address** field. Furthermore, the firewall must be configured to statically map specific ports through the firewall to the Allworx server. This is described in the **NOTE** box on the web page specific to your server's configuration.

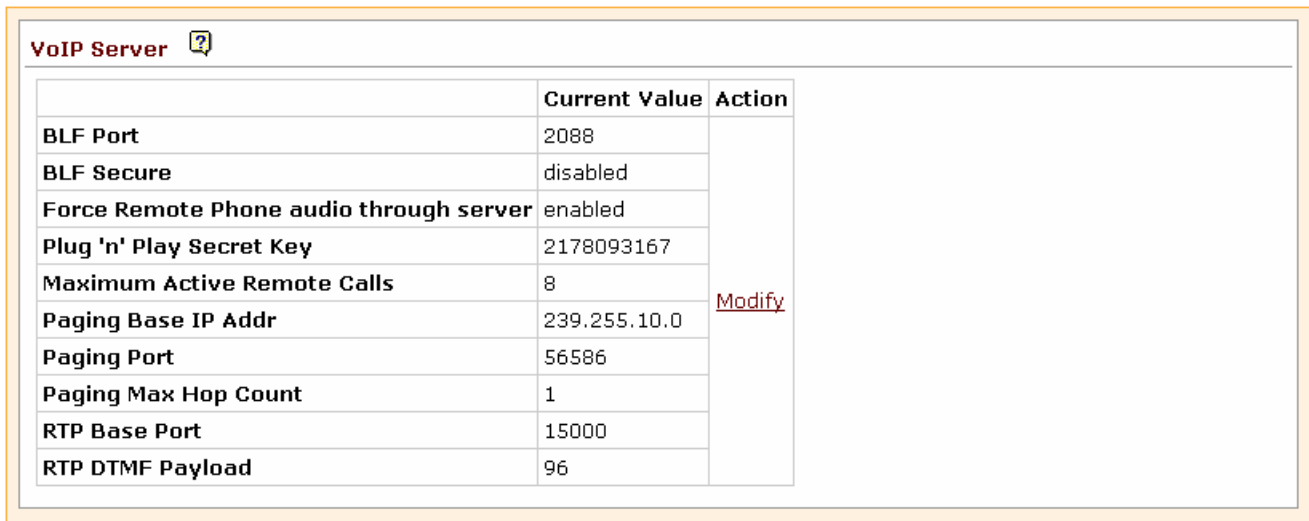
## 14.3 Remote Allworx IP Phone

### 14.3.1 Configuration

Configuration of the remote phone requires setting two configuration parameters in the phone itself. Both are found in the **Config / Network Settings** menu on the phone.

The first parameter is the **Boot Server IP**. This is normally the IP address of the Allworx server's WAN port which can be obtained from the server's **WAN TCP/IP Address** parameter on the **Network / Configuration** page. However, if the Allworx server network mode is set to LAN Host, then this value will be the **Public IP Address** parameter on the **Network / Configuration** page.

The second parameter needed in the phone is the **Remote Plug and Play Key** (called **Remote Plug 'n' Play** on the phone menu). This key is obtained from the **Servers / VOIP Server** page. You will see a page like this:



	Current Value	Action
<b>BLF Port</b>	2088	<a href="#">Modify</a>
<b>BLF Secure</b>	disabled	
<b>Force Remote Phone audio through server</b>	enabled	
<b>Plug 'n' Play Secret Key</b>	2178093167	
<b>Maximum Active Remote Calls</b>	8	
<b>Paging Base IP Addr</b>	239.255.10.0	
<b>Paging Port</b>	56586	
<b>Paging Max Hop Count</b>	1	
<b>RTP Base Port</b>	15000	
<b>RTP DTMF Payload</b>	96	

The **Plug 'n' Play Secret Key** is what should be entered into the phone.

After entering these two parameters into the phone, save the settings (the phone will automatically prompt you when you exit out of the configuration menu) and then reboot the phone.

At this point the remote phone generally operates the same as any other phone on the server's LAN.

#### TIP

If this doesn't seem to work, restore the phone's factory defaults and re-apply the required settings.

### 14.3.2 Remote Phone Behind a Third Party Firewall

In the past all audio from remote phones went through the Allworx server regardless of the configuration. With the addition of the "Force Remote phone audio through server" option bandwidth can be conserved.

By default the checkbox is checked and remote phones work normal. The limitation with this simple setup is bandwidth usage. All WAN-to-WAN calls use twice the bandwidth (180K) of normal LAN-to-WAN calls (90K). This checkbox, located on the **Server / VoIP server** web page, has a **Force audio through server** flag that

causes Allworx to proxy all the RTP packets for WAN-to-WAN calls. Proxies that are configured with RFC 3581 "Symmetric Response Routing" will override this flag since they can help the phone perform the NAT traversal for the audio packets.

**VoIP Server**

**BLF Port**  (typically set to 2088, change if needed for firewall)

**Secure BLF** (typically not checked)

**Force Remote Phone audio through server** (WAN to WAN calls)

**Plug and Play Secret Key**  (6 to 64 characters, use 0-9, and # characters)

**Maximum Active Remote Calls**  (set to at least 1, increase as WAN bandwidth allows)

**Paging Base IP Address**  (Multicast IP/UDP/RTP address, set to 224.0.0.0 through 239.255.254.245)

**Paging Port**  (recommended set to between 49152 through 65535)

**Paging Maximum Hop Count**  (set to between 1 through 255)

**RTP Base Port**  (512 ports used, must be an even number from 15000 to 65024)

**RTP DTMF Payload**  (96-127)

**NOTE**  
It is necessary to restart the Allworx for new VoIP Server settings to take effect.

There are three exceptions: **Force Remote Phone audio through server**, **Maximum Active Remote Calls** and **RTP DTMF Payload**, which may be changed without rebooting the server. If the **RTP DTMF Payload** is changed you must reboot Allworx handsets connected to the system.

By Default, the checkbox is selected and all audio traffic goes through the Allworx server. This typically requires no special configuration on the remote phone's firewall to operate in this manner.

When the checkbox is not selected, audio traffic does NOT travel through the Allworx server when going between remote sites, but instead goes directly between sites thereby reducing latency and saving bandwidth. However, this requires port mapping through the remote phone's firewall such that the other party has a symmetrical view of the ports in use by the remote firewall. See the table below for specific settings in the default configuration. If the phone default settings are changed the ports you need to map may be different.

Description	Port(s)
Configuration	2088
HTTP	8080
RTP Audio	16384 - 32767
SIP	5060

### 14.3.3 Limitations

While connecting the Allworx IP phone to a network behind a NAT firewall generally works well, there are a few limitations.

#### Paging Functions May Not Work

While regular calling and intercom calling works fine, paging functions usually do not. More specifically, sending pages from the remote phone always works, but neither zoned nor overhead pages will typically be heard at the remote phone.

Solution: Paging is implemented using IP multicasting. If all the routers between the Allworx server and the remote phone can be configured to pass multicast packets, then this limitation can be eliminated. Setting up a VPN between the Allworx server and the remote phone may be used to enable this functionality. A full discussion of the general networking details and the configuration of various router brands is beyond the scope of this document. However, the Allworx server details necessary to accomplish this.

On the **Servers / VOIP Server** page of the Allworx server, there are three parameters used to configure where the server transmits zoned pages:

**Paging Base IP Addr** – This is the multicast base IP address used by the system. Each paging zone uses the base address plus an offset. Zone 0 (the overhead zone), uses an offset of 0, zone 1 uses an offset of 1, etc. For example, if the base address was set to 239.255.10.0, then zone 2 would use multicast IP address 239.255.10.2.

**Paging Port** – This is the UDP port number that the packets are sent to. All zones use the same port number, but each have their own multicast IP address.

**Paging Max Hop Count** – This value controls the time-to-live (TTL) count in the IP header of all paging UDP/RTP frames. Typically this value is set to 1 so that the packet will not be sent beyond the local subnet. However, if you have multiple subnets with phones on them, this value will need to be increased.

#### Phones at Different Remote Sites each with a Firewall

When there are phones each at different remote locations and all behind their own NAT firewalls, there may be problems passing audio between them when one remote phone calls another remote phone.

Solution: Statically map (one to one) the remote phone's RTP ports through the NAT firewall. This requires a few steps:

1. The first step is to identify and possibly change the RTP ports used by the phone. Normally, a large range of ports are used. However, setting up a one to one mapping in the firewall may be a time consuming manual operation, you will want to reduce the number of ports used.
2. Go to the **Phone Options** section of the **Phone System / Handsets / View Configuration** page for the Allworx remote IP phone. The **RTP Media Port Range** parameter is the range of ports to be used by this phone. This is configurable.
3. Two ports are required for each active "conversation" on the phone. The phone's intercom capability counts as a "conversation". A conference call uses two ports for each remote caller. There are reasons why having a bigger range than necessary is good. However, when you have to manually map the ports through a firewall, you will want to dramatically reduce the large default range to something you are willing to type into your firewall configuration. A suitable number would be 10 ports.
4. Modify the **Phone Options** to change the **RTP Media Port Range** parameter to reduce the maximum range.
5. The next step is to modify the NAT firewall configuration of the 3<sup>rd</sup> party firewall. You want a one-to-one map of each of the RTP ports through the firewall such that packets arriving at those ports on the firewall's WAN interface are routed to the phone that is inside the NAT firewall. The directions for doing this are unique to each NAT firewall product and therefore beyond the scope of this description.

An alternative solution to this problem is to always route audio through the common Allworx server that both remote phones are associated with. In the **Servers / VoIP Server / Modify** options if the **Force Remote**

**Phone Audio through the Server** option is checked, this should also resolve the problem. However, significantly additional latency may be present in the call and result in unacceptable audio quality.

## Calling through ITSPs

Internet Telephony Service Provider (ITSP) services configured on the Allworx server may not be accessible from remote phones that are behind NAT firewalls.

Solution: Statically map (one to one) the remote phone's RTP ports through the NAT firewall. This requires the same steps as described in the different remote sites phone limitation above.

## **14.4 Remote 3<sup>rd</sup> Party IP Phones**

In addition to support for the Allworx IP phones, the Allworx server supports 3<sup>rd</sup> party remote SIP phones as well. Steps for configuring these are unique to each phone model and brand. However, any of the fully RFC compliant SIP phones that work on the LAN side of an Allworx server typically can be made to work as a remote phone. Please note that the configuration steps can be much more involved and are more challenging to get to work when they are behind other 3<sup>rd</sup> party firewalls. Generally speaking, Allworx recommends using only Allworx IP phones as remote devices.

## **15 Call Routing**

### **15.1 Call Routing Concepts**

#### **15.1.1 Introduction**

When we think of calling an extension, we think of the system causing a particular phone to ring. Thus, if I tell you that my office extension is 106, you expect my office phone to ring when you dial it. Yet, we can imagine some circumstances under which my phone will not ring when you dial 106. For example, if I'm already on the phone, the system may send your call directly to my voicemail rather than give you a busy signal. The Allworx server call routing feature allows a call to an extension to be flexibly directed in this as well as other ways. Some of these other ways are:

- Two phones might ring at the same time with either being able to answer the call.
- One phone might ring for 4 rings; then if no answer, another phone will ring.
- The call will be sent to a particular user's voice mail.
- The call will be sent to an auto attendant.
- The call will be sent to a call queue.
- The call will be routed differently depending on who the caller is (using CallerID).
- The call will be routed differently if the person being called is in their office vs. at a meeting.

In this section, we will explain the concepts necessary to understand how to configure these capabilities.

#### **15.1.2 Connection Attempt**

Suppose that I have an administrative assistant, that I am expecting an important phone call, and that I don't want the caller to have to leave a voicemail message. I'd like to tell the system to first attempt to reach me by ringing my office phone. If I don't answer in 4 rings, then I want the system to call my assistant's phone (using a distinctive ring so the assistant will know it is a call for me). The Allworx server calls each of these attempts to reach someone a "connection attempt." In this example, the system will be instructed to make two connection attempts. The first connection attempt is to ring my office phone 4 times. If no answer, then it should initiate a second connection attempt that will call my assistant.

One connection attempt can ring more than one phone. Suppose that during my work day, I often move back and forth between my office and my lab. I don't want to miss any calls, so I would like the system to ring both phones at the same time and let me answer the call from either one. This would be set up as one connection attempt, but with two phones in it.

#### **15.1.3 Finally Clause**

If the system can't get someone to answer the phone in any of the connection attempts, then we might like the call to be directed to our voicemail (or the auto attendant or to another dialed number or ...). This last direction for the call is called the "finally" clause. It tells the Allworx server what to finally do after all connection attempts have failed. If no connection attempts are defined, then the call is immediately directed to the finally clause.

#### **15.1.4 Primary Route, On-Busy Route, and Call Route**

We have seen how the system seeks to find someone to answer a call. It does this by following the directions specified in a series of connection attempts and a finally clause. The Allworx server refers to this as a "primary route".

What should the system do with the call if a particular connection attempt in a primary route is busy (the phone is busy)? Normally, the system will consider the attempt failed and go on to the next connection

attempt (or the finally clause). This is the same action taken as if the phones weren't answered. What if I want to take a different action if the phones are busy? This can be specified via an optional "on-busy route". Just like the primary route, it is made up of connection attempts and a finally clause. The system uses it to direct a call whenever a connection attempt in the primary route is busy.

The combination of a primary route and an optional on-busy route forms a "call route".

## **15.1.5 CallerID Dependant Call Routes**

Suppose that I want to ensure that all calls from a VIP reach me. If my office phone doesn't answer, I want the system to call my cell phone. I can set the finally clause to dial my cell phone, but can I do this only if the VIP is calling? The Allworx server supports multiple call routes where the call route to use for a given call can depend on a CallerID pattern match. For example, if the VIP's phone is 585-123-4567, then I can create a unique call route that will only be used when the incoming CallerID matches that number. One call route is always designated to be used for non-CallerID-dependant calls.

## **15.1.6 Presence**

I would like to easily change my call route depending on where I am. If I'm on vacation, I don't want to waste my caller's time waiting for my phone to ring 4 times when I know I won't be there to answer it. If I'm on a business trip, I may want my calls to immediately call my cell phone. The Allworx server remembers each user's presence. Each presence can have one or more call routes associated with it. So, when I tell the server that my presence has changed, it immediately begins to use the call routes that are set for my new presence. I don't need to take the time to reconfigure my call routes, just change my presence.

## **15.1.7 User Extensions and System Extensions**

The Allworx server has two types of extensions: user and system. Only a user has a presence. A system extension has call routes without any presence setting.

## **15.1.8 Concept Summary**

### User Extension

- Every user extension has a presence setting.
- Each possible presence has one or more call routes associated with it.
- The selection of which call route to use can depend on the incoming call's CallerID. One call route is independent of the incoming call's CallerID.
- Each call route contains a primary route and an optional on-busy route.
- Each route contains a series of zero or more connection attempts followed by a finally clause.
- Each connection attempt can ring one or more phones.
- The finally clause is executed when all connection attempts have failed to find someone to answer the call. It directs the call to voicemail, the auto attendant, dial a new number, etc.

### System Extension

- Each system extension has one or more call routes associated with it. There is no presence setting to choose a set of call routes.
- In all other ways, it behaves exactly like a user extension.

## **15.2 View and Change a Call Route**

The first step to changing a call route is to select the extension whose call routes you wish to change. Go to the **Phone System / Extensions** page.

**Extensions** [add new Extension](#) (2 of 100 system extensions have been added)

Ext.	Description	Action
0	Operator	<a href="#">View Call Routes</a>
107	<a href="#">User One</a> (User1)	<a href="#">View Call Routes</a>
199	<a href="#">System Administrator</a> (admin)	<a href="#">View Call Routes</a>
212	Conference Room	<a href="#">View Call Routes</a> <a href="#">Delete</a>

Click on the **View Call Routes** link of the extension you want to change.

Notice that each presence has its own set of call routes. If there is only one call route defined for a presence, it applies to all incoming calls. If more than one is defined, all but one has a CallerID pattern to match incoming calls against.

The system must always have a call route that is independent of the incoming call's CallerID. It creates a default call route for this when the extension is created. This call route may not be deleted (notice that no **Delete** link is offered). There can only be one call route like this for each presence. So, when creating a new call route, it must be one that is CallerID dependent. These call routes can be deleted.

To change a particular call route, click its **Modify** link.

**Call Route For Extension 107 - User One (User1)**

**Call Route Selection**

Presence: In Office  apply these changes to **all** the user's presences

On calls from all callers:

**Modify Primary Route**

**Modify On Busy Route** (used if a Primary Route connection attempt is busy)

---

**Call Route**

First connection attempt [add a phone](#) [delete this attempt](#)

User One (Login ID:5100) for 4 rings (Single (int), Double (ext))

[add another connection attempt](#)

Finally...

Hang up

Transfer to Auto Attendant

Transfer to Call Queue Queue 0

**Transfer to Voicemail for user** User One (User1)

Dial number

Update Start Over Cancel

Most of the configuration options on this page should be comprehensible after reading the *Call Routing Concepts* section above. Some additional explanation follows.

Notice the presence setting displayed near the top of the page. Next to it is a checkbox to apply changes made here to all presences. If this call route has no CallerID pattern specified (it is the “all calls” call route), then this call route is copied to the “all calls” call route in all the other presences. If this call route has a CallerID pattern specified, it is copied to the same CallerID patterned call routes in the other presences, creating new call routes if necessary.

To delete a phone from a connection attempt, choose “no selection” from the call appearance drop down list.

To set up a connection attempt so it properly participates in the ringing of a line appearance PFK on an Allworx IP phone, select “Key System Ring Delay” from the call appearance drop down list. See XXX for more information.

Recall that the on-busy route is optional. An inactive on-busy route is one with no connection attempts and a finally clause set to **Hang up**. To make it active, add one or more connection attempts and/or change the finally clause. To make it inactive again, just change it back to the inactive state (delete all connection attempts and set the finally clause to **Hang up**).

## 15.3 Changing a User’s Presence Setting

### 15.3.1 Changing Presence Via an Allworx IP Phone

A user’s presence can be changed via an Allworx IP phone. When the **Mute/DND** button is held down for greater than 1 second, a presence menu will appear. See the “User Guide – Allworx IP Phones” for more information.

### 15.3.2 Changing Presence Via Any Phone

A user’s presence can be changed using any phone connected to an Allworx server by accessing the user’s message center inbox. See the “Phone and Voice Mail Guide” for more information.

### 15.3.3 Changing Presence Via the User Intranet Web Site

A user can login to the Allworx server’s intranet web site to change her own presence setting. The URL is the server’s LAN IP address or “corp.” followed by the server’s configured domain name (example, corp.myallworx.com).

### 15.3.4 Changing Presence Via the Administrative Web Page

Although users can change their own presence setting, the Allworx server system administrator can change a user’s presence by going to the **Business / Users** page, clicking on the **Modify** link of the user to change, and changing the **User Presence** setting.

The screenshot shows a web form titled "User" with a sub-section "Identification". The form contains the following fields:

- Login Name: User1
- Full Name: User [ ] [ ] One
- Password: [ ] Confirm Password: [ ]
- Phone Extension: 107 [ ]
- User Presence: In Office [ ]



## 15.4 Outside Line Call Routing

Outside lines (of any type: CO line, DID Line, SIP Proxy, SIP Gateway, or a Digital Line) have a call route associated with them. Go to **Phone System / Outside Lines** and click the **Modify** link on one of the CO lines.

### Outside Line

**Description**  (typically enter phone number of line connected to the Allworx)  
**Port:** 01  
 **Enable Line Appearance**

---

### Features

**Line has Caller ID service**  
 **Optimize for short loops** (typically unchecked, check for FXD/IADs less than 500 ft. away)  
**Prefix Digits**  (digits dialed by the Allworx after it seizes the line, before user dials)  
**CPC timer**  milliseconds  
(Open Loop Disconnect)

---

### Default Auto Attendant

Select the attendant used to answer when calls received from this source are routed to an Auto Attendant.

---

### Call Route

**Calls received from this CO line go to:**

**Extension**

**Auto Attendant**

**Voicemail for user**

The Call Route section determines how a call coming into the system on this CO line is directed. The options shown are mostly self-explanatory. Below is some additional information.

The Allworx server supports multiple auto attendants. When a call is routed to an auto attendant, it goes to the designated default auto attendant for this outside line.

To use the full flexibility of the Allworx server call routing for any call from an outside line, set the outside line's call route to go to a system extension. Then configure whatever routing is desired for the system extension. Using this, outside calls can be directed in ways such as:

- Route to one phone and then another
- Route to multiple phones concurrently
- Route to a call queue

## 15.5 Example Call Route Configurations

### 15.5.1 Example 1: Ring 1 Phone, Then Voicemail

#### Requirements

When Susan is in her office and a call is made to her extension, her phone should ring distinctively for inside vs. outside calls (an inside call makes a single ring and an outside call makes a double ring). If she doesn't answer in 4 rings, the call should be directed to her voicemail.

## Configuration

Modify the CallerID independent call route associated with Susan's In Office presence such that it has:

- One connection attempt where:
- The phone is Susan's office phone
- The number of rings is 4
- The ring type is Single (int), Double (ext)
- Finally clause set to transfer the call to Susan's voicemail

### **15.5.2 Example 2: Ring 1<sup>st</sup> Phone, Then ring 2<sup>nd</sup> Phone, Then Voicemail**

#### Requirements

Regardless of Susan's presence, when a call is made to her extension, her phone should ring. If she doesn't answer in 4 rings, then her administrative assistant's phone should ring with a distinctive ring so he knows it is a call for Susan. If the assistant doesn't answer in 4 rings, the call should be directed to Susan's voicemail.

#### Configuration

Modify the CallerID independent call route associated with Susan's In Office presence such that it has:

- First connection attempt where:
- The phone is Susan's office phone
- The number of rings is 4
- The ring type is Single (int), Double (ext)
- Second connection attempt where:
- The phone is Susan's assistant's office phone
- The number of rings is 4
- The ring type is Ring Type 4
- Finally clause set to transfer the call to Susan's voicemail
- Select the checkbox to apply these changes to all Susan's presences

### **15.5.3 Example 3: CO Line Rings 2 Phones, Then ring 3<sup>rd</sup> Phone, Then Voicemail**

#### Requirements

Instead of having calls from a CO line go to the auto attendant, the calls should be answered live whenever possible. Tom and Joe work in telephone sales and are responsible for talking with customers. Their manager, Susan, will talk with customers if both Tom and Joe are busy. If no one answers the call, it should be transferred to Tom's voicemail.

#### Configuration

Create a system extension for sales. Change the CO line's call route so that incoming calls go to the sales extension. Modify the sales extension call route such that it has:

- First connection attempt where 2 phones are specified:
- The 1<sup>st</sup> phone is Tom's office phone, 4 rings, ring type is Ring Type 4
- The 2<sup>nd</sup> phone is Joe's office phone, 4 rings, ring type is Ring Type 4
- Second connection attempt where:
- The phone is Susan's office phone, 4 rings, ring type is Ring Type 4
- Finally clause set to transfer the call to Tom's voicemail

## **16 Key System Behavior**

The Allworx server and Allworx IP phones can be configured to behave like a Key System.

### **16.1 Example Configuration**

#### Requirements

An insurance agent called Best Insurance is provisioned with 3 CO lines. The office is staffed by 5 employees, each having an Allworx 9112. The system will behave like a Key System with a PFK on each phone mapped to each of the CO lines. Using the PFK, each user will be able to monitor and directly answer each of the CO lines. If not answered, an incoming call should ring 6 times before routing to a central (not individual user) voicemail for the office.

#### Configuration

1. Create a generic user on the system to receive the central voice mail for the office. Call the user "Best Insurance".
2. Create a system extension to route all incoming calls. Set up the call route so that it has one connection attempt with Key System Ring Delay so the Call Appearance (phone) that will ring 6 times. Configure the call route Finally clause to transfer to voice mail for user "Best Insurance".
3. For each CO line, check the Enable Line Appearance checkbox on the **Phone System / Outside Lines / Modify** page. Configure the call route for each CO line so all calls go to the created system extension.
4. For each Allworx 9112, configure a Line Appearance PFK for each CO line. See **Configuring Allworx IP Phones** Section.

## 17 Direct Inward Dialing (DID)

Direct inward dialing (DID) is a service offered by a local telephone company that provides a block of phone numbers for calling into a PBX without requiring a physical line for each number. In cooperation with the PBX, each number is mapped to a PBX extension. Each PBX user has a unique outside number that can be used to ring the user's phone directly, rather than directing the incoming call to an Auto Attendant.

Configuring the Allworx server for DID service involves 3 steps:

1. Creating a DID block.
2. Configure the call routing plan for the DID block.
3. Create a DID line for each DID trunk line plugged into the server.

Note: Analog DID support is only included on the Allworx 10x product. However DID support is available for Digital Lines and for SIP Proxy (ITSP) based services and they are configured in a similar manner as described here.

### 17.1 Create a DID Block

Click on the **New DID Block** link on the **Direct Inward Dial Blocks** section of the **Phone / Outside Lines** page.

**DID Block**

Starting Phone Number

Total number of phone numbers in the DID Block

DID Routing Plan

Enter the **Starting Phone Number** and **Total number of phone numbers in the DID Block** as specified by the telephone company. Unless you already have an existing **DID Routing Plan** that you want use, leave it as the default to make a new routing plan.

### 17.2 Configure a Call Routing Plan for the DID Block

After the DID block is created, look at the **Direct Inward Dial Blocks** section on the **Phone System / Outside Lines** page to see the routing plan associated with the block.

Block	Action
5551212 Numbers: 10 Plan: Routing Plan 1	<a href="#">Modify</a> <a href="#">Delete</a>

Find the **Plan** parameter value in the **Direct Inward Dial Routing Plans** section on the **Phone System / Outside Lines** page. To configure the routing plan, click on the **Details** link.

**Routing Plan Information**

<b>Description</b>	Routing Plan 1	
<b>Default Extension</b>	0 - Operator	<a href="#">Modify</a>
<b>DID Blocks using this plan</b>	5551200 / 100 numbers	

**Phone Number to Extension Mapping** [add number to table](#)

All phone numbers in this plan use the Default Extension defined above. Click 'add number to table' to route a number to a specific extension.

The routing plan specifies a mapping for each DID phone number to an Allworx server extension. The **Default Extension** will be used as the mapping for any phone numbers not explicitly specified in the **Phone Number to Extension Mapping** list.

### 17.3 Create the DID Lines

The last step in configuring the Allworx server to use DID lines is to configure each of the analog lines that have DID trunk lines plugged into them. Look at the **Analog Outside (CO) Lines** section of the **Phone System / Outside Lines** page.

**Analog Outside (CO) Lines** [scan for new Outside Lines](#)

Outside (CO) Line	Type	Port	Action
CO Line 1	FXO	01	<a href="#">Modify</a> <a href="#">Delete</a>
CO Line 2	FXO	02	<a href="#">Modify</a> <a href="#">Delete</a>
	---	03	<a href="#">New FXO Line</a>
	---	04	<a href="#">New FXO Line</a> <a href="#">New DID Line</a>
	---	05	<a href="#">New FXO Line</a> <a href="#">New DID Line</a>
	---	07	<a href="#">New FXO Line</a> <a href="#">New DID Line</a>
	---	09	<a href="#">New FXO Line</a> <a href="#">New DID Line</a>
	---	10	<a href="#">New DID Line</a>
	---	11	<a href="#">New DID Line</a>
	---	12	<a href="#">New DID Line</a>
	---	13	<a href="#">New DID Line</a>
	---	14	<a href="#">New DID Line</a>
	---	15	<a href="#">New DID Line</a>
	---	16	<a href="#">New DID Line</a>

Click on **New DID Line** for each port where a DID trunk line is plugged in.

The screenshot shows a configuration window titled "Outside (CO) DID Line". It contains the following fields and controls:

- Description: A text input field.
- Port: A dropdown menu with "04" selected.
- Enable Line Appearance: An unchecked checkbox.
- Number of digits sent by CO to identify DID number: A dropdown menu with "1" selected.
- DID Block: A dropdown menu with "assign DID Block Later" selected.
- Buttons: "Add" and "Cancel" buttons at the bottom left.

The **Number of digits sent by CO to identify DID number** must be as specified by the telephone company. Select the **DID Block** created earlier.

## **18 Web, FTP, and CIFS**

Windows file sharing (CIFS) is only available on Allworx 10x server.

### **18.1 Web Sites**

The Allworx server supports a variety of web sites: administrative and user, internal (LAN), external (WAN), auto-generated, customized content, system information, and user information. These will be described below.

The custom content must be HTML only. Server side scripting languages (ASP, server side Java, Cold Fusion, CGI) are not supported.

LAN side Web servers are protected from WAN access when the Allworx server is in one of the network modes that turns on the firewall.

The following terms will be used in the URL and UNC specifications:

- **DomainName:** This is the DNS domain name specified for the Allworx server on the **Network / Configuration** page.
- **LANSideServerName:** This is the DNS name of the Allworx server at the LAN address, corp.DomainName. Alternatively, it can be the LAN IP address.
- **WANSideServerName:** This is the DNS name of the Allworx server at the WAN address, www.DomainName. Alternatively, it can be the WAN IP address
- **HostName:** This is the host name specified for the Allworx server on the **Network / Configuration** page.
- **LoginName:** This is the login name of a user on the Allworx server.

#### **18.1.1 Internal Administration Web Site**

The Allworx server supports an internal (LAN) web site that provides the administrative interface to the server. Two versions of this are available.

- Normal Mode Administrative Web Site: Access to this web site is gained via **http://LANSideServerName:8080**.
- Safe Mode Administrative Web Site: Access to this web site is gained via **http://192.168.2.254:8080**. The safe mode administrative web site is only available when the server boots up in safe mode.

#### **18.1.2 Internal System Info Web Site**

The Allworx server hosts an internal (LAN) company web site that shows a variety of company information including a directory of users, a phone feature guide, distribution lists, a live calls report, etc. From the directory of users, a link to more specific information for each user is available.

To view the web site, go to **http://LANSideServerName**.

#### **18.1.3 Internal Custom System Web Site**

The Allworx server hosts an internal (LAN) company web site composed of custom HTML content.

To view the web site, go to **http://LANSideServerName/export/public/website/**

To add, delete, and modify the files for the web site, use **ftp://LANSideServerName/public/website**

#### **18.1.4 Internal Custom User Web Site**

The Allworx server hosts internal (LAN) per-user web sites composed of custom HTML content.

To view the web sites, go to **http://LANSideServerName/export/users/LoginName/website/**

To add, delete, or modify files for the web site, use **ftp://LANSideServerName/users/LoginName/website**

### **18.1.5 External Custom Web Site**

The Allworx server hosts an external (WAN) company web site composed of custom HTML content.

To view the web site, go to **http://WANSideServerName**.

To add, delete, and modify the files for the web site, from a PC on the LAN use **ftp://WANSideServerName**

## **18.2 Internal FTP Site**

The Allworx server supports an internal (LAN) FTP site that can be used to store and retrieve files from the LAN. No FTP user/password is required to gain access. The URL for the FTP site is **ftp://LANSideServerName**.

## **18.3 External FTP Site**

The Allworx server supports an external (WAN) FTP site that can be used to retrieve files from the WAN. This site is read-only from the WAN. No FTP user/password is required to gain access. The URL for the FTP site is **ftp://WANSideServerName**.

To add or delete files from the site, use **ftp://WANSideServerName** from a PC on the LAN.

## **18.4 Internal CIFS File Server (Allworx 10x only)**

When the file server is enabled on the **Servers / File Server** page, the Allworx server supports an internal CIFS file server. No file permissions are supported. Access is via the UNC path **\\HostName**.



## 19 Auto Attendant

With older phone systems, every office needed someone who answered the phone, routed calls, and took messages. This person usually performed other tasks too and answering the phone created disruptions which prevented the tasks from being accomplished. Now, with Allworx, the phone is answered automatically by the Auto Attendant which frees up the operator for other duties.

Using the Auto Attendant to answer your phone automatically helps direct callers to the person or department they want most. Callers can listen to a list of services and decide which one best suits their need, or use the directories to hear the extension for an employee.

You can setup anywhere from 1 to 9 Auto Attendants depending on your need with each Auto Attendant being assigned to one or more CO/DID Line, SIP Proxy, SIP Gateway, or Digital Line. For example, you may use one Auto Attendant to answer calls for Sales and another for Service. In addition, you can record three greetings for each Auto Attendant: a custom message to be used any time, one to be used during business hours, and the third to be used during the non-business hours.

### 19.1 Configuring the Auto Attendant

Expand **Phone System** and click **Auto Attendants**.

**Auto Attendants**

[Manage the content](#) of the messages played by the Auto Attendants.

---

**x431 - Auto Attendant 1**

Dial-By-Name Menu (#1): enabled  
 Dial-By-Name Prompt: play  
 Dial-By-Name Spell Option: spell first or last name  
 Dial-By-Directory Menu (#2): enabled  
 Dial-By-Directory Prompt: play  
 Dial It Now Prompt: play  
 End Call Prompt: play [Modify](#)  
 Repeat Options Prompt: play  
 Speed Dial Numbers: not allowed  
 Default Extension: not used

Menu Shortcuts								
0	1	2	3	4	5	6	7	8
0	---	---	---	---	---	---	---	---

---

**x432 - Auto Attendant 2**

The nine Auto Attendants are numbered 431 to 439. The list of Attendants shows the attributes assigned to each one. Click **Modify** for the specific Auto Attendant to setup.

## Auto Attendant (x431)

### Features and Prompts

The Allworx allows you to selectively enable certain features and prompts for each Auto Attendant. This is useful if you have recorded your own custom greetings or messages and no longer wish to play the default Allworx prompts.

**TIP**

You may find it helpful to make some changes, then dial the Auto Attendant to test the effect of the new settings.

<b>Description</b>	<input type="text" value="Auto Attendant 1"/>	
<b>Dial-By-Name Menu (#1)</b>	<input type="text" value="enabled"/>	
<b>Dial-By-Name Prompt</b>	<input type="text" value="play"/>	"Press #1 to dial by name."
<b>Dial-By-Name Spell Option</b>	<input type="text" value="spell first or last name"/>	
<b>Dial-By-Directory Menu (#2)</b>	<input type="text" value="enabled"/>	
<b>Dial-By-Directory Prompt</b>	<input type="text" value="play"/>	"Press #2 for a listing of all users and their extensions."
<b>Dial It Now Prompt</b>	<input type="text" value="play"/>	"If you know your party's extension you may dial it now."
<b>End Call Prompt</b>	<input type="text" value="play"/>	"Press 9 or hang up to end your call."
<b>Repeat Options Prompt</b>	<input type="text" value="play"/>	"Press * to listen to these choices again."
<b>Speed Dial Numbers</b>	<input type="text" value="not allowed"/>	(support for dialing 350-399, 34000-34999 from main menu)
<b>Default Extension</b>	<input type="text" value="not used"/>	transfer to this extension if no input for 8 seconds

### Menu Shortcuts

Auto Attendant **menu shortcuts** allow a caller to press a single digit to transfer to an extension. You can define shortcuts for digits 0 through 8. A shortcut can transfer to an internal user, system extension, or to another Auto Attendant.

Digit	Extension
0	<input type="text" value="0 - Operator"/>
1	<input type="text" value="not used"/>
2	<input type="text" value="not used"/>
3	<input type="text" value="not used"/>
4	<input type="text" value="not used"/>
5	<input type="text" value="not used"/>
6	<input type="text" value="not used"/>
7	<input type="text" value="not used"/>
8	<input type="text" value="not used"/>

**Prompts** are messages from the Auto Attendant that gives the caller instructions and **Features** are tasks that the Auto Attendant performs when the caller dials a certain sequence. The selectable **Features and Prompts** available are:

Field	Options	Prompt/Description (if applicable)
Description	N/A	Enter description of the Auto Attendant
Dial-By-Name Menu (#1)	disabled enabled (default)	Allows callers to type the spelling of a user's name based on the setting in the Dial-By-Name Spell Option field
Dial-By-Name Prompt	do not play play (default)	Prompt: "Press #1 to dial by name."
Dial-By-Name Spell Option	spell first or last name spell last name spell first name	Select the spelling method for the Dial-By-Name option
Dial-By-Directory Menu (#2)	disabled enabled (default)	Allows the caller to listen to a list of users and their extension and then enter an extension.
Dial-By-Directory Prompt	do not play play (default)	Prompt: "Press #2 for a listing of all users and their extensions."
Dial It Now Prompt	do not play play (default)	Prompt: "If you know your party's extension you may dial it now."
End Call Prompt	do not play play (default)	Prompt: "Press 9 or hang up to end your call."
Repeat Options Prompt	do not play play (default)	Prompt: "Press * to listen to these choices again."
Speed Dial Numbers	Allowed not allowed (default)	(support for dialing 350-399, 34000-34999 from main menu)

The Auto Attendant can be configured to allow a single number to be dial as **Menu Shortcut**, which will transfer a caller to designated extensions or another Auto Attendant. Select an extension in the drop-down menu for the corresponding digit, there are nine shortcuts available for each Auto Attendant: 0 through 8; "0" is assigned to "0 - operator" by default.

When completed with the configuration, click **Update** to save the setting for the Auto Attendant.

## 19.2 How to Assign the Auto Attendant to an Outside Line

It is very straight forward to select an auto attendant to associate with a particular outside line. This setting is determined by the default Auto Attendant selected in the configuration of the outside line:

1. Go to **Phone System / Outside Lines** and click **Modify** next to the outside line that you would like answered by the Auto Attendant.
2. Under Call Route, make sure that Auto Attendant is selected.
3. Under Default Auto Attendant, select the Auto Attendant you want to answer incoming calls on this line.
4. Click Update to save settings

**Outside Line**

**Description**  (typically enter phone number of line connected to the Allworx)

**Port:** 01

**Enable Line Appearance**

---

**Features**

**Line has Caller ID service**

**Optimize for short loops** (typically unchecked, check for FXD/IADs less than 500 ft. away)

**Prefix Digits**  (digits dialed by the Allworx after it seizes the line, before user dials)

**CPC timer**  milliseconds  
(Open Loop Disconnect)

---

**Default Auto Attendant**

Select the attendant used to answer when calls received from this source are routed to an Auto Attendant.

---

**Call Route**

**Calls received from this CO line go to:**

**Extension**

**Auto Attendant**

**Voicemail for user**

The same procedure can be followed for any of the outside lines, including SIP Gateways and SIP Proxies.

### 19.3 How to Record the Auto Attendant Greetings

In addition to the Prompts selected, you can record three greetings for each Auto Attendant. The greetings and prompts are played in this order:

- If the Custom greeting or any of the prompts are not selected, then they are skipped in order.
- If the caller presses \* to hear the selections again, the Business/Non-Business Hours greeting is skipped.

Follow these steps to record a new greeting:

1. Dial the Auto Attendant extension (431-439) you want to change. You will hear the default welcome greeting.
2. Dial # and 9.
3. After the beep, enter the Administrator password.

Dial	Greeting
1	Business Hours
2	Non-business Hours
3	Custom
#	Return to the Welcome message

*	Replay the options
---	--------------------

4. Press **2** to start recording after the beep. Press **#** when you are finished. You can adapt the following scripts for your message.

Greeting	Sample Script
Business hours	Welcome to <your company name>, your best source for <product>. Dial 1 for store hours and directions. Dial 2 for Sales. Dial 3 for Service. Dial 0 to reach the operator.
Non Business hours	Welcome to <your company name>, your best source for <product>. We are currently closed but will re-open at <opening time>. Our hours are <hours of operation>. If you know your party's extension, you may dial it now. You may also leave a message in our general mailbox at extension <number>.
Custom	<Your company name> is the premier provider of <products>. We specialize in <specialty>. Our latest product is . . .

5. Now Select:

Dial	Task
1	Save the greeting
2	Change the greeting
3	Review the greeting
#	Cancel the changes
*	Replay the options

6. The above steps can be repeated for each of the Auto Attendants that you desire to configure.

## 20 Call Queues

Note that this is an optional feature that requires a feature key. The needed key is referred to as the *Call Queuing Feature Key*.

Call Queues are useful when incoming calls are not to be immediately answered “live”, but will be able to be answered after some delay. The incoming calls go into a “hold” queue and agents (people responsible for answering calls from a queue) can answer each call in first-in-first-out (FIFO) order. The Allworx IP phones provide rich support for working with Call Queues. All other phones provide only very limited ability to work with this feature.

Some of the available features are:

- The caller will hear an initial greeting message when entering the queue. In addition, a status message will replay periodically to all calls in the queue. The replay interval can be configured. These messages can be system default messages or custom messages.
- Using an Allworx IP phone, an agent can login (or logout) his/her phone to the group responsible for handling a particular Call Queue. Once logged in, his/her phone may ring when calls are in the queue, he/she can monitor the status of the queue, and he/she can answer calls in the queue. The conditions under which the agent’s phone will ring can be configured, thus providing significant flexibility in managing the Call Queue.
- A queue can be configured with a maximum call wait time after which a call can be hung up, transferred to an auto attendant, or transferred to a specified user’s voice mail.

### To be able to use Call Queues

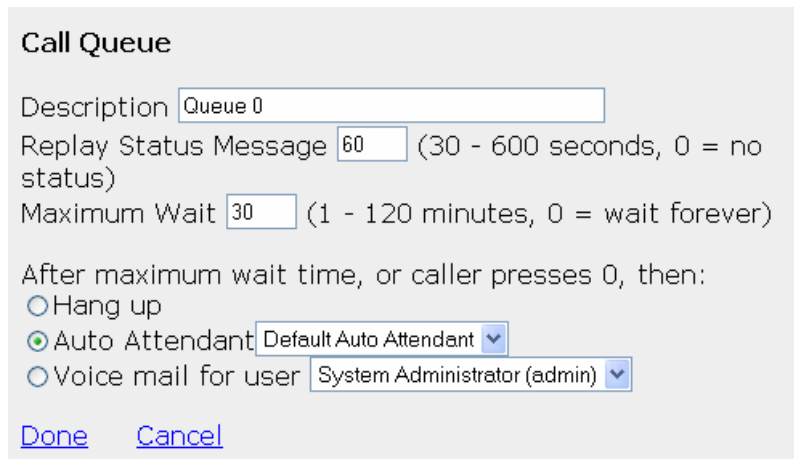
- The Call Queuing Feature Key must be installed.
- The queue must be configured.
- The agent’s Allworx IP phone must be configured.
- The agent must login to the phone and answer calls that are in the queue.
- The system must be configured to route calls to the queue.

## 20.1 Configuring a Queue

The first step in using Call Queues is to configure one of the queues. Go to the **Phone System / Call Queues** page. You will see a page like this:

Queue	Replay Status Message (secs)	Max. Wait (minutes)	After maximum wait is reached, or caller presses 0, then...	Action
0 Queue 0	60	30	transfer caller to Default Auto Attendant	<a href="#">Modify</a>
1 Queue 1	60	30	transfer caller to Default Auto Attendant	
2 Queue 2	60	30	transfer caller to Default Auto Attendant	
3 Queue 3	60	30	transfer caller to Default Auto Attendant	
4 Queue 4	60	30	transfer caller to Default Auto Attendant	
5 Queue 5	60	30	transfer caller to Default Auto Attendant	
6 Queue 6	60	30	transfer caller to Default Auto Attendant	
7 Queue 7	60	30	transfer caller to Default Auto Attendant	
8 Queue 8	60	30	transfer caller to Default Auto Attendant	
9 Queue 9	60	30	transfer caller to Default Auto Attendant	

The system supports 10 queues. To configure a queue, click the **Modify** link. Then click the **change** link on the queue you want to configure. This brings up a browser pop-up like this:



Call Queue

Description

Replay Status Message  (30 - 600 seconds, 0 = no status)

Maximum Wait  (1 - 120 minutes, 0 = wait forever)

After maximum wait time, or caller presses 0, then:

Hang up

Auto Attendant

Voice mail for user

[Done](#) [Cancel](#)

Change **Description** to something meaningful to you as the System Administrator (For example: “Customer Support”). The number in the **Replay Status Message** parameter is the interval, in seconds, between replays of the queue status message to waiting callers. The **Maximum Wait** parameter is the maximum time, in minutes, that a call will wait in the queue (unanswered) before moving to one of the final dispositions shown.

Note that if the caller presses 0 while in the queue, the call exits the queue just as if the maximum wait time was reached. This is especially useful if the final disposition of a call is **Auto Attendant** or **Voice mail** since the caller can exit the queue early without hanging up. When recording a custom queue greeting or status message (see *Managing Custom Queue Message Content*), you may want to mention this feature so your callers know about it.

When finished with the configurations on this page, click the **Done** link and then the **Update** button on the previously waiting page (**Phone System / Call Queues / Modify**).

## 20.1.1 Managing Custom Queue Message Content

The server comes with default messages for the initial greeting when a call enters a queue and the status message that is replayed periodically. To customize these messages, you can either record new messages directly into the server using the phone or record them via some other means and transfer the audio files to the server. The instructions for doing this can be found by clicking on the **manage the content** link near the top of the **Phone System / Call Queues** page.

## 20.2 Servicing a Queue with an Allworx IP Phone

### 20.2.1 Configuring the Phone

An Allworx IP phone can be configured such that one of its Programmable Function Keys (PFK) can monitor the status of a queue and allow the user to answer a waiting call. This type of PFK is called a Queue Appearance. To configure the PFK:

- Go to the **Phone System / Handsets** page and click on the **View Configuration** link for the phone you want to configure.

- Click the **Modify** link in the **Programmable Function Keys** section.
- Select a PFK to designate for this queue.
- Click the drop down arrow, and select **Queue Appearance** for this PFK's function.
- Now click the **define** link that appears. This will bring up a browser pop-up like this:

### Queue Appearance

Call Queue Queue 0 ▼

Login to queue when phone reboots

Ring Type No Ring ▼

The handset will ring when any caller has been in the queue for the specified *Wait Period*, or when there are at least a certain *Number of Callers* in the queue. After hanging up a call, the handset will not ring again for this queue for a period known as the *Rest Time*.

Wait Period 0 (0 to 600 seconds)

Number of Callers 1 (1 to 10 callers)

Rest Time 60 (0 to 600 seconds)

[Done](#)   [Cancel](#)

On this page, the first selection is to choose the particular **Call Queue** to be designated for this PFK. Next is a checkbox to specify that the phone should automatically **Login** to the agent group responsible for servicing the queue. The **Ring Type** might be set to a unique type for this phone so that the agent can easily distinguish calls in the queue from other calls to his phone.

The page contains a description of most of the parameters. These parameters control the ring behavior for this agent's phone when a call is in the queue.

## 20.2.2 Agent Phone Configuration Example

### Requirements

Suppose you have 3 agents to handle calls in a Customer Support queue. You desire Agent 1 and Agent 2 to answer most of the calls, while allowing calls to "overflow" to Agent 3 when necessary. Furthermore, you want to give each agent 2 minutes to finish updating a log about the previous call before their phone will ring with a new call in the queue. You can achieve this by configuring each of the agent's phones as follows:

### Agent Phone Configurations

	Wait Period	Number of Callers	Rest Time
Agent 1	0 seconds	1	120 seconds
Agent 2	0 seconds	1	120 seconds
Agent 3	180 seconds	5	120 seconds



## Commentary

Agent 3's phone will ring when any call has been in the queue for 3 minutes (or 5 or more callers are in the queue). This might happen because Agents 1 and 2 are:

- Already talking to other callers in the queue.
- Away from their desk.
- Have finished with their previous call, but are in their 2 minute rest interval.
- Are ignoring their ringing Customer Support queue appearance because they are on another phone call, talking with someone in their office, etc.

### 20.2.3 Logging in and out of the Queue

When an agent's phone is not logged in to the agent group responsible for handling calls from a queue, the Queue Appearance button will be red and the agent's phone will not ring when a call is in the queue.

While not logged in to the agent group for the queue, the Queue Appearance PFK will flash red when a call is in the queue. If the agent momentarily hits the Queue Appearance PFK while flashing red, he can answer the next call in the queue.

To login to the agent group for that queue, hold down the Queue Appearance button for 1 ½ seconds. The light on the button will then either go out if there are no calls in the queue or flash green if there are calls waiting.

To logout, hold the Queue Appearance button for 1 ½ seconds and the button will change to red indicating that you are logged out.

Note that the auto-login checkbox can be checked on the Queue Appearance PFK configuration page so that the agent's phone is automatically logged in when the phone is rebooted. Then, unless the agent logs out, his phone will always be in the agent group responsible for handling calls in that call queue.

### 20.3 Servicing a Queue with a Non-Allworx IP Phone

As stated earlier, the Call Queue feature is designed to be used with Allworx IP phones while all other phones provide only a very limited ability to work with this feature. The only function a non-Allworx IP phone can participate in is answering a call that is in the queue. Any phone can do this by dialing 441X, where the last digit is the queue number (0-9). The phone will never ring indicating that a call is waiting in the queue.

### 20.4 Configuring Calls To Route To the Queue

A call enters a Call Queue when it is routed from a system or user extension. Therefore, configuring the server so that inbound calls enter a Call Queue is little different from configuring it for any inbound call routing. The same features for the handling of any inbound call can be used to route a call to a Call Queue:

- The outside call can be sent to the Auto Attendant or route directly to the queue extension.
- If the call goes to the Auto Attendant, a menu short cut can be set up to route the call to the queue extension.

See the *Call Routing* section in this document for information on setting up call routes. Both user extensions and system extensions can be set up so the call will route to a Call Queue.

Go to the **Auto Attendant / Menu Shortcuts** section of the **Phone System / Auto Attendants** page to set up an Auto Attendant menu shortcut.

## **20.4.1 Example 1: Call Routing To Auto Attendant and Then Call Queue**

### Requirements

The inbound call will come in to the Auto Attendant. The custom Auto Attendant greeting will include, "For customer support, press 2." When the caller presses 2, they will hear the customer support queue greeting and be placed in the queue.

### Configuration:

1. The inbound call will come in on an outside line. The outside line's call route is set to route calls to the Auto Attendant.
2. A system extension is created for customer support. Its call route is configured so that calls are immediately transferred to the customer support Call Queue.
3. An Auto Attendant custom greeting is recorded that tells the callers to press 2 to reach customer support.
4. An Auto Attendant menu shortcut is configured so that digit 2 calls the customer support system extension.

## **20.4.2 Example 2: Call Routing Directly to Call Queue**

### Requirements

The inbound call will come in directly to the queue.

### Configuration

- A system extension is created for customer support. Its call route is configured so that calls are immediately transferred to the customer support Call Queue.
- The inbound call will come in on an outside line. The outside line's call route is set to route calls directly to the customer support system extension.

## **20.4.3 Example 3: Call Routing To AA, Live Answer Option, and then Call Queue**

### Requirements

The inbound call will come in to the Auto Attendant. The custom Auto Attendant greeting will include, "For customer support, press 2." When the caller presses 2, the customer support person's phone will ring. This allows the call to be answered live, if possible, rather than hearing the queue greeting message. If the call isn't answered after 4 rings, the call will route to the customer support queue and the caller will hear the customer support queue greeting and be placed in the queue.

### Configuration:

1. The inbound call will come in on an outside line. The outside line's call route is set to route calls to the Auto Attendant.
2. An Auto Attendant custom greeting is recorded that tells the callers to press 2 to reach customer support.
3. A system extension is created for customer support. The call route for this is set so the call:
  - Rings the customer support person's phone 4 times.
  - Then if no answer, the call is transferred to the customer support Call Queue.
4. An Auto Attendant menu shortcut is configured so that digit 2 calls the customer support system extension.

## 21 Call Monitors

Call monitors are connection attempts that allow one call to ring multiple phones. Call monitors are analogous to “ringing” Call Queues, in that multiple calls may be ringing on a single call monitor and then will be answered in “first in first out” (FIFO) order.

The notion of a Call Monitor was first available as a single *Key System Ring Delay* feature. This was renamed to call monitors and extended to ten unique instances as of version 5.3; the single *Key System Ring Delay* option remains as one of the available Call Monitors. Call monitor features are only available for Allworx IP phones.

Features of Call Monitors:

- Can ring multiple Allworx IP phones on the system with a single call.
- Can “stack” multiple ringing calls to a single call monitor extension.
- Up to ten available call monitors.
- Allworx handsets can be configured for multiple Call Monitors.
- Allworx handsets can be configured for multiple occurrences of the same Call Monitor.

### 21.1 Difference between Call Monitors and Call Queues

Comparing the functionality of Call Monitors to Call Queues is helpful in explaining the concept of the Call Monitor. Most people are very familiar with a Call Queue and the concept of how incoming calls are answered by the call queuing application where a standard prompt plays out while each caller waits their turn until the next available agent services them. Conceptually, a Call Monitor is the exact same principle except that the Allworx server application never answers the Call Monitor on its own. The incoming caller simply hears ringing to allow the first agent to answering the call to do a live answer of the call.

Call Monitors work best when you desire a live answer of each and every call. Call Queues are preferred if the wait time is typically going to be an extended period of such that you do not want callers to hear extended ringing until the next agent is available to service them.

### 21.2 Configuring a Call Monitor

#### 21.2.1 Modify Call Monitor Description

The description of the Call Monitors can be modified by expanding **Phone System / Call Monitor** and then selecting **Modify** under **Action**. The system supports up to ten call monitors. Press **Update** to accept the new description and return to the **Phone System / Call Monitor** screen.

#### 21.2.2 Setup Call Monitor into Call Route

Call monitors are programmed into call routes via a selection on the call routing configuration screen. To assign a Call Monitor to a specific extension or call route:

1. Navigate to **Phone System / Extensions**
2. Select **View Call Routes** under Actions for the particular extension
3. Select **Modify** for the first Call Route
4. Select **add a connection attempt**, if none are available
5. Under First connection attempted (or any of the connection attempts), select the applicable Call Monitor from the drop-down menu and select the number of rings.
6. Press **Update** when completed

Like all other call routes, Call Monitors can have multiple connection attempts and terminate with: hang up, transfer to Auto Attendant, transfer to voice mail, transfer to queue, and dial number, upon completion of connection attempts. Note: one or more Call Monitors can be programmed into a call route.

## 21.3 Call Monitor with an Allworx IP Phone

The Allworx IP phones need to be configured for the Call Monitor.

### 21.3.1 Configuring the Phone

Allworx IP phone Programmable Function Keys (PFK) can be configured to display the status of and answer a Call Monitor. All phones with a PFK define for a particular Call Monitor will ring when a call is routed to that Call Monitor. To configure the PFK:

1. Expand **Phone System** and select **Handset**
2. Select **View Configuration** for the appropriate SIP Handset
3. Select **Modify** under Action in the Programmable Function Keys (PFK) section
4. For the targeted PFK, select **Call Monitor** from the drop-down menu
5. Select **define** (if revising, select **change**) for this Key under the Type heading, the following pop-up will appear:

Call Monitor

Monitor

Ring Type

[Done](#) [Cancel](#)

6. Select the applicable **Call Monitor** for the PFK from the Monitor drop-down menu, in the above example this is *Monitor 0*.
7. Set the **Ring Type** from the drop-down menu. This allows a unique ring such that the Call Monitor can be distinguished from other calls to this phone.
8. Select **Done** to complete the assignment.
9. Select **Update** to save the new PFK setting.

Additionally, an Allworx IP phone can be programmed to display:

- Multiple Call Monitors per phone to track more than one Call Monitor.
- Multiple occurrences of the same Call Monitor. This allows a user to take more than one call at a time from the same call monitor, so that additional calls are not missed while attending to the current call.

## 21.4 Configuring Calls to Route to the Call Monitor

A call enters a Call Monitor when it is routed from a system or user extension. Therefore, configuring the server so that inbound calls enter a Call Monitor is the same as configuring it for any inbound call routing. The same features for the handling of any inbound call can be used to route a call to a Call Monitor:

- The outside call can be sent to the Auto Attendant or route directly to the Call Monitor extension.

- If the call goes to the Auto Attendant, a menu short cut can be set up to route the call to the Call Monitor extension.

See the **Call Routing** section in this document for information on setting up call routes. Both user extensions and system extensions can be set up to route a call to a Call Monitor.

Go to the **Auto Attendant / Menu Shortcuts** section of the **Phone System / Auto Attendants** page to set up an Auto Attendant menu shortcut.

## **21.4.1 Example 1: Call Routing to Auto Attendant and then Call Monitor**

### Requirements

The inbound call will come in to the Auto Attendant. The custom Auto Attendant greeting will include, "For marketing, press 3." When the caller presses 3, the line will start ringing the Call Monitor key for the marketing group's phones.

### Configuration

1. The inbound call will come in on an outside line. The outside line's call route is set to route calls to the Auto Attendant.
2. A system extension is created for a marketing monitor on the first connection attempt.
3. Configure a Call Monitor Programmable Feature Key for each of the marketing group's phones.
4. An Auto Attendant custom greeting is recorded that tells the callers to press 3 to reach marketing group.
5. An Auto Attendant menu shortcut is configured so that digit 3 calls the marketing group extension.

## **21.4.2 Example 2: Call Routing to Call Monitor and then Transfer to a Call Queue**

### Requirements

The inbound call will ring directly to a Support Call Monitor. If not answered, then will be the call will be transferred to the Customer Support queue.

### Configuration:

1. A customer support system extension is created using the Support Call Monitor on the first connection attempt and that will then transferred to the Customer Support queue.
2. The inbound call will come in on an outside line. The outside line's call route is set to route calls directly to the customer support system extension.

## **22 Parking Orbits**

Parking Orbits can be used to place a call on *system wide hold* via a specially designated extension number that can be picked up by any other handset in the system. For example, you can park a call from your office, then walk to another location in the building and *retrieve* that call back at the new location. Parking is also useful when used in conjunction with Overhead or Zoned Paging such that another party may retrieve a call you have just parked without you having to know what extension that party are currently at.

The Allworx server supports up to nine parked calls at one time where each currently parked call is associated with a specific slot retrieval number in the phone system dial plan numbered from extensions 701 through 709. When a call is newly parked, it is assigned the lowest available slot number. These slots available for parked calls are generally referred to as *Parking Orbits*.

The *Allworx Phone – User’s Guide* describes how a call is places into and retrieved from a Parking Orbit.

### **22.1 Configuring Parking Orbits for Allworx IP Phones**

Allworx IP phones can be configured via its Programmable Function Keys (PFK) to monitor the status of Parking Orbits. The Parking Orbit PFK indicates the parked or idle status for its associated parking orbit. Calls parked by the local station (the handset parking the call) will display differently than calls parked from other stations. The Parking Orbit PFK can also be configured to provide a reminder that a call has been parked.

1. Expand **Phone System** and select **Handset**
2. Select **View Configuration** for the appropriate SIP Handset
3. Select **Modify** under Programmable Function Keys (PFK) section
4. For the targeted PFK, select **Parking Orbit** from the drop-down menu
5. Select **define** for this Key under Type heading.
6. Set the particular **Parking Orbit** (701 – 709) that this PFK is to monitor. A station that is configured to monitor only a subset of parking orbits should start with 701 and work its way up so that the mostly commonly assigned orbits will always be available.
7. Set the Reminder Duration to ring the handset upon call being parked for this elapse time (enter 0 to disable the reminder, or enter a time period from 10 to 600 seconds)
8. Select **Done** to complete the assignment of the PFK settings.
9. Select **Update** to save all PFK assignments.

As always, for the above changes to take affect, the associated phone station must be rebooted. See the phone configuration section for all other details about phone configuration.

#### Notes about Parking Orbits

All analog, Allworx, and 3<sup>rd</sup> Party IP phones can be used to park and retrieve calls, however only Allworx IP phones can be configured to live monitor Parking Orbits and support parked call reminders. Additionally, Allworx IP phones are configurable such that the station’s HOLD button can be used to automatically do either local station HOLD operations or automatic PARK operations with minimal number manual steps.

When manually parking a call, one must use the ATTENDED transfer operation to park the call to extension 700. If you park a call using a BLIND transfer, the remote party will hear the parking orbit extension assigned instead of the user parking the call. If the user wishes to use BLIND transfer to park a call, they should park the call to extension 740 instead of 700. Extension 740 is designed to be used in conjunction with BLIND transfers however only Allworx IP phones monitoring parking orbits will see the orbit number assigned via the station’s LCD display. Consult the *Allworx IP phone – User’s Guide* for more details about phone operations and how to do ATTENDED vs. BLIND transfers.

Note: When Analog Phones or 3<sup>rd</sup> party IP phones wish to park calls, they should always do an attended transfer to extension 700.

## 23 Zoned Paging and Overhead Paging

The Allworx products support two related forms of Paging. The first type of paging is Overhead Paging. This type of paging has its audio go out through the LINE OUT jack of the associated server. If used at a site, one typically hooks the LINE OUT jack to a paging amplifier or some sort of Public Address Announcement system.

The other type of paging is referred to as Zoned Paging. The Zoned Page audio typically emits from a selected set of Allworx IP phones through their speakerphone speakers. Each set of phones that emit the same class of pages is referred to a *zone*. Each station can be in any combination of zones desired. Additionally, any combination of zones can be assigned to the Overhead Paging circuit so that those pages also play their audio out to the LINE OUT jack referred to above.

Allworx systems support a total of 10 paging zones via a common paging circuit. That is, while you can configure and use any combination zones desired and each station can be in any combination of zones desired, for this reason only a single zone can have an active page at any one instant in time.

The 10 paging zones are accessed consecutively via extensions 460 through 469. One extension corresponds to each one of the 10 zones.

### 23.1 Paging Amplifier and Door Release Relay

Most Allworx server products support an internal relay that is controlled to be active when a LINE OUT overhead page is currently active in the system. The relay can alternatively be used to control a door release mechanism so that a phone extension can be dialed to allow someone entry to a secured area. The contacts of the relay associated with these features are available via the DB-9 connector (9-pin D shell "serial" type connector) of the Allworx server. See the installation instructions for connectivity details.

When configured in paging amplifier mode, this relay feature is useful for using the relay contacts to control when power is fed to an external paging amplifier.

When configured in door relay mode, the relay is useful for activating a door release solenoid mechanism of some form.

The relay operation mode is configured on the **Phone System / Paging** configuration page and can be set exclusively to one of the following modes:

- **Door Entry System:** by setting the relay mechanism to this mode, a door entry system can be remotely activated to allow access by dialing extension 403. The relay will activate for a maximum of 5 seconds or will stop when the phone call is terminated, which ever is shorter.
- **Paging Amplifier:** by setting the relay mechanism to this mode, the paging amplifier system will automatically activate immediately preceding each overhead page and then turn back off once the page completes.
- **Unconnected:** setting the relay feature to this mode will completely disable the relay and it will not operate through either mechanism.

Note: These relay based features are *not* available on Allworx 10x server.

### 23.2 Paging Zone Names

The name assigned to each of the paging zones (0 - 9 and corresponding extensions 460 - 469) can be modified to provide a meaningful descriptive name. To change the names of the zone navigate, to the **Phone System / Paging** and select **Modify** in the **Paging Zone Names** section of the page.



If you change the names of any Paging Zones, any handsets with a PFK defined for those Paging Zones will not use the new name until the handset has been rebooted.

## **23.3 Paging Zone Operation on the Handsets**

Each applicable lineout and Allworx handset can be added to or removed from each of the paging zones. By default, each applicable lineout and handset are enable for paging zone 0 and disabled for all others. The paging zones can also be enabled and disabled on the handset configuration page. The handsets can be configured to one of the following relative to all pages received:

- Pages always accepted
- Pages accepted only while on hook
- Pages never accepted

If you change the zones for a handset, it is necessary to reboot the handset for the changes to take effect.

## 24 Abbreviations

BLF – Busy Lamp Field

DND – Do Not Disturb

PBX – Private Branch Exchange. ie: Phone System.

PFK – Programmable Feature Key

PoE – Power Over Ethernet

TLA – Three Letter Acronym

VoIP – Voice Over Internet Protocol