Allworx® System Software Version 9.1

Administrator Guide

Version: G

Updated October 7, 2022

Allworx® System Software Version 9.1

Administrator Guide

Copyright

Documentation

Software

Warranty

This warranty shall not apply to any products to the extent the defect or non-conformance is due to (A) accident, alteration, abuse, misuse, or repair not performed by Allworx, (B) storage other than specified, (C) failure to comply with applicable environmental requirements for the products.

Environmental Conditions

Allworx premise servers and phones:

Operating:	
Temperature	+5° to 40° C / +41° to +104° F
Relative Humidity	5 to 90% (non-condensing)
Storage:	
Low Temperature Point	-40° C / +40° and any convenient humidity
High Temperature Point	+66° C / +150° 15% RH
High Relative Humidity Point	+32° C / +90° 90% RH

Allworx switches:

Operating:	
Temperature	+0° to 40° C / +32° to +104° F
Relative Humidity	10 to 90% (non-condensing)
Storage:	
Temperature	-20° C to +70° C (-4° F to +158° F)
Relative Humidity	10 to 90% RH

Trademarks

The following trademarks are owned by Allworx:

Allworx® Verge™ IP phone series
Allworx® 92xx™ IP phone series
Allworx® Verge™ 9304
Allworx® Verge™ 9308
Allworx® Verge™ 9312
Allworx® Verge™ 9318Ex

Allworx® Reach™
Allworx® Reach Link™
Allworx® Extend™

Allworx® Interact™
Allworx® Interact™ Professional
Allworx® Interact Sync™
Allworx® Interact Softphone™

Allworx® View™
Allworx® View™ ACD

Allworx® OfficeSafe™
Allworx® Migrate™
Allworx® PowerFlex™

Allworx® Connect™ servers
Allworx® Connect™ Vx service
Allworx® Connect™ 731 server
Allworx® Connect™ 536/530 server
Allworx® Connect™ 536 server
Allworx® Connect™ 530 server
Allworx® Connect™ 324/320 server
Allworx® Connect™ 324 server
Allworx® Connect™ 320 server

The Bluetooth® word mark and logos are registered trademarks owned by the Bluetooth SIG, Inc. and any use of such marks by Allworx is under license. Other trademarks and trade names are those of their respective owners.

Revision History

Revision	Date	Description
A	24-SEP-2021	New release for software version 9.1. This is the first release that supports the Allworx Connect Vx service. Information has been added throughout the document to indicate differences in the features available for all of the Connect server models and the Connect Vx instances.
B	21-OCT-2021	Additional updates throughout the document for software version 9.1.
C	24-NOV-2021	Additional updates throughout the document for software version 9.1.
D	25-MAR-2022	Additional updates throughout the document for software version 9.1 that includes support for Px Expanders, the Migrate application, and the ability to be run on both Connect Vx instances and Connect premise servers.
E	01-JUN-2022	Additional updates to provide information about the local Paging feature and Feature Key updates available with Connect Vx service in software release 9.1.3.7. These changes were applied in the *Paging* and *Feature Keys* chapters. Information about the changes needed to accommodate the Google Gmail SMTP setting changes have also been added to the setting description tables in the *Users* and *Email* chapters.
F	08-AUG-2022	Updates to the following chapters: Call Queues/ACD, Handsets, Paging, Px Expander, and Feature Keys. These updates include changes for release 9.1.4.8.
G	07-OCT-2022	Updates for release 9.1.5.6. Description of the new features that apply to both Allworx premise servers and Connect Vx instances. Including user roles available across multi-sites, site name included in multi-site emergency call notifications, disabling of POP3 and IMAP servers, PFK pages available on Verge 9304 and 9308 phones, and the option to delete short voicemails.

Part 1 Introduction

The Allworx System Software Version 9.1 is an application used by Allworx administrators to configure and manage settings for the following:

- *Phone System*
- *Network*
- *Servers*
- *Reports*
- *Maintenance*

Software version 9.1 provides support for the Allworx® Connect™ Vx service which is the Allworx Connect System Software executing on a virtual machine in the Allworx data centers. The Connect Vx service provides the flexibility of the data center in a licensed monthly service.

The Connect Vx service uses the same award-winning, stable software code base used in the Allworx Connect line of premise servers. A Connect Vx instance is a single occurrence of the Connect Vx service dedicated for use by a single business.

Access to the available settings is through the Allworx System Administration web page that has built-in descriptions, help, and tips on many of its pages. Additional information is available in these documents related to Allworx System Software and Allworx applications:

- *Allworx Connect Server family Installation Guide* (premise servers only)
- *Allworx System Software Release Notes for Release 9.1*
- *Allworx My Allworx Manager User Guide*
- *Allworx Advanced Multi-Site Guide*
- *Allworx OfficeSafe Operations Guide* (premise servers only)
- *Allworx SNMP User's Guide* (premise servers only)
- *Allworx Interact Release 5.0 (with support for Interact Softphone) User's Guide*
- *Allworx Reach User's Guide*
- *Allworx View Installation Guide*
- Allworx phone guides
- *Application Notes* for Multi-Tech FaxFinder Setup (third-party products)

All Allworx publications are available when you log in to the Allworx Portal (allworxportal.com) and navigate to **Support & Training** > **Documentation**.

1.1 Who Should Read this Guide

This guide is for Allworx administrators who understand computer networking and basic telephony, have completed the Allworx Partner technical training, and will be responsible for installing and maintaining Allworx servers.

1.2 Guide Organization

This *Allworx Server Administrator Guide* describes the requirements to perform the procedures in this document. Including the following:

- Steps necessary to install, log in, and configure the Allworx premise server.

  Note: *To view the mounting, electrical connections, and input/out accessories of the Allworx* premise *server, see the Allworx Connect Server Family Installation Guide.*

- Steps necessary to manage each Allworx System Administration web page to configure the Allworx premise server and Connect Vx instance. Each administration web page is described in a separate chapter within this document.

1.3 Equipment Requirements

The table below is a complete list of equipment requirements necessary to perform the Allworx System Administration web page operations identified in this guide.

Equipment	Requirements
PC	• Running OS (with latest service pack). • Windows 8/8.1 32-bit • Windows 10 32-bit • Windows 8/8.1 64-bit • Windows 10 64-bit • Windows Server 2012/2012R, 2016, and 2019 • RAM minimum: 2 GB • Monitor resolution: 1024 x 768 (XGA) • Internet connection
Allworx premise server or Connect Vx instance	• Allworx System Software Version 9.1 • Administration permissions and passwords for each Allworx server • IP Address or DNS name of each Allworx premise server or Connect Vx instance
Allworx Portal (allworxportal.com)	• Login permissions and password
Supported Web Browsers	• Microsoft Edge • Microsoft Internet Explorer 11 (latest release with auto upgrade enabled) • Google Chrome (Latest Release) • Mozilla Firefox (Latest Release)

Equipment	Requirements
Additional Documents	
Allworx Connect Server Family Installation Guide (premise servers only)	The guide is specific to the Allworx server model that describes the mounting, electrical connections, and input/output accessories of the Allworx Server. This guide is available on the Allworx Portal at allworxportal.com.
My Allworx Manager User Guide	The guide is specific to My Allworx Manager and describes the features within that application. This guide is available on the Allworx Portal at allworxportal.com.
Allworx Advanced Multi-Site User Guide	The guide describes the advanced set up configurations for multi-site networks. This guide is available on the Allworx Portal at allworxportal.com.
Allworx Verge IP Phone Series Guides	The guide describes the operation, features, and configuration options for Verge devices. This guide is available on the Allworx Portal at allworxportal.com.

1.4 Prerequisites

Each chapter of this document includes a table that lists the prerequisite permissions and feature keys needed for access to the software feature described in that chapter. The following table describes those tables.

Access Permissions	Identifies features that users with assigned roles can access and manage. The Allworx Server Administrator can assign roles to a specific user on the **Phone System** > **Roles** page. See “Roles” on page 3 for more information.
Required Feature Key	Identifies add-on features that are available as a separate purchase from the base feature set for Allworx servers. See “Feature Keys” on page 345 for more information.

1.5 Roles

The following user roles are available.

- **Server Administrator**: Predefined system administrator with access to manage all functions of the Allworx premise server or Connect Vx instance. The Allworx Server Administrator assigns roles, manages the system software administrative functions, manages day-to-day phone system settings, manages the network and VoIP settings, and initiates system backups and/or restarts.
- **System Administrator**: Access to manage the administrative functions of the Allworx premise server or Connect Vx instance. This user permission setting does not allow this role to change the password of the Allworx Server Administrator; however, the Allworx Server Administrator can change the password of the System Administrator.
- **Phone Administrator**: Access to manage day-to-day phone system settings including changes to system recordings, as well as adding, changing, and deleting users, extensions and handsets.

- **Network Administrator**: Access to manage the Network and VoIP settings, as well as SIP proxies and SIP gateways outside lines.
- **Support Technician**: Access to initiate system backups and restarts as well as managing logging operations.

Notes:

- *To enable one user to have roles on different servers in a multi-site network, the Allworx administrator must create separate user accounts for the user on each server, and then assign the roles on each server. Use different user names for each account.*
- *The Allworx administrator can assign users to manage queue and Auto Attendant recordings. See “User Template Settings” on page 233 for more information.*
- *The Allworx administrator can assign users to manage individual queue settings or queue supervisor. See “User Template Settings” on page 233 for more information.*

Contents

Part 2 Allworx System Software Configuration

This section describes the installation and configuration procedures for Allworx Connect premise servers and the Connect Vx service. Configuration is completed using the Allworx System Administration web page. Additionally, this section describes the Allworx System Software compatibility of each Allworx premise server and Connect Vx.

Prerequisites	
Access Permissions	Allworx Server Administrator Allworx System Administrator
Feature Key Required	No
Servers	All

***Note:** Installation of the Allworx Connect Vx service (Allworx System Software Version 9.1) is completed by Allworx Support at the Allworx data center. Configuration of those Connect Vx instances is completed using the Allworx System Administration web page.*

2.1 Allworx System Software Compatibility

Allworx System Software	Allworx Connect Server Model					
	320	324	530	536	731	Vx
System Software 8.0 ***Note**: Version 8.0 is the last software version to support the 24x server.*	✓	✓	✓	✓	✓	
System Software 8.1 through 8.5 ***Note**: Version 8.5 is the last software version to support the x-series servers (6x12, 6x, and 48x).*	✓	✓	✓	✓	✓	
System Software 8.6	✓	✓	✓	✓	✓	
System Software 9.0	✓	✓	✓	✓	✓	
System Software 9.1	✓	✓	✓	✓	✓	✓

2.2 Allworx Server Features and Compatibility

Feature	Allworx Connect Server Model					
	320	324	530	536	731	Vx
Hardware Support						
Network Ports	2	2	3	3	3	
Enhanced Diagnostic Serial Port provides easier connection and faster data transfer	✓	✓	✓	✓	✓	
Supported Web Browsers						
Microsoft Internet Explorer 11	✓	✓	✓	✓	✓	✓
Google Chrome (latest version)	✓	✓	✓	✓	✓	✓
Mozilla Firefox (latest version)	✓	✓	✓	✓	✓	✓
Microsoft Edge	✓	✓	✓	✓	✓	✓
Allworx System Software 9.1						
First support for the Connect Vx service.						✓
Automatic daily backups to cloud storage with restoration completed by Allworx Support.						✓
Automatic software updates outside of business hours.						✓
Automatic failover of server hardware, Internet connection, and system power provided by the Allworx data center.						✓
Ability to assign a role to a user and have that user enjoy the role on the other servers within a multi-site network.	✓	✓	✓	✓	✓	✓
Emergency email notifications include the site name that originated the call from within a multi-site network.	✓	✓	✓	✓	✓	✓

Feature	Allworx Connect Server Model					
	320	324	530	536	731	Vx
Administrators can now disable POP3 and IMAP servers.	✓	✓	✓	✓	✓	✓
Ability to automatically delete short voicemail messages and never save them.	✓	✓	✓	✓	✓	✓
Allworx System Software 9.0						
System extensions can be selected as the owner of a phone handset	✓	✓	✓	✓	✓	✓
Phone plug and play (PnP) system extension assignment and PnP disabled by default	✓	✓	✓	✓	✓	✓
One free Interact Softphone license included with this version	✓	✓	✓	✓	✓	✓
Increase in the number of system extensions available	✓	✓	✓	✓	✓	✓
Allow **Message Center** and **Operator** as selections in the *Primary Dial Plan - Dial Number* and the *Public Contact > Phone Number* fields	✓	✓	✓	✓	✓	✓
Option to suppress the Dialing audio message when transferring from an Auto Attendant	✓	✓	✓	✓	✓	✓
Park notifications automatically disabled when a Park to Extension programmable function key is deleted	✓	✓	✓	✓	✓	✓
By default, the server now uses the music file supplied with the 9.0 software to play as music on hold	✓	✓	✓	✓	✓	✓
By default, *Use Extension Mode* is selected in the *Internal Dial Plan*	✓	✓	✓	✓	✓	✓
Custom logo image can be uploaded for display on Verge phone sleep screens	✓	✓	✓	✓	✓	✓

Feature	Allworx Connect Server Model					
	320	324	530	536	731	Vx
Automatically sends an email to the user alerting them that their Voicemail box is full – no additional configuration for users already receiving Voicemails as emails	✓	✓	✓	✓	✓	✓
Automatically plays a message alerting the Message Center user that their Voicemail box is full – no configuration required	✓	✓	✓	✓	✓	✓
New PFK Programming report provides a searchable listing of the programmable function keys and features assigned to each Verge phone, Interact Softphone, and Reach handset	✓	✓	✓	✓	✓	✓
Enable alert that provides increased visibility of the indicator that the user is in the Busy/No Answer state	✓	✓	✓	✓	✓	✓
Allworx System Software 8.6						
Support for Allworx Interact version 5.0 (with support for Interact Softphone)	✓	✓	✓	✓	✓	✓
Support for up to 1975 users and 1975 system extensions across a multi-site network of Allworx Connect servers ***Note:*** *There is no change to the number of users/system extensions that can be defined on each server.*	✓	✓	✓	✓	✓	✓
Option for ACD agents that miss a call to return to the Ready state after a configurable time delay (Allworx Verge and Allworx Interact Softphone users only).	✓	✓	✓	✓	✓	✓
On-Phone assignment of user or system extensions on phones added using the Allworx System Administration web page - including the Quick Add feature.	✓	✓	✓	✓	✓	✓
Enhancements to the Emergency Call email notifications (emails) and moves this setting to the Emergency Caller ID page on the Allworx System Administration web page.	✓	✓	✓	✓	✓	✓

Feature	Allworx Connect Server Model					
	320	324	530	536	731	Vx
Allworx System Software 8.5.3 or Higher						
Programmable Button Pages	✓	✓	✓	✓	✓	✓
Tone Configuration for Emergency Alert PFK	✓	✓	✓	✓	✓	✓
Enter Configuration Notes	✓	✓	✓	✓	✓	✓
Custom Voicemail to Email Signature	✓	✓	✓	✓	✓	✓
New Default Ring Type Settings for Some PFKs	✓	✓	✓	✓	✓	✓
Enhanced Incoming Call Handling	✓	✓	✓	✓	✓	✓
Reboot All Phones Assigned to a Handset Preference Group	✓	✓	✓	✓	✓	✓
Add Phones and Assign to Users Via CSV Upload	✓	✓	✓	✓	✓	✓
Increased System Event Log Capacity	✓	✓	✓	✓	✓	✓
Create Allworx Handsets Using a Serial Number (Bar Code Support)	✓	✓	✓	✓	✓	✓
Improved SIP Handling for Anonymous Calls	✓	✓	✓	✓	✓	✓
Delete Associated Routing Plan When Deleting a DID Block	✓	✓	✓	✓	✓	✓
Allworx System Software 8.5						
Support up to 250 users					✓	✓
Support for up to 60 users			✓	✓		
Secure Remote Administration	✓	✓	✓	✓	✓	✓

Feature	Allworx Connect Server Model					
	320	324	530	536	731	Vx
Upload and Manage Public Contact images	✓	✓	✓	✓	✓	✓
Import Audit PIN Codes from CSV File	✓	✓	✓	✓	✓	✓
Built-In Music on Hold Options	✓	✓	✓	✓	✓	✓
Include PIN/Password require change when importing users from a CSV file	✓	✓	✓	✓	✓	✓
Extended UTF-8 French and Spanish character support	✓	✓	✓	✓	✓	✓
Select codecs for SIP Proxies or SIP Gateways	✓	✓	✓	✓	✓	✓
Customizable SIP port numbers	✓	✓	✓	✓	✓	
Park to Extension	✓	✓	✓	✓	✓	✓
Incoming call notifications	✓	✓	✓	✓	✓	✓
Dynamic programmable button configuration	✓	✓	✓	✓	✓	✓
Call forward indicator ***Note:*** *Calls cannot be forwarded to phones at different sites within a Multi-Site network.*	✓	✓	✓	✓	✓	✓
User-specific Hot Desk settings	✓	✓	✓	✓	✓	✓
Secure HTTPS when logging into phone admin web page.	✓	✓	✓	✓	✓	
Restore OfficeSafe backup within same Connect server series.	✓	✓	✓	✓		
Allworx System Software 8.4						
Verge 9304 IP Phone	✓	✓	✓	✓	✓	✓

Feature	Allworx Connect Server Model					
	320	324	530	536	731	Vx
Override the current day/night mode and/or greetings from the Audio Message Center	✓	✓	✓	✓	✓	✓
Option to require callers to listen to the greeting/custom message completely	✓	✓	✓	✓	✓	✓
Automatically retrieve feature keys	✓	✓	✓	✓	✓	✓
Enhanced support for international phone numbers (E.164 formats)	✓	✓	✓	✓	✓	✓
Allworx System Software 8.3.7 or Higher						
ACD Queues: Option to disable “No agents logged in alarm setting			✓	✓	✓	✓
Allworx System Software 8.3						
Option to reset custom recordings for Call and ACD Queues	✓	✓	✓	✓	✓	✓
View, upload, and manage directory contact photos	✓	✓	✓	✓	✓	✓
Options menu for callers leaving a Voicemail message	✓	✓	✓	✓	✓	✓
DND programmable button	✓	✓	✓	✓	✓	✓
Support Centrex flash signals on CO lines	✓	✓	✓	✓	✓	
Reach Push Notifications	✓	✓	✓	✓	✓	✓
Reach Extend	✓	✓	✓	✓	✓	✓
Allworx System Software 8.2.14 or Higher						
ACD Queues: Option to disable “No agents logged in” alarm setting	✓	✓	✓	✓	✓	✓

Feature	Allworx Connect Server Model					
	320	324	530	536	731	Vx
Allworx System Software 8.2						
Control permissions for users to manage their directory contact image (8.2.7.x)	✓	✓	✓	✓	✓	✓
Delete a user’s directory contact image (8.2.7.x)	✓	✓	✓	✓	✓	✓
Verge phone series	✓	✓	✓	✓	✓	✓
Expanded set of Ring Types	✓	✓	✓	✓	✓	✓
Hand off between Reach and Verge phones	✓	✓	✓	✓	✓	✓
Reach Remote Control	✓	✓	✓	✓	✓	✓
Sharing Personal Contacts with all of user’s Allworx devices and applications	✓	✓	✓	✓	✓	✓
Maximum number of Personal Contacts **with** images per user.	1,100	1,100	1,100	1,100	1,100	1,100
Maximum number of Personal Contacts **without** images per user.	7,000	7,000	7,000	7,000	7,000	7,000
Total number of Personal Contacts **with** images per server (approximate).	24,000	24,000	60,000	60,000	215,000	215,000
Total number of Personal Contacts **without** images per server (approximate).	144,000	144,000	360,000	360,000	1,290,000	1,290,000
Allworx System Software 8.1						
Five- and six-digit dialing[5]	✓	✓	✓	✓	✓	✓
Number of Auto Attendants Supported	9	9	16	16	32	32
Allworx System Software 8.0						
Reach Link Support	✓	✓	✓	✓	✓	✓

Feature	Allworx Connect Server Model					
	320	324	530	536	731	Vx
SSH Support	✓	✓	✓	✓	✓	
Allworx Server Features						
FXO Ports	0	4	0	6	2	0
FXS Ports	2	2	2	2	2	0
T1 Ports	0	0	0	0	1	0
Base System Extensions Limit	12	12	30	30	30	30
Maximum System Extensions Limit[1]	20	20	60	60	250	250
Base Users	12	12	30	30	30	5
Maximum Users[1]	20	20	60	60	250	250
Maximum Handsets	40	40	100	100	360	360
Maximum External Calls[3]	12	12	30	30	60	60
Conference Bridges[1]	1	1	1	1	4	0
Maximum Callers per Conference	8	8	8	8	30	0
Maximum callers in all conferences combined	8	8	8	8	30	0
Maximum Calls in All Queues[1]	12	12	30	30	60	60
Maximum Calls per Queue[1]	12	12	30	30	60	60
Maximum Number of Queues[1]	10	10	10	10	10	10
Automatic Call Distribution[1]	No	No	Yes	Yes	Yes	Yes
Auto Attendant Ports	4	4	8	8	16	16
Multi-Site Controller[1]	Yes	Yes	Yes	Yes	Yes	Yes
Maximum Servers in a Multi-Site Network	99	99	99	99	99	99
Maximum Multi-Site System Extensions[4]	1975	1975	1975	1975	1975	1975
Maximum Multi-Site Users[4]	1975	1975	1975	1975	1975	1975

Feature	Allworx Connect Server Model					
	320	324	530	536	731	Vx
Voicemail Ports	4	4	8	8	15	15
Activation Required	✓	✓	✓	✓	✓	✓
Secure Web Page Access	✓	✓	✓	✓	✓	✓
Enhanced Codec Support	✓	✓	✓	✓	✓	✓
SIP-Video Pass-Through [2]	✓	✓	✓	✓	✓	✓

[1] Requires an Allworx software feature key.

[2] A SIP endpoint that supports video can register with the Allworx Connect server, and it supports negotiation of video calls with that device. The Allworx Connect server supports up to two video sessions and one audio session per call. The Allworx Connect server supported codecs are: H263, H264, and MP4V-ES.

[3] The total external SIP calls are limited to the *Maximum External Calls* less any TDM (FXO ports and T1 channels) lines configured.

[4] The total number of multi-site users and multi-site system extensions varies upon the maximum users licensed on each Allworx premise server.

[5] Compatible with Reach for Android/Reach for iOS Version 2.0.7 (min) and Interact/Interact Professional 2.3 (min).

2.3 Verge Phone Series Software Compatibility

The Verge phone series requires the following minimum software versions:

Product/Resource	Software Version	
	Verge 9304	Verge 9308/9312/9318 Ex
Allworx System Software	8.4	8.2
Interact Professional	3.12	3.0
Interact Softphone	N/A	N/A
Reach for Android	N/A	3.0
Reach for iOS	N/A	3.0

Note: *The Connect Vx service (Allworx System Software 9.1) supports the Allworx Verge IP phone models Verge 9312, 9308, 9304, and the Verge 9318Ex Expander and Px Expander.*

2.4 Installing and Configuring Allworx Premise Servers

Note: *Installation of Allworx Connect Vx instances is completed by Allworx Technical Support at the Allworx data center. For information, see “Configuring Connect Vx Instances” on page 28.*

To install the Allworx Connect premise servers:

1. Use the *Allworx Connect Server Family Installation Guide* for mounting, electrical connections, and optional input/output accessories specific to the Allworx server model.
2. Plug the PC into the server LAN port (**ETH0**), and set up the network interface on the PC to obtain an IP address automatically (using DHCP).

OS	Instruction
Windows Server 2012	1. Click **Start** and navigate to the Control Panel. 2. Locate **View by**: select **Small Icons** from the drop-down list. 3. Double-click **Network and Sharing Center**. 4. Click **Change adapter settings** in the left column. 5. Right-click **Local Area Connection** > **Properties**. ***Note:*** *For wireless computers, select* ***Wireless Network Connection*** *>* ***Properties***. 6. Click **Internet Protocol Version 4 (TCP/IPv4)** > **Properties**. 7. Click **Obtain an IP Address automatically** and **Obtain DNS server address automatically.** 8. Click **OK** to save the changes.

OS	Instruction
Windows 8 / Windows 10 and Windows Server 2016 and higher	1. Click **Start** and navigate to the Control Panel. In the search box, type **adapter**. 2. Click **Network and Sharing Center**, and then click **View network connections.** 3. Locate and right-click the connection to change, and then click **Properties**. 4. (Optional) If prompted, enter the administrator credentials and confirm. 5. Click to select the *Networking* tab, and then click **Internet Protocol Version 4 (TCP/IPv4)** or **Internet Protocol Version 6 (TCP/IPv6)** > **Properties**. Specify the address settings: IPv4 — Click **Obtain an IP address automatically**, and then click **OK**. IPv6 — Click **Obtain an IPv6 address automatically**, and then click **OK**.

3. Verify that the PC has an IP address on the 192.168.2.x network. It may be necessary to release and renew the IP address on the PC to get an address from the premise server.

   a. Click *Start* and type `cmd` in the *Search* field. A command window opens. Type the following to clear the PC current IP settings:

   ```
   ipconfig /release
   ```

   b. Press **Enter** to clear the PC current IP settings. Type the following to obtain a new IP Address:

   ```
   ipconfig /renew
   ```

   c. Press **Enter**.

4. Use a web browser via the LAN interface on TCP port 8443 to access the Allworx System Administration web page for the Allworx premise server. Enter **https://192.168.2.254:8443** in one of the browsers listed in "Supported Web Browsers" on page 2.

5. Log in to the Allworx System Administration web page using **admin** as both the user name and password. The web page displays the factory default settings at first log in and displays the customized settings with any subsequent log in.

   The server is ready to be configured.

To configure the Allworx Connect premise server:

1. Log in to the Allworx System Administration web page using **admin** as both the user name and password.

2. Locate the left navigation pane of the Allworx System Administration web page and click **Install Checklist.**

3. For a successful configuration follow the order of the steps in the Install Checklist. When a step is complete, click the check box on the Allworx System Administration web page next to each step to avoid duplication. The online Install Checklist provides links to the areas of the Allworx System Administration web page where the steps are performed.

The following Installation Checklist table provides links to the appropriate *Allworx System Software Administrator Guide* chapter for more information about the step.

Installation Checklist for Configuring Connect Server Models 320, 324, 530, 536, and 731

Step	Description	More Information
1	Set the time on server.	"Time" on page 369.
2	For Connect 731 servers only: Program T1 Lines. If connected to T1 interface(s), configure the system to match the settings obtained from the service provider.	"T1 Lines" on page 251.
3	Set the server network configuration: • Network Mode • VLAN settings • Public Interface • Gateway • Server Host Name • Domain Name • Firewall Settings	"Configuration" on page 245.
4	Enable or Disable the DHCP server.	"DHCP" on page 279.
5	Set the DNS server addresses.	"DNS" on page 281.
6	*Optional:* Configure the Px Expanders.	"Px 6/2 Expanders" on page 265.
7	Enable a VPN, if required.	"Virtual Private Network (VPN)" on page 275.
8	Restart server for settings to take effect. ***Note:*** *After restarting the server, close the Install Checklist window, and then re-open it after logging into the server.*	"Restart / Shutdown" on page 363.
9	Activate the server through the Allworx Portal, if it is not already activated.	"Registration" on page 359.
10	Download and enter the required Feature Keys.	"Feature Keys" on page 345.
11	Update the Allworx server to the latest software release, if required.	"Update" on page 381.
12	*Optional:* Configure the use of Primary and Secondary Languages.	"Languages" on page 159.
13	Define the Internal Extension Length and Internal Dial Plan.	"Managing the Internal Extension Length" on page 68. "To manage the Internal Dial Plan:" on page 70.

Step	Description	More Information
14	Add users and associate handsets to users, if available.	“Managing Users” on page 225.
15	Add handsets. Add the Analog and SIP Handsets using Plug and Play or manual programming. Once programmed, check the phone by dialing **#7** from any Auto Attendant Main Menu.	“Managing Analog Handset Configuration” on page 155. “Managing the Allworx Handset Configuration” on page 117.
16	If live answering inbound calls, create a system extension and preferred call routes. Use a Ring Group if live answer with line appearances on Allworx handsets is required. If different sets of handsets need to ring depending on the incoming line, give a descriptive name to a Ring Group, create an extension for each incoming line, and route the call to the Ring Group. Configure the Allworx handsets later to use the Ring Group(s) defined in this step.	“Adding a New Extension” on page 91. “Ring Groups” on page 213
17	Define additional system extensions used for routing to groups or places such as conference rooms.	“Adding a New Extension” on page 91
18	*Optional:* Create and define Call Queues	“Call Queues/ACD” on page 51
19	*Optional:* Define Paging Zones. Define the Paging Zones, add Line Out or Handsets to the required zones.	“Paging” on page 195
20	Add and Configure Outside Lines to the phone system (standard FXO loops, SIP Gateways, SIP Proxies). Enable line appearances, if required, and define call routes.	“Outside Lines” on page 175
21	Configure Allworx handsets by defining the Programmable Function Keys (PFKs).	“Managing the Programmable Function Keys (PFKs)” on page 138
22	*Optional:* Save the Allworx handset configuration as a template, and then apply that template to remaining Allworx handsets. Modify individual handset configurations as required.	“Creating and Using Handset Templates” on page 134
23	Program the operator route (**0**).	“Managing Call Routes” on page 97
24	Record Auto Attendant and Call Queue prompts, if required.	“Custom Recordings” on page 339
25	Set the Dial Plan for the system. Create special Service Groups, if required, and then define the Dialing Rules.	“Dial Plan” on page 67

Continued

Step	Description	More Information
26	Check handset permissions to access outside resources, if required.	“Handsets” on page 103
27	Enter business contact information and schedules.	“Business Information” on page 45 “Schedules” on page 215
28	Check the system: 1. Make 3 to 4 inbound calls (e.g., use cell phone to call the Allworx server). 2. Make outbound local and long distance calls to several area codes.	NA
29	Configure the Email server. 1. Leave incoming WAN email forwarding disabled, unless the server is within a firewall. 2. Enter alternate email domains. 3. Enter spam blocking services (e.g., spamhaus.org).	“Email” on page 283
30	Enable a VPN for additional users, if required.	“Managing Users” on page 225
31	Create aliases for email and Voicemail distribution lists.	“Message Aliases” on page 165
32	Set up and perform a backup using OfficeSafe.	“Backup” on page 337
33	Conduct basic training for each user. • Deliver user documentation: • *Allworx Verge IP Phone Series Quick Start Guide* • *Verge IP Phone Series Function Card* • *FAQs for Allworx Verge IP Phones Users* • *Allworx Verge IP Phone Series Users Guide* • *My Allworx Manager User Guide* • Deliver User Training Videos: • *Allworx Verge IP Phone Overview* • *Using Your Verge IP Phone* • *Using Programmable Buttons (PFKs)* • *Using the Allworx Message Center (Voicemail)* • *Using Contacts*	• Documentation is available by navigating to **Support & Training** > **Documentation** when you log in to the Allworx Portal (allworxportal.com). • Training Videos can be accessed in two ways: • From the Allworx website at allworx.com/resources – select either **Videos - Product Overview** or **Videos - User Training** from the drop-down list in the middle of the page. • From the Allworx Portal (allworxportal.com) – Click the video link on the Support & Training page. The *Allworx Training Video Clicksheet* can be opened from the first link on that page and provides a listing with links to the videos. The *Clicksheet* is a PDF that can be shared with end users so they can access the training videos without having to log in to the Allworx Portal.

2.5 Configuring Connect Vx Instances

Installation of Allworx Connect Vx instances is completed by Allworx Support at the Allworx data center. Configuring Connect Vx instances is outlined in the following table.

Note: *For the Connect Vx service, Allworx provides a unique, strong password for the administrator account. This password must be changed at the first log in and strong passwords are required.*

Configuration Checklist for Connect Vx Instances

Step	Description	More Information
1	Check the time on server.	"Time" on page 369.
2	Program the Network configuration: set the Network Set the server network configuration: • Host Name • Fully Qualified Domain Name	"Configuration" on page 245.
3	Restart server for settings to take effect. ***Note****: After restarting the server, close this window, then open it again after logging in to the server.*	"Restart / Shutdown" on page 363.
4	*Optional:* Configure the Px Expanders.	"Px 6/2 Expanders" on page 265.
5	Activate the Vx instance using the Allworx Portal, if required.	"Registration" on page 359.
6	Download and enter the required Feature Keys, if required.	"Feature Keys" on page 345.
7	(Optional) Configure use of the Primary and Secondary Language.	"Languages" on page 159.
8	Define the Internal Extension Length and Internal Dial Plan.	"Managing the Internal Extension Length" on page 68. "To manage the Internal Dial Plan:" on page 70.
9	Add users. Associate handsets to users, if available.	"Managing Users" on page 225.
10	Add handsets. Add the SIP handsets using Plug and Play or manual programming. Once programmed, check the phone by dialing #7 from any Auto Attendant main menu.	"Managing Analog Handset Configuration" on page 155. "Managing the Allworx Handset Configuration" on page 117.

Continued

Step	Description	More Information
11	If live answering inbound calls, create a system extension and preferred call routes. Use a Ring Group if live answer with line appearances on Allworx handsets is required. If different sets of handsets need to ring depending on the incoming line, give a descriptive name to a Ring Group, create an extension for each incoming line, and route the call to the Ring Group. Configure the Allworx handsets later to use the Ring Group(s) defined in this step.	"Adding a New Extension" on page 91. "Ring Groups" on page 213
12	Define additional system extensions used for routing to groups or places such as conference rooms.	"Adding a New Extension" on page 91
13	(Optional) Create and define Call Queues.	"Call Queues/ACD" on page 51
14	Add and Configure Outside Lines to the phone system (SIP Gateways and SIP Proxies). Enable line appearances, if required, and define call routes.	"Outside Lines" on page 175
15	Configure Allworx handsets by defining the Programmable Function Keys (PFKs). Select the *View Configuration* link for each handset.	"Managing the Programmable Function Keys (PFKs)" on page 138 "Managing Programmable Functions for Interact Softphone" on page 151
16	(Optional) Save the Allworx handset configuration as a template, and then apply that template to remaining Allworx handsets. Modify individual handset configurations as required.	"Creating and Using Handset Templates" on page 134
17	Program operator route (0).	"Managing Call Routes" on page 97
18	Record Auto Attendant and Call Queue prompts, if required.	"Custom Recordings" on page 339
19	Set the Dial Plan for the system. Create special Service Groups, if required, and then define the Dialing Rules.	"Dial Plan" on page 67
20	Check handset permissions to access outside resources, if required.	"Handsets" on page 103
21	Enter business contact information and schedules.	"Business Information" on page 45 "Schedules" on page 215

Continued

Step	Description	More Information
22	Check the system: 1. Make 3 to 4 inbound calls (e.g., use cell phone to call the Allworx server). 2. Make outbound local and long distance calls to several area codes.	NA
23	Configure the Email server. 1. Leave incoming WAN email forwarding disabled, unless the server is within a firewall! 2. Enter alternate email domains. 3. Enter spam blocking services (e.g., spamhaus.org).	"Email" on page 283
24	Create aliases for email and Voicemail distribution lists.	"Message Aliases" on page 165
25	The Allworx data center automatically performs frequent backups. More information can be found on the **Maintenance** > **Backup** page.	For more information contact Allworx Support.
26	Conduct basic training for each user. • Deliver user documentation: • *Allworx Verge IP Phone Series Quick Start Guide* • *Verge IP Phone Series Function Card* • *FAQs for Allworx Verge IP Phones Users* • *Allworx Verge IP Phone Series Users Guide* • *My Allworx Manager User Guide* • Deliver User Training Videos: • *Allworx Verge IP Phone Overview* • *Using Your Verge IP Phone* • *Using Programmable Buttons (PFKs)* • *Using the Allworx Message Center (Voicemail)* • *Using Contacts*	• Documentation is available by navigating to **Support & Training** > **Documentation** when you log in to the Allworx Portal (allworxportal.com). • Training Videos can be accessed in two ways: • From the Allworx website at allworx.com/resources – Select either **Videos - Product Overview** or **Videos - User Training** from the drop-down list in the middle of the page. • From the Allworx Portal (allworxportal.com) – Click the video link on the Support & Training page. The *Allworx Training Video Clicksheet* can be opened from the first link on that page and provides a listing with links to the videos. The *Clicksheet* is a PDF that can be shared with end users so they can access the training videos without having to log in to the Allworx Portal.

Part 3 Phone System

The *Phone System* sections describe the setup and management of the phone system settings specific to the business requirements. Each chapter explains the following:

- Necessary access permissions and feature keys
- Equipment required to perform the procedure
- Procedures to manage the Allworx feature

Feature and procedure differences for the Allworx Connect Vx service are noted in each chapter.

The various *Phone System* pages on the Allworx System Administration web page allow the Allworx administrator to set up, configure, and manage the settings of the following features.

Chapter 3 Audit PIN Code

Audit PIN Code supports call tagging and controlling outside line access. The Audit PIN Code does not support outside line access when using a Line Appearance PFK.

Prerequisites	
Access Permissions	Allworx Server Administrator Allworx System Administrator Phone Administrator role
Feature Key Required	No

Example:

A company charges customers for the tolls and time spent on each call.

To use tagging to properly bill each customer:

- The Allworx administrator assigns each project a unique PIN code.
- The phone user dials 78[1] <PIN code prefix> + <PIN code specific to the project> + <phone number> to access the outside line to work with the customer.
- The accounting department uses the PIN code from the call records to bill each customer.

To specify the number of digits and the service group used by the Audit PIN Code, see “Managing the Services” on page 82 for more information.

Allworx premise servers and Connect Vx instances support:

- Adding multiple PIN codes and associated descriptions from a CSV file
- Performing a bulk delete on the configured PIN codes
- Exporting and importing all PIN codes defined on the Allworx premise servers and Connect Vx instances to the admin PC

To manage an Audit PIN code:

1. Log in to the Allworx System Administration web page and navigate to **Phone System** > **Audit PIN Codes**. Locate the *Audit PIN Codes* pane.

2. Click to select one of the following actions:

Action	Description
add new PIN code	Enter the new PIN code and description in the respective fields, and then click **Add** to save the changes. To change the PIN code length, see “Managing the Services” on page 82.

Continued

[1] Extensions may vary per system. If using a non-default Internal Dial Plan, consult the *My Allworx Manager Phone Functions* tab to determine what extensions to use for the corresponding feature.

Action	Description
add PIN Codes from CSV file	Import multiple PIN codes with a Comma Separated Value (CSV) file. 1. (Recommended) Perform a full system backup before adding multiple PIN codes. 2. Create a CSV file using any text editor or Microsoft Excel and the required attributes (columns): *PIN Code* and *Description*. The CSV file must meet the following requirements: PIN code length must match the length value configured on the Allworx System Administration web page *Dial Plan* page. • PIN codes must only contain the digits **0** through **9**. • PIN code or description values cannot be empty. • Descriptions cannot contain any of the following characters: **% < > ; :** • Descriptions cannot be longer than 32 characters. 3. Click **Choose File**. Locate the file and click **Open** > **Load** > **Process**. 4. Verify that the column heading represents the data supplied. Use the drop-down list to assign the column headings. To not include a column, select a heading value of **Skip**. 5. Review the rows to add. Uncheck a row to exclude it from the import. 6. Click **Add** to import PIN codes. A message appears indicating the number of PIN codes successfully added and/or which PIN codes descriptions were updated. Additional details about skipped users may be available in the system events log. 7. Click **Done** to return to the *Audit PIN Codes* list or **Continue** to repeat this process.
Download PIN Codes to CSV file	Export all current PIN codes defined on the premise servers and Connect Vx instances to a CSV file. This saves the PIN code information file to the PC.
Bulk Edit	Delete multiple PIN codes from the Allworx server by selecting the PIN codes, and then clicking the **Delete** button.
Modify	Change the description. Click **Update** to save the changes.
Delete	Remove the PIN code from the list stored on the server. 1. Confirm this is the PIN code to remove. 2. Click **Delete** to remove the PIN code from the list or **Cancel** to disregard the change.

To enable or disable the Audit PIN Code Verification:

1. Log in to the Allworx System Administration web page and navigate to **Phone System** > **Audit PIN Codes**.

2. Locate the *Audit Pin Code Configuration* pane and click **modify**.

3. Select one of the following options from the drop-down list:

Option	Description
Enabled (default)	The Allworx premise server or Connect Vx instance verifies that the PIN code is the correct length and loaded in the PIN code list.
Disabled	The Allworx premise server or Connect Vx instance only checks for the correct PIN code length.

4. Click **Update** to save changes. Click **Cancel** to ignore the request.

Click here to return to the Installing and Configuring Allworx Premise Servers or Configuring Connect Vx Instances .

Chapter 4 Auto Attendants

Prerequisites	
Access Permissions	Allworx Server Administrator Allworx System Administrator Phone Administrator role
Feature Key Required	No

Answer incoming calls automatically, and then direct the callers to the appropriate person or department using the dial-by-name or company phone directory.

Each Auto Attendant supports the Open and Closed greeting, up to 7 custom greetings, and one custom message with a length limit of 15 minutes per greeting or message. Users with permissions can record and manage custom Auto Attendant greetings and messages or assign each Auto Attendant to a different schedule. See "Number of Auto Attendants Supported" on page 20 for the number of Auto Attendants each Allworx premise server or Connect Vx instance supports.

Example: Use one Auto Attendant to answer calls for Sales and another Auto Attendant to answer calls for Support. Each Auto Attendant plays a greeting specific to the assigned department.

4.1 Setup Checklist

Follow this order of the steps to successfully setup the Auto Attendant. Click the links in the column on the right for more information about each step.

Step	Description	More Information
1	Configure the Auto Attendant.	"Configuring the Auto Attendant" on page 37
2	Create an extension and/or assign the Auto Attendant to an outside line, and then update the call route to the Auto Attendant.	"Extensions" on page 91 or "Managing Analog Central Office (CO) Lines" on page 178
3	Record the custom greetings and messages for each Auto Attendant.	"Recording Auto Attendant Greetings and Messages" on page 41
4	Configure Auto Attendant greetings to change per time of day.	"Schedules" on page 215

4.2 Configuring the Auto Attendant

If the premise server or Connect Vx instance is part of a multi-site network with premise servers or Connect Vx instances that support a higher number of Auto Attendants, users on the premise server or Connect Vx instance at the lower numbered site cannot be included in the higher numbered Auto Attendants configured at another site. Therefore, assign the lower numbered Auto Attendants so that users on the premise server or Connect Vx instance with the least number of Auto Attendants can be included.

Example: Site 1 uses a Connect 324 server (9 Auto Attendants) and Site 2 uses a Connect 731 premise server (32 Auto Attendants). Assign the Auto Attendants used on both sites (e.g. Sales, Tech Support) to Auto Attendants 4301, 4302, etc. to assign users from Site 1 to the Auto Attendant. Users from Site 1 cannot be assigned to Auto Attendant 4310.

To configure an Auto Attendant:

1. Log in to the Allworx System Administration web page and navigate to **Phone System** > **Auto Attendants**. The Auto Attendants display with the assigned extension (4301 to 43xx[1] - where xx is the maximum number of Auto Attendants supported by the Allworx premise server or Connect Vx instance) and Auto Attendant number.
2. Locate the Auto Attendant and click the additional information arrow ►, if necessary. Click one of the following links:

Link	Description
modify	Change the Auto Attendant configuration. Select the settings to update in the drop-down list. See the Auto Attendant Configuration Settings table for more settings information.
reset	Change the configuration to the factory defaults. Select an option: • Reset to default settings, but keep all custom recordings • Delete all custom recordings • Reset to default settings AND delete all custom recordings Click **Reset** to update the settings or **Cancel** to leave the settings as is.
copy	Copies the selected Audio Attendant settings, and optionally custom recordings, and saves them under a new name.

3. Click **Update** to save the settings.

Auto Attendant Configuration Settings

Features and Prompts

Setting	Description
Description	Enter description of the Auto Attendant.
Schedule	Select the schedule created for switching greetings. See "Schedules" on page 215 for more information.
Remote Multi-Site Users	For multi-site networks: • *included in Dial-By-Name and Dial-By-Directory Menus* • *excluded from Dial-By-Name and Dial-By-Directory Menus*

Continued

[1] Extensions may vary per system. If using a non-default Internal Dial Plan, consult the My Allworx Manager Phone Functions tab to determine what extensions to use for the corresponding feature.

Setting	Description
Dial-By-Name Menu (#1)	Enable callers to select an Allworx user by typing the user's name based on the setting in the *Dial-By-Name Spell Options* field. • *enabled* • *disabled* (Default) **Note:** *Requires user to record their name greeting in order to be available in the directory*.
Dial-By-Name Prompt	Prompt: *Press 1 to dial by name*. • *do not play* • *play* (Default)
Dial-By-Name Spell Options	Select the spelling method for the Dial-By-Name option. • *spell first or last name* • *spell last name* • *spell first name*
Dial-By Directory Menu (#2)	Enable the caller to listen to a list of users and extensions, and then enter an extension. • *disabled* • *enabled* (Default) **Notes**: • *The Allworx system disables Dial-By-Directory if assigning more than 50 users to the Auto Attendant.* • *Requires user to record their name greeting to be available in the directory.*
Dial-By-Directory Prompt	Prompt: *Press 2 for a listing of all users and extensions*. • *do not play* • *play* (default) **Note:** *The system automatically disables Dial-By-Directory if assigning more than 50 users to the Auto Attendant.*
Dial-By-Directory List Order	Controls the order in which the directory is spoken. • *list in extension order* • *list in name order*
Dial It Now Prompt	Prompt: *If you know your party's extension you may dial it now.* • *do not play* • *play* (default)
Dialing...Prompt	Plays or does not play the audio dialing message callers hear when they are transferred from the main menu of an auto attendant. This feature is not available, and has no effect on, auto attendant sub menus. • *do not play* • *play* (default) *Continued*

<table>
<tr><th>Setting</th><th>Description</th></tr>
<tr><td><i>Repeat Menu Behavior</i></td><td>Identifies what repeats when requested by the caller.
• <i>replay Custom Message only</i>
• <i>replay Greeting Only</i>
• <i>replay Greeting and Custom Message</i></td></tr>
<tr><td><i>Repeat Options Prompt</i></td><td>Prompt: Press * to listen to these choices again.
• Do not play
• Play (default)</td></tr>
<tr><td><i>Play greeting/ custom messages to completion</i></td><td>Require callers to listen to the greeting/custom message completely. Options include:
• Disabled (default) - callers press a dial pad button to skip both the greeting and the custom message.
• Greeting and custom message - callers cannot skip the greeting or the custom message.
• Greeting only - callers cannot skip the greeting.</td></tr>
<tr><td><i>Speed Dial Numbers</i></td><td>(support for dialing 350-399, 34000-34999* from main menu)
(listed as *250-*299 AND *24000-*24999)
• Allowed
• Not Allowed (default)</td></tr>
<tr><td><i>Day Mode Menu Shortcuts /</i>
<i>Night Mode Menu Shortcuts</i></td><td>Identifies if users can dial the Menu Shortcuts in Day or Night Mode for each Auto Attendant.
• Allowed (default)
• Not Allowed</td></tr>
<tr><td><i>Day Mode Internal Call Restriction</i>
<i>Night Mode Internal Call Restriction</i></td><td>Restricts what internal calls can be made from each Auto Attendant based on the day mode.
• Auto Attendant Default - blocks all calls except the following (examples are from the Default Dial Plan, 3-digit, not using extension mode):
<table>
<tr><td>• Operator (x0)</td><td>• User and System Extensions (x1nn, x2nn)</td></tr>
<tr><td>• Conference Center (x408)</td><td>• Speed Dial 3 and 5 digits (x350-300, x34nnn)</td></tr>
<tr><td>• Other Auto Attendants (x400, x43n)</td><td>• Leave a message (x3 + user extension)</td></tr>
<tr><td>• Call Queues (x44n)</td><td>• Message Center for user (x6 + user extension)</td></tr>
<tr><td>• Message Center (x404)</td><td>• &lt;List of available restrictions&gt;</td></tr>
</table></td></tr>
<tr><td><i>After</i></td><td>Select the number of seconds (1 to 15) with no input, and then indicate the next step.
• Replay Menu
• Transfer to <select an extension/user&gt;</td></tr>
</table>

Continued

Menu Shortcuts

The Allworx administrator can configure the Auto Attendant to enable dialing digits 0 through 9 as single-digit Menu Shortcuts. Dialing the digit transfers a caller to a designated extension, another Auto Attendant, Dial-By-Directory, or Dial-By-Name.

To use the *Dial-by-name* or *Dial-By-Directory* option, enable the option and set the *Dial-By-Name* or *Dial-By-Directory* prompts to **Do not play**.

Setting	Description
Day Mode Menu Shortcuts *Night Mode Menu Shortcuts*	Select one of the following options from the drop-down list: • **disabled -** turns off the Menu Shortcuts option. • **enabled** - select an extension in the drop-down list for the corresponding digit. The default assignment is ‘0 – operator’* and does not provide the option of Dial-By-Directory or Dial-By-Name. • **use Day Mode** - the Menu Shortcuts are the same for both Day and Night Mode. Available on Night Mode Menu Shortcuts only.

* Extensions may vary per system. If using a non-default Internal Dial Plan, consult the My Allworx Manager *Phone Functions* tab to determine what extensions to use for the corresponding feature.

4.3 Recording Auto Attendant Greetings and Messages

Auto Attendants play built-in or custom greetings and messages. Users with Recording Manager permissions can record the greetings off line up to 15 minutes in length, and then import the greetings into the system see “To import or export greetings and messages:” on page 43 for more information. Or, record up to nine greetings and one custom message for each Auto Attendant using the Message Center on the phone.

To enable Recording Manager permissions, see “To modify or delete existing users:” on page 228 and update the following settings:

Setting	Description
Roles	Select System or Phone Administrator for access to Auto Attendants.
Recording Manager	Select the specific Auto Attendants for the user.

The Allworx system plays the greetings, messages, and prompts in this order:

- Business schedule greeting – for the current time of day (See “Managing the Greetings” on page 215.).
- Custom message (this does NOT change based on the business schedule)
- Other selected built-in prompts

***Note:** When routing a caller to an Auto Attendant after playing all prompts, if the caller presses * to hear the selections again, the system skips the business schedule greeting.*

To record a new greeting / custom message or manage the Auto Attendant schedule:

Notes:

- *To modify the greetings (Auto Attendant) or custom messages, the Allworx user must have Allworx System Administrator or Allworx Phone Administrator role permissions.*
- *Allworx does not recommend using a Reach device to record new greetings or queue messages as the ability of the premise server or Connect Vx instance to record greetings is intolerant of network packet loss. As a result, recordings made via lossy networks may have impaired quality. Local or wired networks are best for making these recordings.*
- *For systems with Dual Language Support: Users cannot change languages within the Message Center. To record new messages in a second language, select one of the following options:*
    - *Setup an account configured for the secondary language, and then record the greetings using that account.*
    - *Temporarily modify the user's default language to match the secondary language of the system.*

1. Access the *Message Center* by doing one of the following:
    - Press the phone's Messages (✉) function button twice.
    - Dial **6** + the primary extension from any phone or the company Auto Attendant.
    - Dial **404**[1]. When calling from an outside line or phone not assigned to a user, the system prompts users for a primary extension.
    - (from an outside line dialing directly to your office) While the greeting is playing, dial ***6** + <extension> before the greeting finishes playing.
2. Enter the log in credentials using the assigned extension and PIN code.
3. Press **9** to manage the greetings, and then press **1** to manage the Auto Attendant.
4. Enter the Auto Attendant number (**1** to **xx**[1] – where **xx** is the total number of Auto Attendants supported by the Allworx premise server or Connect Vx instance). Press **1** to manage the greetings for that selected Auto Attendant.

    For example, to choose the Auto Attendant at extension 4309, enter **9#**.

    a. Enter the number (**0** through **8**) of the greeting to record.
    b. Press **2** to record a new greeting.
    c. Record the new greeting and press **#** when complete.
    d. Press **1** to save the greeting.
5. Press **1** to record additional greetings or press **#** to go to the previous menu.

[1] Extensions may vary per system. If using a non-default Internal Dial Plan, consult the My Allworx Manager Phone Functions tab to determine what extensions to use for the corresponding feature.

6. Press **2** to manage the custom message for the Auto Attendant.

Greeting	Sample Script
Greeting 0 (Open)	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.
Greeting 1 (Closed)	Welcome to <company name>, your best source for <product>. We are currently closed, but we will re-open at <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	<Company name> is the premier provider of <product>, specializing in <specialty>. Our latest product is...

To import or export greetings and messages:

Import the greetings and messages recorded off-line onto the Allworx system. The file names have a specific internal format. See "Custom Recordings" on page 339 for more information.

To manage the Auto Attendant schedule:

This option is only available to users with recording manager permissions on Allworx systems.

1. Log in to the Audio Message Center and press **9** on the numeric keypad.
2. Press **1** (to manage the Auto Attendant), and then select the Auto Attendant (4301 to 43xx[1] - xx is the total number of Auto Attendants supported by the Allworx premise server or Connect Vx instance) number to change.
3. Press **3** (to manage the schedule). The following message plays, "The Auto Attendant is using schedule <number>. To select a different schedule, enter the schedule number followed by #."
4. Enter the schedule number, and then enter the # sign. After successfully selecting a different schedule, the user hears, "The Auto Attendant has been changed to use schedule <number>." The Message Center returns to the Manage Auto Attendant Menu.

   If selecting a different schedule is unsuccessful, the user hears, "You must enter a valid schedule number." The Message Center returns to the Manage Auto Attendant Schedule Menu.

4.4 Assigning the Auto Attendant to an Outside Line

The default Auto Attendant determines the setting when selected in the configuration of the outside line. To assign the Auto Attendant to an outside line, see "Managing Analog Central Office (CO) Lines" on page 178 for more information. Follow the same procedure for any of the outside lines, including SIP Gateways and SIP Proxies.

Click here to return to the Installing and Configuring Allworx Premise Servers or Configuring Connect Vx Instances .

[1] Extensions may vary per system. If using a non-default Internal Dial Plan, consult the My Allworx Manager Phone Functions tab to determine what extensions to use for the corresponding feature.

Chapter 5 Business Information

Prerequisites	
Access Permissions	Allworx Server Administrator Allworx System Administrator Phone Administrator role
Feature Key Required	No

The Business Information feature allows the entering of information about the primary business contact.

Providing this information is recommended but not required.

To manage the business information:

1. Log in to the Allworx System Administration web page and navigate to **Phone System** > **Business Information**. The *Business Information* page appears.

2. Click **Modify** and enter the business information in the fields provided.

   For the activated Connect premise servers or Connect Vx instances, there is an option to import the customer business information from the registration information on the Portal.

3. Click **Update** to save change.

Click here to return to the Installing and Configuring Allworx Premise Servers or Configuring Connect Vx Instances .

Chapter 6 Call Park

Place a call in a system-wide hold location so that another phone can retrieve that call. The Allworx System provides two methods to park a call:

Prerequisites	
Access Permissions	Allworx Server Administrator Allworx System Administrator Phone Administrator role
Feature Key Required	No

1. System Park: places a call into the next available park location, and then a different phone can retrieve the call by dialing the park location number.

Example: Park a call for someone who is away from their phone, and then page the recipient to tell them to retrieve the call by dialing the parking orbit.

Notes:

- *If configured, the Park Monitor programmable button on Allworx 92xx IP phone displays the parked calls list showing only the parking orbit number not the actual park to extension recipient. Allworx does not recommend using the Park Monitor programmable button on Allworx 92xx IP phones with Park to Extension calls.*
- *The number of available parking locations on Allworx premise servers or Connect Vx instances is 59 using Parking Orbit extensions between 701 to 709 and 4950 to 4999. The parked call is assigned to the lowest available Parking Orbit number. Extensions may vary per system. If using a non-default Internal Dial Plan, consult the My Allworx Manager Phone Functions tab to determine what extensions to use for the corresponding feature.*

2. Park to Extension: places a call into a parking location for a specific user or group, if enabled. This feature is available in Allworx System Software 8.5 or higher. For information about finding the phone software version, refer to the *Allworx® Verge™ IP Phone Series User Guide* available on the Allworx Portal.

- Supports the Allworx User's connected applications such as the Reach application (including Reach Remote Control) and the Interact Professional and Interact Softphone application modes.
- Notifies the Allworx user if someone has parked a call on the extension or any extension of interest.
- NOT SUPPORTED on Allworx 92xx series IP Phones.

The Park to Extension feature provides the following functionality:

- Parking calls to designated single users or group extensions
- Notification of calls parked, if the user enables notifications
- Updates to the Parked Calls screen to indicate the destination of the Park to Extension calls (Verge phones only)

- Option to continue using the legacy System Park behavior
- Includes the recipient extension for Park to Extension calls or the parking location number for System Parked Calls in the **Reports** > **Call Details** report

6.1 Supported Allworx Applications and Devices

The Allworx System supports the following when parking a call:

	System Park	Park to Extension
Allworx System Software	All versions	Version 8.5 or higher
Allworx Phones	All phones	Verge phones only
Park Programmable Button	All Phones	Verge phones only
Reach Application (including Reach Remote Control)	Yes	Yes
Interact Professional Application Mode	Yes	Yes
Interact Softphone Application Mode	Yes	Yes
Multi-Site Networks	Yes	Yes

6.2 Definitions

The Park to Extension feature introduces new terminology associated with the Allworx system:

- System Park – (legacy Park behavior) places a call into the next available park location, and then a different phone can retrieve the call by dialing the parking location number.

  Example: Park a call for someone who is away from their phone, and then page the recipient to tell them to retrieve the call by dialing the parking orbit.

  - In versions Allworx System Software 8.4 and lower, this was titled “Park.” System parking across sites still requires setting up multi-site parking on the *Call Park* page.
  - Multi-site locations that result from that setup are used only for system-parked calls and would not use any of the 59 parking locations that are available for Park to Extension.
- Park to Extension – Places the call into a parking location for a specific user or group, if enabled. Only available on Allworx System Software 8.5 and higher.
- Retrieve Park from Extension – An Allworx user claims a parked call from a specific extension.
- Parked Call Notifications – Provides automatic notification to the Allworx user that someone parked a call for the extension or any extension of interest.

6.3 Setup Checklist

Follow the order of these steps to successfully set up the Park feature. Click on the links in the column on the right for more information about each step.

Step	Description	More Information
System Park (Default configuration)		
1	(Verge Phones only) Configure the *Park* soft key behavior and the *Parked Calls List Contents*. ***Note**: Allworx 92xx IP phones always perform a System Park when pressing the **Park** soft key or button.*	"Creating and Using Handset Preference Groups" on page 120
2	Configure the *System Park* settings.	"Configuring the System Park Settings" on page 50
3	(Optional) Configure Multi-Site parking.	"Configuring the System Park Settings" on page 50
Park to Extension		
1	Enable parking to specific extensions.	• Individual User: "To modify or delete existing users:" on page 228 • User Template: "Managing User Templates" on page 232 • System Extension: "Managing Extension Settings" on page 96 • Multiple User Extensions: "Managing Extension Settings" on page 96
2	(Verge Phones only) Configure the *Park* soft key behavior and the *Parked Calls List Contents*. ***Note**: Allworx 92xx IP phones always perform a System Park when pressing the **Park** soft key.*	"Creating and Using Handset Preference Groups" on page 120
3	(Verge Phones only) Configure the *Park to Extension* programmable button or buttons.	"Managing the Programmable Function Keys (PFKs)" on page 138
4	Configure the *Call Route* and *Park to Extension* call handling settings.	"Managing Call Routes" on page 97

6.4 Configuring the System Park Settings

This section describes only how to configure the settings for System Park. To configure settings for the Park to Extension feature, follow the links in the preceding table.

1. Log in to the Allworx System Administration web page and navigate to **Phone System** > **Call Park**.
2. In either of the information panes click **modify**.

Setting	Description
Call Park	
Timeout (seconds)	Enter a value in seconds for the call to timeout. Default is 600 seconds.
After timeout	Sends the call to the next stop in the call route. Options include: • Transfer caller to handset that parked call, on busy <select an extension from the drop-down list>. • Transfer caller to extension <select an extension from the drop-down list>. Default is the Default Auto Attendant.
Multi-Site Parking	
Permit other sites to retrieve parked calls from this site.	Enables users at other sites to retrieve calls parked in its Parking Orbits. • The premise server or Connect Vx instance must participate in Multi-Site Parking Orbits. All sites that participate share 150 Multi-Site Parking Orbits at extensions between 4800 and 4949[1]. • See the Allworx Advanced Multi-site User Guide for information on configuring Multi-site parking. 1. Check the box to enable. 2. Enter the number of parking orbits to use per site. The Call Park page displays the Number of Orbits and the Retrieve # for each site.

3. Click **Update** to save the changes.

Click here to return to the Installing and Configuring Allworx Premise Servers or Configuring Connect Vx Instances .

Chapter 7 Call Queues/ACD

Call queues distribute calls to a specific set of users (agents). There are two types of call queues.

- **Ring All** queues that do just that – simultaneously ring the phones of all users signed in to the queue.
- **Automatic Call Distribution (ACD)** queues distribute calls to agents with an assigned ACD Appearance PFK. There are three methods for distributing those calls that are selected when defining the queue settings.

Prerequisites	
Access Permissions	Allworx Server Administrator Allworx System Administrator Phone Administrator role
Feature Key Required	• Call Queuing • ACD (Connect premise servers • ACD Users (Connect Vx instances) • Dual Language - if required

Notes:

- *The Call Queue feature works only with Allworx IP phones, no other manufacturer's phones support this feature.*
- *Pressing the phone **MUTE/DND** button on a phone does not stop incoming queue calls from being sent to that phone. If an ACD call is distributed to this phone, the agent is placed in **Busy No Answer**, and Allworx View reports a missed call.*
- *The 92xx IP phone series and the Verge phone series programmable button LEDs behave differently in the following conditions.*
  - *When the agent logs in to the call queue:*
    - ***92xx IP phone series**: The LED flashes fast-green when a new call is inbound, regardless of the wrap-up status.*
    - ***Verge phone series**: The LED flashes fast-green when a new call is inbound and the agent is not in wrap-up, or flashes fast-red when a new call is inbound and the agent is in wrap-up.*
  - *When the agent is not logged in to the call queue (wrap-up status does not apply)*
    - ***92xx IP phone series**: The LED flashes slow-red when a new call is inbound.*
    - ***Verge phone series**: The LED flashes fast-red when a new call is inbound.*

      Wrap-up Time is the period of time between when the agent hangs up a call and when the system makes them available to receive another ACD queue call. This time is defined in the queue settings.

7.1 Available Features

Call queues provide the following features for Allworx System users.

- Feedback for callers in the queues:
  - Greeting plays when calls enter the queue
  - Configurable periodic status messages while waiting in the Call Queue
  - Ringing for waiting customers to hear as an alternative to periodic status messages
- Flexible queue access for agents:
  - Log in and out of queues
  - Receive calls from a queue or answer the calls in a queue
  - monitor the status of the queues
- Configuration of the maximum wait time for a call before hanging up or transferring to an Auto Attendant, an extension, another queue, or a user's Voicemail.
- Exit a queue at any time by pressing zero – different exit routes can be defined for each queue.
- Statistics for all queues are available from My Allworx Manager as an export file. Allworx premise servers have data streamed to a PC on the network using a TCP streaming port number configured on the Allworx System Administration web page for the premise server.

  Note: *Call queue streaming is not enabled with the Connect Vx service to remove the security risk of transmitting this information over the Internet. The Allworx View application provides an alternative.*

Allworx Call Queues/ACD support

	Allworx Connect Premise Servers and Connect Vx Instance			
	320/324	**530/536**	**731**	**Vx**
Maximum calls in one queue	12	30	60	60
Total calls in all queues	12	30	60	60
Call queues	X	X	X	X
ACD queues		X	X	X

7.2 Call Queue Operation

Note: *For information about the settings available when creating call queues, see "To manage the Call Queue settings:" on page 55.*

Calls entering a Ring All call queue will simultaneously ring all phones that have been assigned a Queue Appearance PFK and are logged in to the queue. Caller ID information for the incoming call cannot be seen until the call is answered. Agent statistics are not recorded for this type of call queue.

Automated Call Distribution Queues direct each call to a specific agent with an assigned ACD Appearance PFK. This type of queue offers additional alarm and routing options. ACD queues also provide a means for setting the time an agent remains in the *Busy/No Answer* state before automatically being made available to receive subsequent ACD calls. An agent in *Busy/No Answer* state has the ability to make themselves available by pressing the ACD PFK on the phone.

Note: *Connect 300 series premise servers do not support ACD queuing.*

Calls in an ACD Queue are allocated to agents based on the *Distribution Mode* selected. Those settings are defined in the following table:

Distribution Mode	Description
Linear Priority	Distributes calls based on a prioritized list of agents. The queue supervisor sets the priority by assigning a unique ranking to each agent. As each call comes in, it goes to the available agent with the highest priority ranking.
Sequential Round-Robin	Distributes calls in a circular manner to the logged-in agents, and evenly distributes those calls so the agents have an opportunity to answer approximately the same number of calls. • Maintains a list of available agents. When a call gets to the front of the queue, the next agent on the list receives it. When agents log in, they are put at the bottom of the list. • After the last agent on the list receives a call, the distribution mode returns to the top of the list. If the agent in line to receive the next call is currently busy with another call, the call goes to the next agent on the list. The busy agent that missed the call moves down the list of agents to receive the next call when they are available.
Fairness-Longest Idle	Distributes calls to logged-in agents that are idle for the longest time to evenly distribute the calls so that all agents spend approximately the same amount of time on calls. • Maintains a list of all available agents. When a call gets to the front of the queue, the next agent on the list receives it. • Places agents at the top of the list after logging in. After completing a call, the agent moves to the bottom of the list.

7.3 Setup Checklist

Complete the following steps in this order for a successful Call Queue setup. Click on the links in the column on the right for more information about each step.

Step	Description	More Information
Ring All Queues		
1	Set the *Distribution Mode* to Ring All.	"To manage the Call Queue settings:" on page 55.
2	Assign a Queue Appearance PFK to phones assigned to agents. Assign Queue Appearance PFK(s) to phones assigned to agents – one PFK for each queue to be serviced on the phone.	"Managing the Programmable Function Keys (PFKs)" on page 138
3	Agents log in to queue with Queue Appearance PFK (by default, Queue Appearance PFKs are set to automatically log in when the phones start up).	*Appropriate Allworx Phone User Guide*
4	(Optional) Assign the Queue Alarm PFK to any Allworx phones.	"Managing the Programmable Function Keys (PFKs)" on page 138
Automated Call Distribution Queues • Linear Priority • Sequential Round-Robin • Fairness - Longest Idle		
1	Set the distribution mode to one of the ACD features.	"To manage the Call Queue settings:" on page 55
2	Assign a user as queue supervisor (the admin user is a queue supervisor).	"Managing User Templates" on page 232
3	Queue supervisor assigns agents to single or multiple queues using the *Call Queue Statistics* settings in My Allworx Manager or the *Agents* area of the *Call Queue/ACD screen.*	*Allworx My Allworx Manager User Guide* "The Call Queue Settings listed in the following table apply to both Ring All and ACD call queues unless noted." on page 57
4	Assign an ACD appearance PFK to the Allworx IP phone (ACD queuing requires Allworx IP phones).	"Managing the Programmable Function Keys (PFKs)" on page 138
5	(optional) Assign the Queue Alarm PFK to any Allworx phones.	
6	Agents log in to queue with ACD Appearance PFK.	"Managing the Programmable Function Keys (PFKs)" on page 138

Continued

Step	Description	More Information
Ring All Queues and ACD Queues		
1	Configure calls to route to a call queue.	“Routing Calls to a Call Queue” on page 60
2	Route calls to the call queue using an Auto Attendant.	“Routing Calls to a Call Queue” on page 60
3	View the call queue statistics.	“Displaying Queue Statistics” on page 61
3	Record the custom greetings and messages for each call queue.	“Recording Queue Greetings and Messages” on page 61
4	Import the custom greetings/messages for each call queue.	“Importing Greetings and Messages” on page 63

7.4 Managing Call Queues

Managing both Ring All and ACD Queues involves defining the following information:

- Custom recordings to play to callers in the queues
- Language settings
- Settings that determine how calls in the queues are distributed and routed

Note: *A total of 10 queues can be defined.*

To manage the Call Queue settings:

1. Log in to the Allworx System Administration web page and navigate to the Phone System > Call Queues/ACD page.

2. Complete the following actions as required:

   a. Click one of the *Call Queues / ACD* options.

Option	Description
Manage the Custom Recordings played by the Call Queues	Provides a short cut to the settings page for the custom recordings played by both Ring All and ACD Queues. See “Custom Recordings” on page 339 for more information.
View and manage the Language setting for the Call Queues	Provides a short cut to the *Languages* settings page. See “Languages” on page 159 for more information. ***Note:*** *This feature is only available to Allworx Server Administrators or Allworx System Administrators.*

b. Click the more information button (▸) to expand a selected queue, and then click one of these options.

Option	Description
modify	1. Change the settings as needed. See the table on page 57 for definitions of the settings available. 2. Click **Update** to save the updated queue settings, or **Cancel** to ignore the request.
reset	1. Select one of these options to manage the queue greetings and settings: • Reset to default settings, but keep all custom recordings. • Delete all custom recordings. • Reset to default settings AND delete all custom recordings. 2. Click **Reset** to save the change, or **Cancel** to ignore the request.

3. Locate the *Queue Streaming Settings* and *ACD Queue Busy Reasons* panes that display at the bottom of the screen.
4. Click **modify** and update the settings listed in the following table as necessary.

Setting	Description
Queue Streaming Settings ***Note:*** *Call queue streaming is not available with the Connect Vx service.*	Monitor the Call Queue statistics in real-time by streaming the data to a client application connected to a specified TCP port on the Allworx service LAN interface. **To set up the streaming queue data:** 1. Select one for the following options from the *Queue Streaming* drop-down list: • **Do not stream Call Queue data -** This is the permanent setting for Connect Vx call queues. • **Stream Call Queue data** 2. Set the *Queue Streaming Port* to the appropriate TCP port setting (**1** through **65535** with the default being **16367**). 3. Click **Update** to save the changes or click **Cancel** to ignore the request. 4. Restart the premise server to have the change take effect. When there is queue activity (e.g. callers enter, are serviced, exit queues, agent logs in or out, etc.) in the data streams. Each record is a complete XML file. See the *Allworx ACD Statistics Collection Internet Interface* document for a complete definition of the record layout. To receive and view this data, use a Telnet application (e.g., HyperTerminal) configured to log data from the TCP port configured on the server for ACD data streaming – client connections limit is 16. *Continued*

Setting	Description
ACD Queue Busy Reasons	Change the reasons why the ACD Queue is busy. 1. Enter the reason description in the available fields as needed. 2. Click **Update** to save the changes or click **Cancel** to ignore the request. 3. Reboot the Allworx handset(s) to have the changes take effect.

The Call Queue Settings listed in the following table apply to both Ring All and ACD call queues unless noted.

Setting	Description
Description[1]	Enter a textual description of the queue (e.g., Sales, Tech Support). The system displays this description in other areas (e.g., statistics, handset display screen, etc).
Distribution Mode	Select one of the following options: • **Call Queue: Ring All** • **ACD: Fairness - Longest Idle** • **ACD: Linear Priority** • **ACD: Sequential Round Robin**
Replay Status Message	Enter a value (seconds) that defines the time between successive status update messages. Entering zero (**0**) disables the status message.
Maximum Wait	Enter a value (seconds) that defines the time callers can wait in a queue. When this time expires, the route for this call is specified in the *When caller leaves queue due to* setting defined later in this table. ***Note:*** *Entering zero (**0**) enables the caller to wait without a limit.*
When queue answers call	Select the option for the caller to hear while waiting in the queue: • **Play queue prompts** • **Do not play prompts (caller hears a ring back)**
Maximum Queue Depth	Enter a value to define the maximum number of calls that can be assigned to the queue simultaneously. ***Note:*** *This value varies based on the server model. See “Allworx Call Queues/ ACD support” on page 52 for more information.*
Queue Depth Yellow Alarm Threshold	Enter a value (number of calls in the queue) to trigger the Queue Alarm PFK for yellow alarm levels. Entering zero (**0**) does not trigger an alarm.
Queue Depth red Alarm Threshold	Enter a value (number of calls in the queue) to trigger the Queue Alarm PFK for red alarm levels. Entering zero (**0**) does not trigger an alarm.

Continued

Setting	Description
Wait Time Yellow Alarm Threshold	Enter a value (seconds) to trigger the Queue Alarm PFK for yellow alarm levels.
Wait Time Red Alarm Threshold	Enter a value (seconds) to trigger the Queue Alarm PFK for red alarm levels.
No Agents Logged In Alarm *(ACD only)*	Turns the alarm on or off. • **Enabled** (default) • **Disabled**
Hold Music Selection	Select the hold music source that callers hear while waiting in the queue from the drop-down list.
Maximum Rings before agent is set to unavailable *(ACD only)*	Enter a value (number of rings) agents have to answer a call. If the agent does not answer the call before the maximum number of rings, the system sets the agent to unavailable (No Answer), and the call returns to the front of the queue. The call rings the next available agent. ***Note:*** *The system does not log out agents for not answering calls from an ACD queue even while on another call.*
Wrap Up Time[1] *(ACD only)*	Enter a value (seconds) the agent has available after ending a call before the system makes the agent available to receive subsequent ACD queue calls. Agents can dismiss or end the wrap up time from the handset.
Time agent allowed in Busy/ No Answer state[1] *(ACD only)*	Enter a value (in seconds) the agent remains in the *Busy/No Answer* state before automatically being made available to receive subsequent ACD calls. An agent in *Busy/No Answer* state always has the ability to make themselves available by pressing the ACD PFK on the phone. ***Note:*** *A value of* ***0*** *for this setting means the agent must manually make themselves available by pressing the ACD PFK. This note describes the system behavior prior to adding the timer in Allworx System Software release 8.6.*
When no agents are logged in *(ACD only)*	Select the option for call when all agents are unavailable: • **Force callers to leave queue immediately** • **Allow callers to wait in queue**
When calls are received with all agents busy *(ACD only)*	Select the option for callers when agents are unavailable: • **Allow callers to enter queue** • **Don't answer, treat as if caller left queue** ***Note***: *When the second option is selected, the call is treated just the same as the setting for "When no agents are logged in."*
When all agents are in No Answer state *(ACD only)*	Select the option for a call when all agents are unavailable: • **Force callers to leave queue immediately** • **Allow callers to wait in queue**

Continued

Setting	Description
Last Agent in queue *(ACD only)*	Select the option for the last agent: • **Is allowed to logout of queue** • **Is NOT allowed to logout of queue** ***Note:*** *If the last agent servicing a queue does not pick up a call within the maximum number of rings, the system sets the agent to unavailable (No Answer). Queue Supervisors can log any agent out, regardless of this setting.*
Distribute calls to busy handsets *(ACD only)*	Select from the drop-down list to enable or disable distributing calls to agent handsets that are currently busy with non-ACD calls. A busy handset is an agent handset with any active call.
Play greeting before call distribution *(ACD only)*	Select from the drop-down list to enable calls to wait for the greeting message to complete if an agent is available, or disable to distribute calls immediately upon entering the queue. In either case, the messages play until the agent picks up the call.
Queue Priority *(ACD only)*	Options are from 0-9. Select a lower number to indicate a higher priority. When an agent is logged into more than one queue, the next call comes from the highest priority queue where calls are waiting. For example, if the VIP Queue has priority 0 and the Support Queue has priority 3, the agent always gets calls from the VIP Queue first. The only time a call from the Support Queue goes to the agent is if the VIP Queue has no calls. Queues that have the same priority function the same way as previous releases.
When caller leaves queue due to	Calls can exit the queue under any of the following conditions: • Maximum wait time expired • No agents logged in/available (ACD only) • Queue is full • Caller presses 0 For each condition, click the more information arrow ▶ and click to select the radio button for one of the following routes for each exit condition. • *Hang up* • *Transfer to extension* <specify extension> • *Transfer to Voicemail for user* <specify user> • *Transfer to Call Queue* <specify call queue>

Continued

Setting	Description
Agents *(ACD only)*	Click **show** to view and assign agents as users in the ACD Queue. To assign an agent as a user in the queue, click to select the check box next to their name. Similarly, deselect the check box to remove the agent from the queue. ***Note:*** *For ACD queues with Linear Priority, enter a number in the text box to specify the agent's order as a user in the queue. Leave the text box blank to remove the agent as a user in the queue.* Click **hide** for no display.

[1] Agent must log out and back into the Queue to use the new value.

5. Configure the Allworx IP phone for handling calls in a queue.

   Configure an Allworx IP phone Programmable Function Key (PFK) as a Queue Appearance or ACD Appearance. See "Managing the Programmable Function Keys (PFKs)" on page 138 for more information. The PFK monitors the status of a queue and answers calls in the queue.

7.5 Routing Calls to a Call Queue

Calls enter a queue when routed there by an extension.

Example 1

Select a queue for the final call route of an extension (refer to this as the "queue extension"), and route the outside line directly to the queue extension. For more information see "Outside Lines" on page 175 for setting up outside lines, and "Managing Call Routes" on page 97 for extensions.

Example 2

Inbound calls can also enter a call queue when coming in through an Auto Attendant. If configured, the Auto Attendant plays a custom greeting. For example, "For Customer Support, press 2." After pressing 2, the caller hears the queue greeting, and the system places the call into the queue.

- Define the call route of the outside line to direct calls to the Auto Attendant ("Outside Lines" on page 175).
- Create a queue extension, and define the call route to immediately transfer calls to that queue extension ("Adding a New Extension" on page 91).
- Configure the Auto Attendant menu shortcut to transfer calls to the queue extension ("Auto Attendant Configuration Settings" on page 38).
- Record an Auto Attendant custom greeting with instructions for the caller to press the digit for the shortcut configured with the queue extension ("Recording Auto Attendant Greetings and Messages" on page 41).

7.6 Supervising Calls

The supervisor presses the Call Supervision PFK, enters an agent's extension, and begins supervising the call. If the supervisor has a BLF PFK for the agent, press the Call Supervision PFK followed by the BLF PFK to initiate the session. There is no indication to the agent that supervision is in progress.

Call supervision is available via a PFK configured on the supervisor's Allworx phone. See "Managing the Programmable Function Keys (PFKs)" on page 138 to configure the handset. Enable the agent's phone for supervision by modifying the Call Supervision setting of the Handset Preference Group. See "Creating and Using Handset Preference Groups" on page 120 for more information.

7.7 Displaying Queue Statistics

Allworx ACD Queuing offers a rich variety of statistics to monitor, track, and analyze queue activity. The statistics can be accessed using three methods:

- View via My Allworx Manager
- Export to an XLS file from My Allworx Manager
- Stream to an external device connected to the server

See the *Allworx View User Guide* (allworxportal.com) for more information.

7.7.1 Queue Statistics Report

All users can see the agents of the logged in queues. The statistics are available for queues determined by if the queue is a Ring All queue or an ACD queue. See the *Allworx My Allworx Manager User Guide* for report information. This document includes the steps for viewing and exporting Ring All and ACD queue information, as well as definitions of the statistic fields.

7.7.2 Live Calls

To display the live calls from the queue, see "Live Calls" on page 325 for more information.

7.8 Recording Queue Greetings and Messages

Call queues play built-in or site-specific greetings and status messages. Users with Recording Manager permissions can record offline and then import the greetings into the system (see "Importing Greetings and Messages" on page 63 for more information), or record up to 9 greetings and 1 status message for each Call Queue using the Audio Message Center.

To enable Recording Manager permissions, see "To modify or delete existing users:" on page 228 and update the Recording Manager setting. Select the specific Call Queue for the user.

To record a new queue greeting and status message:

Notes:

- *Allworx does not recommend using a Reach handset to record new greetings or status messages because the ability of the server to record greetings is intolerant of network packet loss. As a result, recordings made via lossy networks can have impaired quality. Local or wired networks are best for making recordings.*
- *For systems with Dual Language Support: Users cannot change languages within the Message Center. To record new messages in a second language, select an option.*
    - *Set up an account configured for the secondary language and then record the greetings using that account.*
    - *Temporarily modify the user's default language to match the secondary language of the system.*

1. Access the Audio Message Center using one of the following methods:
    - Press the phone Messages (✉) function button twice.
    - Dial **6+**[1] the primary extension from any phone or the company Auto Attendant.
    - Dial **404**[1]. When calling from an outside line or phone not assigned to a user, the system prompts users for a primary extension.
    - (from an outside line dialing directly to your office) While the greeting is playing, dial ***6** + <extension> before the greeting finishes playing.

2. Log in using the assigned Allworx PIN followed by the # sign.

   If configuring the system for Dual Language Support, the system associates the new greetings and messages with the current language. To record greetings for an alternate language, switch languages before proceeding to the next step.

3. Dial **9** to manage recordings, and then dial **2** to manage Call Queue.

4. Enter the number of the Call Queue to manage (**0** through **9**), and then dial **1** for the greeting or **2** for the status message.

Dial	Greeting	Dial	Greeting
1	Manage Call Queue greeting	#	Return to the Auto Attendant
2	Manage Call Queue status message	*	Replay the options

5. Dial **2** to start recording. Begin speaking after the beep.

[1] 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 to use for the corresponding feature.

6. Dial # to stop recording and select from the following options:

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

7. Hang up to end the session.

7.9 Importing Greetings and Messages

Greetings and messages recorded offline can be imported onto the Allworx system. These files use a specific internal format and have a specific file name format.

See "Custom Recordings" on page 339 for more information. File name formats are defined on the Allworx System Administration web page in the *File Naming Conventions* pane at **Maintenance** > **Custom Recordings**.

Click here to return to the Installing and Configuring Allworx Premise Servers or Configuring Connect Vx Instances .

Chapter 8 Conference Center

***Note:** Conference Center is not available with the Connect Vx service. The appropriate changes/ omissions have been made to the Allworx System Administration web page. In this instance, the entire Conference page has been removed for Connect Vx.*

Prerequisites	
Access Permissions	Allworx Server Administrator Allworx System Administrator Phone Administrator role
Feature Key Required	Conference Center

Conference Center enables users to reserve conference bridges using My Allworx Manager while enforcing password restricted access to the conference for attendees.

The Conference Center terminates the call if the conference call extends beyond the scheduled end time if there are other scheduled conference calls.

Server Type	Termination
Allworx Connect 300 and 500 series premise servers	A scheduled or unscheduled conference currently in use automatically terminates when another scheduled conference begins. • An unscheduled conference does not terminate conferences in session. • Supports one active conference at a time.
Allworx Connect 731 premise servers	When using all conference bridges and a new conference is scheduled to begin, the premise server terminates the unscheduled conference with the oldest start time first. • If none of the unscheduled conferences are in use (i.e., all in-use conferences are scheduled conferences), the server terminates the conference farthest past the scheduled duration. • Initiation of an unscheduled conference does not terminate conferences in session.

To manage the conference calls:

1. Log in to the Allworx System Administration web page and navigate to **Phone System** > **Conference Center**. The premise server displays a list of scheduled conferences.
2. Locate the conference and click one of the following actions:

Action	Description
end conference	Terminates the in-process conference call.
modify	Change the description, password, moderator, and enable or disable the conference. Click **Update** to save the changes.
Delete	Remove the conference call from the schedule. Click **Delete** to save changes.

Click here to return to the Installing and Configuring Allworx Premise Servers or Configuring Connect Vx Instances .

Chapter 9 Dial Plan

Prerequisites	
Access Permissions	Allworx Server Administrator Allworx System Administrator Phone Administrator role
Feature Key Required	No

The *Dial Plan* page manages how dialed phone numbers are interpreted and how calls are routed – including calls to outside lines. Allworx Administrators can customize internal user, system, and feature extensions.

***Note:** Allworx user guides can refer to dialing patterns based on the factory default internal dial plan. After making changes to the dial plan, the **My Allworx Manager** > **Phone Functions** tab automatically updates to the new digits. Distribute this sheet to all end users. See "Managing the Internal Dial Plan" on page 70 for more information.*

9.1 Setup Checklist

Follow the order of these steps to successfully set up the Dial Plan. Click the links in the column on the right for more information about each step.

Step	Description	More Information
1	Set up the Internal Extension Length before defining users, handsets, or extensions.	"Managing the Internal Extension Length" on page 68
2	Set up the Internal Dial Plan.	"To manage the Internal Dial Plan:" on page 70
3	Set up the Service Groups.	"Managing Service Groups" on page 73
4	Set up the External Dialing Rules (including Emergency Number Dialing and Email Notification recipients).	"Managing External Dialing Rules" on page 75
5	Set up the Dialing Privileges Groups.	"Managing Dialing Privileges Groups" on page 82

9.2 Managing the Internal Extension Length

Caution:	*Internal extension lengths cannot be decreased AFTER increasing extension length. It is highly recommended that Allworx administrators perform an OfficeSafe Backup before increasing the extension length. Once the system extension length has increased, Allworx administrators can only decrease the extension length by performing an OfficeSafe Restore to reset the Allworx server to the backed-up configuration. Connect Vx service administrators should contact Allworx Support to restore the back-up configuration.*

Configure the extensions to be from three (default) to six digits. All existing extensions expand to the new length. After increasing the internal extension length to five or six digits, the extensions **show available** link is no longer available on the following Allworx System Administration web pages:

- **Phone System** > **Users** > **add new user**
- **Phone System** > **Users** > **Modify**
- **Phone System** > **Extensions** > **add new Extension**

Notes:

- *This feature is compatible with Reach 2.0.7 (minimum) and all modes of the Interact Softphone application.*
- *Set up the Internal Extension Length before defining users, handsets, or extensions.*
- *Unless in Extension Mode, 200 or more users/extensions on a single server or in a multi-site network requires at least four digits. Also, even if in Extension Mode, 900 or more users/extensions in a multi-site network requires at least five digits.*

In addition to the changes in user and system extensions, the following server configurations automatically update when the internal extension length is changed:

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

Extension Length changes do not affect the following server configurations[1]:

- System Speed Dial extensions (350-399, 34000-34999)
- Conference Center (408)

  Note: *Conference Center is not available with the Connect Vx service.*

- System Park extension and Parking Orbits (700-709, 4950-4999)
- Auto-Attendant extensions (400, 4301-43xx*)
- Door Relay (403)

  Note: *Door Relay is not available with the Connect Vx service.*
- Message Center (404)
- Paging extensions (460-469)

  Note: *Paging is not available with the Connect Vx service.*
- Queue extensions (4400-4409, 4410-4419)
- Modifying Internal Dial Plan
- Personal Speed Dials (users must modify since the phone stores the numbers)

* Where xx is the maximum number of Auto Attendants supported by the Allworx server.

The server prevents administrators from saving an Internal Dial Plan with overlapping numbers for Speed Dial numbers and Park to Extension with the following warning message:

Once the extension length has been increased, it can only be decreased by restoring the server from a backup.

To change the extension length:

Caution:	*Internal extension lengths cannot be decreased AFTER increasing extension length. It is strongly recommended that Allworx administrators perform a system backup before increasing the extension length. After the system extension length has increased, Allworx administrators can only decrease the extension length by performing a system restore to reset the Allworx server or Connect Vx instance to the backed-up configuration. Connect Vx service users should contact Allworx Support to restore the configuration from backups.*

Notes:

- *Servers that are part of multi-site networks cannot change the Extension Length.*
- *Existing extensions change after modifying the system extension length.*

1. Log in to the Allworx System Administration web page and navigate to **Phone System** > **Dial Plan**.
2. Locate the *Internal Extension Length* pane and click **modify**.
3. Select the number of digits to use for the extensions from the drop-down list.

[1] Extensions may vary per system. When using a non-default Internal Dial Plan, consult the My Allworx Manager Phone Features tab to determine what extensions to use for the corresponding feature.

4. Click **Update** to save the changes or **Cancel** to disregard the changes.

5. Click **Reboot Phones** to update the handsets with the new internal extension length.

   Note: *Verge phones are automatically notified of the change to the internal extension length by the premise server running Allworx System Software 8.5 or higher or the Connect Vx instance, and the configuration is updated at the phone without action from the user or administrator. If Verge phones are the only phones connected to the premise server or Vx instance, it is not necessary to click* ***Reboot Phones****.*

9.3 Managing the Internal Dial Plan

The Internal Dial Plan specifies the first digits for user extensions and other PBX functions such as forwarding calls and accessing outside lines. There are two configuration modes for the Internal Dial Plan:

Mode	Description
Normal	User and system extensions are a continuous range of extensions numbers. The numeric range varies between 1xx and 9xx. Example: three-digit extensions between 100 and 299 or between 700 and 899. System functions (speed dials and retrieving parked calls) are in other ranges not assigned to user extensions.
Extension	User and system extensions can be in any numeric range. The Allworx System Software reserves only the operator digit (e.g., 0) and the PBX external dial digit (e.g., 9). System functions begin with an asterisk (*). For example, extensions can range between 100 and 899 for three-digit dialing and between1000 and 8999 for four-digit dialing.

To manage the Internal Dial Plan:

1. Log in to the Allworx System Administration web page and navigate to **Phone System** > **Dial Plan**.

2. Locate the *Internal Dial Plan* pane, and click one of the following actions:

Action	Description
modify	Opens the Plan settings table so that the Internal Dial Plan settings can be changed. The *Use Extension Mode* check box is selected by default. ***Note:*** *If the system is part of a Multi-site network, the Allworx administrator cannot change the Internal Dial Plan between Extension Mode and Normal Mode.*
view the *Phone Functions Reference Card*	Opens the My Allworx Manager log in page. Enter the user name and password, and then click **Login**. The *Phone Functions Reference Card* page appears in a new browser window. This page can be printed and provided to Allworx phone users.

3. Select the leading digit from the drop-down list in the first column for each of the settings. During the selection, the table displays examples of the dialing plan in the second column.
4. Click **Update** to save the changes or **Cancel** to disregard the changes.
5. Locate the top message about rebooting Allworx phones and click **reboot Allworx handsets** to update the handsets to the new configuration.

Note: *Verge phones are automatically notified of these changes to the internal dial plan by the server running Allworx System Software 8.5 or higher or the Connect Vx instance, and the configuration is updated at the phone without action from the user or administrator. If Verge phones are the only phones connected to the premise server or Vx instance, it is not necessary to click* ***Reboot Phones****.*

9.3.1 Internal Dial Plan Settings

Notes:

- *It is recommended that you choose leading digits for the dial plan from the settings listed below using a “top-to-bottom” approach. Each time you change the digits in a row, the rows below it are automatically adjusted to only allow valid choices. As a result, some leading digits may be changed by the system in rows that are below the row you just modified.*
- *The Allworx System Software prevents administrators from saving an Internal Dial Plan with overlapping numbers for Speed Dial numbers and Park to Extension with the following warning message:*

  These settings create an overlap between Speed Dial numbers” and “Park to Extension” numbers. Choose different settings to prevent the overlap.

Setting	Description
Use Extension Mode	Click to select this check box to enable *Extension Mode* to allow more of the number range to be available for extensions. For example, with three-digit extensions the *Regular Mode* the available extensions are **100** - **299**; in *Extension Mode* the available extensions are **100**-**899**. With *Extension Mode* enabled only the *External Call* access number and *Operator* number can be changed.
User and System Extensions	Identifies the first number used for phone extensions.
Operator	Identifies the number for callers to dial to contact the internal operator. ***Note:*** *Changing the Operator to something other than zero (**0**) does not automatically change the Operator digit shortcut in the Auto Attendants. If the Operator digit is changed, manually update the Auto Attendants shortcuts. See “Auto Attendants” on page 37 for more information.*
External Call access	Identifies the number to dial first to gain access to an outside line. Follows the External Dialing Rules.

Continued

Setting	Description
Enterprise calling	Enables a third party SIP server to be the central hub for calls between multiple sites that have Allworx premise servers or Connect Vx instances. This provides a centralized phone book and administrative service for the entire VoIP network.
Internal station access	Used internally by the system for direct access to devices.
Speed dial numbers	Identifies the number to indicate a speed dial number follows.
Message Center	Short-cut access to the Message Center to: • Manage presence and presence greetings • Name recording • PIN • Access and listen to voice mail messages (even from another Allworx phone)
Call Functions	Identifies the initial number to dial to access various call functions (park/pickup/audit pin code).
Leave a Voicemail for extension	Identifies the initial number (digit) to dial to access a Voicemail box to leave a message for another user.
Park to Extension	Identifies the initial number (digit) of the prefix used when parking a call to an extension using manual dialing. The default value for this initial digit is **3**.
Retrieve Park from Extension	Identifies the initial number (digit) of the prefix used when retrieving a call parked at an extension. The default value for this initial digit is **3**.
PBX Functions	Identifies the initial number to dial to access various PBX functions - door relay, Conference Center, do not disturb, Auto Attendants, Call Queues, call retrieve, call forwarding, or paging. ***Notes:*** • *Calls cannot be forwarded to phones at different sites within a Multi-Site network.* • *Door relay, Conference Center, and paging are not available with the Connect Vx service.*

9.4 Managing DID (Direct Inward Dialing) Routing Configuration

Allworx administrators can disable or enable the DID-to-extension mapping feature. If enabled, internally dialed DID numbers route directly to the extension configured for the specific number. If disabled, the internally dialed DID numbers route via the External Dialing Rules.

To manage the DID Routing Configuration:

1. Log in to the Allworx System Administration web page and navigate to **Phone System** > **Dial Plan**.
2. Locate the *DID Routing Configuration* pane and click **modify**.
3. Select **Enabled** or **Disabled** from the drop-down list.
4. Click **Update** to save the changes or **Cancel** to disregard the changes.

9.5 Managing Service Groups

A Service Group is a collection of services (T1 and CO Lines, SIP Gateways, SIP Proxies) used for placing outside calls. Allworx System Software uses a variety of services to place outside calls; some of these services are optimum for particular types of calls. For example: the SIP Proxy might be the least expensive way to make long distance calls, but the CO lines are best for local calls. Allworx System Software create several Service Groups automatically. Not all service groups are available on every server model or the Connect Vx instance. For example T1 lines are available only on the Allworx Connect 731 server.

- All T1 Lines
- All SIP Proxies
- All Trunk Devices
- All SIP Gateways
- All T1 Lines, CO Lines and SIP Gateways
- No Devices (use to prevent placing external calls)
- All T1 Lines & CO Lines
- All CO Lines

***Note:** CO and T1 lines are not available with the Connect Vx service. These options have been removed from the Allworx System Administration web page for Connect Vx.*

The Allworx administrator can define additional Service Groups to control the use of services or a set of services for certain dialed calls.

When initiating an outbound call using the Service Group, the services in the group are tried in a top-down order until an idle service is found. The outbound call then uses the first idle service in the list. Therefore, the last step in setting up a Service Group ensures that the order of the services reflects the preferred use priority. When one of the services in the group is a SIP proxy, the system software considers the SIP proxy idle until reaching the *Maximum Active Calls* setting.

To manage the service group:

1. Log in to the Allworx System Administration web page, navigate to **Phone System** > **Dial Plan**.
2. Locate the *Service Groups* pane and click one of the following actions:

Action	Description
add new Service Group	Create an additional Service Group. 1. Enter a *Description* for the new group. 2. Move the preferred services into the *Service Group* box. 3. (optional) User the Move Up or *Move Down* buttons to change the *Services* order. 4. Click **Add** to save the changes or **Cancel** to disregard the changes. 5. Reboot the phones to update the handsets to the new configuration. No further action required.
Copy	Create a new Service Group with the same settings as the copied group.
Modify	Change the settings configuration. 1. Enter a *Description* for the new group. 2. Move the preferred services into the *Service Group* box: • Click to highlight the desired item in the *Services* selection box on the left. • Click **move ->** to add that service to the *Service Group*. ***Note:*** *To take a service out of a Service Group highlight the service in the Service Group selection box on the right and click* ***<- move***. 3. (optional) Use the *Move Up* or *Move Down* buttons to change the *Services* order. 4. Click **Update** to save the changes or **Cancel** to disregard the changes. 5. Reboot the phones to update the handsets to the new configuration. No further action required.
Delete	Remove the current Service Group (the Allworx administrator cannot delete the default groups). Confirm the decision and click **Delete** to remove the Service Group. No further action required.

9.5.1 Configuring Remote Sites as Services

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

Select remote sites as services for handling outbound calls. If the line selection process results in a routing call to a remote site, the call connects using one of the remote sites' outside lines. The dialing rules configured on the remote site determines which lines to use and how to dial the number (with or without area code).

The Allworx System Software automatically prevents configuring the dial plans on multiple sites accidentally to avoid routing a call back and forth among the sites. If a call comes in from a remote site, the receiving premise server or Vx instance does 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 system skips the remote sites and uses another outside line service.

9.5.2 Configuring Service Groups / Handset Outside Line Restrictions

Service Groups direct outbound calls to specific services. The system software selects the first idle service in the group. The handset configuration supports restricting the use of lines further when placing an outside call. The number dialed is used to locate the configured Service Group for the outbound call.

After finding the first idle service in the group, the Outside Line Selection Method in the handset Call Appearance Dialing Privileges Group is checked. If the idle service is restricted for the handset, it finds the next idle service and requires the handset to check again. This continues until the system finds a non-restricted idle service to place the call. If a non-restricted idle service can not be found, the caller hears a fast busy signal to indicate there are no available outside lines.

9.6 Managing External Dialing Rules

The external dialing rules indicate to the Allworx premise server and Connect Vx instance what digit sequences are valid for dialing out on the public phone network. As a user dials digits on an Allworx phone, the system software collects the digits, one at a time to place the call. Use the Dialing Rules and Service Groups for Call Appearances, but not for Line Appearances calls because these latter types of calls directly access outside lines.

Enhanced external dialing rules supports matching specific dialing sequences and then deleting, inserting, and/or appending digit strings to those numbers before sending the dial string to any SIP Gateway, SIP proxy, T1/PRI Line, or CO line. This flexible dialing supports programming the dialing behavior of the Allworx System Software to match specific business needs.

Note: *T1 and CO lines are not available with the Connect Vx service.*

Premise servers running Allworx System Software 8.5 and higher and Connect Vx instances, automatically notify Verge phones of changes to the external dialing rules, and then update that configuration on the Verge phones without action from the user or administrator. If Verge phones are the only phones in use, it is not necessary to reboot the phones after making the changes to NANPA, Home Area Code, and Automatic Route Selection discussed in this section.

The following tables provide some examples.

Number	Description
Local number	Users dial a 7-digit number (normally not 1 + <area code>). The system software collects the 7-digits dialed, and then attempts to make the call. The premise server or Vx instance is not waiting for more digits.

Continued

Number	Description
Long distance	Users normally dial 1 + <area code> + 7-digit local number. The system software recognizes this case distinctly from the local number case, and collects all 11 digits before attempting to make the call.
Some local calling areas	Require dialing a <area code> + 7-digit number (without the 1 prefix) to properly dial some numbers. This implies that these rules may vary depending on the local calling area with an installed Allworx premise server.

The dialing rules automatically detect when an outbound dialed number is associated with an internal extension (local or multi-site). When detecting this case, the system places the call to the internal extension. The system considers 10-digit DIDs for matching and attempts to match all 10-digit dialed calls as well as all 7-digit dialed calls, if the home area code is set. If there are overlapping DID blocks on a local premise server or Vx instance, the system software uses the first matching DID. In a multi-site network, the local premise server or Vx instance uses the DIDs for the local site first followed by the DIDs at the remote sites.

Example:
DID 789-456-0123 maps to extension 101 (external call access number is 9 in this example).

User Dials	Home Area Code set to 789	Call Placed to
9-1-789-456-0123	N/A	Extension 101
9-456-0123	Yes	Extension 101
9-456-0123	No	Phone number: 456-0123

9.6.1 Managing the North American Numbering Plan Administration (NANPA)

The Allworx system software routes calls using the Service Group assigned to the type of number dialed. When enabling or disabling NANPA, it changes the types of numbers dialed that the system supports.

The International Public Telecommunications Numbering Plan defines a numbering plan for the worldwide Public Switched Telephone Network (PSTN) and other data networks. The North American Numbering Plan Administration (NANPA) enables calling a phone number with a leading “+” and when NANPA is enabled (default):

- **North American calling numbers** (+1 xxx xxx xxxx): the Allworx System Software removes the leading “+” for the output calling number (1 xxx xxx xxxx).
- **All other regions** (+N, where N is not “1”, **example**: UK calling number +44 xx xxx xxxx): the Allworx System Software removes the leading “+” and prepends the International Prefix Code “011” to the output calling number (**example**: output UK number 011 44 xx xxx xxxxx).

To manage the NANPA settings:

1. Log in to the Allworx System Administration web page. Navigate to **Phone System** > **Dial Plan** > **External Dialing Rules.**
2. Locate the *North American Number Plan* pane, and click **modify.**
3. Check the box to enable NANPA for installations in North America and disable NANPA for all other locations. When NANPA is disabled, set up external dialing rules to determine which outside lines to use.

   When NANPA is enabled, the Allworx administrator cannot add, modify, or delete the default rules. The rules affected by enabling NANPA are service rules, operator rules, emergency rules, and 11-digit dialing rules.

   Note: *There is one exception: when NANPA is enabled, the Allworx administrator can add to the 11-digit dialing rules if the total number of digits is equal to 11. For all other additions, modifications, or deletions the Allworx administrator must disable NANPA.*

NANPA Enabled Requirements

Rule	Leading Digits	Total Digits	Auto Delete Existing
Service Rule	211	3	Yes
Service Rule	311	3	Yes
Service Rule	411	3	Yes
Service Rule	511	3	Yes
Service Rule	611	3	Yes
Service Rule	711	3	Yes
Service Rule	811	3	Yes
Operator Rule	Operator	1	Yes
Emergency Rule	Emergency	Any	Yes
Rules beginning with 1	1 [any other digits]	Not equal to 11	Yes

4. Click **Update** to save the changes.
5. Locate the message about rebooting Allworx phones and click **Reboot Phones** to update the handsets with the new configuration.

Note: *Verge phone configurations with the changes are automatically updated. No reboot is necessary.*

9.6.2 Managing the Home Area Code Requirements

Some features of the Allworx premise server or Vx instance and phones (example: redialing from call history and when mapping numbers to 11-digit forms to SIP proxies) require knowledge of the home area code. This required information is part of the dialing rules that support those features.

To manage the home area code:

1. Log in to the Allworx System Administration web page.
2. Navigate to **Phone System** > **Dial Plan** > **External Dialing Rules** > **Home Area Code** > **Modify**.
3. Enter the area code in the field provided.
4. Click **Update** to save the change.
5. Locate the message about rebooting Allworx phones and click **Reboot Phones** to update the handsets with the new configuration.

Note: *Verge phone configurations with the changes are automatically updated. No reboot is necessary.*

9.6.3 Selecting the Automatic Route

The dial method controls whether or not to include the area code when the placing a call. If the area code is not properly configured for the local rules, the system may not correctly place local calls. Configure the area codes to use the correct service for the local and other area codes to use the correct number of digits when placing the call.

Note: *When NANPA is enabled (default), any conflicting ARS (Automatic Route Selection) rule overrides the NANPA dialing rule.*

The Automatic Route Selection (ARS) rules allow

- Greater flexibility to support international dialing with the following enhancements:
  - Match calling numbers with leading “+”
  - Pre-pend a leading “+” to an outbound calling number
- Creating custom international dialing plans

To select the automatic route:

1. Log in to the Allworx System Administration web page and navigate to **Phone System** > **Dial Plan**.
2. Locate the *External Dialing Rules* pane and go to the *Automatic Route Selection* information.
3. Click one of the following actions:

Action	Description
▶ **Bulk Edit**	Delete the checked route definitions.

Continued

Action	Description
add new rule	Activate another rule. See “Automatic Route Selection Rule Settings” on page 79 for more settings information. Click **Add** to save the new rule.
Modify	Change the selected rule. See “Automatic Route Selection Rule Settings” on page 79 for more settings information. Click **Update** to save the changes.

4. Locate the message about rebooting Allworx phones and click **Reboot Phones** to update the handsets to the new configuration.

   Note: *Verge phone configurations with changes are automatically updated. No reboot is necessary.*

9.6.3.1 Automatic Route Selection Rule Settings

Setting	Description
Leading Digits	User dialed digits. For areas that require dialing the area code or other type exchange, this is the aaa (area code). For areas that require dialing 1 + area code (or other exchange), this is 1aaa (aaa is the area code/exchange).
Total Digits	Number of digits (1 to 24) including digits 0-9 dialed by the user for the pattern.
Delete Leading Digits	Number of the first 0 to 24 caller-dialed digits deleted from beginning of the dial string before sending the request to a service group.
Insert Leading Digits	Digits not dialed by the user. Inserted at the beginning of the dial string after deleting leading digits before the string passes to the remote device. It is possible to insert 0 to 24 digits (0-9), #, *, or pauses (P).
Append Trailing Digits	Digits added to the end of the dial string - 0 to 24 digits (0-9), #, *, or pauses (P).
Service Group	Select an option from the drop-down list: • **All CO Lines** (Allworx premise servers only) • **All CO Lines & SIP Gateways** (Allworx premise servers only) • **All SIP Gateways** • **All SIP Proxies** • **All Trunk Devices** • **No Devices**

Example 1:

Adding an area code with “Area code NOT dialed”. In this case, the user dials 1234567, the area code is 585, and the output dial string is 15851234567.

Setting	Description	Setting	Description
Leading Digits	0	Insert Leading Digits	1aaa

Continued

Setting	Description	Setting	Description
Total Digits	7	Append Trailing Digits	0
Delete Leading Digits	0		

Example 2:

Adding an area code with “Area code dialed.” In this case, the user dials **5851234567**, and the output dial string is **15851234567**.

Setting	Description	Setting	Description
Leading Digits	aaa	Insert Leading Digits	1
Total Digits	10	Append Trailing Digits	0
Delete Leading Digits	0		

Example 3:

Adding an area code with “1 + area code dialed.” The user dials **15851234567**, and the output dial string is **15851234567**.

Setting	Description	Setting	Description
Leading Digits	1aaa	Insert Leading Digits	0
Total Digits	11	Append Trailing Digits	0
Delete Leading Digits	0		

Example 4:

Adding a specific country while leaving all International calls service group set to **No Devices**. The user dials **44123451234567890** where **44** is the country code (England), **12345** is the area code, and **1234567890** is the 10-digit phone number. The output dial string is **01144123451234567890**. Repeat for each country.

Setting	Description	Setting	Description
Leading Digits	44	Insert Leading Digits	011
Total Digits	17	Append Trailing Digits	0
Delete Leading Digits	0		

9.6.4 Managing the Emergency Number Rules

Prior to configuring the emergency dial plan, the emergency number rule defaults are **911** as the *Emergency Number* and the *Direct Dial* option is enabled (checked).

Notes:

- *Do not enter an Emergency number that conflicts with other dial plan options as this may result in the emergency center not being called.*

  Reboot the Allworx phones when making changes to the Emergency values. Verge phone configurations with the changes are automatically updated. No reboot is necessary.
- *The Allworx System complies with the Kari's Law Act of 2017, by default, which enables users to initiate a call to 9-1-1 from any phone without dialing any additional digit, code, prefix, or post-fix. The law requires installers in the United States to ensure that the final installation of the system complies with these requirements. Users must be able to dial 9-1-1 from any desk phone without any other leading or trailing button presses. It is acceptable for there to be additional methods to dial an emergency number, such as dialing 9-1-1 after the trunk access digit. The law also requires the installer to configure an emergency alert at a central location at the facility or to another person or organization regardless of location. The Allworx System allows emergency alerts to be delivered to multiple destinations by multiple methods. Please refer “Email Notifications” on page 88 for more information.*

To configure emergency number rules:

1. Log in to the Allworx System Administration web page and navigate to **Phone System** > **Dial Plan**.
2. Locate the *External Dialing Rules* pane and find the *Emergency* information
3. Click **Modify**.
4. Update the following fields:

Field	Description
Emergency	Enter the number to dial for emergency situations.
Dial Direct	Click to select the check box to allow users to dial the emergency number without the line access number.

5. Click **Update** to save the changes or **Cancel** to disregard the changes.
6. (optional) Locate the *Emergency Call Email Notification* line and click **Modify**.
   - Click to select the check box to *Enable Email Notifications of Emergency Calls*, if needed.
   - In the *Addresses* text boxes enter the email address or user name of those individuals who are to receive the emergency email notifications.

7. Click **Update** to save the change.

8. Locate the top message about rebooting Allworx phones and click **Reboot Phones** to update the handsets to the new configuration.

   Note: *Verge phone configurations with the changes are automatically updated. No reboot is necessary.*

9.6.5 Managing the Services

To manage the services:

1. Log in to the Allworx System Administration web page and navigate to **Phone System** > **Dial Plan**.
2. Locate the *External Dialing Rules* pane, and then the *Services* table.
3. Click **Modify**.
4. Select the *Service Group* affected in the drop-down list. For the Public SIP Director and PIN Code feature, specify the number of digits.

   Note: *In order to be able to change the PIN code length, the system cannot have any previously configured PIN codes.*

5. Click **Update** to save the changes.
6. Locate the message about rebooting Allworx phones and click **Reboot Phones** to update the handsets to the new configuration.

   Note: *Verge phone configurations with changes are automatically updated. No reboot is necessary.*

9.7 Managing Dialing Privileges Groups

A Dialing Privileges Group is a set of dialing permissions and handset Call Appearances with the same settings. Apply custom configurations to any or all of the site handsets by creating a Dialing Privileges Group, specifying the settings and assigning handset Call Appearances to the group. Changes made to the group settings take effect immediately. Handset Call Appearance dialing permissions determine how to access outside lines, determine which outside lines to use, and enable or block phone numbers.

To manage the dialing privileges groups:

1. Log in to the Allworx System Administration web page and navigate to **Phone System** > **Dial Plan**.
2. Locate the *Dialing Privileges Groups* pane and click one of the following actions:

Action	Description
View	View and modify the current dialing permissions group.
Copy	Create a new dialing privileges group.
Delete	Remove the current dialing privileges group. The Allworx administrator cannot delete the default group or groups with assigned handsets. Therefore, move all handsets into other groups to delete the group.

3. Locate the information to update and click **modify**.

Dialing Privileges Group

When upgrading Allworx system software, create an additional Dialing Privileges Group for each unique combination of Outside Line Connection settings for the existing phones.

Note: *The system does not change settings for existing handsets in this process.*

Dialing Privileges Group settings are described in the following table:

<table>
<tr><th>Setting</th><th>Description</th></tr>
<tr><td><i>Name</i></td><td>Enter a new name in the field</td></tr>
<tr><td><i>Emergency Service Group</i></td><td>Select a group from the drop-down list.</td></tr>
<tr><td><i>Schedule</i></td><td>Associate a schedule with each Dialing Privileges Group to specify different Toll and Internal Call Restrictions for the Dialing Privileges Group based on the schedule. This option supports additional flexibility by limiting which numbers specific handsets can dial at various times of the day. For Example:
• Don’t let the lobby phone dial the door relay or paging zones.
• Don’t let certain employees dial the CEO.
• Don’t let any phone make long distance calls after business hours.
Select a schedule option from the drop-down list, and then use the option drop-down lists to further refine the call restriction type. See the <i>Toll Restriction</i> and <i>Internal Call Restriction</i> panes below for the restriction options.
<table>
<tr><th>Schedule Option</th><th>Restriction Type Available</th></tr>
<tr><td>Not Used</td><td>• Toll Restriction
• Internal Call Restriction</td></tr>
<tr><td>&lt;Available Schedule&gt;</td><td>• Day Mode Toll Restriction
• Night Mode Toll Restriction
• Day Mode Internal Call Restriction
• Night Mode Toll Restriction</td></tr>
</table>
</td></tr>
</table>

Continued

Setting	Description
Toll Restriction	See “Toll Restriction” on page 84.
Internal Call Restriction	See “Internal Call Restrictions” on page 85.
Seize Rule	Select a rule from the drop-down list.
Outside Line Selection Method	Select one of these options: • **Use External Dialing Rules for number dialed** • **User External Dialing Rules, but restrict to these services:** check the appropriate check boxes. **Shortcut**: click **check all** or **uncheck all**. • **Ignore External Dialing Rules and always use this service or Service Group:** select an option from the drop-down list.

Toll Restriction

Block external calls (specific numbers, area codes, etc.). When programming a specific Dialing Privileges Group, the Allworx administrator selects which Toll Restrictions to apply to the Dialing Privileges Group.

The system software enables all numbers defined by the External Dialing Rules unless listed in the Blocked Numbers list.

- Numbers in the Exceptions list override the blocked numbers. If listing a number as both blocked and as an exception, the system software enables calls to that number.
- Entries in the Blocked Numbers list need not be complete phone numbers but can be only the first part of phone numbers. The numbers entered are a pattern, which the Allworx premise server and Connect Vx instance reads left to right. Once the pattern has been matched (see example) the number is blocked. *Example:* Entering 1900 in the Blocked Numbers list prevents all 1-900 number calls.

Entries in the *Exceptions* list should be more specific than those in the *Blocked Numbers* list.

- The *Exceptions to the Blocked Numbers* list does not need to have any entries to specify enabling similar numbers.
- If the *Blocked Numbers* list contains **1** as an entry and the Exceptions to Blocked Numbers list contains **1800**, then users can dial 1-800 numbers but no other long distance number.
- If the *Blocked Number* list contains a complete number (e.g. **19005553850**) then the system software blocks only that number.

Note: *When attempting to block the emergency number, the Allworx System Software requires a confirmation prior to accepting the request.*

Section	Description	
Add	Click to create a new rule.	
	Enter new name	Describe the new rule.
	Blocked Numbers	Enter the blocked numbers in the fields provided.
	Exceptions to Blocked Numbers	Enter the exception numbers in the fields provided.
	Click **Add** to save the change or **Cancel** to disregard the request.	
Modify	Click to update the rule.	
	Update the name	Describe the rule. ***Note****: The Toll Restrictions (Default) name cannot be changed.*
	Blocked Numbers	Enter the blocked numbers in the fields provided.
	Exceptions to Blocked Numbers	Enter the exception numbers in the fields provided.
	Click **Update** to save the change or **Cancel** to disregard the request.	
Delete	Click to remove the rule from the list. Verify this is the rule to delete, and then click **Delete** to remove the rule or **Cancel** to disregard the request. ***Note****: The Toll Restrictions (Default) cannot be deleted.*	

Internal Call Restrictions

Block internal calls (extensions, PBX functions, etc.) When programming a specific Dialing Privileges Group, the Allworx administrator selects which Internal Call Restrictions that apply to the Dialing Privileges Group.

The system software enables all numbers unless listed in the Blocked Numbers list.

- Numbers in the Exceptions list override the blocked numbers.
- If listing a number as both blocked and as an exception, the system software enables calls to that number.
- Entries in the Blocked Numbers list need not be complete phone numbers but can be only the first part of phone numbers. Example: entering 12 in the Blocked Numbers list prevents calling internal extensions 1200 to 1299 or entering *4 in the Blocked Numbers list prevents calling all PBX functions.

Entries in the *Exceptions* list should be more specific than those in the *Blocked Numbers* list.

The *Exceptions to the Blocked Numbers* list does not need to have any entries to specify enabling similar numbers.

<table>
<tr><th>Section</th><th>Description</th></tr>
<tr><td><b>Add</b></td><td>Click to create a new rule.
<table>
<tr><td>Enter new name</td><td>Describe the new rule.</td></tr>
<tr><td>Blocked Numbers</td><td>Enter the blocked numbers in the fields provided.</td></tr>
<tr><td>Exceptions to Blocked Numbers</td><td>Enter the exception numbers in the fields provided.</td></tr>
</table>
Click <b>Add</b> to save the change or <b>Cancel</b> to disregard the request.</td></tr>
<tr><td><b>Modify</b></td><td>Click to make changed to the rule.
<table>
<tr><td>Enter new name</td><td>Describe the new rule.
<i><b>Note</b>: The Internal Call Restrictions (Default) name cannot be changed.</i></td></tr>
<tr><td>Blocked Numbers</td><td>Enter the blocked numbers in the fields provided.</td></tr>
<tr><td>Exceptions to Blocked Numbers</td><td>Enter the exception numbers in the fields provided.</td></tr>
</table>
Click <b>Update</b> to save the change or <b>Cancel</b> to disregard the request.</td></tr>
<tr><td><b>Delete</b></td><td>Click to remove the rule from the list. Verify this is the rule to delete, and then click <b>Delete</b> to remove the rule or <b>Cancel</b> to disregard the request.
<i><b>Note</b>: Internal Call Restrictions (Default) cannot be deleted.</i></td></tr>
</table>

Call Appearances Assigned to Group

Check the box next to a Call Appearance to include it in the group. When removing a Call Appearance from a user-defined group, it moves automatically to the default group.

4. Click **Update** to save the changes or **Cancel** to disregard the request.

Click here to return to the Installing and Configuring Allworx Premise Servers or Configuring Connect Vx Instances .

Chapter 10 Emergency Alerts

Prerequisites	
Access Permissions	*Allworx Server Administrator* *Allworx System Administrator* *Phone Administrator role – (Emergency CID page)*
Feature Key Required	*No*

The Emergency Alert includes the following:

- Sends audible and visual alerts to designated phones immediately after making an emergency call from any local or remote handset.
- Supports email and SMS message notification of emergency calls.
- Allows for sending email notifications to test the settings.

The 911 Alert supersedes any phone functionality except when the Allworx user is in an admin menu.

Caution: *Do not attempt to place emergency (911) calls prior to activating the Connect premise server or Vx instance. If the premise server or Vx instance is not activated the call does not go through.*

The Allworx System complies with the Kari's Law Act of 2017 (by default) which allows users to initiate a call to 911 from any phone without dialing any additional digit, code, prefix, or post-fix. The law requires installers in the United States to ensure that the final installation of the system complies with these requirements. Users must be able to dial 9-1-1 from any desk phone without any other leading or trailing button presses. It is acceptable for there to be additional methods to dial an emergency number, such as dialing 9-1-1 after the trunk access digit. The law also requires the installer to configure an emergency alert at a central location at the facility or to another person or organization regardless of location. The Allworx System allows emergency alerts to be delivered to multiple destinations by multiple methods. Please refer to "Email Notifications" on page 88 for more information.

IMPORTANT: *Prior to configuring the emergency dial plan, the emergency number rule defaults are listed in the following table:*

Default	Description
Not Set	*Emergency Number: 911* *Direct Dial: enabled (checked)*
Set	*Uses Emergency Number and Direct Dial settings as previously set by the administrator.*

- To dial the emergency number without dialing the external line access digit, see "Managing the Emergency Number Rules" on page 81 for more information.
- To configure handsets to receive 911 alerts, assign an Emergency Alert PFK. See "Managing the Programmable Function Keys (PFKs)" on page 138 for more information.

When any handset places an emergency call on the system, handsets with the Emergency Alert PFK produce an audible beeping and also display the following information:

- Handset internal caller ID, if available, or the handset description
- Date and time of the call
- Station number of the handset from which the call originate

10.1 Email Notifications

Email notifications can be sent to the appropriate personnel each time an emergency call is made. These email notifications include information about the handset user, Emergency Caller ID, the location of that handset, and the date and time the call was placed. After designating the recipients of the emergency call email notification, a test email can be sent to verify that the appropriate individuals receive notification.

Status	Description of What Happens When the PFK is Pressed
Active Alert	*Acknowledges the alert, silences the beep, and removes the alert information from the display screen.*
Inactive Alert	*Retrieves information of the last alert stored on the handset. Press the PFK again to close the alert and return to the idle screen.*
Rebooting the handset	*Removes stored alert details from the handset.*

To define recipients of Emergency Call Email Notifications:

1. Log in to the Allworx System Administration web page and navigate to **Phone System** > **Emergency CID**.
2. Locate the *Emergency Call Email Notifications* pane and click **Modify**. The link takes you to the *Dial Plan* page.
3. Click to select the *Enable Email Notifications of Emergency Calls* check box, if needed.
4. Enter the username or email of the individual(s) to receive the email notifications.
5. Click **Update** to save the changes or **Cancel** to ignore the request.
6. Test the email notifications:
   a. Navigate to **Phone System** > **Emergency CID**.
   b. Click **Send Test Email**. A message appears stating the success or failure of the email send.

Notes:

- *For multi-site networks, email notifications provide a line that indicates the site name of where the call originated.*
- *To delete an email or username, simply click in the Addresses text box and press the **Delete** or **Backspace** keys to remove the entry.*

- *For information about defining emergency dialing rules and email notification recipients on the Dial Plan page, see "Managing External Dialing Rules" on page 75.*

To enable alerts on a Reach device, see "Feature Eligibility" on page 236 for more information.

To enable alerts for the Interact Softphone application see "Managing Programmable Functions for Interact Softphone" on page 151.

The Allworx premise server and Connect Vx instance automatically acknowledge active alerts by silencing all handsets beeping after 10 minutes and removing the handset display alert information after 60 minutes.

Additional emergency calls placed from other handsets within 15 seconds result in the system software disregarding the new alerts; the handset stores emergency calls placed after the 15 second time period after the user acknowledges the first alert. Press the PFK or CLEAR soft key to acknowledge an alert.

Emergency alerts supersede any handset functionality (e.g. placing/receiving a call, logging in to 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 blinks. When the user exits the menu screens the handset repeats the audible beeping and alert information.

Note: *Calls do not disconnect when an Emergency alert is propagated to the handset.*

10.2 Managing Emergency Handset Caller ID

The Allworx premise server and Connect Vx instance supports assigning an Emergency Caller ID (CID) number to each Allworx handset. When dialing an emergency number from the handset, the Emergency CID, instead of the normal CID, passes to the emergency call center. For employees not at the main site, the properly configured Emergency CID helps the emergency call center locate the handset placing the call.

Caution:	*Setting Emergency Caller IDs to place emergency calls on a CO line does not work. The Emergency CID does not override the Caller ID of the CO line.*
Caution:	*If using SIP trunks or PRI lines, check with the provider to determine the Caller ID numbers to use, if any, or to configure additional phone numbers as caller IDs for emergency calls. After setting up Emergency Caller ID numbers on the Allworx server, call the emergency phone numbers (e.g., 911) to test each number. Use a phone configured with the caller ID to ensure that the emergency calls connect, route to the correct emergency call center, and if the call center can independently determine the handset location.* *Advise the emergency call center that these test calls are non-emergency calls to test the phone system.*

To configure Emergency Caller IDs for specific handsets:

1. Define an Emergency Caller ID and assign it to the handsets.
2. Give each Emergency CID a *Location* name and associate each with a *Service Group* to use when placing an emergency call.

   Note: *When selecting the **Use External Dialing Rules** service group from the drop-down list, the system software selects the outside line or service group with the area code of the Emergency CID* *number.*

To manage the Emergency Caller ID numbers:

1. Log in to the Allworx System Administration web page and navigate to **Phone System** > **Emergency CID**, and locate the *Emergency Caller ID Numbers* pane.
2. Click one of the following actions:

Action	Description
add new Caller ID Number	*Create another emergency caller ID number.* 1. Enter the *Caller ID number* and *Location*. Use a descriptive handset name for the locations that uses this caller ID. 2. Select a *Service Group* from the drop-down list. 3. Click **Add** to save the changes.
Modify	*Update the Location and Service Group fields.* 1. Enter the new *Location*. 2. Select a *Service Group* from the drop-down list. 3. Click **Update** to save the changes.
Delete	*Click this link to remove the Caller ID number from the list; however, administrators cannot delete Emergency CIDs with assigned handsets. Assign all handsets to another Emergency CID prior to deletion.* *Confirm the Emergency Caller ID Number to be deleted and click* ***Delete*** *in the confirmation window.*

10.3 Assigning the Emergency Caller IDs

To assign using the server administration page:

1. Log in to the Allworx System Administration web page and navigate to **Phone System** > **Emergency CID.** The page displays all handsets on the system in the table in the *Handset Emergency Caller ID Number Assignments* pane. This table includes physical phones, as well as Interact Softphone and Reach handsets.
2. Locate the handset in the *Handset Emergency Caller ID Number Assignments* table.
3. Click **Modify**.
4. Select a *Caller ID Number* from the drop-down list.
5. Click **Update**. If using the handset option, the system requires a phone reboot to display the changes made on the Allworx System Administration web page.

   Note: *Verge phone configurations with the changes are automatically updated. No reboot is necessary.*

Click here to return to the Installing and Configuring Allworx Premise Servers or Configuring Connect Vx Instances .

Chapter 11 Extensions

From the *Extensions* page manage system and user extension call routes and Park to Extension options.

Prerequisites	
Access Permissions	Allworx Server Administrator Allworx System Administrator Phone Administrator role
Feature Key Required	No

11.1 Adding a New Extension

Enables adding an extension to the Allworx system directory.

With Allworx System Software version 9.0, there is a new type of extension available. The new Convenience Extensions do not count against the System Extension limit. There is no limit to the number of Convenience Extensions users can have (within the number space available in the internal dial plan), and they can only be used to route to other extensions or Allworx applications like queues, auto attendants, and Voicemail boxes. These extensions cannot be routed to any devices or external phone numbers.

To add a new System Extension or Convenience Extension to the directory:

Notes:

- *When a new user is added, the extension is created automatically.*
- *After increasing the internal extension length to 5 or 6 digits, the extensions **show available** link is no longer available.*

1. Log in to the Allworx System Administration web page and navigate to **Phone System** > **Extensions**.
2. Click **add System Extension** or **add Convenience Extension**.
3. Update the following fields in the *Extension* area of the screen:

Field	Description
System Extension	Enter a requested extension number or click **show available** and click to select an available extension. Click **hide available** to close the list of available numbers.
Description	Enter a name for the extension, i.e., Conference Room.
Schedule	Select a schedule for the extension to use for business hours from the drop-down list.
Enable parking calls to this extension *(System Extensions Only)*	Check the box to enable the Park to Extension feature for this extension.

4. For Convenience Extensions go to step 6.
5. For System Extensions follow these steps:

   a. Go to the *Primary Call Route* pane and click **add a connection attempt** to add the first connection in the call route when the new extension is dialed.

   From the drop-down menus make the following selections:

   - Select the call destination – in most cases this will be the new extension.
   - Select the number of rings to occur before the call is re-routed.
   - Select the ring type for the call (default is **Single Ring**). See "Ring Families and Ring Types" on page 94 for more information.

   b. Click **add a destination** to include another device that will ring simultaneously when a call is to that extension is received. Provide the same information as in the previous step.

   For example, it may be helpful to include an office extension, a remote location extension, and a mobile phone number in a first connection attempt. This means that each time the extension is dialed, all three phones ring so the user has access to calls no matter their location.

   c. Locate the *Finally* area that appears at the bottom of the *Primary Call Route* pane. This area defines how a call is redirected after the defined connection attempt is unsuccessful (the call is not answered).

   Click to select the radio button for one of the following options.

Option	Description
Hang up (default)	The call ends with a hang up. Requires no further action.
Transfer to Auto Attendant	Select the auto attendant from the drop-down list.
Transfer to Call Queue	Select the call queue from the drop-down list.
Transfer to Voicemail for user	Select the user from the drop-down list.

Continued

Option	Description
Dial number	Enter a new number to which the call is to be forwarded. This includes the following: • Unaudited calls (9 *number*) • Audited calls (78 nnnnn *number*) • Call Park (700) • Park to Extension (300xxxx) • Public SIP Directory calls (8 nnnn) • Door Relay (403) - if connected and configured • Message Center (404) • Message Center for user (6xxxx) • Conference Center (408) • Paging Zones (46n) • Operator (0) • User or System Extension

d. Click **add another connection attempt** if the call is to be forwarded to another destination before final handling.

For example, it may be helpful to forward a call to another person in the same department, or to an extension set up with a system Voicemail.

Select the required information from the drop-down menus as defined in previous steps.

Notes:

- *The Allworx system allows only two attempts to redirect a call (the actions specified in the Finally section). If redirected a third time the call drops. Additional redirects can be a problem when specifying an outside number or an extension in the Dialed number choice as the final redirect. If that last dialed number is not answered, it can send the call in to a loop.*
- *To remove a connection attempt, click* ***delete this attempt***.

e. Go to step 7.

6. For Convenience Extensions locate the *Primary Call Route* pane. This area defines how a call is redirected after the defined connection attempt is unsuccessful (the call is not answered).

Click to select the radio button for one of the following options.:

Option	Description
Hang up (default)	The call ends with a hang up. Requires no further action.
Transfer to Auto Attendant	Select the auto attendant from the drop-down list.

Continued

Option	Description
Transfer to Call Queue	Select the call queue from the drop-down list.
Transfer to Voicemail for user	Select the user from the drop-down list.
Dial number	Enter a new number to which the call is to be forwarded. This includes the following: • Call Park (700) • Door Relay (403) - if connected and configured • Message Center (404) • Message Center for user (6xxxx) • Conference Center (408) • Paging Zones (46n) • Operator (0) • User or System Extension

7. Click **Add** to save the System or Convenience Extension, or **Cancel** to ignore the request.

11.1.1 Ring Families and Ring Types

Phones can be set to ring with different patterns and tones for various reasons, including the following:

- Differentiate between incoming internal calls and incoming external calls
- Identify calls from a specific caller ID
- Differentiate between the lines for the incoming call (including calls on certain Call Appearances, Line Appearances, or ACD queues)
- Help multiple users in a shared space to identify which phone is ringing

The Allworx system provides 8 Ring Type Families and 8 Ring Types within each family. The Allworx Server Administrator chooses the Ring Type in the extension and programmable button definitions. Verge Phone users select the Ring Family to use from the phone.

Note: *The appearance programmable button Ring Type setting overrides any call-route-specific Ring Type choices made when defining the extension, unless the appearance programmable button Ring Type is set to **AUTO** which uses the Ring Type selected for the extension.*

The following table defines the available Ring Types.

	Analog Handset	Allworx Handsets Ring Families 1 - 4	Allworx Handsets Ring Family 5
Single Ring	Single	Single Ring Pitch A	Single Ring Pitch E

Continued

	Analog Handset	Allworx Handsets Ring Families 1 - 4	Allworx Handsets Ring Family 5
Double Ring	Double Ring [short, short]	Double Ring Pitch A	Double Ring Pitch F
Ring Type 1	Double Ring [short, long]	Single Ring Pitch B	Triple Ring [short, long, short] Pitch G
Ring Type 2	Double Ring [long, short]	Double Ring Pitch B	Quad Ring [long, long, short, short] Pitch H
Ring Type 3	Triple Ring [long, long, long]	Single Ring Pitch Tone C	Triple ring [long, long, long] Pitch I
Ring Type 4	Triple Ring [short, short, long]	Double Ring Pitch Tone C	Triple Ring [short, short, long] Pitch J
Ring Type 5	Triple Ring [short, long, short]	Single Ring Pitch Tone D	Triple Ring [long, short, long] Pitch K
Ring Type 6	Triple Ring [long, short, short]	Double Ring Pitch Tone D	Triple Ring [long, short, short] Pitch L

Verge phone users can choose from the 8 phone ring type families using the *Settings* or *Config* menu on the phone. Users of 91xx series and 92xx series phones can choose from 5 ring type families. Ring tone **Family 1** is the default family for 91xx series and 92xx series phones. Ring tone **Family 6** is the default family for the Allworx Verge phone series.

Family	Ring Type Description
Family 1	Default Frequencies (default for 91xx and 92xx series phones)
Family 2	Middle Frequencies
Family 3	High Frequencies
Family 4	Very High Frequencies
Family 5	Varying Frequencies
Family 6	Recorded ring tones with a melodic theme (default for Allworx Verge series phones)
Family 7	Recorded ring tones with a modern theme
Family 8	Recorded ring tones with a traditional theme

11.1.2 Transferring to an Auto Attendant

One of the options in the *Finally* pane when adding a new extension is **Transfer to Auto Attendant**. Outside Lines and internal extensions can be programmed to have an Auto Attendant answer the call, and using Multiple Auto Attendants to give the appearance of different businesses or different departments within a business. If the call route does not define the specific Auto Attendant to use, the answering Auto Attendant is determined by the source of the incoming call.

The following table defines which auto attendant answers the call based on the source of the call:

Source of Call	Answering Auto Attendant
Outside Line - DID Line	Auto Attendant x4301
Outside Line - FXO Line	(Default Attendant defined for the line)
Outside Line - SIP Gateway	(Default Attendant defined for the gateway)
Outside Line - SIP Proxy	(Default Attendant defined for the proxy)
Internal Phone	Auto Attendant at x4301

11.2 Managing Extension Settings

Note: *Extensions with the Park to Extension feature enabled can be easily identified by the automobile icon in the extension description.*

1. Log in to the Allworx System Administration web page and navigate to **Phone System** > **Extensions**.

2. Click the **Bulk Edit** side arrow and check the box next to the extension to select it. Click the box at the top of the column to select or deselect all extensions.

3. Click one of the following actions:

Action	Description
Delete	Removes the selected extensions.
Enable or Disable	Activates or removes the ability for Allworx users to park calls to the selected extensions.
Modify	Opens the Park to Extension settings for the selected **User** extensions. Select **Update** to save the changes.
Modify	Opens the Park to Extension settings for the selected **System** extensions. Select **Update** to save changes.

11.3 Performing a Search

Locate extensions based on extension, description, login name, or site.

To perform a search:

1. Log in to the Allworx System Administration web page and navigate to **Phone System** > **Extensions.**
2. Locate the *Search* line at the top of the page and enter the search criteria.
3. Press **Enter**.

   The table displays the extensions with information that matches the search criteria.

11.4 Managing the Description

Click the description name as a short cut to manage the user. See “To modify or delete existing users:” on page 228 for additional information.

11.5 Managing Call Routes

The building blocks of a call route are the connection attempts and the *Finally* route. In a typical call route, there is one connection attempt and the *Finally* route. The Allworx premise server and Connect Vx instance support configuring the call routes for special purpose routing such as those listed in the following table:

Route	Description
Presence-Specific Routing	When away from the office forward the call directly to Voicemail (User extensions).
Multiple Destinations	Ring multiple phones simultaneously.
Multiple Connection Attempts	Ring a series of phones when the primary phone is not answered.
On Busy Routing	Ring 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 dependent on the Caller ID of the incoming call (User extensions). ***Note***: *When configuring special routing for incoming calls based on CID, if a call matches both the CID name and CID number rules, that call is routed based on the CID name rules.*
Hot Desk Routing	Route the call to a logged-in phone after logging into a shared phone. Default is disabled.

To allow users to define the extension routing using the My Allworx Manager page, see “To modify or delete existing users:” on page 228 for more information.

Notes:

- *The Shared Call Appearance feature does not support the call forwarding (45 + <extension>) function. Therefore, when creating a call route, do not include a Shared Call Appearance extension.*
- *Calls cannot be forwarded to phones at different sites within a Multi-Site network.*

To modify a call route for an extension:

1. Log in to the Allworx System Administration web page, and navigate to **Phone System** > **Extensions**.
2. Locate the extension or the user and click **View**. The page displays the *Extension Information* and associated *Presence* call route information which can be modified.
3. Locate the appropriate information and click to select one of the following options:

Extension Information	
modify *(system extensions)*	1. Click **Extension Information** > **modify** to: • **Description:** enter changes to the description of the extension. • **Schedule**: click to select a schedule to use for this extension from the drop-down list. • **Use different call routes for Day and Night Modes**: click to select the check box to enable this feature based on the selected schedule. • **Enable parking calls to this extension**: click to select the check box to enable. 2. Click **Update** to save the settings or **Cancel** to disregard the request.
modify *(user extensions)*	1. Click **Extension Information** > **modify** to: • *Set Presence Using Schedule:* click to select a schedule to use for this extension from the drop-down list. • *Enable parking calls to this extension:* check the box to enable. 2. Click **Update** to save the settings or **Cancel** to disregard the request.

Continued

Presence (Call Routes)

add new Call Route

Create a call route specific to the user. To update the call route:

1. Locate the Primary *Call Route Selection* pane and check the box or boxes to add the new route to the selected presence.
2. Use the Caller ID of the incoming call to a User extension to determine the call route.

Option	Description
external - Caller ID Number	enter the phone number with area code in the text box. Use the asterisk as a wild card.
internal - phones owned by	select the extension from the drop-down list

3. Locate the *Primary Call Route* pane. Follow the instructions below in **add a connection attempt**.

***Note**: When adding a new call route, only use extensions assigned to a physical phone.*

set the On Busy Route

Configure the next step in the call route if all destinations with a connection attempt of the primary route are busy.

1. Locate the On Busy Call route pane, and select one of the options:
   - **Treat a Busy as no answe**r
   - **Use Call Route below**: follow the steps in the add a connection attempt (below) to configure the next step in the call route.
2. Click **Update** to save the change.

modify

Update the current presence call routing.

1. Locate the P*rimary Call Route Selection* pane and check the box or boxes to add the new route to the selected presence.
2. Use the On calls from all callers to determine the call route:

Modify Primary Route	Updates the call route for all calls meeting the external caller criteria.
Modify On Busy Route	When following a Primary call route and all destination devices are busy during an individual connection attempt (no call appearances are available to receive the call), the call route changes to the On Busy route to follow the assigned sequence. If the On Busy route selection is Treat a Busy as no answer, then the call continues to the next connection attempt specified in the Primary route.

***Note**: Create and save (**Update** button) the primary call route before creating or modifying the On Busy Route.*

3. Locate the *Primary Call Route* pane. Follow the instructions in **add a connection attempt**.

Continued

add a connection attempt

Forward the call to another extension. To setup the connection attempt:

Note: *When adding a connection attempt, only use extensions assigned to a physical phone.*

1. Locate {**no selection**} and select an available location from the drop-down list (see Hot Desk note below).
   - For Follow-Me Anywhere: Enter 9 or 78[1]+ PIN (to gain an outside connection) followed by the phone number in the text box that appears to the right. (see the Follow me anywhere note below).

   Examples†: **9+1+aaa-xxx-nnnn**, **9+1+xxx-nnnn**, **78+ PIN+1+aaa-xxx-nnnn**, or **78+PIN+xxx-nnnn**.
2. (optional) Select the number of rings from the drop-down list. Click the ring style and select an option.

   Note: *The Ring Type setting overrides any call route specific Ring Type choices unless the appearance programmable button Ring Type is set to AUTO, which uses the selected Ring Type in* ***View Call Routes***.
3. (optional) Click **add a destination** and repeat steps 1 and 2 to ring multiple phones simultaneously.
4. (optional) Click **add another connection attempt** and repeat steps 1 and 2 to forward the call to another handset, if alternate phones should ring when the handset(s) in the First connection attempt are not answered. Continue to repeating step 4, as required.
5. Locate the *Finally* box, and select an option for the call if the user or any of the connection attempts do not answer.

   To delete any of the connection attempts, click **delete this attempt**.

Hang up (default)	The call ends - no further action is required.
Transfer to Auto Attendant	Select an option from the drop-down list.
Transfer to Call Queue	Select an option from the drop-down list.
Transfer to Voicemail for user	Select an option from the drop-down list.
Dial number	Enter a new number to forward the call.

The *Dial number* field must be one of the following:

Unaudited calls	**9+number**
Audited calls	**78+nnnnn+number**
Call Park	**700**
Park to Extension	**300 + extension**
Public SIP Directory calls	**8+nnnn**
Door Relay	**403**
Conference Center	**408**

Continued

add a connection attempt

(continued)

Paging Zones	***46n***

Notes: *Conference Center, Paging, and Door Relay are not available with the Connect Vx service.*

User or System Extension

Note: *Use a **P** in a number to insert a 1 second pause before dialing continues.*

Notes:

- ***Hot Desk Routes:*** *enables users to log in to shared phones, receive their calls on that phone, and place calls with their caller ID. Users can initiate the log in using a Hot Desk PFK or by selecting the Hot Desk Login option from the phone Config menu. Users can add Hot Desk destinations manually or automatically to user call routes. If none are present when the user Hot Desks into a phone, then Hot Desk destinations are added as the first connection attempt to all Presence call routes.*
- ***Follow me anywhere****: Users can forward calls to other phones outside of the Allworx System such as cell or home phones. If the recipient does not answer the call, the system directs the call 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 enables callers to leave messages in the default voice mail inbox. If the preferred setting is having callers leave messages on a personal phone voice mail, do not use the Follow-Me-Anywhere features. Instead, use the Finally route to direct calls to a cell or home phone by entering the phone number into the Dial number text box.*
  - *When an outside phone answers the call, the default is for the recipient to hear a prompt requesting to enter a **1** to accept the call. However, the Allworx administrator can configure user extensions so that Follow-Me-Anywhere calls to their extensions require a Message Center password in order to accept the call.*
  - *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.*

Park to Extension

modify (applicable to extensions with this feature enabled)

Configure the following settings specific to the Park to Extension feature:

- **Timeout:** in seconds. The amount of time the parked caller waits before moving to the next step in the call route.
- **After timeout:** define the next step in the call route after the parked call exceeds the timeout limit.
- **Hold Music Selection:** use the drop-down list to select an option.
- **Apply changes to the selected presence(s):** apply the configuration changes to multiple presence(s) by checking the appropriate box (applicable to user extensions only).
- **Apply changes to the selected mode(s):** apply the configuration changes to a specific mode by checking the appropriate box (applicable to user extensions only) Default: Night Mode selected.

4. Click **Update** to save the changes or **Cancel** to ignore the request.

11.6 Deleting an Extension

To remove an extension from the directory:

1. Log in to the Allworx System Administration web page and navigate to **Phone System** > **Extensions**.

2. Locate the extension or the user and click **Delete**.

3. Review the confirmation and click **Delete** to remove the extension.

Click here to return to the Installing and Configuring Allworx Premise Servers or Configuring Connect Vx Instances .

Chapter 12 Handsets

Prerequisites	
Access Permissions	Allworx Server Administrator Allworx System Administrator Phone Administrator role
Feature Key Required	• Generic SIP Handsets • Reach

Use the *Handsets* page to connect and manage Allworx handsets, as well as Reach, Interact Softphone, generic SIP, and analog handsets. The Allworx System Administration web page also provides access to manage handset preference groups, templates, Allworx phone Programmable Function Keys (PFKs), and Interact Softphone programmable functions.

Notes: *The Verge 9304 IP Phone has limited personal contact support (see "Contacts" on page 387 for limitations) and does not support the Reach Remote Control or the Call Handoff features, but it is compatible with the Allworx Interact application.*

12.1 Connecting the Phone to the Customer Network

Handsets receive their configuration information and software updates from the Allworx server through the Allworx System Administration web page. This section includes information and procedures for connecting phones to these types of networks:

- Allworx premise server LAN — With Allworx phones, this connection setup is automatic. Both the phone and Allworx premise server IP addresses are provided by the Allworx server. For more information, refer to "Connecting Allworx Desk Phones to the Customer Network" on page 104.
- Network with a customer-managed DHCP server or on a typical home network — This procedure applies to both premise servers and Connect Vx instances. For more information, refer to "Managing DHCP Settings" on page 104.
- Network with neither a customer-manager DHCP server nor an Allworx premise server or Connect Vx instance — Manually enter the IP addresses of the phone and Connect premise server or Connect Vx instance. For more information, refer to "Using Static IP Addressing" on page 105.

The Allworx Verge IP Phone series provides a quick start guide in the box with the phone and on the Allworx Portal (allworxportal.com). This guide provides instructions for setting up the phone and connecting it to power and the available network.

Notes:

- *To connect Generic SIP handsets to the customer network, refer to the manufacturer's documentation.*
- *Handsets connected to Connect Vx instances are always remote to the instance. Pay special attention to steps below that are specific to networks that include a Connect Vx instance.*

12.1.1 Connecting Allworx Desk Phones to the Customer Network

The following procedures describe connecting Allworx desk phones (92xx and Verge series phones) to the same Local Area network (LAN) as the Allworx premise server. If connecting to a different network, as with Connect Vx instances, see “Adding Handsets to the Allworx Server” on page 108.

12.1.1.1 Managing DHCP Settings

The Allworx phone default is DHCP client enabled. When connecting an Allworx phone to a network with a DHCP server, the phone automatically receives the network setup information.

- If the network DHCP server is the Allworx premise server, the phone connects automatically.
- If the DHCP server is not an Allworx premise server, set up the DHCP server to provide the phone with the Allworx server IP address using the TFTP boot server (Option 66) in the DHCP data set. If the TFTP boot server option is set properly, the phone needs no additional configuration.
- If the phone gets its IP address from a non-Allworx DHCP server and the DHCP server does not provide the TFTP boot server IP address, manually set the boot server IP address (the address of the Allworx premise server) on the phone. For more information, refer to “Using Static IP Addressing” on page 105.
- If the DHCP server is the Allworx premise server or if using a properly configured third-party DHCP server, use the Plug and Play feature to install the Allworx phone. For more information, refer to “Using Plug and Play” on page 109.

If an Allworx phone's DHCP client has been disabled, enable it using one of the following procedures.

To enable DHCP on a Verge phone:

1. Press the phone **Settings** soft key. The *Settings* screen appears.
2. Press the **Admin** soft key and enter the Phone Administration Password. Press **OK**. The *Administrative Settings* screen appears.
3. Navigate to **Network Settings** > **DHCP**. Change the setting to **Enabled**.
4. Press the **Save** soft key, and then press the **OK** soft key.
5. Reboot the Verge phone.

To enable DHCP on a 92xx phone:

1. Press the phone **CONFIG** soft key.
2. Use the arrow buttons to highlight *Network Settings*, and press the select button ☑.

   If prompted for a password, enter **allworx** using the numeric keypad, and then press the select button ☑. The DHCP setting highlights.
3. Use the arrow keys to highlight *Edit Boot Server*.

4. Press the select button ☑ and use the numeric keypad to enter the Allworx premise server IP address. Use the asterisk key (*) for periods. When complete, press the select button ☑.
5. Press the **EXIT** soft key repeatedly until asked to save the settings. Press the **YES** soft key.
6. Reboot the phone: press the **CONFIG** soft key, use the arrow keys to highlight *Reboot Phone*, and press the select button ☑. Answer **Yes** to the prompts.

   The phone reboots and connects using the DHCP server and manually entered settings.

12.1.2 Using Static IP Addressing

If the phone is not using DHCP to acquire its IP address, set the IP address using one of the following procedures.

Note: *Only the boot server IP address is required for connections to a network that has a DHCP server but is not using Option 66. All of the following settings are required if the network has no DHCP server.*

• Boot server (the Allworx premise server or Connect Vx instance IP address or domain name)	• DNS Server IP (Allworx premise server)	• Netmask IP
• Time Server (optional, can be an IP address or domain name of an Allworx premise server) ***Note:*** *For Connect premise server and Connect Vx instance phones, we recommend this be set to* ***time.allworx.net****. For networks that have a DHCP server, the customer's IT should configure the DHCP server to provide a time server IP address.*	• Phone IP	• Gateway IP

To update the Verge phone series static IP address:

1. Press the phone **Settings** soft key. The *Settings* screen appears.
2. Press the **Admin** soft key and enter the *Phone Administration Password*. Press **OK**. The *Administrative Settings* screen appears.
3. Navigate to **Network Settings** > **DHCP**. Change the setting to **Disabled**.
4. Use the navigation buttons to highlight and update the following settings (use the * button for the period):
   - *Static IP*
   - *Netmask* (if necessary)
   - *Gateway*
   - *Boot Server* (the Allworx premise server or Connect Vx instance IP address or domain name)
5. Press the **Save** soft key, and then reboot the Verge phone.

To update the 92xx IP phone series static IP address:

To access the **CONFIG** menu, either wait for the phone reboot to fail or interrupt the reboot by performing one of the following:

- For Allworx 9202 IP phones, press the **MUTE/DND** button three times.
- For all other 92xx IP phones, press the **RELEASE** button three times.

1. Press the phone **CONFIG** soft key.
2. Use the arrow buttons to highlight *Network Settings*, and press the select button ☑. If prompted for a password, enter **allworx** using the numeric keypad, and then press the select button ☑. The *Network Settings* menu appears and DHCP highlights.

   Note: *The 92xx series IP phones also use the password from the VoIP Server page*.
3. Press the select button ☑ until the DHCP setting is **Disabled**.
4. Use the arrow keys to highlight *Edit Boot Server.* Press the select button ☑. Using the phone keypad, enter the IP address or the domain name of the Allworx premise server or Connect Vx instance. Use the asterisk key (*) for periods. When complete, press the select button ☑.
5. Highlight, select, and enter the remaining settings from the list at the beginning of this section. Press the **EXIT** soft key repeatedly until the system prompts you to save the settings. Press the **YES** soft key.
6. Press the **CONFIG** soft key and use the arrow keys to highlight *Reboot Phone*, and press the select button ☑.
7. Answer **Yes** to the confirmation.

   The phone reboots and connects using the manually entered settings, including disabling DHCP.

12.1.3 Managing VLAN Settings

A site using Virtual Local Area Networks (VLANs) requires additional network configuration. Change the setting to **Manual** to reduce the phone boot time if the network settings VLAN is set to **Auto Configure**, and connecting the Allworx premise server or Connect Vx instance to a switch port that does not support a discovery protocol.

The Allworx phone's VLAN configuration options are as follows:

• Allworx System Software release 7.2 or higher (phone firmware version 2.2 or higher)	• Default to VLAN auto configure.
• Automatically configured Allworx phone	• The network utilizes LLDP-MED or CDP to set network host VLAN configurations.
• Manually configured Allworx phone	• If the phone is running an earlier version of firmware or if the network does not use LLDP-MED or CDP.

To configure VLANs on the Verge phone series:

Note: *If the phones are running an earlier version of the firmware or if the network does not use LLDP-MED or CDP, it may be more efficient to upgrade the phones prior to connecting to the site network. Do this in a lab by connecting the phones to an Allworx premise server that uses System Software release 7.2 or higher or to a Connect Vx instance.*

1. Press the **Settings** soft key, and then the **Admin** soft key.
2. Enter the phone administration password (available on the **Servers** > **VoIP** Allworx System Administration web page), and then press the **OK** soft key.
3. Use the navigation buttons to highlight *Network Settings* and press the select button ☑.
4. Navigate to **VLAN Mode** > **Select** > **Manual** > select button. This activates the rest of the VLAN CONFIGURATION settings.
5. Use the navigation buttons to highlight the *VLAN CONFIGURATION* settings. Press the select button ☑ to open each setting. Enter the values and press the select button ☑ to save the entered values.
   - Phone VLAN ID
   - PC VLAN ID
   - Phone VLAN Priority
   - PC VLAN Priority
6. Press the **Save** soft key repeatedly until prompted to save the settings. The *Save Network Settings* screen appears.
7. Press **OK** to acknowledge, and then restart the Verge phone. For more information, see “Restart / Shutdown” on page 363.

To configure VLANs on the 92xx series phone:

1. Press the phone **CONFIG** soft key. Use the arrow buttons to highlight *Network Settings* and press the select button ☑. If prompted for a password, enter **allworx** using the numeric keypad, and then press the select button ☑ if the phone is not registered on the server. Otherwise, use the password on the *VoIP Server* page. The *Network Settings* menu appears.
2. Use the arrow keys to highlight *VLAN*. Press the select button ☑ until the VLAN setting is **Manual.**
3. Use the arrow buttons to highlight *Phone VLAN Settings*. Press select ☑. Enter the values and then press the select button ☑ to save the entered values.
   - Phone VLAN ID
   - Phone VLAN Priority
4. Use the arrow buttons to highlight *PC VLAN Settings*. Enter the values and press the select button ☑ to save the entered values.
   - Phone VLAN ID
   - PC VLAN Priority

5. Press the **EXIT** soft key repeatedly until prompted to save the settings. Press the **YES** soft key.
6. Press the **CONFIG** soft key to reboot the phone, use the arrow keys to highlight *Reboot Phone*, and press the select button ☑. Answer **Yes** to the confirmation.

   The phone reboots and connects using the manually entered settings.

12.1.4 Creating an On-Phone Archive Profile

Allworx phones can store an On-Phone Archive profile using the CONFIG menu on the phone. Download additional profiles to the phone from the premise server or Connect Vx instance using the Handset Preference Groups.

The Verge phone series automatically creates an archive profile each time a user creates and saves a new network profile.

To create the on-phone archive profile for a 92xx IP phone:

1. Press the **CONFIG** soft key on the phone. Use the arrow buttons to highlight *Network Settings*, and press the select button ☑.

   If there is already a connection between the Allworx server and the phone, the system prompts for a password, enter the password from the Allworx System Administration web page. Find that password by navigating to **Servers** > **VoIP**, and then press the select button ☑. The *Network Settings* menu appears.
2. Use the arrow buttons and the select button ☑ to configure the network settings.
3. Press the **ARCHIVE** soft key to save the current network settings as the Archive profile. The Archive profile is used when changing the Network Settings and/or rebooting the phone.

12.2 Adding Handsets to the Allworx Server

After they are connected to the network, the handsets must be added in the Allworx server System Administration web page. This can be accomplished using either Quick Add, Plug and Play, or by entering the information manually.

If it is necessary to restart all of the Allworx handsets click **Reboot Allworx Handsets**. Handsets are not rebooted until they are idle. The premise server or Connect Vx instance automatically sends configuration information to Verge series phones without the need to reboot.

The Allworx premise server or Connect Vx instance automatically contacts the Allworx Portal about registered Verge series devices to communicate up-to-date phone warranty start dates. This registration happens automatically when connecting the Verge series devices to an Allworx premise server or Connect Vx instance. The system also sends a full list of Verge series devices to the Allworx Portal once per week. Allworx Server Administrators can click the **update Portal** link to send the entire list of Verge phones immediately.

Allworx users with permissions to the Allworx Portal can see the Allworx system information in one place (the *Portal Equipment Management* tool) to look up and manage the Allworx system information or to submit an RMA on-line. Allworx Server Administrators not connected to the Internet can manually export phone configuration information and import it onto the Portal.

To perform a search:

Locate handsets based on extension, description, owner, IP address, or caller ID.

1. Log in to the Allworx System Administration web page and navigate to **Phone System** > **Handsets**.
2. Locate the search line near the top of the page and enter the search criteria.
3. Press **Enter**. The table displays the information that matches the search criteria.

12.2.1 Using Quick Add

Quick Add can be used to add Allworx desk phone handsets (92xx and Verge series phones) to Connect premise servers and Connect Vx instances using either a MAC address or serial number. A bar code scanner can be used to enter serial number information directly from the label on the phone or its box.

To use Quick Add:

1. Navigate to **Phone System** > **Handsets**.
2. Click **add new Allworx Handset**.
3. In the *Handset Configuration* pane, click **enable Quick Add**.
4. Scan the phone serial number bar code to populate the *MAC Address* or *Serial Number* field, which immediately submits the form on this page. The browser remains on this page to immediately scan another phone - this is useful when adding multiple phones by scanning the serial numbers. The default selection for *Owner* is changed to **Assign later via phone or web** when using this method. This selection allows the phone’s owner to be selected during Plug and Play installation, by default.

   Notes:

   - *Adding phones automatically without clicking the Add button requires that the bar code scanner be configured to include a “carriage return” at the end of the serial number.*
   - *The Description field of the Allworx Handset pane is now optional. When the Description field is left empty, the MAC address of the phone is used as the description.*
5. Click **disable Quick Add** when the process is complete.

12.2.2 Using Plug and Play

Allworx desk phone handsets (92xx and Verge series phones) can be added to the Allworx premise server or Connect Vx instance using Plug and Play. Set up the network connection to the premise server or Connect Vx instance, and the phones will be registered during their next restart or power up. This tool is particularly useful when adding phones that are connected remotely, as is the case with all Connect Vx instances.

Plug and Play is enabled by unchecking the *Disable Phone Creates via WAN (Remote Phone) Plug and Play* check box on the VoIP Server configuration page of the Allworx System Administration web page. The *Plug and Play Secret Key* can be found on the **Servers** > **VoIP** page. For more information, refer to "VoIP Server" on page 295.

Caution:	• *Note that Plug and Play is disabled by default for both Connect premise servers and Connect Vx instances.* • *Plug and Play allows unauthorized users to add phones to the server without Allworx administrator intervention. To avoid this, disable Plug and Play installation for handsets. See "VoIP Server" on page 295 for more information.* • *Manually add phones to the system when disabling Plug and Play for security reasons or to configure the phone prior to plugging it into the network (for example: pre-configure the phone on the server before an installation at the customer site).*

Plug and Play assigns the default Handset Preference Group or template to each phone added (see "Allworx Handset Settings" on page 117). The user or extension is then selected on the phone screen. For more information about using the phone user interface, refer to the *Allworx Verge IP Phone Series User Guide* or other user guide that relates to the model of Allworx phone.

***Note**: To manually add generic SIP phones from other manufacturers, see "Manually Adding a Generic SIP Handset" on page 114.*

The following Plug and Play options are available:

***Note:** These options appear on the Allworx phone screen and display when Plug and Play is enabled and the phone connects to the Allworx server, but the handset has not yet been added to the System Administration web page.*

These options allow you to select when you assign users to a phone (*Now*, *Later*, or *Via Web*), and whether you are adding a new phone or replacing an existing phone.

Option	Description
Now > Add	Assigns a user to the phone immediately (*Now*). Select from the list of all system users or limit the list to those users with no assigned phones. Reboot the phone to complete the assignment.
Now > Replace	Replaces a compatible, existing Allworx phone. Select from the list of the all Allworx system phones. The phone web administration password, if any, is required to replace a phone. See "VoIP Server" on page 295 to view or change the password. Reboot the phone to complete the phone replacement.
Later	Defers the user assignment. If there is no existing phone configuration from within the Web Admin page, the user assignment prompts display on subsequent reboots.
Via Web	Assign the user via the web administration. The user assignment prompt does not display on subsequent restarts.

- If there is difficulty configuring a phone, restore the phone to the factory defaults, and then re-apply the settings.
- If rebooting an Allworx IP phone on the network and a new version of phone software is available, the phone firmware requests to load the upgrade.

- When using Plug and Play to register a phone, the Connect premise server or Connect Vx instance displays the phone on the *Phone System > Handsets* page. Locate the *SIP Handsets* pane with the correct model and the MAC address. For information about managing the handset configuration settings, refer to "Managing the Allworx Handset Configuration" on page 117.

12.2.3 Manually Adding a New Allworx Handset

Any Allworx handset (including Reach and Interact Softphone) can be added to the Allworx server System Administration web page manually using the procedures in this section.

Note: *Allworx Interact Softphone handsets cannot be added (connected) to Connect Vx instances.*

To manually add an Allworx handset:

1. Log in to the System Administration web page.
2. Navigate to **Phone System** > **Handsets**.
3. Click **add new Allworx Handset**.
4. In the *Handset Configuration* pane enter information in the text fields.

Field	Description
enable Quick Add	Click this link to allow the use of Quick Add. For more information, refer to "Using Quick Add" on page 109.
Model	Select a model number option from the drop-down list.Leave this field blank if adding the handset using the serial number.
MAC Address or Serial Number	Enter the Allworx phone MAC address or serial number that can be found on the phone label.

5. Enter the information in the *Allworx Handset* pane.

Field	Description
Owner	Select an option from the drop-down list.
Extension (optional)	Creates the extension with a call route to ring the handset.
Internal Caller ID Name	Enter the name to display on the Caller ID.
Internal Caller ID Number	Select an option from the drop-down list.
External Caller ID Name	Enter up to 47 characters of the name to display.
External Caller ID Number	Enter up to 24 digits to display.
Emergency Caller ID Number	Select an option from the drop-down list.
Description	Enter a meaningful name.
Dialing Privileges Group	Select a dialing privileges group option from the drop-down list.

Continued

Field	Description
Default Prompt Language	Select a language from the drop-down list; **Primary Language** or **Secondary Language**.

6. Enter information in the *Handset Features* pane.

Field	Description
Hold Music Selection	Select an option from the drop-down list.
Can Place Calls	Click to check the box to allow the extension to place external calls.
Can Receive Calls	Click to check the box to allow the extension to receive external calls.

7. Click **Add** to add the new handset to the Connect premise server or Connect Vx instance.

To manually add a Reach handset:

Note: *If the Reach handset link is not available, no unused Reach licenses are available on the Connect premise server or Connect Vx instance. Additional licenses can be purchased from an Allworx distributor.*

1. Log in to the System Administration web page.
2. Navigate to **Phone System** > **Handsets**.
3. Click **add new Allworx Reach Handset**.
4. Enter the information in the following fields.

Field	Description
Owner	Select an option from the drop-down list.
Extension (optional)	Creates the extension with a call route to ring the handset.
Internal Caller ID Name	Enter the name to display on the Caller ID.
Internal Caller ID Number	Select an option from the drop-down list.
External Caller ID Name	Enter up to 47 characters of the name to display.
External Caller ID Number	Enter up to 24 digits to display.
Emergency Caller ID Number	Select an option from the drop-down list.
Description	Enter a meaningful name.
Handset Configuration Template	Select an option from the drop-down list.
Dialing Privileges Group	Select a dialing privileges group option from the drop-down list.
Default Prompt Language	Select a language from the drop-down list; **Primary Language** or **Secondary Language**.

5. Enter the information in the *Handset Features* pane.

Field	Description
Hold Music Selection	Select an option from the drop-down list.
Can Place Calls	Click to check the box to allow the extension to place external calls.
Can Receive Calls	Click to check the box to allow the extension to receive external calls.

6. Click **Add** to add the new handset to the Connect premise server or Connect Vx instance.

To manually add an Allworx Interact Softphone:

Notes:

- *Allworx Interact Softphone cannot be added to Connect Vx instances.*
- *If the Allworx Interact Softphone link is not available, no unused Softphone licenses are available on the Connect premise server or Connect Vx instance. Additional licenses can be purchased from an Allworx distributor.*
- *Calls on mapped remote handsets do not display in the Active Systems Call window of the Interact Professional application.*

1. Log in to the System Administration web page.
2. Navigate to **Phone System** > **Handsets**.
3. Click **add new Allworx Interact Softphone**.
4. Enter the information in the following fields.

Field	Description
Owner	Select an option from the drop-down list.
Extension (optional)	Creates the extension with a call route to ring the handset.
Internal Caller ID Name	Enter the name to display on the Caller ID.
Internal Caller ID Number	Select an option from the drop-down list.
External Caller ID Name	Enter up to 47 characters of the name to display.
External Caller ID Number	Enter up to 24 digits to display.
Emergency Caller ID Number	Select an option from the drop-down list.
Description	Enter a meaningful name.
Handset Configuration Template	Select an option from the drop-down list.
Dialing Privileges Group	Select a dialing privileges group option from the drop-down list.
Default Prompt Language	Select a language from the drop-down list; **Primary Language** or **Secondary Language**.

5. Click **Add** to add the new handset to the Connect premise server.

12.2.4 Manually Adding a Generic SIP Handset

Note: *Allworx Generic SIP feature keys provide licenses to enable Generic SIP handsets. Allworx administrators can add a small number of handsets without a key (4 on the Allworx Connect 300 series premise servers, 6 on the Allworx Connect 500 series premise servers, and 12 on the Allworx Connect 731 premise servers). No licenses are automatically provided on Connect Vx instances.*

- *Available feature keys provide 1, 5, or 10 licenses each.*
- *For larger numbers of Generic SIP handsets, install multiple feature keys.*

To manually add a generic SIP handset:

1. Log in to the System Administration web page.
2. Navigate to **Phone System** > **Handsets**.
3. Click **add new Generic SIP Handset**.
4. Enter the information in the following fields.

Field	Description
Owner	Select an option from the drop-down list.
Extension	Not applicable to generic SIP handsets.
Internal Caller ID Name	Enter the name to display on the Caller ID.
Internal Caller ID Number	Select an option from the drop-down list.
External Caller ID Name	Enter up to 47 characters of the name to display.
External Caller ID Number	Enter up to 24 digits to display.
Emergency Caller ID Number	Select an option from the drop-down list.
Description	Enter a meaningful name.
Dialing Privileges Group	Select a dialing privileges group option from the drop-down list.
Default Prompt Language	Select a language from the drop-down list; **Primary Language** or **Secondary Language**.

5. Enter the information in the *Handset Features* pane.

Field	Description
Number of Lines	Select an option from the drop-down list.
Login ID	Click to check the box to allow the extension to place external calls.
Password	Click to check the box to allow the extension to receive external calls.

Continued

Field	Description
SIP Trust Level	Click to select the radio button to choose one of the following: • *Authenticate Registrations* - The server requires the device to provide a user name and password when the device registers. Once registered, the device can send invite requests (place a call) to the server unchallenged. The majority of SIP devices support this setting. • *Authentication Registrations and Invites* - The server requires the device to provide a user name and password when the device registers and when the device sends invite requests (places a call) to the server. This setting is more secure, but may not be supported by all devices.

6. Enter the information in the *Handset Features* pane.

Field	Description
Hold Music Selection	Select an option from the drop-down list.
This phone is behind a NAT/firewall and needs traversal assistance	Click to select this check box to activate traversal assistance.
Can Place Calls	Click to check the box to allow the extension to place external calls.
Can Receive Calls	Click to check the box to allow the extension to receive external calls.
Advanced Settings ***Note:*** *Click Reset Default Values to reset all Advanced Settings to the default value.*	
Enable Early Media	Click to select the check box. Allows audio from 183 Session Progress Responses.
Supports Symmetric Response Routing	Click to select the check box. RFC 3581 - include “rport” in requests.
Supports SIP REFER	Click to select the check box. RFC 3515 - “The SIP Refer Method.”
Offer ‘100rel’ support	Click to select the check box.
Obtain DID/DNIS number from	Select from the drop-down list.
Use ( ) in Request URI of outbound calls	Select from the drop-down list.
Local SIP port	Select from the drop-down list.

7. Click **Add** to add the new handset to the Connect premise server.

12.2.5 Manually Adding Analog Handsets

Analog handsets can not be used with the Connect Vx service unless connected through an Allworx Px Expander or a third-party SIP gateway (these handsets are managed on the third-party SIP gateway). For more information see “Px 6/2 Expanders” on page 265.

To connect an analog phone via the premise server FXS Phone Port:

Note: *Analog phones plugged in to Port Expander FXS ports do not automatically display on the Handsets page of the System Administration web page. Use the next procedure to add these analog phones manually.*

1. Plug the phone into one of the premise server FXS phone ports reserved for Inside Phone Extensions.
2. Lift the phone receiver so that the phone is off hook, and refresh the browser window and display the phone in the *Analog Handsets* pane of the Allworx System Administration web page. Then hang up the phone receiver.

To manually add an analog phone:

1. Log in to the Allworx System Administration web page and navigate to **Phone System** > **Handsets** > **Analog Handsets** > **New Analog Handset**. Click the additional information arrow ►, if necessary.
2. Update the settings described in the Analog Handset Settings table.
3. Click **Add** to update the *Analog Handsets* list or **Cancel** to ignore the request.

12.2.6 Testing the Phones

Some suggested steps for verifying that a phone is set up correctly:

- Dial **400**[1] for Auto Attendant
- Enter **#7** — the Auto Attendant plays back the phone configuration information
- Hang up — the phone rings back

If any of these steps fail, check the physical wiring between the phone and the premise server or Connect Vx instance, the network settings, or the phone and premise server or Connect Vx instance configurations.

[1] Extensions may vary per system. If using a non-default Internal Dial Plan, consult the Phone Functions tab of the My Allworx Manager page to determine the extensions to use for the corresponding feature.

12.3 Managing the Allworx Handset Configuration

Allworx handset configuration can be manually managed. As a part of this configuration, Handset Preference Groups are required for all local and remote Allworx handsets, and templates are a useful tool for applying configuration settings. These procedures describe how to manage the Allworx handset settings, assigning a Handset Preference Group, and applying a Handset Template.

For detailed information, refer to “Creating and Using Handset Preference Groups” on page 120 and “Creating and Using Handset Templates” on page 134.

12.3.1 Allworx Handset Settings

To manage Allworx handsets:

1. Log in to the Allworx System Administration web page and navigate to **Phone System** > **Handsets** > **SIP Handsets**. Click the additional information arrow ►, if necessary.
2. Click to select the *Show* check boxes for *Allworx Handsets, Allworx Reach, Allworx Interact Softphones,* and *Generic SIP Handsets* to show the desired handset type(s).
3. (optional) Click the **Bulk Edit** side arrow and check the box next to the handset to select it. Then click one of the following links:

Delete	Remove the selected handsets from the premise server or Connect Vx instance.
Assign	Change the Allworx Handset to the Handset Preference Group newly selected from the associated drop-down list.
Apply	Change the Allworx Handset to the Handset Template newly selected from the associated drop-down list.

4. Review and update the settings of the individual handsets as listed in the following table:

Setting	Description	Applies to:			
		Allworx Soft-phone	Allworx Desk Phone	Allworx Reach App	Generic SIP Phone
<Handset Preference Group Name>	Name of the HPG assigned to the phone. Default setting is **PBX Station (Default)**. Click the link to view the group settings. See “Creating and Using Handset Preference Groups” on page 120 for more information.	Yes	Yes	Yes	No
***View** Configuration*	Modify the current settings. See “To view the handset configuration:” on page 120 for more information.	Yes	Yes	Yes	No

Continued

Setting	Description	Applies to:			
		Allworx Soft-phone	**Allworx Desk Phone**	**Allworx Reach App**	**Generic SIP Phone**
***Add** Call Appearance*	Create another handset Call Appearance. Multiple Call Appearances enable handling calls for multiple users with a single phone. • Every automatically registered phone configuration includes one Call Appearance and two PFKs assigned to the Call Appearance. • Adding a second Call Appearance creates another address to use in call routes. 1. Click **Add Call Appearance.** 2. Click **Modify** for the new Call Appearance, select the user from the drop-down list, and click **Update**. 3. Click **View Configuration**, Programmable Function Keys **modify** > Call Appearance **change**. Select user from drop-down list and click **Done** > **Update**. 4. Locate the handset and click **Reboot**. 5. Click **Phone System**> **Extensions** > **View Call Routes** > **Modify** > **add a destination** > <user - select the unused Login ID number. To specify a different second user -- an example of an Admin Assistant: The office administrative assistant, Susan Bell, must answer the phones of two executives: Tom Brown and Lisa Andrews. • Susan has a Call Appearance for calls to her extension and a separate Call Appearance for each executive. • The Allworx administrator adds a Call Appearance PFK for each executive to Susan's phone. • The call route for each executive is set to ring both the executive handset and the Call Appearance on Susan's handset. • The PFK corresponding to the executive receiving a call flashes so that Susan knows which executive line is ringing and can answer accordingly (e.g. "Good morning, Tom Brown's office...")	Yes	Yes	No	No

Continued

Setting	Description	Applies to:			
		Allworx Soft-phone	Allworx Desk Phone	Allworx Reach App	Generic SIP Phone
Reboot	Restarts the phone. If the phone is in use, the reboot begins when the phone is idle. • **Reboot Allworx Handsets** is available at the top of the *SIP Handsets* pane to reboot all Allworx phones with one action. • One handset reboots every 10 seconds until all phones reboot. ***Note:*** *It is not necessary to reboot Allworx Verge phones and Interact Softphones in order for changes to take effect because these devices are automatically updated with configuration changes.*	Yes	Yes	Yes	No
Replace	Transfers all of the original phone configuration parameters and settings to a new phone. • Replace a defective handset with a new one. If the replacement has fewer PFKs than the original handset, the PFKs from the original handset are copied, in order from the bottom, left of the PFKs, up to the number of PFKs on the replacement handset. • The system replaces original unsupported handset PFK definitions on the replacement handset with default values.	No	Yes	No	No
IP Address	IP addresses assigned to the handset. If the PC has a network communications path to the phone, click the *Handset IP Address* link to open the phone administration page in a separate browser window; see “Accessing the Allworx Phone Administration Web Page” on page 157 for more information.	No	Yes	No	No
Setup	Displays the *Reach Installation Assistance* website.	No	No	Yes	No
Modify	Modify handset *Call Appearance* parameters.	Yes	Yes	Yes	Yes
Delete	Deletes the Call Appearance from the phone. If there is only one Call Appearance, the phone is deleted from the system.	Yes	Yes	Yes	Yes
Ring	Click to verify an operational phone connection.	Yes	Yes	Yes	Yes

5. Reboot the phone after changing any settings on the *View Configuration* page to update the phone to the new settings using **Reboot** described above or manually from the phone.

   Note: *It is not necessary to reboot Allworx Verge phones and Interact Softphone devices in order for changes to take effect because these devices are automatically updated with configuration changes.*

To view the handset configuration:

1. Log in to the Allworx System Administration web page, navigate to **Phone System** > **Handsets** > **SIP Handsets.** Click the additional information arrow ►, if necessary.
2. Click to select the *Show* check boxes for *Allworx Handsets, Allworx Reach, Allworx Interact Softphones*, and *Generic SIP Handsets* to view the desired handset type(s).
3. Click **View Configuration** to see the associated configuration parameters. In addition to the phone summary and status information, the following options display:

Option	Description
Handset Preferences Group	Displays the current preference group. 1. Click **modify** to update the current preference group by making a selection from the drop-down list. 2. Click to select the *Reboot Handset after assigning HPG* check box if needed. 3. Click **Update** to have the change take affect. See “Creating and Using Handset Preference Groups” on page 120 for more information.
Template Options	• **Save**: Click to keep the current handset configuration as a template. • **Apply**: Select a different handset configuration from the drop-down list and then click **Apply**.
Programmable Function Keys	Adjust the PFK assignment options. Click **modify** to update the current settings. See “Managing the Programmable Function Keys (PFKs)” on page 138 for more information.
Interact Appearances	Appearances available on Interact Professional only. Adjust the settings for each appearance. Click modify to update the current setting. See “To manage the PFKs:” on page 138. ***Note***: *The Verge phone series does not support the Interact Appearances features.*

4. Reboot the phone to save changes.

12.3.2 Creating and Using Handset Preference Groups

Each Handset Preference Group is a custom configuration of the handset settings used to configure many handsets easily and efficiently by assigning handsets to the group. The *Handset Preference Group* pane displays the available default and custom preference groups. The PBX and Key System Default groups contain the factory default handset options for the respective modes.

Premise servers running Allworx System Software 8.5 and higher and Connect Vx instances automatically notify Verge phones when updates are made to the *Handset Preference Groups* pane, and then update that configuration on the Verge phones without action from the user or administrator. If Verge phones are the only phones connected to the premise server or Connect Vx instance it is not necessary to reboot the phones after making these changes.

Note: *Settings for existing handsets do NOT change in this process.*

To manage a Handset Preference Group:

1. Log in to the Allworx System Administration web page and navigate to **Phone System** > **Handsets**
2. Locate the *Handset Preference Groups* pane. Click the additional information arrow ▶, if required, to display the handsets assigned to each Handset Preference Group.

   Click one of the following actions:

Action	Description
View	Displays the Handset Preference Group current configuration options. 1. Click **modify** to update. See "Handset Preference Group Settings" on page 122 for more information. 2. Click to select the *Reboot handsets assigned to this Handset Preference Group* check box if phones other than Allworx Verge phones are assigned to the group. 3. Click **Update** to save the changes. ***Notes:*** • *Premise servers running Allworx System Software 8.5 and higher and Connect Vx instances automatically notify Verge phones when PFKs are added or removed, and then update that configuration on the Verge phones without rebooting the phones.* • *The System Software does not allow the modification of default Handset Preference Groups. Copy a default Handset Preference Group, and then click **View** > **modify**.*
Copy	Creates a new Handset Preference Group with the same settings. This new group can then be modified as necessary to make it unique.
Delete	Removes the current Handset Preference Group. If the **Delete** link is unavailable: 1. Click **View**, and locate the *Handsets Assigned To Group* pane. 2. Click **Modify**, and deselect all the associated handsets. 3. Click **Update**, and restart this procedure. ***Note:*** *The default Handset Preference Groups cannot be deleted.*

12.3.2.1 Handset Preference Group Settings

Do one of the following to update the setting:

- Check the box to enable
- Enter text or numbers, as required
- Click the drop-down arrow and select an option from the list

Setting	Description	Applies to			
		Verge Series	92xx Series	Reach App	Softphone
Name	Description of the Handset Preference Group.	Yes	Yes	Yes	Yes
Audible Dialing	Hear DTMF sounds on the handset or speaker when dialing the phone. Default = Enabled (check box selected).	Yes*	Yes*	Yes*	Yes
Auto On Hold	Place an active call on hold when another call comes in (with a free Call/Line Appearance PFK) when pressing the PFK for the new call. **Default** = Enabled (check box selected). • Avoids terminating the first call.	Yes*	Yes*	No	Yes
Auto Retrieve Calls	Enable automatic retrieval of a hold call by going off hook. **Default** = Disabled • If disabled, connect to an open line (if available) when going off hook.	Yes*	Yes*	No	No
Bluetooth	Pair a *Bluetooth* enabled device to the Verge 9312 IP Phone. The Allworx System supports *Bluetooth* standard 4.0, class 1. **Default** = Enabled (check box selected).	9312	No	No	No
Bluetooth Hands-Free PFK is user assignable	Assign the Bluetooth PFK to a programmable button on the Verge 9312 IP Phone. **Default** = Enabled (check box selected).	9312	No	No	No
Call Handoff Timeout	Specify the amount of time (in seconds) before canceling the Call Handoff. ***Note:*** *The Verge 9304 IP Phone does not support the Call Handoff feature.*	Yes	No	Yes	Yes

Continued

Setting	Description	Applies to			
		Verge Series	92xx Series	Reach App	Softphone
*Call History Size**	Specify the number of calls the station keeps in the call history. If specifying a value of zero, the phone does not maintain a Call History to help preserve the privacy of the phone user. Allworx IP Phone series supports displaying up to 200 listings. The Allworx 92xx series phones support displaying a maximum of 99 call history listings.	Yes*[1]	Yes*	No	Yes
Call Supervision	Monitor the handset with another handset that has a Call Supervision PFK. **Default** = Enabled (check box selected)). ***Note:*** *Only the 9202E, 9204/9204G, Verge phones, and Interact Softphone handset can be supervised when being recorded or in a 3-way conference.*	Yes	Yes	No	Yes
Call Timer Display	Display the phone LCD call duration timers. **Default** = Enabled (check box selected).	Yes*	Yes*	No	No
Caller ID Display	Display any caller ID information. **Default** = Enabled (check box selected).	Yes	Yes	No	No
Caller ID Preference	Identify the call information to display in TAPI-compliant PC applications that receive calls using the TSP driver and Allworx IP Phone displays that have only one available field for caller information: • Allworx 9202E status display • Allworx Verge phone appearance programmable button labeling. Select one of the following options to display: • Calling Party Info (Caller ID) • DNIS Information (Dialed Name and Number)	Yes*	Yes*	No	Yes
Cell Phone Dialing	Require users to press the **Send** soft key (☎) to place the call. This feature is not available with Line Appearance calls. Default = **Disabled**.	Yes*	No	No	No
Clock Mode	Display phone station clock in a **12-hour** or **24-hour** format. **Off** disables the clock display.	Yes*	Yes*	No	No

Continued

Setting	Description	Applies to			
		Verge Series	92xx Series	Reach App	Softphone
Codec Preference Order	Check the box to select the codecs. Click and drag the codecs for the preferred codec usage order. Contact the service provider for the preferred codec order. ***Note: G.722 i****s not supported for premise server or Connect Vx instance audio.* This setting defines codec selection order and does not support all codecs for all call types (For example: accessing the Auto Attendant requires **G.711**). The phone attempts to use the first choice but uses the codec required to support the call.	Yes	Yes	Yes	Yes
Configuration Menu	Access the configuration menu when securing phones located in common areas.	Yes	Yes	No	No
Daylight Saving Time	Specify if the handset uses Daylight Savings Time (DST) to compute the local time. • **Off** - Does not use DST • **On** - Follows US rules for DST • **Use current server setting** - Phone and the premise server or Connect Vx instance are in the same time zone ***Note:*** *For remote phones, use the DST setting of the actual location (available further down the page).*	Yes	Yes	No	No
Display Date Format	Change the date display order. • MM/DD/YY • YY/MM/DD • DD/MM/YY ***Note****: If the phone does not display the year (e.g., 9202e phone), the month and day matches the order of the selection without the year.*	Yes*	Yes	No	No

Continued

Setting	Description	Applies to			
		Verge Series	92xx Series	Reach App	Softphone
Display Language	Change the Allworx phone display language. • Requires Allworx System Software 7.6.6.5 or later. • Requires the Dual Language Support feature key. The phone defaults to English during a Factory Reset, functional test mode, or if the Dual Language Support feature key is unavailable. • Not available to change the phone display language within the phone configuration menu.	Yes	Yes	No	No
DTMF Playout	Send DTMF digits during an active call. **Default** = Enabled (check box selected).	Yes	Yes	Yes	Yes
Handset Network Template	Select a Handset Network Profile Template from the drop-down list to download to the handset.	Yes	Yes	No	No
Hold and Park Reminder Mode	Remind the handset user there is a call on hold or parked to an extension for which the user has park notifications set. Select the reminder type: • **No Reminder** - does not notify the user. • **On Hook** - beeps when the phone is put on-hook with the call on hold. • **Timer** - beeps after holding the call for the specified period. • **On Hook and Timer** - beeps after the holding call for the specified period or if placing the handset on hook.	Yes*	Yes*	No	Yes
Hold and Park Reminder Timeout	Specify a length of time (0-600 seconds) before a beep occurs for a call on hold or parked to an extension for which the user has park notifications set. Default = **120** seconds • **Available** - Hold Reminder is **Timer** or **On Hook and Timer.** • **Unavailable** - Hold Reminder is **No Reminder** or **On Hook**.	Yes*	Yes*	No	Yes

Continued

Setting	Description	Applies to			
		Verge Series	92xx Series	Reach App	Softphone
*Hold Button Mode**	Control the behavior of the phone Hold button: • **Hold Calls, Park Lines** - holds calls on Call Appearances. Parks calls on line appearances. • **Hold then Park** - press and release quickly to place the call on hold. Pressing the button longer places the call in a Parking Orbit. • **Park then Hold** - press and release quickly to park the call. Pressing the button longer, places the call on hold. ***Note**: Does not apply to Verge Phones.*	No	Yes*	No	No
Hold Music Selection	Determine the hold music such as Line-In or a **.snd** file.	Yes	Yes	Yes	Yes
Intercom Auto Answer	Answer an incoming Intercom call automatically. **Default** = Enabled (check box selected).	Yes*	Yes*	Yes	Yes
Keypad Dialing	Initiate or transfer a call via the keypad. **Default** = Enabled (check box selected). • Does not prevent the keypad from functioning during an active call. • Prevent the use of the keypad to initiate functions directly with the Allworx premise server or Connect Vx instance (for example: dial number, Call Park, etc.).	Yes	Yes	No	No
Line Appearance(s) Use Dial Plan	If not enabled when selecting a Line Appearance PFK to dial a number, the phone does not: display the number, include the number in the call history, or enable the user to redial the number. A reason for disabling this option - if the CO lines on the system do not follow the North American Numbering Plan (including if the lines connect to another PBX). This feature requires configuring the dial plan. See "Dial Plan" on page 67). **Default** = Enabled (check box selected).	Yes	Yes	No	Yes

Continued

Setting	Description	Applies to			
		Verge Series	92xx Series	Reach App	Softphone
Max Jitter Buffer Size	Alter the size of the jitter buffer. • Variation in network audio packet; the phone experiences latency, resulting in a reduction in audio quality. • Uses a jitter buffer to maximize the audio quality when jitter occurs.	Yes	Yes	No	Yes
Message Waiting Indication (optional for stations with no owner)	Control the Voicemail message indicator for the phone owner. • **No Indication** - provides no visual display on the handset. • **Visual -** illuminates the red LED on the Messages button. • **Stutter Dial Tone** - emits a stutter when a dial tone starts for each call. • **Both** - provides a visual indicator and a stutter dial tone.	Yes	Yes	No	No
Messages Button	Control the behavior of the phone Messages Button. • **Displays Messages List** - view and manage Voicemails via: • Press the Messages button once to use the phone display. • Press the Messages button twice to call the Audio Message Center. • **Calls Message Center** - press the Messages button to call the Message Center and use audio menus to manage Voicemail.	Yes*	Yes*	No	No
Missed Call Tracking	Display the number of calls missed since last making or receiving a call. Select which missed calls to track: • **None** • **Call Appearances Only** • **All Appearance Types**	Yes*	Yes*	No	Yes
Mobile Data Access	Access to Wi-Fi and mobile networks.	No	No	Yes	No *Continued*

Setting	Description	Applies to			
		Verge Series	92xx Series	Reach App	Softphone
NAT/Firewall Traversal Assistance	Default = **Enabled** (check box selected for all Connect Vx handsets, as well as Generic SIP handsets connected to Connect premise servers). **Disabled** (check box <u>not</u> selected for Connect premise servers and all handsets other than Generic SIP). Enables the ability to handle firewalls more efficiently for remotely connected phones. The default setting is included in the default Handset Preference Group.	Yes	Yes	No	Yes
Network Settings	Determine if the handset uses the selected Network Template or relies on the network settings entered on the phone.	Yes	Yes	No	No
Off Hook Auto Answer	Answer any new call when the handset goes off hook. Default = Enabled (check box selected).	Yes*	Yes*	No	No
Off Hook Digits Dialed	Dial specified digits automatically whenever the phone is off hook. • **Example 1**: a service phone placed at a locked door or loading dock • **Example 2**: a phone automatically dials 9# to get an outside line. ***Notes***: • *Always dials these digits when taking the phone off hook, pressing the speaker button, or dialing digits. Pressing the appearance does not cause the digits to be dialed. Example: if configuring the phone to automatically dial '9', press the call appearance PFK to access features that don't start with '9' (e.g. Call Park, Call Forwarding, etc.).* • *Calls cannot be forwarded to phones at different sites within a Multi-Site network.*	Yes	Yes	No	No
Off Hook Ringing	Ring when receiving a new call while the handset is off hook. • Disabled (default) - does not ring the phone, if there is an active call. • Does not affect the appearance LED indicators or the display.	Yes*	Yes*	Yes	Yes

Continued

Setting	Description	Applies to			
		Verge Series	92xx Series	Reach App	Softphone
On Hook Dialing	Dial a keypad number. Accesses the speaker phone automatically if the phone is on hook and the user dials a digit on the keypad. Default = Enabled (check box selected).	Yes*	Yes*	No	No
Paging Mode	Specify the conditions for hearing pages on this handset. Options: • Pages always accepted. • Pages never accepted. • Pages only accepted when the station is on-hook (default).	Yes*	Yes*	No	Yes
Park Soft Key Behavior	Control the functionality of the Park soft key. • **System park**: (default setting) place active and/or held calls on the system wide park for any user to retrieve. • **Park to Extension:** Prompt the user to enter a recipient extension or select a recipient using the **Contact** function button, a **Contact** programmable button, or a **Park to Extension** programmable button. ***Note****: Allworx 92xx IP phones always perform a System Park when pressing the* ***Park*** *soft key.*	Yes	No	No	No

Continued

Setting	Description	Applies to			
		Verge Series	92xx Series	Reach App	Softphone
Parked Calls List Contents	Control the information displayed on the Parked Calls screen. • **All parked calls**: (default setting) displays every parked call in the system. • **Restricted**: limits the Parked Calls screen to display the following types of calls: • Calls parked for this phone owner • Calls parked using this phone • Calls parked for the extensions of configured Parked to Extension programmable buttons • All system-parked calls ***Notes***: • *Allworx phones do not provide notifications for calls that are not eligible for the parked calls list on the phone, even if the owner has set the notification flag for other contacts with parked calls.* • *Verge phones display a message indicating the list is restricted.*	Yes	No	No	Yes
PCP Keep-alive Interval	Adjust the communication time between the Interact application and the Allworx phone, if there are network problems between Interact and the phone that are causing Interact to disconnect from the phone, extending this interval can avoid spurious disconnection and reconnection.	Yes	Yes	No	Yes
Personal Contacts Display	Set the Personal Contacts on all Allworx phones to Unrestricted or Restricted. Allworx users can update this setting on their assigned extension. • **Unrestricted:** Requires phone log in for details and management. Log in is valid until the user leaves the Contacts screen. The unlocked icon is on the Verge phone series status bar only when the user logs in via the Contacts screen. • **Restricted:** Requires login via soft key to see personal contacts including contact PFKs. Log in is valid until user logs out via soft button on Contacts screen. Status always displays on the Verge phone series status bar.	Yes[2]	No	No	No

Continued

Setting	Description	Applies to			
		Verge Series	92xx Series	Reach App	Softphone
Phone SIP Port	Specifies the port that the phone uses to receive SIP commands and responses.	Yes	Yes	No	Yes
Quick Transfer	Enable one-touch call transfers using PFKs that place calls automatically. **Default** = Enabled (check box selected).	Yes	Yes	No	No
Redial Memory	Store the last dialed user extension or external phone number. • Enabled (**default**) • Disabled	Yes*	Yes*	No	No
RTP /RTCP Port Range	Specify the range of UDP ports used for Real Time Protocol audio. • Typically 16384 to 32767 - where the low value must be even numbered and the high value must be odd numbered. • When placing remote phones behind third-party firewalls, under certain conditions, to create mapping rules for each phone behind the firewall, greatly restrict the UDP port range. • See “Px 6/2 Expanders” on page 265.	Yes	Yes	Yes	Yes
Server RPC Timeout	Use with Hot Desk login timeout. **Default** value is 10 seconds. Adjustable from 3 to 30 seconds for network latency.	Yes	Yes	No	Yes
Server SIP Port	Specifies the port that the premise server or Connect Vx instance uses to receive and send SIP commands and responses.	Yes	Yes	No	Yes
SIP NAT Keep-alive Interval	NAT firewalls automatically time out and close connections to protected devices. • If a remote phone is behind such a firewall, this prevents the timeout. • The phone sends messages called keep-alive packets to the Allworx server at the specified frequency. • Set the value to an interval that is shorter than the firewall timeout.	Yes	Yes	No	Yes

Continued

Setting	Description	Applies to			
		Verge Series	92xx Series	Reach App	Softphone
Sleep Mode Timeout	Specify the number of idle minutes that pass before the Verge Phone enters the sleep/ screen lock state. Enter the number of idle minutes.	Yes[3]	No	No	No
SNMP	Use the SNMP agent on the handset with network management tools.	Yes	Yes	No	Yes
Station Mode	Change the phone behavior to PBX Behavior or Key System Behavior. It affects how some of the PFK functions work, see "Managing the Programmable Function Keys (PFKs)" on page 138.	Yes	Yes	No	Yes
Syslog Server Address	Enter the IP address or Domain Name.	Yes	No	No	Yes
Syslog Server Port	Typically set to **514**. Update as necessary for the firewall.	Yes	No	No	Yes
Time Zone	Specify the time zone used to compute the local time. Select the time zone from the drop-down list.	Yes	Yes	No	No
Transfer Mode	Specify how the user completes unannounced (blind) transfers immediately after dialing the recipient phone number. • **Requires hang-up** - default to an Attended Transfer and requires the Allworx user place the phone on hook or press transfer to complete the call. To do a Blind Transfer, the Allworx user must hang up before announcing the call. Default setting. • **Immediate** - completes the call transfer immediately (Blind Transfer) after placing the call to the recipient. For an Attended Transfer, press the Attended soft key before placing a call to the recipient.	Yes	Yes	No	No
Visual On Call	Light the handset Visual Ring Indicator when the handset is off hook. **Default** = Enabled (check box selected).	Yes*	Yes*	No	No
Visual Ringing	Light the Visual Ring Indicator when the phone receives an incoming call. If disabled, the user only hears ringing. **Default** = Enabled (check box selected).	Yes*	Yes*	No	No

Continued

Setting	Description	Applies to			
		Verge Series	92xx Series	Reach App	Softphone

* Indicates the on-handset configuration menu can override the setting.

[1] Allworx 92xx IP phone series have maximum *Call History* size of 99.

[2] Can only override at handset if setting is "Unrestricted".

[3] Can only override at handset to a smaller value.

12.3.3 Multiple Remotely Connected Handsets

In most cases, temporarily enable adding handsets to the Allworx server using the WAN Plug and Play feature (see "Using Plug and Play" on page 109). Then, on the phone configure the server IP address and *Plug and Play Secret Key* and register the phone.

Note: *After new phones have been registered, remember to go back and check the Disable Phone Creates via WAN Plug and Play check box on the Allworx server.*

With Connect VX all phones are considered to be coming from a remote network. Many may be coming from the same site with the same public IP address. The historical recommendation to assign unique RTP Media Port Ranges in a Handset Preference Group (HPG) for each handset using the same IP is only necessary when multiple phones are behind a hostile/aggressive firewall that cannot be updated to allow consistent NAT (one-to-one). Be sure to enable *NAT/Firewall Traversal Assistance* in the HPG for each handset.

If needed, Allworx recommends that the firewall be adjusted as follows:

1. Always disable SIP ALG.
2. Enable source port that keeps the consistent or 1-to-1 NAT.
3. Only after these adjustments, resort to assigning an individual RTP Media Port Range and SIP port per device as described in "Creating and Using Handset Preference Groups" on page 120. When multiple phones are connected remotely to a Connect Vx instance, it may be necessary to build custom Handset Preference Groups to allow the handsets to work with the firewall.

Note: *Be aware that different firewall manufacturers may use different terminology, and have different procedures for making these changes.*

For information about assigning the RTP Media Port Range, see "Multiple Remote Devices Behind the Same Firewall" on page 270.

12.3.4 Assigning Handsets to Handset Preference Groups

Note: *If there is a change to the Display Language setting, the phone displays the current language at the beginning of the reboot and then displays the new language at the end of the reboot.*

When adding new handsets, the premise server and Connect Vx instance automatically assigns the handsets to the Handset Preference Group in the active Handset Template. If the phone factory default options are not accurate for the site, create a custom Handset Preference Group and incorporate it into a new, active phone template before adding the site handsets.

To add handsets manually to Handset Preference Groups:

View Configuration	See “To view the handset configuration:” on page 120 for more information.
Handsets assigned to Group	1. Log in to the Allworx System Administration web page, navigate to **Phone Systems** > **Handsets** page. 2. Locate the *Handset Preference Groups* pane and click **View.** 3. Locate to the **Handsets Assigned To Group** and click **Modify**. 4. Use the check boxes to add or remove the user from the Handset Preference Group. When removing a handset, it automatically moves to the server PBX Station or Key System Station default group.

12.3.4.1 Rebooting Handsets After Modifying Handset Preference Group Settings

A handset that is assigned to a Handset Preference Group must be rebooted for any of the modified settings to be active. Reboot each handset individually at a convenient time, or select the **Reboot handsets assigned to this Handset Preference Group** check box (when updating the Handset Preference Group settings) to initiate a reboot for all assigned handsets.

Note: *Allworx premise servers with Allworx System Software 8.5 and higher and Connect Vx instances automatically update the settings on Verge phones when a change is made to Handset Preference Groups. No reboot is required.*

12.3.5 Creating and Using Handset Templates

To save time and reduce errors while configuring phone and Interact Softphone handsets, the Allworx premise server and Connect Vx instance include templates that store phone configurations for each phone type or allow the creation of customized templates.

To see a list of current templates:

1. Log in to the Allworx System Administration web page, navigate to **Phone System** > **Handsets**.
2. Locate and open (click the additional information arrow ▶, if necessary):
   - *Handset Network Profile Templates* – Displays the current network profile templates. Click **View** to see the available profile templates.
   - *Handset Configuration Templates* – Displays the list of *Active Templates* and *Handset Templates*. Click the phone model link in either table to view that template.

To manage Network Profile Templates:

The phone stores network and registration settings as a Handset Network Profile. Allworx administrators can select a Handset Network Profile to avoid manually changing phone settings for different situations such as connecting to a second Allworx premise server or Connect Vx instance for disaster recovery purposes.

1. Log in to the Allworx System Administration web page, navigate to **Phone System** > **Handsets** > **Handset Network Profile Templates**, and click the additional information arrow ►, if necessary.
2. Click one of the following actions:

<table>
<tr><th>Action</th><th colspan="2">Description</th></tr>
<tr><td rowspan="10"><b>View</b>
<i><b>Note</b>: Phone settings can override the Next Phone Reboot setting. Verify the Handset Network setting. See the phone user guide to update the settings.</i></td><td colspan="2">To associate a new profile with the template, click <b>add profile</b> and update settings. For existing profiles, click <b>modify</b> to update existing settings or <b>delete</b> to remove the template from the list.
<b>Network Profile Settings</b></td></tr>
<tr><td><i>Profile Name:</i></td><td>Enter a description.</td></tr>
<tr><td><i>Phone IP:</i></td><td>Select an option from the drop-down list:
• <b>DHCP</b>
• <b>Use Phone Setting</b>
• <b>It is not possible to assign a static IP address to a phone using a Handset Network Profile</b></td></tr>
<tr><td><i>VLAN:</i></td><td>Select an option from the drop-down list:
• <b>Auto Configure</b> • <b>Hub Debug Mode (92xx series IP phones only)</b>
• <b>Disabled</b> • <b>CDP Enabled</b>
• <b>Manual</b> • <b>LLDP Enabled</b></td></tr>
<tr><td><i>Auto NAT:</i></td><td>Assists phones that are remote and behind a firewall or router using NAT. Select <b>On</b> or <b>Off</b> from the drop-down list.</td></tr>
<tr><td><i>Plug and Play Key:</i></td><td>Enter a new key.</td></tr>
<tr><td><i>Boot Server Address:</i></td><td>Enter the <i>IP Address</i> or <i>Domain Name</i>.
<i>Continued</i></td></tr>
<tr><td>Phone VLAN Settings</td><td>Enter an ID and Priority number.</td></tr>
<tr><td>PC VLAN Settings</td><td>Enter an ID and Priority number.</td></tr>
<tr><td colspan="2"><i>Continued</i></td></tr>
</table>

<table>
<tr><th>Action</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><td>Switch PC Port
<em>(Verge Phone only)</em></td><td>Select an option from the drop-down list:
• Enabled
• Disabled</td></tr>
<tr><td>Switch Port Mirror
<em>(Verge IP Phone only)</em></td><td>Select an option from the drop-down list:
• <em>Disabled</em>
• <em>Network</em> (LAN) - mirrors the network communications going through the phone network port.
• <em>Internal</em> - mirrors the network communications going to the phone CPU.</td></tr>
</table>
Click <strong>Add</strong> to save the new profile.</td></tr>
<tr><td><strong>Copy</strong></td><td>Duplicates the selected Handset Network Profile Template. This new template can be viewed and modified as necessary to make it unique.</td></tr>
<tr><td><strong>Delete</strong></td><td>Remove the profile from the list. Verify the selected template, and then click <strong>Delete</strong> to remove the template. The default template cannot be deleted.</td></tr>
</table>

3. Select **add profile** for more profiles following the steps above.

   After creating a template, assign it to the phone using the Handset Preference Groups. Follow the procedure "Creating and Using Handset Preference Groups" on page 120.

To change the Handset Configuration Template:

The current, default template for each phone type lists in the *Active Templates* list.

1. Log in to the Allworx System Administration web page, navigate to **Phone System** > **Handsets** > **Handset Configuration Templates.** Locate the phone model number, and click **Change**.
2. Select a Handset Template from the drop-down list to use as the default, and then click **Update** to save the change.

To manage the Handset Templates:

Allworx administrators cannot change or delete factory default handset templates.

1. Log in to the Allworx System Administration web page and navigate to **Phone System** > **Handsets** > **Handset Configuration Templates** > **Handset Templates**. Click the additional information arrow ▶, if necessary.
2. Click one of the following actions:

Action	Description
<Template name>	Click a default template to view the settings. Click a non-default template to view/modify the settings.

Continued

Action	Description
Copy	Create a duplicate of the selected Handset Template. This new template can be viewed and modified as necessary to make it unique.
Delete	Remove the Handset Template from the list. ***IMPORTANT:*** *The Allworx premise server and Connect Vx instance do not allow deleting Factory Default or Active Handset Templates. Requires no further action.*

3. Click the Handset Template to open the *View Template* page and select one of these options.

Option	Description
edit name	Enter a new description in the field provided.
Handset Preference Group pane	Click **modify** and select a **Handset Preference Group** from the drop-down list.
Programmable Function Keys	Click **modify**. See “Managing the Programmable Function Keys (PFKs)” on page 138 for more information.
Interact Appearances	Click **modify** and check or uncheck the appropriate check boxes to enable or disable the Interact Appearances, respectively (applicable to 92xx IP phones only).

4. Click **Update** to save the change.
5. Navigate back to the **Phone Systems** > **Handsets** > **SIP Handsets**, and click **Reboot Allworx Handsets**. This reboots the Allworx handsets for the changes to take effect.

To assign a handset template:

1. Log in to the Allworx System Administration web page, navigate to **Phone System** > **Handsets** > **SIP Handsets**, and click the additional information arrow ►, if necessary.
2. Click one of the following links:

Link	Description
+	Bulk edit feature - assigns the Handset Preference Group to multiple handsets at once. 1. Click the check box in the left column to select the phones to apply the Handset Preference Group. 2. Locate the **Handset Template Group** line and make a selection from drop-down list. 3. Click **Apply**.
<User>	1. Locate the line for the specific phone and click **View Configuration**. 2. Locate the *Template Options* pane and select the preferred template in the drop-down list. 3. Click **Apply**.

3. Locate the *SIP Handsets* pane and click **Reboot Allworx Handsets.** This reboots the Allworx handsets for the changes to take effect.

12.4 Managing the Programmable Function Keys (PFKs)

Manage the PFKs (labeled programmable buttons) by describing and assigning a PFK, reordering PFK assignments, and managing the call appearance configuration.

PFK pages are available for Allworx Verge IP Phone models 9312, 9308, and 9304.

Connect premise servers running Allworx System Software 8.5 and higher, or Connect Vx instances, automatically notify Verge phones when PFKs are added or removed, and then update that configuration on the Verge phones without action from the user or administrator. If Verge phones are the only phones connected to the server, it is not necessary to reboot the phones after making these changes.

To manage the PFKs:

1. Log in to the Allworx System Administration web page and navigate to **Phone Systems** > **Handsets**.
2. Locate the *SIP Handsets* pane and click the additional information arrow ►, if necessary.
3. Click **View Configuration** in the handset row. The configuration page appears for that handset.
4. Locate the *Programmable Function Keys* pane.
   a. For Verge 9312 phones click the radio button to select **Standard configuration (with PFK Pages)** or **Expander configuration (no PFK Pages)**.

      The configuration for Verge 9312 phones with physically attached 9318Ex Expanders are automatically set to **Expander configuration (no PFK Pages)** when the phone contacts the premise server or Connect Vx instance during the boot process.

      The Programmable Button Pages feature can be disabled on a 9312 phone that does not have any 9318Ex expanders by manually selecting the **Expander configuration (no PFK Pages)** radio button.

   b. Click **modify**. Notice the numbered row in the table corresponding to the individual phone PFK.

      Users can assign options to more than one column of PFKs. There are links for the left/right sets of PFK buttons for the Verge phones. For Verge 9312 IP phones that are in **Standard configuration (with PFK Pages)**, there are additional links for the left/right sets of PFK buttons for each of the five (5) pages.

      To enable Verge phone users to configure a single or multiple PFKs, click to select the **User Can Edit** check box corresponding to the PFK number.

5. (Optional) Click **Show PFK auto-assignment options** to manage all unused PFKs at once. Click one of the following options:

Option	Description
Assign BLFs to Not Used PFKs.	Commit selected Stations to all unused PFKs. Check the top check box to select or deselect all options at once. Click **Assign** to save the updates.
Reset all BLF PFKs to Not Used.	Update all the BLF PFKs to unused.
Assign Line Appearances to Not Used PFKs.	Commit selected Line Appearances to all unused PFKs. Check the top check box to select or deselect all options at once. Click **Assign** to save the updates.
Reset all Line Appearance PFKs to Not Used.	Update all the Line Appearance PFKs to unused.
Reset All the PFKs to Not Used.	Update all of the handset PFK definitions to unused.

6. Click the drop-down list in the *Type* column to select one of the following functions for each PFK.

PFK Type (function)	Description
ACD Appearance	Automatic Call Distribution Appearance - users log in and out of the ACD queues. When logged in, the user receives and answers calls from the ACD queues. Pressing the PFK toggles between temporarily stopping and starting ACD calls routing to the agent. ***Notes****:* • *Notification of the agent's Busy/No Answer State can be configured by selecting the check box and entering a value in the Audible Notification Interval field.* • *The Ring Type setting (default: **AUTO**) overrides any call route specific Ring Type choices unless the appearance programmable button Ring Type is set to **AUTO**, which uses the Ring Type selected in **View Call Routes.*** • *When **No Ring** is the selected Ring Type the phone flashes green and obey the auto-answering setting.* • *This feature is <u>not</u> available on the Connect 300 series servers.*
Bluetooth Hands-Free	Connect a *Bluetooth* enabled mobile device to the Verge 9312 phone. Pressing the Bluetooth Hands-Free programmable button transitions the call between the connected device and the handset or speaker phone. If there is no active call, users can press to connect to or disconnect from a mobile device. ***Note****: This feature is only available on the Verge 9312 IP phone.*

Continued

<table>
<tr><th>PFK Type (function)</th><th>Description</th></tr>
<tr><td><i>Busy Lamp Field (BLF)</i></td><td>Monitor and dial another specified phone when setting up the BLF function. When pressing the PFK, the behavior of this function depends upon the station <i>Mode</i> selection.
<table>
<tr><td>PBX Behavior</td><td>The phone dials the designated extension.</td></tr>
<tr><td>Key System Behavior</td><td>The phone places an intercom connection to the designated phone.</td></tr>
</table>
<b><i>Note:</i></b> <i>Softphone and Reach handsets are not included in the choice list for BLF PFKs.</i>
See“CreatingandUsingHandsetPreferenceGroups”onpage 120tosetstationMode.</td></tr>
<tr><td><i>Call Appearance</i></td><td>Map to available handset Call Appearances to place or receive calls.
• Supports using each Call Appearance for call routing and for managing calls independently and concurrently on the same phone.
• Mapping more than one PFK to the same Call Appearance supports multiple active calls to that Call Appearance at the same time. The Call Appearance does not display as busy to the call route until all the PFKs defined for that Call Appearance are in use. This is similar to call waiting except the system uses the PFKs to alert and select a new call.
<b>Example of the Busy Receptionist</b>:
• Requirements: A receptionist gets many phone calls each hour. She wants to answer each call while minimizing the possibility of any caller getting a busy signal.
• Phone Configuration: There is one Call Appearance defined on the phone set up with 8 of the phone PFKs mapping to the phone Call Appearance (remaining PFKs support other functions).
• Discussion:
  • The first call comes in, the phone rings and the Call Appearance PFK flashes.
  • A second call comes in. The phone rings and the second Call Appearance PFK flashes.
  • She presses the Hold button to place the first caller on hold and presses the second Call Appearance PFK to answer the second caller.
  • She continues to place callers on hold and answer new calls or switches to another Call Appearance PFK to continue/terminate calls.
<b><i>Note</i></b><i>: The Ring Type setting (default: <b>AUTO</b>) overrides any call route specific Ring Type choices unless the appearance programmable button Ring Type is set to <b>AUTO,</b> which uses the selected Ring Type in <b>View Call Routes</b>.</i></td></tr>
</table>

Continued

<table>
<tr><th>PFK Type (function)</th><th colspan="2">Description</th></tr>
<tr><td rowspan="5"><em>Call Supervision</em></td><td colspan="2">Enable supervisors to dial in and monitor calls for designated handsets in three modes. See “Routing Calls to a Call Queue” on page 60 for more information.</td></tr>
<tr><td>Barge in</td><td>After connecting the call, both participants in the call hear the supervisor. The supervisor can transition to silent monitoring by pressing the phone Mute button.</td></tr>
<tr><td>Whisper</td><td>(Available only when the receiving handset is a 9202E or 9204/9204G series, or a Verge series handset) – Only the user hears sounds from the supervising phone, not the other participant. The MUTE button controls audio going to the user. The supervisor cannot initiate two-way communications with the other participant.</td></tr>
<tr><td>Silent Monitor</td><td>Neither party in the call hear the supervisor. The Mute button on the supervisor handset lights red. The supervisor can speak to the participants of the monitored call at any time by pressing (disabling) the Mute button.</td></tr>
<tr><td colspan="2"><strong><em>Note:</em></strong> <em>Only the 9202E, 9204/9204G, Verge phones, and Interact Softphone handset can be supervised when being recorded or in a 3-way conference.</em></td></tr>
<tr><td><em>Contact</em></td><td colspan="2">Monitor, dial, or transfer a call another specified user. On Verge phones, the Contact PFK provides rolled-up Allworx user status and presence status. See “Contacts” on page 387 for more information.
<strong><em>Notes:</em></strong>
• <em>The Contact PFK for Allworx users does not provide user status or presence status on 91xx/92xx phones. To monitor the phone status, use a BLF PFK instead or connect a Verge phone to a Connect server.</em>
• <em>Each Allworx user can add a contact image associated with their contact information using the Reach application (with or without a handset license) or the Interact Professional application.</em></td></tr>
<tr><td><em>Emergency Alert</em></td><td colspan="2">Receive audible and visual alerts when any local or remote handset on the system makes an emergency call. See “Email Notifications” on page 88 for more information.
<strong><em>Note:</em></strong> <em>Emergency alert notifications are not generated for calls to 988 (National Suicide Prevention Lifeline).</em></td></tr>
</table>

Continued

PFK Type (function)	Description
Function	Allworx phones provide a set of functions that include some or all of the following: **Centrex Flash** — Provide an analog hook flash signal to the CO (when connected) to perform flash-related actions such as call transfer. Allworx users may configure this programmable button. This option is not available with the Connect Vx service. **DND** — Toggle the phone status to Do Not Disturb. Each Allworx user can assign a DND programmable button on the Verge phone. **Headset** — Turn the Headset on and off. If the handset is off-hook with a headset plugged-in, this PFK toggles the audio between the headset and the handset. ***Note:*** *If using an undefined Headset PFK, the speaker button operates the headset*. **Network Profile** — Select to define the network set up – how the server communicates with the phone. **Park** — Place the active call on a system-wide hold. If there are parked calls, the programmable button displays Parked Calls. Press to retrieve a parked call. Allworx users may configure this programmable button. **Personal Speed Dial** — Available for the 92xx IP phone series to automatically dial an extension or PBX function. **Redial** — Calls the last-dialed outbound call placed from the phone, the Interact application, or the Reach Remote Control application. Unless the Allworx Server Administrator enables the Line Appearance(s) Use Dial Plan phone option setting in the Handset Preference Group, the system only redials Call Appearance-dialed calls. Allworx users may configure this programmable button. ***Note:*** *The Verge 9304 IP Phone does not support the Reach Remote Control or Call Handoff features* **Release** — Ends the current call, but keeps the appearance active and the dial tone is heard. Allworx users may configure this programmable button. ***Note:*** *The function options available vary based on the phone model.*
Hot Desk	Log in to shared phones, receive calls, and place calls using the caller ID. Allworx users may configure this programmable button. • Users can initiate the login using a Hot Desk PFK (the PFK is solid red but goes off after a user logs in) or using the phone Config menu and selecting the Hot Desk Login option. • The Hot Desk PFK and all other PFKs remain as originally configured for the phone; configured PFKs do not change when a new user logs in. Allworx systems with Connect servers load the Personal Contacts after logging in. *Continued*

PFK Type (function)	**Description**
Line Appearance	Monitor the status of an outside line, answers incoming calls on that line, and selects the line for outbound calls. When setting up this PFK the user specifies the line. **To enable outside lines available for selection:** 1. Navigate to **Phone System** > **Outside Lines** and go to the *Analog (CO) Lines* pane. 2. Select the Analog (CO) Line, and click **Modify**. 3. Go to the *Outside Line* pane, and check the **Enable Line Appearance** check box. 4. Click **Update** to return to the *Outside Lines* page. **To define the Line Appearance:** 1. Click **define**. 2. Select the *Outside Line* to assign to the PFK from the drop-down list. 3. Select the *Ring Type* from the drop-down list. In addition to 6 custom ring types, selections for this setting include **No Ring**, **Single Ring**, **Double Ring**, and **Silent**. ***Notes***: • *This Ring Type setting (default = **Single Ring**) overrides any call-route-specific Ring Type choices unless the appearance programmable button Ring Type is set to **AUTO**, which uses the Ring Type selected in **View Call Routes**.* • *When the Ring Type is set to Silent, the phone flashes green and obeys the auto-answering setting.* • *When the Ring Type is set to No Ring, the phone flashes red and ignores the auto-answering setting.* **Unique Allworx Functionality:** an enhanced key-system capability relative to SIP devices and T1 Lines. Any SIP proxy, SIP gateway, or T1 Line bearer channel made available as Line Appearance selections when enabled on the respective configuration pages. Through this, the Allworx system presents a common key-system use model to all external voice circuit facilities including VoIP trunks going to an ITSP. **Allworx Verge Phone users**: Cell Phone Dialing mode is not available on Line Appearance Calls.
Messages	Monitor the status of a designated handset Message Center Voicemail inbox. Press to access the inbox. The PFK LED lights red to indicate a new message in the monitored inbox. The Allworx administrator must specify the monitored inbox when setting up the PFK.
Not Used	No action. Select this choice to disable a previously defined PFK.

Continued

PFK Type (function)	Description
Park Monitor	Monitor phone calls assigned to a single parking orbit or multiple parking orbits. The LED lights when a call is waiting in one of the parking orbits. • If assigning only one parking orbit to the PFK and there is a call in the orbit, pressing the PFK retrieves the call. • If assigning multiple parking orbits to the PFK, pressing the PFK displays the listed parked calls in all of the assigned orbits. ***Notes:*** *When viewing parked calls using the Park Monitor PFK, the Allworx phones* ***do not****:* • *include Park to Extension calls in the list of displayed calls.* • *light the Park Monitor PFK, if the only call parked in a parking orbit monitored by the PFK is a Park to Extension call.* • *Remind the phone owner of the Park to Extension call that the phone parked in a parking orbit monitored by the Park Monitor PFK.* • *(Verge Phones only) Include in the label of a Park Monitor programmable button the existence of or the count of Park to Extension calls in orbits monitored by the Park Monitor programmable button.* • *Retrieve a Park to Extension call when pressing the Park Monitor programmable button. If the call in the orbit monitored by a single-orbit Park Monitor programmable button is a Park to Extension call, all button presses are ignored.*
Park to Extension	(Verge Phones only) Park and/or view calls parked to specific recipients on the Allworx system. The Allworx system automatically sets the notifications for the configured extension in the phone owner's contact settings. When defining an eligible recipient (extension) for the programmable button, the Allworx System Software only displays eligible recipients/extensions in the drop-down list. ***Note****: If a configured recipient extension is deleted or disabled after configuring the Park to Extension programmable button, the programmable button displays Invalid Contact in gray text and ceases to function. Allworx Administrators must manually delete or modify the button configuration to resolve the misconfiguration or to clear programmable button space.*
Push to Talk	Provide a one-way, walkie-talkie-like capability. The configured PFK accesses a specific handset. • The user speaks to the target handset user by holding the PFK down and speaking. • To respond, the user of the target handset must place a regular call back to the originator.
Queue Alarm	Map to one of the 10 Call Queues in the system. It notifies the user of the queue activity levels (number of calls in the queue and/or longest wait time). The administrator can configure the queue alarm to include an audible alarm with the queue status displayed on the phone LCD. The PFK alerts when there are no logged-in agents in the queue and the queue is set to force callers to leave the queue when no agents are logged in. ***Note****: This feature is not available on the Connect 300 series servers.*

Continued

<table>
<tr><th>PFK Type (function)</th><th>Description</th></tr>
<tr><td><em>Queue Appearance</em></td><td>Map to one of the 10 Call Queues in the system. It automatically monitors the status of a Call Queue and used to answer calls that are in the queue.Configuration settings:
<table>
<tr><td>Call Queue</td><td>Select one of the available Call Queues from the drop-down list.</td></tr>
<tr><td>Login to queue when phone reboots</td><td>Check the box to enable/disable automatic login after rebooting the phone.</td></tr>
<tr><td>Ring Type
(for more information, see “Ring Families and Ring Types” on page 94.</td><td>Select a unique ring type to distinguish calls to this PFK from other phone calls.
<ul>
<li>When set to <strong>No Ring</strong>, the Queue Appearance never rings. The agent uses the LED to monitor when there are calls in the queue. Press the PFK to service the next call in the queue.</li>
<li>Set to ring (Ring Type other than No Ring) enables the following fields, which control when the Queue Appearance rings:
<ul>
<li><em>Wait Period:</em> Enter a value (seconds) a call must be in a queue before the Queue Appearance starts to ring.</li>
<li><em>Number of Callers:</em> Enter a value (number of callers) that must be in a queue before the Queue Appearance starts to ring.</li>
<li><em>Wrap-up Time:</em> Enter a value (seconds) the agent has available after ending a call before the system makes the agent available to receive the next ACD queue call. Agents can dismiss/end the wrap up time from the handset.</li>
</ul></li>
<li>Meet the following conditions for a Queue Appearance to ring:
<ul>
<li>Log in to the station.</li>
<li>Queue Appearance is idle.</li>
<li>Reach the wait period of number of callers thresholds.</li>
<li>Agent is not in the Wrap-up Time.</li>
</ul></li>
</ul></td></tr>
</table>
<strong><em>Note</em></strong><em>: The Ring Type setting (default: Single Ring) overrides any call route specific Ring Type choices unless the appearance programmable button Ring Type is set to AUTO, which uses the selected Ring Type in </em><strong><em>View Call Routes</em></strong>.</td></tr>
<tr><td><em>Ring Group</em></td><td>Display the status of and enables answering a Ring Group call. When routing a call to a specified Ring Group, all phones ring with a PFK defined for that Ring Group. In addition, Allworx administrators can program an Allworx IP phone to display:
<ul>
<li>Multiple Ring Groups per phone to track more than one Ring Group.</li>
<li>Multiple occurrences of the same Ring Group. This enables a user to take more than one call at a time from the same Ring Group to avoid missing additional calls while attending to the current call.</li>
</ul>
<strong><em>Note</em></strong><em>: The Ring Type setting overrides any call route specific Ring Type choices unless the appearance programmable button Ring Type is set to AUTO, which uses the selected Ring Type in </em><strong><em>View Call Routes</em></strong>.

<em>Continued</em></td></tr>
</table>

PFK Type (function)	Description
Schedule	Display the mode (day or night) of the configured business schedule. • The LED is off for day mode and solid red for night mode. • To configure switching the current mode and greeting of the schedule, see “Schedules” on page 215 for more information.
Shared Appearance	Support handling a set of one or more PFKs by the system as a single appearance shared across multiple handsets. All handsets in the Shared Appearance have common access to calls and call operations within the group of handsets. • Selecting this PFK assigns consecutive PFKs, one for each Shared Call Appearance line. • If there are not enough consecutive PFKs available in a single column, the PFK assignment fails and an error message appears. • If the Shared Call Appearance PFK assignment would overwrite existing PFKs, the system displays an error message and enables canceling the operation. • Shared Call Appearance PFKs display consecutively on the PFK configuration page, the Allworx administrators can move the assignments to different PFKs limited only by the constraints within the particular handset model. ***Note**: The Ring Type setting (default: Single Ring) overrides any call route specific Ring Type choices unless the appearance programmable button Ring Type is set to AUTO, which uses the selected Ring Type in **View Call Routes**.*

The following table lists the default ring type setting for the PFK types.

PFK Type	Default Ring Type Settings
ACD Appearance	AUTO
Call Appearance	AUTO
Line Appearance	Single Ring
Queue Appearance	Single Ring
Ring Group	Single Ring
Shared Appearance	Single Ring

7. In the *Type* column click **change** to further characterize the feature. A drop-down list appears with selections based on the feature selected from the drop-down list (except *Emergency Alert*, *Hot Desk*, and *Not Used*). The table below describes the menu options for each feature.

Setting	Description
Audible Alarm	Check the box to hear the alarm from the phone speaker.
Call Appearance	Select an available user from the drop-down list.

Continued

Setting	Description
Call Queue	Select an available call queue from the drop-down list.
Call Supervision	Select the Call Supervision type. See "Call Supervision" on page 141 for more information.
Contact	Leave unassigned for the Allworx user to assign a Contact, or select a contact from the drop-down list.
Emergency Alert	Change the duration of the audible alarm. The default is 600 seconds, set to 0 to disable the alarm.
Function	Select the function to assign from the drop-down list. See "Function" on page 142 for more information.
Display Only	Check the box for the schedule to control the phone display.
Handset	Select an available handset from the drop-down list.
Messages	Select an available user from the drop-down list.
Outside Line	Select an available outside line from the drop-down list.
Monitored Orbits	Check the boxes of the Parking Orbits to monitor. Optional - select all or clear all to check to clear all check boxes, respectively.
Login to queue when phone reboots	Check to automatically log the phone into the call queue after each reboot.
Reminder Duration	Enter a time limit for the caller to be in the Parking Orbit before the phone rings again. Enter **0** to disable. ***Notes:*** • *If assigning only one parking orbit to the PFK, this setting is the number of seconds (10 to 100) that the parked call waits in the parking orbit before a reminder appears (and sounds) on this phone. The Allworx system only delivers the reminder to the phone that parked the call.* • *If assigning multiple parking orbits to the PFK, the Allworx system does not deliver a reminder.*
Ring Group	Select an available Ring Group to assign from the drop-down list.
Ring Type	See "Ring Families and Ring Types" on page 94 for more information on each option. • No Ring - phone does not ring. • Single Ring • Double Ring • Ring Type 1 • Ring Type 2 • Ring Type 3 • Ring Type 4 • Ring Type 5 • Ring Type 6 • AUTO - uses the defined ring type for the call route.
Schedule	Select an available schedule from the drop-down list.

Continued

Setting	Description
Shared Appearance	Select an available Shared Call Appearance from the drop-down list.
Wait Period	Specify the amount of time for callers to wait in the call queue before the phone rings.
Wrap-up Time	Specify the amount of time each agent can spend in wrap-up.

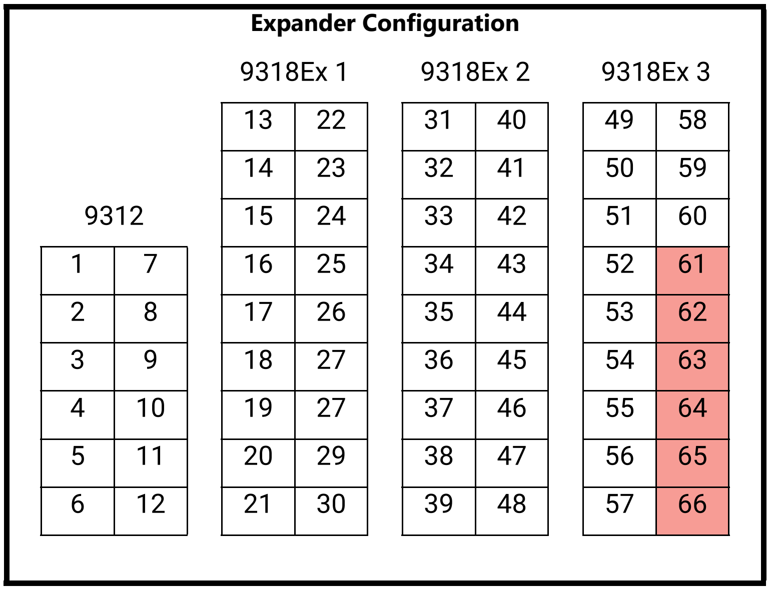
8. Locate the *User Can Edit* column. Click to select the check boxes of the PFKs that Allworx users can modify.
9. Click **Done** to save the change or **Cancel** to disregard the request. Repeat for each PFK, as necessary.
10. Use the *Location* column icons to adjust the order of the programmable function keys.

Icon	Action	Description
↑	Move up	Shift the current PFK definition up one position.
↓	Move Down	Shift the current PFK definition down one position.
☒	Delete	Remove the PFK and shifts all PFK definitions below it up by one location. Because of the shift, PFK definition #1 in each bank shifts “up” to the bottom of the bank to the left. The last PFK definition on the station becomes Not Used (last bank).
☰	Insert	Shift all PFK definitions below it down by one position. Because of the shift, PFK definition 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 phone or expander was in use, it “drops off” the end of the list and is no longer configured.

11. Click **Update** to save the changes or **Cancel** to disregard the request. Premise servers running Allworx System Software 8.5 or higher and Connect Vx instances automatically notify Verge phones when PFKs are added or removed, and then update that configuration without rebooting the phones.

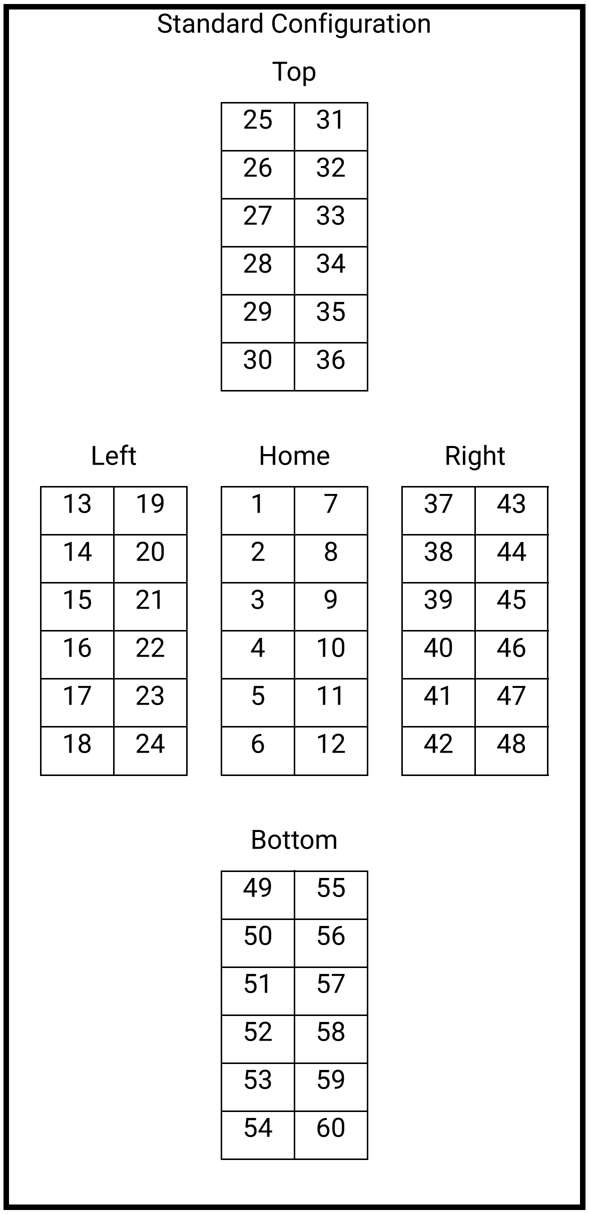
PFK Mapping When Switching PFK Pages Modes

The premise server and Connect Vx instances automatically maps the PFKs between pages and 9318Ex expanders when changing the mode for a Verge 9312 IP phone. This diagram shows the numbering for the PFKs and their locations in each configuration.



Expander Configuration

9312		9318Ex 1		9318Ex 2		9318Ex 3	
		13	22	31	40	49	58
		14	23	32	41	50	59
		15	24	33	42	51	60
1	7	16	25	34	43	52	61
2	8	17	26	35	44	53	62
3	9	18	27	36	45	54	63
4	10	19	27	37	46	55	64
5	11	20	29	38	47	56	65
6	12	21	30	39	48	57	66



Standard Configuration

Top

25	31
26	32
27	33
28	34
29	35
30	36

Left		Home		Right	
13	19	1	7	37	43
14	20	2	8	38	44
15	21	3	9	39	45
16	22	4	10	40	46
17	23	5	11	41	47
18	24	6	12	42	48

Bottom

49	55
50	56
51	57
52	58
53	59
54	60

As the Programmable Button Pages feature provides only 60 PFKs on a Verge 9312 IP phone, the higher-numbered PFKs (i.e., 61 through 66, highlighted in red) in **Expander configuration (no PFK Pages)** will be discarded when the mode is switched to **Standard configuration (with PFK Pages)**. In addition, if buttons 61 through 66 contained any Shared Call Appearance PFKs then all of the PFKs for the associated Shared Call Appearance(s) will be removed, even if those remaining PFKs are programmed on lower-numbered buttons.

PFK Mapping During a 9224 Phone Replacement With a 9312 in Standard Configuration

The premise server and Connect Vx instances automatically maps the PFKs from one device to the other when replacing a 9224 IP phone with a Verge 9312 IP phone in **Standard configuration (with PFK Pages)**. This diagram shows the numbering for the PFKs and their locations on each phone or Tx unit.

9224 w/ three Tx 92/24 expanders

9224		Tx 1		Tx 2		Tx 3	
1	13	25	37	49	61	73	85
2	14	26	38	50	62	74	86
3	15	27	39	51	63	75	87
4	16	28	40	52	64	76	88
5	17	29	41	53	65	77	89
6	18	30	42	54	66	78	90
7	19	31	43	55	67	79	91
8	20	32	44	56	68	80	92
9	21	33	45	57	69	81	93
10	22	34	46	58	70	82	94
11	23	35	47	59	71	83	95
12	24	36	48	60	72	84	96

Standard Configuration

Top

25	31
26	32
27	33
28	34
29	35
30	36

Left		Home		Right	
13	19	1	7	37	43
14	20	2	8	38	44
15	21	3	9	39	45
16	22	4	10	40	46
17	23	5	11	41	47
18	24	6	12	42	48

Bottom

49	55
50	56
51	57
52	58
53	59
54	60

As the Programmable Button Pages feature provides only 60 PFKs on a Verge 9312 IP phone, the higher-numbered buttons (i.e., 61 through 96, highlighted in red) on Tx 2 and Tx 3 will be discarded when the 9224 phone is replaced. In addition, if buttons 61 through 96 contained any Shared Call Appearance PFKs then all of the PFKs for the associated Shared Call Appearance(s) will be removed, even if those remaining PFKs are programmed on lower-numbered buttons.

To manage the Interact Appearance configuration for Allworx 92xx and 91xx series phones:

The Call Appearance on the Allworx phone is for originating and receiving calls and PFKs beyond the physical keys that are available on the actual phone.

- Call Appearance
- Shared Call Appearances
- Line Appearance
- Queue Appearance
- Ring Groups (formerly known as Call Monitors)

When routing calls from the Call Appearance to applications within the Allworx system (e.g., Auto Attendants, Call Queues, or Conference Center), the premise server and Connect Vx instance use or override the call appearance language, depending on the application language setting. The handset rings when any of these appearances ring.

1. Log in to the Allworx System Administration web page and navigate to **Phone System** > **Handsets**.
2. Locate the user name, and click **View** Configuration on the specific handset.
3. Locate the *Interact Appearances* pane, and click **modify** to open the configuration page.
4. Check the boxes to enable the desired Interact Appearances.
5. For each appearance type enabled, click **change** to adjust the appearance settings.

   Note: *See “Ring Families and Ring Types” on page 94 for more information about steps 5 and 6.*
6. Click **Update** to save the changes or **Cancel** to ignore the request.

12.5 Managing Programmable Functions for Interact Softphone

Manage programmable functions by defining and assigning a function to an Allworx Interact Softphone handset to provide functionality for the user. Connect premise servers and Connect Vx instances automatically notify Interact Softphone handsets when programmable functions are added or removed, and when there are changes to the configuration of existing programmable functions.

1. Log in to the Allworx System Administration web page and navigate to **Phone System** > **Handsets**.
2. Locate the Interact Softphone user name, and click **View** Configuration for the specific Interact Softphone handset.
3. Locate the *Programmable Functions* pane and click **modify**.
4. Click **Add a Function**.

5. Select one of the following functions from the drop-down list.

    - ACD Appearance
    - Call Appearance
    - Emergency Alert
    - Line Appearance
    - Park to Extension
    - Queue Alarm
    - Queue Appearance
    - Ring Group
    - Shared Appearance

6. Enter the required information in the *Function* pop-up fields that appear in the gray box next to the drop-down list.
7. Continue to add functions until the handset has the needed functionality.
8. Click **Update** to assign those functions to the Interact Softphone handset.

Note: *Handset Templates can be used to easily and consistently assign groups of programmable functions to Interact Softphone handsets. For more information see “Creating and Using Handset Templates” on page 134.*

12.6 Managing Generic SIP Handset Settings

This section describes managing the available settings for generic SIP handsets connected to the Allworx server.

Notes:

- *On a Connect Vx instance, all handsets are connected remotely. For more information, see “Manually Adding a Generic SIP Handset” on page 114.*
- *If installing Generic SIP handsets on the premise server or Connect Vx instance, Internal Dial Plan changes can modify system software configuration so that Generic SIP phones no longer register.*

Registered phones display on the *Handsets* page with an expiration date/time to indicate a registered phone.

Note: *Allworx Generic SIP feature keys provide licenses to enable Generic SIP handsets. Allworx administrators can add a small number of handsets without a key (4 on the Allworx Connect 300 series servers, 6 on the Allworx Connect 500 series servers, and 12 on the Allworx Connect 731 servers). No licenses are automatically provided with on Connect Vx instances.*

- *Available feature keys provide 1, 5, or 10 licenses each.*
- *For larger numbers of Generic SIP handsets, install multiple feature keys.*

To manage a Generic SIP Handset:

1. Log in to the Allworx System Administration web page and navigate to **Phone System** > **Handsets** > **SIP Handsets**.
2. Click to select the *Generic SIP Handsets* check box. Only the Generic SIP Handsets display.

3. Locate the phone and go to the *Action* column. Click one of the actions listed in the following table and update the options as needed:

Action	Options Available
Modify	Edits can be made to the following fields:

Handset	
Owner	Select an option from the drop-down list.
Internal Caller ID Name	Enter the name to display on the caller ID.
Internal Caller ID Number	Select an option from the drop-down list.
External Caller ID Name	Enter up to 47 characters of the name to display.
External Caller ID Number	Enter up to 24 digits to display.
Description	Enter a meaningful name.
Display in Interact	Check the box to display the extension and phone status. If the box is unchecked, neither the extension nor status display.
Dialing Privileges Group	Select a dialing privileges group from the drop-down list.
Default Prompt Language	Select a language option from the drop-down list. • **Primary Language -** Use the language designated as the default language. • **Secondary Language** - Use the alternate language.

SIP Registration	
Login ID	Create a new Login ID by entering the new ID in the field.
Password **make new password**	Select the password complexity by clicking the password requirements buttons. The Allworx server generates a new password upon request based on the complexity rules, and displays the new password when configuring the Generic SIP device. For existing Generic SIP devices, the system maintains the current password until the Allworx administrator requests a new password.
SIP Trust Level	Click to select the appropriate radio buttons. For optimum protection against fraudulent VoIP calls, select *Authenticate Registrations and Invites*. This protects against fraudulent calls being placed from forged SIP INVITES for already registered phones. If the Generic SIP device cannot support Authenticating SIP Invites, you must configure your network to prevent a fraudulent SIP INVITE from being received by the Allworx server.

Handset Features	
Hold Music Selection	Select the Hold Music to use from the drop-down menu.

Continued

Action	Options Available	
Modify *(continued)*		
	This phone is behind a NAT/firewall and needs traversal assistance	Check the box to activate traversal assistance. **Note:** *If the user is experiencing any connection problems between the handset and the Allworx server or Connect Vx instance (SIP, RTP, SIP registration or anything else SIP-related), selecting this check box may help correct the issue.*
	Can Place Calls	Click to select the check box to enable the extension to place external calls.
	Can Receive Calls	Click to select the check box for the extension to receive external calls.
	Advanced Settings	
	Enable Early Media	Click to select the check box - allow audio from 183 Session Progress responses.
	Supports Symmetric Response Routing	Click to select the check box - RFC 3581 - include “rport” in requests.
	Click **Update** to save the new settings.	
Delete	Removes the handset from the Allworx system. Click **Delete** in the pop-up window to confirm.	
Ring	Creates audible ringing from the handset.	

* Login ID and Password are the credentials for the SIP handset to authenticate with the Allworx premise server or Connect Vx instance.

- If not specifying a Login ID, the server generates one when creating the handset and generates a handset User ID automatically.
- Do not use the same Login ID on multiple phones.

To review the configuration:

1. Login to the Allworx System Administration web page and navigate to **Phone System** > **Handsets** > **SIP Handsets**. Click the additional information arrow ▶, if necessary.
2. Review the installed Generic SIP phone User IDs.
3. Determine if the registration configuration for each Generic SIP phone is the same or different from the current User ID on the System Administration web page *Handsets* page. If there is a difference, modify the on-phone configuration to match the new User ID.

Note: *For generic SIP handsets: unregistered handsets display the registration information in gray italic font while registered handsets display the registration information in the standard black font. Additionally, the last handset reboot date/time and the last handset SIP registration time display for each handset.*

12.7 Managing Analog Handset Configuration

To manage the analog phone settings:

1. Log in to the Allworx System Administration web page and navigate to **Phone System** > **Handsets**.
2. Locate the *Analog Handsets* pane. Click the additional information arrow ▶, if necessary
3. Click one of the following actions:

Action	Description
Modify	Change the current analog handset settings. See the Analog Handset Settings table for more information.
Delete	Remove the analog handset connection from the server. Click **Delete** to confirm the change.
Ring	Test the analog handset connection.

4. Click **Update** to save the changes or **Cancel** to ignore the request.

Analog Handset Settings

Handset	
Port:	This is the port to which the handset is connected. The field is automatically filled in and cannot be modified.
Owner	Select the handset owner from the drop-down list. This list includes both system and user extension owners.
Extension (optional)	If a system extension is entered, the extension is created, if necessary, and the phone is added to the call route of that extension (whether it was new or existing).
Internal Caller ID Name	Automatically populates from Owner selection. Update as necessary. ***Note:*** *The contact information based on the caller ID number (applies to Verge phones only) overrides this setting.*
Internal Caller ID Number	Select an option from the drop-down list.
External Caller ID Number	Optional. Enter information as necessary.
External Caller ID Name	Optional. Enter information as necessary.
Description	Automatically populates from Owner selection. Update as necessary.
Dialing Privileges Group	Select the dialing privileges group to assign to the handset from the drop-down list.
Default Prompt Language	Select the language in which prompts will be played from the drop-down list. Selections are **Primary Language** or **Secondary Language**.

Continued

Handset Features	
Hold Music Selection	From the drop-down list select the source for music to be played when a call is on hold. • **Line-In** • **None** • **moh_supplied.snd** • **moh_supplied_louder.snd**
Can Place Calls	Check the box to allow the handset to place calls.
Can Receive Calls	Check the box to allow the handset to receive calls.
Second Call Handling	Identifies how to manage a second incoming call. • **Busy** • **Call Waiting** • **Not Busy**
Message Waiting Stutter Dialtone	Check the box to enable. When enabled a stutter dial tone is played instead of the normal dial tone to indicate that the owner of the phone has new messages in the message center. A stutter dial tone sounds as if it is being rapidly interrupted or chopped. Use with analog phones that do not have a message waiting light.
Message Waiting Light	Check the box to enable a light to indicate that a message is waiting to be picked up. ***Note:*** *When enabled, select the type of caller ID (Type I or Type II) under the Caller ID Display check box.*
Caller ID Display	Check the box to allow a caller ID to display on the handset. ***Note:*** *When enabled, select the type of caller ID (Type I or Type II) under the Caller ID Display check box.* • **Caller ID Type I SDMF** - check the box to enable. • **Caller ID Type II MDMF** - check the box to enable.
Auto Off-Hook Dialing	Enter the digits for the Allworx phone to automatically dial every time the user takes the phone off hook.
Auto Answer DTMF String	Enter the DTMF digits sent when the user answers a call. The system sends these digits to the FXS device as soon as it answers the call. The following characters are available for use:

DTMF Digits	Timing Controls	Variables
• 0 – 9 • A – D • * • #	• 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	• $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

FAX machine connected to this port	Click to select this check box if a FAX machine is connected. This selection forces a negotiation to the G.711 codec for calls using SIP trunks.

12.8 Accessing the Allworx Phone Administration Web Page

The web administration page is used to set and view the configuration information for Allworx handsets. From this interface you can modify the handset configuration and personal speed dials, and view information such as event logs, call history, and phone configuration parameters. The phone web administration page has the same look and feel as the Allworx System Administration web page, but the password used to access the phone web administration page is NOT the same. The *Phone Administration Password* can be found by navigating to **Servers** > **VoIP** on the Allworx System Administration web page for the appropriate Connect premise server or Connect Vx instance.

Notes:

- *The administrative PC must be able to reach the phone IP address. Therefore, it is not possible to access the phone administration web page unless the administrative PC and the phone are on the same network, or the admin PC has direct access (via VPN) to the phone network.*
- *The Verge Phone series supports secure HTTP when logging in to the phone administration web page.*

To access the phone administration web page of an Allworx handset:

Note: *To learn the web page password, see “VoIP Server” on page 295 for more information.*

6. Access the administrative web page of an Allworx handset using one of the following options.

Option	Description
Access via the Allworx System Administration web page	1. Open the Allworx System Administration web page in a browser window. 2. Navigate to **Phone System** > **Handsets**. 3. Click the link that is the phone’s IP address. ***Note:*** *For Connect Vx, the links to the phones provided on the Handsets page may not be accurate (e.g., phones that are behind a NAT/firewall). Use the second option if this is the case.*
Direct Access Using the Handset IP Address	1. Enter the IP address of the handset in a web browser. 2. Find this IP address using the handset soft keys: **CONFIG** > **Current Status** > **Info.**

Click here to return to the Installing and Configuring Allworx Premise Servers or Configuring Connect Vx Instances .

Chapter 13 Languages

The *Languages* page supports US English and one secondary language for audio prompts. The language configuration supports playing prompts in one of two languages. Callers switch between the two languages by pressing ##.

Note: *To change the handset display to Castilian Spanish or Canadian French, see “Handset Preference Group Settings” on page 122.*

Prerequisites	
Access Permissions	Allworx Server Administrator Allworx System Administrator Phone Administrator role*
Feature Key Required	Dual Language Support
*Not all features on the Languages page are available to Phone Administrators.	

Important information about dual languages:

- Factory-installed primary language is US English.
- Additional languages: Install a Language Pack (available from the Allworx Portal) and select it as either the primary or secondary language.
- Assign a language to the points of origin for new calls (Outside Lines, Users, and handset Call Appearances). The default language is **Primary**.
- Configure the prompts in the following Allworx system call features to use the language of the call point of origin or override it with a specific language:

  - Auto Attendants*
  - Call Queues*
  - Leaving Voicemail
  - Phone Features (Call Park, Call Forward, Do Not Disturb extensions, Displays)

    Note: *Calls cannot be forwarded to phones at different sites within a Multi-Site network.*
  - Conference Center*
  - Follow Me*
  - Message Center*

  * If configured, callers can toggle between languages by pressing ##. Example: An Auto Attendant uses Spanish prompts. The prompt speaks in English “To switch to English, press ##.”

  Note: *Conference Center is not available when using the Connect Vx service.*

- Record and save custom greetings for Auto Attendants and Call Queues, with a length limit of 15 minutes per greeting, separately for the primary and secondary languages. The custom recordings are not a part of the previously downloaded language pack. Therefore, if the primary or secondary language changes, the premise server or Connect Vx instance continues to use the original primary custom recordings. To manage the custom recordings, see “Custom Recordings” on page 339 for more information.
- Incoming calls to the Allworx system from remote Allworx premise server or Connect Vx instance retain the language used by the remote system (navigate to the System Administration web page

settings on the **Phone System** > **Languages** page, and the *Default Prompt Language* setting on the phone call appearance), unless overridden by language settings on the local server.

Note: *All Allworx premise server or Connect Vx instance connected together in a multi-site network must run the same release of software and use the same languages.*

13.1 Installing the Language Pack

The Allworx system default language is US English. After adding the Dual Language Support feature key to the system, the Allworx administrator can install one additional language.

To install an additional language:

1. Download the language pack from the *System Support Files* section on the *Software* download page of the Allworx Portal (allworxportal.com).

2. Unzip the downloaded file and copy the language pack (.alp) file onto the PC.

3. Log in to the Allworx System Administration web page and navigate to **Phone System** > **Languages**.

4. Locate the *Language Pack Installation and Removal* pane and click one of the following options:

Option	Description
Remove	Click to delete the currently installed language pack. Be sure this is the language file to delete - there is no further action after clicking this button.
Choose File	Select the appropriate language pack to install. To install the language pack: 1. Navigate to the location of the language file on the PC, select the **.alp** file and click **Open**. 2. Click **Install**. After the installation is complete, locate the *Server Language Configuration* and click **modify**. 3. Select the new language for the Primary or Secondary language. 4. Select a second available language (e.g. US English) as the Primary or Secondary language. 5. Click **Update** to save the change or **Cancel** to disregard the request.

5. Restart the premise server or Connect Vx instance to have the changes take effect.

13.2 Managing the Language Settings

Features such as Auto Attendants and Call Queues within the Allworx system play audio prompts. To configure outside lines, see “Outside Lines” on page 175. To configure specific handsets, see “Handsets” on page 103.

To control the language behavior of the prompts:

1. Log in to the Allworx System Administration web page, and navigate to **Phone System** > **Languages**. Locate the *Call Application Language Settings* pane.

2. Click **modify**. Locate the feature line and change the settings.

<table>
<tr><th>Setting</th><th>Description</th></tr>
<tr><td><i>Answer Language</i></td><td>Prompts play in the selected language. Select one of the following options from the drop-down list.
<table>
<tr><td>Automatic</td><td>Prompts play in the current language. For calls from an outside line or Call Appearance, the system uses the call origin default language. If calls come from another application (e.g. the call came into a queue from an Auto Attendant), the system uses the language from the previous application (e.g. Auto Attendant).</td></tr>
<tr><td>Primary Language</td><td>Overrides the current language.</td></tr>
<tr><td>Secondary Language</td><td>Overrides the call current language, if installed.</td></tr>
</table></td></tr>
<tr><td><i>Allow Language Change</i></td><td>Enables callers to switch languages when the call reaches an Allworx server feature. To switch languages, callers must press ##. To enable callers to change language for the preferred application, check the Display Language Change box.</td></tr>
<tr><td><i>Language Change Prompt</i></td><td>Change the prompt language when reaching an Allworx premise server or Connect Vx instance feature (except for when leaving a Voicemail message or when using phone features). Select one of the following options from the drop-down list:
<table>
<tr><td><b>Play if needed</b></td><td>The prompt does not play if the caller has already had a chance to change languages in a prior application. For example: if a Call Queue Language Change Prompt setting is <b>Play if needed</b>, and directs a routed call to the queue from an outside line, the language change prompt plays. If the call came through an Auto Attendant that enables language changing, the prompt does not play because the caller already had a chance to select a preferred language.</td></tr>
<tr><td><b>Always play</b></td><td>Every time a call reaches the application, in addition to the prompts normally played, the prompt plays to change the language (“To switch to English, press ##”).</td></tr>
<tr><td><b>Never play</b></td><td>The prompt to change the language does not play. Used when incorporating the prompt to change language to a custom greeting or message. Unavailable for Follow-Me-Anywhere prompts.</td></tr>
</table></td></tr>
</table>

Configuration Examples

Example 1: A company has clients that speak English or Spanish. English-speaking clients use one phone number while Spanish-speaking clients use another phone number. The premise server or Connect Vx instance configuration is:

Configuration	Setup
Primary Language	English
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
Language Change	Enabled
Language Change Prompt	Always play

Results:

- English-speaking clients call the English phone number (CO Line 1) and route to Auto Attendant 1 to hear English prompts as well as a prompt to switch to Spanish. Callers dial the appropriate extension. All additional prompts are in English, i.e., leave a Voicemail or the Follow-Me-Anywhere prompt to record.
- Spanish-speaking clients call the Spanish phone number (CO Line 2) and route to Auto Attendant 1 hearing Spanish prompts as well as a prompt to switch to English. Callers dial the appropriate extension. All additional prompts are in Spanish, i.e., leave a Voicemail or the Follow-Me-Anywhere prompt to record.

Example 2: A company has a Customer Support operation; the technicians speak English or French Canadian. The company has one incoming line for Customer Support calls. All callers are directed to the same Auto Attendant.

- English-speaking callers dial a support queue shortcut serviced by English-speaking technicians.
- French Canadian-speaking callers switch to a second Auto Attendant, and then dial a queue shortcut serviced by French Canadian-speaking technicians. The premise server or Connect Vx instance configuration is:

Configuration	Setup	Configuration	Setup
Primary Language	English		
Secondary Language	French Canadian		

Continued

Configuration	Setup	Configuration	Setup
T1 Language (all lines)	English		
Auto Attendant 1		**Auto Attendant 2**	
Answer Language	Primary	Answer Language	Secondary
Language Change	Disabled	Language Change	Disabled
Shortcuts	• Dial 1 for x4302 (Auto Attendant 2) • Dial 2 for x4401 (Call Queue 1)	Shortcut	• Dial 1 for x4402 (Call Queue 2)
Custom Messages	• "For French Canadian, press 1" (recorded in French Canadian) • "To speak with Customer Support, press 2" (recorded in English)	Custom Message	• "To speak with Customer Support, press 1" (recorded in French Canadian).
Call Queue 1		**Call Queue 2**	
Answer Language	Primary	Answer Language	Secondary
Language Change	Disabled	Language Change	Disabled

Results:

The premise server or Connect Vx instance directs all callers to Auto Attendant 1 to:

Option	Result
Hear an English greeting	Prompts to: • Press 1 for French Canadian. • Press 2 for Customer Support.
Callers press 1	Enter Auto Attendant 2 • Hear the full greeting and prompts in French Canadian. • Prompt to press 1 for Customer Support. • Enter Queue 2 to hear the greeting and status messages in French Canadian. A French Canadian-speaking technician services the call.
Callers press 2	• Enter Queue 1. • Hear the greeting and status messages in English. An English-speaking technician services the call.

Click here to return to the Installing and Configuring Allworx Premise Servers or Configuring Connect Vx Instances .

Chapter 14 Message Aliases

Prerequisites	
Access Permissions	Allworx Server Administrator Allworx System Administrator Phone Administrator role
Feature Key Required	No

Message Aliases allow Allworx administrators to add user or group email addresses on the Allworx premise server or Connect Vx instance.

The Allworx System Software supports unified messaging which allows:

- Combining user Voicemail and email messages into one inbox.
- Forwarding messages to another email account or POP to an email client.
- Using a phone to listen, delete, or forward Voicemail messages – when deleting a Voicemail message via a phone the server inbox deletes the message.
- Deleting unified messages from the server due to a POP or mail forward; the server also deletes the Voicemail, and it is no longer accessible by phone.

14.1 Accessing Voicemail and Email Messages

To access Voicemail and Email messages from the premise server or Connect Vx instance:

- Forward messages to another email account.
- Use a POP3 or IMAP email client to transfer the messages to a PC. IMAP is only available after installing a Mobile VM feature key. See “Email” on page 283 for more information.

14.2 Managing Message Aliases

Note: *If saving a copy of each message on the premise server or Connect Vx instance, users can exceed the server inbox storage space quota. To avoid this, users should manage old messages in the Message Center. To delete saved messages for individual users, see “Deleting User Messages, Recordings, Contacts, or Contact Images” on page 230 for more information.*

Use the Message Aliases feature to forward any incoming message (Voicemail or Email) for a user to other users or to an external (non-Allworx server) email account.

1. Log in to the Allworx System Administration web page and navigate to **Phone System** > **Message Aliases**.
2. Determine the type of Message Alias.
   - *User Message Alias* – Message sent to a specific user that can include multiple addresses. When selecting an extension, the alias is available in the Visual and Audio Message Centers as a recipient of new Voicemails.

- *Group Message Alias* – A distribution list that is available for selection in the Visual and Audio Message Centers as a recipient of new Voicemails.

3. Click one of the following links in the *User Message Aliases* or *Group Message Aliases* pane.

<table>
<tr><th>Link</th><th>Description</th></tr>
<tr><td><b>add new alias</b></td><td><b>Add a new message alias to the <i>premise server or Connect Vx instance</i>.</b>
1. Enter the required information in the first text field.
<table>
<tr><td><b><i>User Message Alias</i></b></td><td><b>From the drop-down list select the user.</b></td></tr>
<tr><td><b><i>Group Message Aliases</i></b></td><td><b>Enter the name for the group.</b></td></tr>
</table>
2. (optional) In the <i>Message Center Alias</i> field click to select a number for the Message Center alias from the drop-down list. The selected number is available in the Message Center as a recipient of new Voicemail messages.
<b><i>Note:</i></b> <i>Do not enter Message Center Alias numbers in the Addresses field. These numbers should only be used interactively when addressing new Voicemails in the Audio and Visual Message Centers.</i>
3. Click to select the <i>Keep copy on server</i> check box to have the premise server or Connect Vx instance leave a copy of the message in the user’s mailbox, in addition to sending it to the <i>Addresses</i> for the alias.
4. In the <i>Addresses</i> field enter the username(s) or external email address(es). Press the <b>Tab</b> key to add lines for multiple addresses.
5. Click <b>Add</b> to save the new message alias.</td></tr>
<tr><td><b>Modify</b></td><td><b>Update an existing message alias.</b>
1. In the <i>Message Center Alias</i> field click to select a number for the Message Center alias from the drop-down list. The selected number is available in the Message Center as a recipient of new Voicemail messages.
<b><i>Note:</i></b> <i>Do not enter Message Center Alias numbers in the Addresses field. These numbers should only be used interactively when addressing new Voicemails in the Audio and Visual Message Centers.</i>
2. Check the <i>Keep copy on server</i> to have the premise server or Connect Vx instance leave a copy of the message in the user’s mailbox in addition to sending it to the <i>Addresses</i> for the alias.
3. Locate the <i>Addresses</i> field and enter the username(s) or external email address(es). Click the <b>Tab</b> key to add lines for multiple addresses.
<b><i>Note:</i></b> <i>Do not enter Message Center Alias numbers in the Addresses field. These numbers should only be used interactively when addressing new Voicemails in the Audio and Visual Message Centers.</i>
4. Click <b>Update</b> to save the changes to the message alias.</td></tr>
</table>

Continued

Link	Description
Delete	Remove the message alias from the premise server or Connect Vx instance. 1. Locate the user in the *Users* list and click **Delete** in the *Action* column for the appropriate message alias. Read the pop-up message and confirm this is the user to remove from the business directory. 2. Click **Delete** to remove the user from the list. No further action is necessary.

Note: *Voicemail to email messages are sent both to and from the user that owns the mailbox that received the Voicemail. All of the entries included in the Address list of the Message Alias are blind copied on the email.*

14.3 Avoiding Common Mistakes when Forwarding Messages

A common error is assigning the Allworx premise server or Connect Vx instance domain name to be the same as an existing domain name. For example, an Internet hosting service provides email for employees as **user@mycompany.com**. Configure the email application to POP the email off the hosting service email server for employees to get email.

When installing the Allworx premise server or Connect Vx instance, it also receives a domain name of mycompany.com. This creates a conflict when configuring the Internet DNS servers sending mail to user@mycompany.com on the external hosting service IP address, but the Allworx DNS server configuration determines that it is responsible for handling email for the same domain name.

To avoid this conflict, do not use the same domain name for both servers. Put user@mycompany.com in the Message Alias Address list for the Allworx premise server or Connect Vx instance to recognize the username and send the email to itself instead of the external IP address.

To setup external accounts (SMTP, POP3 Client, IMAP Client), see “Email” on page 283. When using personal email accounts for External SMTP Accounts or POP3 Clients, see “User Template Settings” on page 233 for more information.

Example 1:

Requirements	Tom (login name tom) does not expect to get email at the Allworx premise server or Connect Vx instance address, but he uses an external email account (tom@yahoo.com). The Allworx server Voicemail should go to the external email account and also be available from his phone.
Configuration	Set up an Allworx User Message Alias for Tom to forward all messages to the external email account, and keep a copy on the Allworx premise server or Connect Vx instance. **To create a new message alias (example):** 1. Set the *User Alias* to **Tom (tom)**. 2. Click to select the **Keep a copy on the server** check box. 3. Set *Addresses* **tom@yahoo.com.**

Continued

Commentary	Tom uses the phone to delete old Voicemail messages. If sending an email to the Allworx account, the Allworx server forwards it to an external account, leaving a copy on the Allworx server. If email accumulates on the server, Tom needs to connect with a POP email client to delete the old messages.

Example 2:

Requirements	Tom is a remote user of the system and does not have a phone. The extension configuration sends all calls directly to Voicemail. Tom wants to access all email and Voicemail messages from his external email account (tom@yahoo.com).
Configuration	Set up an Allworx User Message Alias for Tom to forward all messages to the external email account (make sure the *Keep a copy on the server* check box is NOT checked). **To create a new message alias:** 1. *User Alias* is set to **Tom**. 2. Verify that the *Keep a copy on the server* check box is NOT selected. 3. *Addresses* is set to **tom@yahoo.com**.
Commentary	Tom gets all email and Voicemail messages using the external email account. Since the system deletes the messages off the premise server or Connect Vx instance after forwarding, Tom does not need to periodically delete anything.

Example 3:

Requirements	Tom wants use the Allworx premise server or Connect Vx instance for his email, and his phone to listen to Voicemail messages. Tom does not want the Voicemail sent to his email account.
Configuration	• Set up Tom’s Allworx POP3 Mail Transfer configuration to transfer email messages. • Set up Tom’s PC email application to POP email off the Allworx server without leaving a copy on the server.
Commentary	The server deletes Tom’s email messages as soon POPping to his PC email application. The server keeps Voicemail messages until he deletes them via his phone.

Example 4:

Requirements	Tom wants to use the Allworx server for email. He wants to use his phone to listen to Voicemail messages and wants to send those messages to his email account.
Configuration	• Configure Tom's Allworx server POP3 Mail Transfers for email and Voicemail messages (default). • Set up Tom's PC email application to POP email off the Allworx premise server or Connect Vx instance and leave a copy on the server until deleting the message on his PC.
Commentary	Tom can to listen to Voicemail messages on his phone or PC (via email). If he deletes a Voicemail message using his phone, it remains on the PC. However, if he deletes a Voicemail from the PC, it does not remain on the premise server or Connect Vx instance making it no longer available on his phone. Tom must periodically delete messages from the PC to avoid exceeding the server message quota.

Click here to return to the Installing and Configuring Allworx Premise Servers or Configuring Connect Vx Instances .

Chapter 15 Music On Hold

Prerequisites	
Access Permissions	Allworx Server Administrator Allworx System Administrator Phone Administrator role
Feature Key Required	No

Music on Hold provides audio to callers in queues, calls held on phones, and parked calls. It also supports configuring multiple file sources and playing different music to different callers. System phones dialed into a local Allworx Conference Center do not play hold music into the conference when placing the phone into a hold state.

Music can come from a Line-In source or from audio files stored on the Allworx premise server. Allworx Connect Vx instances do not provide Line-In as a source, but use only audio files stored on the Connect Vx instance. The appropriate changes/omissions for Connect Vx have been made to the Allworx System Administration web page. To use a Line-In source, consult the *Allworx Connect Server Family Installation Guide*.

Allworx premise servers and Connect Vx instances support up to 30 recordings with a maximum storage size limit of 250MB on Connect premise servers and Connect Vx instances. The music on hold provided with the Allworx System Software is set as the default audio to be played when a caller is placed on hold or waiting in a queue. For premise servers this default prevents silence on hold when **Line in** is selected, but the customer does not have a source connected.

15.1 Filename Requirements

The Allworx premise server and Connect Vx service provide two electronic hold music files (default music file: **moh_supplied.snd**), and the Music On Hold file repeats as long as there are callers on hold. These two files provide the same music at different volume levels. If a different style or a site-specific music track is necessary, import it onto the Allworx premise server or Connect Vx instance. See “To import or export greetings and messages:” on page 43 for more information.

Note: *Allworx recommends assigning the files to Handset Preference Groups instead of individual Call Appearances. Assigning the file to a Handset Preference Group updates the Hold Music Selection preference setting for the group. See “Handset Preference Group Settings” on page 122 for more information.*

The system audio (e.g. Auto Attendant greetings) files must be Telephony, raw, mu-law (u-law), mono, 8-bits per sample, 8KHz sample rate and use the following file naming convention:

File name: **moh_n_m.snd** where

- 'n' is a number between 1 and 30. This is a unique number among the Music On Hold files on the system. If importing a Music On Hold file that duplicates the number ‘n’ of a file that is already on the system, the system replaces the existing file.
- 'm' is a user defined string that uniquely identifies the file. Valid characters include ('A'-'Z'), ('a'-'z'), ('0'-'9'), and underscore.

- Sample file name: **moh_1_sales.snd** or **moh_2_service.snd**.

To convert files into an Allworx-supported format, see “Custom Recordings” on page 339.

To assign individual call queues or ACD queues, see “To manage the Call Queue settings:” on page 55.

15.2 Managing the Music On Hold

To manage the Music On Hold:

1. Log in to the Allworx System Administration web page, and navigate to **Phone System** > **Music On Hold**. The following panes display on the page:

Pane	Description
File Statistics	The memory allocation for imported music file.
Music On Hold Source	Individual music file details, assigning music sources to Call Queues, Call Appearances, and handset preference groups.

2. Locate the *Music On Hold Sources* pane and click **modify**. The *Reach Link, Call Queue*, *Handset Preference Group*, and *Call Appearance* tables display.

   Note: *The Allworx system applies the Park to Extension - Default source setting at the time a User or System Extension is created. Manage changes to the Music On Hold Sources settings for Park to Extension for User and System Extensions by navigating to* ***Phone System*** *>* ***Extensions*** *and locating the Bulk Edit pane.*

3. Select the table, and then click the associated *Source* drop-down list to select an available option.

   The Allworx System Software comes with two built-in Music on Hold files from which Allworx Administrators can choose the best option for better playback sound clarity when placing callers on hold. The options are described in the following table:

Option	Description
Line-In	Change the selection by going to a different music source, click Usage, and check the preferred client(s). ***Note:*** *This option is not available with the Connect Vx service.*
moh_supplied.snd	Set the Allworx System to use the default Music on Hold file to the caller on hold.
moh_supplied_louder.snd	Select this file when using the default Music on Hold file (moh_supplied.snd) is too quiet. Using Music on Hold sources with insufficient volume sometimes results in broken-up sound for the caller on hold. This situation is highly dependent on the complete audio path, including third-party equipment. Using this louder file may not work in all cases.
<name.snd>	Set the Allworx System to use custom files for the caller on hold.
None	Set the Allworx System to use no Music On Hold for the caller on hold.

To assign a Music on Hold source to multiple line types, click the **Bulk Edit** additional information arrow ▶ and the music source from the drop-down list. Check the line type boxes to use the Music On Hold source file, and then click the **Assign** button. Click **Confirm** to save the changes.

4. Repeat step 3 to update each available table/line item.

5. Click **Update** to save the change.

Click here to return to the Installing and Configuring Allworx Premise Servers or Configuring Connect Vx Instances .

Chapter 16 Outside Lines

Prerequisites	
Access Permissions	Allworx Server Administrator Allworx System Administrator Phone Administrator role* Network Administrator role*
Feature Key Required	No
* Features are available to Phone Administrators or Network Administrators, but not both roles.	

The *Outside Lines* page supports access to various communication lines. Allworx premise servers and Connect Vx instances support placing and receiving calls over the following line types:

- POTS/CO*
- SIP Proxies
- Px Expanders
- SIP Gateways
- T1/PRI***
- T1/CAS-T1-RBS**

** Applies to Connect 324, 536, and 731 premise servers only and is not supported by Connect Vx service.*

*** Applies to Connect 731 premise server only and is not supported by Connect Vx service.*

Additionally, the Allworx premise servers and Connect Vx instances, and Allworx IP phones support a configuration like a Key system where it is just a push of a button for a specific outside line, and incoming calls illuminate that line's button – one incoming call can go to many people.

Example Configuration:

Requirement	An insurance agency, Best Insurance, has three CO lines. • The office has five employees, each having an Allworx phone. • The system behaves like a Key System with a PFK on each phone mapped to each of the CO lines. • Using the PFK, each employee can monitor and directly answer each of the CO lines. If unanswered, 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". See "Managing Users" on page 225 for more information. 2. Create a system extension to route all incoming calls. Set up the call route so that it has one connection attempt for Key System Ring Delay (Ring Group) that rings 6 times. See "Managing Call Routes" on page 97 for more information. • As part of this configuration of the call route, enter the *Finally Route* to transfer to Voicemail for user "Best Insurance." For each CO line, click to select the *Enable Line Appearance* check box. 3. Configure the call route for each CO line so all calls go to the created system extension. 4. Configure a Line Appearance PFK for each CO line on each Allworx phone. See "Managing the Programmable Function Keys (PFKs)" on page 138 for more information.

16.1 Setup Checklist

Complete the following steps in this order to successfully setup the outside phone lines and the DID routing plan. Click on the links in the column on the right for more information about each step.

Step	Description	More Information
1	Determine the type of phone lines.	“Determining the Type of Phone Lines” on page 177
2	Setup the phone lines.	“Managing Analog Central Office (CO) Lines” on page 178 “Managing SIP Proxies and SIP Gateways” on page 183
3	Setup the DID blocks.	“To manage a DID block:” on page 180
4	Setup and assign a DID call routing plan.	“To configure a Call Routing Plan for the DID Block:” on page 181

16.2 Managing Incoming Call Handling

The Incoming Call Handling facility allows incoming calls to be routed based on their Caller ID information.

Anonymous Call Handling is the call routing when the incoming Caller ID is private. Anonymous Call detection requires receiving Caller ID information that specifies the calling party has requested privacy. By default, the Allworx premise servers and Connect Vx instances route anonymous calls normally, unless otherwise specified.

To manage anonymous call handling:

1. Log in to the Allworx System Administration web page and navigate to **Phone System** > **Outside Lines**.
2. Locate the *Incoming Call Handling* pane, and click the additional information arrow ▶, if necessary**.**
3. Click **modify.** The *Incoming Call Handling* window opens. Click one of the following options for anonymous calls:

Option	Description
Routed normally	Default setting. Follow the specified call route. See “Managing Call Routes” on page 97 for more information.
Routed to extension	Configure a new number to route private calls normally on the system. Select an extension/user from the drop-down list. ***Note**: Not all ITSPs support Anonymous Call Handling.*

4. Click **Update** to save the changes.

Notes:

- *Allworx premise servers with System Software 8.5.3 or higher and Connect Vx instances conform with RFC 5079 when dealing with anonymous call requests, allowing the calling system to understand the reason why the call was rejected.*

The following configuration must be in place for this capability to be in effect:

1.An extension must be defined with a call route that hangs up immediately (i.e., no connection attempts).

2.This extension must be selected for anonymous calls under Phone System > Outside Lines > Incoming Call Handling.

- *When an anonymous call is received on a SIP trunk, the Allworx premise server and Connect Vx instance sends a 433 Anonymity Disallowed response.*

To manage other incoming call handling:

1. Log in to the Allworx System Administration web page and navigate to **Phone System** > **Outside Lines**.
2. Locate the *Incoming Call Handling* pane, and click the additional information arrow ▶, if necessary**.**
3. Click **modify.** The *Incoming Call Handling* window opens.
4. Add a new name or number pattern in a blank *Caller ID Name* or *Caller ID Number* field.
5. Select the extension to which the matching call will be routed.
6. Click **Update** to save the changes.

Up to 1000 patterns for caller ID names and/or numbers can be added. Matches are determined by comparing the leading digits or characters of the rule against the incoming caller ID name or number, respectively. Caller ID names are matched with a case-insensitive comparison ("Private" will match "PRIVATE") and routed as selected. Some examples are:

- A Caller ID Number rule set to "858" will match all calls from this San Diego area code.
- A Caller ID Name rule set to "wireless" will match all calls with the name "WIRELESS CALLER".

To remove an entry, delete the pattern then click **Update**.

16.3 Determining the Type of Phone Lines

The first thing to consider when setting up outside phone lines is what sort of phones lines are coming into the location, and will the number of those lines expand in the future. The Allworx system works with any incoming telephone, SIP, or PRI line currently in place or may obtain in the future. Knowing the types of phone lines required is important when deciding what type of Allworx system is necessary.

If using a T1 line with PRI, use a Connect 731 premise server. Otherwise, any of the Allworx Connect premise servers can handle both CO (regular telephone lines that come in from a Telco) and SIP lines (VoIP calling that goes out a network connection instead of the regular telephone lines). The Allworx Connect Vx service handles SIP lines only.

16.4 Managing Analog Central Office (CO) Lines

Note: *CO lines are not supported by Connect Vx service.*

Central office (CO) lines connect and route telephone calls in the public switched telephone network. By default, the line rings to the default Auto Attendant.

Note: *The CO (FXO) trunk line does not support the Reach Extend feature. The Reach Extend call does not complete when using a CO line. The SIP or T1 PRI line is the only configuration that supports the Reach Extend Feature.*

Limitations with CO lines:

If connecting the parties from one CO (POTS) line to another CO (POTS) line, the announced call transfer feature does not work. Set up the handset so that all transfers are blind transfers by managing the **Handset Preference Group** > **Unannounced Transfer Mode** > **Immediate** option. See "Managing User Templates" on page 232 for more information.

To manage an Outside (CO) FXO Line:

1. Plug in the phone line that comes in from the Telco into one of the FXO ports on the Allworx system and reboot the Allworx premise server.
2. Log in to the Allworx System Administration web page, navigate to **Phone System** > **Outside Lines**.
3. Locate the *Analog (CO) Lines* pane, and click the additional information arrow ▶, if necessary**.** Locate the **Analog (CO) Lines** table, and click one of the following links:

Link	Description
New FXO Line	1. Enter the settings information per "Outside (CO) FXO Line Settings" on page 178. 2. Click **Add** to save the change.
Modify	1. Update the settings per "Outside (CO) FXO Line Settings" on page 178. 2. Click **Update** to save the change.
Delete	Removes the Outside (CO) Line from the premise server. Click **Delete** to remove the line.

Outside (CO) FXO Line Settings

Outside Line	
Description	DNIS display on phones that receive calls on this line.
Notes	Enter information about the outside line. This information will be displayed on the Phone System / Outside Lines page. A maximum of 512 characters may be entered.
Port	Automatically filled in.
Enable Line Appearance	Configure the handsets with Line Appearance PFKs for this line.

Continued

Default Language	Select a language for systems configured with multiple languages to use with Auto Attendant and/or queue prompts for inbound callers.

Features	
Line has Caller ID Service	Display the Caller ID information.
Enable Echo Cancellation	Only disable at the request of Allworx Customer Support.
Enable Comfort Noise	Applicable to Allworx Connects premise servers only. Enable or disable Comfort Noise Generation. Default is enabled, only disable at the request of Allworx Customer Support.
Optimize for short loops	Check for FXD/IADs less than 500 feet away, not typically selected.
Send digits as dialed	Indicate sending outbound numbers dialed exactly as on the handset placing the call. The number converts into NANPA dialing form, so this box is not normally checked. However, in some cases, the service provider or proxy may be doing the conversion automatically and need to defeat the Allworx premise server's conversion mechanism without processing per External Dialing Rules.
Prefix Digits	Enter automatically dialed digits on the line prior to dialed digits by handsets placing outbound calls on this line.
CPC Disconnect timer	Default 350 milliseconds.
Pre-dial delay	Typically 500 milliseconds.
DTMF Duration	Typically 100 milliseconds.
DTMF Gap	Typically 100 milliseconds.

Default Auto Attendant pane	
Select the attendant used to answer when calls received from this source are routed to an Auto Attendant.	Select an option from the drop-down list.

Call Route	
Calls received from this CO line go to:	• Extension - select from the drop-down list. • Auto Attendant • Voicemail for user - select the user from the drop-down list.

To setup Fax Server Support and route an outside line to the device:

The Allworx server provides the ability to send control information in the form of DTMF digits to devices connected to the premise server FXS ports. Use a phone extension phone and/or the dialed number (DNIS) along with arbitrary DTMF characters to control the following devices:

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

The server sends the digits immediately after the device answers and before audio from the calling source is available. To add the device and configure sending the DTMF digits, see “Managing Analog Handset Configuration” on page 155. To receive incoming calls, route an outside line to the attached device port.

1. Create an extension that rings the port of the device. See “Adding a New Extension” on page 91 for more information.
2. Route an outside line to the extension.

Note: *For specific device setup instructions for the Multi-Tech FaxFinder, refer to the Multi-Tech FaxFinder Setup Application Notes document located on the Allworx Portal at (allworxportal.com).*

16.5 Managing Direct Inward Dial (DID) Blocks

Direct Inward Dialing (DID) is a block of phone numbers for calling into a PBX without requiring a physical line for each number offered by a local telephone company. Working with the PBX, it maps each number to a PBX extension. Each PBX user has a unique outside number that rings the user’s phone directly, rather than directing the incoming call to an Auto Attendant.

16.6 Setup Checklist

Follow this order of the steps to successfully configure the Allworx premise server or Connect Vx instance for DID service. The table also provides links to the appropriate chapter for more information.

Step	Description	More Information
1	Create a DID block	“To manage a DID block:” on page 180.
2	Configure the call routing plan for the DID block.	“To configure a Call Routing Plan for the DID Block:” on page 181
3	Create a DID line for each DID trunk line plugged into the server.	

To manage a DID block:

1. Login to the Allworx System Administration web page and navigate to **Phone System** > **Outside Lines**.
2. Locate the *Direct Inward Dial Blocks* pane, and click the additional information arrow ▶, if necessary.

3. Click one of the following actions:

Action	Description
add new DID Block	Create a new direct inward dialing block. 1. Enter the following information: • Starting Phone Number (include area code and exchange) • Total number of phone numbers in DID block (specified by the telephone company) • DID Routing Plan - select the plan from the drop-down list. 2. Click **Add** to save the changes. ***Notes:*** • *If the site phone numbers are over a range of numbers, create DID blocks for each individual or grouping of phone numbers.* • *It is suggested to create a larger DID block that spans multiple DID ranges, even if many of the numbers in the block are not in use for easier management of the blocks.* • *Since there is a limit to the number of assigned DID blocks to any outside line (128 blocks per line), combining DID numbers into larger blocks avoids reaching this limit.*
Modify	Reconfigure the existing settings. 1. Enter the following information: • Starting Phone Number (include area code and exchange) • Total number of phone numbers in DID block (specified by the telephone company) • DID Routing Plan - select the plan from the drop-down list. 2. Click **Update** to save the changes.
Delete	Remove the DID block from the system. 1. Verify the DID block selection. 2. Click to select the *Delete Routing Plan* check box to delete the Routing Plan associated with the DID Block. 3. Click **Delete** to remove the DID Block and the Routing Plan if selected. ***Note:*** *The option to delete the Routing Plan is not presented if the Routing Plan has been assigned to more than one DID Block.*

To configure a Call Routing Plan for the DID Block:

The premise server or Connect Vx instance uses the *Default Extension* to map any unassigned phone numbers to an extension.

1. Create the DID block. See “To manage a DID block:” on page 180 for more information.
2. Log in to the Allworx System Administration web page and navigate to **Phone System** > **Outside Lines.** Locate the *Direct Inward Dial Routing Plans* pane. Click the additional information arrow ► if necessary.

3. Locate the needed Routing Plan and click one of the actions listed in the following table:

<table>
<tr><th>Action</th><th>Description</th></tr>
<tr><td><b>Details</b></td><td>
<b>Routing Plan Information</b>
<p>1. Click <b>modify</b> to change the existing settings.</p>
<table>
<tr><th>Setting</th><th>Description</th></tr>
<tr><td><i>Description</i></td><td>Enter a name for the routing plan.</td></tr>
<tr><td><i>Default Extension</i></td><td>Select the extension from the drop-down list.</td></tr>
<tr><td><i>Default DNIS Name</i></td><td>Display on calls to DID numbers when no specific DNIS Name is specified in the <i>Phone Number to Extension Mapping</i> pane, indicated by $ in the DID-specific DNIS name.
Enter a Dialed Number Identification Service (DNIS). The DNIS name displays on the recipient’s Allworx phone. If there is no DNIS name entered, the originally dialed number displays on the phone.</td></tr>
<tr><td><i>Default Prompt Language</i>
<i>(requires the Dual Language Support feature key)</i></td><td>Each outside line has a default language. When receiving calls over an outside line, the system assigns the default language for that line. Thereafter, when the call reaches some applications within the server (e.g. Auto Attendant, queue), the system uses or overrides the outside line language, depending on the application’s language setting. Select an option from the drop-down list:
• Use Source of call
• Primary Language
• Secondary Language</td></tr>
<tr><td><i>DID Blocks using this plan</i></td><td>Displays the current DID blocks associated with the <i>Routing Plan Information</i>.</td></tr>
</table>
<p>2. Click <b>Update</b> to save the changes.</p>
<b>Phone Number to Extension Mapping</b>
<p>1. Click <b>modify</b> to change the existing settings.</p>
<table>
<tr><td><i>Search term</i></td><td>Enter the search criteria and press <b>Enter</b> to display all phone numbers meeting that criteria.</td></tr>
<tr><td><b>Bulk Edit</b></td><td>Click to apply the operations to more than one <i>Phone Number</i>.
1. Click to select the check boxes next to the <i>Phone Numbers</i>.</td></tr>
</table>
</td></tr>
</table>

Continued

Action	Description	
Details *(continued)*		2. Click **Assign** to assign the following parameters to the selected phone numbers: • *Extension* • *DNIS Name* • *Default Prompt Language (requires the Dual Language Support feature key)* A field appears for selecting the *Extension, Default Prompt Language*, or the entering of the *DNIS Name*. 3. Click **Confirm** to make the change, or **Cancel** to ignore the request.
	<Phone Number>	Click **Modify** to update the following information: • *Extension* - Select the extension from the drop-down list. • *DNIS Name* - Leave the $ to use the DID Block Default DNIS name or enter a DNIS Name for this DID number. • Default Prompt Language - Select the one of the following language options from the drop-down list *(requires the Dual Language Support feature key):* • **Use Plan's Default Prompt Language settings** • **Primary Language** • **Secondary Language** • **Use Source of call**
	2. Click **Update** to save the changes.	
Delete	Remove the DID Routing Plan from the system. 1. Verify the DID Routing Plan selection is correct. 2. Click **Delete** to remove the DID Routing Plan. 3. Click **Delete** in the confirmation window, or click **Cancel** to ignore the action.	

16.7 Managing SIP Proxies and SIP Gateways

Allworx premise servers and Connect Vx instances support connectivity to external SIP-compliant devices such as Internet Telephony Service Provider (ITSP) servers and SIP gateways. The Allworx products interface with three different types of SIP devices based the ability to interact with the Allworx system. SIP Gateways and SIP Proxies are different features with similar configurations.

SIP devices include:

Device	Description
SIP Proxy	A SIP Trunk, an external SIP service for routing calls. Access the SIP Proxy through the Internet or through the wide area network (WAN). • To connect to a SIP proxy (or ITSP), configure the SIP Proxy on the Allworx server. Application notes for configuring Allworx servers with approved ITSPs are available on the Allworx Portal at www.allworxportal.com.
SIP Gateway	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.
Remote Allworx Servers (Multi-Site)	An Allworx server at another site configured to behave as if it is part of the local system. The Allworx administrator can configure the remote Allworx server to provide outside line services for the local server. See the *Allworx Advanced Multi-site User Guide* for information on configuring these services. ***Note:*** *Calls cannot be forwarded to phones on different sites within a Multi-Site network.*

Setting up a SIP line is a bit more complex than setting up a CO line, since the SIP line requires the use of an ITSP, or Internet Telephone Service Provider. To set up the SIP line, be certain that the network settings and configuration are complete. Since the SIP lines require the use of the network to transmit the phone calls, verify the network is set up properly and that network traffic is able to transverse the network and go out successfully to the Internet.

Gather some basic information from the SIP Provider to enable the SIP trunks.

- User ID- some SIP providers require a user ID to activate the service. This is usually the telephone number that is associated with the new SIP line.
- Name or IP Address of the main SIP Server- This is the server that processes calls.
- Name or IP Address of the main Outbound SIP Server- required only if this server is different than the main SIP Server. If it is the same, leave this field blank.
- SIP Registration requirements- provided by the SIP Provider if required. If so, gather the SIP Login ID and SIP Password to register with the SIP Service.
- Registration server- The name or IP Address of the server that used to ‘log in to’ for SIP Service. Required only if this is a different server than the Outbound SIP Server (see above).
- The number of lines ordered from the SIP Provider and the maximum number of calls that the SIP Provider can or will handle on those lines.

After testing the network, get to the Internet through the Allworx server, and have all the necessary information from the SIP provider, set up the SIP proxies for use.

Limitations with SIP Outside Lines:

The following calling features are not available when using SIP trunks or SIP Gateways, except when one of the parties in the call is using an Allworx phone or Px expander:

- Consultation and call transfer (using *, #, or *7) by users of Follow-Me-Anywhere call routes.
- Disconnecting calls (using *#) when accessing outside lines through the Message Center.

To manage a SIP Gateway or SIP Proxy:

SIP Proxies and SIP Gateways have configuration settings specific to using the ITSP or device.

1. Log in to the Allworx System Administration web page and navigate to **Phone System** > **Outside Lines** page.
2. Locate the appropriate pane and click the additional information arrow ►, if necessary.
3. Click the link. Update the parameters (see table below) specifically for the ITSP service in use.

SIP Gateway	
add new SIP Gateway	Click to open the SIP Gateway dialog box. Update the parameters, and then click **Add** to save the request.
Modify	Locate the SIP Gateway in the list and click **Modify**. This opens the SIP Gateway dialog box. Update the parameters, and then click **Update** to save the request.
Delete	Locate the SIP Gateway in the list and click **Delete**. Verify the SIP Gateway selection, and then click **Delete** to remove the SIP Gateway from the list. Requires no further action.
SIP Proxies	
add new SIP Proxy	Click to open the SIP Proxy dialog box. Update the parameters, and then click **Add** to save the request.
Modify	Locate the SIP Proxy in the list and click **Modify**. This opens the SIP Proxy dialog box. Update the parameters, and then click **Update** to save the request.
Delete	Locate the SIP Proxy in the list and click **Delete**. Verify the SIP Proxy selection, and then click **Delete** to remove the SIP Proxy from the list. Requires no further action.

SIP Gateway and SIP Proxy Settings

SIP Gateway	
Description	Assign a name to the SIP Gateway - such as the ITSP name.
Notes	Enter information about the SIP Gateway. This information will be displayed on the Phone System / Outside Lines page. A maximum of 512 characters may be entered.

Continued

Caller ID Name	Display the name of handset or user. Enter a up to 47 characters in the field provided or check a box: • Use External Caller ID Name from handset • Use Caller ID Name from external sources
Caller ID Number	Display the name of handset or user. Enter a up to 24 digits in the field provided or check one of the boxes: • Use External Caller ID Number from handset • Use Caller ID Number from external sources
Number of Line Appearances	Enter a number up to 99 that does not exceed the number of CO lines attached to the gateway.
Send digits as dialed	Use the digits as specified in the External Dialing Rules. Select the check box to enable.
SIP Server	The DNS name or IP address of the proxy server to connect to provided by the ITSP. The port number is usually 5060 but verify with the ITSP.
Default Prompt Language	Each outside line has a default language. When receiving calls over an outside line, the Allworx premise server and Connect Vx instance assigns the default language for that line. Afterwards, when the call reaches some features within the premise server or Connect Vx instance a (e.g. Auto Attendant, Call Queue), the system software uses or overrides the outside line language depending on the application's language setting. The language usage for Allworx audio messages and played greetings for inbound calls is through the SIP Proxy. This feature requires the Dual Language Support feature key. Select an option for the default language from the drop-down list: • Primary Language • Secondary Language
SIP Proxy	
Description	Assign a name to the SIP Proxy - such as the ITSP name.
Notes	Enter information about the SIP Proxy. This information will be displayed on the Phone System / Outside Lines page. A maximum of 512 characters may be entered.
User ID	ITSP typically assigns this value and is often the account phone number.
SIP Server / Port	DNS name or IP address of the proxy server to connect to provided by the ITSP. The port number is usually 5060 but verify with the ITSP.
Outbound Proxy / Port	DNS name or IP address of the outbound redirect server, if it differs from the SIP Server. The system does not require this in many cases.
SIP Registration Required	Use of the SIP proxy server requires a SIP registration. The ITSP assigns the Login ID (limit 40 characters) and Password. If the ITSP uses a registrar server that is different from the SIP proxy server, enter the DNS name or IP address of this server in the Registrar name field.

Continued

Caller ID Name	Display the name of handset or user. Enter a up to 47 characters in the field provided or check a box: • Use External Caller ID Name from handset • Use Caller ID Name from external sources
Caller ID Number	Display the name of handset or user. Enter a up to 24 digits in the field provided or check a box: • Use External Caller ID Number from handset • Use Caller ID Number from external sources
Maximum Active Calls	The Allworx premise server or Connect Vx instance uses this number to limit the total number of the incoming and outgoing active calls with the SIP Proxy. Useful for controlling the network bandwidth, since the Allworx system understands that the SIP proxy is not a LAN local service.
Number of Line Appearances	Enter a number up to 99 that does not exceed the number of CO lines attached to the gateway.
Append Enterprise Prefix to Dial back number of incoming calls.	Add the enterprise dial plan digits (8 by default, *8 for extension mode) to the beginning of the caller's extension of an inbound call from a proxy server. This enables automatic dial back (e.g., selecting a call from the phone Calls list to contact the original caller) to function properly when the proxy server requires enterprise dialing for outbound calls.
Send Digits as Dialed	Indicate sending outbound numbers dialed exactly as on the handset placing the call. • The number converts into NANPA dialing form, so this box is not normally checked. • In some cases, the service provider or proxy may do the conversion automatically and need to override the Allworx premise server or Connect Vx instance conversion mechanism.
Digits Sent	Number of dialed DTMF digits sent to the ITSP when making a call. Default value is all digits. If the number specified is less than the number of digits dialed, the Allworx premise server or Connect Vx instance sends only the trailing digits.
Default Prompt Language	Each outside line has a default language. When receiving calls over an outside line, the Allworx premise server or Connect Vx instance assigns the default language for that line. Thereafter, when the call reaches some applications (e.g. Auto Attendant, Call Queue), the system uses or overrides the outside line language depending on the application's language setting. The language for Allworx audio messages and played greetings for inbound calls is through the SIP Proxy.
SIP Registration - applies to SIP Gateway only	
Gateway uses SIP Registration	If the gateway supports registration, select this option. • Assign an arbitrary Login ID and Password for the gateway to use to register with Allworx. Use this preferred configuration, especially if the gateway uses DHCP to obtain its IP address so that the Allworx premise server or Connect Vx instance always knows how to contact the gateway for outbound calls.
Gateway uses Static IP Address	Use if the gateway does not support registration or if not authenticating the gateway. Contacting the gateway through this mechanism requires the gateway to have a static IP address. The system does not enable DNS names for security reasons.

Continued

<table>
<tr><th>Advanced Settings*</th><th>Checking the box enables the option.</th></tr>
<tr><td><i>show Codec Filter /</i>
<i>hide Codec Filter</i></td><td>Toggle between displaying and hiding the selection boxes that limit which codecs the Allworx system supports when using a SIP proxy or SIP gateway. Selecting no codecs is the same as selecting all codecs.
Options include:
<table>
<tr><td>PCMU</td><td>PCMA</td><td>G729</td><td>GSM</td><td>G722</td><td>G723</td></tr>
<tr><td>G726-40</td><td>G726-32</td><td>G726-24</td><td>G726-16</td><td>G728</td><td>DVI4-8000</td></tr>
<tr><td>DVI4/16000</td><td>L16</td><td>CN</td><td>H263</td><td>H264</td><td>MP4V-ES</td></tr>
<tr><td>t38</td><td></td><td></td><td></td><td></td><td></td></tr>
</table></td></tr>
<tr><td><i>Pad DTMF RTP packets</i></td><td>Some switches and routers discard any UDP packets shorter than 64 bytes. <i>Default</i>: <b>Disabled</b>
• <b>Enabled</b>: the Allworx system pads the DTMF packet and expands the RTP header to make the packet at least 64 bytes long.</td></tr>
<tr><td><i>Enable Early Media</i></td><td>Some service providers send audio before answering an outbound call (using 183 Session Progress in SIP). Use this to relay announcements (e.g. Your call can not be completed as dialed) or remote ring back tones. <i>Default</i>: <b>Disabled</b>.
• <b>Enabled</b>: Allworx system presents the audio to the caller when received.
• <b>Disabled</b>: Allworx system disregards the early audio and generates a ring back tone internally.</td></tr>
<tr><td><i>Supports SIP REFER</i></td><td>Selects the method of transferring calls between multiple remote end-points through the service provider. <i>Default</i>: <b>Disabled</b>.
• <b>Enabled</b>: the Allworx system sends the SIP REFER to the service provider to enable them to connect the two end-points within the network without intervention by the Allworx.
• <b>Disabled</b>: the Allworx premise server or Connect Vx instance acts as a proxy between the two remote ends of the calls.</td></tr>
<tr><td><i>Supports SIP Redirect</i></td><td>Select the method of redirecting forwarded inbound calls back to the service provider answering (e.g., system forwards all calls to a cell phone). <i>Default</i>: <i>Disabled</i>
• <b>Enabled</b>: The system sends a SIP 300 redirect message
• <b>Disabled</b>: The Allworx system negotiates the call setup for the service provider</td></tr>
<tr><td><i>Use E.164 format for phone numbers</i></td><td>Enable this feature to cause rewriting of phone numbers into the international E.164 format (e.g. 800-555-1212 becomes +18005551212). <i>Default:</i> <b>Disabled</b>
• <b>Enabled</b>: If required by the ITSP</td></tr>
<tr><td><i>Offer ‘100rel’ support</i></td><td>Indicate the Allworx supports 'reliability of provisional responses (RFC 3262)'. <b>Default</b>: Disabled</td></tr>
<tr><td><i>Supports Symmetric Response Routing</i></td><td>SIP Proxy only - Some service providers assist the remote end in NAT traversal by supporting RFC 3581 Symmetric Response Routing. <i>Default</i>: <b>Disabled</b>
• <b>Enabled</b>: a remote handset behind a NAT firewall assumes the service provider can correctly detect the audio port to send traffic.
• <b>Disabled</b>: port-forward the handset through the NAT firewall, or use the Allworx for proxying of audio traffic (see “VoIP Server” on page 295).
<i>Continued</i></td></tr>
</table>

Supports user=phone parameter	When enabled, the premise server or Connect Vx instance provides support for the 'user=phone' parameter in URIs. When used, this parameter indicates that the user portion of the URI should be interpreted as a telephone number (tel-URI).
Force audio through server	Force RTP for all calls to or from the proxy through the premise server or Connect Vx instance.
Allow SIP P-Asserted-Identity	SIP Proxy only - The premise server or Connect Vx instance asserts its identity with enabled proxies as well as proxy asserted identity from trusted devices to other trusted devices.
Send SIP Diversion header row	SIP Proxy only. Select an option from the drop-down list: • **never** • **always** • **on redirect**
Obtain DID/DNIS number from [source]	Inbound calls: where the premise server or Connect Vx instance gets the DID and DNIS information. Typically, this is set to **[SIP To: header field]**.
Use [source] in Request URI of outbound calls	This defines the user name 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].

* 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.

Features

Prefix String	Define the DTMF digits pre-pended to the dialed number string when placing outbound calls through the gateway (e.g., ‘9’ for dialing through another SIP PBX).

Default Auto Attendant

Select the auto-attendant to use from the drop-down list when routing inbound calls from this Proxy to an Auto Attendant.

Call Route

Each outside line (CO Line, DID Line, SIP Proxy, SIP Gateway, or a T1 Line) has an associated call route. The *Call Route* pane directs the call coming into the system through T1 Line 1 channel 01.

Calls received from this SIP Gateway go to:	Click a radio button to select the option:

Call Route	Description
Extension	Route incoming calls to a User or System extension. Using a System Extension provides more call routing flexibility and enables using a common route for multiple lines. Select an extension from the drop-down list.

Continued

Calls received from this SIP Gateway go to: *Continued*	*Auto Attendant*	Route an outside line to a designated Auto Attendant defined in the *Default Auto Attendant* pane. Requires no further action.
	Voicemail for user	Send incoming calls directly to a Voicemail box for a User. Select a user from the drop-down list.
	Routed using DID Block(s)	When using DID blocks for incoming calls, enable the DID block for the outside line or each preferred channel, if using T1 Lines. check the box to enable a DID block. To configure the DID Lines: 1. Configure each of the incoming lines using DID blocks.The following line types can use DID blocks: • T1/PRI • T1/RBS • SIP Proxy • SIP Gateway 2. Click on Routed using DID Block(s) and check the block(s) to use for this outside line. ***Note:*** *For T1 Lines, do this for each channel. If all channels use the same settings, check the Apply settings for this line to all lines with the same Port box.*

16.8 Managing Enterprise Dialing

Use the following procedures to configure the Enterprise Client and the Central Hub/Enterprise Server.

16.8.1 Configuring the Allworx Enterprise Client

Configure each Allworx premise server or Connect Vx instance as an enterprise client and direct inter-office calls to the central hub. The system creates a SIP Proxy for the central hub with the call routing set to Proxy is an enterprise server.

The Enterprise Dialing rule 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. See “Internal Dial Plan Settings” on page 71 for more information.

The Allworx dial plan uses an **8** prefix[1] to indicate forwarding the dialed number to the Enterprise Server (premise server or Connect Vx instance).

Example: Dialing 81234 sends a SIP INVITE with a URI of **<sip:1234@centralHubServer>** to the Enterprise Server.

[1] Extensions may vary per system. If using a non-default Internal Dial Plan, consult the My Allworx Manager > Phone Functions tab to determine what extensions to use for the corresponding feature.

16.8.2 Configuring the Central Hub / Enterprise Server

The central hub is a SIP proxy server that:

- Accepts incoming INVITEs from the Allworx premise server or Connect Vx instance
- Determines the final destination for the request
- Forwards the request to the Allworx destination
- Maintains an active list of Enterprise extensions and the mappings to extensions at each site

Example: An enterprise with four-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

* IP Address and SIP Protocol port of the Allworx premise server or Connect Vx instance. This can be static or updated through periodic SIP Registration.

Configure the Enterprise extensions as follows (using three-digit extensions):

Enterprise Extension	User	User Extension	Site
1234	Chris Jones	108	allworx1
1452	Tom Roberts	111	allworx1
4689	Mike Zwick	108	allworx2
5999	Jason Diaz	177	allworx3

Example: **Chris Jones in New York City dials 84689 to reach Mike Zwick.** The SIP INVITE is sent to the central hub with a URI of <sip:4689@centralHubAddress>. The Central Hub validates the sender credentials and finds 4689 in the databases. It creates an INVITE with <sip:108@64.129.42.33:5060> as the URI and sends it to allworx2. Mike Zwick answers the phone and establishes the call.

Later, Chris Jones dials 81452 to reach Tom Roberts. The SIP INVITE is sent to the central hub with a URI of <sip:1452@centralHubAddress>. The Central Hub validates the sender credentials and finds 1452 in its databases. The recipient is on the same server as the sender (allworx1), so the hub responds with a 300 Redirect with a Contact header URI of <sip:111@66.64.219.38:5060>. The Allworx server (allworx1) initiates a call to extension 111. Tom Roberts answers the phone and establishes the call.

To access Enterprise Dialing:

Note: *The steps for configuring and maintaining the SIP centralized server are well beyond the scope of this document. To deploy such an arrangement across sites requires detailed knowledge about the use and administration of SIP proxy servers. Contact Allworx Customer Support for an application note with additional helpful administration.*

1. Log in to the Allworx System Administration web page and navigate to **Phone System** > **Outside Lines**.
2. Click one of the following links:

add new SIP Proxy	Adds another SIP Proxy to the Central Hub.
Modify	Locate the SIP proxy that is the target for the Central Hub, click Modify to update the settings.

3. Locate the **Call Route** and check **Proxy is an Enterprise Server** to indicate the SIP Server is an Enterprise central server. Calls received from this proxy follow the server internal dial plan.
4. Click the **Update** button to save settings.

16.9 Managing T1 Lines

Connect 731 premise servers have one T1 Line interface. Allworx 24x and 48x premise servers have two T1 Line interfaces. There are differences in T1 port functionality between the 24x and 48x premise servers. For more information about T1 Lines or configuring the T1 line, see “T1 Lines” on page 251.

Note: *T1 lines are not supported with the Connect Vx service.*

To manage the T1 Lines:

1. Log in to the Allworx System Administration web page and navigate to **Phone System** > **Outside Lines** page. Locate the *T1 Lines* pane and click the additional information arrow ►, if necessary.
2. Locate the T1 Line and click **modify**. The T1 Line settings page opens. If the T1 option is unavailable, see “Configuration” on page 245 to enable the T1 port.
3. Update the settings, as required, and then click **Update** to save the changes.

T1 Lines Settings

T1 Line	
Description	DNIS display on phones that receive calls on this line.
Port	Automatically filled in.
Default Language	Select a language for systems configured with multiple languages to use with Auto Attendant and/or queue prompts for inbound callers.
Enable Line Appearance	Configure the handsets with Line Appearance PFKs for this line.

Continued

Features	
Line has Caller ID Service	Display the Caller ID information. ***Note:*** *When a call is received from a number that matches a phone number listed in the user's Contacts, the Contact information is used as the Caller ID.*
Enable Echo Cancellation	Only disable at the request of Allworx Customer Support.
Enable Comfort Noise	Applies to Allworx Connect premise servers only. Enable or disable Comfort Noise Generation. Default is enabled, only disable at the request of Allworx Customer Support.
Default Auto Attendant pane	
Select the attendant used to answer when calls received from this source are routed to an Auto Attendant.	Select an option from the drop-down list.
Call Route	
Calls received from this CO line go to:	Click the radio button to select one of the following options: • Extension - select from the drop-down list. • Auto Attendant • Voicemail for user - select from the drop-down list. • Routed using DID Block(s):

16.10 Allworx Port Expanders

See "Px 6/2 Expanders" on page 265 for more information.

Click here to return to the Installing and Configuring Allworx Premise Servers or Configuring Connect Vx Instances .

Chapter 17 Paging

Prerequisites	
Access Permissions	Allworx Server Administrator Allworx System Administrator Phone Administrator role
Feature Key Required	No

Paging provides communication over a speaker in specific areas within a building. As provided on Allworx Connect premise servers, paging is performed by transmitting the page audio on the Local Area Network (LAN) using IP multicast. Because multicast traffic is not supported on the Internet, Connect Vx instances are unable to provide paging in the same way. For Connect Vx instances, local Paging enlists the phone that is placing the page to perform the multicast transmission on behalf of the server.

An Allworx Verge phone has the ability to send a page to other devices connected on the same LAN as the originating Verge phone. Allworx Reach, Softphone, and non-Verge desk phones cannot be used to place a page. Paging calls are not played on devices on other LANs, even if registered on the same Connect Vx instance. Connect Vx paging zones cannot be included in multi-site paging. Paging calls to other premise sites can placed by calling the paging zone extensions on those sites.

Note: *Both local Connect Vx and Connect premise server pages cannot be sent from or received by Interact Softphone and Reach handsets.*

Allworx system software supports up to 10 paging zones via a single paging circuit with one active page at a time. Any attempts to page during another page results in a fast, busy signal.

The types of Paging are:

- **Overhead Paging** - The audio exits through the LINE IN/OUT jack or terminal block of the associated premise server. If used at a site, connect the LINE IN/OUT jack or terminal block to a paging amplifier or a public address announcement system.

  Note: *Overhead paging can be provided with Connect Vx instances by using a third-party solution.*

- **Zoned Paging** - A defined set of phones emitting the same class of pages. The Allworx Server Administrator can assign each handset to be in more than one paging zone. The system assigns any combination of zones to the Overhead Paging circuit (premise servers only) for those pages and also plays the audio out to the LINE IN/OUT jack or terminal block.

  Notes:

  - *Individual phones can only be in four (4) paging zones at one time.*
  - *On all premise servers the paging relay activates any time audio is sent to LINE OUT.*
  - *Paging zones that include Connect Vx instance local Paging cannot include the LINE OUT option because Connect Vx instances do not have a line-level output.*

- *Connect Vx instance paging zones cannot be part of a multi-site group.*
- *Multi-Site paging zones must be managed from a Connect premise server Allworx System Administration web page.*

Managing the paging configuration (i.e., base address and port, maximum hop count, and duration) is done the same way for both local Paging on Connect Vx instances and Paging on Connect premise servers.

For more information about setting *Paging* options, see "To manage the VoIP server:" on page 295. The *Paging Maximum Duration* should be set between 1 and 30 minutes.

17.1 Connecting Paging Amplifier / Door Release Relay

The Allworx premise server internal relay controls a door release mechanism. Users dial a phone extension (default: X403) for entry into a secured area. Connect premise servers have two relays to support a door release and a paging amplifier. The Allworx premise server comes with two sets of C-form relay contacts for connecting external devices to the rear terminal block. Only connect SELV circuits that meet IEC 60950-1, UL 60950-1, or NEC Class 2 circuits. Loop the bare wires of the external device to the corresponding screws on the terminal block and tighten the screws.

Notes:

- *For more information about relay physical connections, see the specific Allworx premise server installation guide available on the Allworx Portal (allworxportal.com).*
- *Allworx Connect Vx instances do not support Door Release Relay; however, similar functionality can be provided using third-party solutions.*

17.2 Paging with Remote Phones

Remote phones do not receive pages. Users can send pages from a remote phone, but do not hear the zoned or overhead pages. To enable paging to a remote phone, set up a VPN between the Allworx premise server and the remote phone. See "VoIP Server" on page 295 for more information.

Notes:

- *Paging is not available with the Connect Vx service.*
- *This document does not cover the configuration of the site firewall for a Connect premise server VPN because that configuration is dependent upon the many possible variations due to individual site requirements.*

17.3 Managing Paging Zones

Use the following procedures to change the paging zone name, manage the paging zone settings, or manage the paging zone operation on handsets. Individual phones can only be in four (4) paging zones at one time.

To change the paging zone name:

1. Log in to the Allworx System Administration web page and navigate to **Phone System** > **Paging**.

   Note: *The Allworx System Administration web page includes the Paging option; however, settings related to functionality not supported by Connect Vx are not displayed.*

2. Locate the *Paging Zone Names* pane and click **modify** to update the information:

Link	Description
Multi-Site Paging Groups	
Not Supported	Multi-Site paging groups are not supported by the Connect Vx service - no options are displayed in this area of the Allworx System Administration web page for Connect Vx instances.
Modify	Enter an updated description in the New Name field, and then click Update to save the change.
Delete	Deletes a multi-site paging group from any of the zones using the group. Click Delete to save the change.
Add new group	Enter a description in the *New Group Name* field, and then click Add to save the change.
Paging Zone Names	
Name	Click in the *Name* field and enter an updated description.
Prepage Tone	Click to select the check box to play a tone before the paging message starts. The system default tone is enabled (checked). Users placing a page hear a tone to indicate that the channel is open to begin speaking.
Multi-Site Group	Click to make a selection from the drop-down list to allow handsets to become part of paging zones that span multiple sites. For Multi-Site Paging, see the *Allworx Advanced Multi-Site User Guide* for more information. ***Note:*** *Not available for Connect Vx instances.*
* Extensions may vary per system. If using a non-default Internal Dial Plan, consult the *My Allworx Manager Phone Functions* tab to determine what extension to use for the corresponding feature.	

3. Click **Update** to save changes. Any changes to paging zone names require a reboot of all handset types. Otherwise, handsets with a PFK defined for those paging zones will not use the new name.

To manage Paging Zones on an Allworx handset:

By default, the system enables each applicable line out and handset for Paging Zone 0 and disables all others.

1. Log in to the Allworx System Administration web page and navigate to **Phone System** > **Paging**. Locate the *Paging Zones* pane.

2. Click **modify**. A table of handset users and *Paging Zones* displays.

3. Click to select the appropriate check boxes for each *Handset* and *Paging Zone* to enable features.

4. Click **Update** to save the changes. Any changes to paging zone names require a reboot of all handset types.

To manage the paging zone operation on handsets:

The Allworx administrator can enable or disable the Paging Zones on the handset configuration page. See “Handset Preference Group Settings” on page 122 for more information.

Click here to return to the Installing and Configuring Allworx Premise Servers or Configuring Connect Vx Instances .

Chapter 18 Roles

Prerequisites	
Access Permissions	Allworx Server Administrator Allworx System Administrator Phone Administrator role*
Feature Key Required	No

* Not all features on the *Roles* page are available to Phone Administrators. These features require Allworx Server Administrator or Allworx System Administrator permissions.

Roles assigns permission levels to users for delegating some of the administrative task management using the assigned Allworx user name and password.

See “Role Permissions” on page 200 for the administrative tasks and delegation permissions.

The following user roles are available.

- **Server Administrator**: Predefined system administrator with access to manage all functions of the premise servers and Connect Vx instances. The Allworx Server Administrator assigns roles, manages the server administrative functions, manages day-to-day phone system settings, manages the network and VoIP settings, and initiates system backups and/or restarts.
- **System Administrator**: Access to manage the administrative functions of the premise servers and Connect Vx instances. The user permission setting does not enable this role to change the password of the Allworx Server Administrator. However, the Allworx Server Administrator can change the password of the System Administrator.
- **Phone Administrator**: Access to manage day-to-day phone system settings including changes to system recordings as well as adding, changing, and deleting users, extensions, and handsets.
- **Network Administrator**: Access to manage the Network and VoIP settings, as well as SIP proxies and SIP gateways outside lines.
- **Support Technician**: Access to initiate system backups and restarts as well as managing logging operations.

Notes:

- *User roles assigned on the server can be active on every Allworx server in a multi-site network by selecting the appropriate option when assigning user roles. For more information, see “Managing Users” on page 225.*
- *The Allworx administrator can assign users to manage queue and Auto Attendant recordings. See “User Template Settings” on page 233 for more information.*
- *The Allworx administrator can assign users to manage individual queue settings or queue supervisor. See “User Template Settings” on page 233 for more information.*

18.1 Managing User Roles

To assign or remove user roles:

When changing the user role and the user is logged into the premise servers and Connect Vx instances, the user must log out and re-login in order to access the changes.

1. Log in to the Allworx System Administration web page and navigate to **Phone System** > **Roles**. The *Roles* page displays.
2. Locate the section of the role, and click the additional information arrow ►, if necessary**.** The Allworx System Administration web page displays a list of users assigned to each role.
3. Click one of the following actions:

Action	Description
show unassigned users	Displays a list of assigned and available users to assign.
hide unassigned users	Displays a list of assigned users.
Assign Role	Enable role permissions to the user account. Designated users have access to the administration functions that are included in the roles. See “Role Permissions” on page 200 for more information.
Remove Role	Remove the assigned role privileges the user account.

Note: *User roles are initially assigned when adding a user to the system. For more information, see “Managing Users” on page 225.*

18.2 Role Permissions

Each assigned user role has access to specific management tasks. Use the table to identify the administrative management access level of each User Role.

Allworx System Administration Web Page	Link	Phone	Network	Support
Home	Allworx Server Model Number	Yes	Yes	Yes
Home	Install Checklist	No	No	No
Home	Logout	Yes	Yes	Yes
Phone System				
Audit PIN Codes	Add new PIN Code - modify	Yes	No	No
	Ad PIN Codes from CSV filed	No	Yes	Yes

Continued

Allworx System Administration Web Page	Link	Phone	Network	Support
Audit PIN Codes	Download PIN Codes to CSV file	No	Yes	Yes
	Configuration - modify	Yes	No	No
	Delete	Yes	No	No
Auto Attendants	Auto Attendant n - modify	Yes	No	No
	reset	Yes	No	No
	copy	Yes	No	No
Business Information	modify	Yes	No	No
Call Park	System Park Settings - modify	Yes	No	No
	Multi-Site System Parking - modify	Yes	No	No
Call Queues / ACD	Manage the Custom Recordings played by Call Queues	Yes	No	No
	View and manage the Language settings for the Call Queues	No	No	No
	Call Queue n Modify	Yes	No	No
	Queue Streaming Settings - modify	Yes	No	No
	reset	Yes	No	No
	ACD Queue Busy Reasons - modify	Yes	No	No
	Queue Streaming Settings - modify	Yes	No	No
Conference Center	Conference X - modify	Yes	No	No
Dial Plan	Reboot Allworx handsets	Yes	No	No
	Internal Extension Length - modify	No	No	No
	Internal Dial Plan - modify	No	No	No
	Internal Dial Plan - see *Phone Functions Reference Card*	No	No	No
	DID Routing Configuration - modify	No	No	No
	External Dialing Rules > NANPA - modify	No	No	No
	External Dialing Rules > Area Code - modify	No	No	No
	External Dialing Rules > Automatic Route Selection - add new rule	No	No	No

Continued

Allworx System Administration Web Page	Link	Phone	Network	Support
Dial Plan *(continued)*	Modify	No	No	No
	Delete	No	No	No
	External Dialing Rules > Emergency - Modify (Emergency Number Rules)	No	No	No
	External Dialing Rules > Emergency Call Email Notifications are to - Modify	No	No	No
	Services > Modify	No	No	No
	Dialing Privileges Groups > View	Yes	No	No
	Copy	Yes	No	No
	Delete	Yes	No	No
	modify	Yes	No	No
	Toll Restriction - add	Yes	No	No
	Modify	Yes	No	No
	Call Appearances Assigned to Group > Modify	Yes	No	No
	Service Groups - add new Service Group	No	No	No
	Modify	No	No	No
	Copy	No	No	No
	Delete	No	No	No
Emergency CID	Emergency Caller ID Numbers - add new caller ID number	Yes	No	No
	Modify	Yes	No	No
	Delete	Yes	No	No
	Emergency Call Email Notifications	Yes	No	No
	Handset Emergency Caller ID Number Assignments > Send Test Email	Yes	No	No

Continued

Allworx System Administration Web Page	Link	Phone	Network	Support
Extensions	add new extension	Yes	No	No
	View call routes	Yes	No	No
	Delete	Yes	No	No
	<username>	Yes	No	No
	Bulk Edit	Yes	No	No
Handsets Analog Handsets	New Analog Handset	Yes	No	No
	Modify	Yes	No	No
	Delete	Yes	No	No
	Ring	Yes	No	No
SIP Handsets	Reboot Allworx Handsets	Yes	No	No
	add new Allworx Handset	Yes	No	No
	add new Allworx Reach Handset	Yes	No	No
	add new Generic SIP Handset	Yes	No	No
	Bulk Edit	Yes	No	No
	handset preference group	Yes	No	No
	View	Yes	No	No
	Copy	Yes	No	No
	Delete	Yes	No	No
	View Configuration	Yes	No	No
	Add Call Appearance	Yes	No	No
	Reboot	Yes	No	No
	Replace	Yes	No	No
	Modify	Yes	No	No
	Delete	Yes	No	No
	Ring	Yes	No	No

Continued

Allworx System Administration Web Page	Link	Phone	Network	Support
Handset Preference Groups	View	Yes	No	No
	Copy	Yes	No	No
	Delete	Yes	No	No
Handset Network Profile Templates	View	Yes	No	No
	Copy	Yes	No	No
	Delete	Yes	No	No
Handset Configuration Templates	Change	Yes	No	No
	Copy	Yes	No	No
	Delete	Yes	No	No
Languages	Manage the custom recordings	Yes	No	No
	Export Primary/Secondary Language Recordings	Yes	No	No
	Import Primary/Secondary Language Recordings	No	No	No
	Language Pack Installation and Removal	No	No	No
	Server Language Configuration	No	No	No
	Call Application Language Settings	No	No	No
Message Aliases	add new alias	Yes	No	No
	modify	Yes	No	No
	delete	Yes	No	No
Music on Hold	manage	Yes	No	No
	Usage	Yes	No	No
Outside Lines Analog CO Lines	Incoming Call Handling >modify	Yes	No	No
	new FXO line	Yes	No	No
	modify	Yes	No	No
	delete	Yes	No	No
	T1 Lines > modify	Yes	No	No

Continued

Allworx System Administration Web Page	Link	Phone	Network	Support
Direct Inward Dial Blocks	add new DID block	Yes	No	No
	modify	Yes	No	No
	delete	Yes	No	No
Direct Inward Dial Routing Plans	Details	Yes	No	No
	Delete	Yes	No	No
SIP Gateways	add new SIP Gateway	No	Yes	No
	modify	No	Yes	No
	delete	No	Yes	No
SIP Proxies	add new SIP Proxy	No	Yes	No
	modify	No	Yes	No
	delete	No	Yes	No
Paging	Paging Amplifier > modify	Yes	No	No
	Paging Zone Names > modify	Yes	No	No
	Paging Zones > modify	Yes	No	No
Public Contacts	add new Public Contact	Yes	No	No
	modify	Yes	No	No
	delete	Yes	No	No
Ring Groups	modify	Yes	No	No
Roles **Note:** *The site designation only appears for multi-site networks.*	System Administrator [Assign Role] [Remove Role] [site designation]	No	No	No
	Network Administrator [Assign Role] [Remove Role] [site designation]	No	No	No
	Phone Administrator [Assign Role] [Remove Role] [site designation]	Yes	No	No
	Support Technician [Assign Role] [Remove Role] [site designation]	No	No	No

Continued

Allworx System Administration Web Page	Link	Phone	Network	Support
Schedules	Greetings > modify	Yes	No	No
	Schedule n > Copy	Yes	No	No
	Schedule n > Delete	Yes	No	No
	Schedule n > modify	Yes	No	No
	Schedule n > add holiday	Yes	No	No
	Schedule n > copy holiday	Yes	No	No
	Schedule n > delete holiday	Yes	No	No
	Schedule n > modify holiday	Yes	No	No
Shared Appearance	add new Shared Call Appearance	Yes	No	No
	Modify	Yes	No	No
	Show Handsets	Yes	No	No
	Delete	Yes	No	No
Users (Click **more** to show additional links)	add new user	Yes	No	No
	add users from CSV file	Yes	No	No
	Modify	Yes	No	No
	Delete	Yes	No	No
	delete messages	Yes	No	No
	delete recordings	Yes	No	No
	Wipe remote devices	Yes	No	No
	Ext. <extension>	Yes	No	No
	Bulk Edit	Yes	No	No
	show/hide templates last applied to user	Yes	No	No
	User Templates > View	Yes	No	No
	User Templates > Copy	Yes	No	No
	User Templates > Delete	Yes	No	No
	Password Requirements > modify	No	No	No

Continued

Allworx System Administration Web Page	Link	Phone	Network	Support
Network				
Configuration	modify	No	Yes	No
Multi-Site	modify	No	No	No
	advanced	No	No	No
	handsets	No	No	No
	delete	No	No	No
	test	No	No	No
Port Expanders	add a port expander	No	Yes	No
	delete	No	Yes	No
	replace	No	Yes	No
	handsets	No	No	No
	outside lines	No	No	No
	px description view	No	Yes	No
	View > Modify	No	Yes	No
	View > Delete	No	Yes	No
	View > Replace	No	Yes	No
	View > Handsets	No	No	No
	Port Expander > Outside Lines	No	No	No
	View > Reboot	No	Yes	No
Static Routes	modify	No	Yes	No
VPN	modify	No	Yes	No
Servers				
DHCP	modify	No	Yes	No
	Active Leases	No	Yes	No
	Known Hosts	No	Yes	No

Continued

Allworx System Administration Web Page	Link	Phone	Network	Support
DNS	flush the cache	No	Yes	No
	modify	No	Yes	No
Email	manage the email queue	No	Yes	No
	modify	No	Yes	No
Reach	modify	No	Yes	No
SNMP	modify	No	Yes	No
VoIP	modify	Yes	Yes	No
Web	modify	No	Yes	No
Reports				
About		Yes	Yes	Yes
Allworx View	Allworx View Settings > modify	Yes	No	Yes
Auto Notification		No	No	No
Call Details	modify	Yes	No	Yes
	Completed Call Details Report			
	• delete	Yes	No	Yes
	• View Report	Yes	No	Yes
	• Export TSV Report	Yes	No	Yes
	• Export XML Report	Yes	No	Yes
Configuration	Generate XML Report	No	No	Yes
	View	No	No	Yes
T1 Lines	T1 Line n > Clear Report	No	Yes	Yes
	T1 Line n > Refresh Report	No	Yes	Yes
Live Calls	Refresh Now	No	No	Yes
Phones		No	No	Yes
Resource Summary	Check server compatibility	Yes	Yes	Yes

Continued

Allworx System Administration Web Page	Link	Phone	Network	Support
System Events	Download	No	No	Yes
	Show Severity Filter	No	No	Yes
Users	<username>	Yes	No	No
	Delete Messages	Yes	No	No
Maintenance				
Backup	modify	No	No	No
	Backup Now	Yes	Yes	Yes
Custom Recordings	File Export > File Naming Conventions	Yes	No	Yes
	Export	Yes	No	Yes
	File Import > Choose File	Yes	No	Yes
Feature Keys	Install	Yes	Yes	Yes
	Submit	Yes	Yes	Yes
	Reach	Yes	Yes	Yes
Feature Keys *(continued)*	Generic SIP Handsets	Yes	Yes	Yes
	Interact Professional	Yes	Yes	Yes
Import / Export	Export Configuration > Export	Yes	Yes	Yes
	Import Configuration > <Choose File>	No	No	No
	Import Configuration > Load	No	No	No
Notes	add or modify	Yes	Yes	Yes
Restart/Shutdown	Restart Now	Yes	Yes	Yes
	Restart Later	Yes	Yes	Yes
	[x] Restart Server	Yes	Yes	Yes
	[x] Restart Phones	Yes	Yes	Yes
Time	Modify	Yes	Yes	Yes

Continued

Allworx System Administration Web Page	Link	Phone	Network	Support
Tools	Network Diagnostics	Yes	Yes	Yes
	Syslog - System Events	Yes	Yes	Yes
	Allworx Technical Support Server	Yes	Yes	Yes
	Advanced Troubleshooting:	Yes	Yes	Yes
	• Network Address Translation (NAT) Information	Yes	Yes	Yes
	• Four Wire Return Loss Measurements	Yes	Yes	Yes
	• Network Device Monitoring	Yes	Yes	Yes
	• Packet Capture Tool	Yes	Yes	Yes
	• SSH	Yes	Yes	Yes
	• Advanced Diagnostic Logging	Yes	Yes	Yes
	• Echo Cancellation Diagnostics	Yes	Yes	Yes
	• RPC Diagnostics	Yes	Yes	Yes
	• Performance Monitoring	Yes	Yes	Yes
Update		No	No	No

Click here to return to the Installing and Configuring Allworx Premise Servers or Configuring Connect Vx Instances .

Chapter 19 Public Contacts

A common set of contacts referencing any person or company managed by the Allworx Server Administrator and are available as read-only contacts to all Allworx users. The Public Contacts are available when users press the Verge phone series Contact function button, the 92xx IP phone function, or dial the assigned speed dial number.

Prerequisites	
Access Permissions	Allworx Server Administrator Allworx System Administrator Phone Administrator role
Feature Key Required	No

When adding a Public Contact, the limitations include the following:

- Each Public Contact stores one phone number labeled as **Work**
- The maximum number of Public Contacts is up to 1,015 – depending on the dial plan
- Only Allworx users can tag the Public Contact as a favorite – available on Verge phones, Reach, and Interact only

To manage a Public Contact number:

1. Log in to the Allworx System Administration web page and navigate to **Phone System** > **Public Contacts**.
2. Click one of the following links (requires only a phone number to add a new contact):

add new Contact	Create a Public Contact number: 1. Select a Speed Dial Number from the drop-down list. 2. Enter the names/description in the appropriate fields, if applicable, including extension 403 (Door Relay), if connected and configured. 3. Enter a the contact phone number in the Phone Number field. Follow the TIP on the page for additional information. 4. Click **Add** to save the change. ***Note:*** *Images for public contacts cannot be added from this screen. After the contact is added, click* ***modify*** *as described further in this table to make changes to the information and add an image.*
add Contacts from CSV file	Add Public Contacts with a Comma Separated Value (CSV) file. 1. Create a CSV file using any text editor or Microsoft Excel with the Phone Number, Speed #, Prefix, First Name, Middle Name, Last Name, Nick Name, Suffix, Organization attributes. The Allworx premise servers and Connect Vx instances automatically match the column types when the CSV file contains the values (exact matches) as column headings in the first row of the CSV file. Required attributes (columns): Phone Number. *Continued*

add Contacts from CSV file

(continued))

Example: CSV file content - the first row is the header and the next two are Public Contact import data:

Phone Number	Speed #	Prefix	First Name	Middle Name	Last Name	Suffix	Organization
9P1P5851234567	350	Mr	John	C	Doe	Jr	Acme Corp
15851234568	351						Widgets Inc

2. Click **Choose File**. Locate the file and click **Open** > **Load** > **Process.**
3. (Optional) Click the **Speed # length** drop-down arrow to select the Speed Dial number of digits.
4. (Optional) Check the box to **Skip records with an existing Speed #**. This is useful to avoid overwriting speed dial numbers.
5. Verify the column heading represents the data supplied. Use the drop-down list to assign the column headings. To exclude a column, select a heading value of **Skip**.
6. Review the rows to add. Uncheck a row to exclude it from the import.
7. Click **Add** to import the users. A message displays indicating the number of Public Contacts successfully added and/or which Public Contacts were skipped during the import. Additional details about skipped Public Contacts numbers may be available in the system events log.
8. Click **Done** to return to the Public Contacts List or **Continue** to repeat this process.

Note: *The Allworx system will not import any record from the data set that is missing required values or cannot be read by the Allworx system. Maximum field length is 1,024 characters and maximum line length is 2,048 characters for each line in the CSV file.*

Modify

Update any of the Public Contact information fields or drag and drop a new JPG or PNG image into the Contact Photo area. To clear the photo, click the **remove** link.

Click **Update** to save the change.

Note: *The Speed Dial Number can not be edited.*

Delete

Remove the public contact from the list.

To delete multiple Public Contacts:

1. Click the **Bulk Edit** additional information arrow ▶.
2. Click to select the check box to the left of the public contact.
3. Click **Delete**.
4. Click **Confirm** in the verification message to delete all of the selected contacts, or click **Cancel** to ignore the request.

Click here to return to the Installing and Configuring Allworx Premise Servers or Configuring Connect Vx Instances .

Chapter 20 Ring Groups

Prerequisites	
Access Permissions	Allworx Server Administrator Allworx System Administrator Phone Administrator role
Feature Key Required	No

The *Ring Groups* (formerly known as Call Monitors) are call routing destinations that enable ringing one call to multiple phones and multiple calls to a single Ring Group. Calls are answered in first in, first out order.

Ring Groups Features:

- Up to 10 available Ring Groups (numbered 0 through 9)
- Ring Group configuration
- Ring multiple Allworx IP phones on the system with a single call
- Stack multiple ringing calls to a single Ring Group extension
- Configure Allworx handsets for multiple Ring Groups
- Configure Allworx handsets for multiple occurrences of the same Ring Group

To configure calls to route to the Ring Group, see “Managing Call Routes” on page 97 for information about setting up Call Routes — assign an extension to the Ring Group, and then configure the incoming call routing to go to the Ring Group extension.

To configure calls to route to an Auto Attendant, see “Auto Attendants” on page 37 for more information.

To configure a Ring Group PFK, see “Managing the Programmable Function Keys (PFKs)” on page 138 for more information.

To modify the description of the Ring Group:

1. Log in to the Allworx System Administration web page and navigate to **Phone System** > **Ring Groups**.
2. Click **modify**.
3. Enter a new ring group description in the *Description* field.

   Note: *If you change the description of a ring group, any handsets (including Verge phones) with a PFK defined for that ring group will not use the new description until the handset has been rebooted.*
4. Click **Update** to save the changes. Click **Cancel** to ignore the request.

Click here to return to the Installing and Configuring Allworx Premise Servers or Configuring Connect Vx Instances .

Chapter 21 Schedules

Prerequisites	
Access Permissions	Allworx Server Administrator Allworx System Administrator Phone Administrator role
Feature Key Required	No

The *Schedules* page provides settings to play the appropriate greetings of the Auto Attendants based on the time of day, and switching between open and closed modes for call routes of system extensions automatically or manually.

The Allworx administrator can define multiple schedules and configure each system extension or Auto Attendant to follow any one of the defined schedules. A schedule consists of defined daily periods, associated open/closed modes, and Auto Attendant greeting names. The Auto Attendant plays the schedule greeting first, and then plays the custom message.

Note: *If a schedule is set for manual mode, the setting for Schedule Mode (DayNight) and associated greeting number do not persist following a reboot. When a premise server or Connect Vx instance boots, the mode and greeting number is set according to the automatic schedule, and then if previously configured as such, the premise server or Connect Vx instance restores the mode to manual.*

To assign a schedule to an Auto Attendant, see “Configuring the Auto Attendant” on page 37 for more information.

21.1 Managing the Greetings

Each business schedule can use up to nine (9) different greetings. The greetings numbers are 0 – 8.

- Greeting 0: Fixed description of **Open**
- Greeting 1: Fixed description of **Closed**
- Greetings 2 through 8: A unique, customer-defined greeting name for each greeting used on the Auto Attendants on the Allworx *premise server or Connect Vx instance*

To manage the greeting names:

1. Log in to the Allworx System Administration web page and navigate to **Phone System** > **Schedules**.
2. Locate the Schedule and click **Show Greeting Names for this schedule**.
3. Click **modify** and enter the new name in the field.
4. Click **Update** to save the changes.

21.2 Managing the Schedules

Use the following procedures to manage the schedules and settings as well as assign the schedules.

Allworx users with Phone Administrator or System Administrator permissions can call into the Allworx System Audio Message Center and use the prompts to navigate to and override the current day/night mode and/or greeting for a Schedule. This enables these Allworx users that cannot make it to the site facility (such as in the case of inclement weather) to control the mode and greetings remotely. After making the necessary changes to the schedule mode, incoming calls route according to the configured mode immediately.

To manage the schedules:

1. Log in to the Allworx System Administration web page and navigate to **Phone System** > **Schedules**.
2. Locate the schedule to manage and click on of the following actions:

Action	Description
▶	Displays additional information and enables modifying the current schedule. See “To modify the schedule using the Allworx System Software:” on page 216 for more information.
modify	Open the schedule so that the parameters (Start, End, Mode, Greeting) can be updated, and periods can be added.
Copy	Duplicates the current schedule. The new schedule name is Schedule <number>: Copy of schedule <number>.
Delete	Removes the schedule.

3. Click **Update** to save the changes.

To modify the schedule using the Allworx System Software:

The purpose of a schedule is to change modes/greetings automatically, based on the Allworx premise server or Connect Vx instance clock. It is possible to disable the automatic control to change the modes/greetings manually.

At installation, the Allworx system defines the following schedules:

- Schedule 0 (open) - The Open default is Monday through Friday, 8:00 – 5:00 and assigns greeting 0. Users can modify but cannot delete this schedule.
- All other hours as Closed and uses greeting 1. Users can modify the schedule time and add schedules to accommodate business needs.

1. Log in to the Allworx System Administration web page, navigate to **Phone System** > **Schedules.**
2. Click the additional information arrow ▶ and locate the schedule to configure.

3. Click one of the following actions:

<table>
<tr><th>Action</th><th>Description</th></tr>
<tr><td><b>Show Greeting Names for this schedule</b></td><td>Displays the Open, Closed, and custom greeting names associated with the schedule.</td></tr>
<tr><td><b>Show resources using this schedule</b></td><td>Displays the Users, System Extensions, Dialing Privileges Groups, and Auto Attendants associated with the schedule.</td></tr>
<tr><td><b>Description: Mode/Greeting Control:</b></td><td>Change the schedule name and toggling between automatic or manual greeting control. If selecting the Manual schedule, users must set the mode/greeting via the handset Schedule PFK.
1. Click <b>modify</b>, and then enter a new name in the description field.
2. Locate the <i>Mode/Greeting Control</i> and select an option from the drop-down list.
<table>
<tr><td><i>Automatic</i></td><td>Sets the mode/greeting automatically by the server according to the schedule.</td></tr>
<tr><td><i>Manual</i></td><td>Sets the mode/greeting by the handset schedule PFK. To change: the user of the handset can press the PFK to set the mode and greeting. See “Managing the Programmable Function Keys (PFKs)” on page 138 for more information.
<b><i>Note</i></b><i>: Even if configuring the schedule for automatic control, use a schedule PFK to override the current mode/greeting. If overridden, control of the mode/greeting returns to the schedule when the next defined time period begins.</i></td></tr>
</table>
3. Click <b>Update</b> to save the change.</td></tr>
<tr><td><b>Schedule is currently set to</b> &lt;Mode&gt;<b>:</b></td><td>Change the schedule mode and greeting to use. If selecting the Automatic Schedule, a daily calendar opens to assign Start, End, Mode, and Greeting requirements, see “Managing the Greetings” on page 215.
To update this information:
1. Click <b>modify</b>.
2. Click <b>Mode</b> and select an option (day or night) from the drop-down list.
3. Click <b>Greeting</b> and select an option from the drop-down list (see “Managing the Greetings” on page 215 for more information).
4. Click <b>Update</b> to save the change.

<i>Continued</i></td></tr>
</table>

Action	Description
<day of week>	Available only with **Automatic** mode. Specify a schedule for each day of the week and assigning a greeting to use for each time period. To manage the time schedule and greetings: 1. Click **modify.** Click: **add period** (Optional) Enter specific start and end time times to the daily schedule. **delete** Removes the time period from the schedule. 2. Locate the **Mode** column and select an option from the drop-down list. 3. Locate the **Greeting** column and select an option from the drop-down list. 4. Click **Update** to save the changes. To save steps modify one day and copy the changes to other days within the same schedule. Click **copy** and select the days that use the same periods.
Holidays	Available only with **Automatic** mode. To add a holiday to the schedule: 1. Click **add holiday**. 2. Locate the newly added holiday and click **modify**. 3. Enter the dates for the holiday. 4. Check the repeat yearly to enable. 5. (Optional) Click **add period** to enter specific start and end time periods to the holiday schedule. 6. Click **Update** to save the changes. To duplicate a holiday schedule: Copy all of the holidays from one schedule to other schedules. This is useful when setting up holidays with new dates for a new year if several defined schedules are available. 1. Click **copy holidays**. 2. Check the box(es) to use the currently selected holiday. 3. Click **Copy** to save the changes.
copy	Duplicate the current schedule. The new schedule name is Schedule <number>: Copy of schedule <number>. Schedule is available to modify.
delete	Remove the current schedule from list. Requires no further action.

To modify the Schedule mode/ greeting remotely:

Note: *To modify the mode/greeting for a schedule, the user (not the administrator) must have Allworx System Administrator or Allworx Phone Administrator role permissions.*

1. Call the Auto Attendant from an outside line, and then do one of the following:
   - Dial 6[1] + the primary extension.
   - Dial 404[1]. The system prompts users for a primary extension.
   - (from an outside line dialing directly to your office) While the greeting is playing, dial 6[2] + primary extension before the greeting finishes playing.
2. Log in using the assigned extension and PIN code.
3. Press 8 to manage schedules.
4. Wait for the prompt: “Enter the number of the schedule you wish to manage followed by the pound sign”, and then enter a schedule number.

   The Message Center responds with “Schedule <number> is set to <mode type> mode, greeting <number>.
5. Select one of the following options:
   - Enter the new greeting number to play.
   - Press 9 to change the mode.
   - Press # to return to the previous menu to manage other Schedules.
   - Press * to listen to the choices again.
6. Hang up after updating the required Schedules.

Click here to return to the Installing and Configuring Allworx Premise Servers or Configuring Connect Vx Instances .

[1] Extensions may vary per system. If using a non-default Internal Dial Plan, consult the My Allworx Manager Phone Functions tab to determine what extensions to use for the corresponding feature.

[2] Extensions may vary per system. If using a non-default Internal Dial Plan, consult the My Allworx Manager Phone Functions tab to determine what extensions to use for the corresponding feature.

Chapter 22 Shared Call Appearance

Prerequisites	
Access Permissions	Allworx Server Administrator Allworx System Administrator Phone Administrator role
Feature Key Required	No

Shared Call Appearance shares a set of one or more PFKs across multiple handsets. All handsets in a Shared Appearance have common access to calls within the group of handsets.

Example:

An incoming call rings on all handsets with the Shared Call Appearance.

- One user answers and places a call on hold.
- Another user retrieves a call the first user placed on hold.

There are two cases for Shared Call Appearances:

- **Call Group** – Users with similar business needs or tasks assigned to a group can answer any calls to the group shared appearance. A handset can place the call on hold and another handset can retrieve the call.
- **Executive/Assistant Arrangement** – An appearance exists on the handsets of both an executive and assistant. The assistant answers the calls to the executive and places the caller on hold for the executive to pick up. The assistant always displays the state of all calls on the executive's handset.

Notes:

- *9202E and Reach handsets do not support the use of Shared Call Appearances.*
- *The Shared Call Appearances feature does not support the call forwarding (45+<extension>) function, nor can calls be forwarded to phones at different sites within a Multi-Site network.*

For more information about placing a call on hold using the Call Shared Appearance, see the appropriate phone user guide. Shared Call Appearances support three distinct types of hold behavior.

Hold Behavior	Description
Public Hold (Verge phone) Shared Hold (92xx IP phone)	Any handset using the Shared Call Appearance can retrieve the call on hold. • To place the active Shared Call Appearance phone call on hold: Verge phone press the **Public** soft key, and 92xx IP phone press the HOLD key. On either phone placing the call into the hold state, the LED flashes slow, green on all phones of the Shared Call Appearance; including the phone used to place the call on hold. • All handsets in the Shared Call Appearance can retrieve the held call. • The system delivers a Hold Reminder to the handset that placed the call on hold in the Shared Call Appearance per the individual phone setting. ***Note:*** *Allworx system software does not support including a call on a shared hold during phone-hosted conferences.* *Continued*

Hold Behavior	Description
Privacy Hold	Only the handset that placed the call on hold can retrieve the call. • To place the call on “privacy” hold: Verge phone press the HOLD function button, and 92xx IP phone quickly press the HOLD function button twice. On either phone placing the call into the hold state, the phone has a fast, alternating green and red LED. • The LED for all other handsets in the Shared Call Appearance become solid red for the Shared Call Appearance line. • If the user does not pick up the call, the phone receives a notification per the phone HOLD reminder settings.
Bridged Hold	The handset placing the call on hold and one other handset with the same Shared Call Appearance can retrieve the call. • To place the call on “Bridged Hold”: • Verge phone: press the **bridge** soft key or the **Intercom** function button. Then dial the second phone number. • 92xx IP phone: place an intercom call to the handset within the same Shared Call Appearance. • The second handset can select the flashing Shared Call Appearance PFK to resume the held call. • If neither party resumes the call, the handset placing the call on hold receives a notification per the individual HOLD reminder settings.

22.1 Setup Checklist

Follow the order of the steps to successfully setup the Shared Call Appearance. Click the link in the column on the right to see more information.

Step	Description	More Information
1	Add a new Shared Call Appearance.	“Managing Shared Call Appearances” on page 222
2	Modify the Shared Call Appearance information, as necessary.	
3	Assign the Shared Call Appearance programmable function keys (PFKs).	“Assigning Shared Call Appearance Programmable Function Keys (PFKs)” on page 224
4	Define the call routes.	“Managing Call Routes” on page 97

22.2 Managing Shared Call Appearances

The Shared Call Appearance has all the attributes assigned to a normal call appearance (Caller ID, hold music, etc.). Outbound Caller ID is common for all outbound calls on a given Shared Call Appearance. If deleting a Shared Call Appearance, the premise server or Connect Vx instance removes it from all handsets.

To manage a Shared Call Appearance:

1. Log in to the Allworx System Administration web page and navigate to **Phone System** > **Shared Appearances**.

2. Click one of the following actions:

<table>
<tr><th>Action</th><th>Description</th></tr>
<tr><td><b>add new Shared Call Appearance</b></td><td>1. Update the Description field and the Number of Lines field (number of PFKS assigned to the phone).
2. Click <b>Add</b> to save the change.</td></tr>
<tr><td><b>Show Handsets</b></td><td>Display the handsets assigned to the Shared Call Appearance. Click <b>Close</b> when complete.</td></tr>
<tr><td><b>Modify</b></td><td>1. Update the <i>Description</i> field and then update the information.
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td><i>Number of Lines</i></td><td>The Number of Lines is not available for change as this affects the number of PFKs on all phones, rendering some phones unable to support the Shared Call Appearance feature.</td></tr>
<tr><td><i>Owner</i></td><td>Select an available option from the drop-down list.</td></tr>
<tr><td><i>Internal Caller ID</i></td><td>Enter up to 47 characters.
<b><i>Note:</i></b> <i>When a call is received from a number that matches a phone number listed in the user’s Contacts, the Contact information is used as the Caller ID.</i></td></tr>
<tr><td><i>Internal Caller ID Number</i></td><td>Select an available option from the drop-down list.</td></tr>
<tr><td><i>External Caller ID Name</i></td><td>Enter up to 47 characters.</td></tr>
<tr><td><i>External Caller ID Number</i></td><td>Enter up to 24characters.</td></tr>
<tr><td><i>Emergency Caller ID Number</i></td><td>Select an available option from the drop-down list.</td></tr>
<tr><td><i>Dialing Privileges Group</i></td><td>Select an available option from the drop-down list.</td></tr>
<tr><td><i>Hold Music Selection</i></td><td>Select an available option from the drop-down list.</td></tr>
<tr><td><i>Can Place Calls</i></td><td>Click the box to enable placing outgoing calls.</td></tr>
</table>
2. Click <b>Update</b> to save the change.</td></tr>
<tr><td><b>Delete</b></td><td>Verify the Shared Call Appearance and click <b>OK</b> to delete it. Reboot all affected phones to remove the Programmable Function Key.</td></tr>
</table>

22.3 Assigning Shared Call Appearance Programmable Function Keys (PFKs)

When assigning a Shared Call Appearance PFK to a handset, the system assigns consecutive PFKs for each Shared Call Appearance line. The Allworx system notifies the Allworx administrator when:

- There are not enough consecutive PFKs available and the PFK assignment fails.
- The Shared Call Appearance PFK assignment would overwrite existing PFKs.The Allworx administrator can choose to cancel the operation.

After the premise server or Connect Vx instance allocates consecutive PFKs for all the lines in the Shared Appearance, the Allworx administrator can move the lines to other PFKs within the constraints of the handset model.

- If replacing a phone that is using a Shared Call Appearance, the replacement phone automatically shares the Shared Call Appearance.
- If the handset has enough PFKs available to accommodate all Shared Call Appearance lines.
- If the handset does not have enough PFKs available, the Allworx system notifies the Allworx administrator, and the handset replacement finishes without adding the Shared Call Appearance to the new handset.

To assign a Shared Call Appearance PFK, see “Managing the Programmable Function Keys (PFKs)” on page 138 for more information.

22.4 Defining Call Routes

Each defined Shared Call Appearance is selectable as a destination in any extension call route. For more information, see “Managing Call Routes” on page 97. In multi-site networks, Allworx administrators can map defined Shared Call Appearances on one site to other sites to use as destinations in the other site call routes.

Click here to return to the Installing and Configuring Allworx Premise Servers or Configuring Connect Vx Instances .

Chapter 23 Users

Prerequisites	
Access Permissions	Allworx Server Administrator Allworx System Administrator Phone Administrator role
Feature Key Required	No

The *Users* page is used to add users and user templates, delete email and/or Voicemail messages, delete recordings of the user name and/or presence greetings, wipe remote devices, and manage password requirements.

The *Name* area for each user displays a red dot (●) next to each user that has not recorded their name in the Message Center.

The user template contains a set of common configuration settings to apply when creating or modifying users, but this template does not include all user settings. Some configuration settings are available at **<user>** > **modify**.

The *System User (Default) Template* contains the factory default settings. For best results create a custom template (optional) and then apply that custom template or the default System User Template when adding new users.

23.1 Setup Checklist

Follow the order of the steps to successfully set up the users. Click the links in the column on the right for more information about each step.

Step	Description	More Information
1	Add a new or modify the user template.	"Managing User Templates" on page 232
2	Add a new user.	"To add a new user:" on page 226
3	Configure or update the password requirements.	"Defining Password Requirements" on page 241

23.2 Managing Users

Use the following procedures to show or hide the template applied to each user, add a new user, and modify or delete existing users.

To show or hide the template applied to each user:

1. Log in to the Allworx System Administration web page and navigate to **Phone System** > **Users**.
2. Locate the *Users* pane, and click the additional information arrow ▶, if necessary.
3. Click the ***show*** *or* ***hide*** *templates last applied to user* to view or conceal the user template applied to each user. An exclamation point (!) indicates a template override.

To add a new user:

Note: *After increasing the internal extension length to 5 or 6 digits, the extensions* ***show available*** *link is not available.*

1. Log in to the Allworx System Administration web page and navigate to **Phone System** > **Users**.

2. Locate the *Users* pane and click the additional information arrow ►, if necessary. Click one of the following actions:

<table>
<tr><th>Action</th><th>Description</th></tr>
<tr><td><b>add new user</b></td><td>Add users one at a time.
1. Update the user settings. See “User Settings” on page 229 for more information.
2. Click <b>Add</b> to save the user. The users table displays the last applied template to each user.</td></tr>
<tr><td><b>Add users from CSV file</b></td><td>Import multiple users with a Comma Separated Value (CSV) file.
1. (Recommended) Perform a full system backup before adding multiple users.
2. Create a CSV file using any text editor or Microsoft Excel and any combination of required and optional attributes. Required attributes (columns): Login Name, Last Name
The Allworx premise server or Connect Vx instance automatically matches the column types when the CSV file contains the values (exact matches) as column headings in the first row of the CSV file.
<b>Example of CSV content only (Header Title must be at TOP of column).</b>
<table>
<tr><th>Header Title</th><th>Content Example</th></tr>
<tr><td>Login Name</td><td>ARader</td></tr>
<tr><td>Last Name</td><td>Rader</td></tr>
<tr><td>First Name</td><td>Alice</td></tr>
<tr><td>Middle Name</td><td>B</td></tr>
<tr><td>Extension[1]</td><td>1008</td></tr>
<tr><td>Phone[2]</td><td>9308 (model number)</td></tr>
<tr><td>Msg Alias[3]</td><td>ARader, group@widgetsinc.com</td></tr>
<tr><td>DID Number[4]</td><td>5855551212</td></tr>
<tr><td>DID DNIS Name[5]</td><td>AliceRader</td></tr>
<tr><td>DID Prompt Language[5]</td><td>Primary
Secondary</td></tr>
</table>
</td></tr>
</table>

Continued

Action	Description
Add users from CSV file *(continued)*	[1] If the extension is not included, the server uses the first available extension. [2] If using Phone, include the phone serial number or the phone model. The server will create a phone and assign to the user when the phone serial number is included. The server will assign the user to an existing unassigned phone of the specified model when the phone model is included. The server sets the In Office call route for the user to ring the phone four times then go to the user's Voicemail when it assigns a phone to the user. The server supports the following phone models in the Phone field: 9102, 9112, 9202, 9202E, 9204, 9204G, 9212, 9212L, 9224, 9304, 9308, 9312 [3] If using Msg Alias, include the Login Name (as shown in the table above) as part of the Msg Alias field when saving a copy of the message on the server. [4] Requires a DID block in place on the Allworx System before importing users with DID numbers from a CSV file. [5] If the DID DNIS Name or DID Prompt Language parameters are not supplied in the CSV file, the Allworx system uses the values from the DID Routing Plan for the DID Number. 3. Click **Choose File**. Locate the file and click **Open** > **Load** > **Process**. 4. (Optional) Enter a PIN and Password for the users. These values are for all records added. If not supplied, the user's password defaults to the Login Name specified during the add. 5. (Optional) Check the box to enable the **Require Password Change** or **Require PIN Change** setting at the next user login. 6. (Optional) Check the box to **Skip records with a Login Name that already exists**. This is useful to avoid overwriting existing users. User names are case sensitive; therefore, JYoung and Jyoung are separate login IDs. 7. Select the template for user settings from the drop-down list. 8. Verify the column heading represents the data supplied. Use the drop-down list to assign the column headings. To not include a column, select a heading value of **Skip**. 9. Review the rows to add. Uncheck a row to exclude it from the import. 10. Click **Add** to import the users. A message displays indicating the number of users successfully added and/or which users were skipped while adding the new users. Additional details about skipped users may be available in the system events log. 11. Click **Done** to return to the User List or **Continue** to repeat this process. ***Note:*** *The Allworx system will not import any user record from the data set that is missing required values, cannot be parsed, or is conflicting with a user currently defined on the system, specifically matching login name, extension, or first, middle, and last name. The maximum field length is 1,024 characters and the maximum line length is 2,048 characters for each line in the CSV file.*

To modify or delete existing users:

When modifying templates already applied to users, changes are NOT automatically applied to the users. To update the user settings, reapply the template to each associated user.

1. Log in to the Allworx System Administration web page and navigate to **Phone System** > **Users** and locate the *Users* pane. Click the additional information arrow ▶, if necessary**.**

2. Select on of the following actions:

Action	Description
▶ **Bulk Edit**	Performs the same change on multiple users, check the box on the left of the appropriate user names. Click the Select Bulk Edit operation drop-down and select an option from the list. • Assign schedule to selected users • Copy User Template settings to the selected users • Delete the contact image for the selected users • Delete the contacts for the selected users • Delete the messages for the selected users • Delete the recordings for the selected users • Delete the selected users • Manage Call Answering Menu Options • Manage the PIN for the selected users • Manage the password for the selected users • Set the permission for selected users to manage their contact image ***Note:*** *Select at least one user, otherwise an error message displays.*
<extension number>	Modify the call routes for the user. See “Managing Call Routes” on page 97 for more information.
Modify	The add new user options and user template options display. To modify the user settings: 1. Click **Modify**, and update the options, as appropriate. See “User Settings” on page 229 and “User Template Settings” on page 233 for more information on the user template options. 2. (Optional) Locate the *User Template* pane and select a new User Template from the drop-down list. Click **Set** to apply all the settings to the user or click **Merge** to apply the settings of the new template while keeping the override settings. Merge does not change any override settings from the last applied template. 3. Click **Update** to save the changes.

Continued

Action	Description
Delete	The premise server or Connect Vx instance removes the user from the list, and the page refreshes with existing users. 1. Locate the user in the *Users* list and click **Delete** in the *Action* column for the appropriate user. Read the pop-up message and confirm this is the user to remove from the business directory. 2. Click **Delete** to remove the user from the list or **Cancel** to disregard the change.
📄	Displays the *Welcome to Allworx* page specific to the user. Copy and paste this information into an email window and send to the user.

User Settings

<table>
<tr><th colspan="2">Identification</th></tr>
<tr><td><i>Login Name</i></td><td>Identify a user name for the new user to log in to My Allworx Manager or other Allworx applications.</td></tr>
<tr><td><i>Full Name</i></td><td>Enter the first, middle, and last name of the new user, per company requirements.</td></tr>
<tr><td><i>Password</i></td><td>Identify a password for the new user to log in to My Allworx Manager or other Allworx applications.
<table>
<tr><td>Password</td><td>The password must contain 4 to 128 characters and comply with the password requirements.</td></tr>
<tr><td>PIN</td><td>Default keypad PIN code: 1234. The new PIN must contain 4 to 16 numeric characters.</td></tr>
</table>
If the user is set up prior to upgrading the premise server or Connect Vx instance, the default PIN code is the same PIN code prior to the upgrade.</td></tr>
<tr><td><i>Confirm Password</i></td><td>Reenter the password for the new user. This step verifies the passwords match.</td></tr>
<tr><td><i>Require Password Change</i></td><td>Enable the user to log in once with the provided password. After a successful log in, the user must change the password.</td></tr>
<tr><td><i>PIN</i></td><td>Used to log in to the Allworx system from a phone keypad, e.g., access Voicemail messages or log in to a ACD queue as an agent.</td></tr>
<tr><td><i>Confirm PIN</i></td><td>Reenter the PIN for the new user. This step verifies the PINs match.</td></tr>
<tr><td><i>Require PIN Change</i></td><td>Enable the user to log in once with the provided PIN. After a successful log in, the user must change the PIN.</td></tr>
<tr><td><i>Primary Extension</i></td><td>Display the next available extension. To select a different extension: click <b>show available</b>, and then select an available extension number.
<b><i>Note:</i></b> <i>After increasing the internal extension length to 5 or 6 digits, the extensions <b>show available</b> link is no longer available.</i></td></tr>
<tr><td><i>Contact Photo</i></td><td>View, add, change, zoom, reposition, or remove the current contact directory image. When adding or changing an image, drag and drop a new JPG or PNG image from a file explorer window into the area provided.
To clear the image, click <b>Remove</b> located beneath the graphic.</td></tr>
</table>

Continued

New User Options - only applies when adding a new user.	
Assign Phone	Click the drop-down arrow and select a Phone Assignment option.
Assign DID Number	Click the drop-down arrow and select a DID Number option. Applies to the DID Routing Plan phone number to extension mapping.
Presence	Select the user presence. Options include: • In Office • At A Meeting • On Vacation • On Business Trip • At Home • Away • Busy
Roles	Click to select a check box to assign additional administrative functionality to the user. See “Managing User Roles” on page 200 for more information about the responsibilities assigned to each role. Selecting the first check box (*User has these roles on all sites in a Multi-Site configuration*) allows the user’s roles to be active on every Allworx server in a multi-site network. The default setting is to have this check box unchecked. ***Notes:*** • *Users with roles from remote sites are included on the primary server Roles page. The Assign Role and Remote Role buttons is replaced with an indicator of the site name. For more information, see “Managing User Roles” on page 200.* • *To assign users to manage queue and Auto Attendant recordings, or to manage individual queue settings or queue supervisor see “User Template Settings” on page 233 for more information.*
User Template	Select the template to use for the settings. Select an option from the drop-down list. Click **Set** to update the user settings or **Merge** to import the user settings (keeps current setting overrides).

When updating the remaining sections on the user page, see “User Template Settings” on page 233 for more information. An exclamation point (!) indicates a template override.

23.3 Deleting User Messages, Recordings, Contacts, or Contact Images

Deleting the user email, Voicemail messages/recordings, personal contacts, and/or a contact image permanently removes the data from the Allworx server.

1. Log in to the Allworx System Administration web page and navigate to **Phone System** > **Users**. Locate the *Users* pane and click the additional information arrow ►, if necessary**.**

2. Locate the username, click **more**, and then click an action:

Action	Description
Delete messages	Select one email and one Voicemail option to Delete. Options include: • Delete all emails • Delete all read emails • Keep all emails • Delete all Voicemail • Delete all saved Voicemails • Keep all Voicemails
Delete recordings	Select the recording type to delete. Options include: • User's name and all of the user's Presence greetings • All of the user's Presence greetings • User's name
Delete contacts	Remove all the user's Personal Contacts from the premise server or Connect Vx instance. Any Verge series phones with PFKs assigned to the deleted contacts change to **Unassigned**.
Delete contact image	Remove the Allworx User's directory contact image.
View contacts info	View a summary of the user's contact source accounts, and counts of the user's personal contacts and the associated images.
Wipe remote devices	Wipe information from the user's remote devices. The user's password must be changed in order to wipe their remote deices. The current password will be remembered by the premise server or Connect Vx instance. When a remote device attempts to login using the current password, the remote device will be instructed to wipe the user's data.

3. Click **Delete** to save the changes.

23.4 Viewing Contacts Info

View the Allworx user's personal contact information - source account, premise server or Connect Vx instance storage, number of contacts, and number of contact images stored on the Allworx premise server or Connect Vx instance. This drop-box is for information only, there are no editable options available.

1. Log in to the Allworx System Administration web page and navigate to **Phone System** > **Users**. Locate the **Users** pane and click the additional information arrow ▶, if necessary**.**

2. Locate the user name, click **more...** in the *Action* column, and then click **View Contacts Info**. The table displays:
   - **Source Account** - Device or application used to create the Personal Contact
   - **Server Storage** - Contacts and/or images stored on the premise server or Connect Vx instance

   Additionally, the drop-box displays the number of stored contacts and images.

3. Click **Close** to return the drop-down box to the original position.

23.5 Wiping Existing User Remote Devices

The Wipe command removes the following information from a lost or stolen remote device:

Application	Login Credentials*	Contact Information	Voicemail Information	Configuration (including backup settings)
Reach	✓	✓	✓	
Interact including Interact Softphone	✓	✓		✓

* Requires the Allworx administrator to change the user password, which restarts the Reach application and Terminates the Interact application.

- Device user must re-log in entering the credentials and using the new password.
- Reach users must reclaim a new license to restore the Voicemail information and to send/receive calls.

1. Log in to the Allworx System Administration web page and navigate to **Phone System** > **Users**.
2. Locate the *Users* pane, and click the additional information arrow ►, if necessary.
3. Locate the user name, and click the **more** option. Select the **Wipe remote devices** option.
4. Type a new user password in the field provided. Confirm the password in the next field.
5. Click **Wipe** to save the change.

23.6 Managing User Templates

User Templates contain a set of common configuration settings applied when creating or modifying users, but do not include all user settings. Some configuration settings are from the **<user>** > **modify** page. Prior to adding users on a new system, review feature options (e.g. Off-Site Access to Outside Lines or the ability to create conferences) to determine which are necessary for all users.

To see the list of users for each template:

1. Log in to the Allworx System Administration web page and navigate to **Phone System** > **Users**.

2. Locate the *User Templates* pane and click the additional information arrow ►, if necessary. A table of the available user templates displays.
3. Select **View** for the appropriate template, and navigate to the *Template Last Applied To Users* pane for the complete list of users.

To manage user templates:

1. Log in to the Allworx System Administration web page and navigate to **Phone System** > **Users**.
2. Locate the *Users Template* pane, and click the additional information arrow ►, if necessary.
3. Click one of the following actions:

Action	Description
View	Open the *User Template* page. The factory default templates are view only, and are not available to modify. To modify new templates: 1. Click **Modify** and update the template options, as appropriate. See "User Template Settings" on page 233 for more information on the user template options. 2. Click **Update** to save the changes.
Copy	1. Select the user template, such as *System User* (Default) and click **Copy**. A new user template displays in the template list with the same user options as the selected template. 2. Click **View** and follow the instructions above to modify the template.
Delete	Remove the template from the list, and the page refreshes with the remaining available user templates. If the delete option is unavailable, click **View** to see the users assigned to the template. Reassign the users to another template, and try again to delete the template.

User Template Settings

Setting	Description
Name	Enter a title for the new user template.
System Features	
Set Presence Using Schedule	Control a user's presence setting with the selected schedule. When the selected schedule mode is set to Day Mode, the user's presence is **In Office**. This enables users to have unique call routing for Day and Night modes.When the schedule mode is set to Night Mode, the user's presence is **Away**. Select from the drop-down list: • **Disabled** • Any schedule available on the Allworx premise server or Connect Vx instance

Continued

<table>
<tr><th>Setting</th><th>Description</th></tr>
<tr><td>*Set Presence Using Schedule*</td><td>Users can override the presence setting using any of the current available methods. However, the presence changes as the schedule mode changes except for the *On Vacation* and *On Business Trip* presence status, according to the following table.
<table>
<tr><th>Current Presence</th><th>Presence after schedule change to Day Mode</th><th>Presence after schedule change to Night Mode</th></tr>
<tr><td>In Office</td><td>In Office</td><td>Away</td></tr>
<tr><td>Away</td><td>In Office</td><td>Away</td></tr>
<tr><td>At Home</td><td>In Office</td><td>Away</td></tr>
<tr><td>Busy</td><td>In Office</td><td>Away</td></tr>
<tr><td>At a Meeting</td><td>In Office</td><td>Away</td></tr>
<tr><td>On Vacation</td><td>On Vacation</td><td>On Vacation</td></tr>
<tr><td>On Business Trip</td><td>On Business Trip</td><td>On Business Trip</td></tr>
</table>
</td></tr>
<tr><td>*Enable Voicemail*</td><td>Click to select the check box to allow callers to leave a Voicemail message for the extension. If disabled (not checked), the user cannot log in to the Message Center and other callers cannot leave a message. When setting up a *Finally…* call route, the user is not in the drop-down list for T*ransfer to Voicemail* for the user.
Limits the Voicemails by the first limit reached among:
• Maximum number of Voicemails
• Maximum Voicemail storage limit (Allworx Connect servers and Connect Vx instance only)
<table>
<tr><td>*Maximum number Voicemails*</td><td>Limits the number of individual Voicemails a user may have at one time. Select an available option from the drop-down list.</td></tr>
<tr><td>*Maximum Voicemail Storage Limit*</td><td>Limits the amount of Voicemails (in minutes) the user can keep at any one time. Select an available option from the drop-down list.</td></tr>
<tr><td>*Call Answering maximum message record time*</td><td>Limits the Voicemail maximum message length from the caller. Select an available option from the drop-down list.</td></tr>
<tr><td>*Call Answering minimum message record time*</td><td>Limits the Voicemail minimum message length from the caller. Select an available option from the drop-down list. Voicemail messages that do not meet this minimum length are deleted.</td></tr>
<tr><td>*Enable Call Answering Options Menu*</td><td>If enabled, the system announces to the caller before recording the Voicemail message that the caller may hang up or press # for more options at the end of the Voicemail. After completing the Voicemail and the caller presses the # key, the system announces the additional options:</td></tr>
</table>
</td></tr>
</table>

Continued

Setting	Description	
Enable Voicemail *(cont'd)*		• End the call and send/save the recorded message. • Listen to the recorded message prior to send/save. • Erase and re-record a Voicemail message. • Cancel the Voicemail recording and erase the message. • To send your message and return to the previous menu (if the caller was previously in an auto attendant on the same site (multi-site), caller returns to that menu). Check the box to enable (default: Enabled).
	Enable Call Answering Options Menu - Dial Extension option	Adds the following option to callers leaving a Voicemail (requires enabling the Enable Call Answering Options Menu - above). • To send your message and dial an extension. Check the box to enable (default is disabled).
Hide user's BLF status	When set to Enabled (status is hidden), the user's BLF status is not available on all Allworx applications - Reach, Interact, and handsets. The BLF status does not include the user's Presence status. Default: Disabled.	
User has permission to modify extension's call routes	Check to the box to enable the user to customize call routes in My Allworx Manager.	
User has permission to create conferences	Check to the box to enable the user to schedule conference calls in My Allworx Manager. This setting is not available with the Connect Vx service.	
User has permission to administer Allworx View	Check the box to enable administrative permissions in the Allworx View application.	
User has permission to manage their contact image.	Check the box to enable the permissions for the Allworx User to manage the system directory contact image associated with their account.	
System-wide Active Calls Display	Phone displays caller ID information. Select an available option from the drop-down list. ***Note:*** *When a call is received from a number that matches a phone number listed in the user's Contacts, the Contact information is used as the Caller ID.*	
Call Recording Allowed	Check the box to enable the user to invoke Call Recording.	

Continued

Setting	Description
Record every call automatically	Directs the Interact Professional application to automatically start the Call Recording feature from the time the Interact Professional user answers the call; the Interact Professional user still has control on the application interface to pause, resume, or stop the recording during the active call. • Check the box to enable. Requires enabling the Call Recording Allowed option.
Default Prompt Language	Identifies which language to use for incoming call prompts.
Enable Hot Desking	Click to select the check box to enable access to the Hot Desking feature. Specify: *Maximum Login Time* — Select an available option from the drop-down list. *Caller ID Name* — Enter the name callers at the opposite end see on the display. *Caller ID Number* — Enter the number callers at the opposite end seen on the display.
Enable parking calls to this user's extension	Enable other Allworx users to park calls to this extension. Click **modify** to adjust the Park to Extension settings for the user's extension. See "Managing Call Routes" on page 97 for more information.
Call Queue Supervisor	Check the appropriate Call Queue boxes to enable supervisor permissions.
Recording Manager	Check the appropriate Auto Attendant or Call Queues to enable recording manager permissions.
Feature Eligibility	**Allworx Reach Configuration:** 1. Enter the number of Reach activations for which the user is eligible. 2. Click to select the check box to *Receive Emergency Alerts in Reach*. 3. From the drop-down lists select the *Handset Configuration Template* and *Dialing Privileges Group* to use for the Reach handsets. **Allworx Interact Configuration (including Interact Softphone):** 1. Click to select the check box to make the user eligible for Interact Professional. 2. Enter the number of Interact Softphone activations for which the user is eligible. From the drop-down lists select the Handset Configuration Template and Dialing Privileges Group to use when creating Interact Softphone handsets. *Continued*

<table>
<tr><th>Setting</th><th colspan="2">Description</th></tr>
<tr><td rowspan="5"><em>Follow Me Calling</em></td><td colspan="2">Route inbound calls to an external number within call routes.
• When receiving a Follow-Me-Anywhere call on an external phone (e.g. cell phone, home phone), a prompt identifies the source of the call and explains how to accept the call. To enable:</td></tr>
<tr><td>PIN required to accept call*</td><td>Requires entering an Allworx PIN code to answer the call.</td></tr>
<tr><td>Require caller to record name*</td><td>Requires the caller to state their name before ringing the Allworx phone.</td></tr>
<tr><td>Primary Phone</td><td>Select a handset from the Primary Phone drop-down list. The Primary Phone selection is independent of the regular phone assignment and call routing. It can be any phone in the system.</td></tr>
<tr><td colspan="2">* If selecting both check boxes the prompt for calls to the user's extension, "Call for (user) from (caller). To accept, enter your PIN followed by the pound sign."
• If the user rejects or does not answer, the incoming call continues along the defined call route.
• If connecting any of the parties via a SIP Trunk or SIP Gateway, the consult and transfer features do not work.</td></tr>
<tr><td><em>Reach Link</em></td><td colspan="2">• User has permission to modify Reach Link settings - check the box to enable.
• Allow Voicemail when attempting to recover lost Reach calls - check the box to enable.
<strong>Note:</strong> <em>In a multi-site network configuration: Reach Link functionality is limited to users and handsets configured on an Allworx premise server or Connect Vx instance with the Reach Link feature key installed.</em></td></tr>
<tr><td><em>Auto Attendant Menus</em></td><td colspan="2">Click to select the check boxes to include the user in the <em>Dial-By-Name</em> and <em>Dial-By-Directory</em> menus.</td></tr>
<tr><td><em>POP3 Mail Transfers</em></td><td colspan="2">Configures the Allworx user for a POP3 request to transfer email to a POP3 client works as email and Voicemail messages, email messages only, or no messages. Select an option. See "Make needed changes to the email server configurations settings described in this table:" on page 284 for more information.
• Email and Voicemail messages
• Email message only
• No messages</td></tr>
</table>

Continued

<table>
<tr><th>Setting</th><th>Description</th></tr>
<tr><td colspan="2"><b>Voicemail Notification and Escalation</b></td></tr>
<tr><td colspan="2">Sends email to specified email address when a Voicemail inbox receives a message on the Allworx System. Cell Phone service providers typically forward email addresses to cell phone numbers as an SMS message to the cell phone. The email messages sent by the Allworx server provide the following information:
• Allworx user name associated with the Voicemail inbox.
• Length of the recorded message.
• Date and time the Voicemail inbox received the message.
• Caller ID name and number of the caller leaving the Voicemail available).
<b><i>Note:</i></b> <i>The Allworx SMTP server sends the email messages, which require a valid network path from the Allworx premise server or Connect Vx instance to the destination mail server through the Internet.</i></td></tr>
<tr><td><i>Notification Mode</i></td><td>Sends alerts each time the inbox receives a new Voicemail.
To configure Voicemail Notification alerts, enable the Notification Mode radio button and enter an SMS Email Address.
• The Email Address is the address of the recipient to alert a new message is available.
• One entry per field; use a message alias to send alerts to multiple recipients. Acceptable entries:
  • Username
  • Email address
  • Message Alias
  • Cell phone number with service provider SMS text message domain (e.g., 7165552000@txt.att.net)
<b><i>Note:</i></b> <i>Find service provider domains at: www.notepage.net/smtp.htm (Check with the Service Provider for more information).</i></td></tr>
<tr><td><i>Escalation Mode</i></td><td>The Voicemail Escalation feature distributes message alerts repeatedly until meeting the set number of retries or until retrieving any Voicemail message.
• The system organizes recipients into levels so that after sending a specific number of message alerts to the recipient(s) at one level, the system begins sending the alerts to the recipient(s) at the next highest level.
<i>Example:</i> A doctor’s office has an “on call hours” Voicemail box. When leaving Voicemail messages in this box, the system sends the notification to the assigned doctor to answer after hour emergencies. If the doctor does not retrieve the call within X minutes, the system sends an escalation message to the next set of backup doctors.
<i>Continued</i></td></tr>
</table>

Setting	Description	
Escalation Mode *(continued)*	Enable the *Escalation Mode* radio button and update the following fields:	
	Level	Order for alerting recipients a caller left a message in the Voicemail inbox.
	Email Address	Address of the recipient(s) to alert when a new message is in the Voicemail inbox. Only one entry per field, use a message alias to send alerts to multiple recipients. The following are acceptable entries: • Username • Message Alias • Email address • Cell phone number with service provider SMS text message domain (e.g., 7165552000@txt.att.net) ***Note:*** *Find a list of service provider domains at: www.notepage.net/smtp.htm (Check with the Service Provider for more information).*
	Notification Period	Elapsed time before sending another email message to the recipients identified in the Level option.
	Maximum Retries	Maximum number of attempts sent to the recipients of the level before the message alerts proceed to the next level. • This does not include the initial email message. • The server makes one more attempt to the recipients than the entered value. • Escalation message alerts stop after sending the maximum number of messages to the last populated level in the table.
	Continue Notifications	Recipients continue to receive message alerts in conjunction with the next level or levels once escalation occurs.

Continued

<table>
<tr><th>Setting</th><th>Description</th></tr>
<tr><td><b>Email Forwarding</b></td><td></td></tr>
<tr><td><i>External Outgoing Mail (SMTP) Server Configuration</i></td><td>Click to select the check box to override the Allworx premise server or Connect Vx instance configuration for the user.
1. Click to select the check box to enable and enter the following information:
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td><i>Server Address</i></td><td>Enter IP Address or DNS name.</td></tr>
<tr><td><i>Server Port</i></td><td>Enter a value.</td></tr>
<tr><td><i>Display Name</i></td><td>Enter a value.</td></tr>
<tr><td><i>Sender’s Email Address</i></td><td>Enter an email address.</td></tr>
<tr><td>Secure Connection</td><td>Select an available option from the drop-down list:
• <i>None</i>: No secure connection.
• <i>SSL</i>: Uses SSL without sending the STARTTLS message at the beginning of the connection prior to doing the SSL handshake.
• <i>TLS</i>: Uses SSL WITH sending the STARTTLS message at the beginning of the connection prior to doing the SSL handshake.</td></tr>
<tr><td><i>Use authentication</i></td><td>Check the box to enable, and then enter the <i>User Name</i> and <i>Password</i>.
<b><i>Note:</i></b> <i>If using Gmail to send outgoing mail, this option must be enabled. In this case, the User Name is the Google user name, and the Google-generated App Password is pasted in the Password field.</i></td></tr>
</table>
</td></tr>
<tr><td><i>VPN Settings</i></td><td>Check the box to enable. Enter a VPN password in the field, and then confirm it.
<b><i>Note:</i></b> <i>The Connect Vx service does not support the use of a VPN, and these settings are not available in the System Administration web page for the Connect Vx instance.</i></td></tr>
</table>

23.7 Defining Password Requirements

PIN codes or passwords enable access to phone functions and applications. The Allworx administrator can require more stringent password requirements for all accounts, as well as require users to change the PIN or password at the next login by using My Allworx Manager.

Phone Functions requiring a Pin Code	Applications requiring a Password
• Message Center (Audio and Visual)	• Interact / Interact Professional / Interact Softphone
• ACD Agent Login	• Reach
• Hot Desk Login	• My Allworx Manager
• Follow Me	

To change the password requirements:

1. Log in to the Allworx System Administration web page and navigate to **Phone System** > **Users**.
2. Locate the *Password Requirements* pane, and click the additional information arrow ▶, if necessary. A message displays indicating if Strong User Passwords are or are not required, and the current password requirements.
3. Click **modify** to change the settings.

Default Settings	Require Strong Passwords Settings
• Default setting: Require Strong Passwords is unchecked. • Only contain letters (A-Z, a-z), digits (0-9), and special characters (above). • Minimum length of 4 characters / Maximum length of 128 characters.	• Check the Require Strong Passwords box to enable, and then select the strong password requirements: • Minimum password length (6 to 128 characters) • Require lower case letter(s) • Require upper case letter(s) • Require numeric character(s) • Require special character(s) • If the password does not already meet all the updated requirements, the user is required to change the password at the next login.

[SP]	!	“	#	$	%	&	‘	,
-	.	/	:	;	<	=	}	>
?	@	`	{	~	(	)	|	*
+	[	\	]	^	_			

4. Click the **Update** button to save the changes.

Click here to return to the Installing and Configuring Allworx Premise Servers or Configuring Connect Vx Instances.

Part 4 Network

The Network sections describe setting up and customizing the network for the Allworx premise server or Connect Vx instance specific to the business requirements. Each chapter explains:

- Necessary access permissions and feature keys
- Necessary equipment to perform the procedures
- Necessary procedures to setup and customize the Allworx premise server or Connect Vx instance network

Feature and procedure differences for the Allworx Connect Vx service are noted in each chapter.

The various *Network* pages on the Allworx System Administration web page allow the Allworx administrator to set up, configure, and manage the settings of the following features:

Chapter 24 Configuration

Prerequisites	
Access Permissions	Allworx Server Administrator Allworx System Administrator Network Administrator role
Feature Key Required	No

The *Configuration* page allows administrators to customize network settings for the needs of their business.

Prior to configuring the network:

- Review the security advisories available at: https://allworxportal.com/resources#security-advisories.
- Perform a backup of the premise server configuration using OfficeSafe. For more information, see "Backup" on page 337.

  ***Note:** Allworx performs daily backups for all Connect Vx instances and stores those backups in the cloud. Restoration of a system is initiated by contacting Allworx Support to perform the restore.*
- Perform a backup of the View database prior to changing the network configuration (For more information, see the *Allworx View User Guide* available on the Allworx Portal at allworxportal.com for more information).

To manage the network configuration:

1. Log in to the Allworx System Administration web page and navigate to **Network** > **Configuration**. The current settings are displayed.
2. Click **modify** to make changes to the configuration as needed.

   ***Note:** For Connect Vx instances, the only active settings are Host Name and Fully Qualified Domain Name. For information about these settings see page 250.*
3. Update the settings described in the following table:

   ***Note:** For security, the Allworx administrator can no longer manage the Allworx server from the Public interface IP Address. The Allworx server requires all updates from a LAN IP Address.*

Setting	Description
Allworx Network Mode	
LAN Host Mode	Click the check box to enable this option that means a security appliance exists between the Allworx premise server and the WAN/ Public Internet; the Allworx premise server is not directly connected to the "outside world." Another device on the Local Phones interface of the Allworx premise server is the primary router to the Internet. The NAT and Firewall functionalities are not available on the Allworx premise server when this setting is selected. For use with another security appliance (i.e. a firewall).

Continued

Setting	Description
Enable NAT (Network Address Translation)	Click the check box to enable this option for devices attached to the LAN(s) of the Allworx premise server with private (non-globally routeable) IP addresses to communicate on a wider network using the server WAN IP Address. This conserves IPv4 addresses. For use when directly connecting the Allworx premise server to the WAN/Public Internet. ***Note:*** *Always enable the Allworx firewall when selecting this option.*
Enable Firewall	Click the check box to enable this option to use the Stateful Firewall on the Allworx premise server. Provides port forwarding and services for VoIP applications. Protects the Allworx premise server and all services running on it from unsolicited Internet access, allowing access to the ports that the administrator deems necessary. For use when directly connecting the Allworx premise server to the WAN/Public Internet.
Enable Stealth Mode	Click the check box to enable this option for additional security. In this mode the Allworx premise server does not respond to PING/ICMP requests, as if the server did not exist, instead of responding with the standard ICMP Port unreachable message.

VLAN Configuration

- The Allworx Network Stack supports up to 16 user-defined VLANs shared between the Ethernet ports. Any VLAN shares the full bandwidth among all the VLANs on that port. Virtual Network Interfaces provide the ability to define multiple virtual interfaces on a single physical interface so the Allworx administrator can separate voice and data. Each virtual interface enables a separate IP address and 802.1Q VLAN tagging setup. The *Configuration* page has an updated section for configuring VLAN settings for the Ethernet ports.
- There is always at least one configured VLAN, which acts as the phone LAN. The phone VLAN can be on any Ethernet port - tagged or untagged. The system does not require configuring any other VLAN interfaces. Any Ethernet interface without enabled VLANs (and without configured PPPoE) is unused.
- Each interface has a uniquely assigned VLAN Tag/ID. The Allworx administrator may configure one interface per physical port as untagged without specifying the VLAN Tag/ID. By default, the WAN port has one untagged interface - VLAN Tag/ID unspecified, and the LAN port (ETH0 on Connect servers) has one untagged interface - VLAN Tag/ID unspecified. Both ports cannot use the same VLAN Tag/ID.
- The Allworx administrator cannot delete the first VLAN in the list because of the assigned Local Phone network. At a minimum, there is always one Ethernet port with a configured VLAN (tagged or untagged) for local phones, but the Allworx administrator can disable all other network interfaces.

SNMP

The server SNMP daemon listens on all VLAN interfaces, and uses the firewall to block access from the public interface. See “SNMP Server” on page 289 to enable or disable SNMP for all interfaces.

Note: *SNMP servers are not currently available with the Connect Vx service.*

Continued

Setting	Description
Upgrades	
During the first major software upgrade to Allworx System Software Release 8.0 and higher, the software imports the settings from a previous version of the Allworx System Software and creates two VLANs	
LAN/untagged	• Imports the IP settings from the legacy LAN IP settings. • Imports the Network Mode settings from the previous software version.
WAN/untagged	• Imports the WAN/untagged VLAN IP settings from the WAN settings, if the WAN settings were “Use either a DHCP Server” or “Use Static Settings”, and the new WAN setting selects VLAN. Otherwise, the WAN/untagged VLAN has its default settings and the WAN setting remains unchanged. • Imports the Network Mode settings from the previous software version.
add VLAN	Click to add a new VLAN to the list. Administrators can define up to 16 VLANs.
Enabled	Click to select the check box to enable the VLAN port. The Allworx System Software checks the LAN ports by default.
Port	Indicate the Physical Ethernet Port by selecting it from the drop-down list. Options include LAN or WAN.
Tagged	Click to select the check box to tag the VLAN.
ID	Manually enter the VLAN (802.1Q) tag.
Description/IP Address	The Allworx System Software identifies LAN phones as Local phones and VLAN phones as public. The first Public VLAN description is fixed, and subsequent description fields are user-defined. The options include: • Click to select the *DHCP* or *Static* radio button. • Enter the <IP Address> if *Static* is selected. • Select the <Net mask > from the drop-down list.
Services	Click to select the check box to enable the services. The first local phone VLAN BLF broadcast is always enabled, and subsequent BLF check boxes are selected by the user.
Action	Click **delete** to remove the VLAN from the list.
Public Interface	
VLAN	• Click to select this radio button if a VLAN interface is serving as the Public interface. • Select the appropriate interface from the drop-down list.

Continued

Setting	Description
T1 Port	Click to select this radio button if using T1 as the gateway.
Default Route	
Gateway	Enter or verify the IP address of the gateway.
External IP Address	Enter or verify the IP address. This external 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 server and the Internet.
***Allworx Interface Blocking Rules* (Optional)**	
Block traffic between <Select Interface> *and* <Select Interface>	Select the available options from the two drop-down lists.
add rule	Saves the new rule to the premise server.
delete rule	Removes the rule from the premise server. There is no confirmation pop-up window, The rule is immediately deleted when the link is clicked.

Firewall (Optional if enabling the firewall, but this section is not available for Connect Vx. Each Connect Vx instance has its own Linux firewall that is pre-configured to only allow activity on the ports that the Connect Vx requires.)

The Allworx System Software supports a simple firewall between any two possible network interfaces to prevent unauthorized access. The Allworx administrator can add rules consisting of the pairs of interfaces. The Allworx System Software drops packets normally routed between the interfaces that are in such a rule. These rules are in effect regardless of the state of the Firewall and NAT check boxes, and do not effect spoof ports.

Upgrades

After upgrading from 8.4 or lower, the administrator will notice that the *DNS Client* and *DNS Server* entries are no longer listed in the Firewall pane. On upgrade both rules are removed from the Firewall rules and translated to NAT rules **if they were enabled in the previous version**.

At the time of the upgrade, the server creates Firewall rules using the current settings for the ports for all protocols/ applications. When the Firewall rules database is built the server converts legacy host Firewall rules. The server first looks for the protocol (TCP/UCP) and port in the Firewall rules database, and if the port and protocol are in that database the firewall rule is enabled for that protocol and port.

If the protocol and port are not found in the Firewall rules database, that means there was a legacy host Firewall rule entry for it, but the server isn't using it for any of the hard coded firewall rules seen on the Allworx System Administration web page. In this case, the server adds a NAT rule entry to preserve the behavior the server had before, but of which the administrator may not have been aware.

When the conversion is done the server clears the host Firewall rules and that database parameter is not used after conversion.

Continued

Setting	Description
The Firewall rules and NAT rules are added to the Configuration Report. For information about generating this report see “Configuration” on page 321. Click to select the following check boxes to allow the associated port to be exposed through the firewall. The default port selections are shown in the *Description* column. A selected check box indicates that the port is enabled – exposed through the firewall.	
Allworx Reach and Remote Allworx Handsets (TCP 8081)	enabled
Allworx View (TCP 54441)	enabled
BLF (UDP 2088)	disabled
HTTPS: Secure Allworx Administration (TCP 8443)[*]	disabled
HTTPS: Secure Allworx My Allworx Manager (TCP 443)[*]	disabled
HTTPS: Secure Remote Administration (TCP 8043)[*]	disabled
IMAP4 (TCP 143)	disabled
Multi-Site Voicemail (TCP 26 premise servers and 54442 for Connect Vx)	disabled
POP3 (TCP 110)	disabled
PPTP (TCP 1723)	disabled
SIP (TCP 5060)	enabled
SIP (TCP 5070)	enabled
SIP (UDP 5060)	enabled
Note: *Up to 10 UDP SIP ports and 2 TCP SIP ports can be added. Ports are automatically added to the firewall when defined in the Allworx System Administration web page on the* ***Servers*** *>* ***VoIP Servers*** *page.*	
SNMP (UDP 161)	enabled
SNTP Client (UDP 4068)	enabled
Network Address Translation Rules (Optional, if enabling NAT)	
Public IF Port #	Enter the port information.
Protocol	Select **TCP** or **UDP** from the drop-down list.
IP Address	Enter the IP address of the port.

Continued

Setting	Description
Local Port #	Enter the port information.
Host Information	
Host Name	Enter the Host information
Fully Qualified Domain Name (FQDN)	Enter the information. ***Notes:*** • *The Fully Qualified Domain Name of a Connect Vx instance is provided by Allworx.* • *It is appropriate for system administrators to change this value if they install their own server certificate. For more information, see “Managing the Web Server Settings” on page 299.*

4. Click **Update** to save the changes. Restart the Allworx server to have the new settings take effect.

Click here to return to the Installing and Configuring Allworx Premise Servers or Configuring Connect Vx Instances .

Chapter 25 T1 Lines

Prerequisites	
Access Permissions	Allworx Server Administrator Allworx System Administrator Network Administrator role Support Technician role
Feature Key Required	No
Servers	Allworx Connect 731

Note: *T1 lines are not available with the Connect Vx service. The appropriate changes/omissions have been made to the Allworx System Administration web page for Connect Vx. In this instance, the entire T1 Lines page has been removed for Connect Vx.*

T1 Lines are the integrated T1 interfaces on Allworx Connect 731 servers that provide a dedicated connection to a service provider. Access to the T1 Line interfaces is through the connectors labeled T1 on the Allworx premise server front panels. The service provider provisions the line to the interface, which dictates the configuration of the T1 Lines. The settings must match the expected configuration of the service provider for proper operation. Configure the lines in use before connecting the premise server to the T1 line.

When using the T1 Line for circuit switched voice operation (PRI or RBS modes), the preferred method is to set all of the T1 Line parameters including the functional definition for each time slot on the T1 line. After setting this configuration, each slot configured to support circuit switch voice calls display as a new outside line. That is, logically treat each separate slot configured for circuit switched voice calls as a separate telephone line.

Note: *The PRI line type is the only configuration that supports the Reach Extend feature.*

The differences are listed in the following table:

Connect Server	The T1 interface operates as the primary Rate ISDN line and T1 data line for connectivity to another site or to an Internet Service Provider. The T1 interface supports both circuit switched voice calls and TCP/IP data. The T1 interface also supports Robbed Bit Signaling (RBS) operation. Use the data connection 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 premise 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. Always configure the Allworx premise server ISDN interface as the user side equipment with the intention of hooking to the service provider Central Office (CO) network side equipment. The Allworx premise server interfaces have a fully integrated CSU/DSU, typically intended for a direct, short haul connection to the service provider smart jack. Consult the product installation instructions for further information. ***Note:*** *When using PRI operation it is important to define exactly one PRI D channel for the T1 Line and a minimum of one PRI B channel. Match the configuration 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.*

Continued

Robbed Bit Signaling / Channel Associated Signaling Support

The Allworx premise server supports classical T1 Robbed Bit Signaling (RBS) trunk lines on a time slot by time slot basis, also referred to as T1 Channel Associated Signaling (CAS). The system supports the following modes:

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

For the above selections, operational use is the same as the corresponding analog interface types. The system implements the precise signaling protocols for each interface in conformance with the procedures documented in EIA/TIA-464C. Inbound Caller-ID is supported on the FX0 modes, if the CO supports it. See “T1 Lines” on page 251 for more information.

Robbed Bit Signaling / Channel Associated Signaling Support

For primary CO line connectivity, the preferred slot choice is the FX0 Ground-Start slot to minimize the possibility for glare conditions, especially when call volume is high. Allworx does not guarantee that the network provides an explicit disconnect signal in FX0 Loop-Start mode. Example termination methods:

Termination Method	Description
User hangs up phone.	Normal call termination.
User hangs up phone under the supervision of the Auto Attendant.	No terminating signal can cause the call to remain live for an extended period of time (tens of seconds) after the original call termination.
Line-side answer supervision	The network provides an explicit signal acknowledging that the fa end has picked up during an outbound call. • Not all FX0 lines support this supplemental feature. • Because not all network equipment can produce this state, calls cannot rely upon it and disregards the state.

Data Support

Notes:

- *The Allworx administrator can configure or reconfigure the T1 lines without a system restart, but changes to the Network Configuration settings do require a system restart after an update.*
- *Since the data support is fully symmetrical, it is possible to connect two Allworx servers back-to-back between the T1 interfaces either on the same site or across sites using a dedicated T1 line that spans between the two sites via the service provider.*

The Allworx premise server configuration enables the Allworx server to carry TCP/IP packets using PPP encapsulation on any combination of slots constituting a full or fractional T1 interface. Even when configuring a T1 interface for circuit switched PRI operations, use extra (non-voice) slots for dedicated data connections as long as the remote end service provider enables this 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, using any combination of slots for data on each T1 Line, there can be only one logical data interface definition per T1 line.

25.1 Restrictions

Connect 731 Servers – Designate one interface as the logical Public interface. Select the Ethernet Public Interface or the T1 interface for routing TCP/IP traffic. Select either Ethernet VLAN or T1-A port as the data WAN interface for the system even though it is possible to provision multiple interfaces simultaneously.

25.2 Configuring the T1 Lines

The following steps describe configuring T1 lines on the Allworx premise server.

To configure the T1 lines:

To change the T1 Lines setting, see “Managing T1 Lines” on page 192 for more information.

To configure the T1 line on the Allworx premise server:

1. Log in to the Allworx System Administration web page and navigate to **Network** > **T1 Lines**.
2. Locate the T1 Line and click **modify.** Set the *Line Mode* to **T1**. If using an NFAS line, check the *Enable NFAS* box.

   It is important to provision T1 Lines not in use as **Disabled**. The disabled state is the factory default setting for each T1 line.

   To resynchronize (bounce) a T1 line:

   a. Log in to the Allworx System Administration web page and set the *Line Mode* to **Disabled**, and then click **Update**.

   b. Follow steps 1 and 2 again, and then continue on to step 3.

T1 Line Setting	Description
Description	Description of the T1 Line interface. Use this description in all other places referring to this line, such as in the Outlines Lines view and configuration pages of the phone system.
Notes	Enter information about the T1 line. This information will be displayed on the Network / T1 Lines page. A maximum of 512 characters may be entered.
Line Mode	The provisioned operational mode for this interface - **T1** and **Disabled** are available.
Line Code/DS0 Channel Speed	Supports both B8ZS and AMI modes. Allworx strongly recommends using B8ZS mode, if the service provider supports it. • Select the setting that matches the service provider setting, but order the lines as B8ZS, **bounce** if the CO switch enables it. • In AMI mode, clear channel data service is not available and only a 56K data rate is available on each slot. Generally, a PRI line should always be set to B8ZS mode.

Continued

<table>
<tr><th>T1 Line Setting</th><th>Description</th></tr>
<tr><td><i>Framing</i></td><td>The Allworx premise server supports both Super Frame (D4) and Extended Super Frame (ESF) modes. Select the setting that matches the service provider configuration, but Allworx recommends having the service provider use ESF mode, if available.</td></tr>
<tr><td><i>Clock Source</i></td><td>Specify the T1 Line data clocking source reference for this interface.
• Network clocking is almost always the preferred setting because the service provider is 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 to hook two devices back-to-back. 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.</td></tr>
<tr><td><i>Loopback Mode</i></td><td>Place the interface into a diagnostic mode for testing purposes. For best results, always select <b>Normal Operation</b>. The use of the test modes is beyond the scope of this document.
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td><i>Normal Operation</i></td><td>Transmit and receive lines that connect normally and disables all loop back features modes.</td></tr>
<tr><td><i>Local Unframed</i></td><td>Does an internal analog loop back on the local interface so that transmit data immediately loops 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, Allworx recommends using B8ZS, ESF, and Clock Source Internal for such tests.</td></tr>
<tr><td><i>Remote Frames</i></td><td>Synchronizes and decodes incoming data at the frame level. These decoded frames are then re-framed locally and sent back out on the transmitted output line.</td></tr>
<tr><td><i>Remote Unframed</i></td><td>Decodes incoming data 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.</td></tr>
</table>
</td></tr>
</table>

Continued

T1 Line Setting	Description
Line Build Out	Determine the pulse shape/transmit power level used on the analog output of the T1 Line interface. • The dB settings are for long haul configurations and the distance settings for short haul configurations. • Always use the short haul settings 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. • Select the length setting that matches the cabled distance between the Allworx premise 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 in use by the service provider. • Select **NONE** if there is no connection of this interface to a PRI based service. • If this parameter is improperly configured the 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, this may affect Caller ID functionality as well. Verify the correct setting from the service provider to set this parameter accordingly.
Voice Channel Selection Order	Determines the order the Allworx PBX attempts to seize a line for outgoing calls within each service group assigned to this T1 Line. This setting 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. • Set this selection to be the opposite direction that the service provider uses for incoming calls. • 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, configure the PBX for Descending Mode. • Starts at the top and hunts toward lower-numbered slots, select Ascending Mode.
Caller ID Name	Since most PRI lines hook directly into the international SS7 telephone signaling network, it is possible to have parties see any Caller-ID string. • For analog phone lines, the CO determines this string. For PRI lines, the Allworx premise server determines it. • Set the caller ID name field to the preferred value for called parties to see when placing outgoing calls on this T1 Line. • The service provider may override these settings.
Caller ID Number	The phone number presented to called parties for outgoing calls. See name setting above for more information.

Continued

<table>
<tr><th>T1 Line Setting</th><th>Description</th></tr>
<tr><td><em>Prefer Originally Dialed Number (RDNIS) for display</em></td><td>This causes displaying T1/PRI originally-dialed/redirected phone number on Allworx phones, if the original call was redirected and the CO provides the original call information.</td></tr>
<tr><td><em>Prefer Originally Dialed Number (RDNIS) for DID lookup/call routing</em></td><td>This causes using T1/PRI originally-dialed/redirected phone number in DID routing, if the original call was redirected and the CO provides the original call information.</td></tr>
<tr><td><em>Channel Assignments</em></td><td>Select the operating mode for each time slot per the provisioning defined by the service provider or device connected to the T1 Line. Improper selections causes poor results. Select an option from the drop-down list or locate the <strong>Set all channels to</strong>: and select an available option.
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>Disabled</td><td>Indicates an unused time slot on this T1 Line.</td></tr>
<tr><td>PRI B Channel</td><td>Bearer channel for ISDN PRI operation used for carrying voice calls. Selecting this mode defines a new outside line for the PBX for each configured slot.</td></tr>
<tr><td>PRI D Channel</td><td>Data-signaling channel for ISDN PRI operation 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 enabling PRI operation on this line, configure exactly one slot as the PRI D channel. Typically, this is slot 24.
When using NFAS, the D channel must be on the T1-A port.</td></tr>
<tr><td>T1 E and M Immediate Start RBS</td><td>Circuit-switched Ear and Mouth mode Robbed Bit Signaling trunk that uses Immediate Start signaling.
Defines a new outside line for the PBX for each slot configured in this mode.
This mode is symmetrical.
Used to hook the PBX back to back to tie PBXs between sites on a leased line.</td></tr>
</table>
<em>Continued</em></td></tr>
</table>

T1 Line Setting	Description	
Channel Assignments *(continued)*	T1 E and M Wink FG-D RBS	Circuit-switched Ear and Mouth mode Robbed Bit Signaling trunk. • Defines a new outside line for the PBX for each slot configured in this mode. • This mode is symmetrical and also used to hook PBXs back-to-back to tie PBXs between sites on a leased line. • Only use DTMF signaling. • The system does not support Multiple Frequency (MF) signaling.
	T1 FXO Loop-Start RBS	Circuit-switched Foreign Exchange Office style interface mode that digitally emulates the standard analog telephone line interface that uses Loop-Start signaling. • 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 connects to the service provider interface that is operating as the FXS side of the interface. • This mode is NOT symmetrical.
	56K Data Channel	Specified that this slot provides 56K bits/ sec of bandwidth for the T1 Line logical data connection. • This mode is typically used if 64K clear channel service is not available. • Only use this mode when selecting **AMI Line Code** mode.
	64K Data Channel	Specifies that this slot provides 64Kbits/sec of bandwidth for the T1 Line logical data connection. • Use this when clear channel data service is available. • Do not select this mode if selecting the T1 Line’s **AMI Line Code** mode.

3. Click **Update** to save the changes. Click **Cancel** to ignore the request.

Click here to return to the Installing and Configuring Allworx Premise Servers .

Chapter 26 Multi-Site

Prerequisites	
Access Permissions	Allworx Server Administrator Allworx System Administrator Network Administrator role
Feature Key Required	• Multi-Site Primary • Multi-Site Branch

The Multi-Site feature supports the ability to integrate multiple sites seamlessly. Allworx administrators can join up to 99 Allworx premise servers and Connect Vx instances in a Multi-Site network with up to 1975 users and up to 1975 system extensions across all sites. The total number of Multi-Site users and Multi-Site system extensions varies with the maximum users licensed on each Allworx premise server and Connect Vx instance.

The Multi-Site feature supports increased multi-site network security and reduces the time necessary to rebuild or rejoin a multi-site network.

Notes:

- *User roles can be set so that these roles are available on all servers in a Multi-Site configuration. For more information, see “User Settings” on page 229.*
- Calls cannot be forwarded to phones at different sites within a Multi-Site network.

26.1 Setup Checklist

Follow the order of the steps to successfully setup the multi-site network. Click the link in the column on the right for more information.

Step	Description	More Information
1	Verify that the Internal Dial Plan is the same on all premise servers and Connect Vx instances in a multi-site network. The Allworx system does not allow sites to join the network if the Internal Dial Plan is different from the Controller site Dial Plan.	“Dial Plan” on page 67
2	Configure and enable multi-site on the Controller before enabling any of the Branch sites. Doing so allows the Branch sites to register immediately.	“Configuring Individual Sites in the Multi-Site Network” on page 260
3	Configure and enable the branch sites.	
4	Build/rebuild (available on the Controller site only) or rejoin (available on the Branch site only) the multi-site network.	
5	Manage the voicemail transfer settings.	“Voicemail Transfer Settings” on page 264

For more information refer to the *Allworx Advanced Multi-Site User Guide* available by navigating to **Support & Training** > **Documentation** when you log in to the Allworx Portal (allworxportal.com).

26.2 Managing the Multi-Site Network

Prior to setting up the multi-site network or for tips to configure the Allworx Phone system for a multi-site network complete the following:

- Read the *Allworx Advanced Multi-Site Setup Guide* for details.
- View customers: Perform a backup of the View database prior to changing the multi-site configuration (see the *Allworx View User Guide* for more information).

26.2.1 Viewing Users and Extensions in a Multi-Site Network

Allworx administrators can join up to 99 Allworx premise servers and Connect Vx instances in a Multi-Site network with up to 1975 users and up to 1975 system extensions across all sites. Locating User and Extension information for that large of a network can be difficult. Use the *Site display filter* field to view a single site or all sites.

To filter user and extension information:

1. Log in to the Allworx System Administration web page and navigate to **Phone Systems** > **Extensions** or **Phone System** > **Users**.

2. In the *Site display filter* drop-down list at the top of the window, select an individual site or **All sites**.

   - The listings for only that site are displayed. If all sites is selected, the users are grouped together by site name.

3. Click on any column heading to sort the listings. For example, click **Ext** to sort by extension.

4. If a single user or extension is required, enter the information in the *Search* text box to have that information displayed.

26.2.2 Configuring Individual Sites in the Multi-Site Network

The Allworx administrator must designate one site in the multi-site network as the Controller Site. This server considers the other sites in the multi-site network as Branch Sites. The Controller Site tracks which sites are in the multi-site network, and maintains and transmits the site list to all other premise servers and Connect Vx instances in the multi-site network.

Notes:

- *Site information (including site configurations) is transmitted directly between sites.*
- *The Controller Site does not manage the configurations at other sites.*

To configure the sites:

1. Log in to the Allworx System Administration web page.

2. Install the Multi-Site Primary and Multi-Site Branch feature keys. See “Feature Keys” on page 345 for more information. Verify that Multi-Site Primary displays in the *Currently Installed Feature* list. If it is not in the list, obtain a Multi-Site Primary key from the Allworx Partner.

3. Navigate to **Network** > **Multi-Site** and click one of the following links:

<table>
<tr><th>Link</th><th>Description</th></tr>
<tr><td><b><i>Configuration</i></b></td><td></td></tr>
<tr><td><b>modify</b></td><td>Update the following settings as required.
1. Specify a multi-site role for this server by clicking the radio button to select the option:
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td><i>Disabled</i></td><td>Ends the multi-site connections. If a server becomes disabled, the other active sites receive a notification, and the Allworx system removes the disabled site from the database.</td></tr>
<tr><td><i>Controller Site</i></td><td>Enter a descriptive site name for this site. The name displays on the Admin page of all sites as the home location for extensions, users, and handsets.</td></tr>
<tr><td><i>Branch Site</i></td><td>Enter the public IP Address or the domain name of the Allworx premise server or Connect Vx instance at the Controller site. The name displays on the Admin page of all sites as the home location of extensions, users, and handsets.</td></tr>
</table>
• In the <i>Site List</i> pane, a message displays <b><Controller Site IP Address> contacted</b>. <b>Pending acceptance from admin at site</b>. This indicates the Branch site sent a request to the Controller site to join the multi-site network. The Branch site stays in this state until the Controller site manually accepts this request.
• The message <b><Controller Site IP Address> is being contacted</b>, indicates the Branch site is waiting for a response from the Controller.
• Click <b>Refresh</b> to verify if the “Pending acceptance” message displays. If the refreshed page continues to display the <b>is being contacted</b> message, there is a problem.
• Verify the Controller site configuration and verify the network communications between sites.
2. Click <b>Update</b> to save the changes.
<b><i>Note:</i></b> <i>If the Branch Site Internal Dial Plan or Extension Length is different from the settings on the Controller site, the system does not enable the Branch site to join the network.</i></td></tr>
<tr><td><b>advanced</b></td><td>Only change the site identifier at the direction of Allworx Customer Support.</td></tr>
</table>

Continued

Link	Description
Go Offline	Disconnect the premise server or Connect Vx instance from the multi-site network. If Offline, the other active sites receive a notification, which clears the premise server or Connect Vx instance credentials and prevents the Offline site from communicating with the other sites on the multi-site.
Rebuild	Rejoin all active sites and those without a pending accept status. Sends a request to Branch premise servers and Connect Vx instances in the list to resend connection information. When rebuilding a Multi-Site network (either by deleting or using the **Rebuild** button), local handsets owned by remote users become "unowned" phones and display **(none)** in the owner column on the Phone System > Handsets > SIP Handsets page.
Rejoin	Send a request to the Controller premise server or Connect Vx instance to re-establish a connection in the multi-site configuration without disabling the premise server or Connect Vx instance and re-entering the branch site data. For premise servers or Connect Vx instances that fail a join attempt.

Site List

This pane provides a list of sites available to add to the multi-site configuration.

<table>
<tr><td><b>Pending Sites</b></td><td>A list of available sites to add to the multi-site configuration.
• <b>Accept</b> - adds the premise server or Connect Vx instance to the multi-site configuration.
• <b>Deny</b> - does not add the premise server or Connect Vx instance to the multi-site configuration.
<i><b>Note:</b> After accepting the sites, the Active Sites table updates from the Pending Sites table. Notice the status that displays in the Inbound Link and Outbound Link columns. It may take a few minutes for all</i> premise servers or Connect Vx instances <i>to report an Active status. "Active" indicates that the Controller site and the Branch site exchanged all required information (i.e. users, extensions, and handsets).</i></td></tr>
<tr><td><b>Active Sites</b></td><td>Display the handsets available on the branch site. Click:
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td><b>handsets</b></td><td>• <b>hide</b> - collapses the list of sites.
• <b>modify</b> - map the specified handsets. Click the check box next to the handset model to enable. Click <b>Update</b> to save the changes.</td></tr>
<tr><td><b>delete</b></td><td>Removes the site from this and all other servers. Click Delete to remove the site.</td></tr>
<tr><td><b>test</b></td><td>If any tests fail, the most likely cause is the configuration of network devices between the sites. Check the firewall settings, port assignments, static routes, and port forwarding between the current site and the remote test site.
• hide - collapses the list of available tests.
• HTTP
• BLF
• SMTP
• SIP
• Audio Call</td></tr>
</table>
</td></tr>
</table>

Continued

Link	Description	
Active Sites *(continued)*	**Rejoin**	Available for each active site to initiate a rejoin from one branch to another without involving the other branches, unless one of the sites is a controller site.

Mapped Handsets

This pane displays a list of handsets mapped from the branch site to the controller site.

Conflicts

This pane displays if there are cases where the same defined extension phone number is on more than one premise server or Connect Vx instance, as a result, conflicts in the data result during the data exchange between sites. Another kind of conflict occurs if users defined on more than one premise server or Connect Vx instance have the same username. Check and resolve conflicts on each premise server or Connect Vx instance:

Entries in the Username and User Extension Conflicts table indicate either an Ext conflict or a Login Name conflict. Look up the extension at each of the conflicting sites.

- If users on different sites are using the same extension, change one of the user's extensions on all but one of the conflicting sites to resolve the conflict.
- If users on different sites are using the same Login name, delete one of the conflicting users and re-add it with a different username.

Note: *This deletes the configurations and saved Voicemails for the deleted user.*

For any entries in the *System Extension Conflicts* table, delete the extension from one of the conflicting sites to resolve the conflict. Remember the call route of the deleted extension, and then add a new extension with that same call route.

Verify that all conflicts have been resolved on all premise servers and Connect Vx instances.

Continued

<table>
<tr><th>Link</th><th>Description</th></tr>
<tr><td colspan="2"><b><i>Voicemail Transfer Settings</i></b>
This pane provides for the configuration of the firewall settings for transferring Voicemail between sites.</td></tr>
<tr><td><b>modify</b></td><td>Update the following settings as required.
1. Enter the information in the text fields provided.
<table>
<tr><th>Setting</th><th>Description</th></tr>
<tr><td><i>TCP/IP Port</i></td><td>Enter the TCP/IP Port number on which this site listens for Voicemail transfer requests. This port number is shared with other sites.</td></tr>
<tr><td><i>Maximum Sessions</i></td><td>Enter the total number of active Voicemail transfer sessions that can occur at one time on this site.</td></tr>
<tr><td><i>Single Message Size Limit (bytes)</i></td><td>Enter the maximum message size in bytes for one message. Entering a 0 equals no limit.</td></tr>
<tr><td><i>Maximum Messages Per Session</i></td><td>Enter the maximum number of messages per each session. Entering a 0 equals no limit.</td></tr>
</table>
2. Click <b>Update</b> to save the changes. Click <b>Cancel</b> to disregard the request.</td></tr>
</table>

Click here to return to the Installing and Configuring Allworx Premise Servers or Configuring Connect Vx Instances .

Chapter 27 Px 6/2 Expanders

Prerequisites	
Access Permissions	Allworx Server Administrator Allworx System Administrator Network Administrator role
Feature Key Required	No

The Px 6/2 Expander increases the system analog capability by adding six (6) FXO and two (2) FXS ports to Connect Vx instances and Allworx Connect premise servers. Allworx administrators can use the Plug and Play installation feature for locally connected Px Expanders.

For detailed unpacking and installation instructions, see the *Allworx Px 6/2 Expander Installation Guide* or *Allworx Verge IP Phone Series Quick Start Guide* that are available by navigating to **Support & Training** > **Documentation** when you log in to the Allworx Portal (allworxportal.com).

Allworx defines a remote device as a Px Expander or phone connected on a Local Area Network (LAN) that is different from the Allworx premise server or Connect Vx instance.

Note: *Px Expanders are always remote to a Connect Vx instance.*

Example:

An Allworx premise server is at the company main office, but an employee has a home office phone.

The Allworx administrator configures the following:

- Allworx premise server for calls to and from the phone as though the employee is at the main office
- Analog phones or CO lines on a remote Px Expander to integrate into the Allworx server network and dial plan

Caution:	• *Do not configure remote handsets to place 911 calls. Allworx cannot guarantee proper routing of 911 emergency calls from remote Allworx phones or analog handsets attached to remote Allworx Px Expanders.* • *During a network connection interruption (such as a power failure) between the Px Expander and the Allworx premise server or Connect Vx instance, regular use of the Px Expander FXO and FXS ports is not possible. The only option to place calls through a Px Expander without a functional network connection is to plug an analog phone into the Power Fail port on the rear of the Px Expander. The CO line connected to FXO port 1 routes the calls placed using this phone. No other ports function.*

27.1 Px Expander Setup Checklist

Follow this order of steps to successfully set up a Px Expander. Click the link in the column to the right for more information.

Step	Description	More Information
1	Change the Px Expander network settings, if needed.	"Changing the Network Settings" on page 269
2	Update the firewall settings, if needed.	"Px Expanders behind a Third-Party Firewall" on page 269 or "Multiple Remote Devices Behind the Same Firewall" on page 270
3	Configure the Px Expander on the Allworx premise server or Connect Vx instance.	"Managing the Px Expander" on page 266
4	Configure the FXS and FXO ports.	"Managing FXO and FXS Ports" on page 268

27.2 Managing the Px Expander

The Allworx System Administration web page lets you display a list of the existing Px Expanders on an Allworx premise server or Connect Vx instance and then manage their settings or add new devices.

Note: *To enter configuration information, see the Allworx Px 6/2 Expander Installation Guide available on the Allworx Portal (allworxportal.com).*

To add or manage a Px Expander on the Allworx server or Connect Vx instance:

1. Set up and configure the Px Expander using the *Allworx Px 6/2 Expander Installation Guide*.
2. Log in to the Allworx System Administration web page and navigate to **Network** > **Port Expanders**.
3. Click one of the following actions:

Action	Description
add a Port Expander	• Enter the settings for the new portal in the fields for the settings described in "Px Expander Settings" on page 267. • Click **Add** to save the change or **Cancel** to clear the request.

Continued

Action	Description	
<Port Expander name> (available after adding a port expander)	Click one of the following links to complete the action.	
	<Port Expander name>	Update the Px Expander settings. See “Px Expander Settings” on page 267 for additional information. Click **Update** to save the change.
	Delete	Removes all related configurations and port definitions from the system.
	Replace	Replace the Px Expander with another Px Expander while automatically transferring all the configuration parameters and settings to the new unit. Use this when replacing a defective Px Expander.
	Handsets	Jumps to the *Handsets* page to configure Px Expander FXS ports.
	Outside Lines	Jumps to the *Outside Lines* page to configure Px Expander FXS ports.
	<IP Address>	Opens the Px Expander information page in a separate browser window.
	Reboot	Restart the Px Expander after making configuration changes to the expander or any of its ports. The reboot starts as soon as all of the Px Expander ports are idle.

Px Expander Settings

The settings in the following table are to be configured for each Px 6/2 Expander.

Setting	Description
MAC Address	Hardware identifier for the Px Expander. This entry cannot be changed.
Description	Name given to the Px Expander. During Plug and Play installation, the *Description* is set to the Px Expander MAC address. Allworx recommends changing it to something more meaningful to the site or configuration.
Codec Preference Order	Set the preferred codec order for the Px Expander. The premise server does not support all codecs for all call types (for example, accessing the premise server Auto Attendant requires G.711). Codec is the method of encoding/decoding the audio sent and received. • The two possible codecs are G.711 and G.729A. G.711 preserves voice quality but takes more bandwidth. G.729A takes less bandwidth but reduces voice quality. • This setting defines the order of codec selection. • The Px Expander attempts to use the first choice but uses whichever required codec to support calls.

Continued

Setting	Description
RTP Media Range (Port to Port)	Specify the range of UDP ports used for Real-Time Transport Protocol communications. • When placing remote Px Expanders behind third-party firewalls, under certain conditions restrict the UDP port range to create mapping rules for each Px Expander behind the firewall. See "Px Expanders behind a Third-Party Firewall" on page 269 for more information.
SIP NAT Keep-alive Interval	Some NAT firewalls automatically time out and close connections to devices. • If a remote Px Expander is behind such a firewall, this setting prevents the timeout. • Messages called keep-alive packets are sent from the Px Expander to the Allworx server at the frequency specified. • Set the value to an interval shorter than the firewall timeout.
Expander SIP Port	Number of the port from which SIP messages are sent by the Px Expander. Use the default value of 5060 unless the Px Expander is behind a third-party firewall and the network requires a different value.
Server SIP Port	Number of the premise server port that receives the SIP messages from the Px Expander.
Time Zone	Specify the time zone that the handset uses to compute its local time. • If the Px Expander is in the same time zone as the Allworx premise server, select **use current server**. • If the Px Expander is remote, use the time zone of its actual location. ***Note:*** *Px Expanders are always remote to Connect Vx instances.*
Daylight Savings Time	Specify if the Px Expander will use Daylight Savings Time (DST) to compute its local time. • If the Px Expander is in the same time zone as the Allworx server, select **use current server**. • If the Px Expander is remote, use the DST setting of its actual location.
Max Jitter Buffer Size	Alter the maximum size of the jitter buffer. Jitter is the variation in network audio packet latency experienced by the Px Expander that results in a reduction in audio quality. The Px Expander uses a jitter buffer to improve the audio quality when jitter occurs.

27.3 Managing FXO and FXS Ports

After installing an Allworx Px Expander, the Allworx administrator can use the Allworx System Administration web page to configure the FXS and FXO ports on the *Handsets* and *Outside Lines* pages, just like the premise server ports.

To set the configuration, navigate to:

- **Phone System** > **Handsets** and locate the *Analog Handsets* pane
- **Phone System** > **Outside Lines** and locate the *Analog (CO) Lines*

On the *Dial Plan* page, the system adds Px Expander FXO ports to the default service groups. Create new custom service groups or modify existing service groups to include the Px Expander FXO ports. Navigate to **Phone System** > **Dial Plan** and locate the *Service Groups* pane.

27.4 Px Expanders behind a Third-Party Firewall

Px Expanders work even when behind a firewall; however, there are exceptions that require additional configuration steps.

By default, all audio traffic from remote phones and Px Expanders runs through the Allworx premise server or Connect Vx instance. When calls to and from remote devices connected to a Connect premise server go out over SIP trunks or over the Internet to other remote devices, the bandwidth usage is 180 Kbytes per second per call which is double a regular incoming call.

This increased traffic may over-extend the available network bandwidth. Enabling audio between devices to go directly from one to the other, rather than through the premise server, can reduce server bandwidth usage. See “VoIP Server” on page 295.

***Note:** If enabling audio between devices when the phone or Px Expander is behind a firewall, the firewall requires modifications to its configuration.*

27.4.1 Changing the Network Settings

If the remote device does not register with the premise server or Connect Vx instance, or if calls to or from the premise server or Connect Vx instance do not connect, change the settings on the firewall and/or Px Expander to enable communications.

To change the network settings on a Px Expander:

1. Locate the *Config Mode* page for Px Expanders (refer to the *Allworx Px Expander Installation Guide* available on the Allworx Portal).

   Make changes to the following settings:

Setting	Description
DHCP	Disabled
Remote Plug and Play key	See “Px Expanders behind a Third-Party Firewall” on page 269.
Boot Server IP	See “Px Expanders behind a Third-Party Firewall” on page 269.
Phone/Port Expander IP	Select an address consistent with the remote site network.
Netmask IP	Network Mask of the remote site network.
Gateway IP	Gateway IP of the remote site network.

2. Log in to the Allworx System Administration web page and navigate to **Network** > **Port Expanders**.

3. Click **Port Expander Description**.

   Set the RTP port range for the phone or Px Expander to **16384** or **16393**. Forward the required IP ports through the firewall at the remote site, per the following table:

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

27.4.2 Multiple Remote Devices Behind the Same Firewall

If there is more than one remote Px Expander behind a firewall, the first course of action (if possible) should be to adjust the firewall settings as follows.

1. Always disable SIP ALG.
2. Enable source port that keeps the consistent or 1-to-1 NAT.
3. Only after these adjustments, resort to assigning an individual RTP Media Port Range and SIP port per device as described in the following procedure.

Notes:

- *Be aware that different firewall manufacturers may use different terminology, and have different procedures for making these changes.*
- *For information about multiple remote handsets, see "Multiple Remotely Connected Handsets" on page 133.*

To assign separate RTP media port ranges and SIP ports to individual Px Expanders:

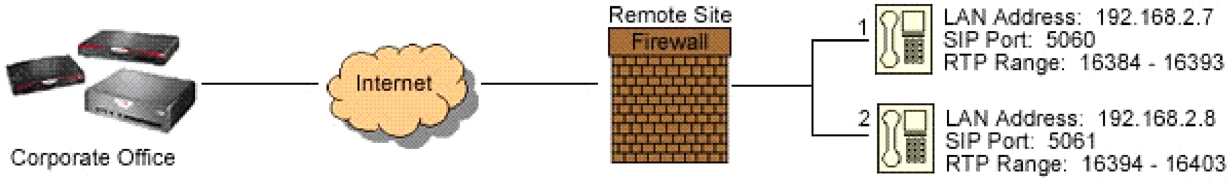
1. Use the phone soft keys to navigate to **Config** > **Network Settings** menu for phones. Locate the *Config Mode* page for Px Expanders (refer to the *Allworx Px Expander Installation Guide* available on the Allworx Portal).

   Change the following settings:

Option	Description
DHCP	Disabled
Remote Plug and Play key	See "Px Expanders behind a Third-Party Firewall" on page 269.
Boot Server IP	See "Px Expanders behind a Third-Party Firewall" on page 269
Phone/Port Expander IP	Select an address consistent with the remote site network.
Netmask IP	Network Mask of the remote site network.
Gateway IP	Gateway IP of the remote site network.

Configure the VoIP settings	See “VoIP Server” on page 295.

2. Log in to the Allworx System Administration web page and navigate to **Network** > **Px Expanders.**
3. Click **Port Expander Description**. Allocate 10 ports for each device in the standard range (e.g. phone1: 16384 to 16393, phone2: 16394 to 16403).
4. Select a different SIP port for each device, starting at 5060 (e.g. phone1: 5060, phone2: 5061).
5. Forward the required IP ports through the firewall at the remote site, per the following table.



Port Type	WAN	LAN	Protocol	IP Address
BLF	2088	2088	UDP	192.168.2.7
SIP	5060	5060	UDP/TCP	192.168.2.7
SIP	5061	5061	UDP/TCP	169.168.2.8
RTP	16384 - 16393	16384 - 16393	UDP	192.168.2.7
RTP	16394 - 16403	16394 - 16403	UDP	169.168.2.8

Note: *Map the BLF port for one of the remote devices. The device that gets the BLF messages from the premise server or Connect Vx instance forwards the BLF information to every other Allworx desk phone in that subnet.*

27.5 Different Remote Site Phones — Each with a Firewall

This is very similar to “Multiple Remote Devices Behind the Same Firewall” on page 270 because it is necessary to do the mappings on each site firewall.

- Map the correct RTP port range for the device that is on the configured firewall.
- Map the BLF port (2088) for one device on each firewall.

Click here to return to the Installing and Configuring Allworx Premise Servers .

Chapter 28 Static Routes

Prerequisites	
Access Permissions	Allworx Server Administrator Allworx System Administrator Network Administrator role
Feature Key Required	No

A *Static Route* occurs when a router forwards traffic using a manually-configured routing entry rather than information from a dynamic routing protocol.

Note: *Static Routes cannot be used with the Connect Vx service. The appropriate changes/ omissions have been made to the Allworx System Administration web page for Connect Vx. In this instance, the entire Static Routes page has been removed for Connect Vx.*

This chapter describes customizing the static routes for the business needs.

To manage the Static Routes:

1. Log in to the Allworx System Administration web page and navigate to **Network** > **Static Routes**.
2. Click **modify** and update the settings:

Setting	Description
Destination	IP Address of the destination network.
Netmask	Select an option from the drop-down list.
Gateway	Enter the Gateway IP Address.
External IP	Enter the External IP Address.

3. Click **Update** to save the changes. Restart the Allworx server for the new Network Static Route settings to take effect.

Click here to return to the Installing and Configuring Allworx Premise Servers .

Chapter 29 Virtual Private Network (VPN)

Note: *VPNs are not available with the Connect Vx service. The appropriate changes/omissions have been made to the Allworx System Administration web page for Connect Vx. In this instance, the entire VPN page has been removed for Connect Vx.*

VPNs (Virtual Private Networks) provide access to remote and secure data. The Allworx Connect premise servers support a single-user diagnostic VPN.

Prerequisites	
Access Permissions	Allworx Server Administrator Allworx System Administrator Phone Administrator role Network Administrator role
Feature Key Required	Virtual Private Network (VPN)*

To enable the VPN PPTP (Point-to-Point Tunneling Protocol) server:

1. Log in to the Allworx System Administration web page and navigate to **Network** > **VPN**. The *VPN* page displays.

2. Click **modify**.

3. Click to select the *Enable VPN PPTP Server* check box.

4. Update the fields with the required information.

5. Click **Update** to save changes.

6. Restart the Allworx server for the VPN changes to take effect.

To enable a VPN for individual users, see “User Template Settings” on page 233 for more information.

Click here to return to the Installing and Configuring Allworx Premise Servers .

Section 5 Servers

The server's features support customizing the premise server and Connect Vx instance types specific to the business requirements. Each chapter explains:

- Necessary access permissions and feature keys
- Necessary equipment to perform the procedures
- Necessary procedures to setup and customize the Allworx server network

Feature and procedure differences for the Allworx Connect Vx service are noted in each chapter.

The various *Server* pages on the Allworx System Administration web page allow the Allworx administrator to set up, configure, and manage the settings of the following premise server and Connect Vx instance types:

Chapter 30 DHCP

Prerequisites	
Access Permissions	Allworx Server Administrator Allworx System Administrator Network Administrator role
Feature Key Required	No

Note: *DHCP server settings are not available with the Connect Vx service. The appropriate changes/omissions have been made to the Allworx System Administration web page for Connect Vx. In this instance, the entire DHCP page has been removed for Connect Vx.*

The DHCP (Dynamic Host Configuration Protocol) server displays the active leases associated with the DHCP server.

Note: *The DHCP server can only support a /24 network.*

30.1 Managing the DHCP Server

The DHCP server settings are displayed on this page along with the following:

- **Active Leases** - These are current client devices that are not expired.
- **Known Hosts** - These are client devices with expired licenses that have an IP address that has not been assigned to another device (i.e. not recycled). The intent is that if a known device ever comes back and submits a DHCP request for a lease, it will receive the same IP address it had before -- as long as that device remains in the list.

To manage the DHCP server:

1. Log in to the Allworx System Administration web page and navigate to **Servers** > **DHCP**. The *DHCP Server* page displays with information panes for the *DHCP Server*, *Active Leases*, and *Known Hosts*.

2. Locate the *DHCP Sever* pane at the top of the page.

3. Click **modify** to update the following settings.

Setting	Description
Enable DHCP Server	Click to select the check box to enable the server. If the server is not enabled, the following fields are grayed-out.
Dynamic Address Range	Enter the endings of the IP addresses in the range using the fields provided.
DHCP Address Reservations	Enter the ending of the TCP/IP address and the MAC address of the DHCP client in the fields provided.
Enable Dynamic DNS	Click to select the check box to enable. When enabled, the DHCP server automatically adds discovered hosts to the DNS (Domain Name System) server list.

4. Click **Update** to save the changes. Restart the Allworx premise server to have the changes take effect.

To Delete a *Known Host:*

1. Log in to the Allworx System Administration web page and navigate to **Servers** > **DHCP**.

2. Locate the *Known Hosts* pane, and click the *IP Address* upward or downward facing arrow to sort the premise servers in ascending or descending order, respectively.

3. Click to select the check the box next to the appropriate *IP Address*.

4. Click **Delete** to remove that host IP address from the list. Removing an entry from this table returns the associated IP address to the pool of available addresses for the new client leases.

Click here to return to the Installing and Configuring Allworx Premise Servers .

Chapter 31 DNS

Note: *DNS server settings are not available with the Connect Vx virtual server. The appropriate changes/omissions have been made to the Allworx System Administration web page for Connect Vx. In this instance, the entire DNS page has been removed for Connect Vx.*

The DNS server resolves and maintains a directory of domain names, and then translates those names to Internet Protocol (IP) addresses.

Prerequisites	
Access Permissions	Allworx Server Administrator Allworx System Administrator Network Administrator role
Feature Key Required	No

To manage the DNS server:

1. Log in to the Allworx System Administration web page and navigate to **Servers** > **DNS**.

2. Click one of the following actions on the *DNS Server* page.

Action	Description	
modify	1. Make required updates the current settings.	
	Operating Mode	
	Normal	Click to select this radio button to have the Allworx premise server attempt to resolve domain names to IP addresses in this order: internal cache, Primary DNS Server (if specified), Secondary DNS Server (if specified), list of well-known DNS Root Name Servers (only if there are no specified Primary or Secondary servers). • *Primary DNS Server* - Enter the IP address in the field provided. • *Secondary DNS Server* - Enter the IP address in the field provided.
	Standalone	Click to select this radio button to have the Allworx premise server not use any external servers to resolve domain names to IP addresses. The Allworx server processes domain names not resolved internally as invalid.
	Host Table	
	DNS Zone	Click the check box to use the Allworx DNS server to host the DNS Zone. Uncheck if another computer hosts the DNS Zone.
	Host Name	Enter the host name.
	IP Address	Enter the host IP address.

Continued

Action	Description
modify *(continued)*	2. Click **Update** to save the changes. 3. Restart the Allworx server for the new settings to take effect.
flush the DNS cache	1. Click the link to clear the locations (IP addresses) of web servers containing recently viewed pages. 2. Click **OK** in the pop-up window that appears when the cache has been flushed.

Click here to return to the Installing and Configuring Allworx Premise Servers .

Chapter 32 Email

Prerequisites	
Access Permissions	Allworx Server Administrator Allworx System Administrator Network Administrator role
Feature Key Required	No

The email server handles and delivers email over a network. The procedures in this chapter describe using the *Email* page to customize the email premise server or Connect Vx instance for the business needs.

Log in to the Allworx System Administration web page and navigate to **Servers** > **Email**. The email premise server or Connect Vx instance displays with the current settings and values.

To manage the email server settings:

Navigate to the *Email Server* pane and click one of these actions.

Action	Description
modify	Change the current email settings. See "To manage the email server settings." on page 283 for more information. • Click **Update** to save the changes. • To modify the settings restart the Allworx server for the new settings to take effect.
manage the email queue	Display a list of the current emails. 1. Select a single email by checking the box in the left column or all the emails by clicking **Select All**. To uncheck all the email check boxes, click **Clear All**. 2. Select one of the available options: **Flush** – Clears the email or emails from the list without Non-Deliverable Receipts (bounced messages). **Flush with NDR** – Clears the email or emails from the list with Non-Deliverable Receipts (bounced messages). **Retry Send Now** – Attempts to resend the email. **Cancel** – Disregards changing the email queue. 3. Click **Refresh Page** to update the emails listed n the table.

To manage the Voicemail to Email Signature:

1. Navigate to the *Voicemail* to *Email Signature* pane and then click **modify**.
2. Enter text for the signature. A maximum of 1000 characters may be entered.
3. Click **Update** to save the changes.

The premise server or Connect Vx instance appends this signature text to every Voicemail to email it sends.

To manage *Email Server* settings:

1. Navigate to the *Email Server* pane; click the more information button (►) to expand the pane if needed.
2. Click **modify**.
3. Make needed changes to the email server configurations settings described in this table:

<table>
<tr><th>Setting</th><th>Description</th></tr>
<tr><td colspan="2"><b><i>Features</i></b></td></tr>
<tr><td><i>Connection Timeout (secs)</i></td><td>Enter a value in seconds.</td></tr>
<tr><td><i>Voicemail Attachment Format</i></td><td>Select an option from the drop-down list.</td></tr>
<tr><td colspan="2"><b><i>SMTP Settings</i></b>
Forward Voicemail and email using external Internet SMTP services such as Gmail and Hotmail. The Allworx System Administration web page includes SMTP server settings to enter login credentials for an existing email account. Use this account for email, Voicemail, and text alerts. For user Voicemail, it sends the email to the address in the user’s Message Alias.</td></tr>
<tr><td><i>Port</i></td><td>Enter a value.</td></tr>
<tr><td><i>Transmit Threads</i></td><td>Enter a value.</td></tr>
<tr><td><i>Transmit Queue Depth</i></td><td>Enter a value.</td></tr>
<tr><td><i>Notify Sender of Delivery Delay</i></td><td>Click to select the check box to enable.</td></tr>
<tr><td><i>Enable use of SMTP Smart Host</i></td><td>Click to select the check box to enable. Enter the following information in the fields provided:
<table>
<tr><td><i>Smart Host Address</i></td><td>Enter IP address or DNS name.</td></tr>
<tr><td><i>Smart Host Port</i></td><td>Enter a value from <b>1</b> to <b>65535</b>, typically <b>25</b>.</td></tr>
<tr><td><i>Smart Host requires authentication</i></td><td>Check the box to enable and provide the following information in the text fields:
• <i>Smart Host User Name</i>
• <i>Smart Host Password</i></td></tr>
<tr><td><i>Email for local domain</i></td><td>Select an option from the drop-down list.</td></tr>
<tr><td><i>Voicemail for local domain</i></td><td>Select an option from the drop-down list</td></tr>
</table></td></tr>
</table>

Continued

<table>
<tr><th>Setting</th><th>Description</th></tr>
<tr><td><i>Enable External Outgoing Mail (SMTP) Server</i></td><td>1. Click to select the check box to enable. Enter the following information in the fields provided:
<table>
<tr><td><i>Server Address</i></td><td>Enter IP Address or DNS name. Enter the IP address or DNS name.</td></tr>
<tr><td><i>Server Port</i></td><td>Enter a value. Enter <b>1</b> to <b>65535</b>, typically <b>25</b>.</td></tr>
<tr><td><i>Display Name</i></td><td>Enter a value.</td></tr>
<tr><td><i>Sender's Email Address</i></td><td>Enter a value.</td></tr>
<tr><td><i>Use authentication</i></td><td>Click to select the check box to enable and provide the following information:
• <i>User Name</i> - Enter the information in the text field.
• <i>Password</i> - Enter the information in the text field.
<b><i>Note:</i></b> <i>When using Gmail to send outbound mail, this field is where the Google-generated App Password should be pasted.</i>
• <i>Secure Connection</i> - Select an option from the drop-down list.
  • <b>None</b> - No secure connection.
  • <b>SSL</b> - Uses SSL without sending the STARTTLS message at the beginning of the connection prior to doing the SSL handshake.
  • <b>TLS</b> - Uses SSL WITH sending the STARTTLS message at the beginning of the connection prior to doing the SSL handshake.</td></tr>
</table>
2. Click <b>Send Test Email.</b></td></tr>
<tr><td colspan="2"><b><i>POP3 Settings</i></b>
Only the email and Voicemail message option transfers Voicemail messages to the PC inbox. Configure the email program on the PC used to receive messages to pop the messages from the Allworx server. Use the following information to configure the email program:
<b><i>Notes:</i></b>
• <i>POP3 settings are read-only for Connect Vx virtual servers.</i>
• <i>Most email programs enable leaving the messages on the server when transferring to the PC. When using this feature, the user may exceed the server inbox quota. To avoid this, Allworx recommends enabling the email program to:</i>
  • <i>Delete all the server email after N days.</i>
  • <i>Delete the email when the user deletes it on the PC.</i>

<i>Continued</i></td></tr>
</table>

Setting	Description
Enable Server	Click to select this check box to enable the POP3 server and make the following settings active. A restart of the Allworx server is required to have any changes take effect. • The default for existing installations is to have this check box enabled (selected). • The default for new installations is to have this check box disabled (not selected). ***Note:*** *Resetting the server to Factory Defaults sets the POP3 server to disabled.*
Port Number	Enter a value in the text field. The default port number for Connect Vx is 54444, and the default port number is 110 for all other Connect premise servers.
Maximum Connections	Enter a value in the text field.
Number Client Threads	Enter a value in the text field.
Max. Depth Client Deferred Queue	Enter a value in the text field.
Min. Poll Period (minutes)	Enter a value in the text field.
Secure Login	Click to select the check box to enable. For the Connect Vx service, secure login is always enabled and cannot be changed.
IMAP Settings IMAP synchronizes email so users can access an account from multiple locations. Configure the PC email application to send and receive messages from the Allworx premise server or Connect Vx instance. The details depend on the application but require: • Entering the Allworx premise server or Connect Vx instance IP address LAN TCP/IP Address (from the **Network** > **Configuration** > **Modify** page) as the incoming IMAP server address. • Entering the same address as the outgoing SMTP server address. • Entering the Allworx user login name / password as the IMAP user / password. • Do not use Secure Password Authentication (SPA). • Do not use SSL to communicate with the Allworx premise server or Connect Vx instance. • Do not use authentication for the outgoing premise server or Connect Vx instance. ***Notes:*** • *IMAP settings are read-only for Connect Vx instances.* • Enabling the IMAP protocol requires a Mobile Link Feature Key on the Allworx premise server or Connect Vx instance.	
Enable Server	Click to select this check box to enable the IMAP server and make the following settings active. A restart of the Allworx server is required to have any changes take effect. • The default for existing installations is to have this check box enabled (selected). • The default for new installations is to have this check box disabled (not selected). ***Note:*** *Resetting the server to Factory Defaults sets the IMAP server to disabled.*

Continued

Setting	Description
Port Number	Enter a value in the text field. The default port number for the Connect Vx service is 54445, and the default port number is 110 for all other Connect premise servers.
Maximum Connections	Enter a value in the text field.
Alternate Email Domains	
<alternate domain name>	Enter a different email domain in the fields provided.
Unsolicited Bulk Email	
Use Block Service(s)	Click to select the check box to enable, and then enter the URL in the field provided.

Click here to return to the Installing and Configuring Allworx Premise Servers or Configuring Connect Vx Instances .

Chapter 33 SNMP Server

Prerequisites	
Access Permissions	Allworx Server Administrator Allworx System Administrator Network Administrator role
Feature Key Required	No

***Note:** SNMP server settings are not available with the Connect Vx service. The appropriate changes/omissions have been made to the Allworx System Administration web page for Connect Vx. In this instance, the entire SNMP page has been removed for Connect Vx.*

The SNMP (Simple Network Management Protocol) server collects information from and configures network devices on an Internet Protocol (IP) network such as:

- Servers
- Hubs
- Routers
- Printers
- Switches

To manage the SNMP server:

1. Log in to the Allworx System Administration web page and navigate to **Servers** > **SNMP**. The *SNMP Server* page displays with the current values.

2. Click **modify** and update the *Enable SNMP Agent* line. Click to select the check box to enable.

3. Click **Update** to save the changes. Any saved changes require restarting the Allworx premise server.

Click here to return to the Installing and Configuring Allworx Premise Servers .

Chapter 34 Reach

Prerequisites	
Access Permissions	Allworx Server Administrator Allworx System Administrator Network Administrator role
Feature Key Required	Reach Link (one feature key for all users)

Allworx Reach extends the rich functionality of Allworx IP phones to iOS and Android devices. The Allworx Reach Link Allworx Reach Extend applications provide additional functionality.

The *Reach* settings use the Reach for Android or Reach for iOS application.

Note: *The Verge 9304 IP Phone does not support the Reach Remote Control or Call Handoff features.*

34.1 Reach Link

Allworx Reach Link™ is a separate feature that supports the Reach application to keep active calls connected as the mobile data network changes. Reach Link plays tones and provides explanations to the other party during network interruptions, and provides recovery methods for calls that cannot be reconnected. Adjusting the Reach Link settings requires permissions enabled within each application.

Note: *In a multi-site network configuration Reach Link functionality is limited to users and handsets configured on an Allworx premise server or Connect Vx instance with the Reach Link feature key installed.*

The following table provides information about where Reach Link settings are entered.

Allworx System Administration web page	My Allworx Manager	Reach Application
• Set the amount of time to determine: • Reach device has lost the premise server or Connect Vx instance connection during an active call. • Begin call restoration after the "Lost Connection Timeout" expires during an active call.	• Set up recovery numbers including descriptions to dial when the connection to an Reach device is lost during an active call per user.	• Set up fallback numbers including descriptions to dial when the connection to a Reach device is lost during an active call per user.
• Select the hold music for the non-Reach user to hear when the Reach connection is lost during an active call.	• Define the restoration number to attempt when an Reach device data connection is lost during an active call per user. • Define the number of rings to wait when attempting a restoration number when an Reach device data connection is lost during an active call per user.	• Define the fallback number to attempt when an Reach device data connection is lost during an active call per user. • Define the final destination when a Reach device data connection is lost during an active call per user.

To manage the Reach Link server:

1. Log in to the Allworx System Administration web page and navigate to **Servers** > **Reach**.
2. In the *Reach Link Server* pane click **modify** and then update the following settings:

Setting	Description
Reach Link Server	Click to select the check box to globally enable or disable Reach Link on all Reach handsets on the premise server or Connect Vx instance.
Lost Connection Timeout (secs)	Enter the amount of time (in seconds) a network is down before the Reach Link reconnection process begins.
Call Recovery Timeout (secs)	Enter the amount of time after starting the Reach Link feature to determine a call is lost.
Hold Music Selection	Select a source for the hold music from the drop-down list.

3. Click **Update** to save the changes. Any saved changes require restarting the Allworx premise server or Connect Vx instance.

34.2 Reach Extend

The Reach Extend feature provides Allworx Reach users with the option to place or receive a call through a cell phone instead of depending on VoIP call quality over Wi-Fi and cellular data networks, while presenting a business Caller ID to remote parties.

This feature is available on a Reach Handset with the following Allworx system setup requirements:

- Connect premise server or Connect Vx instance.
- Trunk lines configured as SIP or T1 PRI lines, or multi-site operation enabled.
  - The Reach Link feature does not work with CO (FXO) trunk lines.
  - If the Allworx system configuration has a CO line as well as SIP and/or PRI lines, and only a CO line is available for a Reach Extend call, that Reach Extend call will not complete. For example, this applies to situations when configuring external dialing rules and choosing a CO line as the Service Group for a particular route selection.

  Note: *T1 and CO lines are not supported with the Connect Vx service.*

- Reach Link feature key installed.

For outgoing calls using the Reach application, users placing calls can select the option to use their cellular service. If selected, the Allworx system automatically places a call to the user's cell number – the user simply needs to answer the cell phone call and press the **1** digit to cause the Allworx system to dial the destination on their behalf using their business Caller ID.

For incoming business calls using the Reach application, the user can select the option to send the ringing call to their cell service. If selected, the call immediately routes to their cell phone to answer using the native cell phone application without answering the call in Reach.

34.3 Reach Push Notifications

Both Android and iOS operating systems have battery management features that restrict background activity in the applications, and the optimal way for VoIP applications to stay connected to the servers (premise or Connect Vx instance) is to use "push notification" services. Allworx Reach users can receive notifications of incoming calls when both the Allworx premise server or Connect Vx instance and the mobile handsets have network connectivity to the Apple Push Notification or the Google Cloud Messaging services. The Allworx administrator configures the Reach Push Notification settings. However, there are no settings in the Reach application for users to modify. Both Android and iOS are encouraging adoption of Push Notifications; therefore, the recommended setting is **Enabled**.

Additionally, Allworx administrators can select **Use Allworx Portal to proxy Push Notifications**, if company network policy or firewall rules require limiting outbound SSL connections to a smaller, more predictable pool of IP addresses (Google and Apple push notification services are highly replicated and the potential IP address ranges are large and unpredictable). There may be circumstances where Allworx Support recommends configuring this on a temporary basis. The recommended setting is **Disabled** so the Allworx premise server or Connect Vx instance uses Google and Apple services directly.

To enable the Reach Push Notifications:

1. Log in to the Allworx System Administration web page and navigate to **Servers** > **Reach**.
2. Locate the *Reach Push Notifications* pane.
3. Click to select the *Enable Reach Push Notifications* check box.
4. (optional) Click to select the *Use Allworx Portal to proxy Push Notifications* check box.
5. Click **Update** to save the changes.

After enabling Push Notifications, the Allworx administrator or an administrator with network administrator permissions can check the push server connection status. Go to **Servers** > **Reach** and locate the *Reach Push Notifications* pane that displays a table with the push service name, domain, resolved IP, and status. This table updates every 10 seconds while the page is active or updates immediately if the user makes a change to the settings.

Click here to return to the Installing and Configuring Allworx Premise Servers or Configuring Connect Vx Instances .

Chapter 35 VoIP Server

Prerequisites	
Access Permissions	Allworx Server Administrator Allworx System Administrator Phone Administrator role Network Administrator role
Feature Key Required	No

The VoIP server supports businesses transferring the traditional phone systems to a dedicated server-based system, and offers a central location to control the internal communications systems.

To manage the VoIP server:

1. Log in to the Allworx System Administration web page and navigate to **Servers** > **VoIP**. The *VoIP Server* page displays with the current values.

2. Click **modify** and update the following settings:

Setting	Description
BLF Port	Typically set to **2088**. If necessary, change for firewall rules. ***Note:*** *This port setting is read-only for Connect Vx instances.*
Secure BLF	Default is unchecked. When enabled, this setting encrypts the checksum of BLF messages making them difficult to spoof.
Force Remote Phone audio through server	For WAN to WAN calls. Select the check box to enable.
Plug and Play Secret Key	Click **show** to see or change the code. Click **hide** to remove from sight. When a new phone attempts to add itself to a server, and is blocked by the feature being disabled or an invalid secret key, a message displays at the top of the Allworx System Administration web page. Clicking the *disabled* link in that message takes the administrator directly to the *VOIP Server* page. Additional messages are also presented in the System Event Log on the server and on the Verge phone start-up screen.

Continued

Setting	Description
Phone Administration Password	Access each handset through a web interface. The phone administration web page has the same look and feel as the Allworx Systems Administration web page; however, the password used to access the phone administration web is NOT the same. • 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). Click **show** to see or change the code. Click **hide** to remove it from sight. ***Note:*** *Users receive an error message when trying to use Allworx as the password. The system does not accept Allworx as the password, enter another password.* **To access the administration page of an Allworx handset:** • From the Allworx System Administration web page and navigate to the **Phone System** > **Handsets** page and then click **handset IP address**. • From a browser, enter the IP address of the handset. Find the IP address using the handset soft keys: **CONFIG** > **Current Status** > **Info**.
Global SIP Connection Limit	Set to at least 1 for SIP trunks, remote phones, remote sites as bandwidth allows.
*Paging Base IP Address**	The multi-cast base IP address used by the premise server. • 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. • Example, if the base address were set to 239.255.10.0, then zone 2 would use multi-cast IP address 239.255.10.2.
*Paging Port**	The UDP port number destination for the packets. All zones use the same port number, but each has its own multi-cast IP address. Enter a value.
*Paging Maximum Hop Count**	Control the time-to-live (TTL) count in the IP header of all paging UDP/RTP frames. Enter a value. • Typically, this value is set to 1 so that the packet is not sent beyond the local subnet. • If there are multiple subnets with phones, increase this value
*Paging Maximum Duration**	Enter a value. Set to between **1** and **30** minutes.
RTP Base Port	Enter a value. ***Note:*** *This port setting is read-only for Connect Vx instances.*
RTP DTMF Payload	Enter a value.
RTP DSCP Tag	Select an option from the drop-down list.
SIP DSCP Tag	Select an option from the drop-down list.
*SIP TCP Ports***	The customizable port(s) the Allworx server receives TCP SIP Messages on. ***Note:*** *This port setting is read-only for Connect Vx instances.*

Continued

Setting	Description
*SIP UDP Ports***	The customizable port(s) on which the Allworx premise server or Connect Vx instance receives UDP SIP Messages. ***Note:** This port setting is read-only for Connect Vx instances, and is preset for ports **5060** and **5070**.*
*Disable Phone Creates via LAN Plug and Play ****	By default, this check box is selected and must be unchecked to allow the plug and play feature to be used.
*Disable Phone Creates via WAN (Remote Phone) Plug and Play****	By default, this check box is selected and must be unchecked to allow the plug and play feature to be used.
Disable Assign User at Phone	Check the box to activate the feature.
Disable PCP Proxy	Check the box to activate the feature.

** Paging is not available with the Connect Vx service.*

***The premise server firewall rules update automatically. The Allworx premise server enables selecting SIP ports for SIP devices from a drop-down list of ports that were valid at boot time. If the Allworx Administrator deletes a SIP port assigned to any device, the Allworx device defaults to the top SIP port defined on the next boot of the Allworx premise server. All devices with assigned, deleted SIP ports are rebooted after changing the ports to the default port when the premise server is rebooted.*

**** Premise servers upgrading from releases prior to 9.0 will retain their existing plug and play settings.*

3. Click **Update** to save the changes. As necessary, restart the Allworx premise server, Connect Vx instance, or handsets.

Setting	Requires a restart		Does not require a restart
	Server or Connect Vx instance	Allworx Handset	
Force Remote Phone audio through server			✓
Phone Administration Password		✓	
Global SIP Connection Limit			✓
Paging Maximum Duration ***Note:** Paging is not available with the Connect Vx service.*			✓
RTP DTMF Payload		✓	
RTP DSCP Tag	✓		

Continued

Setting	Requires a restart		Does not require a restart
	Server or Connect Vx instance	Allworx Handset	
SIP DSCP Tag	✓		
Disable Phone Creates via LAN Plug and Play			✓
Disable Phone Creates via WAN (Remote Phone) Plug and Play			✓
Disable Assign User at Phone			✓
Disable PCP Proxy			✓

Click here to return to the Installing and Configuring Allworx Premise Servers or Configuring Connect Vx Instances .

Chapter 36 Web Server

Prerequisites	
Access Permissions	Allworx Server Administrator Allworx System Administrator Network Administrator role
Feature Key Required	No

The Web server processes requests via HTTP (Hypertext Transfer Protocol) or HTTPS (Hypertext Transfer Protocol Secure). This chapter describes customizing the Web server for the business needs.

Connect premise servers and Connect Vx instances enable HTTPS on the Allworx System Administration web page and My Allworx Manager page.

The Connect premise server and Connect Vx instance default is HTTP **Disabled**. The Allworx administrator can enable or disable HTTP, but cannot disable HTTPS.

Note: *For Connect Vx instances Web Server setting values are read-only and cannot be modified.*

- With HTTP disabled HTTPS is the only communication method:
  - By default access to My Allworx Manager is via secure HTTPS port **443**.
  - By default access to the Allworx System Administration web page is via secure HTTPS port **8443**.
- With HTTP enabled (Connect premise servers only):
  - Access to My Allworx Manager and the Allworx System Administration web page is via the insecure HTTP port on all network interfaces, except the public network interface.
  - The Connect premise servers do not enable insecure HTTP access on the public network interface. With HTTP enabled on a Connect premise server, both HTTP and HTTPS are available on the assigned ports.

36.1 Managing the Web Server Settings

With the release of Allworx System Software 9.1, the configuration of the minimum version of the Transport Layer Security (TLS) protocol has been added to the Web Server settings. This setting affects access to the Allworx System Administration web page and View connectivity.

1. Log in to the Allworx System Administration web page and navigate to **Servers** > **Web**. The *Web Server* page displays with the current values.

   For Connect Vx instances most of these values are read-only and cannot be modified. The only value that can be set for Connect Vx instances is the Minimum TLS Version.

2. In the *Web Server* pane at the top of the page click **modify** to update the values described in the following table:

Field	Description
Settings	
Connection Timeout (secs)	Enter a value for the number of seconds of inactivity before a connection timeout.
Maximum HTTP/HTTPS Sessions	Enter a value for the maximum number of simultaneous sessions – HTTP and/or HTTPS.
Secure Web (HTTPS)	
*My Allworx Manager Secure Port (HTTPS)**	Enter a value - port **443** is the default value.
*Web Administration Secure Port (HTTPS)**	Enter a value - port **8443** is the default value.
Secure Remote Administration Port	Enter a value - port **XXXX** is the default value.
Minimum TLS Version (Available for Connect Vx instances and premise servers.)	Click to select a value from the drop-down menu. To preserve backward compatibility, the default value is **TLS 1.0;** however, **TLS 1.2** is the recommended. ***Note:*** *If this setting is changed to TLS 1.2, any connected instances of View must have a Windows registry modification applied to them.*
Insecure Web Access (HTTP) Check this box to enable HTTP. ***Note:*** *HTTP access on the Connect server's public interface is not supported.*	
*My Allworx Manager Port (HTTP)**	Enter a port number.
*Web Administration Port (HTTP)**	Enter a port number.
* Feature is only available on the Connect servers.	

3. Click **Update** to save the changes.

   To have the change(s) take effect, restart the Allworx premise server.

36.2 Secure Communication: Keys and Signed SSL Certificates

Allworx Connect premise servers generate a public key, private key, and self-signed SSL certificate to use with HTTPS at first boot up, after formatting the premise server disk, and after removing a user-installed, self-signed certificate. The certificate and keys can be reset as described in the table included later in this section.

Connect premise servers and Connect Vx instances present an HTTPS interface for access to both the Allworx System Administration web page and My Allworx Manager page. For secure communication, public and private keys are used to ensure that requests cannot be read or changed during transfer, and a signed SSL certificate authenticates the identity of the server and Connect Vx instance.

Web browsers will present security warning messages when accessing Allworx System Administrator web pages, if the Allworx system does not have an externally-signed certificate installed. By default, Allworx premise servers use a self-signed certificate (which will cause security warnings), unless the administrator has acquired and installed an SSL certificate. Allworx Connect Vx instances include a signed SSL certificate in the ***.hostedallworx.com** domain, so browsers will not present security warnings when using URLs with that domain name. Administrators are also free to install their own SSL certificates if they wish to access their systems with their own domain names.

36.2.1 Managing the Installed Certificate

Only one certificate at a time is installed and active on the Allworx premise server and Connect Vx instance. These steps display information about the currently installed certificate.

Note: *Allworx installs a server certificate on every Connect Vx instance before delivering it to the customer. Connect Vx service system administrators are able to disable this built-in certificate and install one of their choosing following the steps in Obtaining and Installing a Signed SSL Certificate .*

To manage an installed certificate:

1. Log in to the Allworx System Administration web page and navigate to **Servers** > **Web**.

2. Locate the *Installed Server Certificate* pane and click the additional information arrow ►, if necessary, to display the certificate information.

3. Click to select the following:

import/export *(Located in the last paragraph of text at the bottom of the pane.)*	Provides a shortcut to the *Export Configuration / Import Configuration* screen where the current keys and SSL certificate can be exported, or the previously exported keys and SSL certificate can be imported. ***Note:*** *Exporting keys and an SSL certificate can act as a backup when premise server maintenance procedures may destroy the information.*
Reset Server Certificate	Deletes the current certificate and the private key, and then creates a new self-signed certificate and private key. Click **Yes** to proceed and **No** to disregard the request.

36.2.2 Obtaining and Installing a Signed SSL Certificate

1. Create a Certificate Signing Request (CSR) by completing the form on the *Web Server* page of the Allworx System Administration web page. Go to **Server** > **Web** and view the *Server Certificate Signing Request* pane. Click the additional information arrow ►, if necessary.

   Note: *If you receive a message indicting that the site is not secure when opening the Administration web page, click **Details** or **Advanced** and select the option to visit the website anyway. Installing a signed digital certificate ensures that this message no longer appears when accessing the web page.*

2. Enter information in to the text fields. The information provided will be encrypted into the request file that the Certification Authority uses to create the signed SSL certificate.

   Note: *Although the information entered in the text fields is left to the discretion of the administrator, this information should accurately reflect the location and organizational information as dictated by the business.*

3. Click to select the *Include server IP addresses in subject alternative field* check box, if required.

4. Click **Create CSR** to create a CSR hash file that displays in the window.

5. Copy all lines of the file that are displayed and save it as a text file with the extension **.pem**.

6. Submit the text file to a Certificate Authority (CA) that will verify the request (for a fee) and provide a signed SSL certificate (another **.pem** file) for installation on the server.

7. When the certificate is returned by the CA, locate the *Server Certificate Installation* pane and click the additional information arrow ▶, if necessary.

8. Follow the steps included in that pane to install a new certificate for secure web access (HTTPS). Verify that the certificate adheres to the *Certificate Format* guidelines listed after the installation instructions.

9. Click to select a link to perform the following actions:

Action	Description
Show / Hide	Displays or hides an example certificate.
import/export	Navigation shortcut that goes to the *Export Configuration/Import Configuration* page where administrators can import the keys and SSL certificate that have been exported earlier. ***Note:*** *Only files of exported keys and SSL certificates can be imported.*
Install	Starts the certificate confirmation/installation process.
Cancel	Disregards the request.

36.3 Client Certificates for Secure Remote Administration

Allworx provides a method for managing Allworx Connect premise servers and Connect Vx instances remotely over the Allworx server public interface using Client Certificates for Secure Remote Administration generated on the premise server or Connect Vx instance using the Allworx System Administration web page.

After generating a client certificate on an Allworx system, administrators can install that certificate on remote devices such as PCs, tablets, or smart phones in order to manage the Allworx system remotely. Each client certificate is cryptographically tied to the specific Allworx system that generated it; the client certificate only allows access to that specific Allworx system.

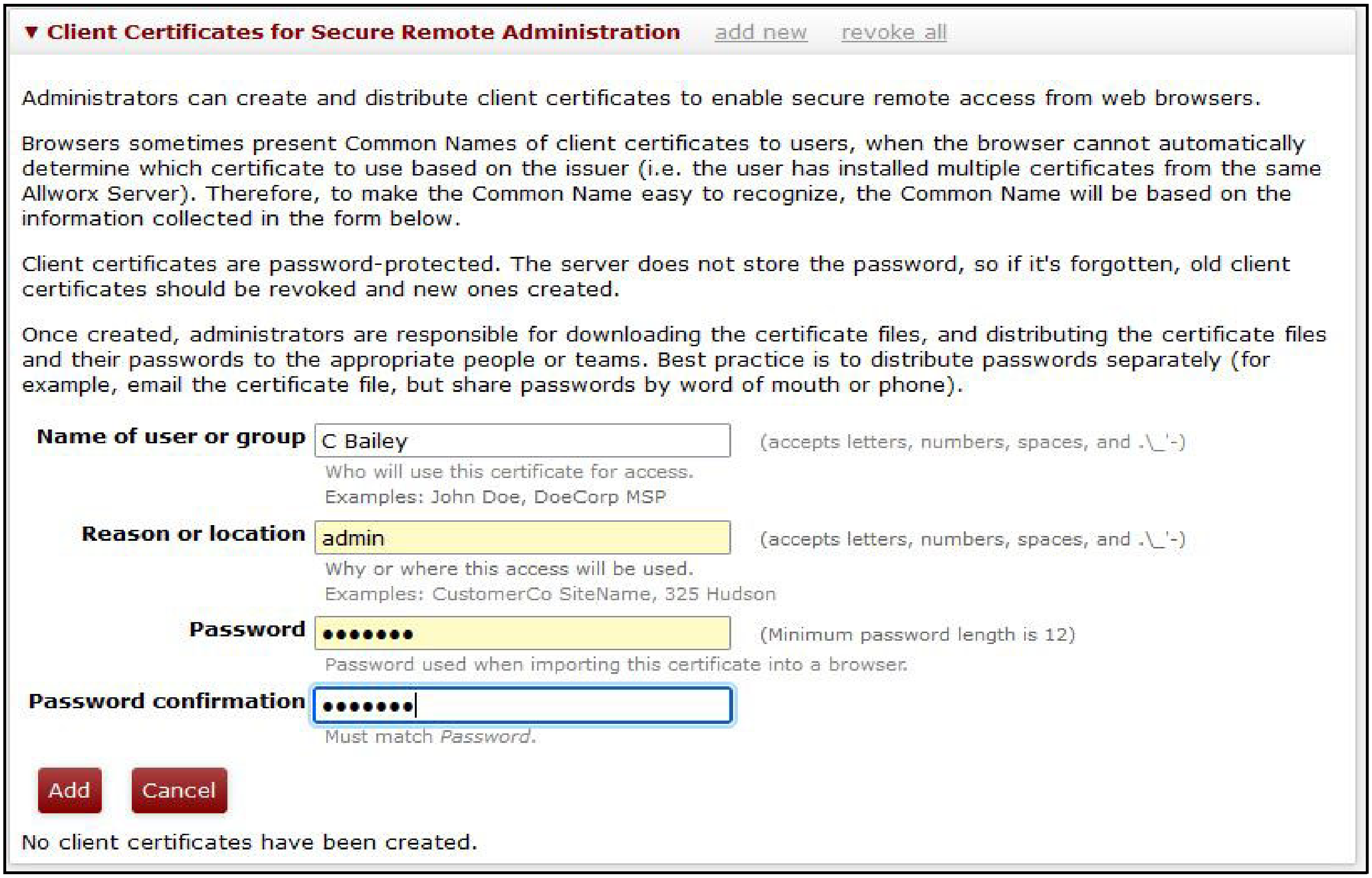
***Note:** Client certificates allow access to the Allworx System Administration web page only and do not provide network-level access to the remote Allworx system (e.g., switches or phones on the private network of that server).*

After creating the first client certificate the Allworx system also generates a Certificate Authority, which uniquely identifies the specific Allworx system.

To add a new Client Certificate for Secure Remote Administration:

1. Log in to the Allworx System Administration web page and navigate to **Servers** > **Web**. The *Web Server* page displays with the current values.

2. At the *Client Certificates for Secure Remote Administration* pane click the additional information arrow ►, if necessary.



▼ Client Certificates for Secure Remote Administration add new revoke all

Administrators can create and distribute client certificates to enable secure remote access from web browsers.

Browsers sometimes present Common Names of client certificates to users, when the browser cannot automatically determine which certificate to use based on the issuer (i.e. the user has installed multiple certificates from the same Allworx Server). Therefore, to make the Common Name easy to recognize, the Common Name will be based on the information collected in the form below.

Client certificates are password-protected. The server does not store the password, so if it's forgotten, old client certificates should be revoked and new ones created.

Once created, administrators are responsible for downloading the certificate files, and distributing the certificate files and their passwords to the appropriate people or teams. Best practice is to distribute passwords separately (for example, email the certificate file, but share passwords by word of mouth or phone).

Name of user or group: C Bailey (accepts letters, numbers, spaces, and ._'-)
Who will use this certificate for access.
Examples: John Doe, DoeCorp MSP

Reason or location: admin (accepts letters, numbers, spaces, and ._'-)
Why or where this access will be used.
Examples: CustomerCo SiteName, 325 Hudson

Password: ••••••• (Minimum password length is 12)
Password used when importing this certificate into a browser.

Password confirmation: •••••••
Must match *Password*.

No client certificates have been created.

3. Click **add new** to open the form to enter the following information:

Text Field	Description
Name of user or group	The individual or group requiring the certificate for access. Accepts letters, numbers, spaces, and ._'-
Reason or location	Why or where this access is used. Accepts letters, numbers, spaces, and ._'-
Password	A password to import this certificate into a browser (Minimum password length is 12 characters). Make a note of the password as it will be required for other tasks.
Password confirmation	Retype to confirm the password; the two passwords must match.

4. Click **Add**. The Allworx System Software generates and adds the client certificates to the table. Click **Cancel** to ignore the request. The certificate can now be downloaded, viewed, and revoked if necessary. For more information, see “To manage Client Certificates for Secure Remote Administration:” on page 304.

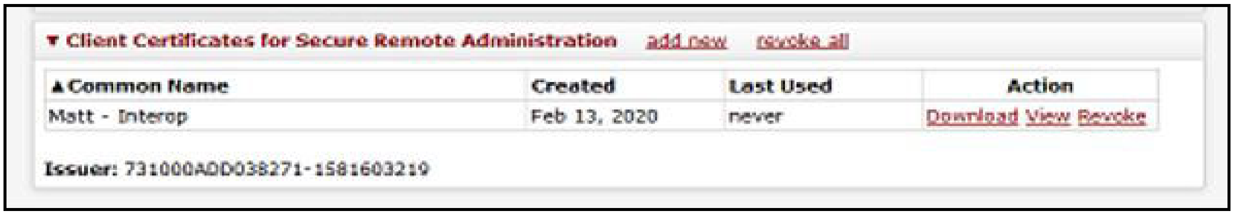
To ensure the ability to remotely access the Allworx system on the remote administration port, Allworx system administrators must first navigate to **Network** > **Configuration** to verify that the *HTTPS: Secure Remote Administration (TCP 8043)* option is **enabled**.

If this option is not enabled, click **modify** to display the configuration options. In the *Firewall* pane, click to select the *HTTPS: Secure Remote Administration (TCP 8043)* check box. This may need to be done via the server LAN prior to the first use of a Client Certificate for Secure Remote Administration.

To manage Client Certificates for Secure Remote Administration:

The Allworx System Software identifies client certificates by *Common Name*, which is a combination of the *Name of User or Group* and *Reason and Location* fields in the creation form.

1. Log in to the Allworx System Administration web page and navigate to **Servers** > **Web**. The *Web Server* page displays with the current values.



▼ Client Certificates for Secure Remote Administration add new revoke all

▲Common Name	Created	Last Used	Action
Matt - Interop	Feb 13, 2020	never	Download View Revoke

Issuer: 731000ADD038271-1581603219

2. Locate the *Client Certificates for Secure Remote Administration* pane; click the additional information arrow ►, if necessary. The table of client certificates displays.

3. Click one of the following actions to manage the client certificates:

Note: *Click a column heading to sort multiple client certificates in ascending or descending order.*

Action	Description
Download	Saves a copy of the client certificate by downloading it to the local computer. Be sure to make a note of the location.
View	Displays detailed information about the client certificate.
Revoke	Invalidates the client certificate -- requires a confirmation and cannot be undone.

After revoking all the client certificates, the Allworx premise server and Connect Vx instance deletes the Certificate Authority; a new Certificate Authority is re-created after generating a new client certificate. During a migration or restore operation, the Certificate Authority and all generated client certificates migrate or restore as well. This allows partners the greatest flexibility in how to create and distribute client certificates for customer premise servers and Connect Vx instances.

Partners that want to manage a fleet of premise servers using a single client certificate can generate the certificate on a “template” server and then clone that server using the Migrate tool. Partners that want to manage the fleet using a unique certificate for each server can do so by not creating any client certificates on a “template” server, and then creating the client certificate on each server individually.

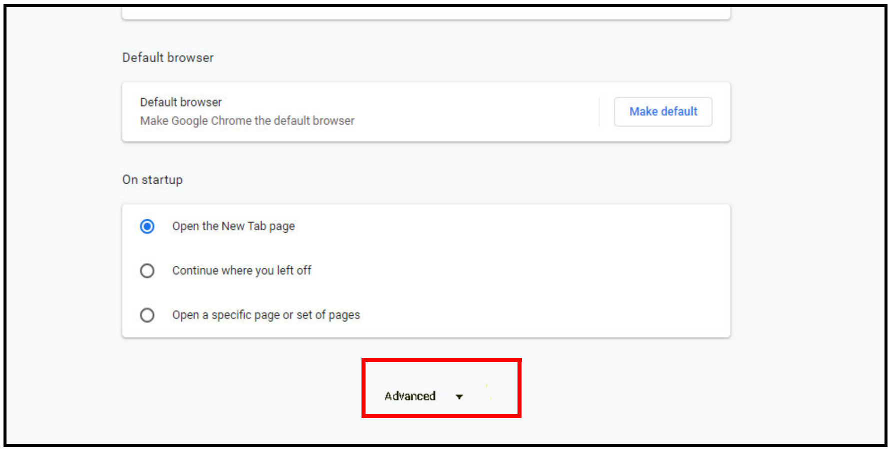
Note: *At this time, the Migrate tool is not available with the Connect Vx service.*

After generating the client certificate Allworx administrators can provide the certificate to one or more administrators to install on a PC or in a web browser. After the installation, administrators can access the Connect premise servers and Connect Vx instances using the public IP address and the secure remote administration port (8043).

To import a certificate (this example uses the Chrome web browser):

1. Open the web browser and click the three dots in the upper right corner.

2. Scroll to the bottom of the list and click **Advanced**.



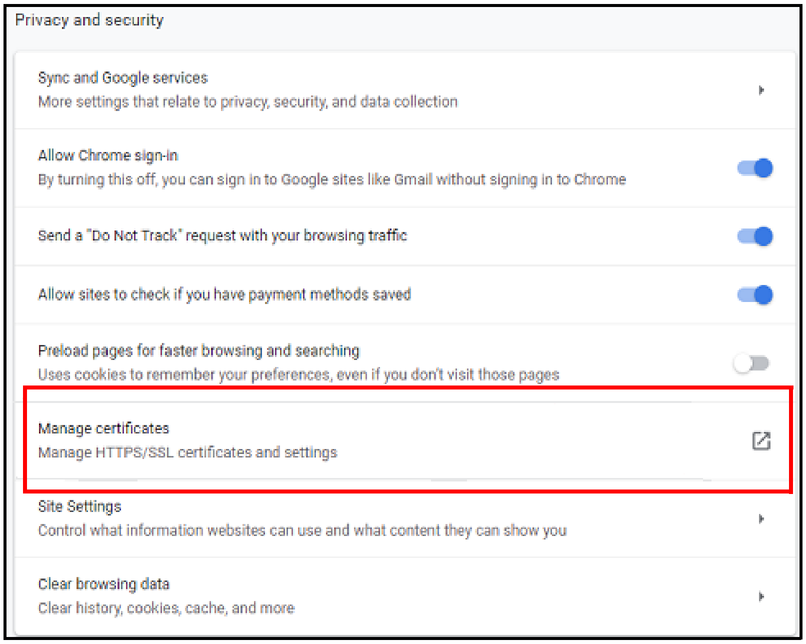
Default browser

Default browser
Make Google Chrome the default browser

On startup

● Open the New Tab page
○ Continue where you left off
○ Open a specific page or set of pages

3. Under *Privacy and security* click (↗)to expand *Manage certificates*.



Privacy and security

Sync and Google services
More settings that relate to privacy, security, and data collection

Allow Chrome sign-in
By turning this off, you can sign in to Google sites like Gmail without signing in to Chrome

Send a "Do Not Track" request with your browsing traffic

Allow sites to check if you have payment methods saved

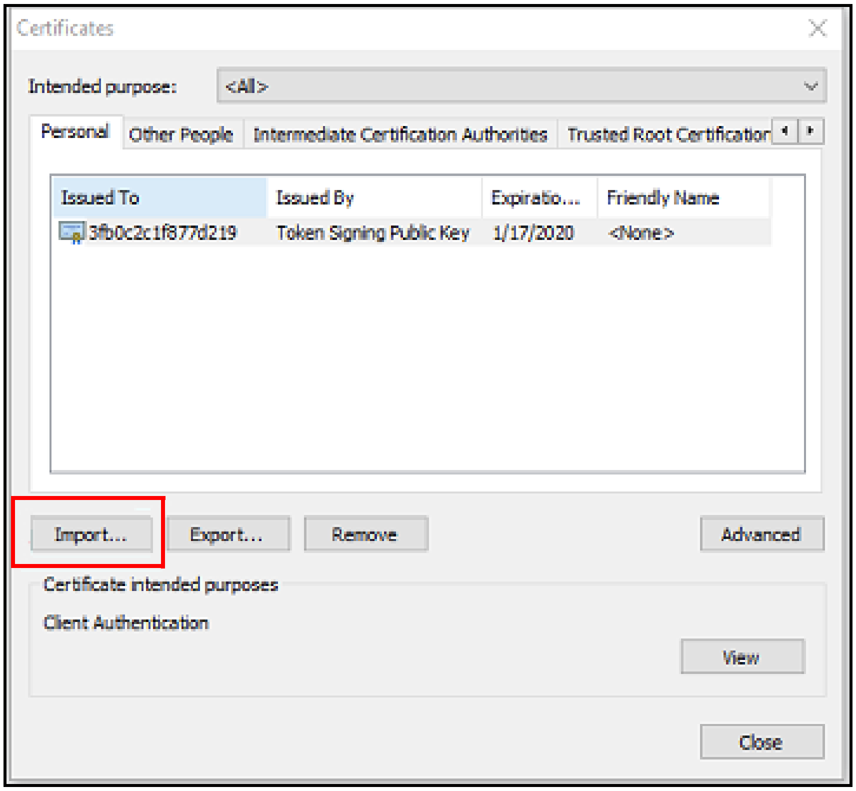
Preload pages for faster browsing and searching
Uses cookies to remember your preferences, even if you don't visit those pages

Manage certificates
Manage HTTPS/SSL certificates and settings

Site Settings
Control what information websites can use and what content they can show you

Clear browsing data
Clear history, cookies, cache, and more

4. Click **Import**. The *Certificate Import Wizard* opens.



Certificates

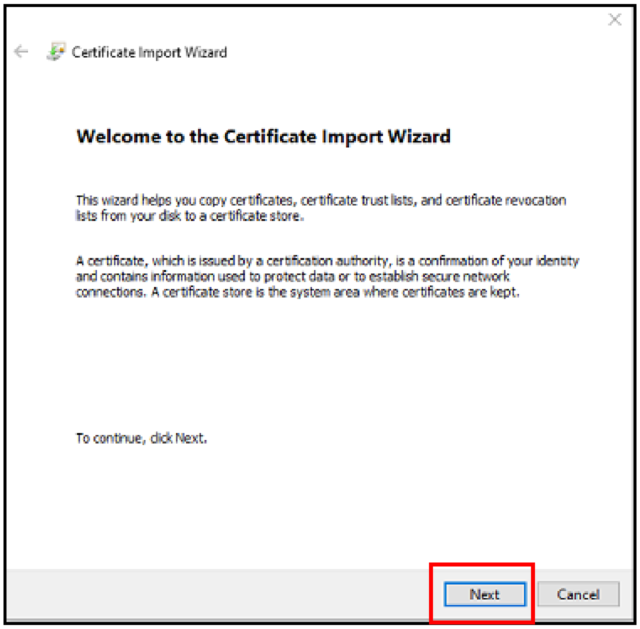
Intended purpose: <All>

Personal | Other People | Intermediate Certification Authorities | Trusted Root Certification

Issued To	Issued By	Expiratio...	Friendly Name
3fb0c2c1f877d219	Token Signing Public Key	1/17/2020	<None>

Certificate intended purposes
Client Authentication

5. Click **Next**.



Certificate Import Wizard

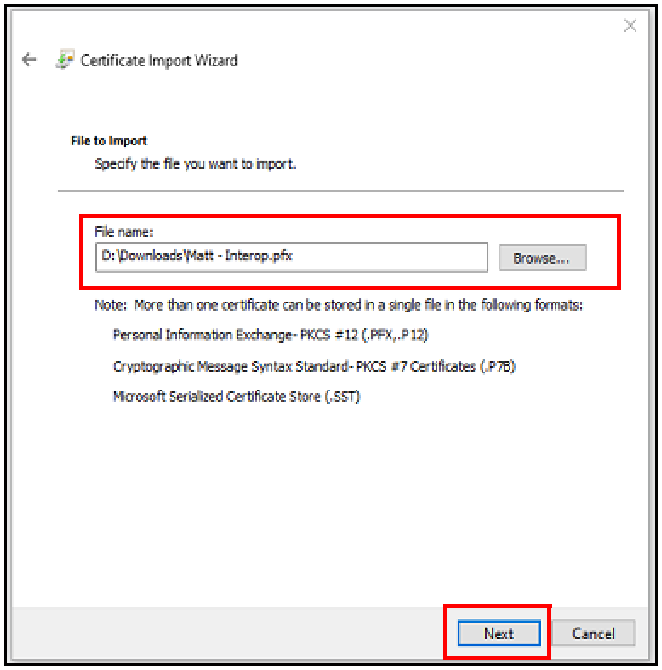
Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

6. Browse to select the certificate that has been downloaded.



Certificate Import Wizard

File to Import

Specify the file you want to import.

File name:

D:\Downloads\Matt - Interop.pfx

Note: More than one certificate can be stored in a single file in the following formats:

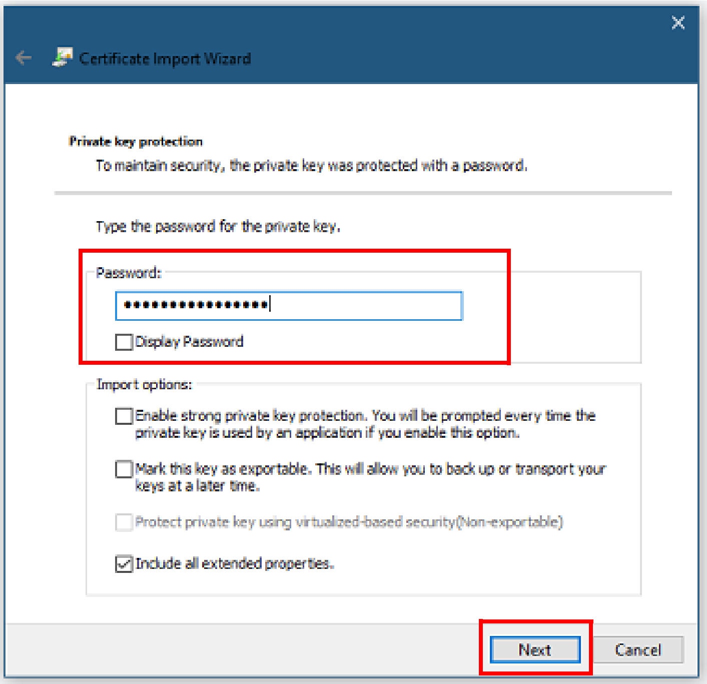
Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

7. Click **Next**.

8. Enter the password that was used when the certificate was created.



Certificate Import Wizard

Private key protection

To maintain security, the private key was protected with a password.

Type the password for the private key.

Password:

••••••••••••••••

□ Display Password

Import options:

□ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

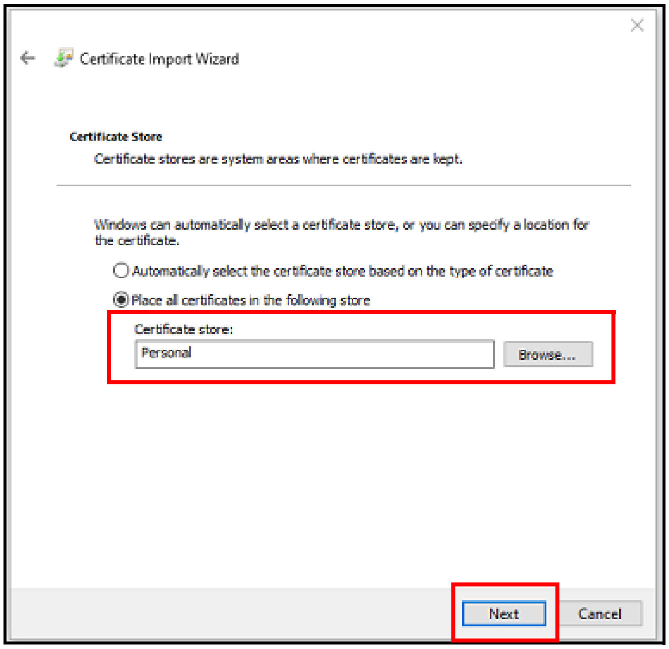
□ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

□ Protect private key using virtualized-based security(Non-exportable)

☑ Include all extended properties.

9. Click **Next**.

10. Click to select the *Place all certificates in the following store* radio button.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

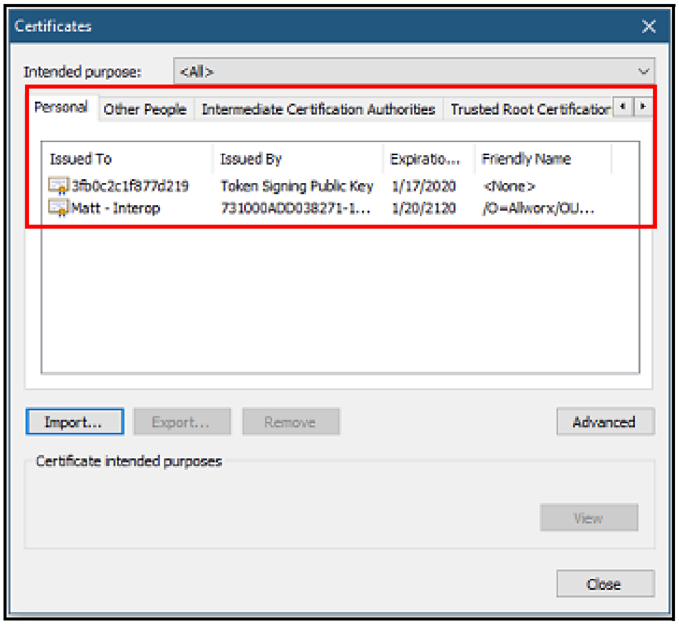
● Place all certificates in the following store

Certificate store:

Personal

11. Click **Browse** to select the *Personal* store, if necessary.

12. Click **Next** and then click **Finish**.



Certificates

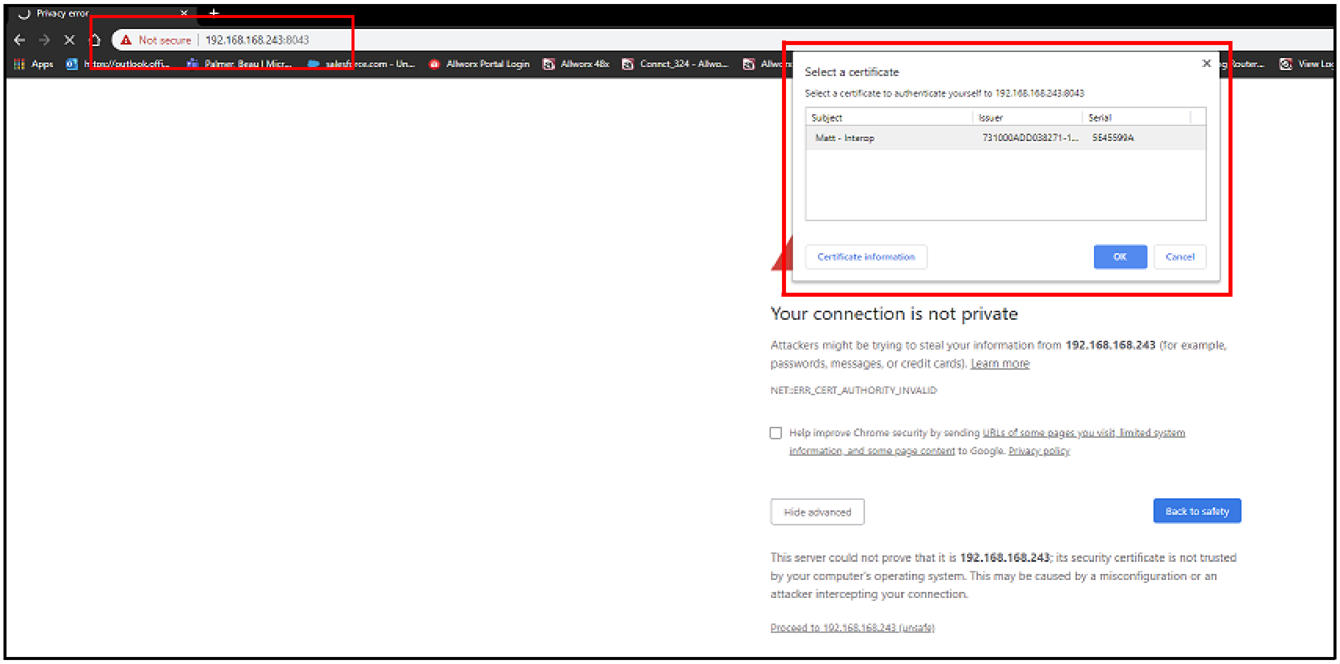
Intended purpose: <All>

Personal | Other People | Intermediate Certification Authorities | Trusted Root Certification

Issued To	Issued By	Expiratio...	Friendly Name
3fb0c2c1f877d219	Token Signing Public Key	1/17/2020	<None>
Matt - Interop	731000ADD038271-1...	1/20/2120	/O=Allworx/OU...

The certificate is successfully imported.

13. Open a new web browser tab and go to the IP Address with client port 8043. In this example, **https://192.168.168.243:8043**.



Select a certificate

Select a certificate to authenticate yourself to 192.168.168.243:8043

Subject	Issuer	Serial
Matt - Interop	731000ADD038271-1...	5E45599A

Your connection is not private

Attackers might be trying to steal your information from **192.168.168.243** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

☐ Help improve Chrome security by sending URLs of some pages you visit, limited system information, and some page content to Google. Privacy policy

This server could not prove that it is **192.168.168.243**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to 192.168.168.243 (unsafe)

14. Accept and continue to the page with the text *Your connection is not private*.

15. Select a certificate from the list.

16. Click **OK**.

17. Log in to the server.

Now when the client or user browses to the web address using https and the client port of 8043 they are not prompted with the security warning, and the system events tracks who logged into the premise server or Connect Vx instance. This is a good method for tracking who logs in and makes changes. However, the event log does not track changes made to their premise server or Connect Vx instance.

Click here to return to the Installing and Configuring Allworx Premise Servers or Configuring Connect Vx Instances .

Section 6 Reports

The Reports features support customizing the reports specific to the business requirements. Each chapter explains:

- Necessary access permissions and feature keys
- Necessary equipment to perform the procedures
- Necessary procedures to setup and customize the Allworx server network

Feature and procedure differences for the Allworx Connect Vx service are noted in each chapter.

The various *Reports* pages on the Allworx System Administration web page enable the Allworx administrator to access the following information:

Chapter 37 About

Prerequisites	
Access Permissions	Allworx Server Administrator Allworx System Administrator Phone Administrator Role Network Administrator Role Support Technician Role
Feature Key Required	No

The *About* page displays information about the Allworx system that includes server model, software version, and last successful premise server backup.

To view the About page:

1. Log in to the Allworx System Administration web page and navigate to **Reports** > **About**. The page displays with the Allworx system information.

   For the Connect Vx service this report does not include temperature, disk, and memory information.

2. Click one of the following actions:

Action	Description
show logged in administrators / hide logged in administrators	Displays or removes the administrators currently logged in to the Allworx system, respectively.
Open Source Licenses	Displays the Open Source Licenses associated with the application. To return to the Allworx System Administration web page click the browser back button.

Click here to return to the Installing and Configuring Allworx Premise Servers or Configuring Connect Vx Instances .

Chapter 38 Allworx View

Prerequisites	
Access Permissions	Allworx Server Administrator Allworx System Administrator Phone Administrator Role Network Administrator Role Support Technician Role
Feature Key Required	• Allworx View CDR • Allworx View ACDR

The Allworx View application is a significantly enhanced version of the Call Detail Record (CDR) streaming feature, which gives dynamic, comprehensive usage reporting on the Allworx phone system The View application provides separate connections and interaction between the Allworx View application and the Allworx premise server or Connect Vx instance, and does not replace the current CDR streaming feature available for Allworx premise servers. CDR streaming is not available when using the Allworx Connect Vx service.

Additionally, the Allworx View ACD add-on application:

- Offers real-time contact center and analysis to maximize agent productivity
- Ensures an optimal experience for customers
- Provides customizable dashboards for supervisors and agents
- Displays the selected information using any popular web browse
- Uses configurable alarms for supervisors and agents to recognize and react to high call volume situations and minimize abandoned calls and frustrated customers

To change the port:

1. Log into the Allworx System Administration web page and navigate to **Reports** > **Allworx View**.
2. Locate the *Allworx View Settings* pane and click one of the following actions:

Action	Description
Reset Allworx View port	• **Port Reset** - shuts down any current connection from an Allworx View client, and then re-initializes the port. The Allworx View client re-connects without user intervention using the same authentication token as when it was previously connected. This is best used as a recovery step when there are connection problems. • **Authentication Token Reset** - (see Modify below) a security-related configuration change that disconnects an Allworx View application client, but with no port reset and requires user authentication for Allworx View to re-connect. This is best used when changing access permissions, such as removing a user with View administration permissions from the system.

Continued

Action	Description
Modify	• **TCP/IP Port** - This value is **54441** for Connect Vx instances and is read-only. For all other Connect premise servers enter the TCP IP Port number in the field. • **Reset Authentication Token** - Check the box to enable.

3. Click **Update** to save the changes.

Click here to return to the Installing and Configuring Allworx Premise Servers or Configuring Connect Vx Instances .

Chapter 39 Auto Notification

The Auto Notification report supports configuring automatic email notifications for specified systems events to specific users. Notifications for expiring feature keys will be sent to all configured notification email addresses. This does not require severity or log text filtering.

Note: *Auto Notification is discussed in the Remote Monitoring of an Allworx Phone System white paper that is available on the Allworx Portal.*

Prerequisites	
Access Permissions	Allworx Server Administrator Allworx System Administrator Phone Administrator Role Network Administrator Role Support Technician Role
Feature Key Required	No

To setup the Auto Notification:

Prior to performing this procedure, set up the email services. See "Email" on page 283 for more information.

1. Log into the Allworx System Administration web page and navigate to **Reports** > **Auto Notification**.
2. Locate the *Auto Notification* pane, and click **modify**. Update the following settings:

Settings	Description	
Auto Notification		
Modify	Update the current settings. Check the Enable Notification check box, if not already checked and edit the settings, as required.	
	Enable Message Severity Filtering	Check the required filters: • Emergency (0) • Critical (2) • Warning (4) • Info (6) • Alert (1) • Error (3) • Notice (5) • Debut (7)
	Enable Log Text Filtering	Check the box to enable and update the settings: • Maximum number of notifications per day - enter a number. (This option is per a 24-hour period from the last Allworx premise server or Connect Vx instance reboot.) • Timeout for sending notifications (min) - enter a number. • Maximum number of messages per notification - enter a number. • Email subject - Enter information. • Email header - Enter information.
	Click **Update** to save the changes.	

Continued

Settings	Description
Flush Pending Notifications	Clear any pending notifications.
Text Filtering - requires enabling in Auto Notification > Modify > Enable Log Text Filtering pane.	
add new text filter	Enter a new text filter. Click **Add** to save the change.
delete all	Delete all of the text filters. Click **OK** to remove the filters.
Modify	Change the text filter information. Click **Update** to save the change.
Delete	Delete the text filter information. Click **OK** to save the change.
Email Addresses - requires enabling in Auto Notification > Modify > Enable Auto Notification.	
add new email address	Enter a new email address. Click **Add** to save the change.
delete all	Delete all the email addresses. Click **OK** to remove the filters.
Modify	Change the email address. Click **Update** to save the change.
Delete	Delete the email address. Click **OK** to delete the email address.

Click here to return to the Installing and Configuring Allworx Premise Servers or Configuring Connect Vx Instances .

Chapter 40 Call Details

The Call Details report supports managing a Call Details Report from the premise server or Connect Vx instance. The buffer limit is 5,000 records on Allworx Connect premise servers and Connect Vx instances.

Prerequisites	
Access Permissions	Allworx Server Administrator Allworx System Administrator Phone Administrator Role Network Administrator Role Support Technician Role
Feature Key Required	No

To change the Call Details Settings:

1. Log into the Allworx System Administration web page and navigate to **Reports** > **Call Details**.
2. Locate the *Call Details Settings* pane and click **modify**. Update the following settings:

Settings	Description	
Call Detail Settings		
modify	1. Change the current settings.	
	Call Detail Storage	Identify what to store. Select an option from the drop-down list. • Do not store calls • Store Completed Calls only • Store Live Calls only • Store Live and Completed Calls
	Call Detail Streaming ***Note:*** *For Connect Vx instances this value cannot be modified and is permanently set to* ***Do not stream calls****.*	Identify what to stream. Select an option from the drop-down list. • Do not stream calls • Stream Completed Calls • Stream Completed Calls only • Stream Live Calls only • Stream Live and Completed Calls
	Call Detail Streaming Port	Enter the port number in the field. The default port number is **16366**. This field is not available for Connect Vx instances.
	2. Click **Update** to save the changes.	

Continued

Settings	Description
Completed Calls Detail Report	
delete	Removes specific calls from the report. Select: • *Delete all calls* • *Delete calls made before* - select the date from the drop-down list. Click **Delete** to save the changes.
Report Start Date	Enter a date in the field and select the number of days to include in the report from the drop-down list.
View Report	Display the report on the computer screen.
Export TSV Report	Export the report to a *Tab Separated Values* format.
Export XML Report	Export the report to an *Extensible Markup Language* format.

Click here to return to the Installing and Configuring Allworx Premise Servers or Configuring Connect Vx Instances.

Chapter 41 Configuration

The Configuration report provides the Allworx premise server or Connect Vx instance configuration information such as, but not limited to system settings, network settings, internal dial plans, phones, and users.

Prerequisites	
Access Permissions	Allworx Server Administrator Allworx System Administrator Support Technician role
Feature Key Required	No

To manage the Configuration Report:

Click the **Generate XLS Report** button to create a configuration report. This report may take up to 10 minutes to complete.

To see the report, click **View** next to the Excel workbook file. The worksheet tabs at the bottom of the report provide specific configuration information.

Click here to return to the Installing and Configuring Allworx Premise Servers or Configuring Connect Vx Instances .

Chapter 42 T1 Lines

Note: *T1 lines are not available with the Connect Vx virtual server. The appropriate changes/ omissions have been made to the Allworx System Administration web page for Connect Vx. In this instance, the entire T1 Lines page has been removed for Connect Vx.*

The T1 Lines report displays the information specific to each T1 Line.

Prerequisites	
Access Permissions	Allworx Server Administrator Allworx System Administrator Support Technician role Network Administrator role
Feature Key Required	No
Servers	Allworx Connect 731
* Not all features on the *Roles* page are available to Phone Administrators. These features require Allworx Server Administrator or Allworx System Administrator permissions.	

To manage the T1 Lines report:

1. Log in to the Allworx System Administration web page and navigate to the **Reports** > **T1 Lines** page. A window displays the information for each T1 Line.
2. Click one of the following options:

Option	Description
Clear Report	Clears the current information from the viewable report.
Refresh Report	Updates the current information on the report.

Click here to return to the Installing and Configuring Allworx Premise Servers .

Chapter 43 Live Calls

The Live Calls report displays the call information in a separate browser window.

Prerequisites	
Access Permissions	Allworx Server Administrator Allworx System Administrator Support Technician role
Feature Key Required	No

To display Live Calls:

1. Log in to the Allworx System Administration web page and navigate to the **Reports** > **Live Calls** page. A separate window opens.
2. Perform one of the following actions:
   a. Click to select the *Auto Refresh* check box.
   b. Click **Refresh Now**. This action requires clicking at least once every 30 seconds.
3. Click the **X** on the browser window or tab to close the Allworx System Administration web page (not the Live Calls window). Do not log out of the web page before closing.

To hide or show the Queued Calls or Active Calls, click **hide** or **show**, respectively.

Click here to return to the Installing and Configuring Allworx Premise Servers or Configuring Connect Vx Instances .

Chapter 44 Phones

Prerequisites	
Access Permissions	Allworx Server Administrator Allworx System Administrator Support Technician role
Feature Key Required	No

This page discusses two reports:

- Download of the diagnostic log files from Verge phones (one phone at a time) registered with this Allworx premise server or Connect Vx instance
- a *PFK Programming* report to view the programmable function keys and features assigned to each Verge phone, Interact Softphone, and Reach handset

To manage the phone diagnostic log files download:

1. Log in to the Allworx System Administration web page and navigate to **Reports** > **Phones**.
2. Locate the *Choose phone* drop-down list and select an available phone in the list.
3. Click **Request files** to pull the diagnostic files for the selected phone to the Allworx premise server or Connect Vx instance.
4. Click **Download files** to download and save those files to the PC.

   Select whether to open or save the file and click **OK** in the *Opening* pop-up window.
5. Click **Remove files** to remove that phone diagnostic log from the report page.

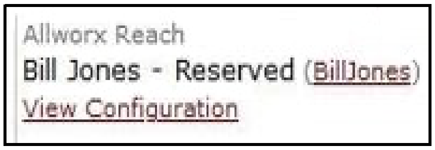
To generate a PFK programming report:

1. Log in to the Allworx System Administration web page and navigate to **Maintenance** > **Phones**.
2. In the *PFK Programming Report* pane make a selection from the *Display phones with selected PFK Type* drop-down message.

   Note: *In addition to the selection of All PFK Types, this drop-down menu displays only the types of PFK currently in use within the system.*
3. The report displays in the pane as soon as a PFK type is selected.

Click **View Configuration** under each phone in the report to go to the **Phone System** > **Handsets** > **View Configuration** page for that phone. Adjustments to the phone configuration can be made from this web page.

For Reach phones, click the name link next to the user name to open the Allworx Reach Configuration window.



Allworx Reach
Bill Jones - Reserved (BillJones)
View Configuration

Click here to return to the Installing and Configuring Allworx Premise Servers or Configuring Connect Vx Instances .

Chapter 45 Resource Summary

The Resource Summary report describes current Allworx premise server and Connect Vx instance configurations, maximum admissible configurations, and current license usage counts. Additionally, the *Resource Summary* page supports viewing the compatibility of the current configuration with other server models and the Last Migration Upload Summary for premise servers.

Prerequisites	
Access Permissions	Allworx Server Administrator Allworx System Administrator Phone Administrator role Network Administrator role Support Technician role
Feature Key Required	No

To manage the Resource Summary report:

1. Log in to the Allworx System Administration web page and navigate to the **Reports** > **Resource Summary** page. The page displays the current Allworx premise server and Connect Vx instance information.

2. (Requires that the service PC has an Internet connection) For premise servers, click **check server compatibility** to determine Allworx server data configuration compatibility with other Allworx server models.

   Checking the server compatibility is helpful if there is a need to replace the current Allworx premise server with a different Allworx premise server model or a Connect Vx instance. The *Migration Compatibility Table* appears.

   Note: *The check server compatibility option is not available with the Connect Vx service Resource Summary report.*

3. At the top of the *Migration Compatibility Table*, select a different Allworx server model from the drop-down menu.

   A table displays with both the current server counts and the selected server model capabilities.

Indication	Description
Green	Configuration is compatible.
Yellow	Configuration is incompatible. Line item describes the issue and suggests a remedy to fix the incompatibility.

Click here to return to the Installing and Configuring Allworx Premise Servers or Configuring Connect Vx Instances .

Chapter 46 System Events

Prerequisites	
Access Permissions	Allworx Server Administrator Allworx System Administrator Support Technician role
Feature Key Required	No

The System Events report displays system information (i.e., server type, MAC address, software version, etc.) and log information.

To manage the System Event Severity filtering:

1. Log in to the Allworx System Administration web page and navigate to **Reports** > **System Events**.

   Note: *For Connect Vx instances this report does not include disk and memory information.*

2. Click one of the following actions:

Action	Description
show Severity Filter / hide Severity Filter	Opens or closes the *Event Severity Filtering* pane, respectively. Check the filter boxes to select the filters to display. Click Apply Filter to save the changes or Reset Default Filter to use the factory default settings.
Download	Downloads the system events to a text (**.txt**) file.

Click here to return to the Installing and Configuring Allworx Premise Servers or Configuring Connect Vx Instances .

Chapter 47 Users

The Users report displays a list of all active users in the business directory including the associated extension, user name, and messages/space used as well as email and Voicemail (*Vmail*) information.

Prerequisites	
Access Permissions	Allworx Server Administrator Allworx System Administrator Network Administrator role
Feature Key Required	No

To manage the *Users* page:

1. Log in to the Allworx System Administration web page and navigate to **Reports** > **Users**.
2. Click one of the following options:

Link	Description
<user>	Open the **Phone System** > **Users** > **Modify** page. See “User Settings” on page 229 for more information.
delete messages	Permanently deletes messages from the Allworx system. Recovering deleted messages requires an OfficeSafe backup or the automatic backup for Connect Vx instances. click to select the types of messages to delete for the user: • *Delete all emails* • *Delete all read emails* • *Keep all emails* • *Delete all voicemails* • *Delete all saved voicemails* • *Keep all voicemails* Click **Delete** to remove the messages. ***Note:*** *To recover deleted messages, perform a system restore using an OfficeSafe Backup for premise servers or a system restoration performed using the automatic backup of a Connect Vx instance. See “To restore premise server data using the Allworx OfficeSafe application:” on page 367 for more information.*

The following information is presented in the *Users* table.

Column	Description
Ext.	Handset extension.
User	The user assigned to the extension. Click on this link to jump to the **Phone System** > **Users** > **Modify** page for that user.
Total # msgs & folders	Total number of messages and folders (email + voicemail + IMAP = 6 folders by default).
space used (MB)	Space used for all folders and their contents in megabytes.

Continued

Column	Description
Inbox > Email > total	The total number of emails in the user's inbox (old + new).
Inbox > Email > new	The number of email messages labeled as new.
Inbox > Vmail > total	The total number of voicemails in the user's inbox (old + new).
Inbox > Vmail > new	The number of voicemail messages labeled as new.
Inbox > Vmail > size (mm:ss)	The size of the voicemail inbox (all messages) in minutes and seconds.
Inbox > Vmail > max size (mm:ss)	The maximum size of the voicemail inbox with all messages in minutes and seconds.
Action	Click **delete messages** to remove messages in the email and voicemail inboxes. A pop-up window opens where you click radio buttons to select from the following options: • *Delete all emails* • *Delete all ready emails* • *Keep all emails* • *Delete all voicemails* • *Delete all saved voicemails* • *Keep all voicemails* Click **Delete** to perform the selected actions.

Click here to return to the Installing and Configuring Allworx Premise Servers or Configuring Connect Vx Instances .

Section 7 Maintenance

The Maintenance features support customizing the performing routine maintenance on the Allworx premise server and Connect Vx instance. Each chapter explains:

- Necessary access permissions and feature keys
- Necessary equipment to perform the procedures
- Necessary procedures to setup and customize the Allworx server network

Feature and procedure differences for the Allworx Connect Vx service are noted in each chapter.

The various *Maintenance* pages on the Allworx System Administration web page allow the Allworx administrator to perform the following maintenance activities:

Chapter 48 Backup

***Note:** The procedure included in this chapter does not apply to Connect Vx. Allworx performs daily backups for all Connect Vx instances and stores those backups in the cloud. Restoration of a system is initiated by contacting Allworx Support to perform the restore.*

Prerequisites	
Access Permissions	Allworx Server Administrator Allworx System Administrator Phone Administrator Role Network Administrator Role Support Technician Role
Feature Key Required	No

Backup supports restoring entire Allworx premise server disk data, not just a specific file, to a PC. It is critical to configure the Allworx premise server to initiate backups frequently, including daily backups, before System Software updates, and before configuration changes.

Assess the data loss requirements in the event a restore from a premise server backup is necessary. In the event of a failure, restore the system from the backup. See "Performing a Premise Server Restore Using Allworx OfficeSafe" on page 367, as well as the *OfficeSafe Operations Guide* (www.allworxportal.com) for more information.

To perform an Allworx premise server backup:

The backup process is initiated from the Allworx System Administration web page and it is monitored using the OfficeSafe application installed on a PC connected to the premise server. The status of a backup is shown with a progress bar on the OfficeSafe Application's *Activity* screen in the *Current Operations* pane The *Activity Log* pane displays the message **Completed Successfully** when the backup has finished.

1. Start the OfficeSafe application on the backup PC. For more information application refer to the OfficeSafe Operations Guide available on the Allworx Portal (www.allworxportal.com).

2. Log in to the Allworx System Administration web page and navigate to **Maintenance** > **Backup**. Click one of the following actions:

Actions	Description	
Modify	Change the backup settings.	
	Start Time	Specify the time of day to begin the backup in hours and minutes using 24-hour format. For example, 5:30pm would be entered as 17 hours and 30 minutes.
	IP Address / Domain Name	Establish the communication between the Allworx server and the PC running the OfficeSafe application. Enter the IP Address of the OfficeSafe PC. In OfficeSafe, the value is available at **Tools** > **Options** > **Network**.
	TCP/IP Port	Enter the TCP/IP Port of the OfficeSafe PC. In OfficeSafe, the value is available at **Tools** > **Options** > **Network**.

Continued

<table>
<tr><td><b>Modify</b>
<i>(continued)</i></td><td><i>Frequency</i></td><td>Select an available option from the drop-down list.
<b><i>Note:</i></b> <i>Selecting the</i> <b><i>Monthly</i></b> <i>frequency from the drop-down list provides Allworx Server Administrators with another drop-down to select the date to perform the monthly Backup.</i></td></tr>
<tr><td></td><td><i>Mode</i></td><td>Select an option from the drop-down list.
• <b>Full</b> - includes all servers in every backup.
• <b>Incremental</b> - Includes only the changes to the server data since the most recent Full backup to merge with previous backup data. This backup mode is helpful to speed the duration of each backup by reducing the amount of transmitted data that to the backup PC during every backup.</td></tr>
<tr><td></td><td colspan="2">Click <b>Update</b> to save the changes. Backups begin at the Start Time on each day based on the Frequency setting.</td></tr>
<tr><td><b>Backup Now</b></td><td colspan="2">Click to start the backup process immediately. See the <i>Allworx OfficeSafe Operations Guide</i> (www.allworxportal.com) for detailed set up information.</td></tr>
</table>

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

- *An existing backup is not found on the PC running OfficeSafe*
- *This is the first backup after the Allworx premise server software has been upgraded*
- *This is the first backup after the Allworx premise server software has been restored*
- *The OfficeSafe PC application has been configured to force a full backup*

3. In the OfficeSafe application go to **View** > **Current Activity** to monitor the progress of the backup.

   When complete, the latest backup is added to the tree view of the premise servers and their backup files displayed on the left side of the OfficeSafe main screen. This view is organized from the newest to the oldest set of backups. Click on either the server name or one of the individual backups to display information for that server in the *Details* pane of the main screen.

To transfer the settings from one premise server to another, see “Import/Export” on page 371 for more information.

To perform an Allworx premise server restore using the OfficeSafe application, see “Performing a Premise Server Restore Using Allworx OfficeSafe” on page 367 for more information.

Click here to return to the Installing and Configuring Allworx Premise Servers or Configuring Connect Vx Instances .

Chapter 49 Custom Recordings

Prerequisites	
Access Permissions	Allworx Server Administrator Allworx System Administrator Phone Administrator Role Support Technician Role
Feature Key Required	No

Custom Recordings supports easy export/import of greetings and messages without the use of FTP. Allworx administrators can select specific recording categories on the Allworx premise server or Connect Vx instance to export to a .ZIP file automatically for use on other premise servers, Connect Vx instances, or to archive.

The Allworx supports these recording types:

- Auto Attendant - one custom message and up to 9 greetings per Auto Attendant.
- Call Queue - one custom message and one greeting.
- Message Center - one name recording and up to 9 greeting/announcements for each user.

Allworx System Software also supports the Music On Hold recording type - up to 30 recordings with a maximum storage size limit of 250MB on Connect premise servers or Connect Vx instances.

49.1 Exporting and Importing Audio Files

Allworx administrators can select single or multiple recording files at once to import onto the current Allworx premise server or Connect Vx instance by selecting files with a drag-and-drop or browse/select capability. After exporting the recordings, the Allworx administrator can import to the preferred language.

Notes:

- *Importing a Voicemail “announcement” for a Presence that currently permits leaving messages, automatically disables leaving messages for that Presence.*
- *Importing a “greeting” for a Presence that currently does not permit callers to leave a message, automatically enables leaving messages for that Presence.*

To export the Custom Recordings:

1. Log in to the Allworx System Administration web page and navigate to **Maintenance** > **Custom Recordings**.
2. Locate the *Custom Recordings - File Export* pane and click the additional information arrow ▶, if necessary. Update the following settings:

Setting	Description
File Naming Conventions	A short cut to the File Naming Conventions described lower on the page.

Continued

Setting	Description
Select Recordings	Check the box to select which recordings to export. • Auto Attendants • Call Queues • User Names and Greetings • Music on Hold
Select type	Select an available option from the drop-down list • Primary Language custom recordings • Secondary Language custom recordings

3. Click **Export** to export the selected recordings to a ZIP file.

4. Click one of the following actions:

Action	Description
Download	Downloads the ZIP file to the PC.
Delete	Removes any previous ZIP files. The settings to export redisplay on the page.

To import the custom recordings:

Note: *If the system is using the Dual Language Support feature, click **Load** for the language in which the messages and greetings are recorded. See "Managing the Language Settings" on page 160 for more information.*

Audio files must be Telephony, raw, mu-law (u-law), mono, 8-bits per sample, 8KHz sample rate. The following procedure uses the sound editing application *Audacity* (available at https://www.audacityteam.org/download/). Converting files using other applications is similar.

Note: *The procedures in this document were developed using Audacity 2.3.3.*

1. Verify the file to import is a **.snd** file. If the file is not a **.snd** follow these steps to convert the file format.
   a. Open an audio file (example: MP3 file) in Audacity. Click **Tracks** > **Mix** > **Stereo Track to Mono** and then change the Project Rate (Hz) value to **8000**.
      - If starting with a mono audio file, go to **Tracks** > **Resample**.
      - Enter **8000** as the *New sample rate (Hz)* value in the *Resample* pop-up window.

   b. Click **File** > **Export** > **Export Audio**.

   c. In the *Export Audio* pop-up window:
      - Select the *Save in* folder.

- Enter the *File name* with the **.snd** extension. See "Audio File Naming Conventions" on page 342.
- Click to select **Other uncompressed files** from the *Save as type* drop-down list.
  - Select **RAW (header-less)** from the *Header* drop-down list

  •Select **U-Law** from the *Encoding* drop-down list

d. Click **Save**. The *Edit Metadata Tags* dialog box opens. Leave all fields blank.

e. Click **OK**.

The custom recording audio files are now in a format that can be imported into the Allworx System Software.

2. Log in to the Allworx System Administration web page, and navigate to **Maintenance** > **Custom Recordings**.

3. Locate the *Custom Recordings - File Import* pane, and click the additional information arrow ▶, if necessary. To see the file name requirements for the recordings, click **File Naming Conventions**.

4. Drag and drop an audio file into the field provided or click **Choose File**, navigate to the file location, and click **OK**.

5. Click one of the following options:

Option	Description
Upload	Identifies the file to install into the Allworx system.
Cancel	Disregards the request to upload the file.

6. Locate the **Select type to install:** and select one of the options from the drop-down list:

Option	Description
Primary Language custom recordings	Imports the file as the Primary Language.
Secondary Language custom recordings	Imports the file as the Secondary Language.

7. Click one of the following options:

Option	Description
Install	Imports the selected file.
Delete	Removes all previously uploaded but uninstalled recordings.

49.1.1 Audio File Naming Conventions

The following table provides examples of the naming conventions for the audio files used by different Allworx System Software (8.5 and higher) features.

Note: *Information specific to each system software can be found on the Allworx System Administration web page at* ***Maintenance*** *>* ***Custom Recordings*** *in the File Naming Conventions panes.*

Feature	Description
Auto Attendant	Format: **aa#x.snd** **#** - Replace with the Auto Attendant number **1** through **32**. **x** - Replace with the greeting number **0** through **8** or **c** for a custom message (use **0** for the open greeting and **1** for closed greeting). Example: **aa20.snd** = auto attendant 2 - open greeting.
Call Queue	Format: **cq#x.snd** **#** - Replace with a Call Queue number **0** through **9**. **x** - Replace with **g** for greeting or **s** for status message. Example: **cq3s.snd** = call queue 3 - status message.
Message Center Name	Format: **vm_u_n.snd** **u** - Replace with the username. Example: **vm_Test_n.snd** = The Test message center.
Message Center Greeting or Announcement	Format: vm_u_#x.snd u - Replace with the username. x - Replace with g for greeting or a for announcement. # - Replace with the type of greeting or announcement (0 through 8): 0 - Default 1 - In office 2- At a meeting 3-On vacation 4- On Business Trip 5- At home 6- Away 7- Busy 8- Reach link lost connection Example: vm_Test_1g.snd = In office greeting for the Test user.

Continued

Feature	Description
Music On Hold	Format: **moh_n_m.snd** **n** - Replace with a number between **1** and **30**. This is a unique number among the Music On Hold audio files on the system. ***Note:*** *If importing a Music On Hold audio file that duplicates the number (**n**) of a file that is already on the system, the system replaces the existing file.* **m** - Replace with a user-defined string that uniquely identifies the file. Valid characters include (**A**-**Z**), (**a**-**z**), (**0**-**9**) and (**_**)underscore. Example: **moh_1_sales.snd** = music on hold with the number 1 and text indicating the audio file is for the sales department.

49.1.2 Adjusting the Audio File Volume

All pre-recorded Allworx prompts have an average volume set to -22.00 dB. It is recommended that custom recordings added to the system match this volume as closely as possible. Audio file volume can be adjusted using Audacity.

1. Open the audio file in Audacity.
2. Click and drag to highlight / select the file.
3. Go to **Analyze** > **Contrast.**
4. Click **Measure Selection** in the foreground line. The volume appears in the text box.
5. Adjust the volume to **-22.00** dB.
   a. With the audio file still highlighted, go to **Effect** > **Amplify**.
   b. The *Amplify* pop-up window opens.
   c. In the *Amplification* text box enter the value to be added to the current volume to bring that volume to the recommended -22.00 dB.

      Note: *Remember that you are working with negative numbers when making the calculation. For example, if the volume of the audio file is **-20.15** dB, the entry in the Amplification text box would be **-1.85** dB to add to the **-20.15** dB equal to **-22.00** dB.*
   d. Click to select the *Allow clipping* check box.

      This selection can cause distortions in audio files with amplification that pushes to the upper and lower ranges. In these cases, listen to the audio and make the necessary adjustments.
   e. Click **OK**.

6. Recheck the volume.
    - Highlight the updated audio file.
    - Go to **Analyze** > **Contrast**.
    - Click **Measure Selection** in the *Foreground* line to display the new volume.
7. Repeat any steps as needed.

Click here to return to the Installing and Configuring Allworx Premise Servers or Configuring Connect Vx Instances .

Chapter 50 Feature Keys

The *Feature Key* page provides a listing of purchasable advanced features that are installed on the Allworx server. New Connect Vx instances do not include built-in feature keys. New Connect premise servers include a base number of users.

***Note:** Feature keys activate features only on the Allworx premise server or Connect Vx instance for which they are generated. As a result, one system cannot use feature keys generated for another system.*

Prerequisites	
Access Permissions	Allworx Server Administrator Allworx System Administrator Phone Administrator Role Network Administrator Role Support Technician Role
Feature Key Required	No

The table displayed on the **Maintenance** > **Feature Keys** page identifies the feature keys available for the connected server type from Allworx; if the feature key is available (installed and enabled); applicable expiration dates; and, if necessary, the total number of licenses available and the number of licenses used. The column row highlights light green if the feature key is active or light yellow if the feature key is expired. To sort the table on the *Feature Keys* page, click any of the table headings.

***Note:** Unless otherwise noted, the following feature keys apply to both Connect premise servers and Connect Vx instances.*

Feature Key	Description
Allworx View CDR* (Connect premise servers only)	Provides dynamic, comprehensive usage reporting on the Allworx phone system. This application uses complete and accurate data of the Allworx phone system for users to make data-driven decisions with an easy-to-use web browser-based user interface. Required for each Allworx server in a multi-site network.
Allworx View ACDR* (Connect premise servers only)	An add-on feature to the Allworx View CDR feature providing customizable dashboards for supervisors and agents, and displays the information - using any popular web browser. Using configurable alarms, supervisors and agents can recognize and react to high call volume situations to minimize abandoned calls and frustrated customers. Requires the ACD and View CDR keys. Required for each Allworx server in a multi-site network.
Automatic Call Distribution (Connect premise servers only)	Directs calls in a queue to agents using a variety of call distribution algorithms without requiring any additional software. This key also enables the method described for the Call Queuing key. • If installing the Automatic Call Distribution feature key, the Call Queuing feature key is not required. • The Automatic Call Distribution feature is not available for Allworx Connect 300 series servers. • For details on Call Queuing and Automatic Call Distribution, "Call Queues/ACD" on page 51.

Continued

Feature Key	Description
Allworx View Users (Connect Vx instances only)	Allworx View provides dynamic, comprehensive usage reporting on the Allworx phone system. This application uses complete and accurate data from the Allworx phone system to help users make data-driven decisions with an easy-to-use web browser-based user interface. Allworx View also furnishes customizable dashboards for supervisors and agents, and displays the information using any popular web browser. Using configurable alarms, supervisors and agents can recognize and react to high call volume situations to minimize abandoned calls and frustrated customers. This single feature key allows user access to all View features. Feature keys are available in 5-license packs and one license must be provided for each user.
ACD Users (Connect Vx instances only)	Automatic Call Distribution directs calls in a queue to agents using a variety of call distribution algorithms without requiring any additional software. This key also enables the method described for the Call Queuing key. • If installing the Automatic Call Distribution feature key, the Call Queuing feature key is not required. • The Automatic Call Distribution feature is not available for Allworx Connect 300 series servers. • For details on Call Queuing and Automatic Call Distribution, "Call Queues/ACD" on page 51. Feature keys are available in 5-license packs and one license must be provided for each user (agent). Each agent can be assigned to multiple queues using only one license.
Call Queuing	Provides the ability to direct inbound calls into Ring All queues. Rings all phones logged into the queue. • Feature is automatically available when installing the Automatic Call Distribution feature key. This option does not require any additional software.
Conference Center (Connect premise server only)	Enables Conference Center feature, and offers password-restricted access for attendees. This option does not require any additional software. ***Note:*** *Conference Center is not available with the Allworx Connect Vx service and this feature key does not appear in the table.*
Dual Language Support	Provides the capability of a second language for all audio and phone screen prompts. The French and Spanish Language Packs are available for download on the Allworx Portal at www.allworxportal.com.

Continued

<table>
<tr><th>Feature Key</th><th>Description</th></tr>
<tr><td>Generic SIP Handsets</td><td>Create new Generic SIP handsets on the system without requiring any additional software.
<ul>
<li>Generic SIP handsets existing in the system prior to the 7.5 upgrade operate without the purchase of a feature key package.</li>
<li>Installing multiple keys for the same or different feature count adds licenses to the server.</li>
<li>Server feature key limits:</li>
</ul>
<table>
<tr><th></th><th colspan="6">Connect servers</th></tr>
<tr><th>License Limit</th><th>320</th><th>324</th><th>530</th><th>536</th><th>731</th><th>Vx</th></tr>
<tr><td>Built-in Licenses</td><td>4</td><td>4</td><td>6</td><td>6</td><td>12</td><td>0</td></tr>
<tr><td>Purchase Limit</td><td>16</td><td>16</td><td>54</td><td>54</td><td>168</td><td>250</td></tr>
<tr><td>Total Server Limit</td><td>20</td><td>20</td><td>60</td><td>60</td><td>180</td><td>250</td></tr>
</table>
</td></tr>
<tr><td>Hardware Warranty
(Connect premise server only)</td><td>Indicates any unexpired warranty key is installed, whether the warranty is the one-year manufacturer’s warranty, an extended warranty, or a ninety-day newly-repaired server warranty.
<b><i>Note:</i></b> <i>The Hardware Warranty is not required with the Allworx Connect Vx service and this feature key does not appear in the table.</i></td></tr>
<tr><td>Interact Professional</td><td>Enables users to control a handset with convenient access to call history and contacts from the Allworx directory and accesses personal directory contacts from the user’s Microsoft® Outlook® application.
<ul>
<li>Integrates with CRM applications to perform lookups based on incoming Caller ID.</li>
<li>Order feature key licenses in increments of 1, 5, and 10; the feature counts are additive. Installing multiple keys for any feature count adds licenses to the server. Each user requires an Interact license.</li>
<li>Server feature key limits:</li>
</ul>
<table>
<tr><th></th><th colspan="6">Connect Servers</th></tr>
<tr><th>License Limit</th><th>320</th><th>324</th><th>530</th><th>536</th><th>731</th><th>Vx</th></tr>
<tr><td>Built-in Licenses</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>0</td></tr>
<tr><td>Purchase Limit</td><td>20</td><td>20</td><td>60</td><td>60</td><td>180</td><td>250</td></tr>
<tr><td>Total Server Limit</td><td>21</td><td>21</td><td>61</td><td>61</td><td>181</td><td>250</td></tr>
</table>
</td></tr>
</table>

Continued

<table>
<tr><th>Feature Key</th><th>Description</th></tr>
<tr><td>Interact Softphone</td><td>Allows users to access the Allworx handset features from their PC and places calls from that PC independent of any desk phone.
• One Interact Softphone license is included with Allworx System Software version 9.0.
• Integrates with Microsoft Outlook contacts
• Programmable functions allow defining and assigning a function to a Softphone handset to provide functionality for the user.
• The feature counts are additive. Installing multiple keys for any feature count adds licenses to the server. Each user requires an Interact Softphone license.
• Server feature key limits:
<table>
<tr><th></th><th colspan="6">Connect Servers</th></tr>
<tr><th>License Limit</th><th>320</th><th>324</th><th>530</th><th>536</th><th>731</th><th>Vx</th></tr>
<tr><td>Built-in Licenses</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>0</td></tr>
<tr><td>Purchase Limit</td><td>40</td><td>40</td><td>100</td><td>100</td><td>360</td><td>360</td></tr>
<tr><td>Total Server Limit</td><td>40</td><td>40</td><td>100</td><td>100</td><td>360</td><td>360</td></tr>
</table>
</td></tr>
<tr><td>Mobile VM
(formerly known as Mobile Link)</td><td>Activates the mobile Voicemail capability of Reach without configuring the Reach application on the mobile device as a handset.</td></tr>
<tr><td>Multi-Site Branch
(Connect premise server only)</td><td>• Enables sites to join a network of sites but not as the controller site.
• Feature is automatically available when installing the Multi-Site Primary feature key.
• Sites without a Multi-Site Primary key are limited to DSS/BLF for a maximum of 10 handsets from other sites.
• This option does not require additional software.
<b><i>Note:</i></b> <i>Although this feature key appears in the list for Connect Vx instances, the feature is enabled with the installation of the Multi-Site Primary feature key.</i></td></tr>
</table>

Continued

<table>
<tr><th>Feature Key</th><th>Description</th></tr>
<tr><td>Multi-Site Primary</td><td>Enables a server to be the Controller in a multi-site network.
• Controls requesting other sites to join a network of sites (up to 99 Allworx servers with up to 1975 users and up to 1975 system extensions across all sites).
<b><i>Note:</i></b> <i>The total number of Multi-Site Users and Multi-Site System Extensions are limited by the maximum users licensed on each Allworx server.</i>
• At least one site in the network must have a Multi-Site Primary key. More than one site can have a primary key.
• This option does not require any additional software.
<b><i>Note:</i></b> <i>For Connect Vx instances, this feature key also enables the Multi-Site Branch feature.</i></td></tr>
<tr><td>Multi-Site Upgrade
(Connect premise server only)</td><td>• Enables changing the Multi-Site Branch feature key to a Multi-Site Primary feature key.
• When upgrading the Multi-Site Branch feature key to a Multi-Site Primary feature key, the <i>Feature Keys</i> list displays Multi-Site Primary - not Multi-Site Upgrade.
• This option does not require additional software.</td></tr>
<tr><td>Reach</td><td>• Enables users to send or receive business phone calls from an iOS or Android device. The server provides a single instance of the Reach application without purchasing a feature key.
• Enables working from remote locations and continue to send, receive, hold, transfer, and park calls; see the handset’s call history and business/personal contacts; and listen, reply, forward, or create Voicemail.
• Enables managing Voicemail options without creating a Reach handset.
• Order Feature key licenses in increments of 1, 5, and 10; the feature counts are additive. Installing multiple keys for any feature count adds licenses to the server. Each Reach device requires a Reach license.
• Enables configuring users to claim licenses.
• Server feature key limits:
<table>
<tr><th></th><th colspan="6">Connect servers</th></tr>
<tr><th>License Limit</th><th>320</th><th>324</th><th>530</th><th>536</th><th>731</th><th>Vx</th></tr>
<tr><td>Built-in Licenses</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>0</td></tr>
<tr><td>Purchase Limit</td><td>20</td><td>20</td><td>60</td><td>60</td><td>180</td><td>250</td></tr>
<tr><td>Total Server Limit</td><td>21</td><td>21</td><td>61</td><td>61</td><td>181</td><td>250</td></tr>
</table>
</td></tr>
</table>

Continued

Feature Key	Description
Reach Link	Keeps Reach calls connected as the mobile device changes networks. See "Reach" on page 291 for more information. ***Note:*** *In a multi-site network configuration Reach Link functionality is limited to users and handsets configured on an Allworx server with the Reach Link feature key installed.* Also enables the Reach Extend feature, which provides the option of placing or receiving a call through a cell voice service instead of depending on VoIP call quality while on Wi-Fi and cellular data networks, while presenting a business Caller ID to remote parties.
Software Upgrade License (Connect premise servers only)	Enables System Software updates. Without this key, only patch updates to the currently loaded release are available. ***Note:*** *Software upgrades are included with the Allworx Connect Vx service.*
T1 License (Connect premise servers only)	Activates the T1-A port. T1 License #1 (Connect 731 servers only). No additional software required. ***Note:*** *Support for T1 lines is not available with the Allworx Connect Vx service and this feature key does not appear in the table.*

Continued

Feature Key	Description
User Expansion License (Connect premise servers only)	Expands the maximum number of users on Allworx-Connect premise servers. The expansion does not require downloading any additional software. A number of user licenses is included with the purchase of Allworx Connect premises servers. No user licenses are built in to the Connect Vx service. It is important to note that one System Extension is included for each user license that is either built-in or provided by the feature keys.

	Connect servers				
Server	**320**	**324**	**530**	**536**	**731**
20 Users	X	X			
50 Users					X
60 Users			X	X	
100 Users					X
150 Users					X
200 Users					X[1]
250 Users					X[1]

[1] Requires the internal extension length to be a minimum of four digits, if not using extension mode.

* Required for <u>each</u> Allworx server (both controller and branch servers) in a multi-site network for comprehensive call data reporting to Allworx View. It is not necessary to install the feature keys on Allworx servers that do not provide call reporting data. The installation of Allworx View keys enable reporting the call data only from a single Allworx server to Allworx View. Allworx View will only report the call data from Allworx servers with the Allworx View CDR and Allworx View ACDR feature keys installed.

To install feature keys - new installation:

1. Log in to the Allworx System Administration web page and navigate to **Maintenance** > **Feature Keys**.

2. Click one of the following options:

Option	Description
Install	Click to automatically retrieve new feature keys from the Allworx Portal.
Enter new Feature Key	1. In the text field enter the feature key code provided. 2. Click **Submit** to retrieve the new features.

To install feature keys - premise server replacement:

During a premise server replacement, end customers that are re-installing an Allworx System do not need the Allworx System Administrator to be present to install the feature keys.

At start up, the Allworx premise server automatically polls the Allworx Portal to download the feature keys associated with the server. If the Allworx premise server is unable to connect to the Allworx Portal initially, that server continues polling until it can download and install the feature keys using the following intervals:

- Every 15 minutes – up to a maximum of four times
- Once a week – if no connection is made during the 15-minute interval cycle
- Upon each reboot

Additionally, the premise server polls the Allworx Portal each week after every reboot to search for new feature keys associated with that server.

50.1 Managing Reach Handset Licenses

Users must install the Reach application on the iOS and/or Android devices to provide softphone capability. See the Allworx Reach User's Guide for information on installing the Reach application.

Each Reach handset requires a license for soft phone capability. The Allworx premise server and Connect Vx instance include one (1) Reach license. To add more Reach handsets, install additional Reach feature keys (available in 1, 5, or 10 license increments). To enable larger numbers of Reach handsets, install multiple feature keys of the same or different license counts. To allocate a Reach license, do one of the following:

- Reserve licenses for specific users by manually configuring the Reach handsets.
- Authorize users to claim licenses on a first come, first served basis using Plug and Play.

To reserve an Allworx Reach license for a specific user:

1. Log in to the Allworx System Administration web page. If necessary, install the Reach feature key. See “Feature Keys” on page 345.
2. Navigate to **Maintenance** > **Feature Keys**, and click **Allworx Reach**.
3. Click **add new**. If the link is unavailable, purchase more licenses. Update the following settings:

Allworx Reach Handset	
Owner	Select an available user from the drop-down list.
Extension	Specify the extension for the handset. If selecting an owner other than admin, the system automatically adds the handset to the In Office call route of the owner. If selecting an Extension, the system creates an extension with a call route to ring this handset. This is typically the case of using a conference room or lab phone that does not require an owner.
Internal Caller ID Name	Automatically populates from *Owner* selection.
Internal Caller ID Number	Automatically populates from *Owner* selection.
External Caller ID Name	Enter up to 47 characters (letters and digits).
External Caller ID Number	Enter up to 24 digits.
Emergency Caller ID Number	Select the appropriate value from the drop-down list.
Description	Automatically populate from Owner selection. Update as necessary.
Handset Configuration Template	Select the appropriate template from the drop-down list.
Dialing Privileges Group	Select the appropriate group from the drop-down list.
Default Prompt Language	Select Primary Language or Secondary Language from the drop-down list.
Handset Features	
Hold Music Selection	Select an option from the drop-down list. See “Music On Hold” on page 171 for more information.
Can Place Calls	Click to select the check box to allow the handset to place calls.
Can Receive Calls	Click to select the check box to allow the handset to receive calls.

4. Click **Add** to save the changes.

5. Click one of the links in the table below to email the setup information to the user.

Link	Description
setup link for all users	Opens a new page with information to connect the device running Reach to the premise server or Connect Vx instance. This link does not contain user-specific information such as username or password.
setup link for <user>	Opens a new browser page containing user-specific information (including login information) to connect the device running Reach to the premise server or Connect Vx instance.

To authorize users to claim licenses:

It is possible to over-allocate the number of installed licenses when authorizing users to claim licenses. See “User Template Settings” on page 233 to adjust the number of Reach activations a user may claim.

- If users have claimed all licenses, the premise server or Connect Vx instance blocks attempts to install Reach handsets.
- If the Allworx administrator creates a Reach handset and assigns an owner before using all the licenses, the owner keeps the installed license and can register the Reach handset.

To manage Reach licenses:

1. Log in to the Allworx System Administration web page. (If necessary) Install the Reach feature key. See “Feature Keys” on page 345 for more information.

2. Navigate to **Maintenance** > **Feature Keys**, and click **Allworx Reach**. The *Allworx Reach* page displays.

3. Click one of the following options:

Option	Description
add new	Click this link to manually add a new Reach Handset. This reserves a license for the owner (user) who can then begin using their reserved Reach handset as soon as they configure the app on their Smartphone. ***Note:*** *This option can also be accessed by navigating to Phone System > Handsets and clicking add new Allworx Reach Handset.*
setup link for all users	Opens a new page with information to connect the device running Reach to the server. This link does not contain user-specific information such as username or password.
setup link	Opens a new page with information specific to the user to connect the device running Reach to the premise server or Connect Vx instance.

Continued

Option	Description
View	Display handset information about a specific user.
Manage	Enable or disable the Allworx Reach license, the Reach Link for handset using the check box.
Delete	Remove the Reach handset from the system and the associated Call Appearances. Click Delete to confirm.

4. Create an email to the Reach user and attach the setup link and the android or iOS Allworx Reach User's Guide. It is available on the Allworx Portal at www.allworxportal.com, and on the Allworx Reach Installation web page (get.allworx.com/reach). Send the email to the user.

50.2 Managing the Interact Professional and Interact Softphone Licenses

Allworx Interact provides Windows PC users with an intuitive, configurable user interface for controlling an Allworx desk phone handset or an Interact Softphone handset (running inside the user's Windows PC). There are three Interact applications modes.

The basic Interact application is a free application mode available to any Allworx user that connects to an Allworx desk phone and allows users to answer a call, put a call on hold, or end a call from their PC desktop.

The Interact Professional is a per-user licensed application mode that also connects to an Allworx phone (handset) and has those same capabilities, but adds a full-featured user interface that includes the ability to transfer, park, or conference a call. Additionally, the Interact Professional user interface provides access to call history, queue status, as well as Allworx System, User, and Personal Contacts.

An Interact Softphone license allows Interact Professional to run the phone (handset) entirely within the Windows PC. Calls are managed with the Interact Professional user interface and the PC microphone and speakers or a PC headset (preferred) for audio hardware instead of a Verge phone. Where a traditional Verge handset associates functions with physical buttons (PFKs), Softphone enables those features from the premise server or Connect Vx instance, and provides feature indications within the user interface. An Interact Softphone license allows the user to switch between controlling a softphone and controlling an Allworx desk phone, if needed.

The Allworx administrator manages which users have access to the licensed features of the Interact Professional and Interact Softphone application modes. Users that see the Interact free screen pop-up feature and would like to upgrade to Interact Professional or Interact Softphone should contact the Allworx administrator to reserve a license or have them make that user eligible to obtain a license from the server. If the Allworx administrator installs the Interact Professional or Interact Softphone feature key on the premise server or Connect Vx instance, all users can use the free features of the Interact application. Users who upgrade from the basic Interact mode to the Interact Professional or Interact Softphone mode see the licensing changes take effect the next time they log out and then log in to the application.

The Allworx Server System Software includes one (1) Interact Professional license. To add more Interact Professional licenses, and to add Interact Softphone licenses, requires purchasing and installing additional feature keys. The Interact Professional feature keys are available in increments of 1, 5, or 10 licenses. Interact Softphone licenses are available as single licenses. To enable larger numbers of these licenses, install multiple feature keys of the same or different license counts.

50.2.1 Interact Professional

To reserve an Interact Professional license:

1. Log in to the Allworx System Administration web page.
2. (If necessary) Install the Interact Professional feature key. See “Feature Keys” on page 345 for more information.
3. Navigate to **Maintenance** > **Feature Keys**, and click **Allworx Interact Professional**. The *Interact Professional* page displays.
4. Click **create** to assign an owner a license select a user from the drop-down list. Enter a description, if necessary.
5. Click the **Add** button to reserve a license.

To manage Interact Professional licenses:

1. Log in to the Allworx System Administration web page and navigate to **Maintenance** > **Feature Keys**, and click **Allworx Interact Professional**. The *Interact Professional* page displays.
2. Click one of the following actions:

Action	Description
setup link for all users	Opens a new page with information to connect Interact to the premise server or Connect Vx instance. This link does not contain user-specific information such as username or password.
Modify	Enables changing the license assignment. Update the settings and click **Modify** to save the changes.
Delete	Removes the Interact communication from the server. Click **Delete** to confirm.
Disable / Enable	Prevents or permits any further communication with the Allworx Server. The link toggles between **Disable** and **Enable**.

To enable users to claim a license:

1. Install the Interact Professional feature key. See “Feature Keys” on page 345. for more information.

2. See To modify or delete existing users: and refer to “Feature Eligibility” on page 236 for more information.

50.2.2 Interact Softphone

To reserve an Interact Softphone license:

1. Log in to the Allworx System Administration web page.
2. (If necessary) Install the Interact Softphone feature key. See "Feature Keys" on page 345 for more information.
3. Navigate to **Maintenance** > **Feature Keys**, and click **Allworx Interact Softphone**. The *Interact Softphone* page displays.
4. Click **add new**.
   - To assign an *Owner* for license select a user from the drop-down list.
   - Enter a *Description*, if necessary.
   - The user can begin using their Interact Softphone as soon as they configure the application on their PC. For more information, see the *Allworx Interact Softphone User Guide* available on the Allworx Portal (allworxportal.com).

   Note: *This option can also be accessed by navigating to **Phone System** > **Handset** and clicking **add new Allworx Interact Softphone** in the SIP Handsets pane.*
5. Click **Add** to reserve a license.

To manage Interact Softphone licenses:

1. Log in to the Allworx System Administration web page and navigate to **Maintenance** > **Feature Keys**, and click **Allworx Interact Softphone**. The *Interact Softphone* page appears.
2. Click one of the following actions:

Action	Description
setup link for all users	Opens a new page with information about how to connect Interact Softphone to the server. This link does not contain user-specific information such as username or password. Copy the link and send it to the user at an email account they can access from the Windows PC where Interact Softphone is installed.
Modify	• Allows the administrator to change the license assignment or update the *Description*. • Update the settings and click **Modify** to save the changes.
Delete	• Releases the Interact Softphone license and removes the setting for that Interact Softphone from the premise server or Connect Vx instance. • Click **Delete** to confirm.

Continued

Action	Description
Disable / Enable	Allows the administrator to disable or enable the Interact Softphone license for the user, but the setup remains and the license is still assigned. This link is useful if a user looses the laptop with Interact Softphone installed. If the laptop is found, the license can be enables without further configuration changes needed.

To enable users to claim a license:

1. Install the Interact Softphone feature key. See “Feature Keys” on page 345. for more information.
2. See “To modify or delete existing users:” on page 228 and refer to “Feature Eligibility” on page 236 for more information.

Note: *Interact Professional and Interact Softphone licenses are independent of each other. Users need only an Interact Softphone license to get the Softphone functionality.*

50.3 Managing Generic SIP Handset Licenses

To manage the Generic SIP Handset licenses:

1. Log in to the Allworx System Administration web page.
2. (If necessary) Install the Generic SIP Handset feature key. See “Feature Keys” on page 345 for more information.
3. Navigate to **Maintenance** > **Feature Keys** > **Generic SIP Handset**.

Action	Description
Create	Display the *Add Generic SIP Handset* page. See “For larger numbers of Generic SIP handsets, install multiple feature keys.” on page 152 for more information.
Delete	Remove the user from the handset. Click **Delete** to save the change.

Click here to return to the Installing and Configuring Allworx Premise Servers or Configuring Connect Vx Instances.

Chapter 51 Registration

Prerequisites	
Alternate Access Permissions	Allworx Server Administrator Allworx System Administrator Phone Administrator Role Network Administrator Role Support Technician Role
Feature Key Required	No

Both Allworx premise servers and Connect Vx instances must be registered and then activated to begin operation.

Completing these tasks provides the following information:

- Generates the Site ID
- Generates the Connect premise server or Connect Vx instance *Activation Code*
- Provides the ability to keeps a deployment history for each Connect premise server and Connect Vx instance -

  For more information about viewing deployment history, refer to the *Allworx Equipment Management Dashboard Guide* available via the link on the *Equipment Management* page.

51.1 Registration

Registration is accomplished from within the Allworx Portal. Activation happens on the premise server or Connect Vx instance, but does not necessarily require interaction with the Allworx System Administration web page.

After registration, the Connect premise server (if connected to the Internet) or Connect Vx instance activate automatically within 15 minutes of registration.

Note: *Any time prior to registration, Allworx System Software can be fully configured and tested, but all phone calls are disconnected after a few seconds.*

To register a Connect premise server:

Note: *This procedure requires Allworx Portal permissions.*

New, unregistered Connect Vx instances automatically open to the registration page at login when connected to the Internet.

1. Log in to the Allworx System Administration web page and navigate to **Maintenance > Registration**.

   Note: *New unregistered premise servers that have an Internet connect will automatically open to the appropriate Allworx Portal page.*

2. Click **Register**. A new web page for the Allworx Portal opens.
3. Log in to the Allworx Portal with the Allworx-assigned username and password.
4. Click **Equipment Management** on the left panel of the Allworx Portal page.

5. On the *Server* tab, click **Add/Register Server**. The *Server Registration* page opens.
6. Enter the *Server Serial Number* in the text box. Refer to *Tips for getting the serial number right* displayed on the page.
7. Click **Continue**. The registration form displays.
8. Fill in the registration form fields.

Field	Description
System Name	Displays in the Server Management dashboard on the portal. Use this description as a nickname for the account, location, or machine.
Street Address 2	Provides additional address details for better delivery.
Additional info	Area for adding notes to view later in the Server Management dashboard on the portal.

9. Click **Register**. An automatically generated email confirmation that includes the *Activation Code* goes to the email address of record for the portal user account. For Connect premise servers that have an Internet connection, activation will automatically occur within 15 minutes. To activate the premise server manually, see “To manually activate a Connect premise server:” on page 361.

   Note: *If the If you are completing registration from a remote location, be sure to gather hard copies of the Activation Code and Feature Key strings to take to the location of the premise server. If an Internet connection is not available, these hard copies can be used to enter the information manually and complete the activation and configuration.*

To register a Connect Vx instance:

Note: *This procedure requires Allworx Portal permissions.*

New, unregistered Connect Vx instances automatically open to the registration page at login. Remember that Connect Vx instances are always connected to the Internet.

1. Log in to the Allworx Portal with the Allworx assigned username and password.
2. Click **Equipment Management** located in the left panel of the portal.
3. The Connect Vx instance will already appear in the *Servers* tab. Click the radio button to select that Connect Vx.
4. Click **Modify/Complete Registration**.
5. Enter the *Server Serial Number* provided by Allworx in the text box. The serial number is already there - no need to enter.
6. Click **Continue**. The registration form displays.

7. Fill in the registration form fields.

Field	Description
System Name	Displays in the Server Management dashboard on the portal. Use this description as a nickname for the account, location, or machine.
Street Address 2	Provides additional address details for better delivery.
Additional info	Area for adding notes to view later in the Server Management dashboard on the portal.

8. Click **Register**. An automatically generated email confirmation that includes the *Activation Code* goes to the email address of record for the portal user account.
9. Connect Vx instances automatically activates within 15 minutes of registration. After this automatic activation monthly billing begins.

51.2 Manual Activation of a Connect Premise Server

Activate the Connect premise server from within the Allworx System Administration web page using the registration-generated *Activation Code*. After the automatic or manual activation of a Connect premise server the warranty clock starts.

To manually activate a Connect premise server:

Note: *For more information refer to the Allworx Connect Server Family Installation Guide for premise servers that is available on the Allworx Portal at www.allworxportal.com.*

1. Log in to the Allworx System Administration web page with the Allworx assigned username and password. Navigate to **Maintenance** > **Registration**.
2. Click one of the following actions:

Action	Description
Activate (With an Internet connection)	Automatically retrieves the *Activation Code* from the portal via the Internet. Automatic activation happens within 15 minutes of the registration if connected to the Internet -- use manual if you don't want to wait the 15 minutes.
Enter Activation Code (No Internet connection)	Manually activate the Connect premise server if no Internet connection is available, or if the 15 minute wait for automated activation is too long. 1. In the field provided enter the *Activation Code* from "To manually activate a Connect premise server:" on page 361. 2. Click **Submit**.

3. The page displays *Server is Activated* and is ready to use.

Note: *Click* ***Refresh*** *to see updated server information.*

Click here to return to the Installing and Configuring Allworx Premise Servers or Configuring Connect Vx Instances.

Chapter 52 Restart / Shutdown

The *Restart/Shutdown* page for premise servers and *Restart* page for Connect Vx instances allows for the reboot or restart of the Allworx server and phones so that settings can take effect.

Prerequisites	
Access Permissions	Allworx Server Administrator Allworx System Administrator Phone Administrator Role Network Administrator Role Support Technician Role
Feature Key Required	No

52.1 Restarting (Rebooting) the Connect Vx Instance and/or Allworx Phones

Caution:	*Restarting the Allworx system ends all active calls.*

To manage the Allworx Connect Vx instance:

1. Log in to the Allworx System Administration web page and navigate to **Maintenance** > **Restart**.
2. Click to select the check box for one of the following actions:

Action	Description	
Restart		
Restart the Allworx Server	Check the box to view these restart options. Click to select the radio button next to the desired option.	
	Normal restart	Reboots the server with the current settings.
	Restart with factory defaults restored	Reboots the server and returns the server settings to the original factory default settings. This option maintains all user data (i.e. Users and Voicemail) To see which Allworx Settings return to the factory defaults, see “Restore Factory Defaults” on page 395.
	Note: *This choice restarts the Connect Vx instance even though the wording is “Allworx Server.”*	

Continued

Action	Description
Restart Allworx Phones	• Click to select the check box to initiate a reboot of the Allworx phones connected to Connect Vx instance. When a phone restart is initiated the Connect Vx instance sends a message to each of the Allworx phones connected to it instructing them to reboot. The messages are sent in a staggered manner to prevent network congestion. It may take several minutes to an hour or more for all the phones to reboot. • Click to select the **Automatically accept phone software update** check box to have the phones automatically confirm/install updates without administrator intervention. If the Allworx Connect Vx instance is also restarted, phone restarts will begin after the Connect Vx instance restarts.
Logged in Administrators	
This area of the screen displays the users currently logged in with administrative permissions.	

3. Click **Restart Now** to begin the restart process immediately.
4. Click **Restart Later** to schedule a time to restart the server.
   - Enter a start date and time in the fields provided.
   - Click **Schedule** to save the change and activate the schedule.

Note: *If the Allworx administrator restarts the Connect Vx instance before the scheduled date and time, the Allworx system cancels the pending restart.*

To manage the Allworx premise server restart from normal mode:

1. Log in to the Allworx System Administration web page and navigate to **Maintenance** > **Restart**.
2. Click to select the check box for one of the following actions:

<table>
<tr><th>Action</th><th colspan="2">Description</th></tr>
<tr><td rowspan="6"><i>Restart the Allworx Server</i></td><td colspan="2">Check the box to view these Allworx server restart options:. Click to select the radio button next to the desired o</td></tr>
<tr><td><i>Normal restart</i></td><td>Reboots the server with the current settings.</td></tr>
<tr><td><i>Restart with factory defaults restored</i></td><td>Reboots the server and returns the server settings to the original factory default settings. This option maintains all user data (i.e. Users and Voicemail) To see which Allworx Settings return to the factory defaults, see “Restore Factory Defaults” on page 395.</td></tr>
<tr><td><i>Enter Migration Mode after restart</i></td><td>Reboots the server for use with the Allworx Migrate tool.
<b><i>Note:</i></b> <i>This option is not available for the Connect Vx service.</i></td></tr>
<tr><td><i>Enter Safe Mode after restart</i></td><td>Reboots the server while only enabling essential system programs and services to start up for adjusting the server operating system. To perform a Restore with the Allworx OfficeSafe application, see “To restore premise server data using the Allworx OfficeSafe application:” on page 367.</td></tr>
<tr><td><i>Shutdown and Power Off</i></td><td>Shutdown and power off the Allworx server from the Allworx System Administration web page.
• <b>Shutdown Later -</b> Schedule a future time to shutdown and power off the Allworx server (the Allworx administrator can cancel the scheduled shutdown). If the Allworx administrator restarts the server before a scheduled shutdown, the Allworx system cancels the pending shutdown.</td></tr>
<tr><td><i>Restart Allworx Phones</i></td><td colspan="2">• Click to select the check box to initiate a reboot of the Allworx phones connected to Connect Vx instance.
When a phone restart is initiated the premise server sends a message to each of the Allworx phones connected to it instructing them to reboot. The messages are sent in a staggered manner to prevent network congestion. It may take several minutes to an hour or more for all the phones to reboot.
• Click to select the <b>Automatically accept phone software update</b> check box to have the phones automatically confirm/install updates without administrator intervention.
If the Allworx premise server is also restarted, phone restarts will begin after the premise server restarts.</td></tr>
</table>

Logged in Administrators

This area of the screen displays the users currently logged in with administrative permissions.

3. Click **Restart Now** to begin the restart process immediately.
4. Click **Restart Later** to schedule a time to restart the server.

- Enter a start date and time in the fields provided.
- Click **Schedule** to save the change and activate the schedule.

***Note:** If the Allworx administrator restarts the premise server before the scheduled date and time, the Allworx system cancels the pending restart.*

To manage the Allworx premise server reboot from safe mode:

***Note:** This option is not available when using the Connect Vx service.*

1. Locate the *Disk Operations* pane on the safe mode screen and click **Mount**.
2. Locate the *Reboot Operations* pane on the safe mode screen and click one of the radio buttons for the following actions:

Action	Description
Reboot in Normal Mode	Restarts the Allworx server and the server is ready for use.
Reboot in Normal Mode with Factory Defaults restored	Restarts the server and returns the settings to the original factory default settings. This option maintains all user data (i.e. Users and Voicemail). To see which Allworx settings return to the factory defaults, refer to “Restore Factory Defaults” on page 395.
Reboot in Normal Mode with Factory Defaults restored AND all user settings and files erased.	Restarts the Allworx server as a clean server with installation software. No previous configuration or user information is available.
Reboot in Safe Mode	Restarts the server while only enabling essential system programs and services to start up for adjusting the server operating system. To perform a Restore with the Allworx OfficeSafe application, refer to “To restore premise server data using the Allworx OfficeSafe application:” on page 367.

3. Click **Reboot**.

To power down the Allworx premise server using the power button:

***Note:** This option is not available when using Connect Vx.*

1. Power off the Allworx premise server:
   a. Press the power button on the server for less than four seconds. The server begins the shutdown process and the power light blinks green to confirm the power-down cycle.
   b. Allow sufficient time for the server to complete the power-down cycle. This process varies in length of time from a few seconds to a few minutes.

   If the Allworx premise server has not properly shut down, force a shutdown by holding the power button for more than four seconds. Finally, if the server does not shut down, as a last resort pull the AC power cord from the wall outlet.

Caution:	*Forcing an Allworx premise server shutdown may cause database corruption conditions causing further service disruption.*

2. Restart the Allworx premise server in one of the following modes:
    - **Safe Mode:** Press and hold the power button for at least 1 second, and then release it before 4 seconds has elapsed. The button flashes amber during the safe mode boot sequence.
    - **Normal Mode**: Press the power button for less than 1 second. The button flashes green during the normal mode boot process. The server restarts and begins to register the Allworx phones. This length of time for this process can vary from a few seconds to a few minutes depending on the size of the system and number of phones.

52.2 Performing a Premise Server Restore Using Allworx OfficeSafe

Note: *This option is not available when using the Connect Vx service. Contact Allworx Support to restore a Connect Vx instance.*

See the *Allworx OfficeSafe Operations Guide* for detailed restore information.

Alternatively, use the Allworx Migrate tool to transfer the settings from one Allworx premise server to another Allworx server. See the *Allworx Migrate Administrator's Guide* for more details.

Both documents are available on the Allworx Portal at allworxportal.com.

To restore premise server data using the Allworx OfficeSafe application:

1. **View customers**: Perform a backup of the View database before performing the restore (see the *Allworx View Users Guide* for more information).
2. Disconnect the Allworx premise server LAN and WAN ports (or the T1 port, if using for the WAN) from the network.
3. Log in to the Allworx System Administration web page and navigate to **Maintenance** > **Restart / Shutdown**.
4. Restart the Allworx premise server into Safe Mode using one of the following methods:

Method	Description
Allworx System Administration web page	1. Check the box for **Restart or Shutdown the Allworx Server.** 2. Click to select the **Enter Safe Mode after restart** radio button. 3. Click **Restart Now**. 4. A warning banner displays. Click **Continue** to confirm the restart. The Allworx server powers down and then powers back up in safe mode. When the system is in safe mode access the safe mode web page.
Front Panel of the Allworx Server	The method used to force entry into safe mode via the Allworx premise server front panel varies by product model. Consult the specific product model Allworx premise server Installation guide for more details.

5. Start the OfficeSafe application on the OfficeSafe PC.

6. Connect the OfficeSafe PC to the ETH0 port of the Allworx Connect premise server.
7. In the OfficeSafe Backup Admin Tool navigate to **Tools** > **Options**.
8. Click the *Network* tab.
9. Verify that the IP address 192.168.2.x is present in the *Active Network Interfaces* list. This tab also provides the IP address and port number of the OfficeSafe PC that is entered on the Allworx System Administration web page Safe Mode screen
10. Click the *Restore* tab.
11. Click to select the radio button of the option that the describes the backup file to use for this restore.
12. Click **OK** to return to the Backup Admin Tool main window.
13. On the Allworx System Administration web page Safe Mode screen OfficeSafe area enter the *IP address of OfficeSafe PC* and the *Port #*.
14. Click **Restore from OfficeSafe**.
15. Click **Accept** on the Confirm Restore Request dialog box to begin the restore.

    Depending on the size of the backup data (and the performance of the network and OfficeSafe PC), it may take several minutes or over an hour to restore the backup. A Restore was successful message displays in the Status pane on the Safe Mode page when the operation completes.
16. Click **Reboot in Normal Mode** and select **Reboot**.

Caution:	*Do NOT select **Reboot the Allworx server in Normal Mode with Factory Defaults** restored. This loses the restored settings during the reboot. If this happens, start the entire restore operation over again.*

After the Allworx premise server restarts complete the following:

- Reconnect the network cables
- Log in to the Allworx premise server
- Verify that the data restored successfully

Click here to return to the Installing and Configuring Allworx Premise Servers or Configuring Connect Vx Instances .

Chapter 53 Time

Prerequisites	
Access Permissions	Allworx Server Administrator Allworx System Administrator Phone Administrator Role Network Administrator Role Support Technician Role
Feature Key Required	No

The Time page provides a means for adjusting the time and date on the Allworx server either automatically or manually.

Notes:

- *No time settings are available for the Allworx Connect Vx service. If the default time and DST are not as required, contact Allworx Support.*
- *The Connect Vx service does not provide an NTP server. Administrators should configure phones and other devices that require an NTP server to use a service available on the Internet. Allworx recommends either **pool.ntp.org** or **time.inscitek.net**.*

For Connect premise servers Allworx strongly recommends using an NTP (Network Time Protocol) server, when the Allworx server has Internet access, to keep the time on all servers in sync — especially Allworx servers in a multi-site network. Differences in server time settings between servers in a multi-site network can lead to errors in phone system features (example: park call duration). For Connect Vx instances the NTP settings are not available.

Note: *When a Verge phone has an invalid NTP configuration, and therefore fails to get time from an SNTP server, the phone now has three indicators:*

- The status bar turns red
- The date is not displayed
- The time-of-day blinks **12:00 AM**

To set the time for Connect premise servers:

1. Log in to the Allworx System Administration web page and navigate to **Maintenance** > **Time**.
2. Click **Modify** in the *Action* column. The *Time* page displays.
3. Update the following settings:

Setting	Description
Note: *Allworx recommends using NTP to set the time automatically for all Allworx premise servers, if the premise server has Internet access. Click to select the check box to enable.*	
NTP Server	Specify an SNTP-server IP address or a domain name.
Poll Period	Specify the number of minutes between polls.

Continued

Setting	Description
Set Time Manually	Specify the time in hours, minutes, seconds, and then the date.
Time Zone	Select the correct time zone from the drop-down list. Check the Automatically adjust clock for Daylight Saving Time box to enable the system to update the time automatically.
Set Time	Saves the current changes.
Get Time	Updates the clock to the current time when using an SNTP server.
Cancel	Disregards the changes.

Click here to return to the Installing and Configuring Allworx Premise Servers .

Chapter 54 Import/Export

Import/Export eases the task of upgrading a site from one Allworx server model to another.

Note: *Import/Export is **not** a substitute for using Allworx OfficeSafe to backup the premise server.*

IMPORTANT:

Prerequisites	
Access Permissions	Allworx Server Administrator Allworx System Administrator Phone Administrator Role Network Administrator Role Support Technician Role
Feature Key Required	No

- *When importing the server settings, the port numbers assigned to native CO lines and analog handsets settings are available.*
- *When importing an Allworx Px 6/2 Port Expander, the Import includes all configured CO lines and analog handsets from the export. Do not modify the port assignments. If the Allworx server does not support CO lines, the Analog CO lines display in the Import file as a conflict.*
- *DID blocks, routes plans, and T1 lines do not display on the Import Configuration screen. The system imports these settings, if included on the export.*

  Note: *T1 lines are not supported by the Connect Vx service.*
- *The export does not include: T1 Line fields, PPP Username, PPP Password, and PPP MTU.*
- *The export does not include contact user-specific metadata such as: Favorite status or Park to Extension notification status.*
- *If the current system is not "clean" and has conflicts with the imported configuration settings, then the new system resolves conflicts for the import settings:*
- *The system appends digits to user login names and incremented, starting at 01, as needed (e.g. jAdams will become jAdams01).*
- *Extensions change to the lowest available extension.*
- *The Allworx premise server and Connect Vx instance do not import phones with conflicting MAC addresses and removes all references (e.g. call routing and BLF PFK assignments).*
- *The Allworx premise server does not import analog phones with unavailable ports and removes all references (e.g. call routing and BLF PFK assignments).*
- *The Allworx premise server and Connect Vx instance do not save SIP handsets and SIP gateway station numbers during an import. If changing station numbers for generic SIP phones or SIP gateways, set up the new station number on each device.*
- *On multi-site configurations, the Export does 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 premise server or Connect Vx instance. The order in the export file determines the available extensions/users. If exceeding the imported extensions/user limit, the premise server or Connect Vx instance disables and does not import the remaining extensions/users.*
- *Do not modify the XML export file.*

To manage the Import / Export:

An export includes all configurable parameters for:

Phone System Settings	Outside Lines	Network Settings
• Users	• CO Lines (Premise servers only)	• Configurations
• User Templates	• T1 Lines (Premise servers only)	• T1 Line Configurations
• System Extensions	• SIP Gateways	• SSL Certificates
• Handsets (all phones and outside lines)	• SIP Proxies	• Digital Lines
• Handset Preference Groups	• DID Blocks & Routing	
• Schedules[1]		
• Shared Call Appearance		
• Routing Plan		
• Speed Dial		
• Email Alias		
• Allworx Port Expander (including all attached analog phones and CO lines)		
VoIP Server Settings	**SIP Proxy Settings**	**Dial Plan Settings[2]**
• All	• All	• Internal Dial Plan
		• External Dial Plan
		• Flexible Dialing Rule
		• External Dial Restrictions
		• Internal Dial Restriction

Continued

VoIP Server Settings	SIP Proxy Settings	Dial Plan Settings[2]
		• Automatic route selection for external dial plan • Dialing Privileges Groups • Non-default Service Groups

[1] Schedules - does not export or import Schedule 0.

[2] Export does not include the Default Toll Restrictions or the Internal Call Restrictions.

To manage importing or exporting the configuration settings:

Log in to the Allworx System Administration web page and navigate to **Maintenance** > **Import / Export** and click one of the following actions:

<table>
<tr><th>Action</th><th>Description</th></tr>
<tr><td><b>Export Configuration</b></td><td>1. Check the box for the available configurations to export listed in the table. To select all the available options, click the check box next to <i>Configuration Type</i>.
2. Click <b>Export.</b> For Connect premise servers and Connect Vx instances: Selecting the SSL Keys and Certificates requires entering a Key Encryption password in the field provided.
After exporting the configuration, the following options are available:
<table>
<tr><td><b>View</b></td><td>Displays the XML file in a separate browser window.
To save the XML file:
1. Right-click and select <b>Save Link As...</b>.
2. Browse to the correct file location and enter a description in the <b>File name</b>: field.
3. Click <b>Save</b> to keep the file.
4. Verify the server receiving the imported configuration settings has none of the above configurations added prior to import. Update the internal dial plan and extension length to match the configuration being imported before the import.</td></tr>
<tr><td><b>Delete</b></td><td>Removes the configuration file.</td></tr>
</table>
</td></tr>
<tr><td><b>Import Configuration</b></td><td>1. Click <b>Choose File</b> to select the configuration file to import. Use the browser to navigate to the file location and highlight the file.
2. Click <b>Open</b> to select the file.
3. Click <b>Load</b> to start the import of the file. It may take a few minutes to load the configuration file.</td></tr>
</table>

Click here to return to the Installing and Configuring Allworx Premise Servers or Configuring Connect Vx Instances .

Chapter 55 Tools

Tools is a set of various features to supports troubleshooting server communication problems.

Prerequisites	
Access Permissions	Allworx Server Administrator Allworx System Administrator Phone Administrator Role Network Administrator Role Support Technician Role
Feature Key Required	No

55.1 Network Diagnostics

1. Log in to the Allworx System Administration web page and navigate to **Maintenance** > **Tools**.
2. Locate the *Network Diagnostics* pane, and click the additional information arrow ►, if necessary**.**
3. Update the following settings:

Setting	Description
Enter an IP Address or Domain Name	Type in site *IP Address* or *Domain Name*.
Select a Function:	Click one of the following options: • **Ping** (Connect premise server only) • **DNS Get Address From Name** • **DNS Get Name From Address** • **MX Record Lookup** • **Trace Route** (Connect premise server only) • **Bandwidth Test** • **Discover DHCP Servers** (Connect premise server only) • **What is my External IP?** The results display in the space at the bottom of the pane.

55.2 Syslog - System Events

1. Log in to the Allworx System Administration web page and navigate to **Maintenance** > **Tools**.
2. Locate the *Syslog - System Events* pane and click the additional information arrow ►, if necessary.

3. Click one of the following options:

Option	Description
Start	Enter an IP Address and Port in the field provided to transmit the system events to a specified Syslog server.
setup	Send automatic notification of selected system events. See "Auto Notification" on page 317 for more information.

55.3 Allworx Technical Support Server

Connect to the Allworx support server to allow Allworx Technical Support access to the Allworx System Administration web page.

1. Log in to the Allworx System Administration web page and navigate to **Maintenance** > **Tools**.
2. Locate the *Allworx Technical Support Server* pane, and click the additional information arrow ►, if necessary.
3. Enter the *Support Server IP Address* information in the field provided.
4. Click **Connect** to begin.

55.4 Advanced Troubleshooting

1. Log in to the Allworx System Administration web page and navigate to **Maintenance** > **Tools**.
2. Locate the *Advanced Troubleshooting* pane, and click the additional information arrow ►, if necessary.
3. Locate the appropriate information and click the additional information arrow ►, if necessary:

Setting	Description
Advanced Diagnostic Logging (Allworx premise servers and Connect Vx instances) Only enable at the direction of Allworx Customer Support to assist support engineers in troubleshooting a problem. Allworx premise server or Connect Vx instance performance degrades when enabled.	
Call Control *Backplane* *Messages*	Check the box to enable.
SIP Messages	Check the box to enable.

Continued

Setting	Description
T1 / PRI Messages (Connect premise servers only)	Check the box to enable.
T1 / RBS Messages (Connect premise servers only)	Check the box to enable.
Advanced	Update the fields with the required information: • *Module Name* • *Level Mask*
Capture	Enter a value in minutes (1 to 60) for the diagnostic messages.
Stop	Ends the advanced diagnostic logging.
View	Display the advanced diagnostic log in a separate browser window.
Delete	Removes the advanced diagnostic log.
Echo Cancellation Diagnostics (Connect premise servers only) The Echo Cancellation Diagnostics test requires an active call on the selected line. The test takes about one minute to complete. To end the test early, hang up the active call.	
Capture	1. From the drop-down list select the line to test. 2. Click **Capture** to run the test. Existing test results are overwritten. 3. When complete, click **Download** to view the results.
Delete	Removes the test results.
Four Wire Return Less Measurements (Connect premise servers only) A noise measurement defined for the LAN and associated components. This tool is not available for the Connect Vx service.	
Capture	Capture four wire return loss values, verify the analog CO lines are not active. Incoming or outgoing calls while the test is running causes the test to capture incorrect data. Click to start the test.
Refresh	Resets the current page to check the Packet Capture Tool status when writing packets to the file.
View	Display the information log in a separate browser window.
Delete	Removes the log from the server.

Continued

Setting	Description
Network Address Translation (NAT) information (Connect premise servers only) A method of modifying network address information in Internet Protocol (IP) datagram packet headers while it is in transit across a traffic routing device. This tool is not available for the Connect Vx service.	
Capture	Starts gathering the NAT information for the log.
View	Display the NAT information log in a separate browser window.
Delete	Removes the NAT log from the server.
Network Device Monitoring (Connect premise servers only) Watching a computer network for slow or failing components. Only enable at the direction of Allworx Customer Support to assist support engineers in troubleshooting a problem. Allworx server performance degrades when enabled. This tool is not available for the Connect Vx service.	
Check All	Selects all displayed devices for network device monitoring.
Uncheck All	De-selects all displayed devices for network device monitoring.
<device>	Check the box selects specific devices for network device monitoring.
Capture	Enter a value in hours (0 to 99) for the network diagnostic monitoring. The value 0 hours indicates the network device monitoring is running continuously.
Open	View the network device monitoring log.
Stop	Ends the network device monitoring.
Delete	Removes the Network Device Monitoring log from the server.
Packet Capture Tool (Connect premise servers only) Intercepts and logs traffic passing over a digital network. Only enable this tool at the direction of Allworx Customer Support to assist support engineers in troubleshooting a problem. Allworx premise server performance degrades when enabled.	
Network Interfaces	Check the box to enable. • ETH0 Port Interfaces • ETH0/untagged | Local Phones • ETH1 Port Interfaces • ETH1/untagged | Local Phones • ETH2 Port Interfaces • *IP Addresses* • *Source IP Address* - Enter the address in the field provided. • *Destination IP Address* - Enter the address in the field provided *Continued*

Setting	Description
Capture	Enter a value in minutes (0 to 60) for the network diagnostic monitoring. The value 0 minutes indicates the packet capture tool is running continuously.
Stop	Ends the packet capture tool.
Open	View the packet captures.
Refresh	Resets the current page to check the Packet Capture Tool status when writing packets to the file.
Delete	Removes the packet capture file from the server.
Performance Monitoring *(Allworx premise servers and Connect Vx instances)* The Allworx premise server and Connect Vx instance collects system performance data in the background, which may assist Allworx Support engineers in troubleshooting a problem. Save the file to disk before making it available to download, in RRD format, which requires specialized tools to view.	
Write	Click to collect and save the system performance file to disk.
Open	Click to view the RRD system performance file.
Delete	Click to remove the RRD system performance file from the premise server or Connect Vx instance.
RPC Diagnostics *(Allworx premise servers and Connect Vx instances)* RPC Diagnostics mode allows Allworx Support to view the content of messages between the premise server and phones. ***Note:*** *This diagnostic should only be enabled to assist support engineers with troubleshooting a problem.*	
Start	1. Enter the number of minutes (**1**-60) to allow the viewing of the messages. 2. Click **Start**.
Stop	Click to end the viewing of messages.
SSH (Connect premise servers only) Using one computer to securely log onto another computer that is part of the same network. This tool is not available for the Connect Vx service. ***Note****: The Allworx System Software 8.0 and higher application does support a full pseudo-tty terminal. To avoid warnings in the SSH client, disable the pseudo-tty on the SSH client. When enabled, users see a warning message, but SSH is still operable. Only Allworx Connect servers support SSH.* Only enable at the direction of Allworx Customer Support to assist support engineers in troubleshooting a problem. Allworx server performance degrades when enabled.	
Enable SSH	Click to Enable the SSH. Enter a port that is not in use by another service on this server.
Disable SSH	Click to Disable the SSH. Click Refresh to redisplay the page with SSH disabled.

55.5 Replace Phone Software

Replace phone software ONLY at the direction of Allworx Customer Support. The Phone Model selected **must match** the chosen file.

Replacing software for an incorrect phone model may result in phones that no longer function!

To replace phone software:

The table at the top of the window provides a listing of the current phones and the installed software.

1. Select the phone software to replace from the drop-down list.
2. Click **Choose file** to select the file containing the phone software. A browser window opens. Navigate to the software file and click **Open**
3. Click **Replace** to change the current phone software file.

55.6 Custom Phone Logo

This tool provides a method for uploading a custom logo that can be displayed on the Allworx Verge phones when in Sleep Mode. The Verge phones must be rebooted to load the new logo.

Logo graphic files can be in the following formats:

- GIF
- PNG
- JPEG/Exif
- JPEG/JFIF
- SVG

The file can be no larger than 96 kilobytes and bitmap images can have a resolution no higher than 272 pixels wide by 80 pixels high. Bitmap images smaller than 272 x 80 are not scaled up.

To upload a logo image file:

1. Log in to the Allworx System Administration web page and navigate to **Maintenance** > **Tools**.
2. Locate the *Custom Phone Logo* pane, and click the additional information arrow ▶, if necessary.
3. Click **Add**,
4. Click **Choose file** to browse to the file location, and click **Open** in the *File Upload* window.
5. Click **Add** to upload the image file, or click **Cancel** to ignore the request.
6. Reboot the Verge phones to have the logo appear on the screens.

Click here to return to the Installing and Configuring Allworx Premise Servers or Configuring Connect Vx Instances .

Chapter 56 Update

Prerequisites	
Access Permissions	Allworx Server Administrator Allworx System Administrator Phone Administrator Role Network Administrator Role Support Technician Role
Feature Key Required	Yes

The *Update* page supports upgrading the Allworx System software version on Connect premise servers. The page displays the current software version number, build date, and indicates if there is a current software upgrade license feature key available on the Allworx server.

Note: *This tool is not available for the Connect Vx service. Connect Vx instances include automatic updates initiated by Allworx. After a Connect Vx instance software update, both 92xx and Verge 93xx series phones automatically reboot to upgrade to the new software and firmware versions. The 92xx series phones display a prompt that will timeout and allow the phone to complete the update.*

Before initiating an upgrade, be aware that:

- Downgrading from one release to an earlier release results in undesirable behavior and is not supported.
- Allworx highly recommends running an OfficeSafe backup prior to the upgrade (see “Backup” on page 337.).
- View customers: Allworx highly recommends performing a backup of the View database prior to the upgrade (see the *Allworx View User Guide* for more information).
- The upgrade requires a server restart. Because this causes disconnections and disruption of data, verify that the system is idle (no phone or data users) when performing the upgrade.
- After installation, close all browser windows and open a new browser window before proceeding. If there is a browser session open during the upgrade, the Allworx System Administration web page may not display properly.
- For the reliable operation of Allworx multi-site installations, upgrade all servers in the network to the same software release.
- See “Allworx Server Features and Compatibility” on page 14 for supported web browsers.

Notes:

- *Upgrading from prior major releases of the Allworx System Software to the current release requires the installation of a Software Upgrade Feature Key, or that the premise server be in the initial software warranty period.*
- *Do not skip software releases to install Allworx System Software. For example, if upgrading from release 8.4 to 9.0, install 8.5, 8.6, and finally release 9.0.*

To update the premise server:

1. Log in to the Allworx System Administration web page and navigate to **Maintenance** > **Update**.
2. Click one of the following update actions:

Action	Description
Download update from web	The premise server determines if new software releases are available. If an upgrade is available, the option to install them is available. Select the software version, and then click **Download Update**.
Upload update from PC	1. Navigate to the Allworx Portal and download the update file (allworxportal.com). 2. Unzip the downloaded file. 3. Click **Choose file** > **Browse** to navigate to the location of the Allworx System Software file. 4. Select the file, and click **Open**. The *Update* page displays. 5. Click **Load**. A warning message displays for any inconsistencies such as: • Update version is the same or lower than the current version • Update is for a different Allworx premise server model

3. Select one of the options listed in the following table to activate the System Software update.

Option	Description
Activate Update Now	The update begins immediately. 1. Click **Activate Update Now**. 2. (optional) Check the **Automatic Update** box to update Allworx phone firmware automatically. 3. Click **Start Update**.
Activate Update Later	Schedule the update to begin at another time — up to one week later. 1. Click **Activate Update Later**. 2. (optional) Check the **Automatic Update** box to update Allworx phone firmware automatically. 3. Select the date and time to begin the update, 4. Click **Submit Schedule**. The *Update* page displays with the scheduled date and time for the System Software update.
Cancel	Ends the update and returns to the main *Update* screen.

Notes:

- *The first server restart after an upgrade can be slower due to the upgrade processing.*
- *After the installation is complete close all browser windows and open a new browser window before proceeding. If there is a browser session open during the upgrade, the Allworx System Administration web page may not display properly.*

After the update, and if the **Automatic Update** option is selected, both 92xx and Verge 93xx series phones automatically reboot to upgrade to the new software and firmware versions. The 92xx series phones display a prompt that will timeout and allow the phone to complete the update.

Without **Automatic Update** selected, Verge 93xx series phones do not update unless the phone reboots either through user action or because the phone tried to re-register when the premise server was updating (the re-registration fails and causes the phone to reboot and the update is automatically installed). The 92xx series phones display the prompt that now does not timeout and requires user action.

Notes:

- *The premise server staggers the automatic phone reboots so that the phones stagger their requests for update files in order to keep from getting too many simultaneous requests.*
- *92xx series phones can only be upgraded to newer versions of firmware and software. Verge 93xx series phones can be either upgraded or downgraded to a previous version.*

To interrupt the phone boot cycle:

Use one of the following methods if it is necessary to interrupt the phone boot cycle.

1. 92xx series IP phones, do one of the following to display the *Initialization load aborted* message on the phone screen.
   - 9202e phone: Press the **Mute/DND** button three times.
   - All other 92xx phones press the **Release** function button three times, and then press one of the following soft keys:
     a. **Config** - Requires entering the admin password (**allworx**). Navigate to the *Network Settings* options. Update and save the options as necessary.
     b. **Reboot** - Restarts the phone.
     c. **FCNTST** - Starts the function test operation.
2. Verge Phones
   a. Start the Boot cycle, and then press and hold the programmable button located on the right side, third from bottom during the initialization sequence until the button lights amber (approximately 10 seconds). The *Settings* screen displays.

b. Press the **Admin** soft key and enter the Phone Admin Password (**allworx**).
c. Press the **Select** button and select the **Network Settings** option.
d. Update the Network Settings as required, and then press the **Back** soft key twice.
e. Press the **Reboot** soft key to start the phone with the new settings.

If an Allworx IP phone displays a *Config / Init Erro*r, reboot it again. If that is not successful, restore factory defaults from within the handset *Configuration* menu.

Click here to return to the Installing and Configuring Allworx Premise Servers or Configuring Connect Vx Instances .

Appendix A Acronyms

Abbreviation	Definition
ACD	Automatic Call Distribution
BLF	Busy Lamp Field
CDR	Call Detail Record
CO	Central Office
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 Subscriber
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol
ITSP	Internet Telephony Service Provider
LAN	Local Area Network
NAT	Network Address Translation
NTP	Network Time Protocol
PBX	Private Branch Exchange
PFK	Programmable Function Key
PoE	Power Over Ethernet
POP	Post Office Protocol
PPTP	Point-to-Point Tunneling Protocol

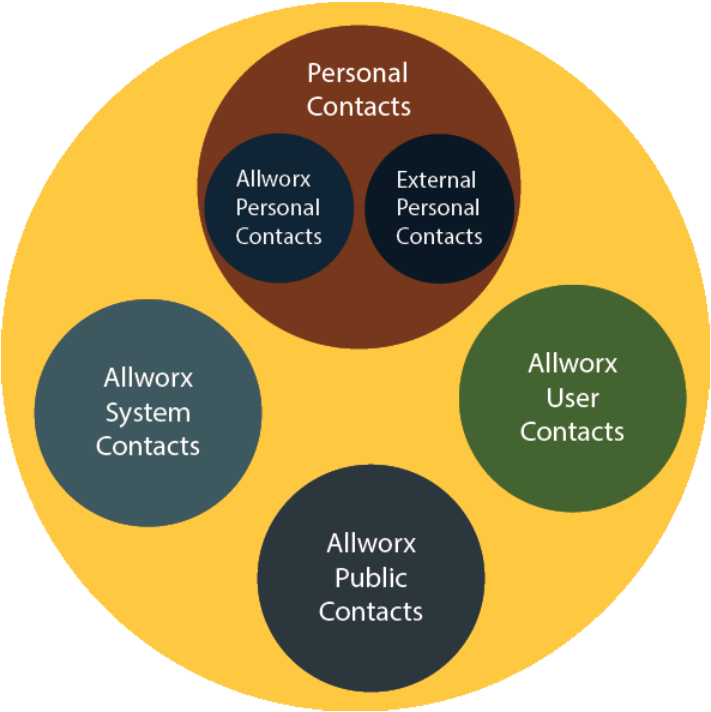
Abbreviation	Definition
RTP	Real-time Transport Protocol
SIP	Session Initiation Protocol
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
URI	Uniform Resource Identifier
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol
WAN	Wide Area Network

Appendix B Contacts

The Allworx System supports four types of contacts on the Verge phone series:

- User and System contacts – these are contacts with an internal Allworx extension assigned. The Allworx Server Administrator manages these contacts.
- Public Contacts – these are system-wide contacts (formerly known as Speed Dial). The Allworx Server Administrator manages these contacts.
- Personal Contacts – (only available on Allworx systems with a Connect premise server or Connect Vx instance) these contacts are managed by the Allworx user.
  - **Allworx Personal Contacts**
    - Created from the Verge phone, the Interact application, or a Reach device contact application.
    - Imported from a **.CSV** file or vCard within the Interact application.
  - **External Personal Contacts**
    - Synchronized from a Reach device originating application (device app such as Contacts or People).
    - Synchronized from an account such as a Gmail email account or an Outlook email account.

Visual example of Contacts:



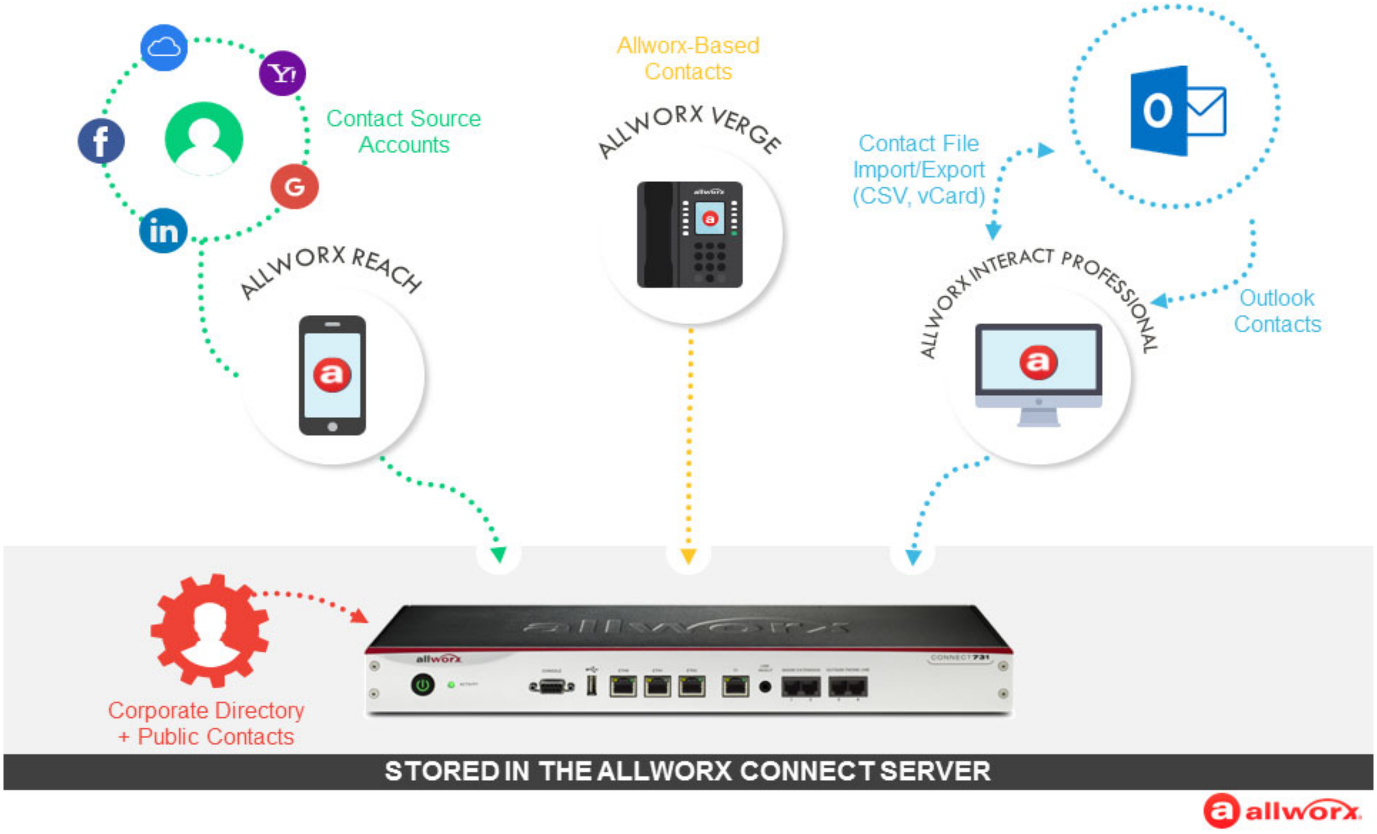
Sharing Contacts

The Allworx system shares the User, System, and Public Contact types with all of the Allworx user's connected Allworx phones, Reach devices, and the Interact application. Within the Reach and Interact Professional applications, Allworx users control sharing and synchronizing the Personal Contacts to the devices assigned to the Allworx user. See the Reach for iOS, Reach for Android, or the Interact and Interact Professional User Guide for more information about sharing Personal Contacts.

Notes:

- *The Allworx Connect* premise server or Connect Vx instance *is not a contact manager for Personal Contacts. Example: If a Personal Contact is available in the Reach device app (i.e. Contacts) and the same Personal Contact is available in the user's email account (i.e. Gmail), the Personal Contact displays twice when viewing the contacts.*
- *The Verge 9304 IP Phone fully supports Allworx User, System, and Public contacts while having limited Personal Contact support. Allworx Users can add up to 100 Allworx Personal Contacts on the phone, which are only available on that phone - not with other Allworx phones and applications (including the Hot Desk feature).*
- *The Verge 9304 does not support External Personal Contacts (contacts synchronized from the external accounts using Reach or Interact applications).*

Visual example of sharing contacts using a Connect premise server:



Contact Privacy

Allworx Server Administrators can manage the privacy in Handset Preference Group settings - **Personal Contacts Display.** See “Handset Preference Group Settings” on page 122 for more information.

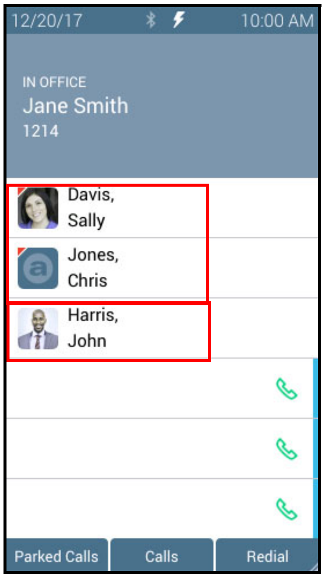
Verge Phone Series

If set to Unrestricted, Allworx users can adjust the setting on the Allworx Verge phone. On the **Settings** > **Phone Preferences** > **Display** > **Personal Contacts**, Allworx users can set their privacy to:

- **Unrestricted** - Contact matches are displayed in Voicemail, call history, and ringing calls and require phone log in to view or modify details. Login is valid until the user exits the screen.
- **Restricted** - Contact matches are displayed in Voicemail, call history, and ringing calls and after authentication via soft key to see personal contacts including Contact programmable buttons. Log in is valid until user logs out via soft button on Contacts screen or automatically logged out when the phone is rebooted or enters Sleep mode. Contact lock status always displays on the Verge phone series status bar.

Examples:

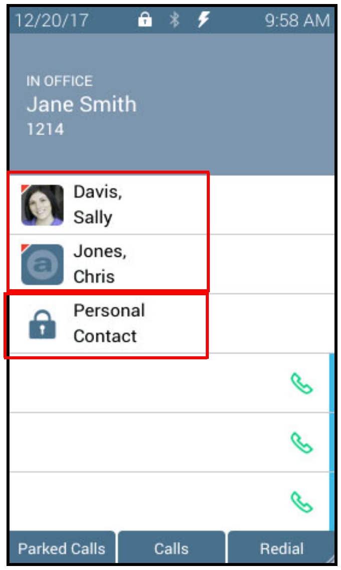
Unrestricted



Allworx User Contacts

Personal Contact

Restricted



Allworx User Contacts

Personal Contact

Reach for iOS and Reach for Android

On the **Info tab** > **Settings** > **Contacts and Accounts:**

- Choose which contact source accounts (e.g. Google Contacts, iCloud) to share with your Allworx devices and applications.
- Disconnect a contact source account from your Allworx devices and applications at any time.
- Choose to share the contact source account with the Reach app on your mobile device only or with all Allworx devices and applications.

Interact Application

On the **Options** > **Settings** > **Contacts** page:

- Choose which contact source accounts (e.g. Outlook) to share with your Allworx devices and applications.
- Disconnect a contact source account from other Reach devices.

Data Protection

Only the Allworx user has access to their personal contacts; the Allworx Server Administrator cannot access the user's personal contacts. Allworx users can prevent others from seeing the personal contacts on their Verge phone by restricting access by requiring an Allworx PIN to unlock the Verge phone.

Managing Personal Contacts

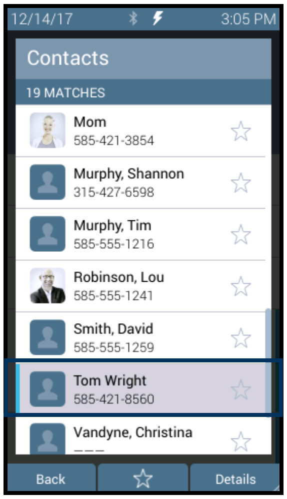
Allworx users can manage and update Personal Contacts by using the originating device or application. The *Contact Details* screen identifies the originating application in the *Account* line. Only the Allworx user can add, edit, or delete each Allworx Personal Contact. Allworx Server Administrators can delete all of a user's personal contacts from the Connect premise server or Connect Vx instance permanently, see "Deleting User Messages, Recordings, Contacts, or Contact Images" on page 230 for more information. Allworx Server Administrators cannot limit the individual user's number of Personal Contacts stored on a Connect premise server or Connect Vx instance.

Notes:

- *Each Allworx user can add a contact image associated with their contact information using the Reach application (with or without a handset license) or the Interact Professional application.*
- *The Allworx Server Administrator can control the permissions for users to manage their directory contact image. See "Users" on page 225 for more information.*
- *The Allworx Server Administrator can delete an Allworx User's directory contact image. See "Deleting User Messages, Recordings, Contacts, or Contact Images" on page 230 for more information.*
- *The Reach application enables users to update an External Personal Contact IF the email account (e.g., Gmail) used to create the contact is available on the Reach mobile device.Follow the on screen instructions to update these contacts; the on screen instructions are similar to the instructions described in the user guide.*
- *The Reach application does not enable users to update External Personal Contacts synchronized from the Interact Professional application using Outlook email.*
- *Allworx Users are limited to adding up to 100 Allworx Personal Contacts on the Verge 9304 IP phone, which are only available on that phone - not with other Allworx phones and applications.*

Example:

Jane Smith needs to update her Personal Contact, Tom Wright. Since Jane uses the Verge phone, Reach for iOS, and the Interact application, she needs to determine how she added Tom to her Personal Contacts. Jane opens the Contact Details for Tom Wright and scrolls to look at the Account line and learn how she added Tom to her Personal Contacts.

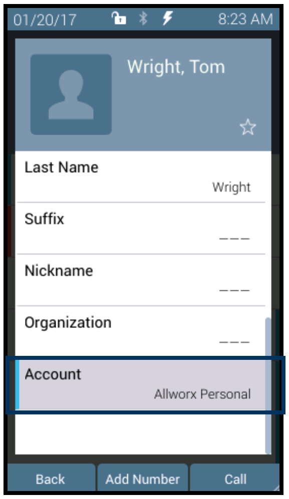


12/14/17 3:05 PM

Contacts

19 MATCHES

Mom	585-421-3854
Murphy, Shannon	315-427-6598
Murphy, Tim	585-555-1216
Robinson, Lou	585-555-1241
Smith, David	585-555-1259
Tom Wright	585-421-8560
Vandyne, Christina	---



01/20/17 8:23 AM

Wright, Tom

Last Name	Wright
Suffix	---
Nickname	---
Organization	---
Account	Allworx Personal

If the Account line reads:

- **Allworx Personal**: Jane added Tom Wright using her Verge phone, Reach device, or Interact application. To update the contact information about Tom, Jane can use her Verge phone, the Reach application or the Interact Professional application.

  *Example: **Allworx Personal***

- **Allworx User, Allworx System, Allworx Public*** – The Allworx Server Administrator manages these contacts using the Allworx System Software.

  *Example: **Allworx Users***

- Source account: Jane used Reach or Interact to synchronize her contacts with her Verge phone. There are three synchronized contact labels that may display:
  - **Email account**: Jane used the Reach application to synchronize her contacts from her email account (such as Gmail). To update the contact information about Tom, Jane must do so in her contacts application. **Example:** username@gmail.com
  - **Reach device:** Jane used an iOS or Android app (such as Contacts) to manage her contacts stored on her device, but the contacts are not associated with a third party service. To update the contact information about Tom, Jane must do so on the identified device in the appropriate Contacts app on the device synchronizing with the Allworx System.

    ***Note:** Reach for iOS version 11 or higher will look like these contact types due to iOS 11 restrictions.*

    *Example: **<Samsung SM-T530NU>***

- **Outlook account**: Jane used the Interact Professional application to synchronize her contacts from her Outlook account. To update the contact information about Tom, Jane must do so in her Outlook application.

  Example: ***Outlook:\\PersonalFolders\Contacts***

* The only user-editable options for these contacts types are the Favorite status and the choice of default phone number on the Verge phone, Reach application or Interact application.

Speed Dial

The Verge phones do not support Speed Dial numbers. To configure a Personal Contact on the Verge phone to perform the same as the 92xx IP phone series Personal Speed Dial Number, use the PIN phone number label.

Verge Phone Contact Buttons

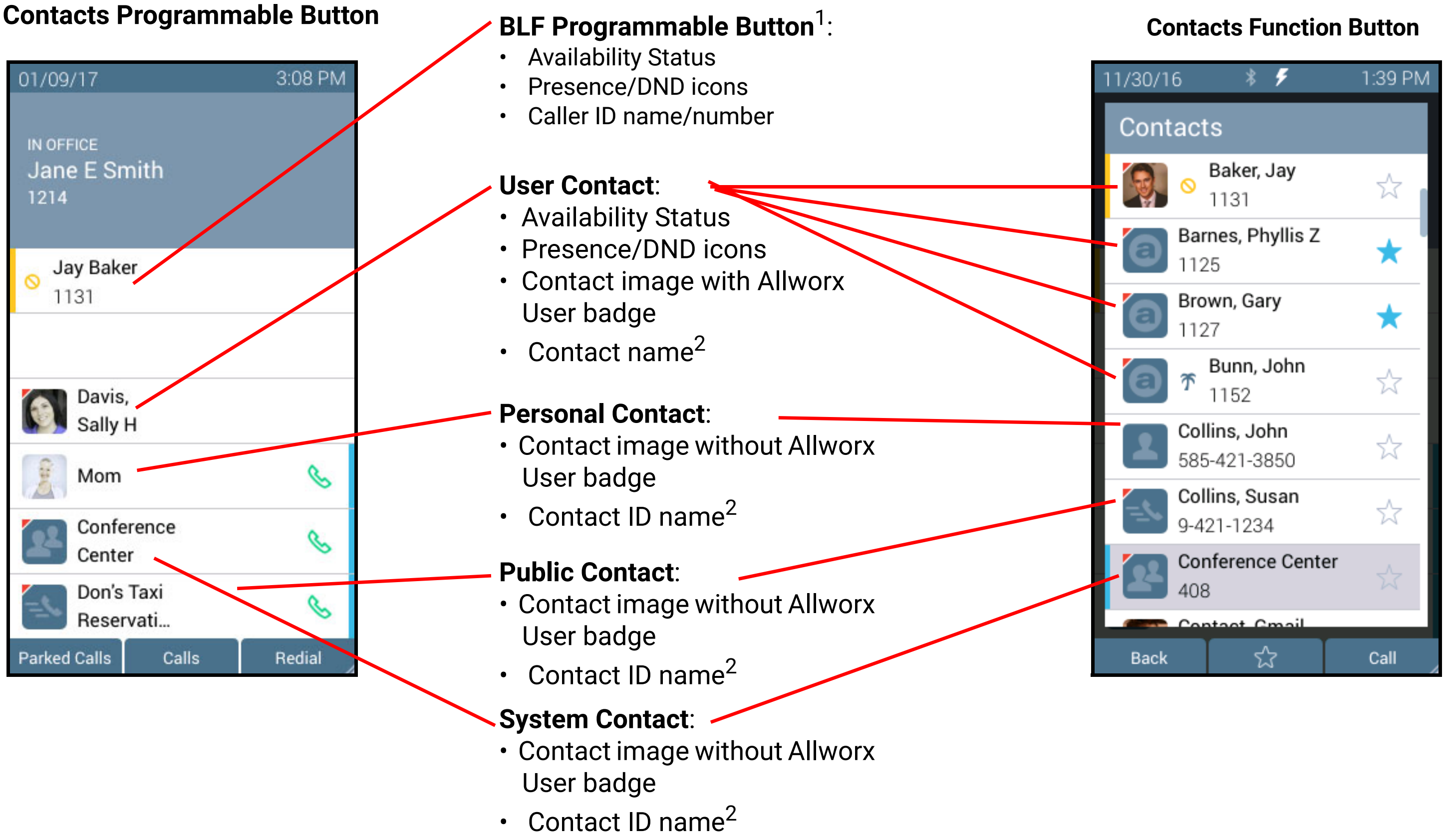
The Verge phone series has both a Contacts (👤) function button and a Contact programmable button. The Contacts programmable button (if available), is configurable by either the Allworx Server Administrator or the Verge phone user (with available permissions)

- **Contact function button** - Opens the Contacts screen.
- **Contact programmable button** - Immediately dials or transfers a call to the extension or contact phone number. There may be one or multiple Contact programmable buttons configured on the Verge phone.

Each button type displays the following information:

- Contact availability (User Contacts only)
- Image and Allworx directory badge (if either are available)
- Presence setting (if other than In Office, User Contacts only)
- Contact name/number
- Favorite status

Verge phone Contact programmable button and function button examples:



Contacts Programmable Button

Contacts Function Button

BLF Programmable Button[1]:

- Availability Status
- Presence/DND icons
- Caller ID name/number

User Contact:

- Availability Status
- Presence/DND icons
- Contact image with Allworx User badge
- Contact name[2]

Personal Contact:

- Contact image without Allworx User badge
- Contact ID name[2]

Public Contact:

- Contact image without Allworx User badge
- Contact ID name[2]

System Contact:

- Contact image without Allworx User badge
- Contact ID name[2]

[1] BLF programmable button - does not report the User Contact's presence state. Only the Allworx Server Administrator can assign this programmable button.

[2] Caller name/number only available on the Contacts screen. Press the Contacts Function Button to view.

Appendix C Restore Factory Defaults

The Allworx System restores the following settings to the Factory Defaults when performing a **Maintenance** > **Restart** > **Restart with factory defaults restored.**

Phone System > Call Details	Call Detail Storage Call Detail Streaming Call Detail Streaming Port
Phone System > Call Park	Timeout (seconds) After timeout:
Phone System > Dial Plan	Emergency • Emergency Number Rules • Number Dialed • Service Group • Dial Direct Services • Long Distance Services - Service Group • International Calls - Service Group • Outside Line Seizure - Service Group
Phone System > Languages	Primary Secondary
Phone System > Outside Lines	Incoming Call Handling • Anonymous calls are routed normally • All Caller ID Name and Caller ID Number patterns are cleared Notes are cleared
Phone System > Paging	Door Relay Mode Paging Zones: • LINE OUT
Network > Configuration	Allworx Network Mode • LAN Host Mode • NAT • Firewall • Stealth Mode

Network > Configuration *(continued)*	VLAN Configuration Public Interface • VLAN • PPPoE (on WAN Port) • PPPoE Username • PPPoE Password • PPPoE Service Name • PPPoE MTU Default Route Default Gateway • External IP Address Interface Blocking Rules Host Information • Host Name • Domain Name (DNS) Firewall • All check boxes for services
Network > T1 Lines	PPP Username PPP Password PPP MTU
Network > Multi-Site	Voicemail Transfer Settings • TCP/IP Port • Maximum Sessions • Single Message Size Limit (bytes) • Maximum Messages Per Session
Network > Static Routes	Static Route Table Entries
Network > VPN	VPN PPTP Server PPTP Network Address PPTP Network Mask PPTP Port Number PPTP Max Tunnels PPTP MTU

Servers > DHCP Server	Server • Dynamic DNS • Dynamic Start Address • Dynamic End Address • DHCP Address Reservations
Servers > DNS Server	Operation mode • Primary DNS Server • Secondary DNS Server Host Table • Allworx DNS Server hosts the DNS Zone • Host Name / IP Address
Servers > Email	Features • Connection Timeout (secs) • Voicemail Attachment Format
Servers > SMTP Settings	SMTP Port SMTP Transmit Threads SMTP Transmit Queue Depth SMTP Notify Sender of Delivery Delay Use SMTP Smart Host • Smart Host Address • Smart Host Port • Smart Host requires authorization • Smart Host User Name • Smart Host Password • Smart Host - Email for local domain • Smart Host - Voicemail for local domain Use External Outgoing Mail (SMTP) Server • External Outgoing mail (SMTP) Server Address • External Outgoing mail (SMTP) Server Port • External Outgoing Mail (SMTP) Display Name • External Outgoing Mail (SMTP) Sender’s Email Address • External Outgoing mail (SMTP) Sender requires authentication

Servers > SMTP Settings *(continued)*	POP3 Settings • Port Number • Maximum Connections • Number Client Threads • Max. Depth Client Deferred Queue • Min. Poll Period (minutes) • Secure Login IMAP Settings • Port Number • Maximum Connections Alternate Email Domains • [entries] Unsolicited Bulk Email • Use Block Services • Block Services
Servers > SNMP	Enable SNMP Agent
Servers > VoIP Server	BLF Port Secure BLF* Force Remote Phone audio through server Plug and Play Secret Key Phone Administration Password Global SIP Connection Limit Paging Base IP Addr Paging Port Paging Max Hop Count RTP Base Port RTP DSCP Tag SIP DSCP Tag * When enabled, this setting encrypts the checksum of BLF messages making them difficult to spoof.
Servers > Web	Connection Timeout (secs) Maximum HTTP/HTTPS Sessions My Allworx Manager Secure Port (HTTPS) Web Administration Secure Port (HTTPS) My Allworx Manager Port (HTTP) Web Administration Port (HTTP)

Maintenance > Backup	Start Time Frequency IP Address / Domain Name TCP/IP Port Mode
Maintenance >Notes	Notes are cleared
Maintenance >Time	Use NTP Server NTP Server NTP Server Poll Period
Maintenance > Tools	Advanced Troubleshooting • SSH port Syslog - System Events • Start/Stop • IP Address • Port

866.ALLWORX (866.255.9679) or 585.421.3850
www.allworx.com
Version: G Revised: October 7, 2022