

# **Allworx<sup>®</sup>**

# **System Administrator's Guide**

(Release 7.2.3.x)



No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopy, recording, or otherwise without the prior written permission of Allworx.

© 2010 Allworx Corp. All rights reserved. Allworx, a wholly owned subsidiary of PAETEC Holding. All other names may be trademarks or registered trademarks of their respective owners.

## Table of Contents

1	Introduction .....	1
1.1	Who Should Read This Guide .....	1
1.2	Purpose.....	1
1.3	Allworx Family of Servers .....	1
2	Accessing Web Administration .....	4
3	Configuring a New Allworx Server.....	5
3.1	Feature Keys.....	5
4	Upgrading Server Software.....	8
4.1	Upgrade from Release 7.0 and Lower .....	8
4.2	Upgrading from Release 7.1 to 7.2 .....	8
4.3	Activating Server Software.....	10
4.4	Options after upgrading to 7.2 .....	10
5	Network Configuration .....	11
5.1	Network Mode: Standard Router.....	12
5.2	Network Mode: LAN Host.....	13
5.3	Network Mode: NAT/Firewall .....	14
5.4	Network Mode: NAT/Firewall with DMZ .....	16
5.5	Network Mode: NAT/Firewall with Stealth DMZ .....	17
5.6	Example 1: Secure Firewall .....	17
5.7	Example 2: Secure Firewall with 3 <sup>rd</sup> -Party Email Server.....	18
6	Internal Dial Plan and Extension Length.....	19
6.1	3-Digit vs. 4-Digit Extensions .....	19
6.2	Modifying Internal Dial Plan .....	21
6.3	Multi-site Calling.....	22
7	Adding Users .....	23
7.1	User Templates.....	23
8	Adding Handsets.....	27
8.1	SIP Phones .....	27
8.2	Analog Phones.....	30
8.3	Testing Phones .....	31
9	Configuring Allworx IP Phones.....	32
9.1	Introduction .....	32
9.2	Why Multiple Call Appearances are Useful.....	33
9.3	View Configuration.....	33
9.4	Programmable Function Keys (PFKs).....	33
9.5	Call Assistant Appearances .....	38
9.6	Handset Preference Groups .....	39
9.7	Handset Templates .....	45
9.8	Phone Web Administration .....	47
10	Outside Lines .....	49
10.1	Anonymous Call Handling.....	49
10.2	Allworx Port Expanders.....	49
10.3	Fax Server Support.....	51
10.4	SIP Proxies and SIP Gateways.....	52
10.5	Digital Lines .....	57
11	Dialing Rules and Service Groups .....	64
11.2	North American Numbering Plan Administration (NANPA).....	65

11.3	Defining Service Groups .....	66
11.4	Configuring Area Codes.....	67
11.5	Remote Sites as Services .....	68
11.6	Dialing Privileges Groups.....	68
11.7	Interaction between Service Groups and Handset Outside Line Restrictions.....	70
12	Unified Messaging .....	71
12.1	Access Mechanisms .....	71
12.2	Access Examples.....	73
13	Backing up and Restoring Data .....	75
13.1	How to Create a Backup .....	75
13.2	How to Restore Data.....	78
13.3	Server-to-Server Backup and Restore .....	81
13.4	Exporting and Importing Backup Files .....	81
14	Remote Allworx Phones and Port Expanders.....	83
14.1	General Network Configuration Requirements .....	83
14.2	Allworx Server Behind a 3 <sup>rd</sup> -Party NAT Firewall.....	83
14.3	Setting Up Remote Allworx Devices.....	84
15	Call Routing .....	90
15.1	Basic Routing.....	90
15.2	Multiple Destinations.....	91
15.3	Multiple Connection Attempts .....	92
15.4	On Busy Routing.....	92
15.5	Follow-Me-Anywhere .....	92
15.6	Caller ID Based Routing .....	93
15.7	Day & Night Routing.....	94
15.8	Changing a User's Presence Setting .....	94
15.9	Outside Line Call Routing .....	95
16	Follow-Me-Anywhere .....	97
17	Voicemail Notification & Escalation Message Alerts.....	99
17.1	Notification Mode .....	99
17.2	Escalation Mode .....	99
18	Key System Behavior.....	101
18.1	Example Configuration.....	101
19	Direct Inward Dialing (DID) .....	102
19.1	Create a DID Block .....	102
19.2	Configure a Call Routing Plan for the DID Block.....	102
19.3	Create the DID Lines .....	103
20	Emergency Support .....	105
20.1	Emergency Handset Caller ID.....	105
20.2	Emergency Alerts.....	107
21	Call Supervision .....	109
22	Day-Night Mode .....	110
23	Auto Attendant .....	111
23.1	Configuring the Auto Attendant.....	111
23.2	Recording Auto Attendant Greetings and Messages .....	114
23.3	Assigning the Auto Attendant to an Outside Line .....	115
24	Call Monitors .....	117
24.1	Configuring a Call Monitor .....	117
24.2	Call Monitor with an Allworx IP Phone .....	117
24.3	Configuring Calls to Route to the Call Monitor .....	119

25	Parking Orbits .....	121
25.1	Configuring Call Parking Orbits.....	121
25.2	Configuring Parking Orbits for Allworx IP Phones.....	121
26	Zoned Paging and Overhead Paging.....	123
26.1	Paging Amplifier and Door Release Relay.....	123
26.2	Paging Zone Names .....	123
26.3	Paging Zone Operation on the Handsets.....	124
27	Dual Language Support.....	125
27.1	Language Pack Installation.....	126
27.2	Language Settings .....	126
27.3	Custom Messages .....	129
27.4	Configuration Examples.....	129
28	System Settings Import / Export .....	131
29	Abbreviations .....	134

- This page intentionally left blank -

## 1 Introduction

### 1.1 Who Should Read This Guide

This guide is to be read by people who will be installing and maintaining Allworx servers. The reader is expected to have a computer networking and basic telephony background and to have completed the Allworx Partner technical training.

### 1.2 Purpose

The Allworx server web administration interface has built-in descriptions, help, and tips on many of its pages. Therefore, not all the features or all the parameters of each feature are discussed here. This guide discusses only those features and parameters that require additional explanation beyond what is on the web pages.

This manual applies to Allworx System Software Release 7.2.3.x. The following are additional documents related to Allworx server software release 7.2:

- *Allworx User's Guide, Release 7.2.3.x*
- *Allworx Server Software Release Notes, Release 7.2.3.x*
- *Allworx Phone Guides*
- *Allworx Queuing and Automated Call Distribution Guide*
- *Allworx Advanced Multi-site Setup Guide*
- *Multi-Tech FaxFinder Setup Application Notes*

A System Administrator's Guide for Releases 7.1 and lower are available on the Allworx Partner Portal ([www.allworx.com](http://www.allworx.com)).

### 1.3 Allworx Family of Servers

The award-winning Allworx family of servers includes the Allworx 6x, Allworx 24x, and Allworx 48x servers. The servers differ in features and capabilities. The table below depicts which Allworx server offers which capabilities:

## Feature Comparison

Feature	Allworx 6x	Allworx 24x	Allworx 48x
Number of users	30 (up to 60 with Feature Key)	24 (up to 150 with Feature Key)	48 (up to 250 with Feature Key)
CO Lines	6 FXO Ports	3 FXO Ports	3 FXO Ports
T1 Support	N/A	Integrated single PRI or RBS	Integrated NFAS, Dual PRI or RBS
Extensions	60 (up to 120 with Feature Key)	48 (up to 300 with Feature Key)	96 (up to 500 with Feature Key)
Analog phones	2 FXS Ports	5 FXS Ports	5 FXS Ports
VoIP	SIP 2.0	SIP 2.0	SIP 2.0
Multi-site	100 Sites	100 Sites	100 Sites
Voicemail	8-port Voicemail	16-port Voicemail	16-port Voicemail
Presence Management	7 settings per User with 7 Voicemail Greetings	7 settings per User with 7 Voicemail Greetings	7 settings per User with 7 Voicemail Greetings
Auto Attendants	9	9	9
Conference Bridges	One (1) 8-seat Bridge	Four (4) 8-seat Bridges	Four (4) 30-seat Bridges
Door Relay	Included	Included	Included
Paging Output	Included	Included	Included
Paging Zones	10 Customizable Zones	10 Customizable Zones	10 Customizable Zones
Storage	Compact Flash	Hard Disk with Mirror Option	Solid State Drive
Email SMTP Server	Supported with Optional External USB Hard Drive	Supported	Supported with Optional External USB Hard Drive
Email POP3 Server	Included	Included	Included
Email IMAP4 Server	Included	Included	Included
Unified Messaging	Included	Included	Included
Network Integration	LAN: Ethernet WAN: Ethernet, PPPoE	LAN: Ethernet WAN: Ethernet, T1, PPPoE	LAN: Ethernet WAN: Ethernet, T1, PPPoE
Automatic Call Distribution	10 queues; 16 total calls in all queues	10 queues; 32 total calls in all queues	10 queues; 32 total calls in all queues



Firewall Security	Stateful Packet Inspection	Stateful Packet Inspection	Stateful Packet Inspection
Call Assistant	Available	Available	Available
Mobile Link	Available	Available	Available
VPN	Available	Available	Available
Dual Language Support	English, Castilian Spanish, French Canadian available	English, Castilian Spanish, French Canadian available	English, Castilian Spanish, French Canadian available

## 2 Accessing Web Administration

The administrative interface to the Allworx server is accessed using a web browser via the LAN interface on 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.
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, log in using the default password: admin.

When the Allworx server mode is set to NAT/Firewall, NAT/Firewall with DMZ or NAT/Firewall with Stealth DMZ, the administrative interface to the Allworx server may also be accessed via the WAN interface on TCP port 8080. This feature is enabled by clicking the checkbox labeled "Allow admin configuration on WAN interface" on the Network Configuration page. After enabling this feature and rebooting the Allworx server, open your browser and enter the URL of <http://<Server WAN IP Address>:8080>.

Note: The WAN administrative option is not available with T1 or PPPoE WAN configurations.

## 3 Configuring a New Allworx Server

Log into the Allworx server Web Admin page. When the Home page appears, click on the [Install Checklist](#) link (on the left side) to bring up a new window that lists the steps necessary to set up a new system. Each step has a description that is followed by a link to the Web Admin page to execute the step. These steps are ordered to aid in a successful configuration. Most of the administrative pages for 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.

### 3.1 Feature Keys

Feature Keys allow access to advanced features that may be purchased separately from the base feature set for Allworx servers. Newly-purchased or existing keys issued for a specific Allworx server can be automatically downloaded from the Allworx key database and installed by selecting the Install button from the Maintenance / Feature Keys page.

[Home](#) > [Maintenance](#) > [Feature Keys](#)

**Feature Keys**

**Install**

keys from Internet (requires server access to the Internet)

**MAC Address:** 00-00-00-00-00-00

**Currently Installed Features:**

- Call Queuing
- Call Assistant
- Conference Center

**Installed Keys:**  
ehXg-Pgww-y\$u0-8vxn-ydQC-rYYP

**Enter new Feature Key:**

**TIP**

For information about purchasing additional Feature Keys please call 1-866-255-9679 (1-866-ALLWORX) , or visit [www.allworx.com](http://www.allworx.com).

**TIP**

Feature Keys are case sensitive. Uppercase and lowercase characters must be entered exactly as specified in the key.  
  
It is easy to confuse some characters (0 vs O, 1 vs l, for example). It is recommended that you cut and paste your feature key into the field above.

## Available Feature Keys:

### User Expansion Licenses

The maximum number of users on a given server model can be expanded beyond the base number by adding feature keys. These options do not require any additional software to be downloaded.

Key	6x	24x	48x
48 Users		X	
60 Users	X		
100 Users		X	X
150 Users		X	X
200 Users			X
250 Users			X

Call Queuing – provides the ability to direct inbound calls into queues. These calls will ring the phones of any designated users available to service the calls.

Automatic Call Distribution – Automatic Call Distribution is an enhanced queuing feature that directs calls in a queue to agents using a variety of call distribution algorithms. This key also enables the method described for the Call Queuing key. If the Automatic Call Distribution feature key is installed, the Call Queuing feature key is not required.

Note: For details on configuring and using Call Queuing and Automatic Call Distribution see the *Allworx Queuing and Automated Distribution Guide*.

Call Assistant – This key enables the Allworx Call Assistant and the TSP driver. The Allworx Call Assistant is a PC-based answering system which brings the power of enterprise attendant consoles directly to small business. An Allworx phone must be used with this software and additional software is required.

Note: TSP (Telephony Service Provider) is a separate PC driver that enables dialing from within the Microsoft Outlook contact list.

Conference Center – Allworx Conference Center provides conference bridges, a method of reserving the conference nodes for immediate or future use, and offers password-restricted access for attendees. This option does not require any additional software to be downloaded.

Hardware Maintenance – Obtaining this key through the Allworx Partner Portal places the Allworx server under a Hardware Maintenance agreement.

Mobile Link - This key enables interaction between the Allworx system and iAllworx. iAllworx is a free iPhone application that allows users to set their presence, review their conferences and receive and send voicemails.

Dual Language Support – Allworx Dual Language Support provides the ability to have a second language for default audio prompts. Language Packs containing the audio prompts in languages other than US English are available for download from the Allworx Partner Portal at [www.allworx.com](http://www.allworx.com).

Multi-Site Primary – Allworx Advanced Multi-site provides the ability to seamlessly integrate multiple sites. The Primary key enables a site to be the Controller site for the network. It also enables a larger number of BLF/DSS between sites than the Multi-site Branch key.

Multi-Site Branch – Allworx Advanced Multi-site provides the ability to seamlessly integrate multiple sites. The Branch key enables sites to join a network of sites. At least one site in the network must have a Multi-site Primary Key.

Software Maintenance – This key enables system software updates. Obtaining this key through the Allworx Partner Portal places the Allworx server under a Software Maintenance agreement.

T1/PRI License #1 (48x only) – Activates the T1-A port on an Allworx 48x system.

T1/PRI License #2 (48x only) – Activates the T1-B port on an Allworx 48x system. This does not include the license for the first T1. You must install T1 license #1 in order to activate the T1 #2.

Virtual Private Network (VPN) – Virtual Private Network (VPN) is used for remote and secure data access. This key is not required for opening a single-user remote diagnostic VPN. This option does not require any additional software to be downloaded.

Note: Feature Keys will activate features only on the Allworx server for which they are generated. Therefore, Feature Keys generated for one system cannot be used on any other system.

## 4 Upgrading Server Software

Before performing an upgrade, be aware that:

- If you are updating from Release 7.0 or lower, significant changes to multi-site networking have been made that require additional feature keys and configuration steps in order for site-to-site features to continue to operate. Multi-site networks will cease to function until all sites are updated, the new keys are procured and installed, and additional configuration is done on each site. Details of Release 7.2 Advanced Multi-site can be found in the Allworx Advanced Multi-site Setup Guide that is available for download on the Allworx portal.
- Downgrading from one release to an earlier release will result in undesirable behavior and is not supported.
- It is highly recommended that you perform an OfficeSafe backup prior to performing the upgrade (See Section 13, Backing up and Restoring Data).
- The upgrade will require a reboot of the server. Since this would cause disconnections and disruption of data, the system should be idle (no phone or data users) when the upgrade is done.

To upgrade the software on the server, go to the Maintenance / Update web administration page. Although most popular web browsers can be used for Allworx administration, Microsoft Internet Explorer 7 or higher is recommended for performing software upgrades.

### 4.1 Upgrade from Release 7.0 and Lower

When upgrading Allworx systems running System Software Release 7.0 or lower to System Software Release 7.2, it is necessary to first install Release 7.1. Refer to the Upgrading Server Software section of the Admin Guide that corresponds to the software currently loaded on the server for detailed instructions. If updating using manual FTP, note that the names of the files and the number of files in the upgrade package are different from those in prior updates.

**WARNING:** The upgrade to System Software Release 7.1 makes a number of system changes that cannot be undone. Take extra care to be sure that a viable backup is available in the event that a return to the original release is necessary.

Once System Software Release 7.1 has been installed, install Release 7.2 using the procedures in this document.

### 4.2 Upgrading from Release 7.1 to 7.2

To upgrade to Release 7.2, navigate to the Maintenance / Update page. There are two options: (1) Download update from web and (2) Upload update from PC.

#### Option 1: Download Update From Web

When 'download update from web' is chosen, the server will determine if new software releases are available. If either a new Production software release or a new Pre-production software release or both are available, the option to install them will be presented.

Choose the desired software version, and then select the **Download Update** button.

**Update**

**Current version:** 7.1.0.17  
**Build Date:** Dec 2 2009, 14:15:30

**Choose update:**

☒ **Production Release 7.1.0.19**  
☐ **Pre-production 7.1.0.20**

## Option 2: Upload update from PC

The update files can be downloaded to a PC from the Allworx portal ([www.allworx.com](http://www.allworx.com)) and then uploaded to an Allworx server. The use of FTP to put the software upgrade files on the server has been eliminated. Instead a single update file is uploaded onto the server through the Admin page. Select the Browse button to navigate to the location of the Allworx server software file that was downloaded from the Allworx portal. Choose the file and then select Open. On the Update page, select the Load button. The page will display the current version of software and the software version of the file that was loaded on the system. A warning message will be displayed for any inconsistencies such as:

- Update version is same or older than the currently-running version
- Update is intended for a different Allworx server model

## 4.3 Activating Server Software

Once software has been loaded onto the Allworx server, using either option explained above, the System Administrator can immediately activate the update, schedule the update to be activated at a later time, or cancel the update procedure.

**Update**

**Current version:** 7.1.0.14  
**Build Date:** Nov 10 2009, 13:01:38

**Activate Update**

Click "Activate Update" to update

Current version: 7.1.0.14  
Update version: 7.1.0.20

To schedule an update for a later time, select the **Activate Update Later** button. Enter the number of hours the server should wait before activating the update into the text box and then click the **Submit Schedule** button. The Update page will display the date and time the update is scheduled to occur.

**Update**

**Current version:** 7.1.0.10  
**Build Date:** Oct 8 2009, 10:54:21

**Active Update**

The following update is scheduled to occur at Tue Oct 20 02:12:44am 2009  
Current version: 7.1.0.10  
Update version: 7.1.0.11

Would you like to cancel the scheduled update?

## 4.4 Options after upgrading to 7.2

Once a system has been upgraded to Release 7.2, additional options are available for subsequent upgrades:

- **Reboot All Phones** – Choosing this option will cause all attached phones to reboot automatically after the upgrade is complete. One phone will reboot every 10 seconds until all have been rebooted.
- **Automatically update phone firmware** – Choosing this option will cause all rebooted phones to automatically install the phone firmware upgrade if the just-installed server load includes a newer phone version. The phone will allow five minutes for a user to cancel the upgrade using a phone softkey before installing the update.



## 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.



[About](#)

[Phone System](#)

[Business](#)

**[Network](#)**

[Configuration](#)

[Static Routes](#)

[Digital Lines](#)

[VPN](#)

[Servers](#)

[Reports](#)

[Maintenance](#)

[Need help?](#)

[Install Checklist](#)

[Logout]

[Home](#) > [Network](#) > Configuration

---

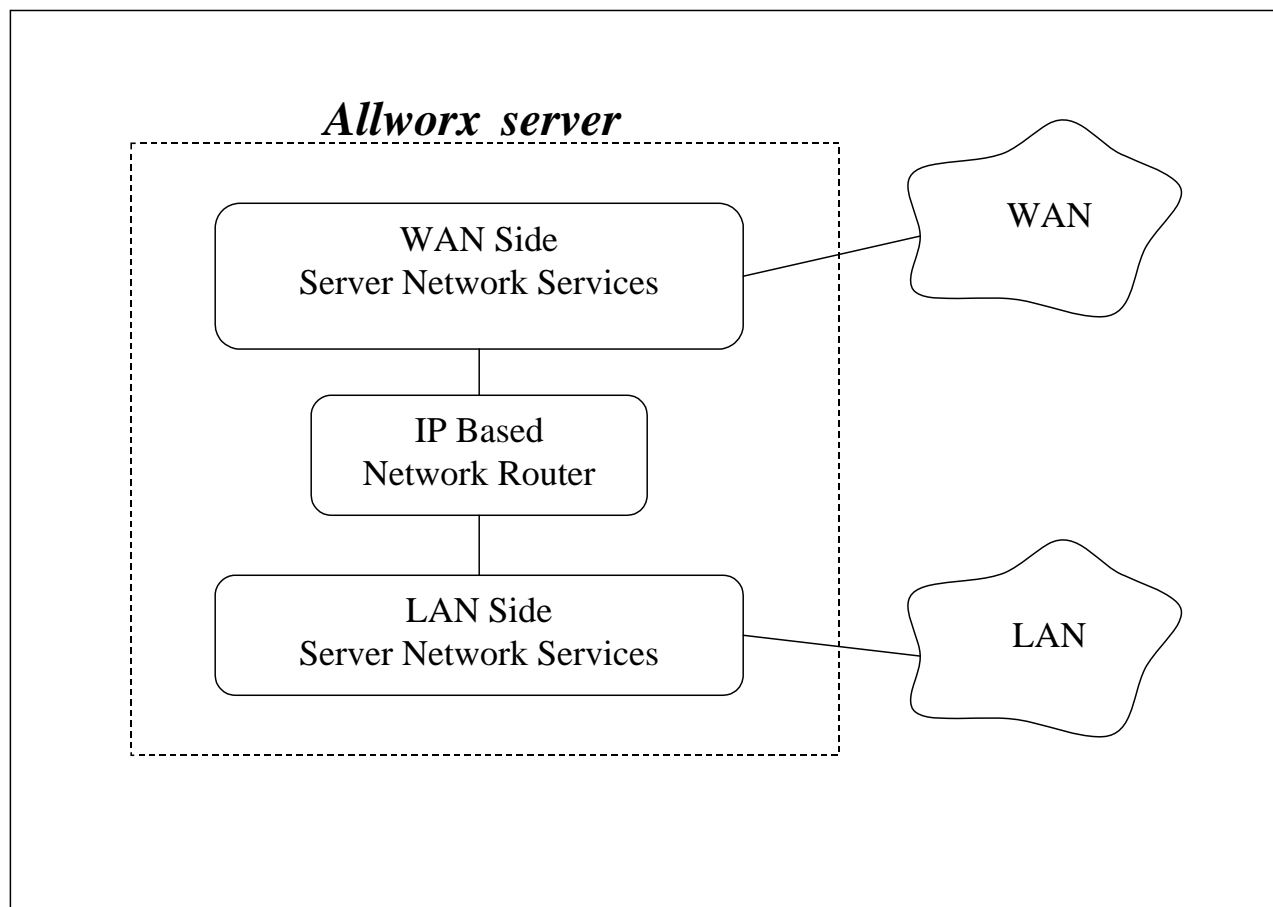
**Configuration**
[modify](#)

	Current Value
<b>Network Mode</b>	NAT/Firewall with DMZ
<b>LAN IP Address</b>	192.168.32.254
<b>LAN Subnet Mask</b>	255.255.255.0
<b>WAN Settings Method</b>	Static
<b>WAN IP Address</b>	192.168.1.1
<b>WAN IP Subnet Mask</b>	255.255.255.0
<b>Gateway</b>	192.168.1.254
<b>PPPoE Username</b>	
<b>PPPoE Service Name</b>	
<b>PPPoE MTU</b>	1492
<b>LAN Addresses and Ports exposed through Firewall</b>	
<b>DNS Server ( 53 )</b>	enabled
<b>DNS Client ( 4069 )</b>	enabled
<b>FTP ( 20,21 )</b>	disabled
<b>HTTP ( 80 )</b>	enabled
<b>POP3 ( 110 )</b>	enabled
<b>IMAP4 ( 143 )</b>	disabled
<b>Communications Center ( 1112,2112,2113 )</b>	disabled
<b>PPTP ( 1723 )</b>	enabled
<b>Remote Allworx Handsets ( 2088,8081 )</b>	enabled
<b>SIP ( 5060 )</b>	enabled
<b>SMTP ( 25 )</b>	enabled
<b>SNTP Client ( 4068 )</b>	enabled
<b>Host Name</b>	allworx
<b>Domain Name (DNS)</b>	allworx.inscitek.com

The Network Modes are described below.

## 5.1 Network Mode: Standard Router

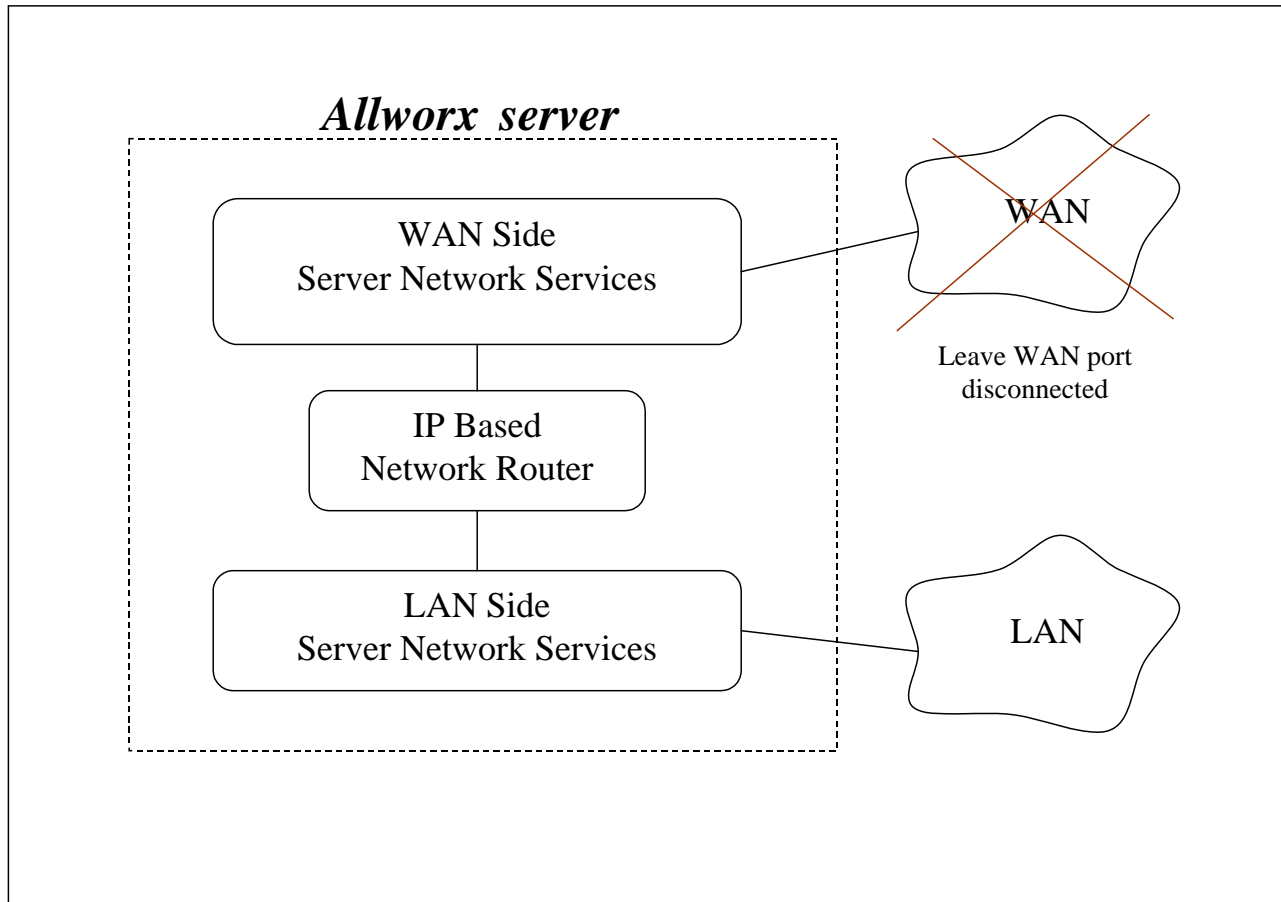
When the network mode is set to Standard Router, the logical network capability is as shown in the diagram below:



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 was 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.

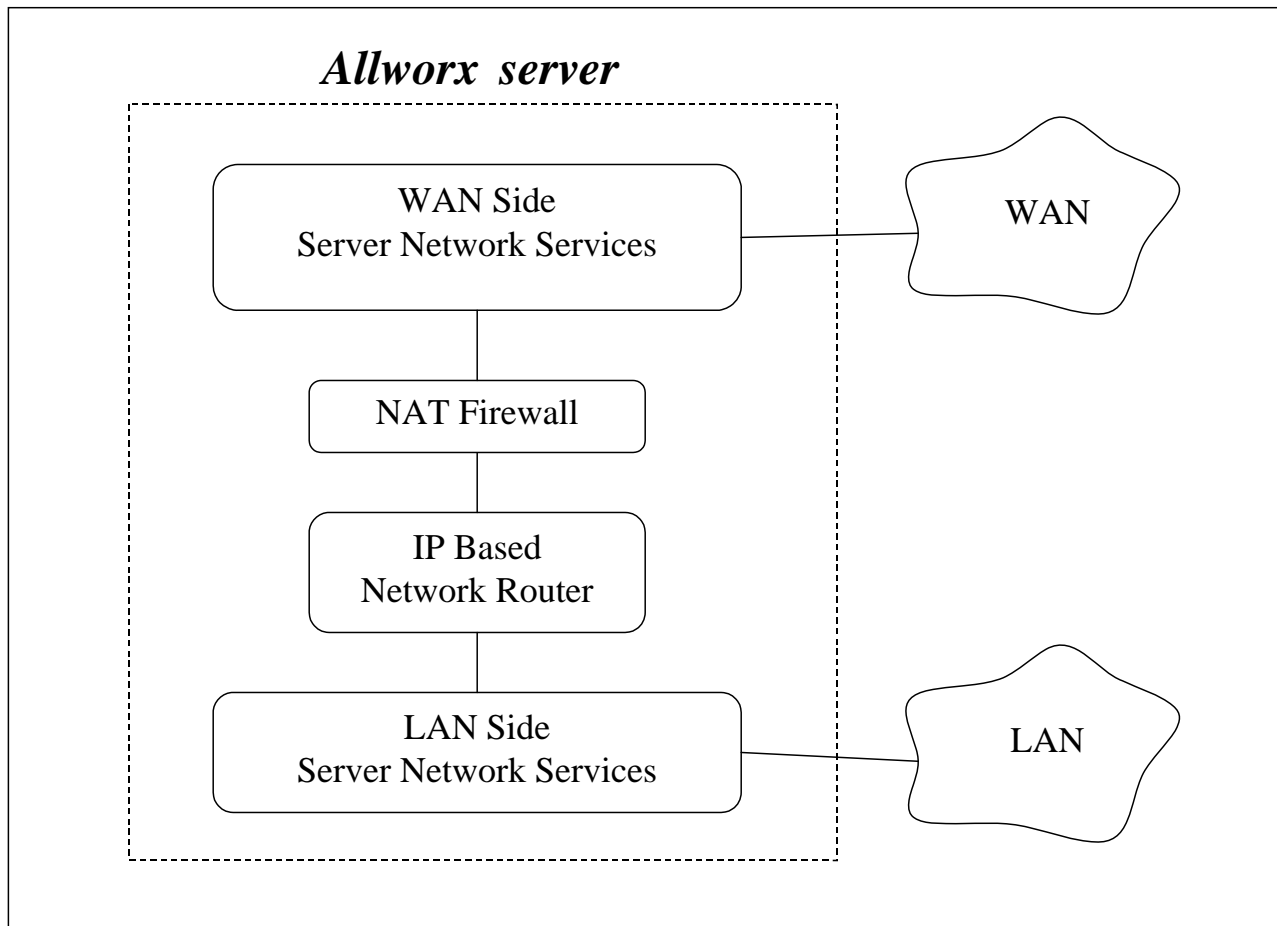
This mode is the same as Standard Router except that when the DHCP server is enabled, it will pass out the configured Gateway address (set on the Network / Configuration / Modify page) as the DHCP router (gateway) option instead of giving out the Allworx server's LAN address.

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:



For security purposes, this mode's default settings permit 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). Because of this, the addresses of devices on the LAN are not visible on the WAN, yet they have access to the WAN for outbound traffic. 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"/>
<input type="text"/>	TCP ▼	<input type="text"/>	<input type="text"/>

For example, if a PC on the LAN is hosting a website that must be accessible from the Internet, its http port (port 80) must be exposed through the firewall. To permit access to this web server, create a new entry, entering 80 for the WAN Port #. Choose TCP for the Protocol, enter the PC's IP Address (e.g. 192.168.101.9) and the Local Port # of 80.

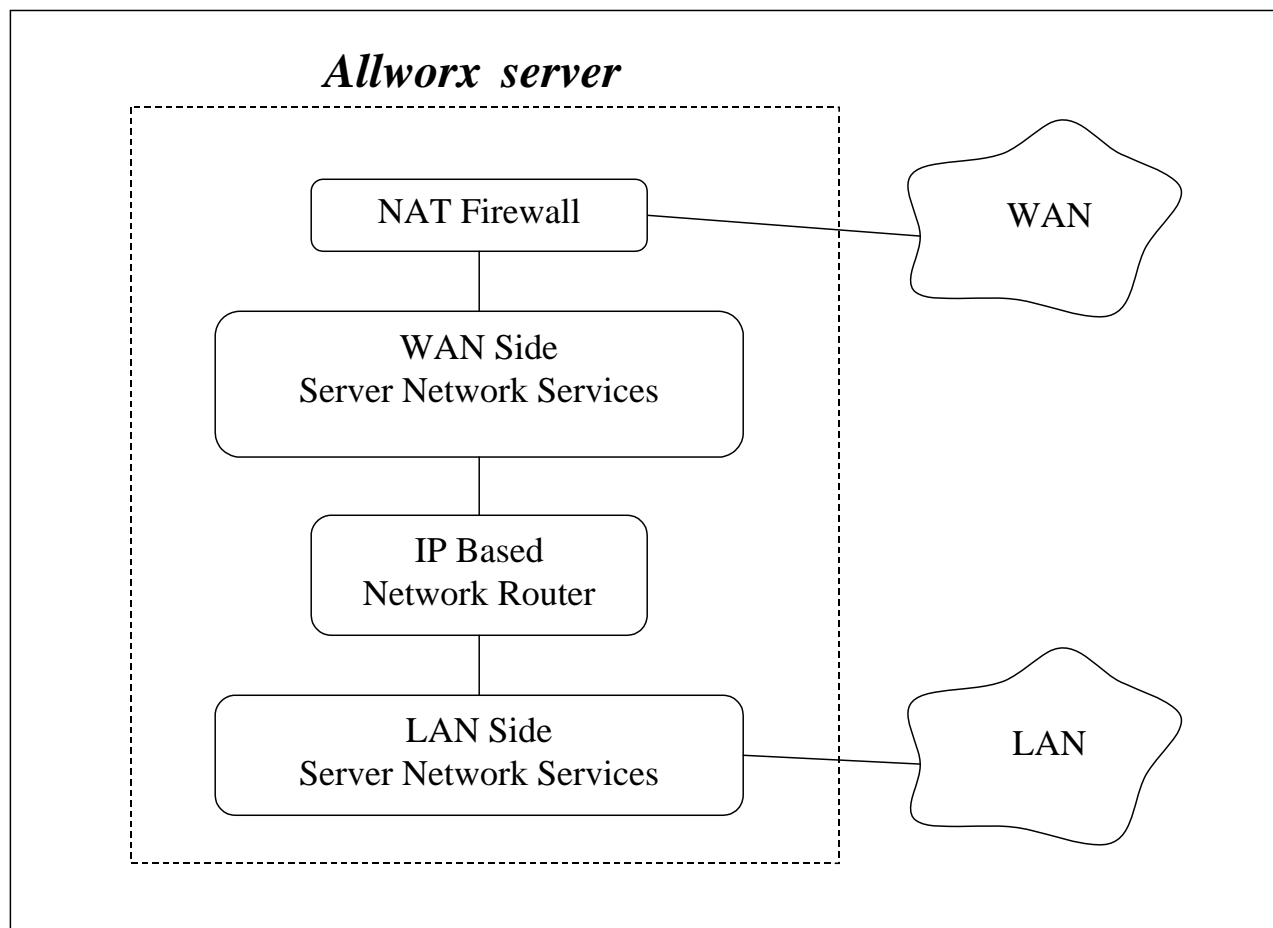
**Note:** The WAN and LAN Port #s must always be the same.

If port 80 of a PC on the LAN is exposed this way, the Allworx port 80 http service must be disabled. Uncheck the HTTP (80) checkbox in the Allworx Services section of the page. If the Allworx Internet web page is to be used, leave the Allworx HTTP box checked and change the http port on the PC to some other port number (e.g. port 5000).

Due to security requirements, the Allworx server's LAN IP address should not be used as an IP Address, in the table above. Port 8080 of the Allworx server is never exposed to its WAN interface. To access the Allworx LAN interface from the Internet, use the server's VPN feature, instead.

## 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 #
	TCP ▼		
	TCP ▼		
	TCP ▼		
	TCP ▼		
	TCP ▼		
	TCP ▼		
	TCP ▼		
	TCP ▼		
	TCP ▼		
	TCP ▼		
	TCP ▼		
	TCP ▼		

Allworx Services (ports) exposed through DMZ:	
<input checked="" type="checkbox"/> DNS Server (53)	<input type="checkbox"/> Communications Center (1112,2112,2113)
<input checked="" type="checkbox"/> DNS Client (4069)	<input checked="" type="checkbox"/> PPTP (1723)
<input type="checkbox"/> FTP (20,21)	<input checked="" type="checkbox"/> Remote Allworx Handsets (2088,8081)
<input checked="" type="checkbox"/> HTTP (80)	<input checked="" type="checkbox"/> SIP (5060)
<input checked="" type="checkbox"/> POP3 (110)	<input checked="" type="checkbox"/> SMTP (25)
<input type="checkbox"/> IMAP4 (143)	<input checked="" type="checkbox"/> SNTP Client (4068)

Note: The checkboxes are for specific Allworx services that can also be configured in the LAN address list. They are provided as a convenience as compared to filling in the list.

## 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. SNTP 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 Internal Dial Plan and Extension Length

The server admin interface permits administrators to change the number of digits (i.e. length) and numeric ranges of internal extensions.

The extension length setting configures extensions to be either three (3) digits or four (4) digits long. This capability influences other server features and has some limitations that are discussed below.

The Internal Dial Plan specifies the first digit for user extensions and other PBX functions such as forwarding calls and accessing outside lines. The dial plan can be configured to meet the needs of the customer by:

- Matching extensions to DID numbers
- Keeping extensions the same as they were prior to the introduction of the Allworx system
- Changing the PBX outside line access to a digit other than "9" to avoid accidental 911 calls

Both extension length and the internal dial plan affect many of the system's features. For this reason, it is recommended that these decisions be made and the options be configured early in the installation process.

### 6.1 3-Digit vs. 4-Digit Extensions

#### 6.1.1 Setting Extension Length

New Allworx servers are factory-configured for 3-digit extensions. If 3-digit extensions are to be used, no configuration change is required. If 4-digit extensions are to be used, it is recommended that the extension length be changed to four digits before any Users, Handsets, or Extensions are defined. Change the extension length using the following procedure:

1. Log into the server admin interface
2. Go to Phone System / Dial Plan
3. Under Internal Dialing Rules, choose the Modify link for User and System Extensions are 3 digits in length
4. Change the User and System Extensions to 4 digits in length
5. Click the Update link
6. If any handsets have already been configured, reboot them

#### 6.1.2 Extension Length Changes on Existing Systems

When an existing server with 3-digit extensions is switched to 4-digit extensions, the user and system extensions will automatically change to four digits. The server will add a one (1) to the start of each extension. For example, if a user had the extension x104, the extension will automatically be changed to x1104. A system extension of x231 will be adjusted to x1231.

Switching back from 4-digit extensions to 3-digit extensions is not recommended. If the switch is made, all extensions will be shortened to three digits by removing the first digit (e.g. an extension of x1205 will become x205). However, this can lead to conflicts (e.g. x1100 and x2100 would shorten to the same 3-digit extension). For this reason, switching from 4-digit extensions to 3-digit extensions will be prevented if there are any extensions outside the range of x1100-x1299. For sites using a non-default internal dial plan, all extensions must be in the range of x100 – x299. For example, if the site's extensions are 4xxx – 5xxx, all extensions must be in the range of 4100-4299, in order to switch to 3-digit extensions. If there are extensions

outside of this range but a switch from 4-digit extensions to 3-digit extensions is desired, all extensions that are outside the range must be changed or deleted.

The following phone functions are affected when the extension length setting is changed. The format of the number to dial is the same but the number of digits changes, depending on whether extensions are set to three digits or four digits.

Function	Format <sup>†</sup>	3-digit Example <sup>†</sup>	4-digit Example <sup>†</sup>
Leave a voicemail	3 + extension	3199	31199
Check voicemail	6 + extension	6199	61199
Call forwarding	45 + extension	45199	451199
Answer alternate extension	7 + extension	7199	71199

In addition to the changes in user and system extensions, the following server configurations are automatically modified when the extensions are changed from three digits to four digits:

- Extension call routes including Internal Caller-ID checking
- Incoming outside line call routes
- DID mappings
- System Speed Dials (the Speed Dial extension doesn't change but the extension that is dialed as a result changes)
- Speed Dial PFK (differs from Personal Speed Dial PFK)
- Default Extensions, extensions accessed by Shortcuts, and "Dial By Directory" listings of Auto Attendants
- Call Detail Records (prior records are unaffected by the change)
- Off hook digits dialed for handsets

## Functions Not Changed

The following are not affected:<sup>†</sup>

- Personal Speed Dials (these are stored on the phones so they must be modified by the users)
- System Speed Dial extensions (350-399, 34000-34999)
- Call Park extension and Parking Orbits (700-709)
- Auto-Attendant extensions (400, 431-439)
- Door Relay (403)
- Message Center (404)
- Conference Center (408)

<sup>†</sup> Extensions may vary per system. If you are using a non-default Internal Dial Plan, consult the Phone Features tab of the My Allworx Manager page to determine what extensions are being used for the corresponding feature.

- Paging extensions (460-469)
- Queue extensions (4400-4409, 4410-4419)

## 6.2 Modifying Internal Dial Plan

The Phone System / Dial Plan page includes a table of the Internal Dial Plan. The dial plan can be changed by clicking the [Modify](#) link.

[reset table to factory default dial plan](#)

		Plan
<input type="button" value="2,3"/>	2xxx 3xxx	User and System Extensions
<input type="button" value="0"/>	0	Operator
<input type="button" value="9"/>	9 + external number	External Call access (follows External Dialing Rules below)
<input type="button" value="8"/>	8 + enterprise number	Enterprise calling
<input type="button" value="5"/>	5nnn	Internal station access (reserved for system)
<input type="button" value="1"/>	150-199 14nnn	Speed dial numbers
<input type="button" value="6"/>	60nn + remote site extension 6 + user extension	Remote Site access Message Center
<input type="button" value="7"/>	700 call park 701-709 call retrieve 7xxxx call pickup 78 + pin code	Call Functions (park/pickup/audit pin code)
<input type="button" value="1"/>	1 + user extension	Leave a voicemail for extension
<input type="button" value="4"/>	403 door relay 408 conference center 42n do not disturb 43n auto attendants 44nn call queues 45xxxx call forwarding 46n paging	PBX Functions

The selections are made by choosing the leading digit for groups of dialing patterns from a pull-down list. Selecting a digit for one pattern affects the digits that are available for use with other patterns. As selections are made, the lists are automatically adjusted to include only valid remaining digits. For this reason, it is recommended that selections be made starting at the top of the page.

### Important Notes

There are a few rules about what can be changed:

1. The Allworx user guides frequently refer to dialing patterns based on the factory default Internal Dial Plan. When changes are made to the dial plan, the server's Phone Functions Reference Card is automatically updated with the new digits. We recommend printing and distributing this sheet to all end users. The page can be viewed by clicking the "[view the Phone Functions Reference Card](#)" link on the Dial Plan page.
2. Extensions must be a consecutive range of 200 numbers (or 2000, when using 4-digit extensions). The available ranges are: 100-299; 200-399; 300-499; 400-599; 500-699; 600-799; 700-899, 800-999.

3. The asterisk (“\*”) can be used as a leading digit for the PBX Functions group (e.g. Call Forwarding). It is not available as a choice for other functions.
4. When installing multiple sites with multiple Allworx servers, each server should be configured with the same internal dial plan. If the dial plans differ, routing of calls between the sites will not be reliable.
5. Changing the Operator to a digit other than “0” will not automatically change the Operator digit shortcut in the Auto Attendants. If the Operator digit is changed, the Auto Attendants shortcuts should be adjusted accordingly.

## 6.3 Multi-site Calling

For reliable calling between sites in a multi-site network, it is recommended that:

- All Allworx servers have the same software release installed.
- All Allworx servers have the same extension length.
- All Allworx servers have the same internal dial plan.

## 7 Adding Users

### 7.1 User Templates

User Templates contain a set of common configuration settings and can be applied when creating or modifying users. Not all user settings are included in the templates. Some settings must be configured for each user from their user modify page.

Available User Templates are displayed in a table in the Business / Users page, with options to View (modify), Copy, and Delete groups. The system includes a default "System User" template. This template contains the factory default user settings. When Allworx servers are upgraded to Release 7.0 or higher the System User template is assigned as the base template for all users. None of the settings for existing users are changed in this process. When new users are added, the System Administrator may apply the System User template or a custom template can be created for a desired combination of settings.

#### 7.1.1 Adding and Modifying User Templates

To add a new User Template, start by creating a copy of an existing group, such as the System User template. Click on the template's Copy link. This will create a new template with the same user options as the original.

**User Templates**

Name	Action
System User (Default)	<a href="#">View</a> <a href="#">Copy</a>
Copy of System User (Default)	<a href="#">View</a> <a href="#">Copy</a> <a href="#">Delete</a>
Marketing Template	<a href="#">View</a> <a href="#">Copy</a>
Sales Template	<a href="#">View</a> <a href="#">Copy</a> <a href="#">Delete</a>

The copy can be customized by clicking [View](#) to display the template, then clicking the [Modify](#) link. The template can be renamed and configured with a combination of settings that is appropriate for all or a subset of the site's employees. Then as the users are added, the template can be applied thus automatically configuring the user with the template's options. Prior to adding users on a new system, it is a good idea to determine what feature options are desired for which users (e.g. Off-site Access to Outside Lines or the ability to create conferences).

When modifying templates that have already been applied to users, changes are NOT automatically applied to the users of that template. In order to update the user settings, the template must be re-applied to each user with which it is associated.

When viewing a template, all users to whom the template has been applied will be listed at the bottom of the page.

#### 7.1.2 Adding New Users

When adding a new user, the feature configuration settings are not displayed until a template is chosen.

<b>Identification</b>	
<b>Login Name</b>	mcopper (must start with a letter; use only letters, digits, and underscores)
<b>Full Name</b>	Mary Copper
<b>Password</b>	•••• (at least 4 characters, use only letters and digits)
<b>Primary Extension</b>	1000 (select an unused extension from 1000 to 2999) <a href="#">show unused</a>
<b>Phone Assignment</b>	
<b>Phone</b>	Unassigned
<b>User Template</b>	
Select a new template for user settings	Make a selection
<b>NOTE</b> You must select a template before you	<div> <div>Make a selection</div> <div>Marketing Template</div> <div>Sales Template</div> <div>System User (Default)</div> </div>

Once a template is selected, the screen is populated with the template settings as well as other settings that are not part of the template. Any settings that are changed are automatically flagged with an exclamation point (!) to indicate that the template has been overridden.

The users table on the Users page displays the template that was last applied to each user. If any template settings for a given user have been overridden, the User Template name will be marked with an exclamation point (!). Clicking on the template name opens the template's View page.

### 7.1.3 Modifying Users

Settings for a given user can be modified by clicking the user's [Modify](#) link and making changes to the settings. However, if a new template has been created or if the user's existing template has been modified, the template must be applied (or re-applied) from within the user's Modify page.

<b>User Template Options</b>	
System User (Default) was the last template applied to this user.	
Select a new template to apply:	System User (Default)
Then choose <a href="#">Set</a> or <a href="#">Merge</a> to change:	System User (Default)
<b>System Features</b>	<div> <div>Copy of System User (Default)</div> <div>Marketing Template</div> <div>Sales Template</div> </div>

There are two options for applying a template, Set and Merge. First, the template to be applied must be selected from the User Template Options pull-down list. Click the [Set](#) link to apply all of the template's settings to the user. However, for users that have some template overrides, it may be desirable to maintain the overridden settings. In this case, use the [Merge](#) link. Merge will not change any settings that were overrides from the last template that was applied.

Whether [Set](#) or [Merge](#) is used, additional changes to settings can be made before clicking the Update button.

### 7.1.4 Deleting User Templates

User Templates can be deleted by clicking on their [Delete](#) links. However, templates that were last applied to any users cannot be deleted so their [Delete](#) links will not be displayed. Apply a different template to all associated users before attempting to delete it.

## **7.1.4.1 User Template Settings**

The following user settings can be configured within the User Templates:

### System Features

- Enable Voicemail
- Maximum Number of Voicemails
- User has permission for Off-Site Access to outside lines
- User has permission to send voicemail to all users (by dialing 9 from voicemail Send menu)
- Operator Extension (used when caller dials 0 when leaving voicemail)
- Voice Activity Detection
- User has permission to modify extension's call routes
- User has permission to create conferences
- User is a Call Queue Supervisor
- Call Assistant Active Calls [Brief Display / Full Display / Not Displayed]
- Call Assistant Recording Calls Allowed
- Maximum size Universal Inbox
- Default Language

### Follow Me Calling

- Password required to accept calls
- Require caller to record name

### Auto Attendant Selection

User is included in Dial-By-Name and Dial-By-Directory menus.

- Auto Attendant 1
- Auto Attendant 2
- Auto Attendant 3
- Auto Attendant 4
- Auto Attendant 5
- Auto Attendant 6
- Auto Attendant 7
- Auto Attendant 8
- Auto Attendant 9

### POP3 Mail Transfers

- Email and Voicemail messages
- Email message only
- No messages

### VPN Settings

- Allow VPN Settings

### External POP3 Accounts

- Poll Period

## **7.1.4.2 User settings that are NOT included in User Templates**

### Follow Me Calling

- Primary Phone (used for quick transfer from cell phone)

## Voicemail Notification and Escalation

- Notification and Escalation Disabled
- Notification Mode
- Escalation Mode

## VPN Settings

- VPN Password

## External POP3 Accounts

- Mail Server / Username on Mail Server / Password



## 8 Adding Handsets

### 8.1 SIP Phones

#### 8.1.1 Plug-and-Play

Allworx phones can be added to the system using plug-and-play installation. Once the network connection to the server is set up, the phones will register with the server the next time they reboot or power up. VoIP phones from other manufacturers can be manually added. See Section 8.1.3.2, Generic Phones.

Depending on the DHCP configuration on the site's LAN, some network configuration of the phone may be required:

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 Phone 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 difficulty configuring a phone, restore it to factory defaults and reapply the desired settings.*

When an Allworx IP phone is booted on the network, if a new version of phone software is available, the phone will ask if you would like to load the upgrade.

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.

An Allworx IP phone can be assigned to a user or replace an existing phone when it is first connected to the Allworx system. The following options are available:

- Assign a user to the phone (NOW / ADD). Select from the list of all system users or limit the list to those users with no phones assigned. Reboot the phone to complete the user assignment.

- Replace compatible existing Allworx phone (NOW / REPLACE). Select from the list of the all Allworx system phones. The phone web administration password, if any, is required to replace a phone. To view or change the password, navigate to Web Admin Servers / VoIP page. Reboot the phone to complete the phone replacement.
- Defer user assignment (LATER). The user assignment prompt will be displayed on subsequent reboot if the phone has not already been configured from within the Web Admin.
- Assign via the Web Admin (VIA WEB). The user assignment prompt will not be displayed on subsequent reboots.

## **8.1.2 Plug-and-Play Security**

Allworx handset plug and play installation provides a convenient method for adding phones to the Allworx server. However, this feature permits unauthorized users to add phones to the server without the knowledge of the System Administrator. The Allworx System provides security by permitting the System Administrator to disable plug and play installation of handsets.


The following options are available on the Servers / VoIP page:

### **Disable Handset Creates via LAN Plug and Play**

This option prevents handsets on the Allworx server LAN from installing by plug and play. By default, this option is unchecked, meaning plug and play is enabled. When checked, phones must be manually added on the Phone System / Handsets page.

### **Disable Handset Creates via WAN (Remote Phone) Plug and Play**

This option prevents handsets on the Allworx server WAN (i.e. remote handsets) from installing by plug and play. Installation is prevented, even if the remote handset is programmed with the server's plug and play secret key. By default, this option is unchecked, meaning plug and play is enabled. When checked, phones must be manually added on the Phone System / Handsets page.





VoIP Server 	
BLF Port	2088 (typically set to 2088, change if needed for firewall)
<input type="checkbox"/> Secure BLF	(typically not checked)
<input checked="" type="checkbox"/> Force Remote Phone audio through server	(WAN to WAN calls)
Plug and Play Secret Key	3751074287 (6 to 64 characters, use 0-9, and # characters)
Phone Administration Password	573659321 (0 to 16 characters, use A-Z, a-z, 0-9, and # characters)
Maximum Active Remote Calls	8 (set to at least 1, increase as WAN bandwidth allows)
Paging Base IP Address	239.255.10.0 (Multicast IP/UDP/RTP address, set to 224.0.0.0 through 239.255.254.245)
Paging Port	56586 (recommended set to between 49152 through 65534)
Paging Maximum Hop Count	1 (set to between 1 through 255)
Paging Maximum Duration	1 (set to between 1 through 30 minutes)
RTP Base Port	15000 (512 ports used, must be an even number from 15000 to 65024)
RTP DTMF Payload	96 (96-127)
<input type="checkbox"/> Disable Phone Creates via LAN Plug and Play <input type="checkbox"/> Disable Phone Creates via WAN (Remote Phone) Plug and Play	

Note: Any handsets that have been added to the system will plug-and-play, regardless of these settings.

## 8.1.3 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 before 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 [add 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"/>
<div style="border: 1px solid gray; padding: 5px;"> <p><b>TIP</b></p> <p>If an <i>Owner</i> other than 'admin' is selected the handset will automatically be added to the owner's <i>In Office</i> call route.</p> <p>If an <i>Extension</i> 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.</p> </div>	
Handset Configuration	
Model	Allworx 9224 
Login ID	<input type="text"/>
Password	<input type="password"/>
MAC Address	<input type="text"/>

Select the phone model and fill in the required fields.

## **8.1.3.1 Allworx Phones**

For Allworx phones, 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: 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.

## **8.1.3.2 Generic Phones**

If the phone is not an Allworx IP phone, 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: 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.

## **8.2 Analog Phones**

Plug the phone into one of the server's FXS phone ports reserved for Inside Phone Extensions. Lift the phone receiver so that the phone is off hook. Refresh the browser window. Your phone will now appear in the Analog Handsets section of the page. Hang up the phone receiver.

Analog phones that are plugged into Port Expander FXS ports do not automatically appear on the Handsets page. They must be added, manually.

## 8.3 Testing Phones

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

1. Dial 400<sup>†</sup> 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.

---

<sup>†</sup> Extensions may vary per system. If you are using a non-default Internal Dial Plan, consult the Phone Features tab of the My Allworx Manager page to determine what extensions are being used for the corresponding feature.

## 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.

Handset	Line	Owner	Caller ID	Identification	Action
<b>Allworx 9224</b>	<a href="#">PBX Station (Default)</a>			<a href="#">View Configuration</a> <a href="#">Add Call Appearance</a> <a href="#">Reboot</a> <a href="#">Replace</a>	
MAC: 00-0A-DD-80-01-46 <a href="#">192.168.2.3</a> :5060					
Alex Smith	1	asmith	Alex Smith	User ID: 5102 Login ID: 5102 (expires: Nov 24, 2009 10:21 am)	<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:

**PBX Station (Default)** – This is the Handset Preference Group that the handset is currently a part of. Clicking the link will display the settings of the group. See Section 9.6, Handset Preference Groups, for more information.

**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** – 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. A Reboot Allworx Phones button is provided to reboot all phones with one action. One handset will be rebooted every 10 seconds, until all phones have been rebooted.

**Replace** – 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.

**IP Address** – This is the IP address assigned to the handset. Clicking the link will open the Phone Administration page in a separate browser window. See Section 9.8, Phone Web Administration, for more information.

**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](#) link described above or manually from the station.

## 9.2 Why Multiple Call Appearances are 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 Function Keys (PFKs) 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 for each SIP handset can be viewed by clicking on its [View Configuration](#) link. In addition to summary information, the following settings are displayed:

- Programmable Function Keys
- Call Assistant Appearances
- Template Options
- Handset Preferences Group

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

## 9.4 Programmable Function Keys (PFKs)

For each PFK on the phone, there is a numbered row corresponding to the individual PFK. The PFK can be configured by clicking the drop down arrow and choosing one of the available functions. The following are the supported PFK types. Each type is described below.

- ACD Appearance

- Busy Lamp Field (BLF)
- Call Appearance
- Emergency Alert
- Call Monitor
- Call Supervision
- Day-Night Mode
- Function
  - Centrex Flash
  - Headset
  - Info
  - Park
  - Personal Speed Dial
  - Redial
- Line Appearance
- Messages
- Not Used
- Parking Orbit
- Queue Alarm
- Queue Appearance
- Speed Dial

## **9.4.1 ACD Appearance PFK**

The PFK is used to service calls in ACD queues. Users log in and out of ACD queues with this PFK. When logged in, the user can receive and answer calls from ACD queues.

## **9.4.2 Busy Lamp Field (BLF) PFK**

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.



### 9.4.3 Call Appearance PFK

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 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.

### 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.

### 9.4.4 Emergency Alert PFK

Handsets with this PKF will receive audible and visual alerts whenever an emergency call is made from any local or remote handset on the system. See Section 20, Emergency Support

, for more information.

### 9.4.5 Call Monitor PFK

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. See Section 24, Call Monitors, for more information.

### 9.4.6 Call Supervision PFK

Call Supervision allows a supervisor to train agents by listening in on their calls. In addition, supervisors can participate in calls by “barging in” and speaking to both parties. See Section 21, Call Supervision, for more information.

### 9.4.7 Day-Night Mode PFK

The PFK displays the status of Day and Night mode and can be configured to manually toggle between the modes. The LED is off when in Day mode and solid red when in Night mode. See Section 22, Day-Night Mode , for more detailed information.

### 9.4.8 Function PFK

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

Centrex Flash – Allows external calls to be transferred to external numbers without tying up CO lines connected to your Allworx server.

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.

Info – The button is used to get information regarding the other buttons on your phone.

Park – Allows a PFK to be programmed to perform the Park operation with a press of a button. When a Park PFK is defined, the Hold button can no longer be used to perform the parking operation and can only perform the dedicated hold function.

Personal Speed Dial – Dials a number that is programmed directly on the phone. The mapping of the Personal Speed Dial Numbers defined in the handset to the PFK is as follows. The uppermost Personal Speed Dial PFK is associated to the lowest Speed Dial entry number on the handset.

Redial – Redials the last dialed number. Unless the Line Appearance(s) Use of Dial Plan phone option is enabled, only Call Appearance-dialed calls can be redialed.

### 9.4.9 Line Appearance PFK

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.

## **9.4.10 Messages PFK**

The PFK automatically monitors the status of the designated user's Message Center voicemail inbox and when pressed, automatically accesses the inbox. The PFK LED turns red when there is a new message in the monitored inbox. Specify the user whose inbox is to be monitored when setting up the PFK.

## **9.4.11 Not Used**

No action. Select this choice to disable a previously-defined PFK.

## **9.4.12 Parking Orbit PFK**

The PFK can be mapped to one of the nine Parking Orbits. When calls are parked they are sent into a Parking Orbits 701 through 709<sup>†</sup>. Calls waiting in a parking orbit will time-out after 10 minutes causing the call to be redirected to the Auto Attendant. A PFK can be set up to answer a call in any one of the 9 Parking Orbits. See Section 25, Parking Orbits, for more information

## **9.4.13 Queue Alarm PFK**

The PFK is mapped to one of the 10 Call Queues in the system. It notifies the user of the queue's activity levels (number of calls in the queue and/or longest wait time). It can be configured to include an audible alarm with the queue's status displayed on the phone's LCD.

## **9.4.14 Queue Appearance PFK**

The PFK is mapped to one of the 10 Call Queues in the system. It automatically monitors the status of a Call Queue and can be used to answer calls that are in the queue.



## **9.4.15 Speed Dial PFK**

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



## **9.4.16 Enhanced PFK Administration**

















































With the introduction of the Allworx 9224 phone and Allworx Tx 92/24 Expander, it is possible to have up to 96 PFKs on a single phone. Enhanced PFK Administration provides a System Administrator with tools and flexibility in managing the PFKs of all Allworx phones.

## 9.4.16.1 Moving Up and Moving Down

On each handset's View Configuration page, every PFK has a Move Up  and Move Down  button. These buttons allow the Administrator to swap a PFK definition with the PFK above (Move Up) or below (Move Down) the selected PFK.

## 9.4.16.2 PFK Insert and Delete

Delete  or Insert  buttons are displayed next to each PFK. Clicking Delete eliminates the PFK and shifts all PFK definitions below it up by one location. As a result of the shift, PFK definition #1 in each bank of 12 shifts "up" to the bottom (to position number #12) of the bank to its left. The last PFK definition on the station becomes Not Used (position #12 of the last bank). Clicking the Insert button next to a PFK shifts all PFK definitions below it down by one position. As a result of the shift, PFK definition #12 in each bank of PFKs shifts "down" to the top (to position number #1) of the bank to its right. If the last PFK on the station (handset or Expander) was in use, its definition will "drop off" the end of the list and will no longer be configured.

Key	Type	Location
1	Busy Lamp Field (BLF) Alex Smith (Login ID:5103) <a href="#">change</a>	   
2	Speed Dial 408 - Conference Center <a href="#">change</a>	   
3	Speed Dial 4400 - Tech Support Tier 1 <a href="#">change</a>	   
4	Call Supervision Barge In (default mode at start of call) <a href="#">change</a>	   
5	Call Supervision Silent Monitor (default mode at start of call) <a href="#">change</a>	   
6	Day-Night Mode Display and Control <a href="#">change</a>	   
7	Messages System Administrator (admin) <a href="#">change</a>	   
8	Parking Orbit Orbit 701 Ring reminder for parked calls is disabled. <a href="#">change</a>	   
9	Not Used	   
10	Not Used	   
11	Call Appearance 000add810142 Ring Type: AUTO <a href="#">change</a>	   
12	Call Appearance 000add810142 Ring Type: AUTO <a href="#">change</a>	   

## 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 PFKs, 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 2.2 Quick Reference Guide* 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 Handset Preference Groups

A Handset Preference Group is a set of handset options and a list of handsets with those options. Handset Preference Groups allow handsets to be configured easily and efficiently. Custom configurations can be applied to any or all of a site's handsets by creating a Handset Preference Group, specifying the handset options, and assigning handsets to the group. Unlike with User Templates, no additional configuration steps are required to apply the options. Changes made to the group's settings take affect as soon as the handsets are rebooted.

The Handset Preference Groups are displayed in a table in the Phone System / Handsets page, with options to View (modify), Copy, and Delete groups. The system includes a PBX and Key System Default groups that contain the factory default handset options for their respective modes. New Handset Preference Groups are created for each unique combination of handset options for existing phones when Allworx servers are upgraded to Release 7.0 or higher. Phones with those options automatically become members of the corresponding group.

Note: Settings for existing handsets are NOT changed in this process.

**Handset Preference Groups**

Name	Action
PBX Station (Default)	<a href="#">View</a> <a href="#">Copy</a>
Key System Station (Default)	<a href="#">View</a> <a href="#">Copy</a>
Marketing HPG	<a href="#">View</a> <a href="#">Copy</a> <a href="#">Delete</a>
Preference Group #1	<a href="#">View</a> <a href="#">Copy</a>

## 9.6.1 Creating and Modifying Handset Preference Groups

To create a new Handset Preference Group, start by creating a copy of an existing group, such as one of the System Default groups, clicking on the existing group's [Copy](#) link. This will create a new group with the same handset options as the original group. The new group's name, settings, and handset assignments can be modified by clicking the [View](#) and then the [Modify](#) link on either the options section or the Handsets Assigned to Group section.

The SIP Handset table displays the Handset Preference Group of each handset. Clicking on the group name opens the group's View page.

## 9.6.2 Adding Handset Preference Group Options to Handset Templates

A Handset Template is a combination of a Programmable Function Key (PFK) setup and Handset Preference Group options. When a new phone is added, the "Active" Handset Template for its model (9212, 9224, etc.) is automatically applied. To incorporate a Handset Preference Group into a new Handset Template, navigate to the View Configuration page of an existing handset (Phone System / Handsets / View). Configure the PFKs, choose a Handset Preference Group, and click Save in the Template Options section. Refer to Section 9.7, Handset Templates for more information on creating and using Handset Templates.

## 9.6.3 Assigning Handsets to Handset Preference Groups

Handsets can be assigned to Handset Preference Groups in several different ways. When new handsets are added, they are automatically assigned to the Handset Preference Group that is in the active Handset Template. Therefore, if the factory default phone options are not appropriate for the site, time can be saved by creating a custom Handset Preference Group and incorporating it into a new Active phone template before adding the site's handsets.

Handsets can be manually added to Handset Preference Groups in two ways. The first is through the handset's View Configuration page. Select the [Modify](#) link of the Handset Preference Group section, choose a group, then select the Update button. The second way is from the Handset Preference Group page. Select the [View](#) link of a group and then the [Modify](#) link of the Handsets Assigned To Group section. Handsets can be viewed, added, and removed from a group. When a handset is removed, it is automatically moved to the server's PBX Station or Key System Station default group. To move a handset to a different group, select the checkbox associated to the handset from within the desired group's configuration page (View / Modify Handsets Assigned To Group) or apply a handset template with a different Handset Preferences Group.

**Handsets Assigned To Group**

Select a handset's check box to include it in the group. Clear a handset's check box to remove it from the group.

<input type="checkbox"/>	<b>Alex Smith</b> (MAC:00-0A-DD-82-00-20)
<input checked="" type="checkbox"/>	<b>Jane Allright</b> (MAC:00-0A-DD-81-01-42)
<input checked="" type="checkbox"/>	<b>Mary Copper</b> (MAC:00-0A-DD-80-01-27)
<input type="checkbox"/>	<b>Noel A Umbridge</b> (MAC:00-0A-DD-82-9F-D4)
<input type="checkbox"/>	<b>Peter Albright</b> (MAC:00-0A-DD-81-01-E3)
<input type="checkbox"/>	<b>Thomas Annabel</b> (MAC:00-0A-DD-82-5B-C2)



## 9.6.4 Deleting Handset Preference Groups

Handset Preference Groups can be deleted by clicking on their Delete links. However, default groups and groups that have handsets assigned to them cannot be deleted. Therefore, all handsets must be moved into other groups in order to delete the group.

## 9.6.5 Handset Preference Group Settings

The following is the list of settings that can be configured within a Handset Preference Group:

- Station Mode
- Call Assistant / TSP Driver (TAPI) Display\*
- Call Assistant Display Mode
- Call History Size\*
- Clock Mode\*
- Codec Preference Order
- Daylight Saving Time
- Hold Button Mode\*
- Hold Reminder Mode\*
- Hold Reminder Timeout\*
- Jitter Buffer Size
- Message Waiting Indication
- Missed Call Tracking
- Off Hook Digits Dialed
- Paging Mode\*
- Redial Memory\*
- RTP Media Port Range
- SIP NAT Keep-alive Interval
- SIP Port
- Time Zone
- Audible Dialing\*
- Auto On Hold\*
- Auto Retrieve Calls\*
- Call Supervision
- Call Timer Display\*
- Caller ID Display
- Configuration Menu
- DTMF Payout
- Intercom Auto Answer\*
- Keypad Dialing
- Line Appearance(s) Use Dial Plan
- Off Hook Auto Answer\*
- Off Hook Ringing\*
- On Hook Dialing\*
- Visual Ringing\*

\* indicates settings that can be overridden from within the on-handset configuration menus.

Many of these options are easily understood from the web page. However, some of the more complicated ones will be described next.

## 9.6.6 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 as described in Section 9.4, Programmable Function Keys (PFKs).
- 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 Assistant / TSP Driver (TAPI) Display – Selects which call information is displayed in the Call Assistant and in TAPI-compliant PC applications that receive calls using the TSP driver. The phone may be configured to cause these applications to display either dialed name/number or regular caller ID name/number information but not both.

Call Assistant Display Mode – Controls how this phone is displayed in Call Assistant Directory tab. The options are:

- Normal – The extension and the phone's status are displayed
- Hide Status – The extension is displayed and the phone's status always shows as Idle
- Hide Completely – Neither the extension nor the status is displayed.

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: This setting defines the order of codec selection. Not all codec's are supported for all call types (for example, accessing the server Auto Attendant requires G.711). The phone will attempt to use the first choice but will use whichever codec is required to support the call.

Daylight Savings Time – Specifies if the handset will use Daylight Savings Time (DST) to compute its local time. Select Use Current Server Setting if the telephone is in the same time zone as the server. For a remote phone, you may want to use the DST setting of its actual location.

Hold Button Mode – Controls the behavior of the phone's Hold button:

- Hold Calls, Park Lines – Holds calls on call appearances. Parks calls on line appearances
- Hold then Park – If pressed and released quickly, the call is held. If the button is pressed for longer, the call is parked
- Park then Hold – If pressed and released quickly, the call is parked. If the button is pressed for longer, the call is held



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 whenever 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.

Hold Reminder Timeout – If Hold Reminder mode is Timer, this is the length of time (in seconds) before the call beeps.

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 voicemail 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.

Missed Call Tracking – Display the number of calls missed since last making or receiving a call. Select which missed calls to track:

- Call Appearances Only
- All Appearance Types

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<sup>†</sup> to get an outside line.

Note: 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' (e.g. 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.

---

<sup>†</sup> Extensions may vary per system. If you are using a non-default Internal Dial Plan, consult the Phone Features tab of the My Allworx Manager page to determine what extensions are being used for the corresponding feature.

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 Port Range – 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 Chapter 14, Remote Allworx Phones, for more information

SIP NAT Keep-alive Interval – Some NAT firewalls will automatically time out and close connections to devices it protects. If a remote phone is behind such a firewall, then this setting prevents the timeout. Messages called keep-alive packets are sent from the phone to the Allworx server at the frequency specified. The value should be set to an interval that is shorter than the firewall timeout.

SIP Port – This is the UDP port number used for the SIP protocol by the phone. The default value of 5060 should be used unless the port expander is behind a 3<sup>rd</sup>-party firewall and the network requires a different value.

Time Zone – Specifies the time zone that the handset uses to compute its local time. Select Use Current Server Setting if the telephone is in the same time zone as the server. For a remote phone, you may want to use the time zone of its actual location.

#### *Checkbox parameters*

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

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.

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.

Call Supervision – When enabled, the handset can be monitored by another handset that have a Call Supervision PFK.

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

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

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.

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

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.

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.).

**Line Appearance(s) Use of Dial Plan** – If not enabled, the phone number that is 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 Section 11, Dialing Rules and Service Groups).

**Off Hook Auto Answer** – If enabled, the phone answers any new call when it goes off hook.

**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.

**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.

**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 Handset 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>
Allworx 9212	9212 (Factory - Key)	<a href="#">View</a> <a href="#">Activate</a>
Allworx 9212	9212 (Factory - PBX) <b>[ACTIVE]</b>	<a href="#">View</a>
Allworx 9202	9202 (Factory) <b>[ACTIVE]</b>	<a href="#">View</a>
Allworx 9224	9224 (Factory - Key)	<a href="#">View</a> <a href="#">Activate</a>
Allworx 9224	9224 (Factory - PBX) <b>[ACTIVE]</b>	<a href="#">View</a>

### 9.7.1 Default Handset 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 Handset 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 Handset 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. The template will include the PFK setup and the Handset Preference Group from the phone.
3. Save the current configuration as a template by clicking Save in the Template Options section of the View Configuration page.

Template Options	
Save	this handset configuration in a template
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 Handset Template

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.

The phone will be configured with the PFK setup from the template and will be assigned to the Handset Preference Group.

## 9.7.5 Deleting a Handset Template

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

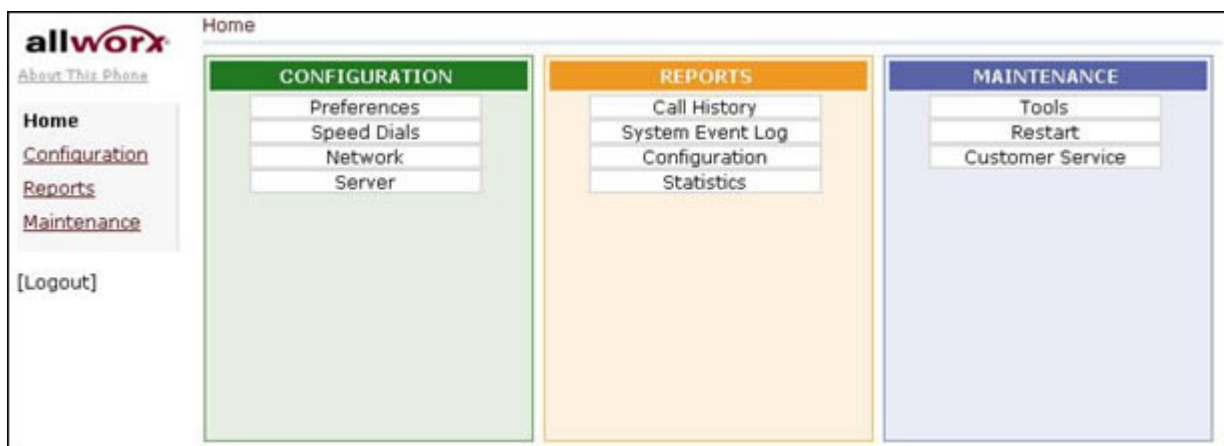
## 9.7.6 Modifying a Handset Template

Handset templates can be saved, applied, and deleted but cannot be directly modified. To modify a handset template, 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.


## 9.8 Phone Web Administration

Each handset can be accessed through a web interface in order to:

- View stored configuration information of the handset
- Modify the handset's configuration and personal speed dials
- View information (event log, call history, phone configuration parameters)



The Phone Web Administration page has the same look and feel as the server Admin page. However, the password used to access the phone admin page is NOT the same. To view the Phone Web Administration page password, navigate to Servers / VoIP page. To change the password, select the Modify link.

VoIP Server  [Modify](#)

	Current Value
BLF Port	2088
BLF Secure	disabled
Force Remote Phone audio through server	enabled
Plug 'n' Play Secret Key	3751074287
Phone Administration Password	573659321
Maximum Active Remote Calls	8
Paging Base IP Addr	239.255.10.0
Paging Port	56586
Paging Max Hop Count	1
Paging Maximum Duration (minutes)	1
RTP Base Port	15000
RTP DTMF Payload	96
Phone Creates via LAN Plug and Play	enabled
Phone Creates via WAN (Remote Phone) Plug and Play	enabled

There are two ways to access the administration page of an Allworx handset.

1. From the Server Admin page, navigate to the Phone System / Handsets page, and then click the IP address link associated with the handset
2. From a browser, enter the IP address of the handset. The IP address can be found on the handset under CONFIG / Current Status / Info

## 10 Outside Lines

### 10.1 Anonymous Call Handling

Anonymous Call Handling provides the System Administrator with a way to handle calls for which the caller has requested privacy. Such calls can be routed to a specific extension.

Navigate to Phone System / Outside Lines and select the modify link to configure Anonymous Call Handling. Private calls can either be routed normally on the system or to any user or system extension, including the operator.

**Anonymous Call Handling**

**NOTE**  
 Anonymous Call detection requires that Caller ID information is received and that it specifies that the calling party has requested privacy. Anonymous calls are routed by the server according to the selection below.

**Anonymous calls are:**

☒ **Routed normally**

☐ **Routed to extension** 0 - Operator

Note: Not all ITSPs support Anonymous Call Handling.

### 10.2 Allworx Port Expanders

The Allworx Px 6/2 Expander provides expansion of the system's analog capability by adding six (6) FXO and two (2) FXS ports to any Allworx server. The Px 6/2 Expander features plug-and-play installation for locally-connected units. Remote installation is possible using an approach similar to installing remote Allworx phones. For detailed installation instructions, see the *Allworx Px 6/2 Expander Installation Guide*.

Settings that apply to the port expander, overall are available on the Port Expanders page. Use the following information to configure these settings on installed Allworx Px 6/2 Expanders:

To configure Allworx port expanders, go to the Port Expanders section of the Network page.

[Home](#) > [Network](#) > [Port Expanders](#)

**Port Expanders**

[add a Port Expander](#)

**Px1: 000ADD022009** (Px 6/2 Expander)
 [Delete](#)
[Replace](#)
[Handsets](#)
[Outside Lines](#)

IP Address	MAC Address	Last Reboot Time	
<a href="#">192.168.2.2</a>	00-0A-DD-02-20-09	Apr 23, 2008 06:16 pm	<a href="#">Reboot</a>

This shows a list of all Allworx port expanders known to the Allworx server. A number of functions are available by clicking port expander-specific links.



Port Expander Functions:

Description/View Configuration – Clicking on the port expander's Description opens its configuration page. This allows you to view and modify the configuration.

Delete – Delete the port expander. All related configurations and port definitions are removed from the system.

Replace – This allows the port expander to be replaced by another while automatically transferring all the configuration parameters and settings to the new unit. This is typically used when replacing a defective port expander with a new one.

Handsets – Clicking this link jumps to the Handsets page where port expander FXS ports can be configured.

Outside Lines – Clicking this link jumps to the Outside Lines page where port expander FXO ports can be configured.

IP Address – Clicking on the IP address will open the port expander's web admin page in a separate browser window or tab. Use this link to view the port expander's event log or view/modify its on-board settings.

Reboot – Clicking this button will reboot the Port expander. Port expanders must be rebooted after configuration changes are made to the expander or any of its ports. When the button is clicked, the reboot will start as soon as all of the port expander's ports are idle.

## 10.2.1 Port Expander Options

Clicking on the port expander's Description opens its View Configuration page. This page is used to show and modify the options for that port expander. To change the configuration, click the Modify link. Other options are identical to those on the Port Expanders page.

The following configuration items are listed:

MAC Address – This is the hardware identifier for the port expander. It cannot be changed.

IP Address – This is the network address for the port expander. Clicking on it will open the port expander's web admin page in another browser window or tab. The IP address cannot be changed.

Description – This is the name given to the port expander. During plug-and-play installation, the Description is set to the port expander's MAC address. Changing it to something more meaningful to the site or configuration is recommended.

Codec Preference Order – Sets the preferred codec order for the port expander. The codec is the method of encoding/decoding the audio sent and received. 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:** This setting defines the order of codec selection. Not all codec's are supported for all call types (for example, accessing the server Auto Attendant requires G.711). The port expander will attempt to use the first choice but will use whichever codec is required to support calls.



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 port expander the most secured from snooping and denial of service activities. However, when remote port expanders are placed behind 3<sup>rd</sup>-party firewalls, under certain conditions the UDP port range may need to be restricted so that mapping rules can be created for each port expander behind the firewall. See Section 14, Remote Allworx Phones, for more information.

SIP NAT Keep-alive Interval – Some NAT firewalls will automatically time out and close connections to devices they protect. If a remote port expander is behind such a firewall, then this setting prevents the timeout. Messages called keep-alive packets are sent from the port expander to the Allworx server at the frequency specified. The value should be set to an interval that is shorter than the firewall timeout.

SIP Port – This is the UDP port number used for the SIP protocol by the port expander. The default value of 5060 should be used unless the port expander is behind a 3<sup>rd</sup>-party firewall and the network requires a different value.

Time Zone – Specifies the time zone that the handset uses to compute its local time. Select Use Current Server Setting if the port expander is in the same time zone as the server. For a remote port expander, you may want to use the time zone of its actual location.

Daylight Savings Time - Specifies if the port expander will use Daylight Savings Time (DST) to compute its local time. Select Use Current Server Setting if the port expander is in the same time zone as the server. For a remote port expander, you may want to use the DST setting of its actual location.

Jitter Buffer Size – Jitter is a variation in network audio packet latency experienced by the port expander, resulting in a reduction in audio quality. The port expander 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.

## **10.2.2 Configuring FXO and FXS Ports**

Once a port expander is installed, its FXS and FXO ports can be configured on the Handsets and Outside Lines pages, just like the server's own ports. On the Dial Plan page, port expander FXO ports are automatically added to the default service groups. New custom service groups can be created or existing ones modified to include the port expander's FXO ports.

## **10.3 Fax Server Support**

Allworx Systems provide the ability to send control information in the form of DTMF digits to devices connected to the servers FXS ports. An extension phone number and/or the dialed number (DNIS) along with arbitrary DTMF characters can be used to control the following devices:

- Analog FAX servers (e.g. Multi-Tech FaxFinder)
- External paging amplifiers
- External voicemail servers

The digits will be sent immediately after the device answers and before any audio from the calling source is available.

To add the device and configure which DTMF digits will be sent, navigate to Phone System / Handsets page.

1. Select the New Analog Handset link for the desired port
2. Add a description of the device

3. Click **Add** button
4. Select the Modify link for the device
5. Enter the DTMF digits to send into the Auto Answer DTMF String text box. These digits will be sent to the FXS device as soon as it answers the call. The following characters can be used:
  - DTMF digits:
    - 0 – 9
    - A – D
    - \*
    - #
  - Timing controls:
    - P generates a one second pause
    - + increases the duration and gap of all DTMF tones by 50ms
    - - decreases the duration and gap of all DTMF tones by 50ms
  - Variables:
    - \$xN sends the last N digits (0 for all digits) of the dialed extension
    - \$nN sends the last N digits (0 for all digits) of the DNIS number

For the device to receive incoming calls, an outside line must be routed to the port to which the device is attached. To route an outside line to the device:

1. Create an extension that rings the port of the device
2. Route an outside line to the extension

Note: For specific device setup instructions for the Multi-Tech FaxFinder, please refer to the application notes, located on the Allworx Partner Portal at [www.allworx.com](http://www.allworx.com).

## 10.4 SIP Proxies and SIP Gateways

The Allworx servers support connectivity to external SIP-compliant devices such as Internet Telephony Service Provider (ITSP) servers and SIP gateways. The Allworx products interface with four different types of SIP devices based on how they interact with the Allworx system:

SIP Proxy – A SIP Proxy refers to a SIP Trunk, an external SIP service for routing calls. The SIP Proxy is accessed through the Internet or through the wide area network (WAN). To connect to a SIP proxy (or ITSP), it must be configured on the Allworx server. Application notes for configuring Allworx servers with approved ITSPs are available on [www.allworx.com](http://www.allworx.com)

SIP Gateway – A SIP Gateway is a SIP-compatible device that extends the connectivity of the Allworx PBX. Examples are FXO, FXS or T1 expander gateways. Typically, SIP Gateways connect to the Allworx server via an Ethernet interface directly to the Allworx server LAN.

SIP Handsets – A SIP handset is a SIP-compatible phone that registers with the Allworx server. See Section 8, Adding Handsets for information about connecting Allworx or 3<sup>rd</sup>-party SIP handsets.

Remote Allworx – A Remote Allworx is an Allworx server at another site that is configured to behave as if it is part of the local system. The remote system need not be the same server model as the local Allworx system but it must be running the same software version and must be using the same number of digits for its extensions.

SIP Gateways and SIP Proxies are different but are configured in a very similar manner. Both types of devices are added to the system through the Phone System / Outside Lines page.

## 10.4.1 Configuration

SIP Proxies and SIP Gateways have configuration settings that are specific to the ITSP or device being used. To configure a new SIP Proxy, click the [add new SIP Proxy](#) link. It will open a page with parameters that need to be configured specifically for the ITSP service being used. Use the [add new SIP Gateway](#) link to define a new gateway. Once a SIP Proxy or SIP Gateway is defined on the Outside Lines page, it is necessary to enter the configuration screen again to configure Advanced Settings. Click the [Modify](#) link to make adjustments to the Advanced Settings.

## 10.4.2 Details about SIP Proxies

### Account Settings

**Description** – This field is used to assign a name to the SIP Proxy. It can be the ITSP name or any name that is useful to the System Administrator.

**User ID** – The ITSP typically assigns this value. This ID is often the phone number for the account.

**SIP Server** – This is the DNS name or IP address of the proxy server you are connecting to. This is obtained from the ITSP. A port number is usually 5060 but it should be verified with the ITSP.

**Outbound Proxy** – This is the DNS name or IP address of the outbound redirect server if it is different from the SIP Server. In many cases this is not required.

**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 Caller ID name that will be used for outbound calls. Some ITSPs may ignore this or refuse calls if set.

**Caller ID Number** – The Caller ID Number that will be used for outbound calls. Some ITSPs 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 here is fewer than the number of digits dialed by the user, only the trailing digits are sent. The default value (all digits) is typical.

Default Language (Requires the Dual Language Support feature key) – This is the choice of languages that will be used for Allworx audio messages and greetings that are played for inbound calls through the SIP Proxy.

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

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 Section 10.4.3, Enterprise Dialing Feature, below for more information.

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.

## **Advanced Settings**

These settings are specific to the ITSP. For instructions on configuring them for Allworx partner ITSPs, download the ITSP Application Notes from [www.allworx.com](http://www.allworx.com).

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 proxying of audio traffic (see Servers / VoIP Server). Typically this checkbox is not checked.

Use SIP Diversion for deflected calls - Some service providers support the SIP "Diversion" header (draft-levy-diversion-08.txt) to identify the proxy account when transferring or deflecting calls that include Calling Party information.

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.

Use E.164 format for phone numbers - Enabling this feature causes rewriting of phone numbers into the international E.164 format (e.g. 800-555-1212 becomes +18005551212). Typically this is unchecked unless required by the ITSP.

Offer '100rel' support - Used to indicate the Allworx supports 'reliability of provisional responses (RFC 3262)'. Typically this checkbox is enabled.

Obtain DID/DNIS number from [source] – For inbound calls, this describes where the server should get DID and DNIS information from. 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 Uniform Resource Identifier (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].

## 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 Section 10.4.2, Details about SIP Proxies, for more information about the common fields. Parameter information specific to SIP Gateways is detailed here.

Gateway uses SIP Registration – If the gateway supports registration, choose this option. Assign an arbitrary Login ID and Password for the gateway to use to register with Allworx. 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).

## 10.4.3 Enterprise Dialing Feature

The Enterprise Dialing feature allows a *third party* SIP server to be the central hub for calls between multiple sites that have Allworx servers. This provides a centralized phone book and administrative service for the entire VoIP network.

### 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<sup>†</sup> 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.

## **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 (using 3-digit extensions):

Enterprise Extension <sup>†</sup>	User	User Extension <sup>†</sup>	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<sup>†</sup> 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<sup>†</sup> 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

<sup>†</sup> Extensions may vary per system. If you are using a non-default Internal Dial Plan, consult the Phone Features tab of the My Allworx Manager page to determine what extensions are being used for the corresponding feature.



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.

## **How to Set Up Enterprise Dialing**

1. Go to the Phone System / Outside Lines page.
2. Either Add New SIP Proxy or, if it has already been added, Modify the 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:** 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.

## **10.4.4 Limitations with SIP Outside Lines**

The following calling features are not available when SIP trunks or SIP Gateways are used:

- Consultation and call transfer (using \*# or \*7) by recipients of Follow-Me-Anywhere call routes.
- Disconnection (hang up) of calls (using \*#) when accessing outside lines through the Message Center.

However, these features ARE available when one of the parties in the call is using an Allworx phone or port expander.

## **10.5 Digital Lines**

Allworx refers to the integrated T1 interfaces on Allworx 24x and 48x servers as Digital Lines. The Allworx 24x and 48x servers have two T1 Digital Line interfaces that are accessed through the connectors labeled T1-A and T1-B. There are differences in T1 port functionality between the 24x and 48x servers.

### Allworx 24x

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-A interface also supports Robbed Bit Signaling (RBS) operation. 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.

### Allworx 48x

One or both of the T1 interfaces can operate as Primary Rate ISDN lines, Robbed Bit Signaling (RBS) lines and/or as T1 data lines for connectivity to another site or to an Internet Service Provider. That is, the

interfaces support both circuit switched voice calls and TCP/IP data. 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.

## **PRI Support**

The Allworx server 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.

## **NFAS Support**

Non-Facility Associated Signaling (NFAS) is a PRI where multiple T1 lines share the same D channel. The Allworx server supports NFAS using the National Standard ISDN, Lucent Custom 4ESS, Lucent Custom 5ESS, Nortel DMS-100 switch types.

**Note:** The configuration must match the provisioning defined by the Central Office. A typical configuration has 23 B channels on slots 1 through 23 and one D channel on slot 24 of the primary T1 line, plus 24 B channels on slots 1 through 24 of the secondary T1 line. To configure NFAS on the Allworx system, the NFAS line with the D channel must be connected to the T1-A port.

## **Robbed Bit Signaling (RBS) Support**

The Allworx server supports classical T1 Robbed Bit Signaling (RBS) trunk lines on a time slot by time slot basis. Sometimes this functionality is referred to as T1 Channel Associated Signaling (CAS). The following modes are supported:

- FXO Loop-Start
- FXO Ground-Start
- E&M Wink Start
- E&M Feature Group B
- E&M Immediate Start

For the above selections, operational use is basically the same as the corresponding analog interface types. The precise signaling protocols for each interface are implemented in conformance with the procedures documented in EIA/TIA-464C. Inbound Caller-ID is supported on the FXO modes, if the CO supports it and the check box is enabled on the Outside Lines / Digital Lines / Modify page.

For primary CO line connectivity, the FXO Ground-Start slot choice is typically preferred to minimize the possibility for glare conditions, especially when call volume is high. Furthermore, it is not guaranteed that the network provides an explicit disconnect signal in FXO Loop-Start mode. Normally, the user would terminate a call by hanging up the phone. However, if a call is under the supervision of the auto-attendant, the lack of a terminating signal can cause a call to remain live for an extended period of time (tens of seconds) after the



call should be dead. Some FXO lines support a supplemental feature known as line-side answer supervision where the network provides an explicit signal acknowledging that the far end has picked up during an outbound call. Because not all network equipment can produce this state, calls cannot rely upon it and the state is ignored.

Neither of the FXO modes supports Direct Inward Dialing (DID). However, the E&M modes do support DID, and are required if DID operation is desired. The other advantage of the E&M modes is that both of them are symmetrical protocols and can be used to connect two PBX's back-to-back, which is not possible with the FXO configurations. To be clear, whichever mode is selected both ends must match and only E&M is symmetrical.

The Allworx server supports the configuration of any of the above modes freely mixed on the T1 line for any time slot, and also allows data to be delivered simultaneously as desired. This is commonly referred to a fractional T1 line configuration. Additionally, while not commonly needed, PRI can be configured simultaneously as well.

## Data Support

The Allworx server 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 a T1 interface 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:** 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.

## Restrictions

Only one interface may be designated as the logical WAN interface for the 24x and 48x systems. 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 are able to 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.

## 10.5.1 Configuration

The configuration of the Digital Lines is dictated by how the service provider provisions the line to which the interface is. The settings must match the service provider's expected configuration or improper operation will

result. Fully configure the line or lines that are being used before physically connecting the server to the T1 line.

## Configuration Hint

When using a Digital Line for circuit switched voice operation (PRI or RBS modes), 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.

## 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: 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.

Loop-back 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 toward lower-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 Caller-ID string you desire them to see. For analog phone lines, your CO determines this string but for PRI lines, the Allworx server 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.

Prefer Originally Dialed Number (RDNIS) for display – This causes T1/PRI originally-dialed/redirected phone number to be displayed on Allworx phones if the original call was redirected and the original call information is provided by the CO.

Prefer Originally Dialed Number (RDNIS) for DID lookup/call routing – This causes T1/PRI originally-dialed/redirected phone number to be used in DID routing, if the original call was redirected and the original call information is provided by the CO.

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.

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. When using NFAS, the D channel must be on the T1-A port.

T1 E and M Immediate Start RBS – A circuit switched Ear and Mouth mode Robbed Bit Signaling trunk that uses Immediate Start signaling. Specifying this mode defines a new outside line for the PBX for each slot configured in this mode. This mode is symmetrical and can be used to hook PBXs back to back to tie PBXs between sites on a leased line.

- T1 E and M Wink FG-B RBS – A circuit-switched Ear and Mouth mode Robbed Bit Signaling trunk. Specifying this mode defines a new outside line for the PBX for each slot configured in this mode. This mode is symmetrical and can be used to hook PBXs back-to-back to tie PBXs between sites on a leased line. Only DTMF signaling is used. Multiple Frequency (MF) signaling is not supported.
- T1 E and M Wink FG-D RBS – A circuit-switched Ear and Mouth mode Robbed Bit Signaling trunk. Specifying this mode defines a new outside line for the PBX for each slot configured in this mode. This mode is symmetrical and can be used to hook PBXs back-to-back to tie PBXs between sites on a leased line. Only DTMF signaling is used. Multiple Frequency (MF) signaling is not supported.
- T1 FXO Loop-Start RBS – A circuit switched Foreign Exchange Office style interface mode that digitally emulates the standard analog telephone line interface that uses Loop-Start signaling. Specifying this mode, in effect, defines a new outside line for the PBX for each slot configured in this mode. If call volume is high, this mode is less desirable than FXO Ground-Start Operation. This is intended to connect to the service provider interface that is operating as the FXS side of the interface. This mode is NOT symmetrical.
- T1 FXO Ground-Start RBS – A circuit switched Foreign Exchange Office style interface mode that digitally emulates the standard analog telephone line interface using Ground-Start Signaling. Specifying this mode, in effect, defines a new outside line for the PBX for each slot configured in this mode. The Ground-Start operation is able to minimize the possibility of glare especially when call volumes are high, making it more preferable than Loop-Start. This is intended to connect to the service provider interface that is operating as the FXS side of the Ground-Start interface. This mode is NOT symmetrical.
- 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

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 but 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
- All Digital Lines & CO Lines
- All Digital Lines, CO Lines & SIP Gateways
- All SIP Gateways
- All SIP Proxies
- All Trunk Devices



**WARNING:** Calls can be routed to Remote Allworx sites in order to use the remote sites' outside lines. However, remote sites should not be the only method available for external calls to be placed. Loss of Internet connectivity between the local site and the remote site (at either end) may disable the ability to place calls including 911 Emergency calls.

**Note:** The Digital Line Service Group is only available on Allworx 24x and 48x servers.

Additional Service Groups can be defined by the System Administrator to control the use of services or set of services for certain dialed calls.

## 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 outside lines, directly.

The server's dialing rules utilize the North American Numbering Plan (NANP). If your Allworx server is located in an area that does not use NANP, then access outside lines using Line Appearance PFKs or by dialing '9#'. Lines can also be accessed by dialing 9 then the phone number. The system will wait six (6) seconds before initiating the call to make sure that the user has finished dialing. To initiate the call immediately, press the # key after the last phone number digit.

## 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 locations.

When NANPA is disabled (unchecked) access outside lines using the steps described in the Exceptions section, above.

## 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**

CO Line One (CO)  
Digital Line 1 - 01 (Digital Line)  
Digital Line 1 - 02 (Digital Line)  
Proxy 1 (SIP Proxy)  
test (SIP Gateway)

move ->

<- move

**Service Group**

move up

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.

300 Main Street • East Rochester, NY 14445 • Toll Free 1-866-ALLWORX • 585-421-3850 • www.allworx.com  
© 2010 Allworx Corp. All rights reserved. Allworx, a wholly owned subsidiary of PAETEC Holding. All other names may be trademarks or registered trademarks of their respective owners.

Revised: September 1, 2010

Page 66



## 11.4 Configuring 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
		Area Code dialed	All Digital Lines, CO Lines & SIP Gateways
Home 555		Area Code NOT dialed	Co Lines
all others		1 + Area Code dialed	All SIP Proxies

**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. If the **Home** Area Code has not been set, seven digit numbers will be routed using the "All Trunk Devices" Service Group.

The area codes should be configured for two reasons: (1) To make sure the correct service is used for the local and other area codes and (2) to make sure that the correct number of digits are used when the call is placed. The Dial Method controls whether or not the area code is to be included when the call is placed. If the area code is not properly configured for the local rules, local calls may not be placed correctly.

To configure area codes, perform the following steps:

1. In the External Dialing Rules section of the Dial Plan page, in the Area Code table, click Modify.
2. 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 digits that will be sent by the Allworx server for local calls, whether or not the phone user dials the area code.
3. 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.
4. Set up any additional area codes for which you must dial the area code, but not a 1 prefix.
5. Choose the desired Service Group for each of the area code entries.
6. 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, 7-digit phone numbers (nnn-nnnn) will be routed using the Service Group selected for the Home Area Code. If the Home Area Code has not been set, 7-digit numbers will be routed using the All Trunk Devices Service Group.

## 11.5 Remote Sites as Services

Remote sites can be selected as services for handling outbound calls. If the line selection process results in a call being routed to a remote site, the call will be connected using one of the remote site's outside lines. The dialing rules that are configured on the remote site will determine which of its lines are used and how the number will be dialed (e.g. with or without area code).

It is possible to accidentally configure the dial plans on multiple sites in such a way that a call could be routed back and forth among the sites. The Allworx system will automatically prevent this from occurring. If a call comes to a server from a remote site, the receiving server will not forward the call to the same or other remote sites. If the dialing rule that the call is using on the receiving site includes any remote sites, the remote sites will be skipped and some other outside line service will be used.

**WARNING:** Remote sites should not be the only method available for external calls to be placed. Loss of Internet connectivity between the local site and the remote site (at either end) may disable the ability to place calls including 911 Emergency calls.

## 11.6 Dialing Privileges Groups

A handset Call Appearance's dialing privileges determine if and how outside lines can be accessed, which outside lines can be used, and what phone numbers are allowed or blocked. A Dialing Privileges Group is a set of dialing privileges and a list of handset Call Appearances with those privileges. Dialing Privileges Groups allow handsets to be configured easily and efficiently. Custom configurations can be applied to any or all of a site's handsets by creating a Dialing Privileges Group, specifying the privileges, and assigning handset Call Appearances to the group. Unlike with User Templates, no additional configuration steps are required to apply the options. Changes made to the group's settings take affect immediately.

The Dialing Privileges Groups are displayed in a table in the Phone System / Dial Plan page, with options to View (modify), Copy, and Delete groups. The system includes a system default group. Unlike default User Templates and Handset Preference Groups, the settings of the default Dialing Privileges Group can be modified. When Allworx servers are upgraded to Release 7.0 or higher, additional Dialing Privileges Groups are created for each unique combination of Outside Line Connection settings for the existing phones. The handset Call Appearances with those options automatically become members of the corresponding new group.

Note: Settings for existing handsets are NOT changed in this process.

### Dialing Privileges Groups

Name	Action
Dialing Privileges (Default)	<a href="#">View</a> <a href="#">Copy</a>
Copy of Dialing Privileges (Defa	<a href="#">View</a> <a href="#">Copy</a>
Dialing Privileges Group #1	<a href="#">View</a> <a href="#">Copy</a>
Tech Support DPG	<a href="#">View</a> <a href="#">Copy</a> <a href="#">Delete</a>

Dialing Privileges Group settings include the following:

- Emergency Service Group

- Outside Line Selection Method
- Toll Restrictions

## 11.6.1 Toll Restrictions

The server applies Toll Restrictions through the use of two lists: Blocked Numbers and Exceptions to Blocked Numbers. By default, all numbers are allowed unless listed in the Blocked Numbers list. Numbers in the Exceptions list override the blocked numbers. That is, if a number is listed as both blocked and as an exception, calls to that number will be permitted. Entries in the Blocked Numbers list need not be complete phone numbers but can be only the first part of phone numbers. For example, entering 1900 in the Blocked Numbers list will prevent all 900 number calls.

Entries in the Exceptions list should be more specific than those in the Blocked Numbers list. As examples, if the Blocked Numbers list contains "1" as an entry and the Exceptions to Blocked Numbers list contains "1800", then toll-free numbers can be dialed but no other long distance number will be allowed. If the Blocked Number list contains a complete number (e.g. 19005553850) then only that number is blocked. The Exceptions to Blocked Numbers list need not have any entries to specify that similar numbers are allowed.

Dialing Privileges Group <a href="#">Modify</a>			
<b>Name</b>	Dialing Privileges (Default)		
<b>Emergency Service Group</b>	All Trunk Devices		
<b>Seize Rule</b>	Dial 9, or 78+PIN, to access outside line		
<b>Outside Line Selection</b>	Use External Dialing rules for number dialed		
<b>Toll Restriction</b> <a href="#">Modify</a>			
<table border="1"> <thead> <tr> <th>Blocked Numbers</th> </tr> </thead> <tbody> <tr> <td>1800...</td> </tr> </tbody> </table>	Blocked Numbers	1800...	<div> <b>TIP</b>                      The system determines if a phone number is allowed to be dialed based on three rules:                 </div> <ol style="list-style-type: none"> <li>1) By default, all numbers are allowed (i.e. nothing is blocked).</li> <li>2) The <b>Blocked Numbers</b> table is a list of exceptions to rule #1. ("All numbers except these patterns are allowed.")</li> <li>3) The <b>Exceptions to Blocked Numbers</b> table is a list of exceptions to rule #2. ("Block as specified except for these patterns").</li> </ol> <p>The <b>Exceptions</b> table should have more specific entries than the <b>Blocked Numbers</b> table (e.g. block "421", but allow "42155").</p>
Blocked Numbers			
1800...			
<table border="1"> <thead> <tr> <th>Exceptions to Blocked Numbers</th> </tr> </thead> <tbody> <tr> <td>18005553850</td> </tr> </tbody> </table>		Exceptions to Blocked Numbers	18005553850
Exceptions to Blocked Numbers			
18005553850			
<b>Call Appearances Assigned To Group</b> <a href="#">Modify</a>			
James A Rochester (Px1 Port:07) Mary Copper (Login ID:5100)			

## 11.6.2 Managing Handsets in Dialing Privileges Groups

Handset Call Appearances can be added to Dialing Privileges Groups by selecting a group from the drop down menu within the Call Appearance's Modify page.

Select the View link of a group and then the Modify link of the Call Appearances Assigned To Group section in order to view, add or remove handsets from a group. When a handset Call Appearance is removed, it is automatically moved to the Dialing Privileges (Default) Group. To move a handset to a different group, select

the handset's checkbox from within the desired group's configuration page (View / Modify Call Appearances Assigned To Group).

Call Appearances Assigned To Group
Select a Call Appearance's check box to include it in the group. Clear a Call Appearance's check box to remove it from the group.
<input checked="" type="checkbox"/> Alex Smith (Login ID:5103)
<input type="checkbox"/> Alex Smith (L2) (Login ID:5105)
<input type="checkbox"/> James A Rochester (Px1 Port:07)
<input checked="" type="checkbox"/> Jane Allright (Login ID:5102)
<input type="checkbox"/> Mary Copper (Login ID:5100)
<input checked="" type="checkbox"/> Noel A Umbridge (Login ID:5106)
<input type="checkbox"/> Thomas Annabel (Port:08)

## 11.6.3 Deleting Dialing Privileges Groups

Dialing Privileges Groups can be deleted by clicking on their Delete links. However, the default group and groups that have handsets assigned to them cannot be deleted. Therefore all handsets must be moved into other groups in order to delete the group.

## 11.7 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. The server will choose the first idle service in the group. However, a handset can be configured to further restrict its use of lines when placing an outside call. According to the number dialed, the configured Service Group is found for a particular outbound call.

1. When the first idle service in the group is found, the Outside Line Selection Method in the handset Call Appearance's Dialing Privileges Group is checked.
2. If the idle service is restricted for the handset, then the next idle service is found and the handset check is made again.
3. This continues until a non-restricted idle service is found to place the call.
4. 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 or IMAP 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. 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 send and receive messages from the Allworx server. 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.

## **12.1.4 IMAP Client**

IMAP provides for synchronizing email so that an account can be accessed from multiple locations. Enable the IMAP protocol in the Network / Configuration page. In addition, the port number and maximum number of connections can be set on the Servers / Email page.

Each user’s PC email application needs to be configured so it can send and receive messages from the Allworx server. 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 IMAP server address.
- Enter the same address as the outgoing SMTP server address.
- Enter the Allworx login name and password for the user as the IMAP 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.



## 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.

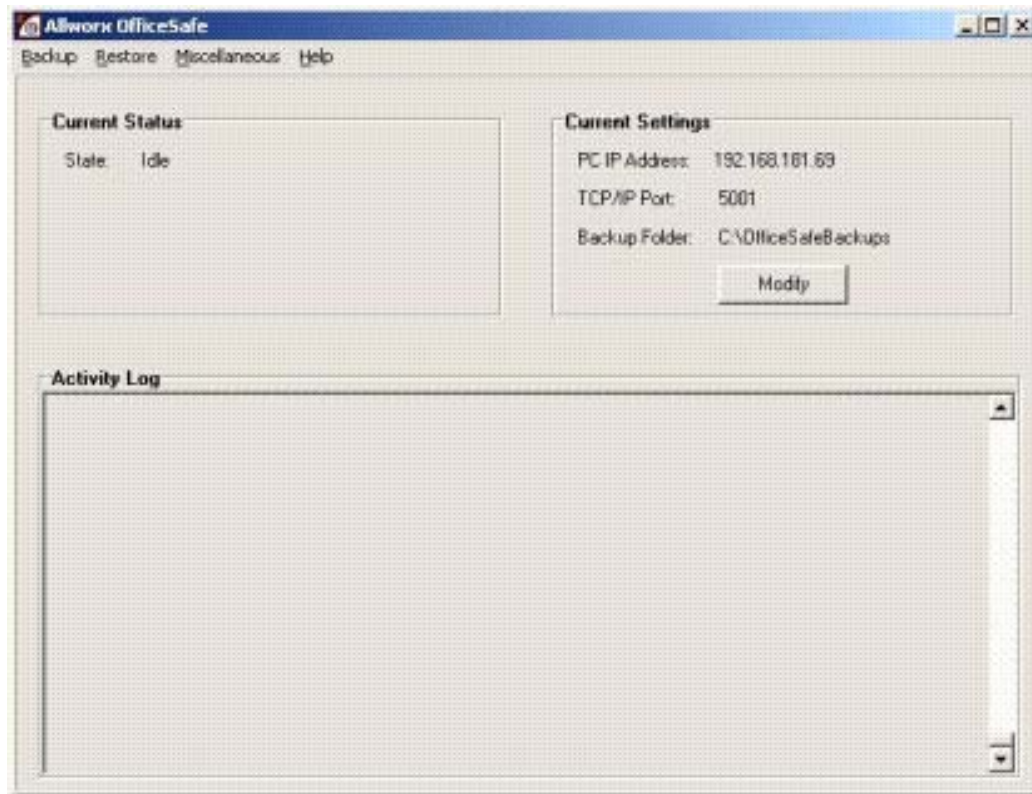
OfficeSafe is optimized for restoring the entire Allworx server disk. It is not possible to restore only a particular file.

### 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:\OfficeSafeBackup. 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 following options are available from the OfficeSafe application under Backup Options:

Override Allworx Server Backup Mode – 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 – 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.

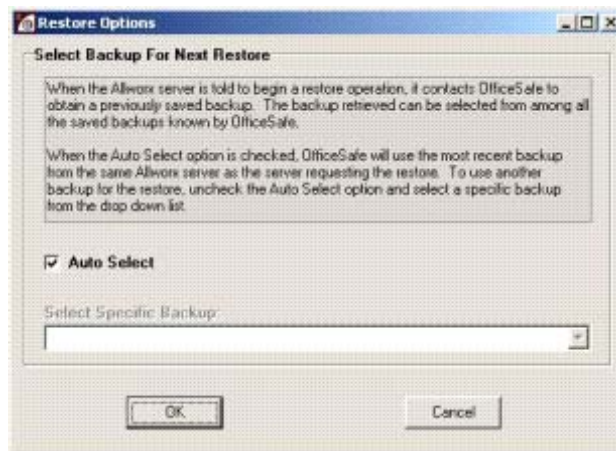
## 13.2 How to Restore Data

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 recent 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.
  1. Select Enter Safe Mode after restart.
  2. Click Restart.
  3. Type SAFEMODE into the pop-up window.
  4. 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**



- 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:

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**  
To update the software:  

- Perform an OfficeSafe backup**  
If you later wish to downgrade to a previous version of software you must restore from the saved OfficeSafe backup.
- Format the disk**
- Load an upgrade file**  
Enter the full pathname of the upgrade file  
   
 (it may take a few minutes to load an upgrade file)
- Activate the Update**  
Select the "Update" button below to activate the update.

- In the OfficeSafe section of the screen, enter the IP Address of OfficeSafe PC that is plugged into the server's LAN port.

- Select the Restore from OfficeSafe button.

Note: The PC that will provide the restore image must be running OfficeSafe.

- Select Accept on the Confirm Restore Request dialog box to begin the restore.
- 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.

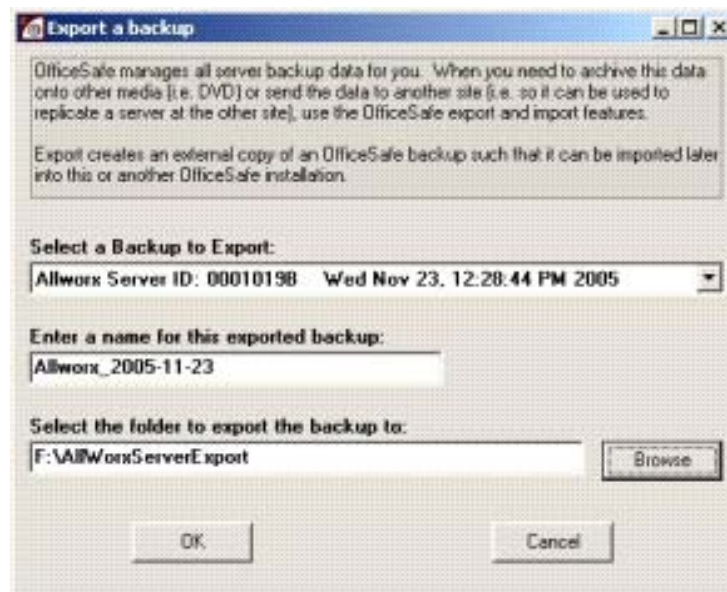
## 13.4 Exporting and Importing Backup Files

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 \\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 \\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 Allworx Phones and Port Expanders

A remote device is one where the phone or port expander is on a different Local Area Network (LAN) than the Allworx server. An example of this is where the Allworx server is set up at the company's main office but an employee has an office phone at home. The system can be configured so that calls to and from that phone work just as though the employee was at the company's main office. Similarly, analog phones and CO lines on a remote port expander can be configured so that they are seamlessly integrated into the server's network and dial plan.

**Caution:** Correct routing of 911 emergency calls for remote Allworx phones and analog handsets attached to remote Allworx Port Expanders cannot be guaranteed. Do not configure remote handsets if they may be used for placing 911 calls.

**Caution:** If the network connection between the Port Expander and the Allworx server is interrupted, regular use of the Port Expander's FXO and FXS ports will not be possible. The only option for placing calls through a Port Expander that does not have a functional network connection to its Allworx server is to plug an analog phone into the Power Fail port. Calls placed using this phone will be routed to the CO line connected to FXO port 1. No other ports will be functional.

### 14.1 General Network Configuration Requirements

Several different network configurations can be used:

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 or port expander can be directly connected to the Internet.
4. The remote phone or port expander 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 a 3<sup>rd</sup>-Party NAT Firewall

To support remote devices and SIP Proxy usage when the Allworx server is behind a single 3<sup>rd</sup>-party NAT firewall, the server's Network Mode must be in LAN Host Mode. See Section 5.2, Network Mode: LAN Host.

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 IP address in the Public IP Address field. In addition, it may be necessary to configure the firewall to statically map specific ports. This is described in the NOTE box on the web page and is discussed further, below.


## 14.3 Setting Up Remote Allworx Devices

Configuring a remote phone or port expander requires setting two configuration parameters on the device.

The first parameter is the Boot Server IP. This is normally the IP address of the Allworx server's WAN port. That 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 required parameter is the Plug 'n' Play Secret Key. This key is displayed on the Servers / VoIP page on the server:

[Home](#) > [Servers](#) > [VoIP Server](#)

VoIP Server  <a href="#">Modify</a>	
	Current Value
BLF Port	2088
BLF Secure	disabled
Force Remote Phone audio through server	enabled
Plug 'n' Play Secret Key	123456
Phone Administration Password	123456
Maximum Active Remote Calls	1000
Paging Base IP Addr	239.255.10.0
Paging Port	56586
Paging Max Hop Count	1
Paging Maximum Duration (minutes)	1
RTP Base Port	15000
RTP DTMF Payload	96
Phone Creates via LAN Plug and Play	enabled
Phone Creates via WAN (Remote Phone) Plug and Play	enabled

To enter the Boot Server IP and Plug 'n' Play Secret Key into the phone, press the Config softkey and choose the Network Settings menu. To enter the information into an Allworx Px 6/2 Expander, enter Config Mode. See the *Allworx Px 6/2 Expander Installation Guide* for more information.

## 14.3.1 Phone or Port Expander behind a 3<sup>rd</sup>-Party Firewall

Remote phones and port expanders usually work well, even if they are behind a firewall. There are several exceptions, each of which requires additional configuration steps. Those steps are described below.

Most problems with firewalls are avoided by the system by routing remote audio traffic through the server. By default, all audio traffic from remote phones and port expanders runs through the Allworx server. Although this avoids problems, it uses up bandwidth of the network connection to the server. When calls to and from remote devices go back out over SIP trunks or over the internet to other remote devices, the bandwidth usage is 180 Kbytes per call, double that of a regular incoming call.

This traffic can degrade the audio quality of calls that use the Internet. However, there is a server setting that can reduce the effect by allowing audio between devices to go directly from one to the other, rather than through the server. The setting is Force Remote Phone Audio through Server which can be found on the Servers / VoIP page. Disabling it will reduce server bandwidth usage. However, if this is done and the phone or port expander is behind a firewall, some configuration of the firewall may be required.

[Home](#) > [Servers](#) > [VoIP Server](#) > [Modify](#)

**VoIP Server** ?

BLF Port

2088

(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

716585315

(6 to 64 characters, use 0-9, and # characters)

Phone Administration Password

6565

(0 to 16 characters, use A-Z, a-z, 0-9, and # characters)

Maximum Active Remote Calls

1000

(set to at least 1, increase as WAN bandwidth allows)

Paging Base IP Address

239.255.10.0

(Multicast IP/UDP/RTP address, set to 224.0.0.0 through 239.255.254.245)

Paging Port

56586

(recommended set to between 49152 through 65535)

Paging Maximum Hop Count

1

(set to between 1 through 255)

Paging Maximum Duration

1

(set to between 1 through 30 minutes)

RTP Base Port

15000

(512 ports used, must be an even number from 15000 to 65024)

RTP DTMF Payload

96

(96-127)

☐ Disable Phone Creates via LAN Plug and Play

☒ Disable Phone Creates via WAN (Remote Phone) Plug and Play

Update

Start Over

Cancel

**NOTE**  
It is necessary to restart the Allworx for new VoIP Server settings to take effect.  
  
The following settings do *not* require a reboot if changed:  
**Force Remote Phone audio through server**  
**Maximum Active Remote Calls**  
**Paging Maximum Duration**  
**RTP DTMF Payload**  
**Disable Phone Creates via LAN Plug and Play**  
**Disable Phone Creates via WAN (Remote Phone) Plug and Play**  
  
If the **RTP DTMF Payload** is changed you must reboot Allworx handsets connected to the system.

The following sections describe some common configurations and solutions to potential problems.

### 14.3.1.1 Difficulty Connecting Calls

If the remote device does not register with the server or if calls to and from it cannot be connected, settings on the firewall and the phone or port expander may have to be changed to enable communications through the firewall. Perform the following steps:

1. Disable DHCP on the handset or port expander. For phones, this setting is on the Config / Network Settings menu. On port expanders, the setting is found on the Config Mode page. Change the following settings:
  - DHCP – Disabled

- Remote Plug 'n' Play key – Set according to the procedure in Section 14.3.1, Phone or Port Expander behind a 3<sup>rd</sup>-Party Firewall.
  - Boot Server IP – Set according to the procedure in Section 14.3.1, Phone or Port Expander behind a 3<sup>rd</sup>-Party Firewall.
  - Phone/Port Expander IP – Choose an address that is consistent with the remote site's network.
  - Netmask IP – Network Mask of the remote site's network.
  - Gateway IP – Gateway IP of the remote site's network.
2. Limit the range of RTP ports that the device will use. This is set on the Server Admin page. For phones, go to PHONE SYSTEM / Handsets / View Configuration. For port expanders, go to Network / Port Expanders and click on the port expander Description. Set the RTP port range for the phone or port expander to 16384 to 16393.

Forward the required IP ports through the Firewall at the remote site, per the table below.

Port Type	WAN	LAN	Protocol
BLF	2088	2088	UDP
SIP	5060	5060	UDP
RTP	16384 - 16393	16384 - 16393	UDP

### 14.3.1.2 Multiple Remote Devices behind the Same Firewall

If there is more than one remote Allworx device behind a firewall, settings on the firewall and the phone or port expander must be changed to enable this configuration. Perform the following steps:

Disable DHCP on each handset or port expander. For phones, this setting is on the CONFIG / Network Settings menu. On port expanders, the setting is found on the Config Mode page. Change the following settings:

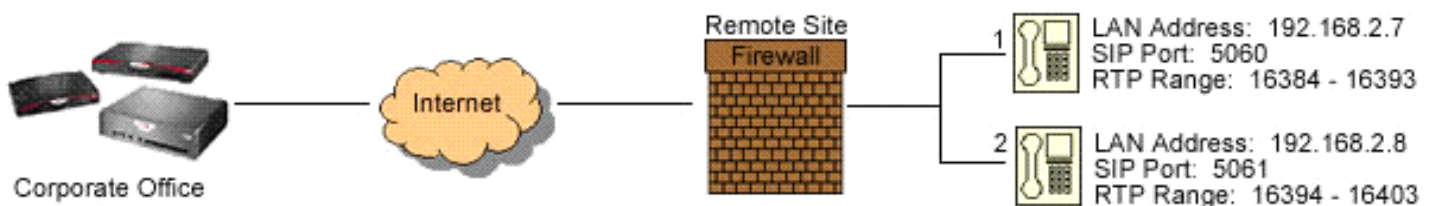
- DHCP – Disabled
- Remote Plug 'n' Play key – Set according to the procedure in Section 14.3.1, Phone or Port Expander behind a 3<sup>rd</sup>-Party Firewall.
- Boot Server IP – Set according to the procedure in Section 14.3.1, Phone or Port Expander behind a 3<sup>rd</sup>-Party Firewall.
- Phone/Port Expander IP – Choose an address that is consistent with the remote site's network.
- Netmask IP – Network Mask of the remote site's network.
- Gateway IP – Gateway IP of the remote site's network.

Limit the range of RTP ports that each device will use and allocate different ranges for different devices. For phones, go to PHONE SYSTEM / Handsets / View Configuration. For port expanders, go to Network /

Port Expanders and click on the port expander Description. Allocate 10 ports for each device in the standard range (e.g. phone1: 16384 to 16393, phone2: 16394 to 16403).

Also on the device's Configuration pages, choose different SIP ports for the devices, starting at 5060 (e.g. phone1: 5060, phone2: 5061).

Forward the required IP ports through the firewall at the remote site, per the table below.



Port Type	Global	Local	Protocol	IP Address
BLF	2088	2088	UDP	192.168.2.7
SIP	5060	5060	UDP	192.168.2.7
SIP	5061	5061	UDP	169.168.2.8
RTP	16384 - 16393	16384 - 16393	UDP	192.168.2.7
RTP	16394 - 16403	16394 - 16403	UDP	192.168.2.8

Note that the BLF port need only be mapped for one of the remote devices.

### 14.3.1.3 Phones at Different Remote Sites, Each with a Firewall

This case is very similar to Case 14.3.1.2, Multiple Remote Devices behind the Same Firewall, above. The difference is that mappings must be done on each site's firewall. Be sure to map the correct RTP port range for the device that is on the firewall being configured. Also, the BLF port (2088) must be mapped for one device on each firewall.

### 14.3.1.4 Remote Phones Cannot Receive Pages

While regular calling and intercom calling works fine, paging remote phones does not. Sending pages from the remote phone works but neither zoned nor overhead pages will typically be heard at the remote phone.

In order to enable paging to a remote phone, a VPN must be set up between the Allworx server and the remote phone. The Allworx server settings changes are described below. Steps for configuring the site's firewall for the VPN vary widely so they are not covered, here.

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 Address – 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 has its 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.



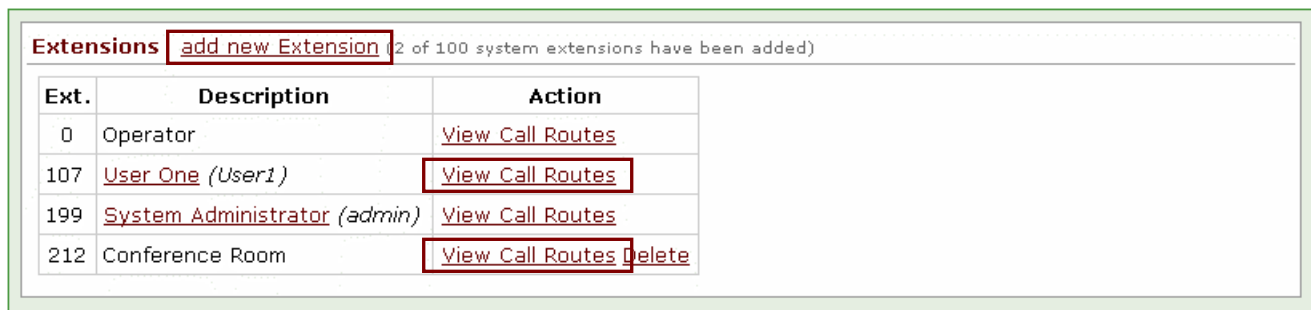
## 15 Call Routing

The Phone System / Extensions page displays User and System extensions. Some special purpose routing of calls to these extensions is possible. Examples of these optional routes are:

- Presence Specific Routing – When on vacation, forward the call directly to voicemail (User extensions).
- Multiple Destinations – Ring multiple phones simultaneously.
- Multiple Connection Attempts – Rings a series of phones when the primary phone is not answered.
- On Busy Routing – Rings alternate phone(s) when the line is busy (User extensions).
- Follow-Me-Anywhere – Forward the call to a cell phone or home phone.
- Caller ID Based Routing – Separate call route that is dependant on the Caller ID of the incoming call (User extensions).
- Day & Night Routing – Different routes are followed when the Allworx server is in Day mode vs. Night mode (System extensions)

Different call routes can be established for each of the seven (7) user presences. In Office, At A Meeting, On Vacation, On Business Trip, At Home, Away, and calls received when Busy can be directed to go to different destinations.

The System Administrator can configure permissions for users to define the routing of their extensions using the My Allworx Manager page by enabling the corresponding checkbox on the Business / Users page. The following sections describe how to define the routing of an extension, starting with basic routing.



The screenshot shows the 'Extensions' page in the Allworx system. At the top, there is a link 'add new Extension' and a status message '(2 of 100 system extensions have been added)'. Below this is a table with three columns: 'Ext.', 'Description', and 'Action'.

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>

### 15.1 Basic Routing

The building blocks of a call route are the Connection Attempts, Destinations, and Finally route. In the typical call route, there is one Connection Attempt and the Finally route.

1. Log into the Admin page of the Allworx System and navigate to the Phone System / Extensions page.
2. To create System extensions, follow the steps below. For user extensions, proceed to the next step.
  - a. Select the add new Extension link (See figure above).



- b. Enter the desired number for the system extension. Use the [show unused](#) link to view a table of available extensions.
  - c. Enter a description for the extension.
  - d. Skip to Step 4.
3. To Modify a User extension:
  - a. Select the [View Call Routes](#) link for a user (See figure above).
  - b. Below each Presence there is a section labeled Call Route for calls from all callers. Scroll to the desired presence state, and then select the [Modify](#) link to the right.
4. In the Call Routes section, if a connection has not yet been added, click on the [add a connection attempt](#) link. If the First connection attempt is already established, go to the next step.
5. The drop down menu that appears in the First connection attempt section provides a list of Handsets, User Extensions, Call Monitors, and the Follow Me option. Choose the desired destination.
6. The last step is to configure the Finally route, which is the desired ending for the call if the call is not answered.
7. For User extensions, any changes made to the call route of one presence can be assigned to the other presences by checking the apply these changes to **all** of my presences check box.
8. Once satisfied with the selections, click the Update button at the bottom of the page. To see the button, scrolling down may be required.

## 15.2 Multiple Destinations

To ring several phones at once, repeat the Basic Routing procedure, not including step 7.

Under the desired connection attempt, click the [add a destination](#) link. This will create another destination drop down menu.

Pull down the menu and choose an additional phone to ring along with the phone that was previously chosen.

Repeat the steps above to add more phones to ring simultaneously for the connection attempt.

Once satisfied with the selections, click the Update button at the bottom of the page. To see the button, scrolling down may be required.

## 15.3 Multiple Connection Attempts

If alternate phones should ring when the handset(s) in the First connection attempt are not answered, create additional connection attempts to receive the calls. Repeat the Basic Routing procedure and the Ring Several Phones at Once (if applicable), not including step 7.

1. Below the First connection attempt section, click on the [add another connection attempt](#) link. This will create another connection attempt section (ex: Second, Third, etc).
2. Configure the connection attempt using the options discussed in other procedures.
3. Once satisfied with the selections, click the Update button at the bottom of the page. To see the button, scrolling down may be required.

## 15.4 On Busy Routing

To avoid having callers hear a busy signal when calling a User extension, an alternative On Busy call route can be configured.

1. Follow the Basic Routing procedure to set up the initial call route for the presence. Once the Extensions page is displayed, select the [Modify](#) link of the presence call route.
2. Select the Modify On Busy Route radio button.
3. Select the Use Call Route below: radio button. A new call route section will appear.
4. Set up the call route using the other procedures.
5. Once satisfied with the selections, click the Update button at the bottom of the page. To see the button, scrolling down may be required.

Note: The primary call route must be created and saved (Update button) before the On Busy Route is created or modified.  
Additional call attempts will be ignored when the busy route is configured to use a call route instead of treating a busy as no answer.

## 15.5 Follow-Me-Anywhere

Calls can be forwarded to other phones outside of the Allworx System such as cell or home phones. If the recipient does not answer the call, it will be directed back to the system in order to follow the rest of the configured call route. In following the rest of the call route, unanswered Follow-Me-Anywhere calls may eventually be directed to the Finally route, which permits callers to leave messages in the default voicemail inbox. If having callers leave messages on the personal phone's voicemail is preferred, do not use the

Follow-Me-Anywhere features. Instead, use the Finally route to direct calls to the cell or home phone by entering the phone number into the Dial number text box.

Note: When an outside phone answers the call, the default is for the recipient will hear a prompt requesting that a 1 be entered to accept the call. However, User extensions can be configured so that Follow-Me-Anywhere calls to their extensions require a Message Center password in order to accept the call (See Section 16, Follow-Me-Anywhere, for more information).

1. Using the Basic Routing procedure or a combination of the other procedures, select Follow Me → from the drop down menu in the connection attempt.
2. In the text box that appears to the right, enter 9<sup>†</sup> or 78<sup>†</sup>+PIN (to gain an outside connection) followed by the phone number.

Examples<sup>†</sup>: 9+1+aaa-xxx-nnnn, 9+1+xxx-nnnn,  
78+PIN+1+aaa-xxx-nnnn, 78+PIN+xxx-nnnn

3. Select the desired number of rings. The Follow-Me-Anywhere feature requires the recipient to listen to a message and enter a code. Therefore, increment the normal number of rings by at least two in order to give the recipient extra time to answer the call.
4. Once satisfied with the call route selections, click the Update button at the bottom of the page. To see the button, scrolling down may be required.

## 15.6 Caller ID Based Routing

The Caller ID of the incoming call to a User extension can be used to determine the call route.

1. Click on the View Call Routes link, next to the User extension that is adding a Caller ID-based route (See figure above).
2. Select the add new Call Route link next to the presence that is to be configured.
3. Choose the radio button for either external or internal calls.
4. For calls from external numbers, enter the phone number with area code in the text box. For calls from internal extensions, choose the extension from the drop down menu.
5. Use the other procedures (e.g. Basic Routing) to develop the intended route for the call.
6. Once satisfied with the call route selections, click the Update button at the bottom of the page. To see the button, scrolling down may be required.

---

<sup>†</sup> Extensions may vary per system. If you are using a non-default Internal Dial Plan, consult the Phone Features tab of the My Allworx Manager page to determine what extensions are being used for the corresponding feature.

## 15.7 Day & Night Routing

System Extensions can be configured to follow one call route when the Allworx System is in Day Mode and another when the System is in Night mode. (See Section 22, Day-Night Mode, for more information).

1. Follow the Basic Routing procedure to set up the Day Mode call route for the extension. Once the Extensions page is displayed, select the View Call Routes link (See Figure 16).
2. Select the Modify link in the Extension Information section.
3. Enable the Use different call routes for Day and Night modes checkbox and then click the Update button.
4. Select the Modify link in the Night mode section. Use the other procedures to develop the intended route for the extension.
5. Once satisfied with the call route selections, click the Update button at the bottom of the page. To see the button, scrolling down may be required.

## 15.8 Changing a User's Presence Setting

### 15.8.1 Changing Presence via an Allworx IP Phone

When the Mute/DND button is held down for greater than one second, a presence menu will appear. Scroll to the desired presence setting and then press the Select button. See the *Allworx Phone Guide* for more information.

### 15.8.2 Changing Presence via the Allworx Message Center

1. Access the Allworx Message Center by either pressing the Message button on an Allworx handset, dialing extension 404<sup>†</sup>, or by dialing 6<sup>†</sup> + extension.
2. Select option 4 'To Change Your Message Center System Settings'.
3. Press 1 'To Change Your Presence Setting'.

See the *Allworx User Guide* for more information.

### 15.8.3 Changing Presence via the My Allworx Manager page

1. Open a web browser and enter the Allworx server's LAN IP address into the address field.  
Default: <http://192.168.2.254>

---

<sup>†</sup> Extensions may vary per system. If you are using a non-default Internal Dial Plan, consult the Phone Features tab of the My Allworx Manager page to determine what extensions are being used for the corresponding feature.

2. Click Login. An Allworx username and Message Center password are required to again access to the call routing features.
3. Select the My Presence tab.
4. Choose the appropriate presence and then click the Change Presence button.

## 15.8.4 Changing Presence via the Web Admin Page

Although users can change their own presence setting, the System Administrator can change a user's presence by going to the Business / Users page, clicking on the Modify link of the user, and changing the User Presence setting.

The screenshot shows the 'User' modification page in the Allworx web interface. The 'Identification' section contains the following fields:

- Login Name: User1
- Full Name: User (first name) and One (last name)
- Password: masked with dots
- Confirm Password: masked with dots
- Phone Extension: 107 (dropdown menu)
- User Presence: In Office (dropdown menu, highlighted with a red box)

## 15.9 Outside Line Call Routing

Each outside line (CO Line, DID Line, SIP Proxy, SIP Gateway, or a Digital Line) has a call route associated with it. Go to Phone System / Outside Lines and click the Modify link on one of the CO lines.

☐ Apply settings for this line to all lines with the same Port

---

**Digital Line**

Description: Digital Line 1 - 01  
 Port: T1-A  
 Default Language Primary Language   
☒ Enable Line Appearance

---

**Default Auto Attendant**

Select the attendant used to answer when calls received from this source are routed to an Auto Attendant.  
 Auto Attendant 1 (x431)

---

**Call Route**

Calls received from this Digital Line Slot go to:

☐ Extension choose an extension   
☒ Auto Attendant  
☐ Voicemail for user Alex Smith (asmith)   
☐ Routed using DID Block(s):

☐ 4259000 / 10 Numbers / Routing Plan 1

The Call Route section in the figure above determines how a call coming into the system through Digital Line 1 channel 01 is directed.

- Extension – Incoming calls can be routed to a User or System extension. Using a System Extension provides more call routing flexibility and allows for a common route to be used for multiple lines.
- Auto Attendant – When an outside line is routed to an Auto Attendant, it goes to the designated Auto Attendant that is defined in the Default Auto Attendant section.
- Voicemail for user – Calls that come into the System would go directly to a voicemail box for a User.
- Routed using DID Block(s) – When using DID blocks for incoming calls, the DID block has to be enabled for the outside line or each desired channel, if using digital lines (See Section 19, Direct Inward Dialing (DID) for more information).

## 16 Follow-Me-Anywhere

The Follow-Me-Anywhere Calling feature allows inbound calls to be routed to an external number within call routes. If the call is rejected or unanswered then the inbound call will continue along the defined call route. Previously, external numbers were only allowed to be at the termination of the call route (the Finally attempt), which limited the routing destination of the call if the recipient did not answer. (See Section 15.5, Follow-Me in the Call Routing section, for more information)

When users receive a Follow-Me-Anywhere call on their external phone (e.g. cell phone, home phone), they hear a prompt that identifies the source of the call and how to accept the call. The content of the prompt and the acceptance method for user extensions are configurable from the Business / User page. There are checkboxes for requiring a Message Center password to accept the call and for requiring that the caller record their name. If both checkboxes are checked, the prompt for calls to the user's extension will be: "Call for (user) from (caller). To accept, enter your password followed by the pound sign."

**Note:** System extensions that use Follow-Me-Anywhere will receive the default prompt: "A call is being forwarded to you from an Allworx system. Press one to accept the call."

Follow Me Calling	
<input type="checkbox"/>	Password required to accept call
<input checked="" type="checkbox"/>	Require caller to record name
Primary Phone	<input type="text" value="Unassigned"/> (used for quick transfer from cell phone)

The recipient of the call can consult another employee or transfer the caller to any extension (user, system or remote site) in the Allworx System.

### Consult

1. During the call press \*# to obtain a dial tone while placing the caller on hold.
2. Dial the extension of the person that is to be consulted.
3. To end the consultation and return to the caller press \*#.

### Announced (Attended) Transfer

During the call press \*# to obtain a dial tone while placing the caller on hold.  
Dial the extension to which the caller is to be transferred.  
Talk to the new recipient.  
Hang up to complete the transfer.

### Unannounced (Blind) Transfer

During the call press \*# to obtain a dial tone while placing the caller on hold.  
Dial the extension to which the caller is to be transferred.  
Immediately hang up to complete the transfer.



## Quick Transfer

- While active on a call, the recipient can blind transfer the caller to their primary phone using \*7.
- To designate a Primary Phone, navigate to the Business / Users page. Select a handset from the Primary Phone drop down menu under the Follow Me Calling section (See figure above).
- The Primary Phone choice is independent of the user's regular phone assignment and call routing. It can be any phone in the system.

Note: The consult and transfer features will not work if any of the parties are connected via a SIP Trunk or SIP Gateway.

## 17 Voicemail Notification & Escalation Message Alerts

Voicemail Notification & Escalation Message Alerts send SMS text messages to cell phones and/or email addresses when a voice message has been left in a specified voicemail inbox on the Allworx System.

The SMS text messages provide the following information:

- Allworx username associated with the voicemail inbox.
- Caller ID name and number of the caller who left the voicemail (if available).
- Date and time the voicemail was received by the voicemail inbox.
- Length of the recorded message.
- Current amount of new voicemails in the voicemail inbox.

Note: The SMS text messages are sent via the Allworx SMTP server, which requires a valid network path from the Allworx to the destination mail server through the Internet.

### 17.1 Notification Mode

Voicemail Notification will send the recipient(s) an alert every time a new voicemail is received in the voicemail inbox.

To configure voicemail Notification alerts, navigate to the Business / Users page and enable the Notification Mode radio button.

SMS Email Messages – The address of the recipient(s) that are to be alerted of a new message in the voicemail inbox. Only one entry is permitted per field, therefore a message alias may be used to send alerts to multiple recipients.

The following are acceptable entries:

- Username
- Message Alias
- Cell phone number with service provider SMS text message domain (e.g. 7165552000@txt.att.net)
- Note: A list of service provider domains can be found at: [www.notepage.net/smtp.htm](http://www.notepage.net/smtp.htm) (Check with the Service Provider for more information).
- Email address

### 17.2 Escalation Mode

The Voicemail Escalation feature distributes message alerts repeatedly until a set number of retries have been met or until any voicemail message has been retrieved. Recipients are organized into levels such that after a certain number of message alerts are sent to the recipient(s) at one level, the alerts to the recipient(s) at the next highest level begin.

To configure voicemail Escalation alerts, navigate to the Business / User page and enable the Escalation Mode radio button.

Level – The order in which recipients are alerted that a message has been left in the voicemail inbox.

SMS Email Messages – The address of the recipient(s) that are to be alerted of a new message in the voicemail inbox. Only one entry is permitted per field, therefore a message alias may be used to send alerts to multiple recipients.

The following are acceptable entries:

- Username
- Message Alias
- Cell phone number with service provider SMS text message domain (e.g. 7165552000@txt.att.net)
- Note: A list of service provider domains can be found at: [www.notepage.net/smtp.htm](http://www.notepage.net/smtp.htm) (Check with the Service Provider for more information).
- Email address

Notification Period – Period of time that elapses before another SMS message is sent to the recipients of the level.

Maximum Retries – Maximum number of messages sent to the recipients of the level before the message alerts proceed to the next level of the table. This does not include the initial SMS message, therefore the recipients will be sent one more message than the value entered.

Note: Escalation message alerts will stop once the maximum number of messages has been sent to the last populated level in the table.

Continue Notifications – Recipients will continue to receive message alerts in conjunction with the next level or levels once escalation occurs.

Example:

A doctor's office has an "on call hours" voicemail box. When voicemail messages are left in this box, the notification is set to the doctor who is assigned to answer after hour emergencies. If the doctor does not retrieve the call within X minutes an escalation message is sent to the next set of backup doctors.

## 18 Key System Behavior

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

### 18.1 Example Configuration

#### Requirements

An insurance agent called Best Insurance is provisioned with 3 CO lines. The office is staffed by five employees, each having an Allworx phone. 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 voicemail 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 voicemail 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 phone, configure a Line Appearance PFK for each CO line. See Configuring Allworx IP Phones section.

## 19 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.

### 19.1 Create a DID Block

Click on the [add 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.

### 19.2 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.

<b>Direct Inward Dial Blocks</b> <a href="#">add new DID Block</a>	
<b>Block</b>	<b>Action</b>
(555) 555-2000 Numbers: 100 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.

<b>Routing Plan Information</b> <a href="#">modify</a>	
<b>Description</b>	Routing Plan 1
<b>Default Extension</b>	0 - Operator
<b>Default DNIS Name</b>	
<b>Default Language</b>	Use Source of call
<b>DID Blocks using this plan</b>	(555) 555-2000 / 100 numbers

<b>Phone Number to Extension Mapping</b> <a href="#">add number to table</a>				
Phone Number	Extension	DNIS Name	Default Language	Action
(555) 555-2000	1001 - Mary Cooper	Support Line 1	Use Source of call	<a href="#">Modify</a>
(555) 555-2001	1000 - Alex Smith	Support Line 2	Use Source of call	<a href="#">Modify</a>

**TIP**

Phone Numbers that do not appear in the table above use the Default Extension for this DID Block as defined above.

To remove a phone number from the table, select Modify, then change the number to use the default extension.

The routing plan specifies a mapping for each DID phone number to an Allworx server extension. The plan also permits entry of a Dialed Number Identification Service (DNIS) name for each phone number. The DNIS name will be displayed on the recipient's Allworx phone. If no DNIS name is entered, the originally dialed number will be displayed on the phone. The Default Extension will be used as the mapping for any phone numbers not specified in the Phone Number to Extension Mapping list.

## 19.3 Create the DID Lines

The last step in configuring the DID lines is to configure each of the incoming lines that will use DID blocks. DID blocks can be used by the following line types:

- T1/PRI
- T1/RBS
- SIP Proxy

- SIP Gateway

Below is the Modify window for a T1/PRI Digital Line.

<input checked="" type="checkbox"/> <b>Apply settings for this line to all lines with the same Port</b>
<b>Digital Line</b>
<b>Description:</b> Digital Line 1 - 01 <b>Port:</b> T1-A <b>Default Language</b> Primary Language <input type="button" value="v"/> <input checked="" type="checkbox"/> <b>Enable Line Appearance</b>
<b>Default Auto Attendant</b>
Select the attendant used to answer when calls received from this source are routed to an Auto Attendant. Auto Attendant 1 (x431) <input type="button" value="v"/>
<b>Call Route</b> <input type="button" value="?"/>
<b>Calls received from this Digital Line Slot go to:</b> <input type="radio"/> <b>Extension</b> choose an extension <input type="button" value="v"/> <input type="radio"/> <b>Auto Attendant</b> <input type="radio"/> <b>Voicemail for user</b> Alex Smith (asmith) <input type="button" value="v"/> <input checked="" type="radio"/> <b>Routed using DID Block(s):</b> <div><a href="#">check all</a>   <a href="#">uncheck all</a> <input checked="" type="checkbox"/> 4259000 / 10 Numbers / Routing Plan 1</div>

Click on "Routed using DID Block(s)" and check the block or blocks to use for this outside line.

Note: For Digital lines, this must be done for each channel. If all channels will use the same settings, select "Apply settings for this line to all lines with the same *Port*".



## 20 Emergency Support

### 20.1 Emergency Handset Caller ID

An Emergency Caller ID (CID) number can be assigned to each Allworx handset. When an emergency number is dialed from the handset, the Emergency CID will be passed to the emergency call center instead of the CID that would normally be used. For those employees who are not located at the main site, the Emergency CID will help the emergency call center identify the location of the handset that placed the call.

Note: The Emergency CID will not override the Caller ID of a CO line. If you are using SIP trunks or PRI lines, check with your provider to determine what Caller ID numbers they will accept, if any or to configure additional numbers as acceptable. After setting up Emergency Caller ID numbers, test every number (by calling 911) to ensure that emergency calls are connected that they are being routed to the correct emergency call center. Be sure to tell the call center that it is a non-emergency call and that you are testing your phone system.

Each Emergency CID is associated with a Service Group to be used when placing an emergency call. When "Use External Dialing Rules" is chosen as the Service Group, the outside line or Service Group will be based on the area code of the Emergency CID number.

#### External Dialing Rules

North American Numbering Plan Administration (NANPA) enabled <a href="#">Modify</a>				
Area Code	Exchange	Number Dialed	Service Group	Action
716		9+716-xxx-nnnn 9+1+716-xxx-nnnn	Verizon (Co)	<a href="#">Modify</a>
Home 585		9+xxx-nnnn 9+1+585-xxx-nnnn	All Digital Lines, CO Lines & SIP Gateways	
all others		9+1+aaa-xxx-nnnn	All Digital Lines	

#### 20.1.1 Add Emergency Caller ID Numbers

To add Emergency Caller ID numbers to the Allworx system, navigate to Phone System / Emergency CID. Under the Emergency Caller ID Numbers section, select the [add new Caller ID Number](#) link. Enter the Caller ID number and desired location in the appropriate fields. Choose a Service Group and then select the Add button. Only one entry can be created per Emergency CID number.

#### 20.1.2 Assign Emergency Caller ID via Admin Page

Emergency Caller IDs can be assigned to a handset through the server's Admin page, phone's Admin page or from the handset CONFIG menu.

Note: An Emergency CID can be assigned to more than one handset.

From the server's Admin page, navigate to Phone System / Emergency CID. All handsets on the system are listed in the table under the Handset Emergency Caller ID Number Assignments. To assign an Emergency CID number to a handset, select the [Modify](#) link. Choose a Caller ID Number / Location and then click the

Update button. The table will display the Emergency CID, Location and Service Group assigned to the handset.

Emergency Caller ID Numbers <a href="#">add new Caller ID Number</a>			
Caller ID Number	Location	Service Group	Action
(315) 597-1111	Mary's House	Verizon (Co)	<a href="#">Modify</a> <a href="#">Delete</a>
(585) 421-3850	Rochester	All Trunk Devices	<a href="#">Modify</a> <a href="#">Delete</a>
(716) 555-1234	Buffalo	Use External Dialing Rules	<a href="#">Modify</a> <a href="#">Delete</a>

Handset Emergency Caller ID Number Assignments				
Handset	Caller ID Number	Location	Service Group	Action
000add820020	<i>Emergency Caller ID not specified</i>			<a href="#">Modify</a>
Alex Smith	(585) 421-3850	Rochester	All Trunk Devices	<a href="#">Modify</a>
Mary Copper	(315) 597-1111	Mary's House	Verizon (Co)	<a href="#">Modify</a>

## 20.1.3 Assign Emergency Caller ID via Handset

A new Caller ID can be added or handsets can be assigned an existing Emergency CID number. Any Emergency CID entered via the phone's Admin page or CONFIG menu will override the existing CID number assignment for the handset.

Note: When assigning an Emergency CID number to a handset from the server's Admin page, the Caller ID number will not be displayed on the phone's Admin page or under the CONFIG menu.

### Phone's Admin Page

Log into the Admin page of the handset. Navigate to the Configuration / Preferences page and then select the [Modify](#) link. Scroll to the bottom of the page. Enter a new or existing CID number in the Emergency Caller ID Number field and then select the Update button. A phone reboot is required for changes to be reflected on the server's Admin page.

### Handset CONFIG Menu

From the handset, select the CONFIG softkey and choose Preferences. Scroll to the bottom of the list of settings. Select the Emergency Caller ID Number option to enter a new or existing Caller ID number. A phone reboot is required for changes to be reflected on the server's Admin page.

### Emergency CID displayed on Admin page

When a new Emergency Caller ID number is added via a phone's Admin page or CONFIG menu, an Emergency CID entry will be created in the Emergency Caller ID Numbers table on the server's Admin page. The Description of the handset is used as the Location and the Service Group is set to 'All Trunk Devices'.

After a phone reboot, the Emergency CID will be displayed in bold green text on the server's Admin page. Select the [show details](#) link to see the previously assigned Emergency CID (if any) for each handset. To

return to the previous Emergency CID assigned, delete the Caller ID number using the phone's Admin page or CONFIG menu.

Emergency Caller ID Numbers [add new Caller ID Number](#)

Caller ID Number	Location	Service Group	Action
(315) 597-1111	Mary's House	Verizon (Co)	<a href="#">Modify</a> <a href="#">Delete</a>
(585) 421-3850	Rochester	All Trunk Devices	<a href="#">Modify</a> <a href="#">Delete</a>
(585) 421-5555	Alex Smith	All Trunk Devices	<a href="#">Modify</a> <a href="#">Delete</a>
(716) 555-1234	Buffalo	Use External Dialing Rules	<a href="#">Modify</a> <a href="#">Delete</a>

Added to table →

Handset Emergency Caller ID Number Assignments [hide details](#)

Numbers in **bold green** have been specified at the handset.

Handset	Caller ID Number	Location	Service Group	Action
000add820020	<i>Emergency Caller ID not specified</i>			<a href="#">Modify</a>
Alex Smith	<b>(585) 421-5555</b> <small>(585) 421-3850</small>	Alex Smith	All Trunk Devices	<a href="#">Modify</a>
Mary Copper	(315) 597-1111	Mary's House	Verizon (Co)	<a href="#">Modify</a>

Overrides previous CID →

## 20.1.4 Delete an Emergency Caller ID

Emergency CID numbers can be deleted by clicking on the [Delete](#) links. However, Emergency CIDs that have handsets assigned to them cannot be deleted. Therefore, all handsets must be assigned another CID prior to deletion.

## 20.2 Emergency Alerts

The 911 Alert feature sends audible and visual alerts to designated handsets immediately after an emergency call is made from any local or remote handset. Additionally, the Allworx system supports email and SMS message notification of emergency calls.

To configure handsets to receive 911 alerts, assign an Emergency Alert PFK. When an emergency call is placed from a handset on the system, handsets with the PFK will produce an audible beeping and display:

- Owner of the handset which placed the call
- Station number of the handset the call originated from
- Date / time of the call

During an active alert, pressing the PFK will acknowledge the alert, silence the audible beep and remove the alert information from the display screen. Pressing the PFK when there is not an active alert on the handset will retrieve information of the last alert stored on the handset. Rebooting the handset will remove stored alert details from the handset.

The Allworx system will automatically acknowledge active alerts by silencing the beeping on all handsets after 10 minutes and by removing alert information from each handset display screen after 60 minutes. If additional emergency calls are placed from other handsets within 15 seconds, the new alerts will be ignored. The next emergency call placed after the 15 second time period will be stored on the handset and will be displayed once the user or system acknowledges the first alert. The user can acknowledge an alert by pressing the PFK or CLEAR softkey.

Emergency alerts will supersede any handset functionality (e.g. placing/receiving a call, logged into message center), except when the user of the handset is in an admin menu (e.g. viewing directory, CONFIG menu settings, changing presence setting). In this case, the PFK will blink. Once the user exits the menu screens, the alert's audible beeping and information will be propagated on the handset.

Note: Calls will not be disconnected when an Emergency alert is propagated to the handset.

## 20.2.1 Emergency Call Email Notifications

The Allworx system can be configured to send out textual notifications to email and SMS accounts every time an emergency call is placed. The notifications include the user assigned to the handset (station number, for unowned handsets) and the date / time of the call.

To enable Emergency Call Email Notifications, navigate to the Phone System / Dial Plan page, and then enter the recipients of the notifications in the text fields. Valid entries include username, message alias, email address, and SMS address (cell number and domain).

**Emergency Call Email Notification**

☒ **Enable Email Notifications of Emergency Calls**

Addresses

Enter one email address per line.  
NOTE: System users can be specified by just their username, otherwise enter the entire email address.

## 21 Call Supervision

Call Supervision is accomplished through a PFK that can be configured on the supervisor's Allworx phone. The PFK can be programmed for Barge in, Silent Monitor or Whisper Mode. In addition, the agent's phone must be enabled for supervision. This is done by modifying the Call Supervision setting of the agent's Handset Preference Group.

To initiate supervision, the supervisor presses the Call Supervision PFK and enters the agent's extension. If the supervisor has a BLF PFK for the agent, the session can be initiated by pressing the Call Supervision PFK followed by the BLF PFK. There will be no indication on the agent's phone that supervision is in progress.

Barge in – Once the call is connected, anything the supervisor says will be heard by both participants in the call. The supervisor can transition to silent monitoring by pressing the Mute button on their phone.

Whisper (9204 only) – Sounds from the supervisor's phone are only heard on the agent's phone. The supervisor's MUTE button only controls audio going to the agent. The supervisor will not be able to initiate two-way communications with the third participant.

Silent Monitor – Sounds from the supervisor's phone are not heard by either party in the call. The Mute button on the supervisor's handset is enabled and is lighted red. The supervisor can speak to the participants of the monitored call at any time by pressing (disabling) the Mute button.

### Important Notes

- The supervision call is terminated when the original call ends.
- The supervision call is terminated if the agent parks the call or puts it on hold.
- The supervisor can put the call on hold without terminating the supervision call.
- The supervisor cannot park or transfer the call to another phone.
- The supervisor can conference in another participant.
- The newly-conferenced participant must press their MUTE button to maintain the silence when in Silent Monitor mode. Otherwise, their voice will be heard.
- The agent will not be able to conference in another party while the supervision call is in progress unless the agent is using an Allworx 9204 phone. The agent cannot initiate a conference if the call is being supervised in Whisper mode.
- The agent will not be able to record a call using Allworx Call Assistant during a supervised call unless the agent is using an Allworx 9204 phone. The agent cannot record a call if it is being supervised in Whisper mode.
- The Call History on the agent's handset will not have any record of that call.
- The supervised calls appear as normal calls between stations in the server's Call Detail Records.
- The original call and supervised call will be displayed as separate calls in the Live Calls and Call Assistant Active Calls tab.
- Whisper mode requires that the agent have an Allworx 9204 Phone.


## 22 Day-Night Mode

The Day-Night mode feature is used to control the Auto Attendant greetings played and system extension call routes followed, if configured for different Day-Night mode behavior, based on the business's hours of operation. The server can be set to either automatically switch between Day and Night modes or allow a user to initiate the change manually. Automatic switching depends on the Day Mode Hours scheduled by the System Administrator. However, the current mode can be overridden manually.

By default, the server is in Automatic Control. The hours of operation are defined as Monday through Friday, 8 am to 5 pm, and closed Saturday and Sunday. The Day Mode Hours fields can be configured to switch between the modes multiple times during the day. In addition, Holiday hours can be added to override the Daily hours based upon a certain date(s).

To change either the Day-Night Control setting, Automatic or Manual, or to edit the predefined Daily and/or Holiday hours, select Business / Day-Night Mode then the Modify link.

Note: The server will automatically define blank fields as Night Mode.



[About](#)

[Phone System](#)

**Business**

[Contact Information](#)

[Message Aliases](#)

[Users](#)

**Day-Night Mode**

[Network](#)

[Servers](#)

[Reports](#)

[Maintenance](#)

[Need help?](#)

[Install Checklist](#)

[\[Logout\]](#)

[Home](#) > [Business](#) > Day-Night Mode

---

**Day-Night Mode**

System is currently operating in **Day Mode**, set to Night Mode

Day-Night Control Automatic Modify

---

Day Mode Hours	Action
<b>Daily</b>	
Sun * Night Mode *	
Mon 08:00 AM - 05:00 PM	
Tue 08:00 AM - 05:00 PM	
Wed 08:00 AM - 05:00 PM	
Thu 08:00 AM - 05:00 PM	
Fri 08:00 AM - 05:00 PM	<a href="#">Modify</a>
Sat * Night Mode *	
<b>Holiday</b>	
07/04/2007 - 07/04/2007 08:00 AM - 12:00 PM 01:00 PM - 05:00 PM	

**TIP**  
You can define system extensions to follow different call routes for Day and Night Modes!

The Day and Night modes can be changed manually using either of the following options:

1. Day Mode or Night Mode button (depends on current state) at the top of the Business / Day-Night Mode page.
2. Day-Night Mode defined PFK on a handset. See Section 9.4.7, Day-Night Mode PFK, for more information.



## 23 Auto Attendant

Auto Attendants answer incoming calls automatically and help direct callers to the person or department they want. Callers can listen to a list of services and decide which one best suits their need, use the dial by name option to connect to an employee directly, or listen to the company phone directory for the extension of an employee.

You can set up anywhere from 1 to 9 Auto Attendants depending on your need. Each Auto Attendant can be assigned to one or more CO Line, DID Line, SIP Proxy, SIP Gateway, or Digital Line. For example, one Auto Attendant can be used to answer calls for Sales and another for Service. In addition, three types of greetings can be recorded for each Auto Attendant: a custom message to be used any time, one to be used when the server is in Day Mode, and the third to be used when the server is in Night Mode.

### 23.1 Configuring the Auto Attendant

From the Home page, click Phone System and then click Auto Attendants.

**Auto Attendants**

[Manage](#) the custom recordings played by the Auto Attendants.

[View](#) and manage the Language settings for the Auto Attendants.

**x431 - Main** [modify](#)

Include Remote Users: disabled  
 Dial-By-Name Menu (#1): enabled  
 Dial-By-Name Prompt: do not play  
 Dial-By-Name Spell Option: spell first or last name  
 Dial-By-Directory Menu (#2): disabled  
 Dial-By-Directory Prompt: N/A (menu is disabled)  
 Dial It Now Prompt: do not play  
 Repeat Options Prompt: do not play  
 Speed Dial Numbers: not allowed  
 Default Extension: 0

Menu Shortcuts									
0	1	2	3	4	5	6	7	8	9
0	432	433	---	1196	1216	---	---	---	---

The nine Auto Attendants are numbered 431 to 439<sup>†</sup>. The list of Auto Attendants show the attributes assigned to each one. Click the [Modify](#) link for the specific Auto Attendant to set up.

<sup>†</sup> Extensions may vary per system. If you are using a non-default Internal Dial Plan, consult the Phone Features tab of the My Allworx Manager page to determine what extensions are being used for the corresponding feature.



## 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="Main"/>	
<b>Include Remote Users</b>	<input type="button" value="disabled"/>	enable to include multi-site users dial-by-name, dial-by-directory
<b>Dial-By-Name Menu (#1)</b>	<input type="button" value="enabled"/>	
<b>Dial-By-Name Prompt</b>	<input type="button" value="do not play"/>	"Press #1 to dial by name."
<b>Dial-By-Name Spell Option</b>	<input type="button" value="spell first or last name"/>	
<b>Dial-By-Directory Menu (#2)</b>	<input type="button" value="disabled"/>	
<b>Dial It Now Prompt</b>	<input type="button" value="do not play"/>	"If you know your party's extension you may dial it now."
<b>Repeat Options Prompt</b>	<input type="button" value="do not play"/>	"Press * to listen to these choices again."
<b>Speed Dial Numbers</b>	<input type="button" value="not allowed"/> (support for dialing 350-399, 34000-34999 from main menu)	
<b>Default Extension</b>	<input type="button" value="0 - Operator"/>	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.

Digit	Extension
0	<input type="button" value="0 - Operator"/>
1	<input type="button" value="432 - Allworx Product Division"/>
2	<input type="button" value="433 - Allworx Consulting"/>
3	<input type="button" value="not used"/>
4	<input type="button" value="196 - Accounting"/>
5	<input type="button" value="216 - Allwork Inquiries"/>
6	<input type="button" value="not used"/>
7	<input type="button" value="not used"/>
8	<input type="button" value="not used"/>
9	<input type="button" value="not used"/>

“Prompts” are messages from the Auto Attendant that give 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.  Note: Dial-By-Directory will automatically be disabled if there are more than 50 users assigned to the Auto Attendant
Dial-By-Directory Prompt	do not play play (default)	Prompt: Press #2 for a listing of all users and their extensions.  Note: Dial-By-Directory will automatically be disabled if there are more than 50 users assigned to the Auto Attendant
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 <sup>†</sup> from main menu)

<sup>†</sup> Extensions may vary per system. If you are using a non-default Internal Dial Plan, consult the Phone Features tab of the My Allworx Manager page to determine what extensions are being used for the corresponding feature.

The Auto Attendant can be configured to allow digits 0 through 9 to be dialed as single-digit Menu Shortcuts. Dialing the digit will transfer a caller to a designated extension or another Auto Attendant. Select an extension in the drop-down menu for the corresponding digit. '0' is assigned to '0 – operator' by default<sup>†</sup>. If the Internal Dial Plan is modified so that the Operator is changed to a digit other than 0, the shortcut will automatically be adjusted to dial the new Operator digit. However, shortcut 0 will still be used for the Operator. If you wish to change which shortcut is used, first update the Internal Dial Plan then modify the shortcuts.

When the configuration changes are complete, click Update to save the settings.

## 23.2 Recording Auto Attendant Greetings and Messages

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

- Day Mode Greeting (or Night Mode Greeting, depending on the time of day)
- Custom Message
- Other configured prompts.

Note: After all prompts have been played, if the caller presses \* to hear the selections again, the Day-Night Mode greeting is skipped.

Follow these steps to record a new greeting:

1. Dial the Auto Attendant extension (431-439<sup>†</sup>) you want to change. You will hear the default welcome greeting.

Note: If the system is configured for Dual Language Support, the new greetings and messages will be associated with the current language in this Auto Attendant. To record greetings and messages for an alternate language for use by this Auto Attendant, switch languages before proceeding to the next step.

2. Dial # and 9.
3. After the beep, enter the Administrator password, followed by the pound sign.
4. Choose the Greeting or Message to be recorded.

Dial	Greeting
1	Day Mode Greeting
2	Night Mode Greeting
3	Custom Message
4	Manage Call Queues
#	Return to the Auto Attendant

<sup>†</sup> Extensions may vary per system. If you are using a non-default Internal Dial Plan, consult the Phone Features tab of the My Allworx Manager page to determine what extensions are being used for the corresponding feature.

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

5. 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
Day Mode	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.
Night Mode	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 . . .

6. Now select:

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

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

## 23.3 Assigning the Auto Attendant to an Outside Line

It is straightforward 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.

<b>Outside Line</b>	
<b>Description</b>	CO Line - 01 (typically enter phone number of line connected to the Allworx)
<b>Port:</b>	01
<input checked="" type="checkbox"/> <b>Enable Line Appearance</b>	
<b>Default Language</b>	Primary Language
<b>Features</b>	
<input type="checkbox"/> <b>Line has Caller ID service</b>	
<input type="checkbox"/> <b>Optimize for short loops</b>	(typically unchecked, check for FXD/IADs less than 500 ft. away)
<b>Prefix Digits</b>	(digits dialed by the Allworx after it seizes the line, before user dials)
<b>CPC Disconnect timer</b> (Open Loop Disconnect)	350 milliseconds
<b>Pre-dial delay</b>	500 milliseconds (typically 500ms)
<b>DTMF Duration</b>	100 milliseconds (typically 100ms)
<b>DTMF Gap</b>	100 milliseconds (typically 100ms)
<b>Default Auto Attendant</b>	
Select the attendant used to answer when calls received from this source are routed to an Auto Attendant.	
Auto Attendant 1 (x431)	
<b>Call Route</b>	
<b>Calls received from this CO line go to:</b>	
<input type="radio"/> <b>Extension</b>	choose an extension
<input checked="" type="radio"/> <b>Auto Attendant</b>	
<input type="radio"/> <b>Voicemail for user</b>	Alex Smith (asmith)

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

## 24 Call Monitors

Call Monitors are call routing destinations that allow one call to ring multiple phones. Multiple calls can ring a single Call Monitor. Calls are answered in first in, first out (FIFO) order.

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.

### 24.1 Configuring a Call Monitor

#### 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.

#### Set up 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 voicemail, transfer to queue, and dial number, upon completion of connection attempts.

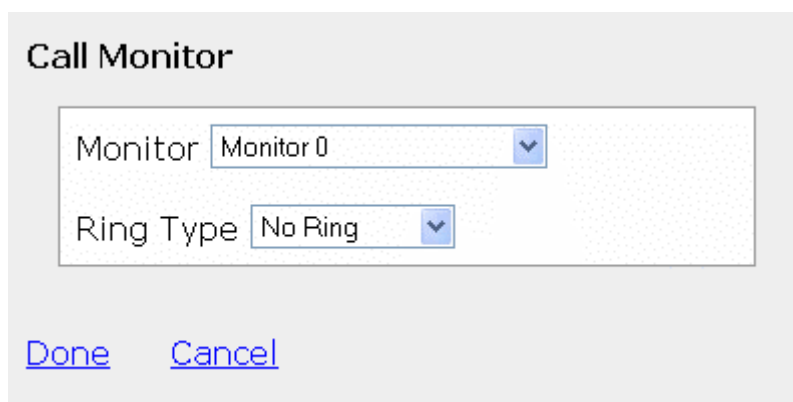
Note: One or more Call Monitors can be programmed into a call route.

### 24.2 Call Monitor with an Allworx IP Phone

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

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:



The image shows a 'Call Monitor' configuration window. It has a title bar 'Call Monitor'. Inside, there are two dropdown menus. The first is labeled 'Monitor' and has 'Monitor 0' selected. The second is labeled 'Ring Type' and has 'No Ring' selected. At the bottom of the window, there are two buttons: 'Done' and '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.

In addition, 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.



## 24.3 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.

### **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 Function 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.

### **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, 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.

## 25 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 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. Each parked call is held in a slot at an extension between 701 and 709<sup>†</sup>. When a call is parked, it is assigned the lowest available slot number. These slots are referred to as Parking Orbits.

The *Allworx Phone Guide* describes how a call is placed into and retrieved from a Parking Orbit.

### 25.1 Configuring Call Parking Orbits

The parked call timeout (10 to 3600 seconds) and the call routing pattern at timeout can be configured from the Phone System / Call Park page. The call can be transferred to any system extension or return to the Call Appearance of the handset that originally parked the call. By default the timeout duration is set to 600 seconds and the routing is 'Transfer call to the Default Auto Attendant'.



### 25.2 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.

<sup>†</sup> Extensions may vary per system. If you are using a non-default Internal Dial Plan, consult the Phone Features tab of the My Allworx Manager page to determine what extensions are being used for the corresponding feature.

6. Set the particular Parking Orbit (701 – 709<sup>†</sup>) 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 elapsed 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.

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 so the station's HOLD button can be used to automatically do either local station HOLD operations or automatic PARK operations with a minimal number of manual steps.

**Note:** The only option for parking calls using analog phones or 3<sup>rd</sup>-party IP phones is to perform an announced location park by transferring the call to extension 700<sup>†</sup>.

---

<sup>†</sup> Extensions may vary per system. If you are using a non-default Internal Dial Plan, consult the Phone Features tab of the My Allworx Manager page to determine what extensions are being used for the corresponding feature.

## 26 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 IN/OUT jack or terminal block of the associated server. If used at a site, one typically hooks the LINE IN/OUT jack or terminal block 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 IN/OUT jack or terminal block as 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.

### 26.1 Paging Amplifier and Door Release Relay

Allworx servers have an internal relay that can be used to control a door release mechanism. This makes it possible to dial a phone extension to allow someone entry to a secured area. The relay contacts are available via the DB-9 connector (9-pin D shell serial type connector) or terminal block on the Allworx server. See the server's installation instructions for details.

When using the LINE IN/OUT jack, the relay operation mode must be 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<sup>†</sup>. The relay will activate for the duration of the phone call or five (5) seconds, whichever 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.

### 26.2 Paging Zone Names

The name assigned to each of the paging zones (0 - 9 and corresponding extensions 460 - 469<sup>†</sup>) 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.

<sup>†</sup> Extensions may vary per system. If you are using a non-default Internal Dial Plan, consult the Phone Features tab of the My Allworx Manager page to determine what extensions are being used for the corresponding feature.

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.

## 26.3 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.

---

<sup>†</sup> Extensions may vary per system. If you are using a non-default Internal Dial Plan, consult the Phone Features tab of the My Allworx Manager page to determine what extensions are being used for the corresponding feature.

## 27 Dual Language Support

The Allworx server supports having a second language in addition to US English for audio prompts heard by users of the system. The system can be configured to play one language in particular circumstances and a different language in others. Callers can be permitted to switch between the two languages by pressing '##'. This is an optional feature that requires the Dual Language Support feature key.

Note: Only the default audio prompts are available in languages other than US English. Text on the Web Admin pages and telephone displays are in English.

Some important aspects of Dual Language support:

- US English is factory-installed as the Primary language. A Language Pack (available from the Allworx Reseller Portal) can be installed and selected as either the Primary or Secondary language.
- Points of origin of new calls (Outside Lines, Users, and handset Call Appearances) are each assigned a language. The language is configurable but defaults to Primary.
- The language of the prompts played by the following call applications in the Allworx system can be configured to use the language of the call's point of origin or override it with a specific language:
  - Auto Attendants
  - Queues
  - Leaving Voicemail
  - Phone Features (When Call Park, Call Forward, Do Not Disturb extensions are dialed)
  - Conference Center
  - Follow Me
  - Message Center
- The following applications can be configured to permit users to switch languages by pressing '##'.
  - Auto Attendants
  - Queues
  - Conference Center
  - Follow Me
  - Message Center
- Applications that allow switching can be configured to play a language change prompt. The prompt will be played in the opposite language. That is, the prompt "To switch to English, press ##" will be spoken in English when played for an Auto Attendant that is configured with Spanish prompts.
- Custom greetings and messages for Auto Attendants and Queues can be recorded separately for the Primary and Secondary languages. The recordings are saved as Primary and Secondary and are not associated with the specific language. Therefore, if the actual language that is used as Primary changes, the original Primary custom recordings will continue to be used when the system is using the new Primary language. The same is true for recordings assigned to the Secondary language. To re-assign the Primary recordings to the Secondary language and vice-versa, the recordings must be exported then imported to the desired language.
- Calls that come into the system from Remote Allworx servers will retain the language that was being used by the remote system, unless overridden by application language settings on the local server.

Note: All interconnected Allworx servers must run the same release of software and be outfitted with the same languages.



## 27.1 Language Pack Installation

The system's default language is US English. Once the Dual Language Support feature key has been added to the system, additional languages can be installed.

To install an additional language:

1. Download the language pack from the software download page of the Reseller Portal at [www.allworx.com](http://www.allworx.com).
2. Unzip the download and copy the language pack (.alp) file onto the PC.
3. Log into the Allworx Administration page.
4. Navigate to Phone System / Languages.
5. In the Language Pack Installation and Removal section of the page, click the Browse or Choose button.
6. Navigate to the location of the language file on the PC. Select the .alp file and click Open.
7. Click the Install button.
8. If the installation was successful, choose the Modify link next to Server Language Configuration.
9. Select the new language for the Primary or Secondary language, as desired.
10. Choose a second available language (e.g. US English) as the Primary or Secondary language then click Update. The Languages page is displayed.
11. For the changes to take effect, the server must be restarted. Click the restart link to view the restart options. Reboot the server in Normal Mode.
12. Once the reboot is complete, log in and navigate to the Languages page. Verify that the languages are configured, as desired. Using the procedures below, configure the system behavior.

## 27.2 Language Settings

### 27.2.1 Outside Lines

Each outside line has a default language. When calls are received over an outside line, they are assigned the default language for that line. Thereafter, when the call reaches some applications within the server (e.g. Auto Attendant, Queue), the outside line language will be used or overridden, depending on the application's language setting.

Outside line default language can be set in the following locations:

- CO Line
- SIP Proxy
- SIP Gateway

- DID Routing Plan – Default route
- DID Routing Plan – Mapped extensions
- Digital Lines – Each line

Default Language choices:

- Primary – When calls from the outside line are routed to applications within the Allworx System (e.g. Auto Attendants, Queues, Conference Center), if the application's language is set to Automatic, the prompts will be played in the system's Primary language.
- Secondary – When calls from the outside line are routed to applications within the Allworx system, if the application's language is set to Automatic, the prompts will be played in the system's Secondary language, if one has been installed.
- Use Source (DID Routing Plans only) – When calls from the DID line are routed to applications within the Allworx System, if the application's language is set to Automatic, the prompts will be played in the language choice that was set for the outside line that is using the DID Routing Plan. For example, if a SIP Proxy's default language is Secondary and the default language of the extension mapped in the DID Routing Plan is Use Source, calls will be assigned Secondary as their language.

Note: In a DID Routing Plan, if a default language other than Use Source is selected, the DID Routing Plan's default language will override the Outside Line's language.

To set the default language for an Outside Line:

1. Navigate to Phone System / Outside Lines.
2. Choose the CO, Digital, SIP Gateway, or SIP Proxy to be configured.
3. Locate the Default Language list box.
4. Pull down the list and select the desired setting.
5. Select the Update button.

## 27.2.2 Remote Allworx

The default language for calls coming from a Remote Allworx server cannot be set. These calls will already have been assigned a default language on the remote server. For language selection in a multi-site installation to work properly, all servers must be running the same software version and have the Dual Language Support feature key installed.

## 27.2.3 Call Appearances

Call Appearances can be used to originate calls. Therefore, each has a default language setting. For each phone's Call Appearances, choose the language that best meets the needs of the user(s) of the phone. If a phone has multiple Call Appearances, the Call Appearances can be assigned different default languages.

When calls from the Call Appearance are routed to applications within the Allworx System (e.g. Auto Attendants, Queues, Conference Center), the Call Appearance language will be used or overridden, depending on the application's language setting.

To set the default language for a Call Appearance:

1. Navigate to Phone System / Handsets.
2. Locate the handset to be configured.
3. Click on the Modify link for the desired Call Appearance.

4. Locate the Default Language list box.
5. Pull down the list and select the desired language.
6. Select the Update button.

## 27.2.4 Call Applications

Various applications (e.g. Auto Attendants, Queues) within the Allworx system play audio prompts. The language behavior of the prompts can be controlled using the settings on the Phone System / Languages Web Admin page. Select the modify link next to the Call Application Language Settings section label to change the following individual settings:

### Answer Language

This setting controls the language of the prompts using the following options:

- Primary – Prompts will be played in the Primary language. This overrides the call's current language.
- Secondary – Prompts will be played in the Secondary language, if one is installed. This overrides the call's current language.
- Automatic – Prompts will be played in the call's current language. For calls coming from an Outside Line or Call Appearance, the default language of the call's origin will be used. If calls came from some other application (e.g. the call came into a Queue from an Auto Attendant), the language that was used in the previous application (e.g. Auto Attendant) will be used.

### Allow Language Change

When a call reaches an application, this setting permits the caller to switch languages, if they desire. To switch languages, callers must press the pound key twice (##). To permit callers to change language, for the desired application, check the box in the Allow Language Change box.

### Language Change Prompt

When a call reaches an application (except for when leaving a voicemail message or when using phone features), this setting controls whether a prompt to change language is played using the following options:

- Always play – Every time a call reaches the application, in addition to the prompts that are normally played, the prompt to change the language is played (e.g. "To switch to English, press ##")
- Never play – The prompt to change the language is not played. This is useful when the prompt to change language can be incorporated into a custom greeting or message. This option is not available for Follow-Me-Anywhere prompts.
- If Needed – The prompt will not play if the caller has already had a chance to change languages in a prior application. For example, if a Queue's Language Change Prompt setting is If Needed and a call is routed directly to the queue from an outside line, the language change prompt would be played. If the call came through an Auto Attendant in which language changing was permitted, then the prompt would not be played. In this case the prompt is not played because the caller already had a chance to choose their preferred language.

## 27.2.5 User Default Language

In addition to the settings already described, Allworx users have a default language setting. This language choice is used when accessing the Message Center and when receiving Follow-Me-Anywhere calls. If the

Message Center Answer Language is Automatic, when a user logs into their Message Center account, their default language will be used, without regard to the outside line or call appearance they used to access their account. Similarly with Follow-Me-Anywhere calling, if the Follow-Me external phone number is called from within the user's extension route, when the user answers the call, they will hear the prompts in their default language. However, if the application's Answer Language is set to Primary or Secondary, that setting will override the user's default language.

## 27.3 Custom Messages

Custom greetings and messages for Auto Attendants and Call Queues can be recorded, exported, and loaded for either or both the Primary and Secondary languages.

See Section 23.1, Configuring the Auto Attendant, and Section 23.2, Recording Auto Attendant Greetings and Messages for information on recording greetings and messages. Information on exporting and loading custom message files is available within the Web Admin pages. Navigate to Phone System / Languages / Manage Custom Recordings.

## 27.4 Configuration Examples

### Example 1

A company has some clients that are English-speaking and others that are Spanish-speaking. Clients call to speak to company employees that speak the same language as they do. English-speaking clients are given one phone number while Spanish-speaking clients are given another.

#### Configuration

System Primary Language=English

System Secondary Language=Spanish

CO Line 1: Default language=Primary, routed to Auto Attendant 1

CO Line 2: Default language=Secondary, routed to Auto Attendant 1

All applications: Answer Language=Automatic, Allow Language Change=Enabled, Language Change Prompt=Always play

#### Result

English-speaking clients call the English phone number (CO Line 1) and are routed to Auto Attendant 1 where they hear English prompts as well as a prompt to switch to Spanish. Callers dial their representative's extension. All additional prompts will be in English such as the prompt to leave a voicemail or the Follow-Me-Anywhere prompt to record their name.

Spanish-speaking clients call the Spanish phone number (CO Line 2) and are routed to Auto Attendant 1 where they hear Spanish prompts as well as a prompt to switch to English. Callers dial their representative's extension. All additional prompts will be in Spanish such as the prompt to leave a voicemail or the Follow-Me-Anywhere prompt to record their name.

### Example 2

A company has a Customer Support operation in which some technicians are English-speaking and some are French Canadian-speaking. The company has one incoming line for Customer Support calls.

In this example, all callers are directed to the same Auto Attendant. English-speaking callers will dial a shortcut to a support queue that is serviced by the English-speaking technicians. French Canadian-speaking callers will be switch to a second Auto Attendant and then dial a shortcut to a queue that is serviced by the French Canadian-speaking technicians.

## **Configuration**

System Primary Language=English

System Secondary Language=French Canadian

T1 Language (all lines)=English

Auto Attendant 1: Answer Language=Primary, Allow Language Change=disabled

Call Queue 1: Answer Language=Primary, Allow Language Change=disabled

Auto Attendant 2: Answer Language=Secondary, Allow Language Change=disabled

Call Queue 2: Answer Language=Secondary, Allow Language Change=disabled

Auto Attendant 1 has two shortcuts

Dial 1 for x432 (Auto Attendant 2)

Dial 2 for x4401 (Call Queue 1)

Auto Attendant 2 has one shortcut

Dial 1 for x4402 (Call Queue 2)

Auto Attendant 1 has a custom message that says:

“For French Canadian, press 1” (recorded in French Canadian)

“To speak with Customer Support, press 2” (recorded in English)

Auto Attendant 2 has a custom message that says:

“To speak with Customer Support, press 1” (recorded in French Canadian)

## **Result**

Callers will be directed to Auto Attendant 1 where they will hear an English greeting, a prompt to press 1 for French Canadian, and a prompt to press 2 for Customer Support.

English callers will press 2 to enter Queue 1 where they will hear the greeting and status messages in English. Their call will be serviced by an English-speaking technician.

French Canadian callers will be directed press 1 to enter Auto Attendant 2 where they will hear the full greeting and prompts in French Canadian including a prompt to press 1 for Customer Support. They will press 1 to enter Queue 2 in which they will hear the greeting and status messages in French Canadian. Their call will be serviced by a French Canadian-speaking technician.

## 28 System Settings Import / Export

System Administrators will be able to transfer settings from one server to another by exporting the settings from one and importing them into the other. This will ease the task of upgrading a site from one Allworx server model to another model.

Not all settings can be transferred in this way. Import/Export is not a substitute for using Allworx OfficeSafe to backup the system. The following is a list of the settings that can be exported and imported:

An export will include all configurable parameters for:

- Users
- System extensions
- Allworx handsets
- Analog phones
- Allworx Port Expander (including all attached analog phones and CO lines)
- Outside lines:
  - CO Lines
  - Digital Lines
  - SIP Gateways
  - SIP Proxies
- DID blocks and routing
- Digital line configurations
- User Privilege Groups
- Handset Preference Groups
- Dialing Privilege Groups

To export configuration settings, select the Export button. This will place the current system settings into an XML file. Next, click the [View](#) link to save the exported XML file for import on to another system.

The server that is to receive the imported configuration settings should be “clean”, meaning none of the above configurations have been added to the system prior to import. Update the internal dial plan and extension length to match the configuration being imported before the import is performed.

To load the exported configuration settings of one server onto another, enter the full pathname of the XML file into the Load a configuration file field and then select the Load button.

The screenshot displays two sections of the Allworx System Administrator's Guide. The top section, titled "Export Configuration", contains a button labeled "Export" followed by the text "configuration settings to a file.". The bottom section, titled "Import Configuration", contains a message: "A configuration file has not been loaded onto the server. Before you can import configuration settings, you must first load a configuration file." Below this message is a label "Load a configuration file: (enter the full pathname of the configuration file)" followed by a text input field containing the path "C:\Users\qausser\Desktop\log\Server Export\6x\2006-2-4\export\_1.xml" and a "Browse..." button. At the bottom of this section is a "Load" button and a note in parentheses: "(it may take a few minutes to load a configuration file)".

Once the file has been loaded, all configuration settings to be imported will be displayed. The System Administrator can exclude parameters from the import by unchecking the associated box. To finish the import process, select the Import button.

**Import Configuration**

the checked entries.

**User Templates**

Name
<input checked="" type="checkbox"/> Sales Dept

**Handset Preference Groups**

Name
<input checked="" type="checkbox"/> Tech Support

**Dialing Privileges Groups**

Name
<input checked="" type="checkbox"/> Marketing Dept

**Users**

User	Extension
<input checked="" type="checkbox"/> Alex Smith (asmith00)	1001

**System Extensions**

Ext.	Description
<input checked="" type="checkbox"/> 1002	test

**CO Lines**

Description	Port
<input checked="" type="checkbox"/> Verizon	01

**Analog Handsets**

Description	Owner	Port
<input checked="" type="checkbox"/> Peter Albright		04

**Phones**

Description	Owner	Model	MAC Address	Line Num
<input checked="" type="checkbox"/> Noel A Umbridge		Allworx 9212	00-0A-DD-80-01-27	1
<input checked="" type="checkbox"/> Mary Copper		Allworx 9202	00-0A-DD-82-00-20	1
<input checked="" type="checkbox"/> Alex Smith	asmith00	Allworx 9224	00-0A-DD-80-01-46	1

**Digital Lines**

Description	Port
<input checked="" type="checkbox"/> Digital Line 1	T1-A
<input checked="" type="checkbox"/> Digital Line 2	T1-B

the checked entries.
   
 import.

## Important Notes

- The port numbers assigned to native CO lines and analog handsets can be modified when importing the settings.
- When importing a Allworx Px 6/2Port Expander, all configured CO lines and analog handsets from the export are included. The port assignments cannot be modified.



- DID blocks and routes plans and digital lines do not appear on the Import Configuration screen. These settings will always be imported when included on the export.
- Digital line fields PPP Username, PPP Password and PPP MTU are not include in the export.
- If the current system is not “clean” and has conflicts with the imported configuration settings, then conflicts will be resolved for the import settings in the following manner:
  - Digits will be appended to user login names and incremented, starting at 01, as needed (e.g. jAdams will become jAdams01)
  - Extensions will be changed to the lowest available extension
  - Phones with conflicting MAC addresses will not be imported and all references will be removed (e.g. call routing and BLF PFK assignments)
  - Analog phones with no available port will not be imported and all references will be removed (e.g. call routing and BLF PFK assignments)
- SIP handsets and SIP gateway station numbers may not be preserved on an import. If station numbers are changed for generic SIP phones or SIP gateways, then the new station number must be set up on each device.
- On Multi-site configurations, the Export will not include references to extensions, users or outside lines at remote sites.
- Imported extensions/users are limited to the total number available in the imported system. The available extensions/users are determined by the order in the export file. If the imported server's extensions/user limit is exceeded, the remainders are disabled and will not be imported.
- The XML export file should not be modified.
- Server with version 7.0 will export only user, system extension and Allworx handset parameters and only a subset of these parameters. Exports from 7.0 can be imported into servers with 7.1 or greater versions. Exports from 7.1 or greater cannot be imported into servers with 7.0.

## 29 Abbreviations

BLF – Busy Lamp Field

DHCP – Dynamic Host Configuration Protocol

DID – Direct Inward Dialing

DND – Do Not Disturb

DNS – Domain Name System

DOD – Direct Outward Dialing

DTMF – Dual Tone Multi-Frequency

FTP – File Transfer Protocol

FXO – Foreign Exchange Office

FXS – Foreign Exchange Station

HTTP – Hypertext Transfer Protocol

IP – Internet Protocol

ISP – Internet Service Provider

ITSP – Internet Telephony Service Provider

LAN – Local Area Network

NAT – Network Address Translation

PBX – Private Branch Exchange

PFK – Programmable Function Key

PoE – Power Over Ethernet

POP – Post Office Protocol

PPTP – Point-to-Point Tunneling Protocol

RTP – Real-time Transport Protocol

SIP – Session Initiation Protocol

SMTP – Simple Mail Transfer Protocol

SNTP – Simple Network Time Protocol

TCP – Transmission Control Protocol

UDP – User Datagram Protocol

URI – Uniform Resource Identifier

VoIP – Voice over Internet Protocol

WAN – Wide Area Network