

Deploying Corporate Android Devices on Closed Network

VMware Workspace ONE UEM

You can find the most up-to-date technical documentation on the VMware website at:

<https://docs.vmware.com/>

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Copyright © 2021 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

Contents

- 1** How to Deploy Corporate Owned Android Devices on a Closed Network 4
 - Supported Enrollment Methods 5
 - Configure Android EMM Settings in the Workspace ONE UEM Console 5
 - Enable AirWatch Cloud Messaging for Push Notification Capabilities 6

- 2** QR Code Enrollment For Closed Network Devices 7
 - Configure and Host a PAC file for Network Configuration 7
 - Host the Workspace ONE Intelligent Hub App on the Closed Network 7
 - Creating a QR code for Closed Network Enrollment 7
 - Enrolling the device using a QR code 8

How to Deploy Corporate Owned Android Devices on a Closed Network

1

You can configure Workspace ONE UEM to manage your corporate owned Android devices that are enrolled and deployed within a closed network. A closed network here refers to one in which devices cannot connect to Google services. The environment can simply be an intranet or deployment in a region where Google services are not available. This page covers corporate-owned device deployments on a closed network, not BYOD devices.

How it works

When enrolling a Work Managed device, the Intelligent Hub adds a managed Google account to the device. The managed Google account is used to push public applications and related policies through the Managed Play Store.

When Workspace ONE UEM is set up for a closed network deployment, the managed Google account is not added on the device. Therefore, devices need not connect to Google to complete enrollment. Profiles (with the exception of Public App Auto Update), Products, and Internal Applications (uploaded to the Workspace ONE UEM console) can be pushed to the device since these resources are delivered from Workspace ONE to the device directly without Google connectivity.

Closed Network Considerations

When deploying corporate owned devices on a closed network without connection to Google services, consider the following:

- Only Work Managed enrollment is possible. Corporate Owned Personally Enabled (COPE) is not available without Google connectivity.
- Public applications cannot be deployed as there is no access to the Play Store. By extension, Public App Auto Update profiles also cannot be applied.
- Applications must be uploaded to the Workspace ONE UEM console as an internal app for deployment to devices on closed networks.
- If you wish to set up only a portion of your devices in a closed network, you must complete the Android EMM Registration using [Managed Google Accounts](#).
- You must use AirWatch Cloud Messaging to manage your Android devices in real time. Firebase Cloud Messaging is not supported as devices cannot connect to these servers.

This chapter includes the following topics:

- [Supported Enrollment Methods](#)
- [Configure Android EMM Settings in the Workspace ONE UEM Console](#)
- [Enable AirWatch Cloud Messaging for Push Notification Capabilities](#)

Supported Enrollment Methods

Barcode Staging - Zebra only

For organizations managing Zebra devices, Barcode Staging enrollment methods using the StageNow are supported in closed networks.

If your organization deploys applications only through Product Provisioning, there are no additional PAC file setup requirements.

If your organization deploys applications uploaded to the Apps & Books > Applications section of the Workspace ONE UEM Console:

- A PAC file must be hosted on an http/https endpoint within the closed network to skip Google connectivity checks performed by the Android Download Manager during enrollment and application provisioning. Please see the **Configure and host a PAC file for network configuration** for the recommended PAC file configuration.
- For any Wi-Fi configurations added to the device manually or through profiles, add an "Auto" Proxy configuration using this PAC file.

QR Code Enrollment

For all other devices, the only supported enrollment method is QR Code enrollment.

Organizations using this method need to meet the following requirements:

- The Workspace ONE Intelligent Hub for Android application must be hosted on an http/https endpoint within the closed network so the device can download the app during enrollment.
- A PAC file must be hosted on an http/https endpoint within the closed network to skip Google connectivity checks performed by the Android Download Manager during enrollment and application provisioning.
- For any Wi-Fi configurations added to the device manually or through profiles, add an "Auto" Proxy configuration using this PAC file.

Configure Android EMM Settings in the Workspace ONE UEM Console

The Workspace ONE UEM Console configuration varies based on whether all or some of your Android devices are connected to a closed network.

If all managed Android devices are connected to a closed network

You do not need to complete the Android EMM Registration. This configuration may apply to organizations operating in areas with restricted access to Google services, such as China.

- 1 Navigate to **Groups & Settings > All Settings > Devices & Users > Android > Android EMM Registration** at the customer-type Organization Group.
- 2 Enable "**Deploy without Google registration if you are operating on a closed network or are unable to communicate with Google Play**".

If some managed Android devices are connected to a closed network

Configure Workspace ONE to enroll Work Managed devices without a Google account in a specific Organization Group. The instructions below assume that you already setup Android Enterprise by registering with Google using [Managed Google Accounts](#).

- 1 Navigate to the organization group under which devices for closed network will be configured.
- 2 Navigate to **Groups & Settings > All Settings > Devices & Users > Android > Android EMM Registration**.
- 3 Under the **Enrollment Settings** tab, set the **Work Managed Enrollment Type** to **AOSP/ Closed Network**.

Enable AirWatch Cloud Messaging for Push Notification Capabilities

VMware AirWatch Cloud Messaging (AWCM) provides secure communication to your back-end systems with the VMware AirWatch Cloud Connector (ACC). The ACC uses AWCM to securely communicate with Workspace ONE UEM powered by AirWatch. AWCM streamlines the delivery of messages and commands from the UEM console to devices by eliminating the need for end users to access the public Internet or use consumer accounts, such as Google IDs. AWCM serves as a comprehensive substitute for Firebase Cloud Messaging (FCM) for Android devices when operating within a closed network. Detailed installation guidance is available [here](#).

Once AWCM has been installed:

- 1 Navigate to **Group & Settings > All Settings > Devices & Users > Android > Intelligent Hub settings > AirWatch Cloud Messaging**.
- 2 Enable **Use AWCM instead of FCM As Push Notification Service**.

QR Code Enrollment For Closed Network Devices

2

This chapter includes the following topics:

- [Configure and Host a PAC file for Network Configuration](#)

Configure and Host a PAC file for Network Configuration

Devices that ship with Google services pre-installed (also known as GMS devices) test their connectivity to certain Google endpoints when connecting to Wi-Fi networks. If these connectivity checks fail, out-of-box enrollment and provisioning of Internal Applications uploaded to the pages fail.

If the network being used to enroll the device is also closed and has no access to Google endpoints, it is possible to skip the connectivity checks by using a Proxy Auto-Configuration (PAC) file that simply directs the device to make connections directly, without the use of proxies.

The contents of the PAC file:

```
function FindProxyForURL(url, host) {  
  return "DIRECT";  
}
```

Note that an actual proxy server is not required. A PAC file with the contents above should be hosted on an http/https endpoint within the closed network.

Host the Workspace ONE Intelligent Hub App on the Closed Network

During work managed enrollment, the device downloads the Workspace ONE Intelligent Hub. Since the device does have access to Google Play, the application file must be hosted on an http/https endpoint within the closed network for download. The latest version of the Workspace ONE Intelligent Hub can be downloaded from the [My Workspace ONE](#) portal.

Creating a QR code for Closed Network Enrollment

See [Generate a QR Code with the Enrollment Configuration Wizard, Android](#) for steps to create the QR code.

To create a QR code for closed-network enrollment, you must:

- 1 Set the **Workspace ONE Intelligent Hub** option to **Hosted on an external URL**.

- 2 Enter the http/https endpoint within the closed network from which the Workspace ONE Intelligent Hub can be downloaded in the URL text box.
- 3 Set **Configure optional Wi-Fi for the device to connect to prior to enrollment** to **None**.

For closed-network deployments, you must manually add the network during out-of-box setup.

Enrolling the device using a QR code

- 1 Power on the device. The setup wizard prompts the user to tap the Welcome screen six times. The taps have to be done in the same place on the screen.

For Android 8.0+ devices, proceed to step 2 in order to download the QR Code reader. For Android 9.0+ devices, the camera will open automatically after you complete the six taps, so you can skip to step 3.

- 2 Connect to Wi-Fi and download a QR code reader by following these steps:

- Select 'Add Network' to manually configure a network.
- Enter the SSID and password of the closed network.
- Under Advanced options, set Proxy as Proxy Auto-Config and enter the http/https URL of the PAC file location.
- Proceed with connecting to the Wi-Fi.
- The device should connect to the Wi-Fi network and skip any connectivity checks to Google.
- The setup wizard automatically downloads a QR code reader. The QR code reader app automatically starts once complete.

- 3 Scan your QR code. If you already connected to Wi-Fi as part of step 2 since you're using an Android 8.x device, skip to step 5.

- 4 Ensure that Wi-Fi details are not included in the QR code. This is covered in the above section titled 'Creating a QR code for closed-network enrollment'. You will be prompted to connect to a network.

- Select 'Add Network' to manually configure a network.
- Enter the SSID and password of the closed network.
- Under Advanced options, set Proxy as Proxy Auto-Config and enter the http/https URL of the PAC file location.
- Proceed with connecting to the Wi-Fi.
- The device should connect to the Wi-Fi network and skip any connectivity checks to Google.

- 5 The setup wizard then automatically downloads the Workspace ONE Intelligent Hub and will begin enrolling the device into Workspace ONE UEM.