Unite Axess for Smart Devices
– Customer Deployment Considerations

Customer deployment considerations – this guide will help you plan deployment of Unite Axess for Smart Devices

Deploying smart devices with connectivity to multiple information systems for the purpose of sending mobile alerts can be a daunting task–thoughtful deployment strategies and planning are the key to success.

System components overview

There are five basic system components to enable smart devices with professional messaging:

1. **Base system** – Unite Connectivity Manager (h/w appliance & software) or Unite Communication Server (software only)
2. **Unite Axess for Smart Devices & Unite Application Manager** (software)
3. **Windows® server environment** (hardware & software)
4. **iOS, Android smart devices** (mobile device hardware)
5. **Unite Axess app** (mobile device software)

Each of these components is necessary for the successful implementation of an integrated solution.

1. Base system – Unite Connectivity Manager (Unite CM) or Unite Communication Server (Unite CS)

The Unite base system supports overall messaging functionality including 2-way interactive messaging, user management and overall administration. Unite CM includes software licensing deployed on Ascom Elise 3 appliance. Redundancy option is available.

2. Unite Axess For Smart Devices & Unite Application Manager

Unite Axess for Smart Devices is a software application enabling alerts and messaging for mobile staff on iOS and Android devices. This software resides on a Windows® server. Redundancy option is available. Unite Application Manager software is required to manage installation of the Unite Axess application software.

3. Windows® server environment

Refer to Windows® server environment requirements on page 3 for specifics.

4. Smart devices

Unite Axess supports 2-way interactive messaging with both Android (OS 6.x, 7.x) and iOS (10.x, 11.x) smart devices. Smart devices must be able to support 3G, 4G or LTE data connectivity and/or WLAN connectivity to enable messaging.

5. Unite Axess App

Unite Axess for Smart Devices app may be downloaded for iOS devices only from Ascom Partner Extranet site. iOS Demo version is available for download on Apple App Store.

Best practice recommendations

- Manage timing of device OS updates to assure the best interoperability with the Ascom app – check Ascom device OS support before upgrading your devices
- Implement Mobile Device Management (MDM) security software to monitor, manage and secure employee's mobile devices, and protect sensitive company data stored on these devices
- Connect devices to both a wireless carrier and WLAN networks to provide failover capability and maximize network uptime and reliability
- Require PIN code for device access (Required for data protection)
- Require user name and password for app access (Required for data protection)
- Perform a WiFi assessment to assure appropriate facility coverage
- Utilize direct socket connection for primary message notification rather than Google or Apple push notification services (Apple/Google push notifications services can serve as backup)
- A pilot and phased rollout significantly reduces implementation risks
- Select your most knowledgeable users for any pilot deployment to assure appropriate and useful feedback

Customer responsibilities

- Supply smart devices to be used by staff, or support Bring Your Own Device (BYOD)
- Subscribe to carrier voice/data services for chosen smart devices with an appropriate service level agreement, ensuring appropriate wireless coverage
- Configure smart device settings to connect devices to WLAN (if WLAN connectivity desired or needed)
- Load Unite Axess app on mobile devices to be utilized for messaging
- Provide Windows® 2008/2012 server for the Ascom software, configured with MS SQL Server
- Purchase a signed security certificate for the Windows® server to ensure a trusted source to cover both 3G/4G and WiFi domains. Self signed certificates are not supported
- Configure firewall to allow Unite Axess for Smart Devices application server communication with Apple Push Notification Service (APNS) or Google Cloud Messaging and direct socket connection
- Enable setup of Secure Reverse Proxy for messaging interaction via the Internet
- Provide 3rd party mobile device management software
- Ensure adequate WLAN coverage, appropriate IT infrastructure, provisioning of smart devices and compliance with data protection and security policies.

User authentication and encryption

Access to information stored in the smart device app, including alert messages and Chat (text) messages, requires authentication between the user and Unite Axess user database. Authentication utilizes both the user identification (ID) and password to gain access to information stored in the app. This process helps ensure information privacy and data security. All message communication, including Chat and alert messages are encrypted over-the-air for security purposes.

Message notification options

There are two message notification options supported by Ascom: direct socket connection and Apple/Google push notification services. Both options should be configured during the installation process.

Direct socket connection

The smart device has a connection enabled to a port on the Axess server specified during installation. This connection port works regardless of which communications connection (wireless carrier or WiFi) is utilized. Direct socket connection is recommended for mission-critical messaging to ensure prompt message delivery. This option requires a port to be opened in the firewall. The Axess server always attempts to deliver messages using this as the primary option.

Apple/Google push notification services

A secondary option for message delivery but timing is not guaranteed...only best effort is made. This is not recommended for mission-critical messaging. This delivery option should be configured as a backup to direct socket connection.

Mobile device support

Ascom supports both iOS and Android devices including smartphones and tablets. Specific device testing is part of the verification process to ensure the best possible user experience. Android and iOS devices can of course be used together in a mixed-device environment. The following devices will be tested as part of the verification process:

- Ascom Myco
- Samsung Galaxy S7, S8, A5, A8, A10.1
- Samsung XCover 3, Xcover 4
- Apple iPhone 5S, 6, 6S, 7, 8

Wireless carrier support

Our solution supports any carrier network utilizing 3G, 4G or LTE for data connectivity. 2G/EDGE is not supported by our application due to lack of support for simultaneous voice and data - meaning an alert message will not break through until the voice call has ended. This is unacceptable for mission-critical communications.

Caution: LTE can be problematic if the wireless carrier and handset do not support VoLTE. Then CSFB (Circuit Switched Fallback) will be used which may result in a data connection that is not available for up to 10 seconds when switching between voice and data.

Mobile Device Management (MDM) software

MDM is software utilized to manage, administrate and secure mobile devices which may be deployed across multiple service providers and multiple mobile operating systems. MDM software is often combined with additional security measures to create a more secure environment to protect sensitive company data stored on mobile devices. MDM solutions typically support smart devices and offer an efficient way to view and manage all devices from a central point of administration. MDM solutions allow you to define enterprise settings, policies and restrictions for devices without requiring user interaction. These policies often include passcode/PIN enforcement, user restrictions, WiFi, VPN, email, applications and more. A MDM solution is an essential component of any deployment, and Ascom strongly recommends using this tool.

Microsoft® Windows® environment

Hardware requirements

- Windows® Server 2008 or 2012
- RAM: 4GB
- Processor: 2GHz 64-bit processor
- Disk Space:
  - 10GB with SQL Express 2008 R2
  - 20GB with SQL Express 2012
- Network card: Ethernet 100/1000 Mbit/s

Software requirements

- Microsoft .NET Framework 4.6
- Internet Information Server IIS 7.5, IIS 8 and IIS 8.5
- Microsoft Windows®
  Microsoft SQL Server 2008 R2 Standard or Express,
  Microsoft SQL Server 2012 Standard or Express,
  Microsoft SQL Server 2014 Standard or Express

(Note: may reside on same server as Unite Axess application)

Device configuration

When you need to deploy and configure a large number of smart devices there are differing options based on the device itself. Mobile device management software, as discussed previously, provides the most advanced capability. Other options to load the app and configure devices are also available, either provided as a separate tool from the vendor, or as native functionality. Detailed instructions are available in the Unite Axess for Smart Devices Installation Guide.

Wireless data connectivity

Wireless data connectivity is extremely important because it enables messaging for devices using the Unite Axess app. There are two options: data connectivity via WLAN or through a wireless carrier network. To be able to receive and respond to alert messages you must have a data connection at all times. Coverage inside a facility is critical regardless of your data connection choice – no coverage, no messaging.

If your devices support only WLAN connectivity, then there is no coverage for your devices outside the range of your WLAN network. This option may reduce or eliminate carrier network charges, but limits use of the device to inside the WLAN coverage area.

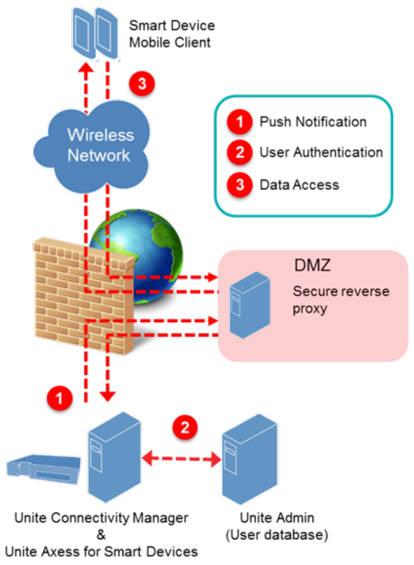
Wireless carrier networks can operate inside and outside facility walls and provide broader coverage, but this coverage may result in monthly service charges. Some may choose to deploy devices using both WLAN and wireless carrier connectivity to maximize use and reliability. Regardless of your data connectivity choice, verifying coverage for the applicable use-cases is a must. Mission-critical communication necessitates reliable connections and uptime. Performing a wireless survey inside your facility is the best way to ensure adequate coverage.

Adding to an existing Ascom system

Ascom on-site wireless devices like paging, DECT and VoWiFi devices were designed with specific messages alert features. These features, including color-coded messages and distinctive alert tones, help users easily distinguish message priorities. Those same features are also supported in the Unite Axess app. Other features, including centrally defined event priorities and softkey response buttons, are also supported on both device platforms. Unite Axess is the perfect complement to an existing Ascom installation. Your investment in Ascom devices and existing Unite integrations can be can be leveraged with the Unite Axess app.

Solution architecture overview

- Alert messages are pushed to the smart device.
- All message communication is encrypted end-to-end for maximum security.
- User authentication performed via Unite Admin and required to access messages.
- Secure reverse proxy support required for app interaction.



Ascom
Grimbodalen 2
402 76 Gothenburg
Sweden
Phone: +46 31 55 93 00
www.ascom.com