Service Bulletin

Security Advisory

No. 20130326-0074 / Revised 05-23-2014

Related Products

- Allworx server 6x
- Allworx server 6x12
- Allworx server 24x
- Allworx server 48x

Related Software

- Allworx server software 7.6.x and earlier

Overview

One of the primary advantages of the Allworx family of products is its flexibility in configuration and settings in a way that is easy to understand. Security is an important consideration, and we are constantly striving to improve our systems to protect our partners and their customers. It is also equally imperative that you never knowingly put your customer in a situation where it is easy for fraudulent attacks to compromise their Allworx systems.

We are investigating reported instances and have seen fraudulent SIP registration attacks that search public IP addresses and gain access to either an Allworx server or, most recently, to remote Allworx handsets not installed behind a firewall. We have also received reports of recent toll fraud incidents in which fraudulent attacks take over the SIP registration of an Allworx handset attached to a public network. This document summarizes the security best practices to prevent security compromises.

Refer to Service Bulletin: Security Advisory No. 20130206-0074 for additional information.

What You Should Do

When installing an Allworx system, it is imperative to use the proper security settings so that hostile, unauthorized attempts to access the system do not result in situations where either remote access or the spoofing of handsets can occur. Most often, the result is unauthorized calling and toll fraud. Compromises usually start with port scans to determine if a host is a candidate for unauthorized access. Disabling the use of ports often discourages a fraudulent attack, and the attacker will move on to another IP.

Changing Passwords

Use strong passwords for server and phone administration pages. Change the password so outside users cannot easily guess it. The new password should be a minimum of eight alpha/numeric characters that are both upper and lower case. **DO NOT** use simple passwords such as “1234” or “Allworx”.

To change the admin password:

1. Log in to the Allworx server admin page.
2. Navigate to **Business** > **Users**. The Users page displays.
3. Locate the Users section, and then locate the Administrator, System line in the table. Click the **Modify** link. The Modify page displays.
4. Locate the Identification section, and then the Password field.
5. Type a new password in the field that contains at least eight upper/lowercase characters and digits.

   DO NOT use simple passwords such as “1234” or “Allworx
6. Locate the Confirm Password field and re-type the password exactly as in the Password field.
7. Click **Update** to save the changes.

To change the user password:

1. Log in to the Allworx server admin page.
2. Navigate to **Business** > **Users**. The Users page displays.
3. Locate the Users section, and then locate the user line in the table. Click the **Modify** link. The Modify page displays.
4. Locate the Identification section, and then the Password field. To require users to change the password:

   Locate the **Require Password Change** and **Require PIN Change** checkboxes. The server default (checked) requires the user to update each password at next login. If the Allworx Server Administrator unchecks the box, the user does not need to update the password at the next login.
5. Type a new password in the field that contains at least eight upper/lowercase characters and digits.

   DO NOT use simple passwords such as “1234” or “Allworx
6. Locate the Confirm Password field and re-type the password exactly as in the Password field.
7. Click **Update** to save changes.

To change the Plug ‘n’ Play Secret Key:

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

1. Log in to the Allworx server admin page.

2. Navigate to **Servers** > **VoIP** and click the **modify** link.

3. Locate the VoIP Server section. If the Plug ‘n’ Play Secret Key and/or the Phone Administration password is hidden, click the **show** link. This displays each password.

4. Type a new password that contains at least eight upper/lowercase characters and digits in each field.

   DO NOT use simple passwords such as “1234” or “Allworx.

5. Click the **hide** link for each field.

   For additional security, disable the Plug ‘n’ Play options. Check the boxes in the bottom of the section.

Option	Description
Disable Phone Creates via LAN Plug ‘n’ Play	This option prevents installing Plug ‘n’ Play handsets on the Allworx server LAN. The system default is unchecked, which enables Plug ‘n’ Play. When checked, manually add the phones to the Phone System > Handsets page.
Disable Phone Creates via WAN (Remote Phone) Plug ‘n’ Play	This option prevents installing Plug ‘n’ Play handsets on the Allworx server WAN (i.e. remote handsets). The system prevents installation, even if programming the remote handset with the server’s Plug ‘n’ Play secret key. The system default is unchecked, which enables Plug ‘n’ Play. When checked, manually add the phones to the **Phone System** > **Handsets** page.
Disable Assign User at Phone	This option prevents assigning a user to a newly installed phone using the Plug ‘n’ Play User Assign menu on the phone. Note: Previously added Handsets to the system re-register with the server, regardless of these settings.

6. Click **Update** to save changes.

To change the password on a 3rd-party SIP phone:

1. Log in to the Allworx server admin page.

2. Navigate to **Phone System** > **Handsets**.

3. Locate the SIP Handsets section, and then the Show line. Check the Generic SIP Handsets box and the list filters to show only the generic SIP handsets.

4. Locate the Generic SIP handset in the table and click the **Modify** link.

5. Locate the SIP Registration section.

6. Enter a new Password for the phone to authenticate with the server.

7. Click **Update** to add the new handset to server.

8. Configure the 3rd-party phone following its particular configuration instructions using the User ID, Login ID, (shown on the updated **Phone System** > **Handsets** page), and the entered password.

   When registering a phone with the server, its entry on the Handsets page will indicate it is registered that by displaying an expiration date and time.

Note: Each Generic SIP handset requires a license in order to operate. Server keys provide licenses. Allworx Server Administrators can add a small number of handsets without a key (2 on 6x12 6 on 6x, and 12 on the 24x and 48x). Generic SIP handsets that are on the system prior to upgrading to 7.5 will continue to operate without licensing. Available feature keys provide one, five, or 10 licenses each. To enable larger numbers of Generic SIP handsets, install multiple feature keys of the same or different license counts.

Change the Network Configuration

1. Log in to the Allworx server admin page.

2. Navigate to **Network** > **Configuration**. The Configuration page displays.

3. Click the **modify** link at the top of the table.

4. Locate the WAN Configuration section, and then locate the Allow admin configuration on WAN interface checkbox.

   If the server is behind another firewall, inside a secure network, check the box. Otherwise, leave the box unchecked.

   If exposing the server's WAN directly to the internet, leave the box unchecked.

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

Security Improvements

The SIP Registration Passwords for Allworx Handsets are no longer settable. During a reboot from the administration web page, the system regenerates the registration password.

The Allworx Handset requires a valid login to obtain the Configuration Report.

SIP Registration is no longer contained in the Configuration Report from the Allworx Handset.

Please implement the following practices when installing any Allworx system:

Server

- Install the server behind a firewall or connect it to the public internet using the WAN port. **DO NOT** connect the Allworx LAN port directly onto the public internet.

- Disable Allworx WAN services (ports) not in use.
- Change voicemail ports (SMTP and IMAP) to non-standard port numbers.
- Verify that there is no exposure of the Admin Page (Port 8080) to the Public network. **DO NOT** port forward directly to the LAN port of an Allworx server from the customer's router. For remote maintenance, use the Allworx VPN. Navigate to **Home** > **Network** > **VPN** > **modify** to configure the VPN settings.

When configuring WAN interface to connect to the public internet:

- Enable the server in NAT Firewall mode, preferably with Stealth DMZ. In stealth mode, the WAN interface does not respond to "pings" from other devices.

Remote phones

Password protection is very important to avoid fraudulent attacks on remote phones. Implement the following practices when installing an Allworx remote phone:

- Use proper firewall protection to connect remote Allworx phones to the public Internet. Allworx handsets provide web access to important information, including its login credentials and SIP Registration password. Phones with weak Phone Administration Passwords can easily have the SIP Registration passwords stolen.
- Disable Phone Creates via LAN and WAN Plug 'n' Play except during phone installation.

Px Expander

- Change the Px admin password from the default value.
- Use proper firewall protection to connect remote Allworx Px Expanders to the public Internet. The Px Expander provides web access to important information, including its login credentials and SIP Registration password.
- Disable Phone Creates via LAN and WAN Plug 'n' Play except during phone installation.