End-User Experience for Android Operating Systems

This document contains the following sections:

- Enrollment System User Experience
- Enrollment Wizard User Experience
- Common Android Issues

Overview

The Android operating system presents a challenge when it comes to offering a consistent user experience because the different vendor and operating system combinations behave in slightly different ways. During the device configuration process, the Wizard makes every attempt to provide a seamless experience by detecting the OS version on the device and providing the appropriate user prompts during the onboarding process.

The Wizard application automates the configuration process, resolves software conflicts, and migrates your Wi-Fi connection to the secure network.

Supported Android Versions

The enrollment Wizard supports the following operating systems for Android devices: 2.1 (Eclair), 2.2 (Froyo), 2.3 (Gingerbread), 3.0 (Honeycomb), 3.1, 3.2, and 4.0 (Ice Cream Sandwich), 4.1, 4.2, and 4.3 (Jelly Bean), 4.4 (KitKat), and 5.0 (Lollipop), as well as a 'support next version' flag.

Note >>
Networks may not support all versions of the Android OS. Contact the network help desk to verify the supported Android versions.

This document provides an example of the prompts a user might see when using the XpressConnect application. Depending on the configuration set up by the network administrator, the device manufacturer, and operating system, the user prompts can vary.

Additionally, the enrollment Wizard is a highly-customizable application. Screen icons, color schemes, and messaging can all be customized by the network administrator. This guide provides examples with generic screens and messaging, which might be different than what is displayed on the device.

Enrollment System User Experience

The Enrollment System provides the prompts that guide the user through the sequence of steps that make up the enrollment workflow. During this process, the user enters information as requested, and makes selections about user type, device type, among others. The sequence of steps for the enrollment differ, depending on the selection that is made.

Welcome Screen With AUP

When the user enters the enrollment URL on their device, the Login (or Welcome) screen displays. The login screen is typically customized with the logo, colors, and text for the organization or institution. The screens in this example use the default look and feel of the application.

Note >>
If you have set up a captive portal, the user connects to onboarding SSID and is redirected to the ES Welcome page to start the enrollment process.

FIGURE 1. Enrollment Welcome Screen
An acceptable use policy (AUP) prompt displays a message and requires that the user signal acceptance to continue. The text on the Welcome screen or Start button can be customized.

**User Type Prompt**

If required by the network, the user might see a User Type prompt. For example, an Employee might be required to enter domain credentials, and a Guest or Partner might be required to enroll using their social media credentials.

**FIGURE 2. User Type Prompt**
Select the user type to continue. This example follows the *Employee* workflow.

**User Credentials**

If required by the network, a prompt similar to the one below requires the user to enter network credentials.

**FIGURE 3. User Credential Prompt**
Enter the user credentials and tap *Continue*.

**Device Type**

If required by the network, the user might see a Device Type prompt. For example, a Personal device selection might add a prompt for a MAC address, and a IT-Issued device would be allowed to bypass the MAC address prompt.

**FIGURE 4. Device Type Prompt**
Select a device type to continue. This example follows the *Personal Device* workflow.

**BYOD Use Policy**

A BYOD use policy prompts the user to accept the conditions for using a personal device on a secure network.

**FIGURE 5.  BYOD Use Policy**
Review the use policy and tap the *Continue* button.

**Android-Specific Configuration Instructions**

The application detects the user agent for the Android operating system and provides the correct configuration instructions. This screen includes the steps to install the application and to configure the device.

**FIGURE 6. Instructions for Android Devices**
Tap **Step 1: First, Install the App** to start the installation process.

**Download and Install Application**

The application is available from Google Play Store, Amazon Market, and as a Direct Download from a local web server. The network administrator can limit the download options. In which case, the download prompt may not display all three options.

**FIGURE 7. Select Installation Method**
Select the installation method to continue.

**Install from Google Play**

If permitted by the network configuration, the application can be installed from the Google Play Store.

**FIGURE 8. Install from Google Play Store**
Tap *Install* to continue.

**Accept Access Request**

To run the enrollment wizard and configure the device, the application requires access to a couple of systems on the device.

**FIGURE 9.  Access To Device Systems**
Tap *Accept* to continue.

**Return to Configuration Screen**

After the application has been installed on the device, you might be prompted to open the application from the Google Play Store installation screen. Do not open the application from this screen.

**FIGURE 10. Installation Finished**
Do not tap the Open button. Use the Back arrow to return to the Installation and Configuration screen.

**Close Download Options**

If you are returned to the Installation and Configuration screen, you might need to close the installation options pop-up.

**FIGURE 11. Close Download Options Window**
Tap the X in the top-right corner of the pop-up window to continue.

**Install from Amazon Market**

If permitted by the network configuration, the application can be installed from the Amazon Market.

**FIGURE 12. Install From Amazon Market**
Click *Install* to start the installation process.

**Return to Configuration Screen**

After the application has been installed on the device, you might be prompted to open the application from the Amazon Market installation screen. Do not open the application from this screen.

**FIGURE 13. Installation Finished**
Do not tap the Open button. Use the Back arrow to return to the Installation and Configuration screen.

**Local Download**

If permitted by the network configuration, the application is available for download from a local web server. Go to the device Downloads to locate the application.

**FIGURE 14. Local Download**
Double-tap the XpressConnect application to start the installation process.

**Accept Access Request**

To run the enrollment Wizard and configure the device, the application requires access to a couple of systems on the device.

**FIGURE 15. Install Application**
Click *Install* to continue.

**Return to Configuration Screen**

After the application has been installed on the device, you might be prompted to open the application from the Amazon Market installation screen. Do not open the application from this screen.

**FIGURE 16. Application Installed**
Do not tap the *Open* button. Tap *Done*, or use the Back arrow to return to the Installation and Configuration screen.

**Configure Application**

Return to the *Installation and Configuration* screen and tap *Configure Your Device*.

**FIGURE 17. Configure Your Device**
After the application is installed, the Wizard opens to start configuring the device. See the following sections for an example of the Wizard user experience on Android devices.

**Enrollment Wizard User Experience**

The Wizard is the dissolvable application that runs during enrollment. The Wizard examines the device operating system and configuration to determine how to proceed with configuring the device for the secure network.

The user experience is slightly different for devices running Android OS version 4.3, and earlier than it is for devices running newer Android versions. Namely, in the older versions, you are prompted to install the credentials into the keystore.

The following sections provides example screens that a user might see during the Wizard configuration process.

**User Experience Example for Android Version 4.3, and Later**

The device configuration process is more streamlined, with fewer user prompts, for Android devices running a newer version of the operating system.

For the user experience for devices running older Android versions, see User Experience Example for Android Version 4.2, and Earlier.

**Accept Device Changes**

After you tap *Configure Your Device*, the Wizard runs to install the network configuration on the device.

The configuration wizard assesses the current configuration state of the device and displays the list of changes that need to be made.

**FIGURE 18. Changes Made to Device**
The following changes will be made to your device:

- The wireless client on your device will be configured to connect to 'DVES-Secure'.
- 5 CA certificate(s) will be installed.
- 1 user certificate will be installed.
- Your device will be connected to the 'DVES-Secure' network.

Tap **Continue** to allow the application to make the listed changes on the device.

**Attempting to Connect to the Network**

After configuring the device, the application attempts to move the device to the secure network.

**FIGURE 19. Attempting to Connect**
**Note**

In some configurations, the device is configured, but not migrated to secure network. In these cases, the network administrator allows the device to be pre-configured, for use when the device is in range of the secure network.

**Connected**

When the enrollment process is finished, the application indicates that the device has been moved to the secure network.

**FIGURE 20.** Connected
When the application has successfully configured the device and migrated it to the secure network, a message displays indicating that the process has completed.

**User Experience Example for Android Version 4.2, and Earlier**

The user experience is slightly different for devices running Android OS version 4.3, and earlier. Namely, the user is prompted to install the credentials into the keystore. Before each certificate prompt, the application displays a message that tells you how to respond on the credential extraction and installation screens.

**Changes Made to Your Device**

After you tap *Configure Your Device*, the Wizard runs to install the network configuration on the device.

**FIGURE 21. Accept Device Changes**
Tap *Continue* to allow the application to make the listed changes on the device.

**Passcode PIN or Pattern Lock**

The Android OS requires the user to enter your passcode PIN or pattern to unlock the keystore and install the certificates on the device.

The application provides instructions for responding to these prompts. Read each screen carefully and respond as directed to the screens that follow.

**FIGURE 22. Prompt to Respond to Passcode Lock**
Tap *OK* to continue.

**Confirm the Screen Lock Passcode**

Confirm the screen lock passcode to allow the application to install the certificate into the keystore.

---

**Note >>**

Certain Android devices do not allow a pattern to secure the keystore. This is a function of the Android OS and not the XpressConnect application. In these cases, the user is prompted to enter a PIN passcode for the screen lock before they can continue.

---

**FIGURE 23. Pattern Lock**
Enter the passcode PIN or pattern lock to continue.

**How to Respond to Certificate Installation Prompts**

Before each certificate prompt, the application displays a message that tells the user how to respond on the following credential extraction and installation screens.

Read each screen carefully and respond as directed to the screens that follow.

**FIGURE 24. How to Respond to Certificate Prompts**
Tap OK to continue.

**Extract Certificate**

The device requires access to the keystore to extract the certificate.

**FIGURE 25. Password to Extract the Certificate**
Tap OK to extract the certificate, as instructed on the previous screen.

**Name the Certificate**

The application pre-populates the certificate name based on the network configuration.

**FIGURE 26. Name the Certificate**
Unless prompted otherwise, tap OK to keep the default name.

**Note >>**

If the network has been configured for additional credentials, you might be required to repeat the previous 3 steps (Message, Extract, Name Certificate).

**Attempting to Connect to the Network**

After configuring the device, the application attempts to move the device to the secure network.

**FIGURE 27. Attempting to Connect**
The application continues the connection process without user intervention.

**Obtaining IP Address**

The Wizard ensures that association and authentication are successful, and verifies that an IP address is received.

**FIGURE 28. Obtaining IP Address**
The application continues the connection process without user intervention.

**Connected**

When the enrollment process is finished, the application indicates that the device has been moved to the secure network.

**FIGURE 29. Connected**
Congratulations! Your device is now configured to use this network.

As part of the configuration of your network, certificates were installed in to your devices certificate store. Android will not allow you to uninstall this app as long as those certificates are installed. To clear all certificates, go to Settings -> Security -> Clear all credentials.

Your device is now configured to use the network. It is not necessary to run this program again unless you experience difficulties connecting to your wireless network.

Your IP address is 192.168.7.61

When the application has successfully configured the device and migrated it to the secure network, a message displays indicating that the process has completed.

**Common Android Issues**

This section describes issues with using XpressConnect on the Android operating system that might prompt you to contact the network help desk.

**Retrieve Log Files**

Administrators can direct users with connection issues to email a log file from the Android device to the Support team. Tap the menu button on the top right of the screen and select *E-mail log file*.

**FIGURE 30. How to Send a Log File**
Passwords and Lock Screen PINs

The Android operating system stores portions of the data needed to authenticate in an encrypted key store. On Android versions prior to version 4.0, a password is needed to access the key store. Starting with version 4.0, the lock screen pin is the password that is used to access the key store, which is why the operating system requires that the lock screen to be enabled.

To clear the key store, Go to the Settings screen, select Security, and scroll to the bottom of the screen and select Clear Credentials.

Blank Certificate Field

Android does not have a supported method for getting certificate chains in to the key store for use in authentication. Because of this, XpressConnect uses workarounds to make the authentication system use certificate chains. However, some workarounds do not show up in the settings screen.

In addition, if Android claims the certificate was installed in the key store and then the authentication fails, the application falls back to our workaround methods. This is done because some devices claim to have installed the certificate, but actually don't.

Certificate Passwords

Android APIs do not allow XpressConnect to specify the password when the application inserts the certificate into the key store. The workaround is to use a password prompt to install the certificate. You simply enter the password that is displayed in the password prompt and XpressConnect installs the certificate.

Android .netconfig File

If you tap the link to Continue with configuration of the network and receive a message that says it downloaded a file called android.netconfig, they need to check the device for the following issues:
1. You do not have the XpressConnect Wizard installed, so the server cannot instruct the device to start the application and use the file.

2. You were prompted to Play Online or Download when tapping the link, and selected Download. The user must select Play Online for the wizard to start up.

3. There is a misconfiguration in the server. Contact the local help desk for more information.

**Memory Card**

In some cases, the XpressConnect Wizard stores data on the memory card in the device. If you remove or change the memory card, authentication fails, and you must redeploy the wizard with the new memory card in the device to get it working properly.

**Uninstalling the Application**

It is sometimes necessary to remove the 802.1X configuration and certificates provided by the wizard before you can uninstall the application. This is enforced by the device OS, and not by the XpressConnect Wizard.

If you encounter issues while attempting to uninstall the XpressConnect application from your Android device, check the following settings:

**Remove Device Administrator**

If the device has any settings configured that use Android’s device administration capabilities (such as mobile device management), the XpressConnect Wizard creates an administrative user during installation and this user must be removed before XpressConnect can be uninstalled.

Go to *Settings > Security*, select *Device Administrator* and uncheck the XpressConnect administrative user.

**FIGURE 31. Remove Device Administrator**
**Remove Certificates**

If there are certificates on the device that were installed by the Wizard, they should be removed. Go to Settings > Security and select Clear Credentials (or Clear Storage).

**FIGURE 32. Remove Certificates**
Remove SSID

The user might be required to remove the SSID from the device. Go to Settings > Wi-Fi and locate the SSID for the network, and tap Forget.

FIGURE 33. Forget Network
Remove Log Files

If the XpressConnect log files remain on the device, they can be removed. Mount the device as a drive, and locate the XpressConnect.log and xpc_old.log files on the device internal storage.