



ZENworks 2020 Update 3 Mobile Management Reference

November 2022

Legal Notices

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see (<https://www.microfocus.com/en-us/legal>).

© Copyright 2008 - 2022 Micro Focus or one of its affiliates.

The only warranties for products and services of Micro Focus and its affiliates and licensors (“Micro Focus”) are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Contents

About This Guide	9
Part I Getting Started	11
1 Supported Devices for Mobile Management	13
2 Overview	15
3 ZENworks Mobile Management Workflow Configuration Tasklist	17
4 Feature List	19
5 Using the Getting Started Page	23
Support for the iPadOS platform	23
6 Configuring User Sources	25
6.1 Enabling a User Source for Mobile Device Enrollment	25
6.1.1 Procedure	25
6.2 Configuring the Attribute for ActiveSync Server Authentication	26
7 Configuring an MDM Server	29
7.1 Firewall Configuration	30
7.1.1 Firewall Ports	30
7.1.2 Endpoint URLs	30
7.2 Adding an MDM Server	35
7.2.1 Procedure	35
7.3 Testing the Outbound Capability of MDM Servers	36
7.4 Securing MDM Servers	36
7.5 MDM Servers and APNs Configuration	37
7.6 Removing MDM Servers	37
7.7 Configuring a Default DNS Name	38
7.8 Configuring a Proxy Server	39
8 Enabling Push Notifications	41
8.1 Enabling Push Notifications for iOS Devices	41
8.1.1 Prerequisites	41
8.1.2 Creating and Importing an APNs Certificate	41
8.1.3 Renewing an Expired APNs Certificate	42

9	Creating and Assigning a Mobile Enrollment Policy	43
	Creating a Mobile Enrollment Policy	43
	Editing Mobile Enrollment Policy	45
	Assigning a Mobile Enrollment Policy	45
	Procedure	45
10	Configuring an ActiveSync Server	47
	Connecting to a New ActiveSync Server	47
	Prerequisites	47
	Procedure	47
	Linking a User Source to an ActiveSync Server	49
	Procedure	49
11	Creating and Assigning a Mobile Email Policy	51
	Creating a Mobile Email Policy	51
	Assigning a Mobile Email Policy	53
	Procedure	53
	Part II Enrolling Mobile Devices	55
12	Prerequisites	57
13	Inviting Users to Enroll Devices	59
14	Enrolling iOS Devices	61
	What is a supervised device?	61
	Enrolling devices using the Apple Device Enrollment Program	61
	Linking ZENworks to the Apple Deployment Programs Account	63
	Assigning Devices	64
	Syncing Devices	65
	Viewing DEP Devices	65
	Managing the DEP Profile	67
	Assigning Users	71
	Enrolling a DEP Device	72
	Renewing a DEP Token	72
	Removing a DEP Server	73
	Re-assigning Devices	73
	Enrolling an iOS Device through Apple Configurator	73
	Prerequisites	73
	Procedure	74
	Enrolling an iOS Device Manually	77
15	Enrolling Android Devices	91
	What is Android in the enterprise?	92
	Enrolling the Organization to Android Enterprise	92
	Creating and Assigning Android Enterprise Enrollment Policy	94
	Enrolling Devices in the Work Profile Mode	94

Enrolling Devices in the Work-managed Device Mode	101
Enroll using AFW identifier	101
Enroll using a QR code	108
Enroll Managed Device using a QR code	109
16 Enrolling an Email Only Device	113
17 Allowing Manual Reconciliation by the User	119
18 Viewing Device Information	123
Part III Managing Mobile Devices	127
19 Viewing Device Status	129
20 Securing a Device	131
20.1 Mobile Device Control Policy	131
20.1.1 Creating a Mobile Device Control Policy	131
20.1.2 Editing a Mobile Device Control Policy Setting	132
20.1.3 Assigning a Mobile Device Control Policy	153
20.2 Mobile Security Policy	154
20.2.1 Creating a Mobile Security Policy	154
20.2.2 Editing a Mobile Security Policy Setting	155
20.2.3 Assigning a Mobile Security Policy	164
21 Monitoring Device Compliance	167
Creating and Assigning a Mobile Compliance Policy	167
Viewing the Compliance Dashboard	168
22 Provisioning Applications	169
22.1 Distributing iOS App Store Apps	170
22.1.1 Prerequisites	170
22.1.2 Procedure	170
22.2 Distributing iOS Enterprise Apps	172
22.2.1 Procedure	172
22.3 Distributing VPP Apps	172
22.3.1 Linking ZENworks to the Apple VPP Account	173
22.3.2 Creating VPP Bundles	175
22.3.3 Assigning VPP Bundles	176
22.3.4 Updating VPP License Summary	177
22.3.5 Renewing a VPP Token	177
22.3.6 Revoking App Licenses	178
22.3.7 Deleting VPP Subscription	178
22.4 Distributing iOS Update Bundles	179
22.4.1 Assigning the iOS Update Bundle	180
22.5 Distributing Android Apps	180
22.5.1 Distributing Android Enterprise Apps	180
22.5.2 Updating Android Apps	181

22.6	Distributing Corporate Wi-Fi Settings	182
22.6.1	Creating a Wi-Fi Profile bundle	182
22.6.2	Managing the Wi-Fi Profile Bundle	185
22.7	Assigning Bundles	186
22.7.1	Assigning iOS App Store App, Enterprise, Profile, and Corporate Bundle	186
22.8	Specifying App Configuration Parameters	188
22.8.1	Procedure	188
22.9	Installing a Bundle using a Quick Task	190
22.9.1	Procedure	190
22.10	Viewing Information of Apps Installed on Devices	191
23	Viewing Apps Catalog	193
	Overview of the Apps Catalog Page	193
	Editing App Permissions	195
24	Refreshing a Device	197
	Initiating a Scheduled Refresh	197
	Timed Refresh	198
	Manually Triggered Refresh	198
	Refresh Device Quick Task	198
	Refresh Device on the User Portal or the ZENworks App	199
25	Collecting Mobile Device Inventory	201
	Mobile Inventory Scan	201
	Viewing Mobile Inventory	202
	Viewing Standard Reports for Mobile Devices	203
	Creating Custom Reports for Mobile Devices	203
26	Initiating Quick Tasks	205
	Refresh Device	205
	Install Bundle	205
	Procedure	206
	Reboot or Shutdown Devices	206
	Lock Device and Unlock Device	206
	Locking a Device	206
	Unlocking a Device	207
	Unenrolling a Device	207
	Send Message	207
	Procedure	208
27	Bypassing Activation Lock	209
	Enabling Activation Lock Bypass	209
	Disabling Activation Lock Bypass	209
	Retrieving the Activation Lock Bypass Code	210
	Viewing the Activation Lock Bypass Code in ZCC	210
	Exporting the Activation Lock Bypass Code	210
	Activating the Device Using the Activation Lock Bypass Code	211

28 Locating a Device	213
Prerequisites	213
Procedure	214
Notifying Users of Device Location	214
29 Enabling Factory Reset Protection on Android Work-Managed Devices	215
Specifying corporate accounts to provision devices	215
Wiping Factory Reset Protection Data	216
30 Protecting Intune Apps	217
30.1 Prerequisites	217
30.2 Configuring Microsoft Graph API	218
30.2.1 Application Registration	218
30.2.2 Access Token	219
30.2.3 User Association	220
30.3 Policy Sync Schedule	220
30.4 Creating the App Protection Policy	221
30.4.1 Creating iOS Intune App Protection Policy	221
30.4.2 Creating Android Intune App Protection Policy	222
30.5 Editing the App Protection Policy Settings	223
30.5.1 Procedure	223
30.5.2 Publishing the App Protection Policy	232
30.6 Assigning the App Protection Policy	233
30.6.1 Procedure	233
30.7 Disabling or Enabling the App Protection Policy	233
30.8 Viewing and Wiping Intune Protected Apps	234
31 Managing Email Notifications	237
32 Unenrolling Devices	239
Procedure	239
33 Unenrolling the Organization from Android Enterprise	241
Unenrolling the Organization	241
A Best Practices	243
Migrating to Apple Business Manager	243
Best Practices	243
Troubleshooting Scenarios	244

About This Guide

This *Mobile Management Reference* includes information to help you successfully use the Mobile Management feature within ZENworks Configuration Management.

The information in this guide is organized as follows:

- ♦ [Part I, “Getting Started,” on page 11](#)
- ♦ [Part II, “Enrolling Mobile Devices,” on page 55](#)
- ♦ [Part III, “Managing Mobile Devices,” on page 127](#)
- ♦ [Appendix A, “Best Practices,” on page 243](#)

Audience

This guide is intended for ZENworks administrators and end users.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation.

Additional Documentation

ZENworks 2020 is supported by other documentation (in both PDF and HTML formats) that you can use to learn about and implement the product. For additional documentation, see the [Online Documentation](#) site.

Getting Started

The following sections provide information on how to get started with the Mobile Management feature in ZENworks Configuration Management. You should already have installed your ZENworks system. If not, see the *ZENworks Server Installation*.

- ◆ Chapter 1, “Supported Devices for Mobile Management,” on page 13
- ◆ Chapter 2, “Overview,” on page 15
- ◆ Chapter 3, “ZENworks Mobile Management Workflow Configuration Tasklist,” on page 17
- ◆ Chapter 4, “Feature List,” on page 19
- ◆ Chapter 5, “Using the Getting Started Page,” on page 23
- ◆ Chapter 6, “Configuring User Sources,” on page 25
- ◆ Chapter 7, “Configuring an MDM Server,” on page 29
- ◆ Chapter 8, “Enabling Push Notifications,” on page 41
- ◆ Chapter 9, “Creating and Assigning a Mobile Enrollment Policy,” on page 43
- ◆ Chapter 10, “Configuring an ActiveSync Server,” on page 47
- ◆ Chapter 11, “Creating and Assigning a Mobile Email Policy,” on page 51

1 Supported Devices for Mobile Management

Mobile Management capabilities are supported on the following devices:

Device	Functionality
Android 5.0 or newer (Work Profile enrollment)	<ul style="list-style-type: none"> ◆ Security Policy Enforcement
Android 6.0 or newer (Work-managed device enrollment)	<ul style="list-style-type: none"> ◆ Device Control Policy Enforcement ◆ Email synchronization for Exchange ActiveSync accounts ◆ Device Management: Refresh Device, Send Message, Lock Device, Unlock Device, locating the device and Unenroll (Full Wipe and Selective Wipe) ◆ Remote configuration and installation of apps through bundles ◆ Enrollment as work profile mode, work-managed device mode. <p data-bbox="865 1003 1453 1066">The ZENworks Agent app installed on Android devices enables in managing these devices.</p>
iOS version 10.x and newer	<ul style="list-style-type: none"> ◆ Security Policy Enforcement ◆ Device Control Policy Enforcement ◆ Remote configuration and email synchronization of Exchange ActiveSync accounts ◆ Installation of Apps through bundles ◆ Installation of Configuration Profile ◆ Managing Intune Apps (enrollment is not required to use this feature) ◆ Subscription to Apple Volume Purchase Program ◆ Enrollment through the Apple Device Enrollment Program ◆ Enrollment using Apple Configurator ◆ Device Management: Refresh Device, Lock Device, Unlock Device, enabling lost mode, locating the device, reboot/shutdown of the device, enabling activation lock bypass and Unenroll (Full Wipe and Selective Wipe) <p data-bbox="865 1759 1453 1822">The MDM profile installed on iOS devices enables in managing these devices.</p>

Device	Functionality
Devices using Exchange ActiveSync version 12.1 and newer	<ul style="list-style-type: none"> ◆ Email synchronization for Exchange ActiveSync accounts ◆ Security Policy Enforcement ◆ Device Control Policy Enforcement ◆ Device Management: Unenroll Device (Full Wipe) ◆ ActiveSync enrollment for the following device platform is also included: <ul style="list-style-type: none"> ◆ Windows version and newer
Apple TV (Experimental)	<p>The following features are supported on Apple TV on an experimental basis and should be used for evaluation purposes only:</p> <ul style="list-style-type: none"> ◆ Enrollment of Apple TV devices using the Apple Device Enrollment Program ◆ Assignment of iOS profile bundles to Apple TV devices. <p>We do not support deployment of these features in a production environment. Technical support will not be provided for any issues reported on these features.</p>

2 Overview

Mobile device management helps you to secure and manage any corporate or employee-owned mobile devices that are being used in the workplace. Mobile management in ZENworks uses the capabilities of ZENworks Configuration Management, which is the same management console and system infrastructure that has been managing laptops, desktops and servers over the years. By leveraging the features of ZENworks, you can perform multiple management operations on mobile devices:

- ♦ **Enroll (register) mobile devices** to your ZENworks Management Zone. Users can enroll their devices as:
 - ♦ **Fully Managed:** Android, iOS devices are supported. Full management of an Android device is enabled using the ZENworks Agent App that is installed on the device. Full management of an iOS device is enabled using the MDM profile that is installed on the device.
 - ♦ **Email Only:** Devices with native Exchange ActiveSync capabilities are supported, that is, iOS, Android, and Windows devices.
- ♦ **Manage Android devices using Android enterprise** that lets you securely manage corporate data by enrolling devices in the work profile or work-managed device mode.
- ♦ **Utilize Apple Device Enrollment Program (DEP) and Apple Configurator** to streamline deployment of multiple corporate owned iOS devices.
- ♦ **Enforce security and mobile control policies** on Fully Managed (Android, iOS, devices) and Email-only (that include Windows devices) devices. With a security policy, you can set password restrictions, inactivity timeout, and enforce encryption on the device. With a device control policy, you can control the use of applications such as the device camera, voice assistant, web browser, and other applications installed on the device.
- ♦ **Distribute and manage Apple VPP apps** on Fully Managed iOS devices purchased with your organization's Volume Purchase Program (VPP) account, by using the existing Bundles and Subscription workflow in ZENworks.
- ♦ **Synchronize email** from ActiveSync servers on Fully Managed (Android, iOS,) and Email-only devices (that include Windows devices). You can also remotely configure the default email client on iOS devices.
- ♦ **Support for Direct Boot** is also included for Android 7.0+ devices. This feature enables the ZENworks Agent to always be active on an Android device even before the device is unlocked after a reboot. Administrators can enforce policies such as the Compliance policy, remove the Work Profile or factory reset the device, even if the device has not been unlocked.
- ♦ **Secure apps that use the Intune SDK** without the users having to enroll their devices ZENworks Management Zone.

For more information on the complete set of features supported by ZENworks, see [Feature List](#).

3 ZENworks Mobile Management Workflow Configuration Tasklist

To use the Mobile Management feature, refer to the following workflow in the order of the listed tasks:

Task	Details
<input type="checkbox"/> Review concepts essential to understand the Mobile Management feature.	For information, see “Overview” on page 15.
<input type="checkbox"/> Configure a user source in the ZENworks Management Zone.	For instructions, see “Configuring User Sources” on page 25.
<input type="checkbox"/> Configure an MDM Server to enable communication with mobile devices.	For instructions, see “Configuring an MDM Server” on page 29.
<input type="checkbox"/> Enable push notifications on Android, iOS devices.	For instructions, see “Enabling Push Notifications” on page 41.
<input type="checkbox"/> (Optional) Configure a proxy server for all mobile management related communication.	For instructions, see “Configuring an MDM Server” on page 29.
<input type="checkbox"/> Configure and manage email access on mobile devices by configuring an ActiveSync Server and by creating and assigning a Mobile Email Policy.	For instructions, see “Configuring an ActiveSync Server” on page 47.
<input type="checkbox"/> Create and assign an enrollment policy.	For instructions, see “Enrolling Mobile Devices” on page 55.
<input type="checkbox"/> Create and assign device control and mobile security policies to secure the mobile devices.	For instructions, see “Securing a Device” on page 131.
<input type="checkbox"/> Provision and manage apps on iOS and Android devices.	For instructions, see “Provisioning Applications” on page 169.
<input type="checkbox"/> Manage and maintain mobile devices in the ZENworks Management Zone.	For instructions, see “Managing Mobile Devices” on page 127.

4 Feature List

Based on the platform, that is iOS, and Android devices that are enrolled as fully managed devices, ZENworks Configuration Management supports the following features as a part of managing mobile devices:



Feature	Platform		Details
	iOS	Android	
Enrollment of Android devices in the work profile and work-managed device modes (Android in the enterprise).		✓	For more information, see Enrolling Mobile Devices .
Enrollment of iOS devices using Apple Device Enrollment Program	✓		For more information, see Enrolling Mobile Devices .
Enrollment of iOS devices using Apple Configurator	✓		For more information, see Enrolling Mobile Devices .
Setting up and managing ActiveSync email account	✓	✓	For more information, see Configuring an ActiveSync Server .
Provisioning of work apps from managed Google Play using Android in the enterprise		✓	For more information, see Provisioning Applications .
Provisioning of VPP apps	✓		For more information, see Provisioning Applications .
Provisioning of Apple App Store Apps	✓		For more information, see Provisioning Applications .
Provisioning of Configuration Profiles	✓		For more information, see Provisioning Applications .
Provisioning custom in-house apps	✓		For more information, see Provisioning Applications .
Provisioning Wi-Fi configuration settings	✓	✓	For more information, see Provisioning Applications .


Feature	Platform		Details
	iOS	Android	
Pre-configuring App Parameters.	✓	✓	For more information, see Specifying App Configuration Parameters For iOS , this feature is applicable for only, App Store, Enterprise, and VPP bundles.
Applying Password, Encryption and Device Inactivity restrictions	✓	✓	For more information, see Securing a Device .
Placing restrictions on specific features of the device	✓	✓	For more information, see Securing a Device .
Enabling factory reset protection		✓	For more information, see Enabling Factory Reset Protection on Android Work-Managed Devices .
Protecting Intune Apps	✓		For more information, see Enabling Factory Reset Protection on Android Work-Managed Devices .
Bypassing Activation Lock Code	✓		For more information, see Bypassing Activation Lock .
Direct Boot Support		✓	This feature is supported from Android 7.0+ devices. If any compliance or unenroll actions are initiated on a device, then these actions will be applied even before the device is unlocked after a reboot.
Collecting hardware and software inventory details of a device	✓	✓	For more information, see Collecting Mobile Device Inventory .
Monitoring compliance of a device.		✓	For more information, see Monitoring Device Compliance .
Locating a Device	✓	✓	For more information, see Locating a Device .
Locking a Device	✓	✓	For more information, see Initiating Quick Tasks .

Feature	Platform		Details
	iOS	Android	
Unlocking a Device	✓	✓	For more information, see Initiating Quick Tasks .
Enabling Lost Mode	✓		For more information, see Initiating Quick Tasks .
Rebooting a device	✓	✓	For more information, see Initiating Quick Tasks .
Shutting down a device	✓		For more information, see Initiating Quick Tasks .

5 Using the Getting Started Page

The Getting Started with Modern Management page enables you to setup the zone and complete certain pre-configuration activities required to enroll Windows 10 MDM devices, Android devices and iOS/iPadOS devices. Subsequently, tasks required to successfully manage these enrolled devices are also displayed on this page.

To access the **Getting Started** page, in ZCC, click (in the left navigation pane). Each configuration task on this page includes an icon with a  or  mark indicating its completion status and one or more links to the page where you complete the task.

Additionally, you can click the Help  icon appearing against each task or the **Help** link provided at the top right corner of each page for information on the task.

For more information on the Managing Windows 10 Devices, Managing Android Devices, and Managing iOS/iPadOS devices section, see [ZENworks Modern Management](#)

Prior to using the Modern Management feature, ensure that the following requirement is met:

- ♦ **Install and Configure ZENworks:** The Modern Management feature is integrated with ZENworks Configuration Management. To install and configure ZENworks Configuration Management, see [ZENworks Server Installation](#).

Support for the iPadOS platform

From the 2020 Update 1 release onwards, ZENworks supports the iPadOS platform, that is, iPad devices with iOS version 13 or a later version installed on them. All settings that are applicable for iOS devices are now applicable for iPadOS devices as well.

This feature is by default in a disabled state and needs to be enabled after migrating to the ZENworks 2020 Update 1 release version. To enable the iPadOS platform, you need to run the following `zman` command from the command prompt:

zman feature-enable-platform-ipados (zman fepi): On executing this command:

- ♦ All existing iPad devices with iOS 13 or a later version, move from the iOS dynamic group to the iPadOS dynamic group. Any existing assignments that were applied to the moved devices as part of the iOS dynamic group, will no longer be applicable. You need to manually re-create these assignments for the iPadOS dynamic group.
- ♦ iPadOS devices will no longer be part of the existing enrollment rules that were applied to iOS devices. You need to re-create these enrollment rules for iPadOS devices. For more information on enrollment rules, see [Creating and Assigning a Mobile Enrollment Policy](#).

After executing the `zman fepi` command, you need to refresh all iPadOS devices that are already enrolled in the zone. Also, to view the devices in the iPadOS Dynamic Group immediately, you need to recalculate group members either by clicking Recalculate Group Members displayed in the left pane under Group Tasks in ZCC or by executing the `zman dgr` command.

6 Configuring User Sources

User-based management is an important facet of modern management in ZENworks. A device that is enrolled (registered) to the ZENworks zone must have a user associated with it. Therefore, for users to enroll their mobile devices, a user source must be configured in ZENworks and this user source must be configured to support mobile device enrollment. A user source is an LDAP directory that contains the user accounts of users to whom you want to distribute ZENworks content, in order to manage their devices. While configuring a user source you must define the enrollment options, which will be applied while enrolling the device, for example; you can enroll a device with or without providing the registration domain.

This chapter explains how a user source that you have already configured in ZENworks can be enabled for mobile device enrollment. For more information on adding a user source, see [ZENworks User Source and Authentication Reference](#).

- [Section 6.1, “Enabling a User Source for Mobile Device Enrollment,” on page 25](#)
- [Section 6.2, “Configuring the Attribute for ActiveSync Server Authentication,” on page 26](#)

6.1 Enabling a User Source for Mobile Device Enrollment

6.1.1 Procedure

- 1 In ZENworks Control Center, click **Users** (in the left navigation pane) to display the list of User Sources.
- 2 Next to the user source, click **Details** to display its property pages.
- 3 In the Summary tab, do one of the following:

Allow simple enrollment: Simple enrollment removes the domain requirement and enables users to enroll devices by providing only their user name.

Simple enrollment is allowed for only one user source. To allow simple enrollment, next to the **Simple Enrollment** field click **Yes**. After you enable simple enrollment for one user source, it is not available for any other user source. Also, if you change this setting from one user source to another, then you might have to re-configure the email accounts, as it might not work properly.

NOTE: If you are configuring a user source for the first time, then simple enrollment will be enabled by default.

Domain Alias: As simple enrollment is allowed for only one user source, if you have multiple user sources in the zone, you can authenticate the user by providing the domain alias, specified in this setting. To edit the default domain alias, click **Edit**, specify the domain name and then click **OK**.

NOTE: The domain name is pre-populated as soon as you add a user source.

You can decide what to use as your domain name. For example, you can use your organization's name, your organization's domain name, or your ActiveSync server domain name (if applicable). Since users need to supply the domain name on their mobile devices, it is recommended that you make it as easy as possible for them to remember and type. The following are valid domain name examples: `mycompany`, `mycompany.com`. You should avoid using `ZENworks_Default` as the domain name.

NOTE: If a configured user source is deleted and the same user source is configured again, then all those mobile devices that were enrolled using the earlier user source, would have to be re-enrolled to the ZENworks Management Zone. However, before re-enrolling these devices ensure that the respective device objects are deleted from ZCC.

6.2 Configuring the Attribute for ActiveSync Server Authentication

While configuring an email account on a device by using a Mobile Email Policy, the user is automatically authenticated to the ActiveSync Server that is configured in the zone. ZENworks initially obtains the user credentials (such as the user's Email ID) from the associated user source (LDAP directory configured in the zone) and using these credentials the user is authenticated to the ActiveSync Server to which the user belongs. The user is logged in to the email account, if the credentials provided in the user source match with the ones configured in the ActiveSync Server. However, the user credentials with which the user logs into the ActiveSync Server to retrieve emails might be different from the credentials that he/she uses to login to the LDAP directory. In such cases, you can define the LDAP attribute that ZENworks must query and use as the user name while retrieving emails from the ActiveSync Server.

For example: consider that the configured LDAP directory is the NetIQ eDirectory and the email application is GroupWise. The default attribute that is used to authenticate a user to GroupWise is the **Mail** attribute. The preferred email address of a user published in the NetIQ eDirectory is in the format *first name.last name@domain.com*, due to which authentication to GroupWise might fail. In this scenario, you can edit the **ActiveSync Logon Attribute** and select **UniqueID**, which can be the user name of the GroupWise user.

The default attribute is **Mail** but you can modify this attribute. You can define attributes for a specific user or for a user folder. These attributes differ based on the LDAP directory configured in the zone.

To edit the attribute:

- 1 Navigate to **Users** on the left pane in ZCC.
- 2 Click a User Source Folder or drill down to a specific user. Click **Details** next to the User Source Folder or the User.
- 3 Click **Edit** next to the **ActiveSync Server Logon Attribute**.

The various attributes that can be defined are:

- ♦ **NetIQ eDirectory:** If the NetIQ eDirectory is configured in the zone, then you can define the following attributes to authenticate to the ActiveSync Server:
 - ♦ **CN:** The common name of the user.
 - ♦ **Mail:** The email address of the user.

- ♦ **UniqueID:** The unique user identifier.
- ♦ **Other:** Specify the custom attribute defined in the configured LDAP directory.
- ♦ **Active Directory:** If Active Directory is configured in the zone, then you can define the following attributes to authenticate to the ActiveSync Server:
 - ♦ **UserPrincipalName:** An Internet-style login name for a user based on the Internet standard RFC 822.
 - ♦ **sAMAccountName:** The logon name used to support clients and servers running earlier versions of the operating system, such as Windows NT 4.0, Windows 95, Windows 98, and LAN Manager.
 - ♦ **Mail:** The email address of the user.
 - ♦ **Other:** Specify the custom attribute defined in the configured LDAP directory.

For either of these LDAP directories, you can also select **Inherited**, to inherit the attribute defined at the user folder level.

If you modify these settings and if the assigned Mobile Email Policy does not use the ZENworks Server as the proxy server, then you need to republish or reassign the Mobile Email Policy. The modified settings are automatically applied on the email accounts configured with Mobile Email Policies that use the ZENworks Server as the proxy server.

7 Configuring an MDM Server

An MDM Server is a ZENworks Primary Server with an *MDM* role, that acts as a gateway server and is the sole access point for managing mobile devices. To ensure that the ZENworks Server and the enrolled mobile devices can communicate with each other at all times, an MDM role must be assigned to at least one Primary Server in the zone. Apart from allowing devices to contact ZENworks, MDM Servers allow ZENworks to establish outbound connections to perform activities such as contact the push notification server to send relevant notifications to devices and manage VPP subscriptions. If the outbound connection is initiated from ZENworks Control Center (ZCC) whose ZENworks Server does not have outbound access, then this server will route these requests through one of the MDM Servers.

IMPORTANT: If the MDM Server is in the DMZ, then you need to ensure that the MDM Server is able to access the ZooKeeper service on port 6789. If the MDM Server is unable to access the ZooKeeper service, then some mobile management features might not work as expected. For more information on the ZooKeeper service, see [ZENworks Primary Server and Satellite Reference](#).

If you plan to use a Primary Server as an MDM server, to ensure communication with iOS, and Mac devices, you need to ensure that the issued certificate meets the following criteria:

- ◆ Validity of the certificate does not exceed 2 years.
- ◆ Alternate DNS name is specified in the certificate.
- ◆ EKU (Extended Key Usage) value is specified as Server Authentication.
- ◆ Key Size should be at least 2048 bits.
- ◆ Signature hash algorithm should be from the SHA-2 family.

NOTE: If there are multiple MDM Servers in the zone, all these would be used for outbound connections, but inbound connections will be limited to those servers to which devices have enrolled.

For more information on reminding the MDM Server Certificate, see [ZENworks SSL Management Reference](#).

- ◆ [Section 7.1, “Firewall Configuration,” on page 30](#)
- ◆ [Section 7.2, “Adding an MDM Server,” on page 35](#)
- ◆ [Section 7.3, “Testing the Outbound Capability of MDM Servers,” on page 36](#)
- ◆ [Section 7.4, “Securing MDM Servers,” on page 36](#)
- ◆ [Section 7.5, “MDM Servers and APNs Configuration,” on page 37](#)
- ◆ [Section 7.6, “Removing MDM Servers,” on page 37](#)
- ◆ [Section 7.7, “Configuring a Default DNS Name,” on page 38](#)
- ◆ [Section 7.8, “Configuring a Proxy Server,” on page 39](#)

7.1 Firewall Configuration

Typically, MDM Servers must reside in the DMZ thereby allowing mobile devices to make inbound connections even when they are outside the firewall. Like other external-facing servers, the ZENworks MDM Server faces the Internet from within the DMZ. This lets the enterprise firewall protect the MDM Server from external attacks.

7.1.1 Firewall Ports

To enable both internal and external access to the MDM server, certain firewall ports must be open. The ZENworks MDM Server accepts most inbound connections using HTTPS on port 443.

Apple Push Notification service: Both the MDM server and the iOS clients communicate with each other using the Apple Push Notification service (APNs). For outbound connections, the MDM server uses ports 443 and 2197 to Apple's 17.0.0.0/8 block. Port 5223 must be open in the firewall to enable mobile devices to connect to the APNs server, so that the APNs can send messages to these mobile devices that are within your network.

Firebase Cloud Messaging: Both the MDM server and the Android clients communicate with each other using the Firebase Cloud Messaging (FCM) service. For outbound connections, open port 443 to connect to the FCM service from the MDM Server as well as the Android clients. For mobile devices that are within your network, to receive messages, FCM typically uses port 5228, but it sometimes uses 5229 and 5230.

A detailed list of the ports to be enabled for each ZENworks feature is provided in the next section.

7.1.2 Endpoint URLs

The MDM Server and the end-user devices must be able to reach certain endpoints to access apps and services. The endpoint URLs are listed below:

Apple

Feature	URL	Port	Additional Information
Server Connections			
Apple Push Notification Service See Enabling Push Notifications for iOS Devices	https://api.push.apple.com/ www.novell.com	TCP 443/ 2197	

Feature	URL	Port	Additional Information
Apple Device Enrollment Program See Enrolling devices using the Apple Device Enrollment Program .	https://mdmenrollment.apple.com/session	HTTP/HTTPS 443	
Apple Volume Purchase Program See Distributing VPP Apps	https://vpp.itunes.apple.com/WebObjects/MZFinance.woa/wa/VPPServiceConfigSrv	HTTP/HTTPS 443	This is a static URL based on which the dynamic URLs to perform specific VPP operations can be retrieved.
iOS App Store App Bundle See Distributing iOS App Store Apps	https://itunes.apple.com	HTTP/HTTPS 443	App Store apps

Device Connections

Apple Push Notification Service See Enabling Push Notifications	courier.push.apple.com(17.0.0.0/8)	TCP 5223 and 443	
--	---	------------------	--

Android

Feature	URL	Port	Additional Information
Server Connections			
Firebase Cloud Messaging See Enabling Push Notifications	https://fcm.googleapis.com/fcm	TCP Port 443, 5228-5230	

Feature	URL	Port	Additional Information
Android Enterprise See Enrolling Android Devices	https:// www.googleapis.com	TCP 443	Used to invoke the Google EMM API in the ZENloader and ZENserver services.
	play.google.com www.google.com	TCP 443	Google Play Store Play Enterprise re-enroll
	fonts.googleapis.com *.gstatic.com	TCP 443	Google fonts User Generated Content (e.g. app icons in the store)
	accounts.google.com accounts.google.com.*	TCP 443	Account Authentication Country-specific account auth domains
	crl.pki.goog ocsp.pki.goog	TCP 443	Certificate Validation
	apis.google.com ajax.googleapis.com	TCP 443	GCM, other Google web services, and iFrame JS
	clients1.google.com payments.google.com google.com	TCP 443	App approval
	notifications.google.com	TCP 443	Desktop/Mobile Notifications
Device Connections			
Firebase Cloud Messaging See Enabling Push Notifications	fcm.googleapis.com fcm-xmpp.googleapis.com	TCP/443,5228-5230	Firebase Cloud Messaging (Find My Device, EMM Console -DPC communication, like pushing configs)
	fcm-xmpp.googleapis.com	TCP/5235,5236	When using persistent bidirectional XMPP connection to FCM server.

Feature	URL	Port	Additional Information
Android Enterprise See Enrolling Android Devices	play.google.com	TCP 443	Google Play and updates
	android.com	TCP,UDP/5228-5230	gstatic.com,googleusercontent.com - contains User Generated Content (e.g. app icons in the store). *gvt1.com, *.ggpht, dl.google.com, dl-ssl.google.com, android.clients.google.com- Download apps and updates, Play Store APIs gvt2.com and gvt3.com are used for Play connectivity monitoring for diagnostics.
	google-analytics.com		
	googleusercontent.com		
	*gstatic.com		
	*gvt1.com		
*.ggpht.com			
dl.google.com			
dl-ssl.google.com			
android.clients.google.com			
*gvt2.com			
*gvt3.com			
	*.googleapis.com	TCP 443	EMM/Google APIs/PlayStore APIs
	accounts.google.com	TCP 443	Authentication
	accounts.google.[country]		For accounts.google.[country], use your local top-level domain for [country]. For example, for Australia use accounts.google.com.au, and for United Kingdom use accounts.google.co.uk.
	pki.google.com	TCP 443	Certificate Revocation list checks for Google-issued certificates
	clients1.google.com		
	clients2.google.com	TCP 443	Domains shared by various Google backend services such as crash reporting, Chrome Bookmark Sync, time sync (tlsdate), and many others.
	clients3.google.com		
	clients4.google.com		
	clients5.google.com		
	clients6.google.com		
	omahaproxy.appspot.com	TCP 443	Chrome updates.

Intune

Feature	URL	Port	Additional Information
Intune App Protection See Protecting Intune Apps	https://login.microsoftonline.com/	HTTP/HTTPS (443)	Get Microsoft Graph API configuration details
	https://graph.microsoft.com/v1.0/deviceAppManagement/androidManagedAppProtections	HTTP/HTTPS (443)	Test the validity of the access token.
	https://graph.microsoft.com/v1.0/deviceAppManagement/managedAppStatuses/managedAppList	HTTP/HTTPS (443)	List all the apps while creating the Intune App Protection policy.
	https://graph.microsoft.com/beta/deviceAppManagement/iosManagedAppProtections	HTTP/HTTPS (443)	Create and assign the iOS Intune App Protection policy.
	https://graph.microsoft.com/beta/deviceAppManagement/androidManagedAppProtections	HTTP/HTTPS (443)	Create and assign the Android Intune App Protection policy.
	https://graph.microsoft.com/v1.0/groups	HTTP/HTTPS (443)	Lists the groups present in Azure.
	https://graph.microsoft.com/v1.0/users	HTTP/HTTPS (443)	Lists the users present in Azure.
	https://graph.microsoft.com/v1.0/users/{AZURE_USER_GUID}/wipeManagedAppRegistrationsByDeviceTag	HTTP/HTTPS (443)	For the wipe action.

Feature	URL	Port	Additional Information
	https://graph.microsoft.com/v1.0/users/{AZURE_USER_GUID}/managedAppRegistrations	HTTP/HTTPS (443)	Lists the registered apps on the user's device.
	https://graph.microsoft.com/v1.0/deviceAppManagement	HTTP/HTTPS (443)	Obtain the wipe status of the device.
	https://graph.microsoft.com/v1.0/organization/	HTTP/HTTPS (443)	URL to get tenant name from the tenant ID

7.2 Adding an MDM Server

Adding an MDM Server indicates that an MDM role is assigned to one of the Primary Servers. One or more Primary Servers can be added as MDM Servers. The number of MDM Servers would depend on the scalability needs and configuration. Before adding an MDM Server ensure that the following prerequisites are met:

- ◆ All MDM Servers must have inbound and outbound connectivity. Inbound connectivity means that an MDM Server must be able to receive requests from outside the organization's firewall (in this case the mobile devices). Outbound connectivity means that an MDM Server must successfully be able to make connections outside the organization's firewall. ZENworks will not verify this while adding an MDM Server or during any operation involving the MDM Server.
- ◆ You also need to ensure that all Primary Servers in your zone have the ZENworks 2020 version or newer deployed on it.

The Apple Push Notification service (APNs) and Firebase Cloud Messaging (FCM) can be configured only if an MDM role is assigned to one or more Primary Servers.

7.2.1 Procedure

- 1 On the Getting Started with Mobile Management page, click **Add MDM Server**. Alternatively, from the left hand side navigation pane of ZCC, navigate to **Configuration > Infrastructure Management > MDM Servers**.
- 2 Click **Add**.
- 3 Select one or more Primary Servers that need to be configured with the MDM role and click **OK**.


7.3 Testing the Outbound Capability of MDM Servers

After adding an MDM Server, you can test its outbound connectivity by clicking **Test Certificate** while configuring the Apple Push Notifications service (APNs) or by clicking **Test API Key** while configuring Firebase Cloud Messaging (FCM). If the configuration is valid, both these options will test the connection to the APNs and GCM servers from each of the MDM Servers. If the connectivity fails from one or more MDM Servers, the failed servers would be listed. You can perform these actions in the respective push notifications configuration sections of ZCC. For details, see [Enabling Push Notifications](#).


NOTE: If any ZCC operation involving an MDM Server fails, check the `zcc.log`, `services-messages.log`, and the `loader-messages.log`.

7.4 Securing MDM Servers


Since MDM Servers are exposed to the Internet at all times, it becomes important to secure access to the services on these servers. The services are categorized into Administration, Endpoint, and the ZENworks Setup page. ZENworks allows you to control access to each of these categories by clicking any of the following icons appearing against a configured MDM server:


- ◆ **Administration Access:** Click  to allow or deny specific IP addresses from accessing Administration functions such as ZCC, ZMAN and so on.

NOTE: You need to ensure that administration access is not denied for all or else ZCC will remain inaccessible, except from the MDM server in which the access was allowed or denied. Ensure that all Primary Servers in your zone are allowed access so that the internal operations between these servers are not restricted. However, these filters are not applicable for an Appliance web console.

- ◆ **Endpoint Access:** Click  to allow or deny certain IP addresses from accessing endpoint functions such as the ZENworks User Portal, the ZENworks Agent app and so on.

NOTE: Ensure that all Primary Servers in your zone are allowed access so that the internal operations between the ZENworks Servers will not be restricted.

- ◆ **Tools Access:** Click  to allow or deny certain IP addresses from accessing tools and downloads through the ZENworks Setup URL.

For each of these categories, you can configure filters by clicking . By default, access is allowed for all devices. For each filter, you need to specify the following:

- ◆ Specific IP address, comma separated IP addresses, or an IP range. Each IP address can be specified in CIDR format or the regular format.
- ◆ **Allow** or **Deny** access to the specified IP address
- ◆ A short description about the specified set of IP addresses.

Filters are evaluated in the order in which they are listed. If the same IP address appears in multiple filters, then the type of access specified in the first filter is given precedence over the type of access specified in the second filter. For example: The IP address 10.0.0.1 specified in the first filter is

denied administration access. However, if the same IP address, appearing as a part of an IP range (10.0.0.0 - 10.255.255.255) that is specified in the second filter, is allowed administration access, then precedence is given to the first filter and IP address 10.0.0.1 will be denied administration access. You can also look up an IP address to identify whether access is allowed or denied for it, by specifying it in the **Test access for an IP** field. This action is also performed based on the order in which the filters are listed.

After configuring the access controls for one server, you can replicate the same access control configuration in another server. To do this, you need to select the MDM Server for which the access controls are already configured. Subsequently, click **Copy Access Controls**. In the Copy Access Controls window, select the access controls that you want to copy and **Add** the server to which these access controls need to be copied.

NOTE: Configuring access controls for an MDM Server that is an Appliance does not secure the Appliance Administration Console. To secure it, you need to specify access restrictions in the Appliance Administration Console itself. For details, see [ZENworks Appliance Deployment and Administration Reference](#).

If a device's IP address is denied access but the device is still able to contact the ZENworks Server, then you need to check whether the device is communicating with ZENworks using the proxy server. In this case, you need to deny access to the proxy server's IP address, if you are sure that no other devices are using this proxy server.

7.5 MDM Servers and APNs Configuration

The Apple Push Notification service (APNs) configuration consists of the APNs keystore, which contains the Apple-signed certificate that is required to send push notifications to iOS devices. The APNs keystore is first created on one of the MDM Servers when the first APNs Certificate Signing Request (CSR) is created. When you import the Apple-signed certificate, it is first imported to this keystore and then replicated to the other MDM Servers in the zone, if any. Whenever a new certificate is imported, it would be imported into one of the MDM Servers and is subsequently replicated to other MDM servers in the zone. If MDM Servers are added or removed after APNs is configured or if the APNs configuration has changed, the latest configuration will be replicated on all the MDM Servers in your zone.

When the last MDM Server in the zone is removed, then the APNs configuration will be deleted entirely.

7.6 Removing MDM Servers

If you want to remove a Primary Server that is designated as the MDM Server in your zone, then you must first remove the MDM role from this Primary Server.

IMPORTANT: Ensure that you do not delete all the MDM servers in your zone, as at least one MDM server is required for ZENworks to manage mobile devices. If you need to remove the last MDM server in your zone, then before removing the server ensure that you delete the Android Enterprise subscription from the zone.

To remove the role, you need to:

- 1 Click **Configuration** on the left hand side navigation pane in ZCC.
- 2 Click **Infrastructure Management > MDM Servers**.
- 3 Select one or more MDM Servers and click **Remove**.

NOTE: If you have removed an MDM role from a server, then you can add it back to the same server only after 30 minutes from the time the role was removed, as the cleanup action to remove the MDM role might take up to 30 minutes to complete.

Since mobile devices contact the MDM Server to which they are enrolled and if mobile devices are enrolled to a server that you have chosen to remove from the zone, then you will have to re-enroll these mobile devices to the zone using another MDM Server. Before re-enrollment, ensure that you delete the corresponding device objects in ZCC. However, if you are upgrading or replacing the MDM Server with another server, then the enrolled devices will automatically reconcile with the replaced server.

7.7 Configuring a Default DNS Name

If an MDM Server can be contacted using multiple DNS names, then you can specify the default DNS name that mobile devices will use to communicate with the MDM Server. To set the default DNS name, select the Primary Server that has the MDM role assigned and navigate to **Settings > Infrastructure Management > Default DNS Name**. You can select the default DNS name from the drop-down list displayed on this page.

ZENworks detects all the network interfaces that are attached to the MDM Server with the corresponding DNS names. The drop-down lists the DNS names along with the Additional DNS Names configured for the Primary Server.

If the default DNS name is modified, then you might have to remind the Primary Server certificate so that the newly configured DNS name is also part of the server certificate that mobile devices will use while enrolling to the zone.

IMPORTANT: Before a certificate remind, ensure that you include all the DNS names in the **Additional DNS Name** settings in ZCC (**Configuration > Management Zone Settings > Infrastructure Management > Additional DNS Names**).

Also, if mobile devices are enrolled to this Primary Server, re-enroll these devices if the previously configured DNS name is not reachable anymore. You might have to re-publish any assigned Mobile Email Policies so that the new DNS name setting takes effect.

7.8 Configuring a Proxy Server

You can define an HTTP Proxy Server to enable MDM Servers to connect to the Internet through the proxy server. These proxy servers can be used by the MDM Servers to contact the APNs Server, FCM Server, and managed mobile devices. To configure a proxy server, navigate to **Configuration > Management Zone Settings > Infrastructure Management > HTTP Proxy Settings > HTTP Proxy Settings for MDM Servers**.

- ◆ **Proxy Host:** Specify the IP address of the Proxy Server.

NOTE: As Apple currently supports only IPv4 addresses, you need to specify an IPv4 address as the Proxy Host. However, when Apple extends its support to include IPv6 addresses in the future, then you can specify IPv6 addresses as the Proxy Host.

- ◆ **Port:** Specify the port number on which the Proxy Server is listening.
- ◆ **Proxy Server requires authentication:** Select this option if the Proxy Server requires authentication information from the server. On selecting this option, you can specify the credentials to authenticate to the Proxy Server.
- ◆ **Test URL:** Specify the URL of a web application or a web server and click **Test Proxy** to verify the connection of the specified Proxy Server. The Test URL should be specified in the following format, for example: `https://www.microfocus.com`.

NOTE

- ◆ Proxy Server details are cached in the ZENworks Server memory. If you modify the Proxy Server details, then it will take at least 15 minutes for these changes to become effective on all servers.
 - ◆ Proxy Server should be configured to allow HTTP and SSL communication.
-

8

Enabling Push Notifications

Push notifications can be sent to Android Devices and Apple Devices to enable communication between the ZENworks Server and the ZENworks Agent app (for Android devices) or the ZENworks Server and the MDM profile (for iOS devices) installed on the device.

- ♦ [Section 8.1, “Enabling Push Notifications for iOS Devices,” on page 41](#)

8.1 Enabling Push Notifications for iOS Devices

Apple Push Notification service (APNs) enables a ZENworks MDM Server to notify an iOS device when the server requires information from the device or has changes for the device. The ZENworks MDM Server communicates with the Apple Push Notification service, which then pushes the notification to the device. After receiving the push notification, the device contacts the ZENworks MDM Server directly to provide the requested information or to receive the changes.

8.1.1 Prerequisites

- ♦ **An APNS Certificate:** In order to use the Apple Push Notification service, an Apple Push Notification service certificate is required. The APNs certificate allows the ZENworks MDM Servers and iOS devices to authenticate securely to the service. Apple Push Notification service certificates are issued by Apple. The following sections help you create the Certificate Signing Request (CSR), submit the request to Apple, and import the Apple-issued APNs certificate into your ZENworks system.
- ♦ **MDM Server:** An MDM role is assigned to a Primary Server and appropriate ports are opened in the firewall. For more information, see [Configuring an MDM Server](#).

8.1.2 Creating and Importing an APNs Certificate

- 1 On the Getting Started with Mobile Management page, navigate to the **Apple Devices** section, click **Configure APNs**. Alternatively, from the left hand side navigation pane of ZCC, navigate to **Configuration > Push Notification > Apple Push Notification**.
- 2 Create a Certificate Signing Request:
 - 2a Click **Create a Certificate Request**.
 - 2b Specify the following certificate details:
 - Organization Apple ID:** Valid Apple ID in email format (for example, user1@mycompany.com). Best practice dictates that this should be an Apple ID created specifically for managing your corporate Apple Push Notification service certificate and not an Apple ID used for a general developer account or a personal account.
 - Organization Unit:** Name of the organizational unit (division, department, or so forth) to which you belong. For example, *IT, IS Department, Technical Services Group, or Business Services*.
 - Organization Name:** Name of your organization.

City or Locality/State/Country: Location information for your organization.

- 2c Provide the credentials (user name and password) of your Micro Focus Customer Center account.

The Certificate Signing Request must be signed by Micro Focus as an approved Mobile Device Management (MDM) vendor. Your Micro Focus Customer Center credentials enable Micro Focus to sign the request.

- 2d Click **Submit for Signing**.

- 2e After the Certificate Signing Request file is signed by Micro Focus, save the signed Certificate Signing Request (CSR) file to a location of your choice.

- 3 Submit the Certificate Request to Apple and download the APNs Certificate:

- 3a Click **Apple Push Certificates Portal**.

- 3b Sign in with your Apple ID and password.

- 3c Follow the prompts to upload your CSR file and create an APNs certificate.

- 3d Download the APNs certificate.

- 4 Import the APNs Certificate in ZCC:


- 4a Click **Import APNs Certificate**.

- 4b Browse and select the APNs certificate file, then click **OK**.

The APNs certificate is imported to your system and the certificate's subject, expiration date, and key length are displayed.

- 4c To check that the certificate is valid and that your ZENworks system can communicate with the Apple Push Notification service, click **Test Certificate**. This option will test the connection to APNs from each of the MDM Servers configured in the zone. If the connectivity fails from one or more MDM Servers, then the failed servers are listed.

8.1.3 Renewing an Expired APNs Certificate

- 1 On the Getting Started with Mobile Management page, navigate to the **Apple Devices** section, click **Configure APNs**. Alternatively, from the left hand side navigation pane of ZCC, navigate to **Configuration > Push Notification > Apple Push Notification**.
- 2 Ensure that the existing Certificate Signing Request is available. To create a CSR, follow the steps described in [Step 2](#).
- 3 Click **Apple Push Certificates Portal**.
- 4 Sign in with your Apple ID and password.
- 5 Click **Renew** against the certificate that you want to renew. You can identify the certificate based on its **Subject**, which can be viewed by clicking , and the **Expiration** date.
- 6 Follow the prompts to upload the CSR and download the renewed APNs certificate.
- 7 In ZCC, import the APNs certificate by following the steps described in [Step 4](#).

IMPORTANT: If the APNs certificate has expired, ensure that you do not revoke or create a new certificate, or else you will have to re-enroll all mobile devices that were initially enrolled using the earlier certificate.

9 Creating and Assigning a Mobile Enrollment Policy

For devices to be enrolled (registered) in your ZENworks Management Zone, you must create a Mobile Device Enrollment policy and assign it to users who will enroll devices. Mobile Enrollment policy decides which user can enroll devices, what devices the user can enroll, the mode to be used for device enrollment, and the location and naming of the device. Depending on the diversity of needs in your organization, you can create a single Mobile Enrollment policy for all users or you can create multiple policies for users with different needs.

- ♦ “Creating a Mobile Enrollment Policy” on page 43
- ♦ “Editing Mobile Enrollment Policy” on page 45
- ♦ “Assigning a Mobile Enrollment Policy” on page 45

Creating a Mobile Enrollment Policy

- 1 On the **Modern Management > Getting Started > Managing Android Devices** page, navigate to the **Enrollment Policy** section, click **New Enrollment Policy** to display the Create New Policy wizard.
Alternatively, from the left hand side navigation pane of ZCC, navigate to **Policies > New > Policy**.
- 2 On the Select Platform page, select **Mobile** and then click **Next**.
- 3 On the Select Policy Category page, select **General Mobile Policies** and then click **Next**.
- 4 On the Select Policy Type page, select **Mobile Enrollment Policy** and then click **Next**.
- 5 On the Define Details page, specify a name for the policy, select the folder in which to place the policy and then click **Next**.
- 6 On the Configure Device Ownership page:
 - 6a You can select the ownership type for the device, such as **Corporate** or **Personal**. The ownership is categorized based on the enrollment methods:
 - ♦ Apple Device Enrollment Program
 - ♦ Apple Configurator
 - ♦ ZENworks User Portal
 - ♦ ZENworks Agent App

You can also enable the **Allow the device user to select ownership type** option to allow users who are enrolling their devices using the ZENworks User Portal or the ZENworks Agent App, select the appropriate ownership type of the device,

Mobile policies enable you to provide two groups of settings, one group that is applied to corporate-owned devices and a second group that is applied to personally-owned devices.

For example, the Mobile Security policy lets you configure different password, encryption, and lockout settings for corporate-owned devices versus personally-owned devices.

6b Click **Next**.

7 On the Configure Device Management page:

7a The default settings allow the user to choose the management level (**Managed Device** or **Email Only**) during enrollment.

NOTE: This option is applicable for enrollment using the ZENworks End User Portal.

The device management options are explained below:

- ◆ **Yes, allow users to enroll their devices as fully managed devices:** Enables users to enroll their devices as a **Managed Device** only.
 - ◆ **Do not show option for ActiveSync - only enrollment:** Removes the ActiveSync Only (Email Only) enrollment option, forcing devices to enroll as fully managed devices.
 - ◆ **No, allow users to enroll their devices as ActiveSync -only:** Removes the fully managed option, forcing devices to enroll as ActiveSync Only (Email Only) devices.

7b Click **Next**.

8 On the Configure Mobile Enrollment Rules page, note the folder and naming settings for the default **All Devices** rule in the list, then click **Next**.

Enrollment rules determine the enrolling device's display name and folder placement in ZENworks Control Center.

The predefined **All Devices** rule allows all devices to enroll, uses the device model and user's name for the device name, and places the device in the **Mobile Devices** folder. If the default rule does not meet your needs, you can modify or remove the **All Devices** rule and add additional rules as needed. For example, you can create a rule to place all Android devices in one folder and all iOS devices in another.

NOTE: Due to changes in the Google privacies, the Work Profile devices running on Android 11 and above are unable to access device identifiers such as Wi-Fi Mac Address, Serial Number, and IMEI.

The device enrollment on Android 11 and above, Work Profile is not supported if any of these device identifiers are used as a criterion for device enrollment.

Suggested alternative: It is recommended to use a combination of the following identifiers on the Android 11 and above Work Profile for device enrollment:

- ◆ OS versions
- ◆ Device model

9 On the Configure the Un-enrollment Settings page you can configure the un-enrollment settings, which will take effect when users un-enroll their devices from the ZENworks Server or the management zone. Select any one of the following for a corporate-owned device or a personally-owned device and click **Next**:

- ◆ **Retire Device:** The device is retained in the zone, however the status is set as retired. When the device is retired, ZENworks does not manage the device anymore, but the device data and history is retained.
- ◆ **Delete Device:** The device is removed from the zone.

NOTE: These settings are not applied when the user removes the work profile from Android devices enrolled in the work profile mode.

10 On the **Summary** page, you can perform the following actions:

- ◆ **Create as Sandbox:** Creates a Sandbox-only version of the policy. A Sandbox version of a policy enables you to test it on your device before actually deploying it
- ◆ **Define Additional Properties:** Enables you to edit the default settings configured in the policy.

Click **Finish** to complete creating the policy.

Editing Mobile Enrollment Policy

If **Define Additional Properties** is selected at the time of policy creation, then you will be re-directed to the edit page. Alternatively, navigate to **Policies** and select the Mobile Enrollment Policy you want to edit. You can edit any of the configured settings within the Mobile Enrollment Policy. Additionally, the Mobile Enrollment Policy lets you configure the following:

- ◆ Select **Allow Manual Reconciliation by User** by navigating to **Details > Advanced Setting**. This feature allows the end user to manually reconcile their devices to an existing device object during enrollment. For more information, see [Allowing Manual Reconciliation by the User](#).

If you change the enrollment policy settings after mobile devices are enrolled to the zone, then the updated enrollment policy settings are not applied to the already enrolled devices. However, if the un-enrollment settings are modified after the user enrolls the device, then only the updated un-enrollment settings are applied to the user's device. Also, un-enrollment is not applicable for those devices that are enrolled as Email Only (ActiveSync only) devices.

Assigning a Mobile Enrollment Policy

Mobile Enrollment policy should be assigned to only users.

Procedure

- 1 On the Getting Started with Mobile Management page, navigate to the **Enrollment Policy** section, click **Assign Policy** to display the Assign Policy wizard, then click **Add**. Alternatively, from the left hand side pane in ZCC, navigate to Policies. Select a policy and click **Action > Assign to User**.
- 2 In the Select Object dialog box, browse and select the users to whom you want to assign the policy, click **OK** to add them to the **Users to be Assigned** list, then click **Next**.
- 3 On the Select Object dialog box, browse for and select the policy to be assigned to a user, click **OK** to add them to the **Policies to be Assigned** list, then click **Next**.
- 4 Review the summary page and click **Finish** to complete the assignment.

10 Configuring an ActiveSync Server

ZENworks can act as a gateway to relay incoming and outgoing email traffic to devices from the Microsoft Exchange or the GroupWise Mobile Server, by using the ActiveSync protocol. This requires you to connect your ZENworks Server to the Email Servers, which uses Exchange ActiveSync version 12.1 or newer, through which your mobile device users receive their email. These email servers will hereon be referred to as an *ActiveSync Server*. ZENworks supports both the Microsoft Exchange and GroupWise Mobility Servers.

After configuring the required ActiveSync Servers, to enable ZENworks to synchronize and manage the corporate email accounts on the enrolled device, you need to create and assign a Mobile Email Policy. It also entitles Android, iOS, and Windows devices enrolled to the ZENworks Server to send or receive corporate data through the ActiveSync Server. For more information, see [Creating and Assigning a Mobile Email Policy](#).

NOTE: For users of the GroupWise mailing system where users are defined in the NetIQ eDirectory, ZENworks uses only those email addresses that are specified in the *username@domain.com* format. Also, LDAP Authentication should be enabled in your GroupWise system. For more information, see the [GroupWise Online Documentation](#).

- ♦ [“Connecting to a New ActiveSync Server” on page 47](#)
- ♦ [“Linking a User Source to an ActiveSync Server” on page 49](#)

Connecting to a New ActiveSync Server

Prerequisites

A backend Exchange Server should be configured with user mailboxes.

Procedure

- 1 On the Getting Started with Mobile Management page, navigate to the **ActiveSync Servers** section and click **New ActiveSync Server**. Alternatively, from the left hand side navigation pane of ZCC, click **Configuration > ActiveSync** tab.
- 2 In the ActiveSync Servers panel, click **New** to display the New ActiveSync Server dialog box.
- 3 Fill in the following fields:
 - ♦ **Server:** Specify a display name for the ActiveSync Server. This can be any name you want for display purposes. It does not have to match the actual server name.
 - ♦ **Address:** Specify the hostname or IP address of the ActiveSync Server.
 - ♦ **Domain:** Specify the registration domain that is associated with the ActiveSync Server.
 - ♦ **Port:** Specify the listening port for the ActiveSync Server.
 - ♦ **Use SSL:** Select this option to enforce a secure connection with the ActiveSync Server.

- ♦ **Link to User Source:** Select the ZENworks user source (LDAP directory) with which you want the ActiveSync Server to be associated.

When a user enrolls a device using the domain name, the user is authenticated via the user source and directed to the ActiveSync Server.

If multiple ActiveSync Servers are linked to the same user source, you can specify the order in which the servers are contacted. You can re-order the user sources by navigating to **Users > <User Source> Details > Mobile Management > Linked ActiveSync Servers**.

4 Test user authentication to the ActiveSync Server:

4a Click **Test Authentication**.

4b Specify the credentials for an active account on the ActiveSync Server.

NOTE: The user name is required. You can specify the user name in the following two formats:

- ♦ domain\user name (example.com\testuser1)
- ♦ email ID format (testuser1@example.com)

4c Click **Test**.

4d If the test is successful, click **Close**.

If the test fails, specify the user name and password again, or try a different user name and password. If the test fails again, verify that the server address and port are correct, then retry the test.

IMPORTANT: For email based authentication, the email address should be present in the configured user source for successful ActiveSync enrollment on the device. For users of the GroupWise email system, you need to publish these email addresses to eDirectory. For details, you can refer to the GroupWise Documentation.

5 Save the ActiveSync Server connection:

5a Click **Create Server**.

5b If you are prompted to accept the ActiveSync Server's certificate (because a secure connection is being used), click **Accept**.

If you are unsure of the certificate, you can click **View Certificate** to review it. If you choose to reject the certificate, you are returned to the Create ActiveSync Server dialog box.

6 Run the following configure action on all primary servers after configuring the ActiveSync Server in a zone:

```
microfocus-zenworks-configure -c HTTPMethodSettingConfigureAction
```

By default, the HTTP method `OPTIONS` is disabled in ZENworks. You must run the `microfocus-zenworks-configure -c HTTPMethodSettingConfigureAction` configure action to support ActiveSync communication.

You can delete or edit the parameters of the ActiveSync Server. To edit the parameters of the ActiveSync server, click an ActiveSync Server and modify the parameters. If the ActiveSync Server that you want to modify is already configured with a Mobile Email Policy, then you have to republish or reassign the policy after modifying the server details.

You can delete a configured ActiveSync Server by selecting the server and clicking **Delete**. To delete an ActiveSync server that is configured with an Mobile Email policy, you have to change the ActiveSync Server in the Mobile Email Policy and then delete the ActiveSync Server.

NOTE: You must run the `microfocus-zenworks-configure -c HTTPMethodSettingConfigureAction` configure action if you are removing an ActiveSync Server.

Linking a User Source to an ActiveSync Server

The Linked ActiveSync Servers panel lets you link the user source to one or more ActiveSync Servers. When a user in the user source enrolls a device, the linked ActiveSync Servers are used to provide the user's email on the device.

Procedure

- 1 In ZENworks Control Center, click **Users** (in the left navigation pane) to display the User Sources list.
- 2 Click **Details** next to the user source to display its property pages.
- 3 Click the **Mobile Management** tab.
- 4 In the **Linked ActiveSync Servers** panel, click **Add**, select an ActiveSync Server from the list and click **OK**.

11 Creating and Assigning a Mobile Email Policy

You need to create a Mobile Email Policy to manage the corporate email account of devices within your zone. With this policy you can grant permissions to configure an email account, maintain email synchronization settings, restrict or allow users to move between email accounts and other third party applications. To enable ZENworks to manage all corporate emails sent and received on the enrolled mobile device, you need to allow the ZENworks Server to act as a proxy server for the ActiveSync Server, in the assigned Mobile Email Policy. This will route all email traffic through the ZENworks Server.

However, this policy also gives you the option to send or receive emails on these devices directly from an ActiveSync Server for a specific set of users. The configuration of an email account differs as per the mode in which the device is enrolled. For more information on the various enrollment modes, see [“Enrolling Mobile Devices” on page 55](#).

- ♦ **iOS device enrolled as a fully managed device:** If a Mobile Email Policy is assigned to a fully managed iOS device, then an email account of the device’s in-built email client is automatically configured on the device based on these settings. If the assigned Mobile Email Policy does not use ZENworks as the proxy server, the device can send or receive corporate emails. However, the email account will not be managed by ZENworks.
- ♦ **ActiveSync Only devices:** To enable ZENworks to manage the corporate email account on a device enrolled as an ActiveSync Only device, the assigned Mobile Email Policy should have the ZENworks Server acting as a proxy for the ActiveSync Server. If the assigned Mobile Email Policy does not use the ZENworks Server as the proxy server or if no Mobile Email Policy is assigned to a device, then ZENworks will not be able to manage corporate emails on the device.

NOTE: For **fully-managed Android** devices, ZENworks supports enrollment only in the work profile or work-managed device modes. Therefore, it is recommended that you do not assign a Mobile Email Policy to these devices. The email account on these devices should directly communicate with the configured ActiveSync server. To configure the corporate email account, you can provision bundles with apps such as Gmail. For more information, see [Provisioning Applications](#).

However, if you are using ZENworks as the proxy for the configured ActiveSync Server, then assign the Mobile Email Policy to the device and ensure that the **Allow Manual Reconciliation by User** setting is enabled in the assigned Mobile Enrollment Policy. For more information, see [Allowing Manual Reconciliation by the User](#).

- ♦ [“Creating a Mobile Email Policy” on page 51](#)
- ♦ [“Assigning a Mobile Email Policy” on page 53](#)

Creating a Mobile Email Policy

- 1 On the Modern Management > Getting Started page, navigate to the **Managing iOS/iPadOS devices Email Policy** section and click **Create Email Policy**.

Alternatively, from the left hand side navigation pane of ZCC, navigate to **Policies > New > Policy**.

- 2 On the Select Platform page, select **Mobile**, then click **Next**.
- 3 On the Select Policy Category page, select **General Mobile Policies**, then click **Next**.
- 4 On the Select Policy Type page, select **Mobile Email Policy**, then click **Next**.
- 5 On the Define Details page, specify a name for the policy, select the folder in which to place the policy, then click **Next**.
- 6 On the **Automatic Email App Configuration** page, the settings in the **Corporate** column are applied to devices whose ownership is defined as Corporate. The settings in the **Personal** column are applied to devices whose ownership is defined as Personal. Set the following values and click **Next**.
 - ◆ **Account Name:** Specify the email account name that will appear on the email account configured on the device.
 - ◆ **Period to sync email:** Syncs emails to the device as per the number of days set in this field. Set an appropriate value to indicate the period of time for email messages to be displayed on the device.
 - ◆ **Allow messages to be moved to other email accounts:** Enables the user to move emails between email accounts. Also, it allows the user to reply or forward email messages from another email account rather than from the original email account.
 - ◆ **Allow recent addresses to be synced:** Enables recent addresses to be synced to the email account configured on the device.
 - ◆ **Use account in third party applications:** Enables the user to send emails from a third party application.
 - ◆ **Allow the use of Mail Drop to send large attachments:** Enables the user to attach large files in emails using the Mail Drop feature. Using this feature, you can upload attachments up to 5 GB. Applicable on iOS version 11.0 or later versions.
 - ◆ **Platform Support:** The platform columns show support for a setting. A green dot ● indicates that the platform supports the setting. These settings are currently supported for iOS (iOS 8 or higher) versions only.
 - ◆ **Do not use ZENworks Server as Proxy Server:** You can ignore this option if you want to use the ZENworks Server as the proxy server to send or receive mails on the device. However, if you want to directly connect to a configured ActiveSync Server to relay emails to your device, then select this option. If this option is selected, from the **ActiveSync Server** drop-down list, select a specific ActiveSync Server from the list of configured ActiveSync Servers in ZCC. If an ActiveSync Server is not already configured in ZCC, then this feature will be disabled.
- 7 On the **Summary** page, you can perform the following actions:
 - ◆ **Create as Sandbox:** Creates a Sandbox-only version of the policy. A Sandbox version of a policy enables you to test it on your device before actually deploying it
 - ◆ **Define Additional Properties:** Enables you to edit the default settings configured in the policy.

Click **Finish** to complete creating the policy.

Assigning a Mobile Email Policy

If a Mobile Email Policy is not assigned to a user or a device that has just enrolled to the ZENworks Management Zone or if the Mobile Email policy is unassigned from an already enrolled device, then the user receives an email stating that corporate emails cannot be sent or received on the device. You can edit the contents of this email in ZENworks Control Center by navigating to **Configuration > Management Zone Setting > Event and Messaging > Email Notifications**. Click the relevant email and edit its contents.

Procedure

- 1 On the Modern Management > Getting Started > Managing iOS/iPadOS devices, click **Assign Policy**. To assign the policy to users, from the **Policies** list, select the check box in front of the policy and then click **Action > Assign to User**. To assign the policy to devices, from the **Policies** list, select the check box in front of the policy and then click **Action > Assign to Device** to assign the policy to devices.
- 2 In the Select Object dialog box, browse for and select the users or devices to whom you want to assign the policy, click **OK** to add them to the list, then click **Next**.
- 3 If the policy is assigned to a device, then Policy Conflict Resolution page is displayed. In this page you can set the precedence for device-associated policies and user-associated policies for resolving conflicts that arise when policies of the same type are associated to both devices and users. Define any of the following and click **Next**:
 - ♦ **User Precedence:** User-associated policy will override the device-associated policy. Select this option to apply policies that are associated to the users first, and then to the devices.
 - ♦ **Device Precedence:** Device-associated policy will override the user-associated policy. Select this option to apply policies that are associated to the devices first, and then to the users.
 - ♦ **Device Only:** Select this option to apply policies that are associated to devices alone.
 - ♦ **User Only:** Select this option to apply policies that are associated to users alone.
- 4 Review the summary page and click **Finish** to complete the assignment.



Enrolling Mobile Devices

This section explains the manner in which mobile devices can be enrolled in the zone. The topics discussed are as follows:

- ♦ [Chapter 12, “Prerequisites,” on page 57](#)
- ♦ [Chapter 13, “Inviting Users to Enroll Devices,” on page 59](#)
- ♦ [Chapter 14, “Enrolling iOS Devices,” on page 61](#)
- ♦ [Chapter 15, “Enrolling Android Devices,” on page 91](#)
- ♦ [Chapter 16, “Enrolling an Email Only Device,” on page 113](#)
- ♦ [Chapter 17, “Allowing Manual Reconciliation by the User,” on page 119](#)
- ♦ [Chapter 18, “Viewing Device Information,” on page 123](#)

Before enrolling (registering) a device to the ZENworks Management Zone, you need to understand the different ways in which ZENworks can manage a device. This will help you in evaluating the manner in which the device needs to be managed, thereby enabling you to select the right enrollment options.

ZENworks lets users enroll their devices as a managed device or as an email only device. You can set this option in the Mobile Enrollment Policy.

- ♦ **Managed Device:** Enables ZENworks to fully manage a device by performing various device management operations such as apply policies to the device, deploy applications on the device, synchronize email for Exchange ActiveSync accounts, and capture device information (inventory). Only iOS, or Android devices can be enrolled as fully managed devices. Full management of an Android device is performed through the ZENworks Agent App that is hosted on the Google Play Store. Full management of an iOS device is performed through the device’s in-built MDM client.
- ♦ **Email Only (ActiveSync Only):** Enables ZENworks to manage only the corporate email account on the device. Also, certain policies that are enforceable through the ActiveSync protocol can be applied. Mobile devices are enrolled to the ZENworks MDM Server using the ActiveSync email clients present on the devices. Android, iOS, and Windows devices can be enrolled as Email Only devices. Devices enrolled as Email Only devices can be managed in the following ways:
 - ♦ **Server Only Mode:** In this case, ZENworks will not be managing the email account on the device. ZENworks can only apply certain policies that are enforceable through the ActiveSync protocol, such as the Mobile Device Control Policy and Mobile Security Policy. ZENworks can also remotely wipe the devices. This might occur due to any one of the following reasons:
 - ♦ A Mobile Email Policy is not assigned to the device.
 - ♦ The assigned Mobile Email Policy does not use ZENworks as the proxy server between the configured ActiveSync Server and the device. The policy directly connects to the configured ActiveSync Server.

- ♦ The ActiveSync server is not linked to the associated user source.
- ♦ The ActiveSync server is not valid for the user.
- ♦ **Proxy Mode:** In this case, corporate emails on the device will be managed by ZENworks. Also, ZENworks can apply certain policies that are enforceable through the ActiveSync protocol, such as the Mobile Device Control Policy and Mobile Security Policy, and can remotely wipe the devices. In a proxy mode, a Mobile Email Policy, with the ZENworks Server acting as the proxy server, is assigned to the device or the user.

NOTE: You can enroll 1000 mobile devices simultaneous without any additional load on the Primary Server. While enrolling, the Windows MDM requires a server with Internet connectivity. For more information on MDM Server, see [Chapter 7, “Configuring an MDM Server,”](#) on page 29.

12 Prerequisites

Before enrolling a mobile device to ZENworks, you need to ensure that the following prerequisites are met. Prerequisites that are specific to a mobile device platform or a type of enrollment will be explained in the relevant sections:

Task	Details
Add a User Source	For more information, see Configuring User Sources .
Add an MDM Server	For more information, see Configuring an MDM Server .
Enable Push Notifications	For more information, Enabling Push Notifications .
Create and assign a Mobile Enrollment Policy	For more information, Creating and Assigning a Mobile Enrollment Policy .
Add an ActiveSync Server (Optional)	If you want to enable ZENworks to synchronize emails for Exchange ActiveSync accounts, an ActiveSync server should be configured. For more information, see Configuring an ActiveSync Server .
Create and assign a Mobile Email Policy (Optional)	If you want to enable ZENworks to manage the corporate emails sent and received on the device, then create and assign a Mobile Email Policy. For more information, see Creating and Assigning a Mobile Email Policy .

IMPORTANT: If the ZENworks MDM Server is in the DMZ and after upgrading the zone to the ZENworks 2020 release version, if you face issues while enrolling or managing iOS and Android devices, ensure that you open the ZooKeeper ports 6789, 6790 and 6791 between the Primary Server on the network and the MDM Server in the DMZ. For more information on ZooKeeper, see [Managing ZooKeeper](#).

13 Inviting Users to Enroll Devices

You can send an invite letter to users to have them enroll their devices to ZENworks. To do this:

- 1 Click **Users** in the left hand pane in ZCC.
- 2 Select a user folder or a specific user.
- 3 Click **Action > Invite User**.

You can preview the email notification in different languages by selecting the appropriate language from the **Preview Language** drop down. However, the email will be sent in the language set in the Mobile Enrollment Policy, which should be assigned to the selected users. The contents of the pre-configured email can be customized to suit your requirements. You can edit the content by navigating to **Configuration > Event and Messaging > Email Notifications > Invite Users**. For more information, see [Managing Email Notifications](#).

Before clicking the **Send** button, you should also select the **MDM Server** to which the users should enroll their devices. This MDM Server will be resolved to the macro variable `$HOSTNAME$` present in the pre-configured email. All macro variables will be resolved when the email is sent to the user

NOTE: Ensure that an SMTP server is configured, which will enable you to send the email notification.

For Android devices, after the user downloads the ZENworks Agent App, the user can tap the **Scan to autofill** icon on the app to auto-fill the login credentials in the ZENworks Agent app. On tapping the icon, the device camera will open and the user needs to scan the QR code appearing under the **To enroll an iOS, BlackBerry or Windows mobile device** section of the default Invite email. After scanning the QR code, the user will be redirected to the ZENworks Agent app. All the login credentials except the user password will be autofilled in the app. The user needs to only specify the password to login to the app. For more information on enrolling Android devices, see [Enrolling Android Devices](#).

14 Enrolling iOS Devices

This section explains how an iOS device can be enrolled as a fully managed supervised and fully managed non-supervised device.

NOTE: During the enrollment of device, the associated device object will be present in the Pending Enrollment folder in ZCC and will be displayed as an iOS device. However, after completing the enrollment process and after the device syncs with the ZENworks Server, it is displayed as device.

- ♦ [“What is a supervised device?” on page 61](#)
- ♦ [“Enrolling devices using the Apple Device Enrollment Program” on page 61](#)
- ♦ [“Enrolling an iOS Device through Apple Configurator” on page 73](#)
- ♦ [“Enrolling an iOS Device Manually” on page 77](#)

What is a supervised device?

- ♦ Enrolling the device using the Apple Device Enrollment Program
- ♦ Enrolling the device using Apple Configurator

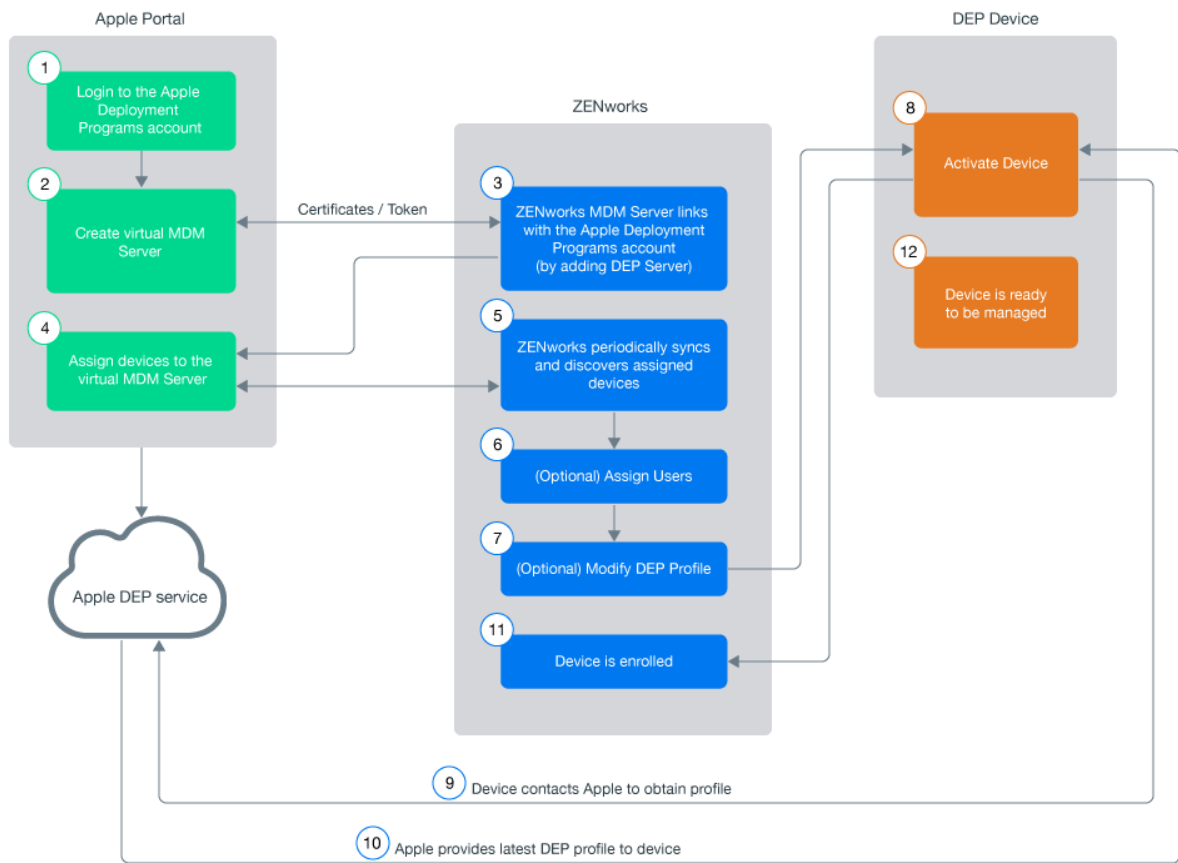
To enroll a device in the non-supervised mode, you can manually enroll the device using the ZENworks User Portal. For more information, see [Enrolling an iOS Device Manually](#).

Enrolling devices using the Apple Device Enrollment Program

The Device Enrollment Program (DEP) is part of the Apple Deployment Programs and provides administrators with a streamlined way to deploy multiple corporate owned iOS devices. Upon device activation, over-the-air configuration of the device is immediate and enrollment with the MDM server is automatic. There is no need for IT administrators to physically access each device to complete the setup. The benefits of this program are:

- ♦ Zero-touch enrollment of devices to the MDM Server
- ♦ Wireless supervision of devices
- ♦ Enforce MDM Enrollment of devices
- ♦ Lock MDM Profiles on the devices
- ♦ Streamlined setup process

The procedure to enroll devices to the Apple Device Enrollment Program (DEP) using ZENworks is summarized in the following workflow. However, as a prerequisite, you need to first set up a DEP account and associate your sales information with it. For more information on setting up a DEP account, see the [Apple Support Documentation](#).



NOTE: With the iOS 11.x release, you can associate any iOS 11.x device to an existing DEP account (even if these devices are not purchased directly from Apple or an Apple reseller) using the Apple Configurator tool. For more information on associating these devices using the Apple Configurator tool, see [Enrolling existing devices to the Apple Device Enrollment Program for simplified provisioning with ZENworks](#).

To know more about the Apple Deployment Program, you can also watch the following videos to know more about the Apple Deployment Program:

IMPORTANT: If you are enrolling devices using Apple School Manager, ensure that the Device Manager role is assigned to your Apple School Manager account. For more information, see the [Apple School Manager Help](#).

The workflow associated with enrolling DEP devices are as follows:

- ◆ [“Linking ZENworks to the Apple Deployment Programs Account” on page 63](#)
- ◆ [“Assigning Devices” on page 64](#)
- ◆ [“Syncing Devices” on page 65](#)
- ◆ [“Viewing DEP Devices” on page 65](#)
- ◆ [“Managing the DEP Profile” on page 67](#)
- ◆ [“Assigning Users” on page 71](#)
- ◆ [“Enrolling a DEP Device” on page 72](#)

- ♦ “Renewing a DEP Token” on page 72
- ♦ “Removing a DEP Server” on page 73
- ♦ “Re-assigning Devices” on page 73

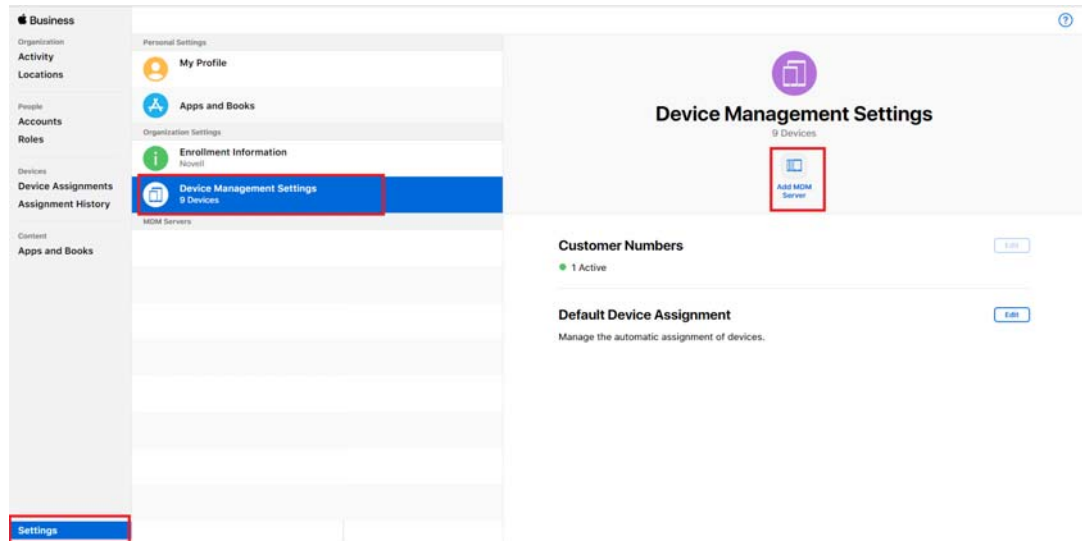
Linking ZENworks to the Apple Deployment Programs Account

A DEP Server links the ZENworks MDM Server to the virtual MDM Server that you need to create in the DEP portal.

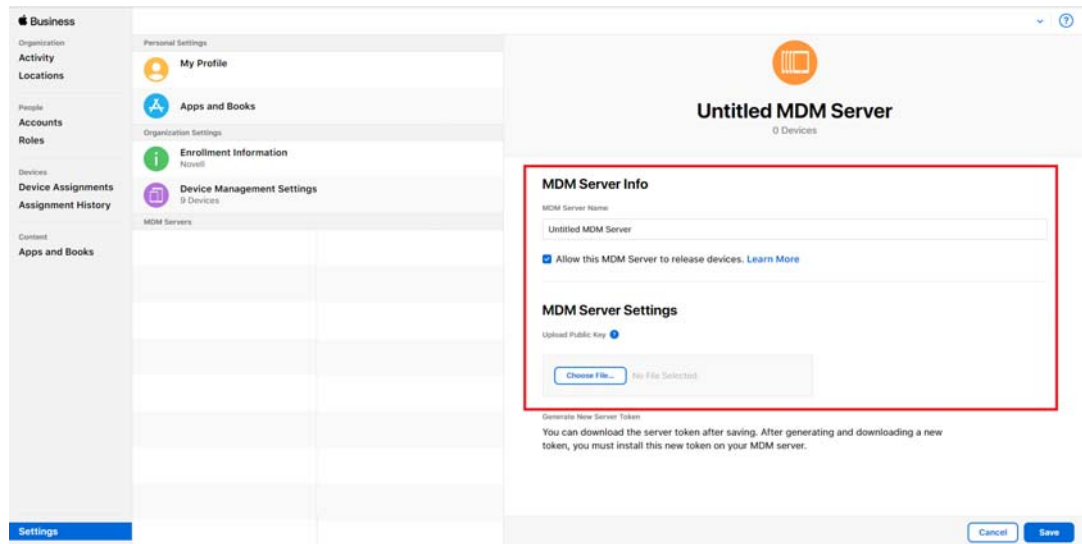
A ZENworks MDM Server can be linked to multiple virtual MDM Servers. However, a virtual MDM Server that is already linked with a ZENworks MDM Server, cannot be linked to another ZENworks MDM Server. The devices assigned to these virtual MDM Servers will enroll to the associated ZENworks MDM Server.

To add a DEP Server:

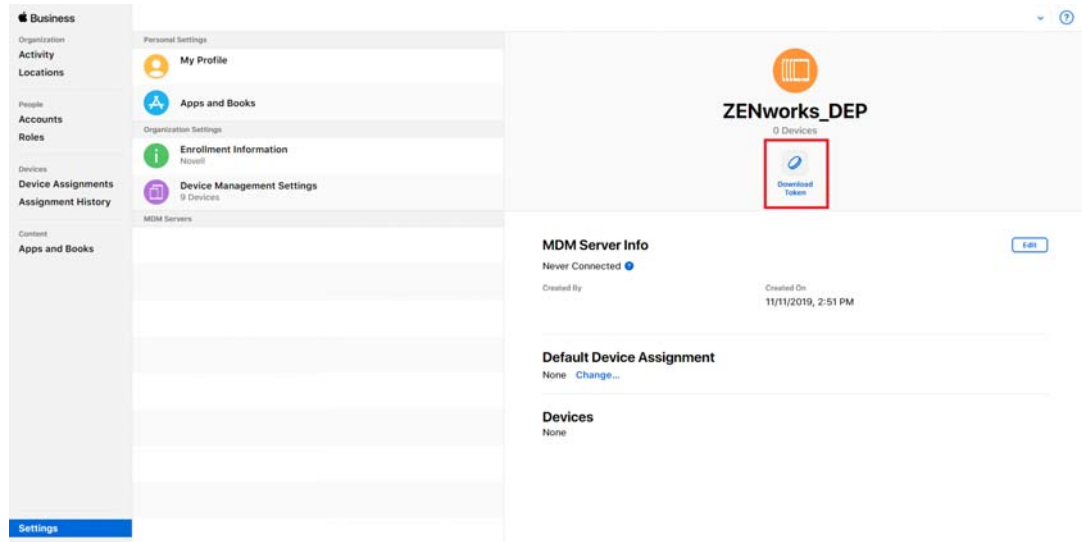
- 1 On the Modern Management > Getting Started > Managing iOS/iPadOS Devices page, click **Add DEP Server**. Alternatively, navigate to **Configuration > Management Zone Settings > Discovery and Deployment > Apple Device Enrollment Program**.
- 2 Click **Add** to link a ZENworks MDM Server to your deployment program account.
- 3 Click the Browse icon, select an MDM Server and click **Download** to download and save the Public Key certificate of the selected MDM Server.
- 4 Click the **Apple Business Manager** or the **Apple School Manager** portal and sign in using your DEP account credentials. On this portal:
 - 4a Navigate to **Settings** on the left pane of the page.
 - 4b Click **Device Management Settings** in **Organization Settings**. Click **Add MDM Server** on the right pane.



- 4c Specify a name for the DEP Server.
- 4d Upload the Public Key of the ZENworks MDM Server that you had saved earlier in the **MDM Server Settings** section. Click **Next**.



4e Click **Download Token** and download the token issued by Apple and click **Next**.



5 In ZCC, click **Upload** to upload the DEP token issued by Apple to the selected ZENworks MDM Server. This token enables the ZENworks MDM Server to securely connect with the Apple DEP web service.

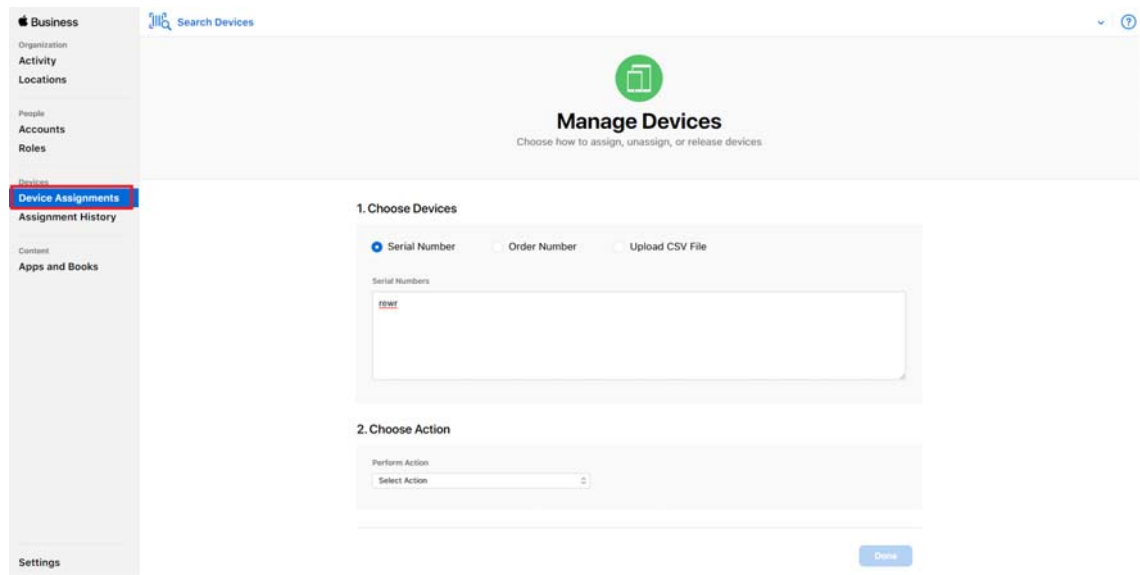
6 Click **Add DEP Server**. You have now created a DEP Server in ZCC.

Assigning Devices

You need to create at least one virtual MDM Server in the Apple portal before you begin assigning devices.

- 1 Click the [Apple Business Manager](#) or the [Apple School Manager](#) portal and click **Device Assignments** on the left pane of the page.
- 2 You can assign devices based on:
 - ◆ **Serial Number:** Specify each serial number separated by a comma.

- ◆ **Order Number:** The quantity and type of devices are displayed.
- ◆ **Upload CSV File:** Upload a comma-separated value (CSV) file that contains a list of device serial numbers.



- 3 Select the virtual MDM Server to which you want to assign the devices, in the **Choose Action** drop down menu.
- 4 Click **OK**.

NOTE: Only those devices that are assigned to the virtual MDM Server in the Apple portal are identified as DEP devices in ZCC. If a DEP enabled device is enrolled to ZENworks (using ZENworks User Portal) but is not assigned to the virtual MDM Server in the Apple portal, this device will not be identified as a DEP device.

Syncing Devices

After a DEP Server is configured in ZCC, ZENworks syncs with the Apple DEP web service and discovers assigned devices and populates the devices in ZCC. Subsequently, ZENworks initiates a periodic sync on a daily basis to update the latest device assignments. To perform this sync immediately, you can also click **Sync All** on the Apple Device Enrollment Program page (**Configuration > Management Zone Settings > Discovery and Deployment > Apple Device Enrollment Program**). To view the discovered devices in ZCC, see [Viewing DEP Devices](#).

Viewing DEP Devices

To view the discovered devices, navigate to **Devices > Discovered > Apple DEP Devices**.

On clicking a device, the following tabs are displayed:

- ◆ [Summary](#)
- ◆ [Settings](#)

Summary

This page provides a summary of the device's general information.

◆ Device Details

- ◆ **Serial Number:** Serial number of the device.
- ◆ **Model:** Model of the device.
- ◆ **Description:** Short description of the device.
- ◆ **Color:** Color of the device model.
- ◆ **Asset Tag:** Asset tag that is used by the organization to monitor a device.
- ◆ **Device Assigned Date:** Date on which the device was assigned to the virtual MDM Server in the Apple portal.
- ◆ **Device Assigned By:** Administrator who has assigned the device to the virtual MDM Server in the Apple portal.
- ◆ **Deployment Status:** Enrollment status of the device. If the device is enrolled in ZENworks then the status is displayed as **Managed**. If the device is discovered by ZENworks but not enrolled to the ZENworks MDM Server, then the status is displayed as **Discovered**.

◆ Server Details

- ◆ **MDM Server:** ZENworks MDM Server to which the device will be enrolled.
- ◆ **DEP Server:** DEP Server to which the device is associated.

◆ User and Organization Details

- ◆ **Assigned User:** User to whom the device is assigned. Only this user can enroll the device through DEP. To edit this field, you need to have *Modify Apple DEP Device Rights* assigned to you. This option is applicable for DEP enrollment only.
- ◆ **Organization Name:** Name of the organization associated with the linked deployment program account.
- ◆ **Organization Phone Number:** Phone number of the organization associated with the linked deployment program account.
- ◆ **Organization Address:** Address of the organization associated with the linked deployment program account.

◆ DEP Profile Details

- ◆ **Assignment Status:** DEP profile assignment status. The various statuses are:
 - ◆ **Assigned:** DEP Profile assignment on the device is successful.
 - ◆ **In Progress:** DEP Profile assignment is in progress.
 - ◆ **Failed:** DEP Profile assignment to the device has failed.
 - ◆ **Blocked:** Device is blocked due to errors reported after three attempts to assign the profile. You need to contact Apple to resolve any issues with the device. Subsequently, to unblock the device you need to do the following:
 - ◆ Delete the device from the virtual MDM Server.
 - ◆ Click **Sync All** on the Apple Device Enrollment Program page in ZCC, to remove the device from ZCC.
 - ◆ Assign the device back to the virtual MDM Server. Click **Sync All** or wait for the periodic sync initiated by ZENworks, to populate the device in ZCC.

- ◆ **Device not accessible:** Device is either disowned or is re-assigned to another virtual MDM Server.
- ◆ **Assignment Time:** The time at which the profile was assigned to the device in the Apple portal.
- ◆ **Last Push Time:** The time at which the profile was last pushed to the device by Apple during device enrollment.

Settings

This page lets you modify the DEP profile. For more information see, [Managing the DEP Profile](#).

Managing the DEP Profile

The settings that govern the enrollment process of a DEP enabled device is known as the DEP Profile. The DEP profile in ZCC is segregated as follows:

- ◆ **General and Skip Item Settings:** Lets you modify the initial setup process of the device. For more information, see [Editing General and Skip Item Settings](#).
- ◆ **Host Certificates:** Lets you configure the certificate of the host device to allow pairing of devices. For more information, see [Uploading a Host Certificate for Pairing](#).

On installing ZENworks Configuration Management (ZCM), a DEP profile with default values is assigned to the **Apple DEP Devices** folder (**Devices > Discovered**). Subsequently, the discovered DEP devices that appear within this folder inherit the default profile. ZENworks lets you modify this DEP profile as per the needs of the organization. The profile can be modified at the folder level or for a specific device. The modified DEP profile will be applied on only those devices that are to be newly enrolled or are reset to their factory settings.

The updated profile is assigned to the devices in the Apple portal. Before the users begin enrolling their devices, ensure that the modified DEP profile is successfully assigned to the device in the Apple portal. View the **Assignment Status** of the device by navigating to **Devices > Discovered > Apple DEP Devices**.

The modified DEP profile is received by the device when the device is activated. Ensure that you do not modify the settings while the users are enrolling their devices. If the incorrect settings are assigned to the device, then a factory reset is required.

To edit the DEP profile at **Apple DEP Devices** folder level,

- ◆ Navigate to **Devices > Discovered**. Click **Settings** next to the **Apple DEP Devices** folder.

To edit the DEP profile for a specific device:

- ◆ Navigate to **Devices > Discovered > Apple DEP Devices > <Select a Device> > Settings**. To override the DEP Profile settings configured at the folder level and to configure new settings, click **Override**. Click **Revert**, to use the inherited settings.

Editing General and Skip Item Settings

General Settings: The general profile settings are as follows:

- ♦ **Allow pairing of devices with a host computer:** Enables the user to pair a device. If set to **Yes** then the device can pair with any device. If set to **No**, then the device can pair with only those host devices that have their certificate configured in the DEP Profile.
- ♦ **Set device as supervised:** Enables supervision of devices. This setting is ignored on iOS 13 and later devices devices, as supervised mode is mandatory for these devices.
- ♦ **Allow user to remove the MDM profile from the device:** Enables the user to remove the configured MDM profile. This setting is enabled if the device is set as Supervised.

NOTE: If the device is not Supervised, then the user has the option to remove the MDM profile. If the device is Supervised, it is recommended that you do not enable this setting, as devices cannot be managed if the MDM profile is removed.

- ♦ **Allow user to skip applying the MDM profile on the device:** Enables the user to skip enrollment of the device with the MDM Server. This setting is ignored on iOS 13 and later devices devices, as DEP enrollment is mandatory for these devices.
- ♦ **Specify the support phone number displayed during enrollment:** Displays the defined customer support phone number.
- ♦ **Specify the support email address displayed during enrollment:** Displays the defined customer support email address.
- ♦ **Specify the department name displayed during enrollment:** Displays the defined department or location name.
- ♦ **Specify the default language to be selected during enrollment:** The specified language will be automatically selected during the enrollment of the device. You need to specify the language in either the two-letter ISO 639-1 format or the three-letter ISO 639-2 format. An example of these formats are as follows:

Language	ISO 639-1	ISO 639-2
English	en	eng
French	fr	fre
German	de	ger

For more information, see http://www.loc.gov/standards/iso639-2/php/English_list.php.

- ♦ **Specify the default region to be selected during enrollment:** The specified region will be automatically selected during the enrollment of the device. You need to specify the region in the two-letter ISO 3166-1 format, which is the capitalized region code representing a country. An example of this format is as follows:

Region	ISO 3166-1
United States	US
United Kingdom	UK
Australian	AU

For more information, see <https://www.iso.org/obp/ui/#search>.

NOTE: The defined phone number, email address, or department name, might not be displayed on some iOS devices.

Skip Item Settings: If selected, the following screens related to initial configuration settings are skipped:

- ◆ The **Passcode** screen, which enables the user to create a passcode.

NOTE: If this screen is skipped, then Touch ID and Apple Pay cannot be specified.

- ◆ The **Location Services** screen, which helps in determining the user's current location.
- ◆ The **Restore apps and data** options screen, which enables the user to restore data from backup.
- ◆ The **Move from Android** options screen, which enables the user to migrate data from an Android device. This option will be disabled, if **Restore apps and data** is selected.
- ◆ The **Apple ID** screen, which enables the user to specify the Apple ID.
- ◆ The **Terms and Conditions** screen. If this option is selected, these Terms and Conditions are automatically accepted by the device.
- ◆ The **Touch ID** screen, which enables the user to use biometrics to unlock the device or authenticate to apps. Applicable for iPhone 5s, 6, 6+, iPad Air 2, and iPad Mini 3 only.
- ◆ The **Apple Pay** setup screen, which enables the user to make digital payments. Applicable for iPhone 6, 6+, iPad Air 2, and iPad Mini 3 only.
- ◆ The **Display Zoom** screen, which enables the user to use the standard or zoomed view of the device display. Applicable for iPhone 6 and 6+ only.
- ◆ The **Siri** screen, which enables the user to setup Siri.
- ◆ The **Diagnostics** screen, which enables the user to send diagnostic data to Apple.
- ◆ The **Display Tone** options screen, which enables the user to adjust the white balance on the device display. Applicable for devices that use the True Tone display feature such as iPad Pro.
- ◆ The **Home Button Sensitivity** options, which enables the user to specify how the Home button should be used. Applicable for devices that use the 3D touch-enabled Home button, such as iPhone 7.
- ◆ The **Keyboard** screen, which enables the user to specify the keyboard settings. Applicable on iOS 11.0 and later versions .
- ◆ The **Onboarding** screen, which contains onboarding informational screens. Applicable on iOS 11.0 and later versions .

- ♦ The **Watch Migration** screen, which enables the user to migrate Apple Watch from the previous iPhone to the current device. Applicable on iOS 11.0 and later versions .
- ♦ The **Privacy** screen that controls which apps can access information stored on the device. Applicable on iOS 12.0 and later versions .
- ♦ The **iMessage and FaceTime** screen, which enables users to activate their phone number with iMessage or FaceTime.
- ♦ The **Screen Time** screen, which provides information on the time spent by users on their devices. Applicable on iOS 12.0 and later versions .
- ♦ The **Mandatory software update** screen, which enables users to install the latest software update. Applicable on iOS 12.0 and later versions .
- ♦ The **Screensaver** screen, which enables users to use aerial screensavers on Apple TV. Applicable for tvOS only.
- ♦ The **Touch to Setup** screen, which enables users to set up Apple TV using an iOS device. Applicable for tvOS only.
- ♦ The **Home Screen Sync** screen, which enables users to set up Apple TV's home screen layout. Applicable for tvOS only.
- ♦ The **TV Provider Sign in** screen, which enables users to sign-in to the TV provider. Applicable for tvOS only.
- ♦ The **Where is this Apple TV?** screen. Applicable for tvOS only.
- ♦ The **Device to Device Migration** pane, which enables users to skip the Device to Device Migration pane. Applicable on iOS 13 and later versions .
- ♦ The **SIM Setup** pane, which enables users to skip the Add Cellular Plan pane. Applicable for iPhone XS, iPhone XS Max, iPhone XR.
- ♦ The **Welcome** pane, which enables users to skip the Get Started pane. Applicable on iOS 13 and later versions .

Uploading a Host Certificate for Pairing

The **Allow pairing of devices with a host computer** option appearing in the [Editing General and Skip Item Settings](#), lets iOS devices pair with host devices through the feature called host pairing. If this option is set to **Yes** then the device can pair with any host device. However, if this option is set to **No**, then the device can pair with host devices that have their certificates configured in the DEP profile. This certificate should be configured in the DEP profile for the device to continue pairing with the host device.

To upload the certificate at folder level,

- ♦ Navigate to **Devices > Discovered**. Click **Settings** next to the **Apple DEP Devices** folder. Click **Host Certificates**.

To upload the certificate for a specific device:

- ♦ Navigate to **Devices > Discovered > Apple DEP Devices > <Select a Device> > Settings > Host Certificates**.

On the **Host Certificates** page, click **Add** and upload the certificate obtained using Apple Configurator. The certificate files should be in any one of the following formats:

- ♦ .CER

- ♦ .CRT
- ♦ .DER
- ♦ .PEM

Adding Anchor Certificates to Manage DEP Devices Using a Reverse Proxy

To manage DEP devices using a Reverse Proxy server, Anchor certificates need to be configured. By default, ZENworks packages only a limited set of Anchor certificates with the DEP profile. Hence, in scenarios where a Reverse Proxy is used, more Anchor certificates need to be added.

To add Anchor certificates:

1. Place the CA certificate in the %ZENWORKS_HOME%/conf/security folder of the Primary Server. This CA is the issuer of the reverse proxy server's SSL certificate.
2. Name the certificate as DEP-AdditionalCert.der.
3. Log into ZCC and navigate to **Configuration > Discovery and Deployment > Apple Device Enrollment Program**.
4. (Conditional) If not already done, add the Primary Server as a DEP server.
5. Assign the iOS DEP device to the Primary Server in the Apple Device Enrollment Program (DEP) portal.
6. Configure the required DEP settings by navigating to **Devices > Discovered > Apple DEP Devices (settings) > General and Skip Setup Item Settings**.

NOTE: Every time the DEP-AdditionalCert.der certificate is replaced or changed, the DEP settings have to be modified and applied to make sure that the DEP profile is updated with the newly placed DEP-AdditionalCert.der certificate.

7. Unbox the DEP enabled iOS device, or erase the device if already enrolled, and then boot it up.
8. Complete the setup. The device is listed as a managed device in ZCC.

You can now enroll all the DEP devices and manage them using the Nginx Reverse Proxy Server.

Assigning Users

A DEP device can be assigned to a specific user, which will restrict other users from enrolling the device using Apple DEP. However, the same device can be enrolled through the ZENworks User Portal using another user's credentials. To ensure that the assigned user enrolls using Apple DEP only and not the ZENworks User Portal, disable the **Allow user to skip applying the MDM profile on the device** option appearing in the [Editing General and Skip Item Settings](#).

To assign a user:

1. Navigate to **Devices > Discovered > Apple DEP Devices**.
2. Select a DEP device.
3. On the summary page, click **Edit** next to the **Assigned User** field and specify the user to whom the device should be assigned.

Enrolling a DEP Device

Enrolling a DEP device is simple for an end user, as you can enable the user to skip most of the device activation prompts by modifying the DEP profile.

Turn on the device and follow the setup prompts to enroll the device. After the user configures the Wi-Fi settings, log-in to the device with the user credentials. If the device is assigned to a specific user, then the credentials of only this user should be specified or else enrollment will fail.

After the device enrolls, you can view the **Deployment Status** of the device in ZCC, which should have changed from **Discovered** to **Managed**. You can view this status on the device's summary page. For more information, see [Viewing Device Information](#). The enrolled device object is also created within the **Mobile Devices** folder (**Devices > Mobile Devices**) or in the appropriate folder as defined in the Mobile Enrollment Policy.

NOTE: Before re-enrolling a device, if the ownership (corporate or personal) is modified in the Mobile Enrollment Policy, the modified ownership is not applied on the re-enrolled device. The ownership defined during the initial phase of enrollment is considered.

A device that was enrolled using the ZENworks User Portal is being re-enrolled through Apple DEP using another user's credentials, then ensure that the earlier device object is deleted in ZCC.

Renewing a DEP Token

A token can be renewed in any of the following scenarios:

- ◆ Token has expired
- ◆ A certificate remind has taken place.

To renew a token:

- 1 Navigate to **Configuration > Management Zone Settings > Discovery and Deployment > Apple Device Enrollment Program**.
- 2 Select a DEP Server and click **Renew Token**.

NOTE: The **Renew Token** option can be applied on only one DEP Server at a time. If multiple DEP Servers are selected, then this option will be disabled.

- 3 Click **Download** to download and save the Public Key certificate of the selected MDM Server.
- 4 Click **Deployment Program Web Portal** and sign in using your Deployment Program account credentials. On this portal:
 - 4a Navigate to **Settings** on the left pane of the page.
 - 4b On the left pane, click the MDM Server whose token you would like to renew.
 - 4c Click **Edit** and upload the Public Key of the ZENworks MDM Server that you had saved earlier in the **Upload New** field within **MDM Server Settings**. Click **Apply**.
 - 4d Click **Download Token** and download the token issued by Apple and click **Done**.
- 5 In ZCC, click **Upload** to upload the DEP token issued by Apple to the selected ZENworks MDM Server. This token enables the MDM Server to securely connect with the Apple DEP web service.
- 6 Click **Renew**.

Removing a DEP Server

On removing the DEP Server from the ZENworks Management Zone, the DEP Profile from the associated devices are automatically unassigned. The Discovered devices are removed from the zone but the Managed devices will continue to be managed by the ZENworks MDM Server.

To remove the DEP Server from your ZENworks Management Zone:

1. Navigate to **Configuration > Management Zone Settings > Discovery and Deployment > Apple Device Enrollment Program**.

NOTE: Before removing the DEP Server in ZCC, if you delete the virtual MDM Server in the Apple portal, then the associated DEP Server is not automatically deleted by ZENworks. As a best practice, we recommend that you remove the DEP Server in ZCC and then proceed to remove the virtual MDM Server.

Re-assigning Devices

You can re-assign devices to another virtual MDM Server (assuming that a DEP Server in ZCC already links ZENworks with this virtual MDM Server). After re-assignment, ZENworks deletes and creates a new discovered device object. If a device is re-signed:

- ♦ The Assigned User of this device (if any) is reset.
- ♦ The modified DEP Profile (if any) assigned to the device is reset and the new device object inherits the settings applied to the Apple DEP Devices folder.

Enrolling an iOS Device through Apple Configurator

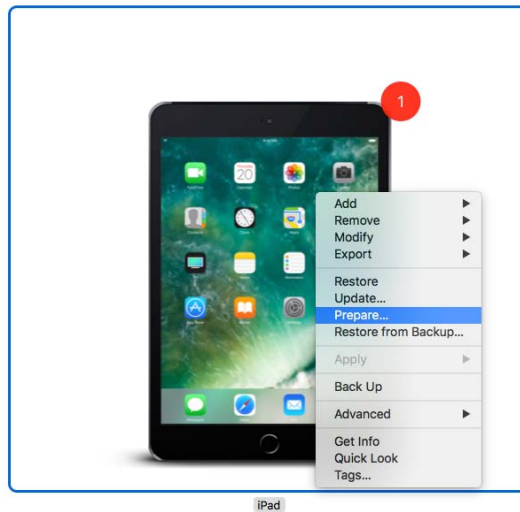
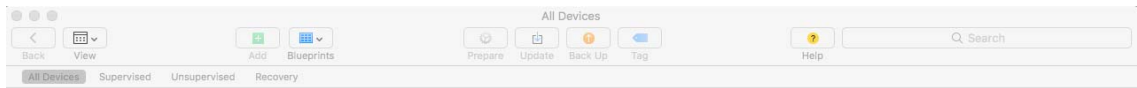
Apple Configurator is a Mac OS X tool that assists administrators in the deployment of iOS devices in business or education settings. Apple Configurator makes reassigning devices quick and simple, allowing the next user to start with a clean slate of content.

Prerequisites

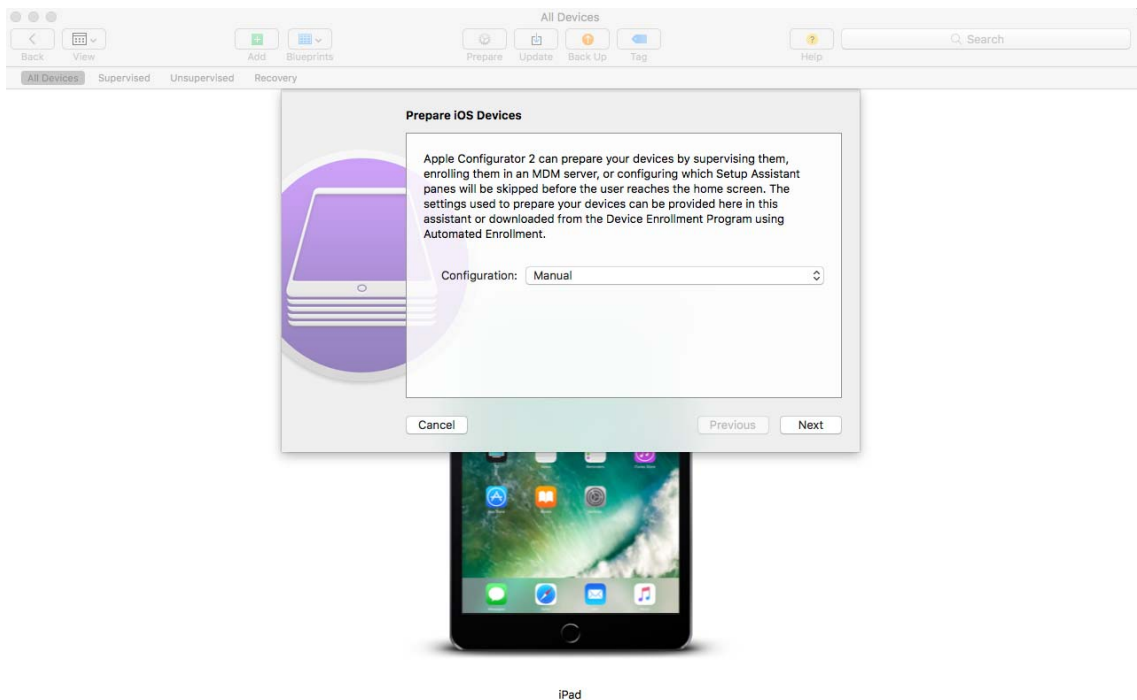
- ♦ Copy the Apple Enrollment URL, which specifies the MDM Server to which the device will enroll. To obtain this, in ZCC navigate to **Configuration > Infrastructure Management > MDM Servers**. Select a MDM Server and click **Apple Enrollment URL**.

Procedure

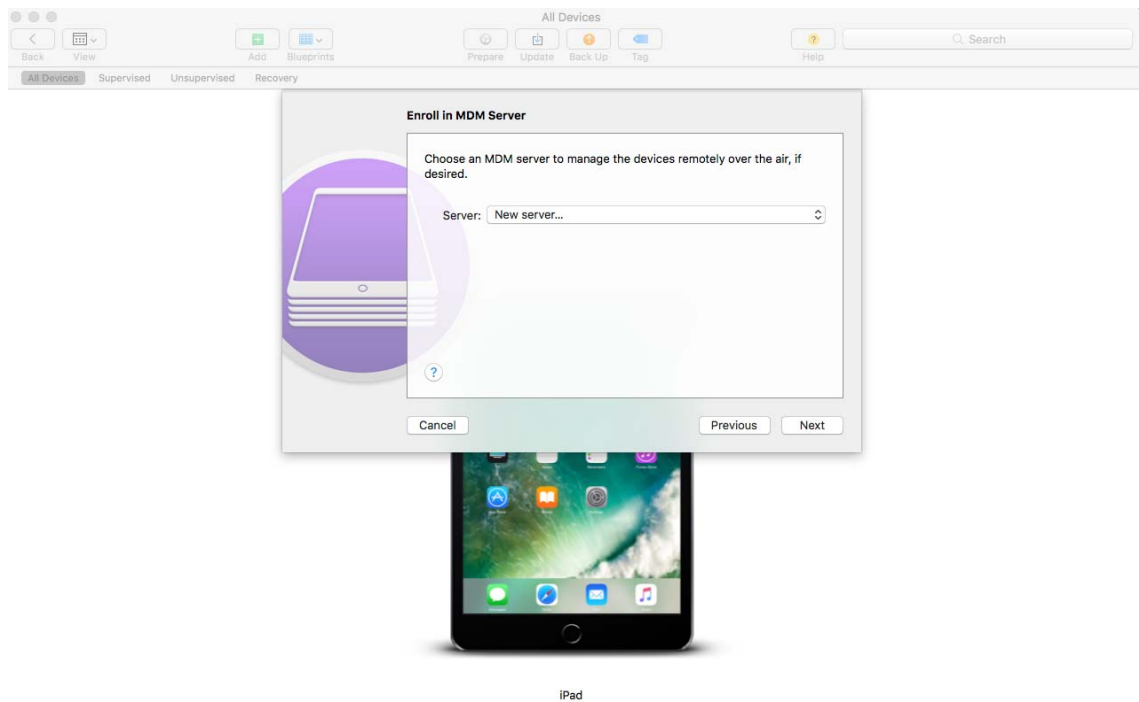
- 1 Connect the device through the USB port to the Mac.
- 2 Right-click and select **Prepare** or select **Prepare** from the top menu bar in the Apple Configurator.



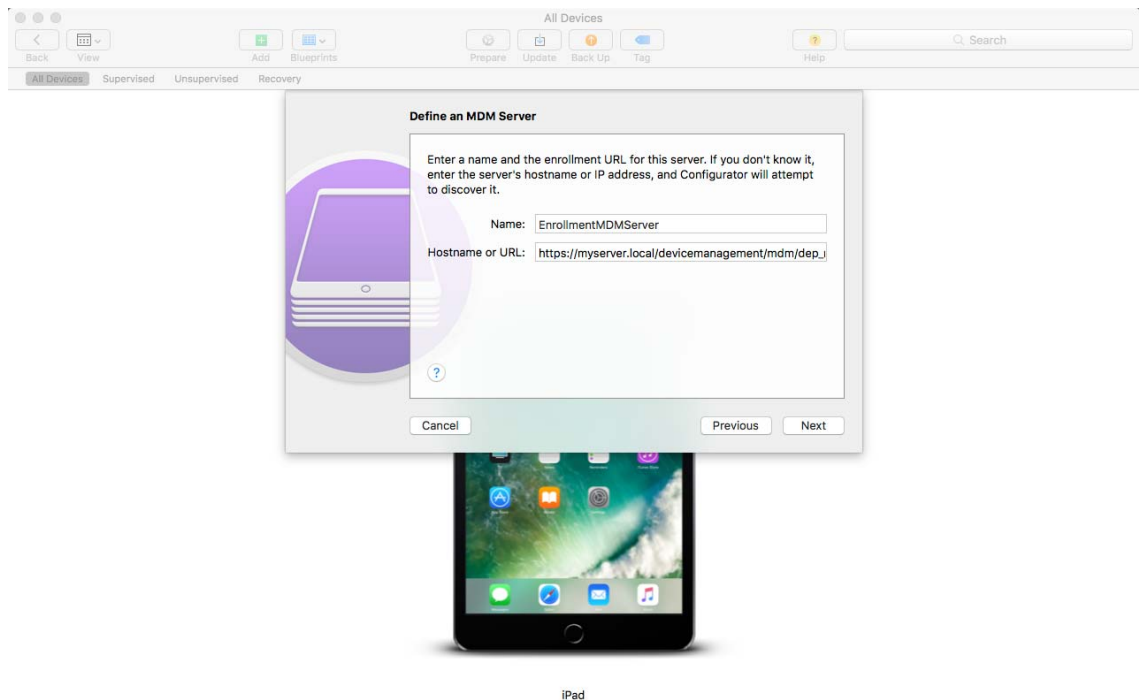
3 Select **Manual** in the **Configuration** drop down menu. Click **Next**.



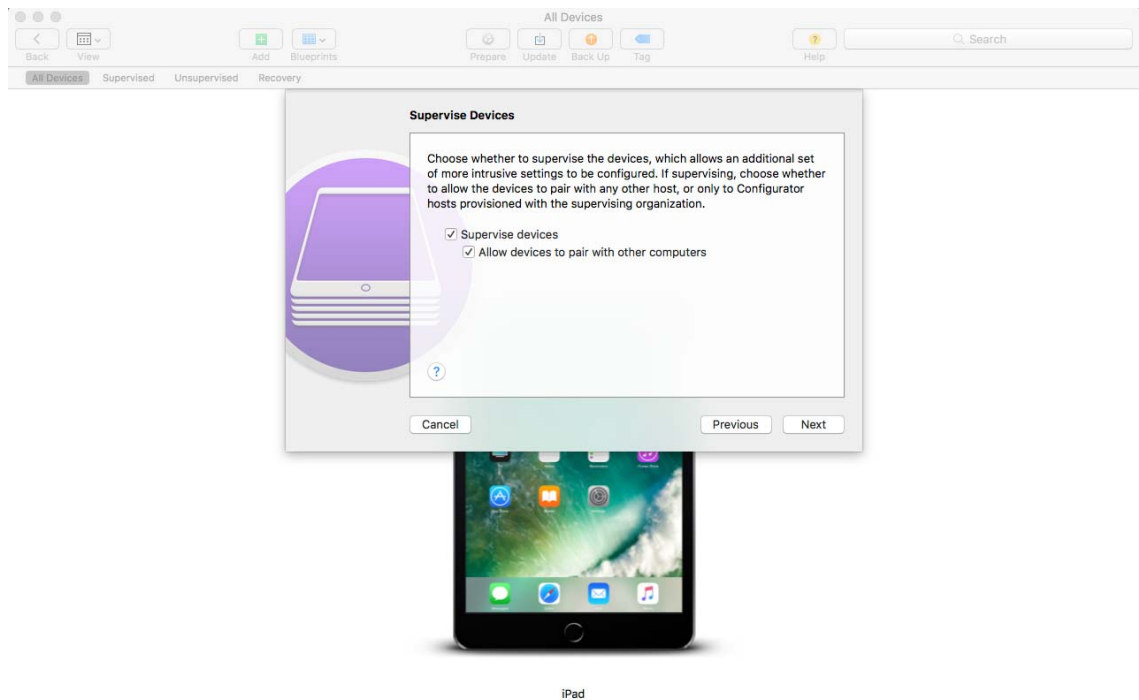
4 Select the MDM Server to which you want the device to enroll. If you do not have the MDM Server saved in the drop-down menu, then select **New Server**.



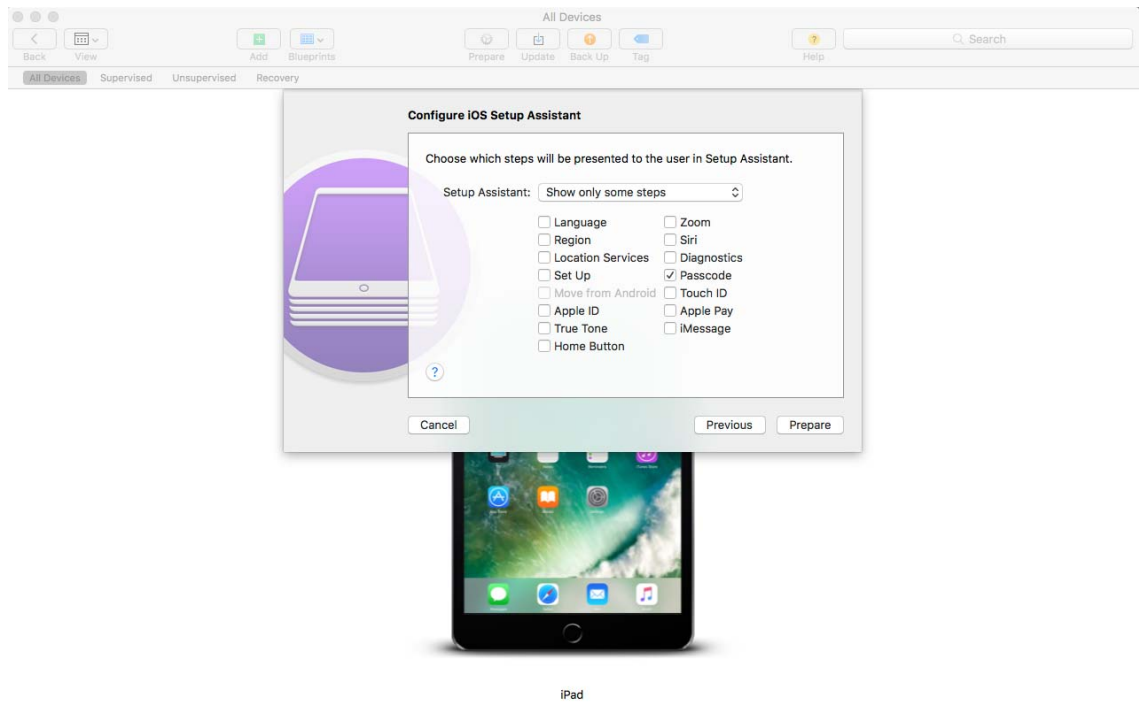
- 5 Specify a name for the server and paste the Apple Enrollment URL copied from ZCC. To obtain this, in ZCC navigate to **Configuration > Infrastructure Management > MDM Servers**. Select a MDM Server and click **Apple Enrollment URL**. Copy the URL and paste it in the Define an MDM Server page in the Apple Configurator. This MDM Server will be saved for future use.



- 6 Select **Supervise devices**, if you want to set the device as supervised. The check box to **Allow devices to pair with other computers** is automatically enabled.



- 7 Select the organization that will supervise these devices.
- 8 Select the appropriate option from the **Setup Assistant** drop-down menu, if you want to skip certain setup steps during enrollment of the device. Check the setup items that should be presented during device enrollment.



- 9 Click **Prepare** to prepare the connected device.

After the preparation stage, the device will reset to its factory settings. After the device is reset, follow the prompts that will be displayed on the device as configured in the **Configure iOS Setup Assistant** page in the Apple Configurator. After entering the Wi-Fi password, the user will be prompted for the user credentials.

After the device enrolls, the device object is created within the Mobile Devices folder (**Devices > Mobile Devices**) or in the appropriate folder as defined in the Mobile Enrollment Policy.

Enrolling an iOS Device Manually

This scenario shows you how to enroll an iOS device as a non-supervised device using the ZENworks User Portal. The following enrollment procedure was performed on an iOS 12.2 device.

- 1 In the Safari browser on the device, enter `ZENworks_server_address/zenworks-eup`, where `ZENworks_server_address` is the DNS name or IP address of the ZENworks MDM Server.

NOTE: Ensure that the Safari browser is not running in the private mode if the iOS version of the device is less than 11.

iOS devices 10.3 and later versions no longer use SHA-1 signed certificates. You need to move to SHA-256 certificates to ensure that the device enrolls to ZENworks successfully. For more information, see [Apple Support \(https://support.apple.com/en-us/HT207459\)](https://support.apple.com/en-us/HT207459).

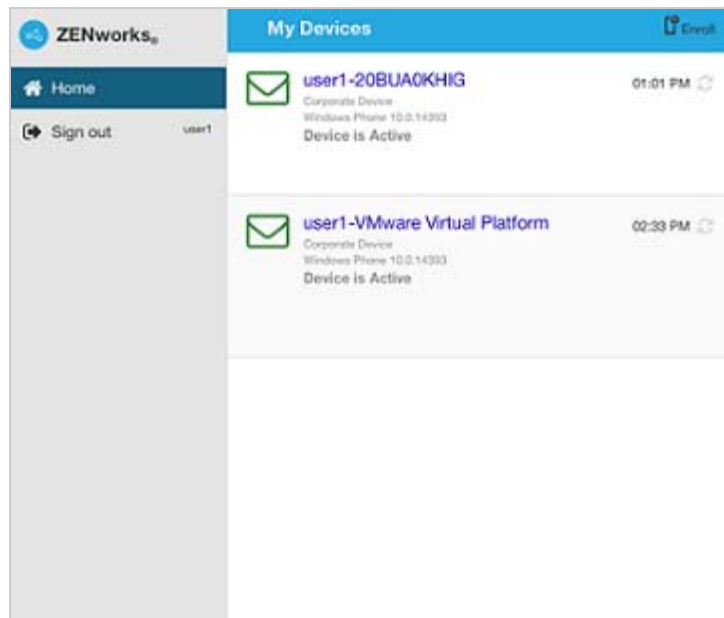
The login screen for the ZENworks User Portal is displayed. You use the ZENworks User Portal to enroll devices to the zone.



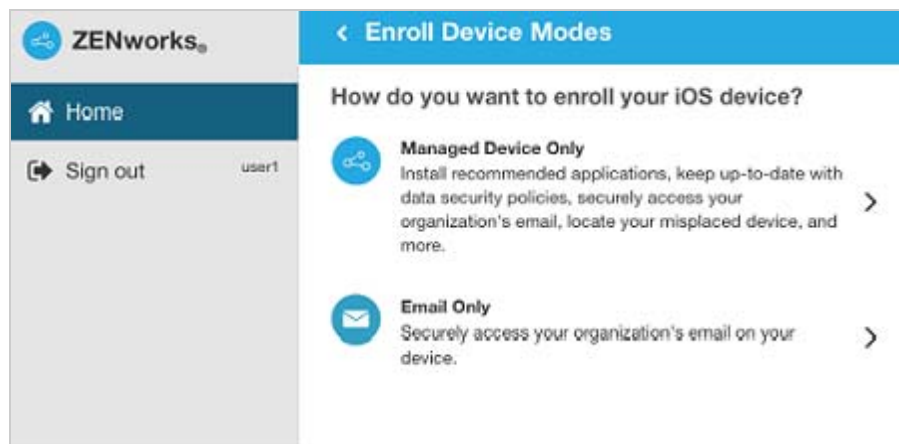
- 2 Enter the user's user name and password. If **Allow Simple Enrollment** option is selected for the user source to which the user belongs, then the registration domain need not be specified or else specify the registration domain. For information, see [Enabling a User Source for Mobile Device Enrollment](#). Tap **Sign In**.

NOTE: If the **Allow Simple Enrollment** option is not enabled or the registration domain name is not configured, then you can specify the configured user source name in the **Domain** field while enrolling a device.

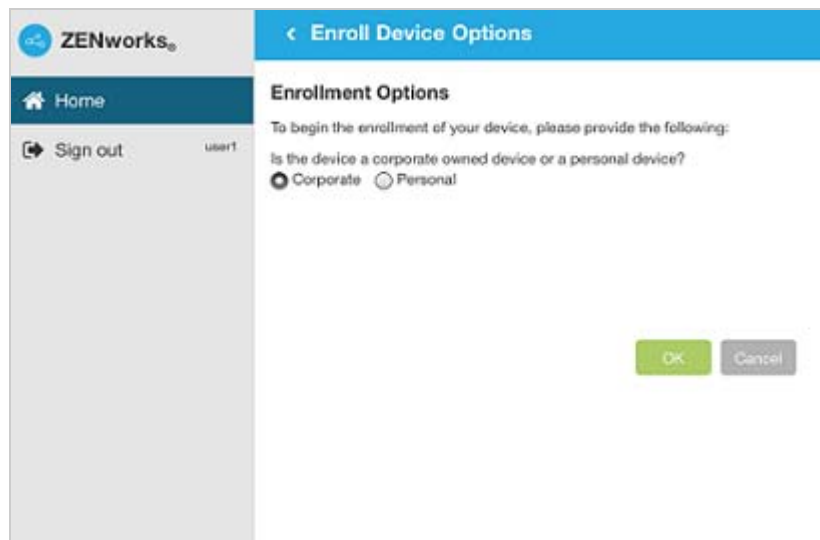
All devices associated with the user, are displayed in the ZENworks User Portal.



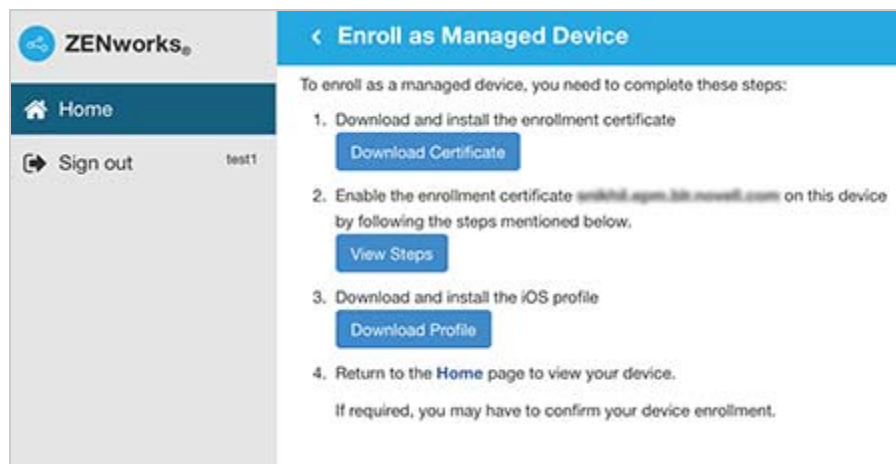
- 3 Tap **Enroll** in the upper-right corner to display the enrollment options for the device. The enrollment options are determined by the user's Mobile Enrollment policy.



- 4 Tap **Managed Device Only** to display the **Enroll Device Options** screen. If you have configured your Mobile Device Enrollment policy to allow the user to specify the device ownership (corporate or personal), you are prompted for that information. Select the appropriate device ownership option and click **OK**.

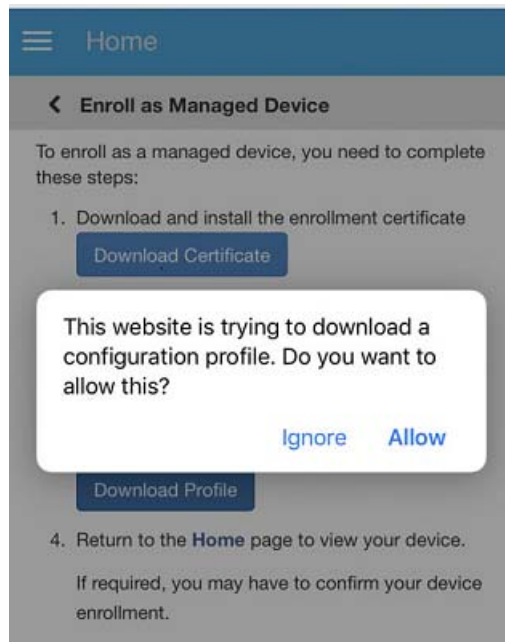


5 Tap Download Certificate.

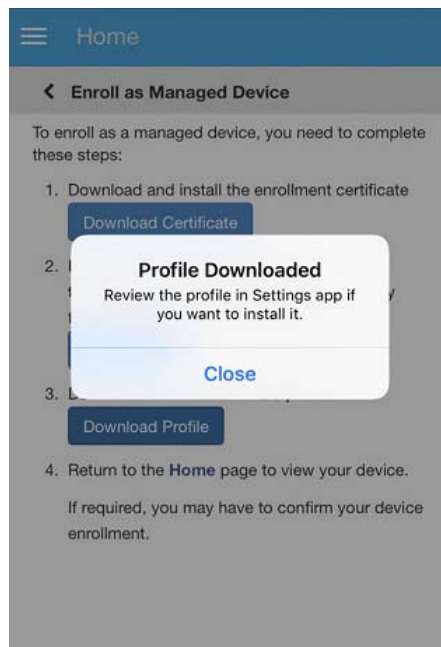


NOTE: If you are enrolling an iOS 12.1.2 or older device, on clicking **Download Certificate**, you will be navigated to the **Install Profile** screen. Click **Install** and follow the prompts to install the profile.

5a Allow the website to download the configuration profile.



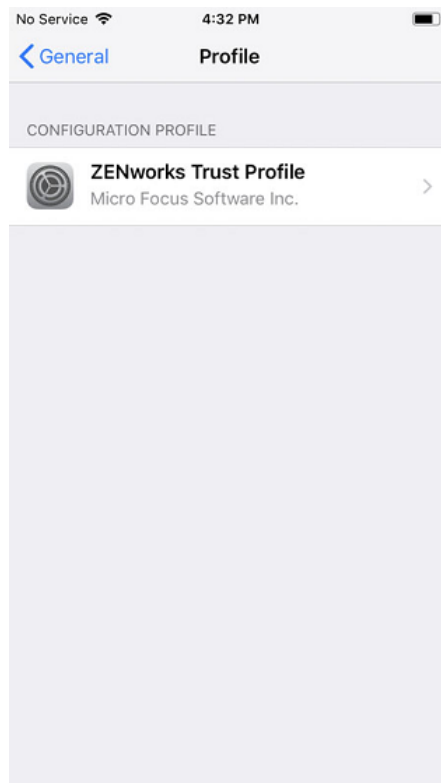
5b The configuration profile will be downloaded. You can now proceed to the **Settings** menu to download the profile.



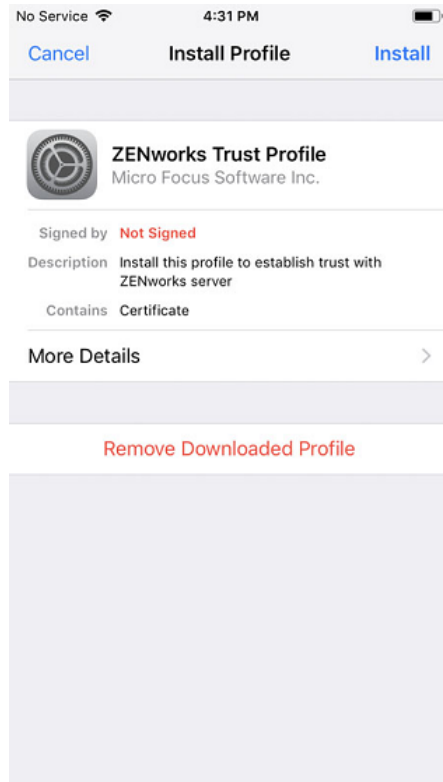
5c Navigate to the **Settings** menu on the device, click **General > Profiles**.



5d Tap ZENworks Trust Profile.



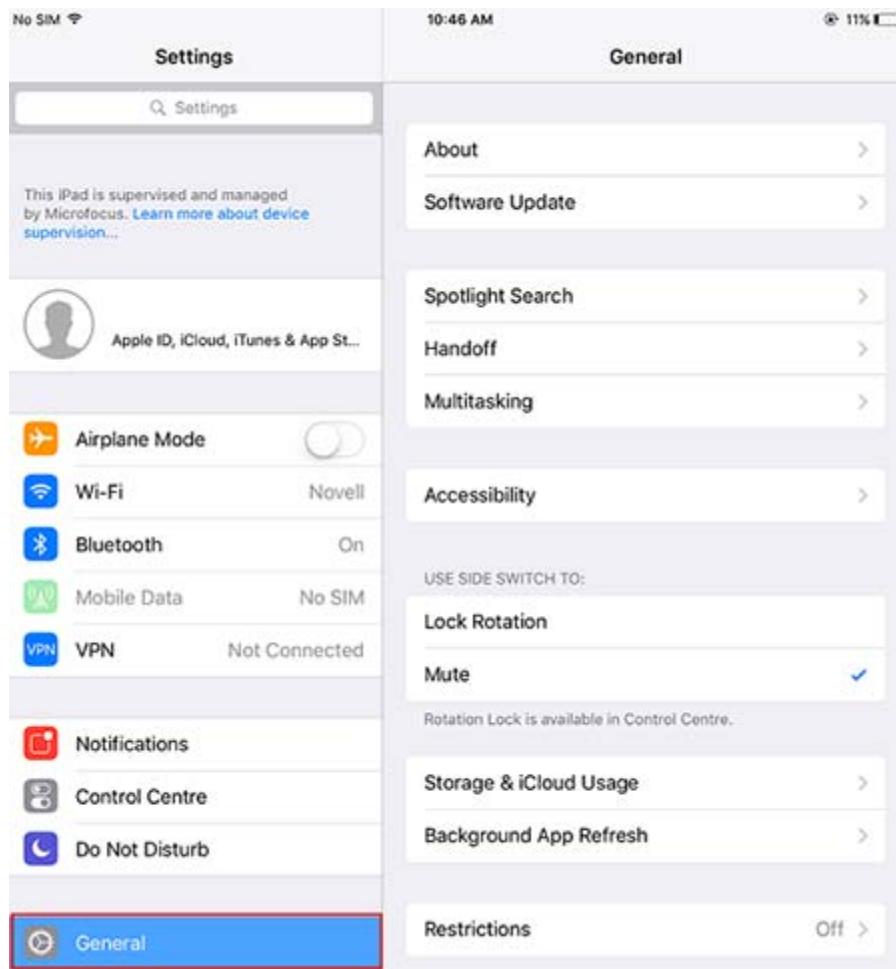
5e Install the profile.



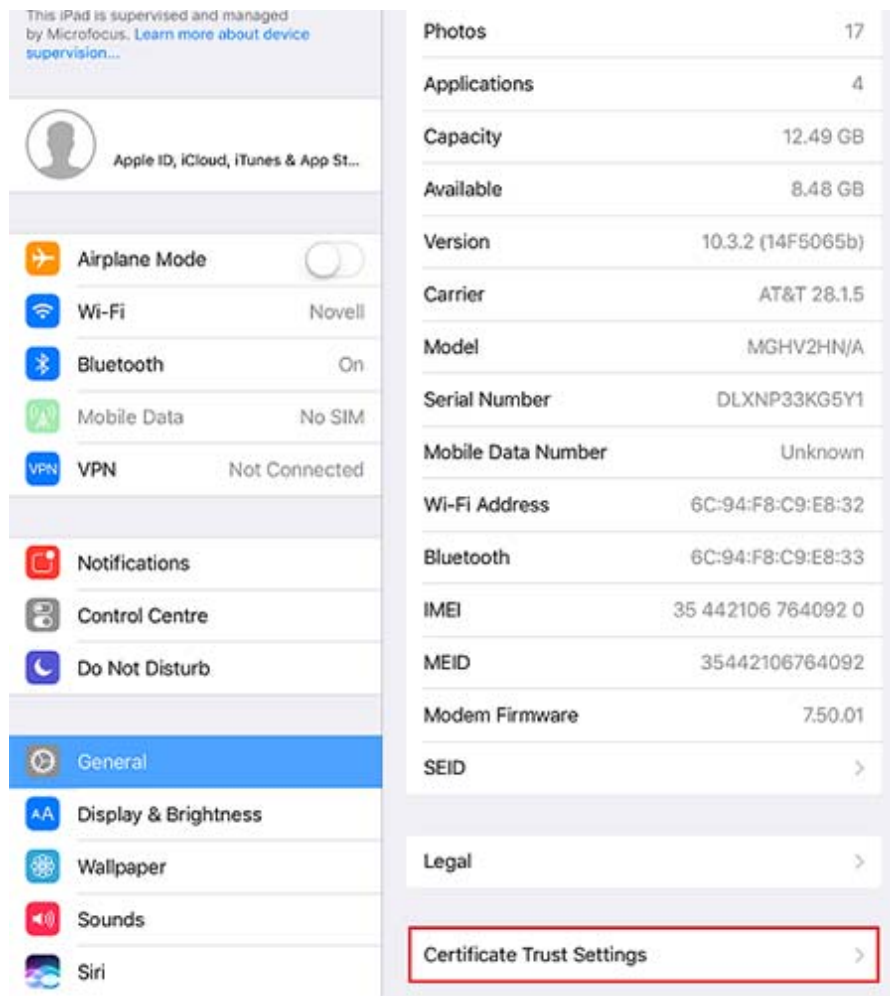
6 Enable the enrollment certificate on the device. To enable the certificate:

NOTE: These steps are not applicable for an iOS 10.2 or older device and you need to proceed with installing the ZENworks Device Enrollment Program Profile.

6a Navigate to the **Settings** menu on the device and click **General > About**.



6b Click Certificate Trust Settings.



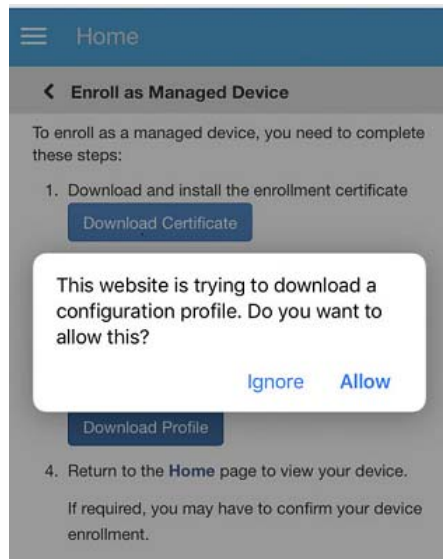
- 6c Enable the root certificate displayed on the screen and follow the prompts to install the root certificate. Navigate back to the EUP page.



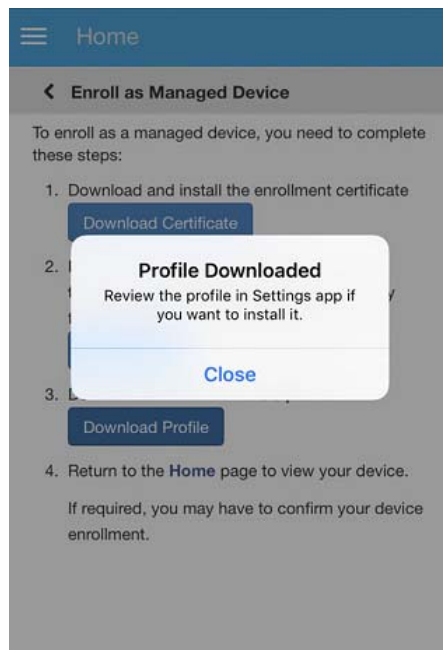
- 7 Tap **Download Profile** in the Enroll as Managed Device screen.

NOTE: If the user is enrolling an iOS 12.1.2 or older device, then on clicking **Download Profile**, the user will be navigated to **Install Profile** screen. Tap **Install** and follow the prompts to install the profile.

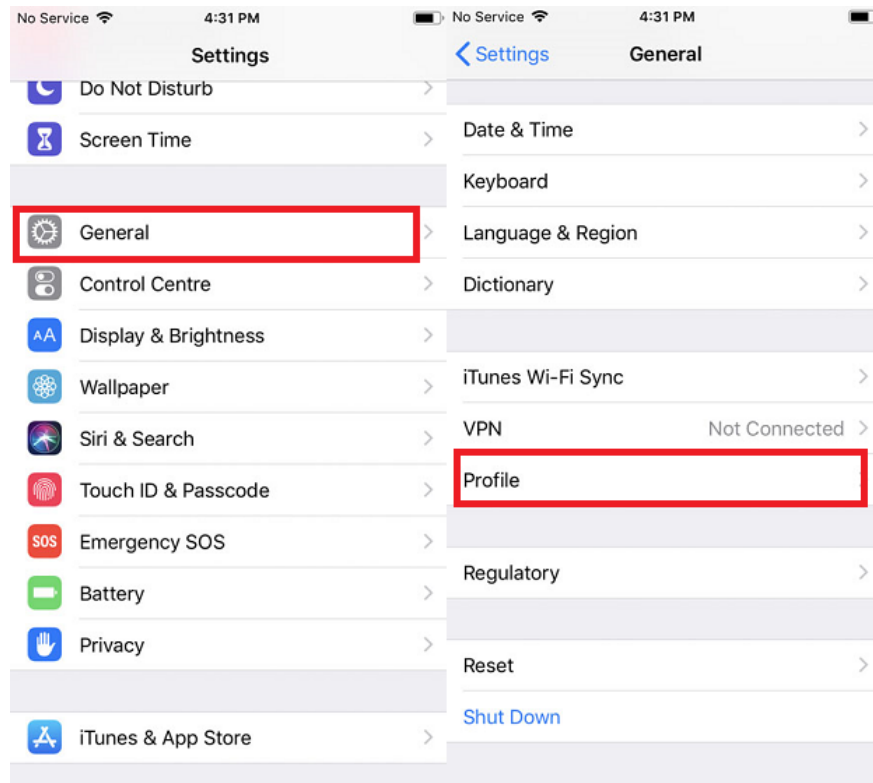
- 7a Allow the website to download the profile.



7b The configuration profile will be downloaded. You can now proceed to the **Settings** menu to download the profile.



7c Navigate to the **Settings** menu on the device to install the profile and tap **General > Profiles**.

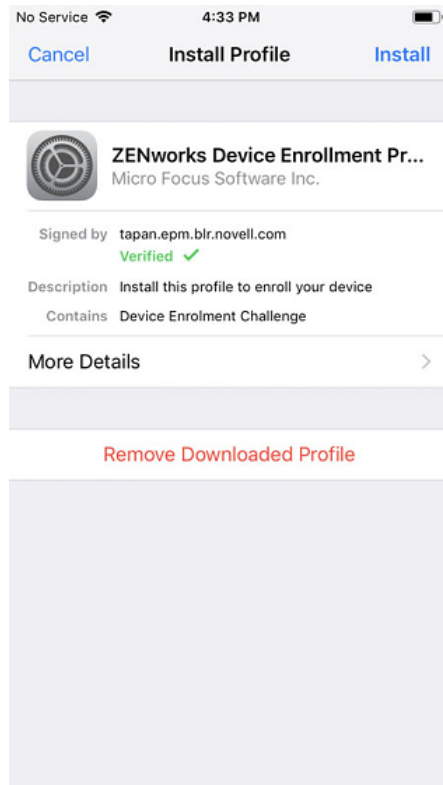


7d Tap ZENworks Device Enrollment Program Profile.



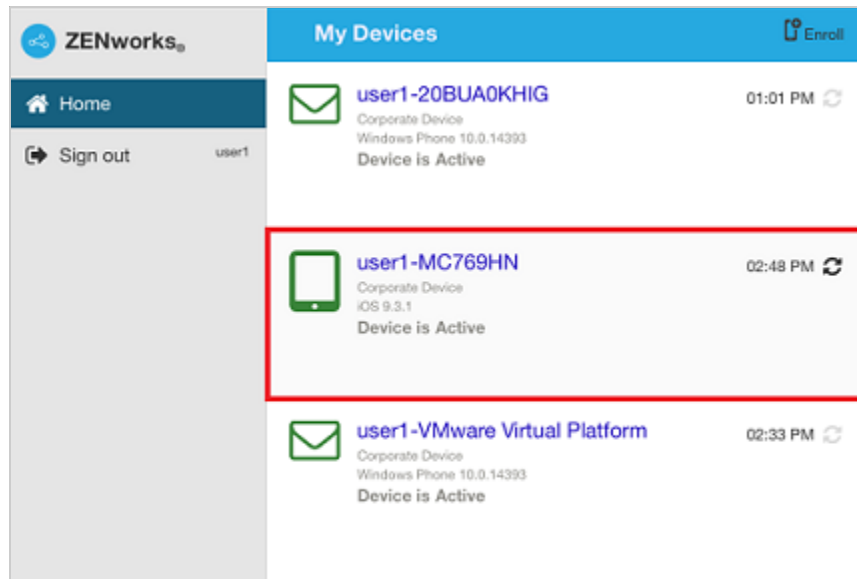
The ZENworks Device Enrollment Program Profile contains the MDM profile required for ZENworks to manage the device.

7e Tap **Install** and follow the prompts to install the profile.



8 Navigate back to the EUP page. The device is displayed in the My Devices list with the status as **Enrollment in Progress**. You need to refresh the browser to update the status to **Device is Active**.

NOTE: If the device remains in **Enrollment in Progress** state for a considerable amount of time, then in the ZENworks User Portal, tap the refresh icon appearing against the device.



At this point in time, you can view the enrollment mode on the Device Information page in ZCC. To view the device information, from the left hand side navigation pane in ZCC, click **Devices > Mobile Devices** (or navigate to the folder as configured in the Mobile Enrollment Policy) and select the appropriate device. The enrollment will be displayed as **iOS MDM**.

- 9 An email account is automatically set up on the device based on the Mobile Email Policy assigned to the user or the device.

NOTE: If an Exchange ActiveSync account was manually configured on the iOS device before it was enrolled, then it should be deleted as an email account will be automatically configured on the iOS device if a Mobile Email policy is assigned.

After the device is enrolled to the ZENworks Management Zone, the enrollment mode of the device is displayed as **iOS MDM + ActiveSync** on the Device Information page in ZCC.

15 Enrolling Android Devices

This section explains the procedure of enrolling Android devices as a fully managed device. ZENworks has stopped support for the basic mode of enrollment that uses the Device Admin API, for Android devices. This comes after Google’s announcement to deprecate the Device Admin API from the Android P release. ZENworks will now support only two ways of enrollment for Android devices; the work profile mode and the work-managed device mode, which are part of the Android enterprise program. For more information on the deprecation of the Device Admin API, see see (<https://community.microfocus.com/collaboration/zenworks/w/zenworkstips/26056/removal-of-the-device-admin-api-for-android-devices>)

IMPORTANT: If a user has already enrolled the device in the basic mode as a part of an earlier ZENworks release, then on upgrading the ZENworks zone to the 2020 version, you need to create an Android Enterprise Subscription and assign the Android Enterprise Enrollment policy to the same user. This will ensure that the user’s device is active in the zone and the device will automatically reconcile to the work profile mode or the work-managed device mode from the basic mode of enrollment. If these prerequisites are not met, then the device is automatically unenrolled and retired.

If the retired device needs to be re-enrolled to the ZENworks 2020 zone, then unretire the device. Ensure that you have an active Android Enterprise Subscription and assign the Android Enterprise Enrollment Policy to the associated user of the unretired device. You can now have the user re-enroll the device in either of the two modes.





- ♦ [“What is Android in the enterprise?” on page 92](#)
- ♦ [“Enrolling the Organization to Android Enterprise” on page 92](#)
- ♦ [“Creating and Assigning Android Enterprise Enrollment Policy” on page 94](#)
- ♦ [“Enrolling Devices in the Work Profile Mode” on page 94](#)
- ♦ [“Enrolling Devices in the Work-managed Device Mode” on page 101](#)
- ♦ [“Enroll Managed Device using a QR code” on page 109](#)

What is Android in the enterprise?

Android in the enterprise is a program for mobile devices running on the Android operating system that enables IT admins to manage and secure mobile business applications on users' devices. ZENworks currently supports the work profile mode and the work-managed device mode of enrollment.

- ♦ The work profile mode, also known as the Profile Owner mode, creates dedicated containers on devices for corporate apps and data, thereby enabling the organization to manage only the corporate data without compromising on the security of the users' personal data. This mode is intended for the BYOD scenario, where the user gets to bring their own devices to the workplace.
- ♦ The work-managed device mode, also known as the Device Owner mode, enables administrators to manage the entire device, thereby restricting the device to corporate use only. This mode is mainly intended for corporate-owned devices.

To know more about Integrating ZENworks with Android Enterprise, you can also refer to the following videos:

 <http://www.youtube.com/watch?v=26o-ouQjOt8>  <http://www.youtube.com/watch?v=k0AuS9wpgsM>  <http://www.youtube.com/watch?v=tNuWRZQEYAc>  <http://www.youtube.com/watch?v=1E9feu9-OBc>

Enrolling the Organization to Android Enterprise

To get started with Android enterprise, you need to first create an Android Enterprise Subscription in ZCC to enroll your organization to the program.

Prerequisites

Before creating the subscription, ensure that following prerequisites are met:

- ♦ You should have a Google ID, preferably a corporate ID, for example: yourid@gmail.com or yourid@companyname.com)
- ♦ At least one MDM server should be configured
- ♦ User source should be configured
- ♦ Firebase Cloud Messaging (FCM) should be configured
- ♦ You should have Novell Customer Center credentials (you need to have an active ZENworks maintenance entitlement)

Procedure

To create the Android Enterprise Subscription:

1. In ZENworks Control Center, click **Subscribe and Share**.
2. In the Subscriptions panel, click **New** and select **Subscription**.
3. Select **Android Enterprise Subscription**, and click **Next**.

4. In the **Define Details** page, perform the following:
 - a. **Subscription Name:** Specify a name for the subscription.
 - b. **Folder:** Type the name or browse and select the ZENworks Control Center folder where you want the subscription to reside.
 - c. **Description:** Provide a short description for the subscription.
5. In the **Configure Android Enterprise** page, specify the Novell Customer Center (NCC) credentials, and click **Enroll**.

NOTE: Ensure that you have disabled the pop-up blocker for the ZCC page.

You will be re-directed to a sign-up UI page hosted by Google Play.

- a. In the Google sign-up page, click **SIGN IN**.
 - b. Specify the corporate email ID or Google ID and password. Click **Next**.
 - c. Click **GET STARTED**.
 - d. Follow the prompts to complete the registration process.
 - e. Click **COMPLETE REGISTRATION** after which you will be redirected back to ZCC.
6. In ZCC, click **Next**.
 7. In the **Select User Context** page, select user contexts that you want to associate with the Android enterprise management, and then click **Next**. Users that are part of the selected user context will be allowed to enroll their devices in the work profile or work-managed device modes, using this subscription. However, you also need to ensure that an Android Enterprise Enrollment Policy is assigned to these users. For more information, see [Enrolling Mobile Devices](#).
 8. In the **Select Languages** page, select the languages in which the app details should be fetched from Google. The retrieved details will be used to display app details in the Apps Catalog page and information within a bundle such as permissions and managed configurations.

NOTE: Selecting multiple languages might result in delays while retrieving app details.

9. Specify the frequency to run Android Enterprise Subscription, based on which the ZENworks server initiates a connection with the Google server to retrieve the latest information about the associated apps, their permissions, manage configuration, and update the information in the Android App bundle created.

You can choose to run the schedule at a daily or hourly interval. By default, the frequency is configured as Daily, 23:00 hours (11:00 PM).

Click **Finish** to complete creating the Android enterprise subscription.

Creating and Assigning Android Enterprise Enrollment Policy

Along with the Mobile Device Enrollment Policy, to enroll an Android device, you also need to create and assign an Android Enterprise Enrollment Policy. While assigning this policy, you need to ensure that it is assigned to the same set of users who are part of the user context associated with the Android Enterprise Subscription.

To create an Android Enterprise Enrollment Policy:

- 1 Click **Policies** in the left hand pane in ZCC.
- 2 Click **New > Policy**.
- 3 Select **Mobile** and click **Next**.
- 4 Select **Android** and click **Next**.
- 5 Retain the default selection, **Android Enterprise Enrollment Policy**, and click **Next**.
- 6 Specify a policy name, a policy folder and a short description of the policy. Click **Next**.
- 7 Review the summary page and click **Finish**.

To assign this policy to relevant users:

- 1 In the **Policies** panel, select the policy you want to assign.
- 2 Click **Action > Assign to User**.
- 3 Follow the prompts to assign the policy.

NOTE: For this policy, device assignments are supported only for those devices that have already been enrolled using the Device Admin API (the basic mode of enrollment) and need to be re-enrolled to the zone in the work profile or work-managed device mode. From the ZENworks 2017 Update 4 release onwards, the basic mode of enrollment has been deprecated.

When you complete the wizard, the assigned users are added to the policy's Relationships page. You can click the policy to view the assignments.

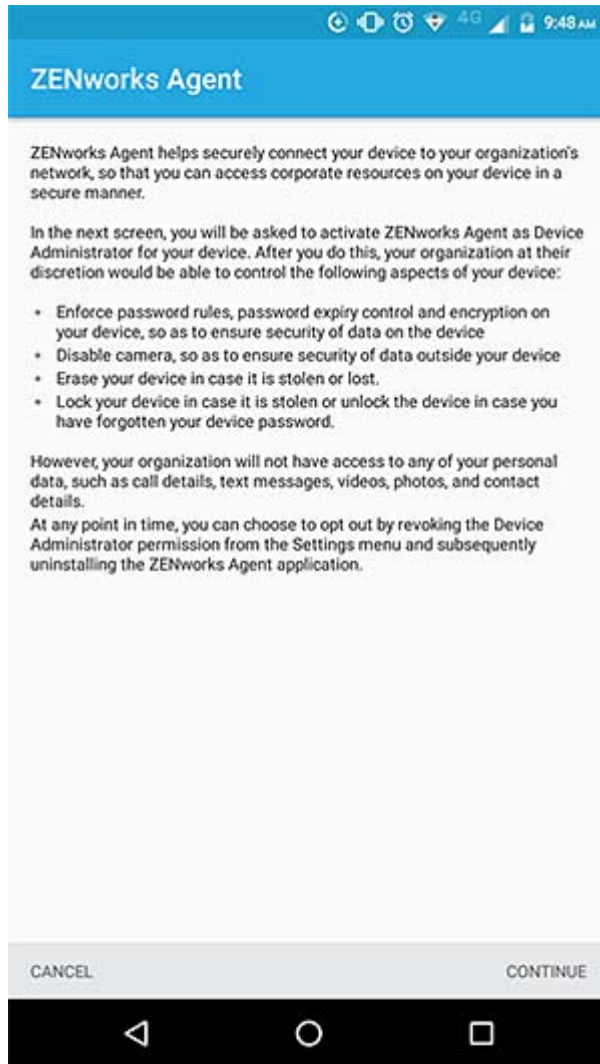
Enrolling Devices in the Work Profile Mode

The scenario elaborated in this section is meant for users who are enrolling their devices to ZENworks for the first time. For users who have already enrolled their devices in the basic mode (Android App only) and want to enroll in the work profile mode, see [Work Profile Enrollment for Existing Users](#).

IMPORTANT: Work profile enrollment fails if the device is connected over a Virtual Private Network (VPN).

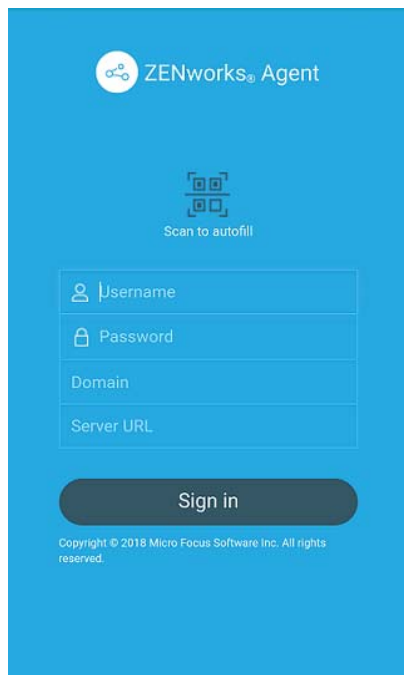
Procedure

- 1 The user installs the ZENworks Agent App from Google Play Store. Alternatively, the user can follow the procedure mentioned in the invite letter to download the ZENworks Agent app.
- 2 After installation, the user clicks **Open**. A brief description of the ZENworks Agent is displayed. The user clicks **Continue**.

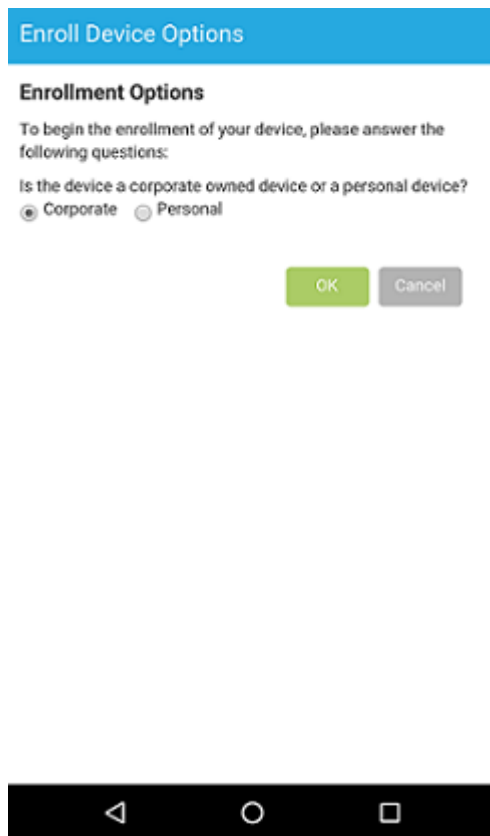


- 3 The user logs into the app by specifying the following:
Username, Password, Domain, Server URL: Specify the username, password, and registration domain (if **Allow Simple Enrollment** is disabled for the user) along with the server URL of the ZENworks MDM Server.

Alternatively, the user can also scan the QR code in the Invite Email to autofill the login credentials. To do this, tap **Scan to autofill** in the ZENworks Agent app. If the user has enabled the permission to allow ZENworks to access the device camera, then the camera will automatically open and the user needs to point the camera to the QR code appearing in the **To enroll an iOS, BlackBerry or Windows mobile devices** section of the default Invite Email. After scanning the QR code, the user is redirected to the ZENworks Agent App, in which all the login details are automatically filled and the user has to only specify the login password.

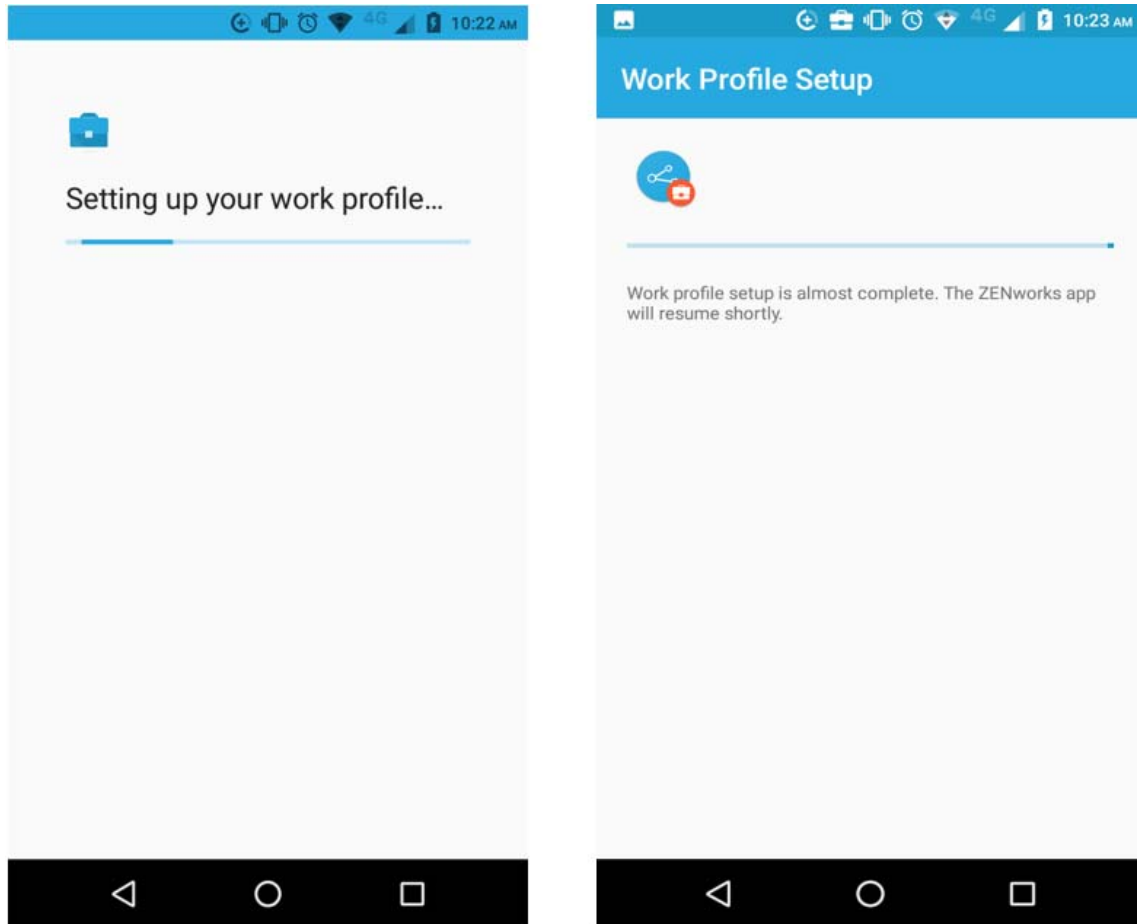


- 4 If you have configured the Mobile Enrollment policy to allow the user to specify the device ownership (corporate or personal), the user is prompted for that information. Tap **OK**.

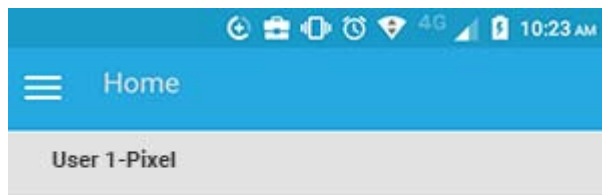


- 5 Follow the prompts appearing in the remaining screens and the device will automatically set up a work profile and enroll to ZENworks. The following screens are displayed during work profile setup.

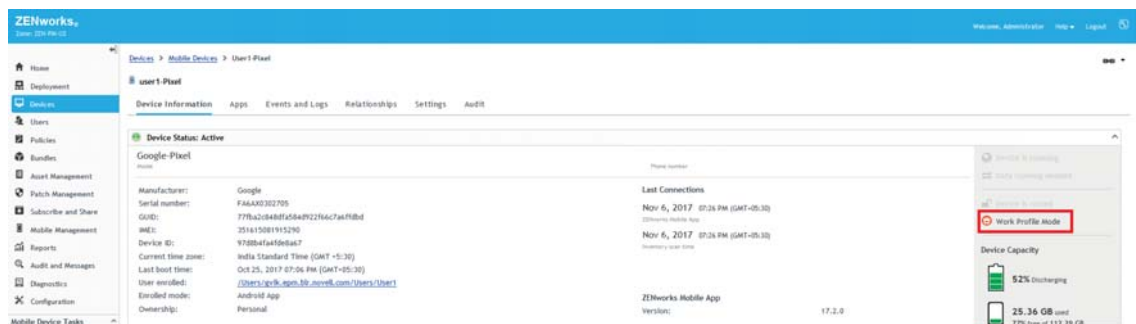
NOTE: Ensure that the user does not interrupt the work profile setup process.



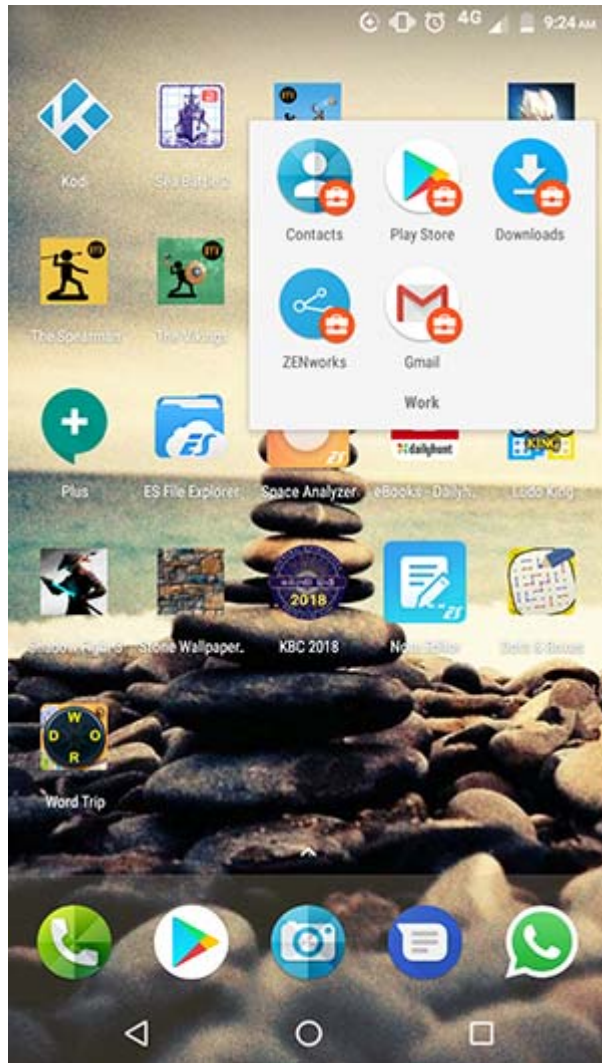
- 6 The ZENworks Agent App Home screen is displayed that shows the device as enrolled and active.



- The device information can now be viewed in ZCC. Click **Devices > Mobile Devices** (or navigate to the folder as configured in the Mobile Enrollment Policy) from the left hand navigation pane in ZCC. Click the appropriate device and view its details in the **Summary** page. The enrollment mode is displayed as **Android App** and **Work Profile Mode** is also enabled.



- 8 After your device is enrolled, a Badge icon attached to the ZENworks Agent App icon and other system apps will help differentiate work apps from personal apps.



Using managed configurations, you can remotely configure the corporate email account within the work profile of a device using apps such as Gmail. Therefore, it is recommended that you do not assign a Mobile Email Policy to devices that are to be enrolled in the work profile mode. Also, the ActiveSync account should directly communicate with the configured ActiveSync server rather than using ZENworks as the proxy.

Ensure that you approve the ZENworks Agent app, installed within the work profile, in managed Google Play and assign it to all the users. This ensures that the user is notified of any updates made to the ZENworks Agent app and these updates are applied automatically.

NOTE: On an Android 8.0+ device that has a device password already enabled, ZENworks will send a notification to confirm the existing device credentials (PIN, pattern or passcode) immediately after enrollment. When the user confirms the device credentials, the **Reset Password Enabled** status displayed on the Device Information page in ZCC, is activated. This will enable you to send the **Unlock Device** quick task, if the user forgets the device's credentials. For more information on this quick task, see [Unlocking a Device](#).

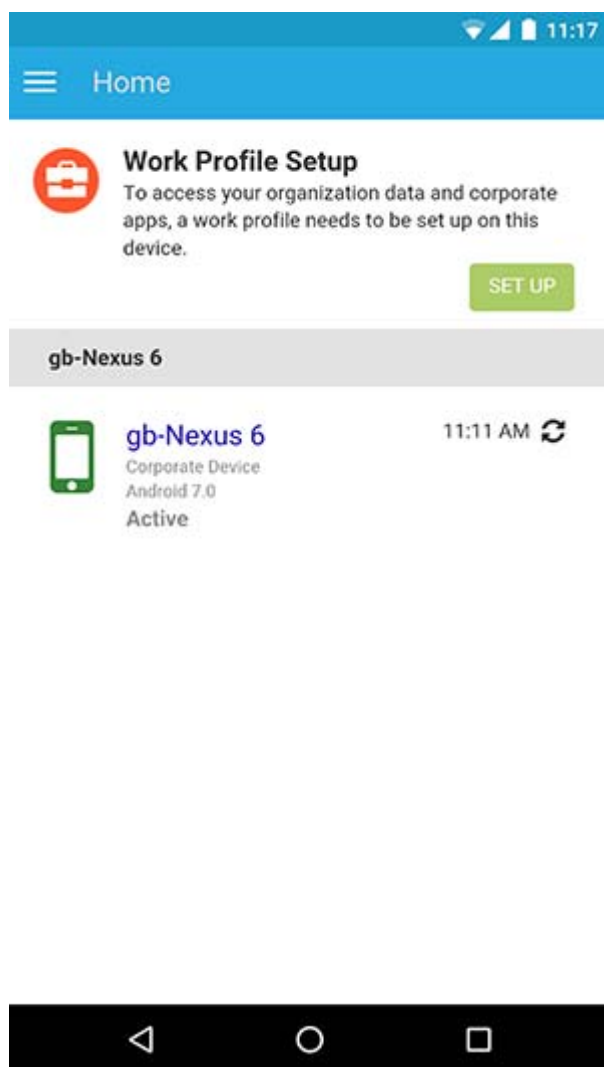
Work Profile Enrollment for Existing Users

For users who have already enrolled to ZENworks using the basic mode of enrollment (Android App only) and now want to be enrolled in the work profile mode, assign the Android Enterprise Enrollment Policy to these users.

NOTE: If you have already configured an ActiveSync account, then it is recommended that you remove this account. With managed configurations, you can remotely configure the corporate email account within the work profile of a device using apps such as Gmail. The ActiveSync account should directly communicate with the configured ActiveSync server rather than using ZENworks as the proxy.

For users who have already enrolled in the basic mode, it is recommended that you enable the **Allow Manual Reconciliation by User** setting in the assigned Mobile Enrollment Policy, till all the users are enrolled in the work profile mode. This will allow users to manually reconcile their devices to the existing device objects present in ZCC, if required,

After assigning the Android Enterprise Enrollment Policy, the users receive a notification on their devices to set up a work profile when they open the ZENworks Agent app.



The user clicks **Set Up** and follows the prompts to set up the work profile. The device will automatically set up the work profile. You can view **Work Profile Mode** enabled in the device's information page in ZCC (**Devices > Mobile Devices ><Click the device> > Summary**).

Enrolling Devices in the Work-managed Device Mode

To enroll an Android device as a work-managed device, the user needs to start up the device. For an existing user or if the user has already turned the device on and completed device setup, a factory reset of the device will be required.

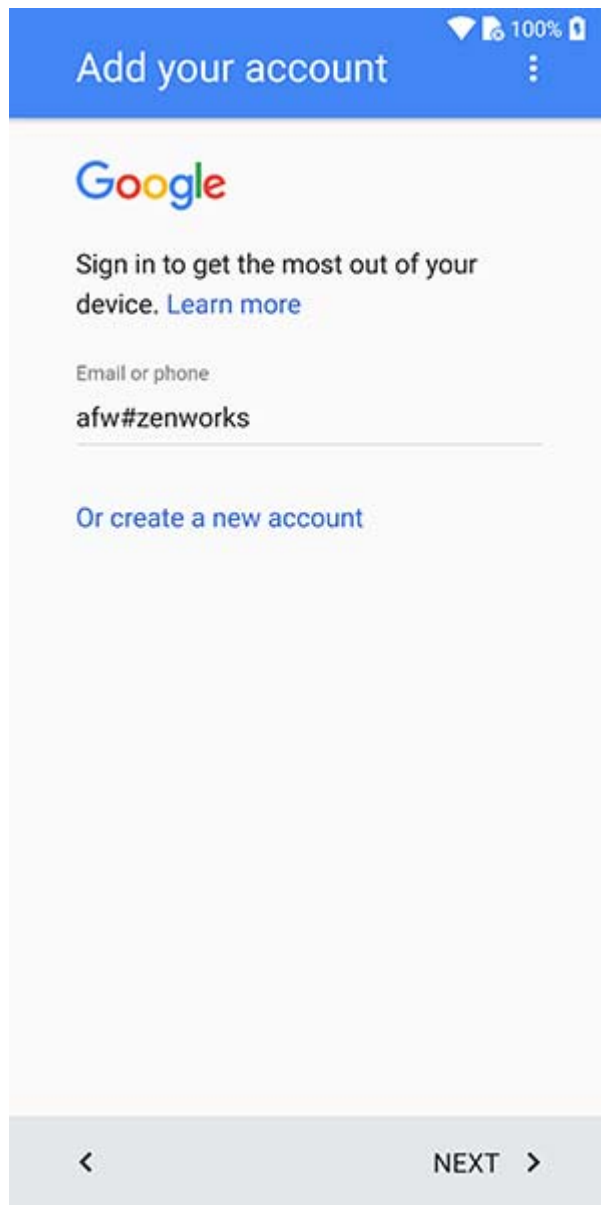
You can enroll Work Managed devices in the following ways:

- ◆ [“Enroll using AFW identifier” on page 101](#)
- ◆ [“Enroll using a QR code” on page 108](#)

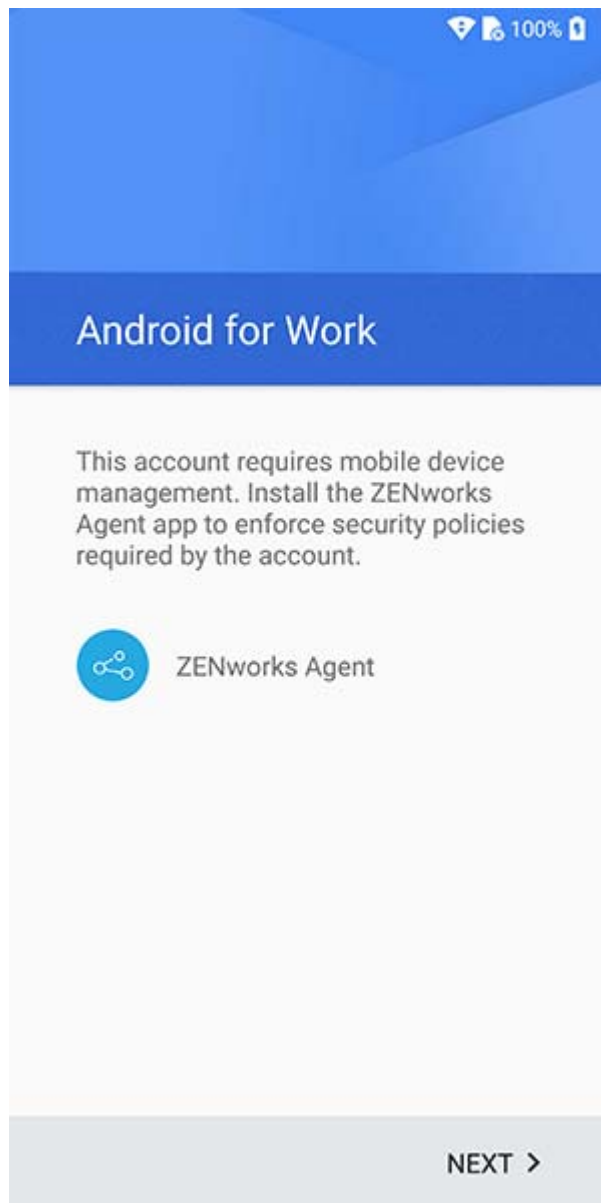
Enroll using AFW identifier

Procedure

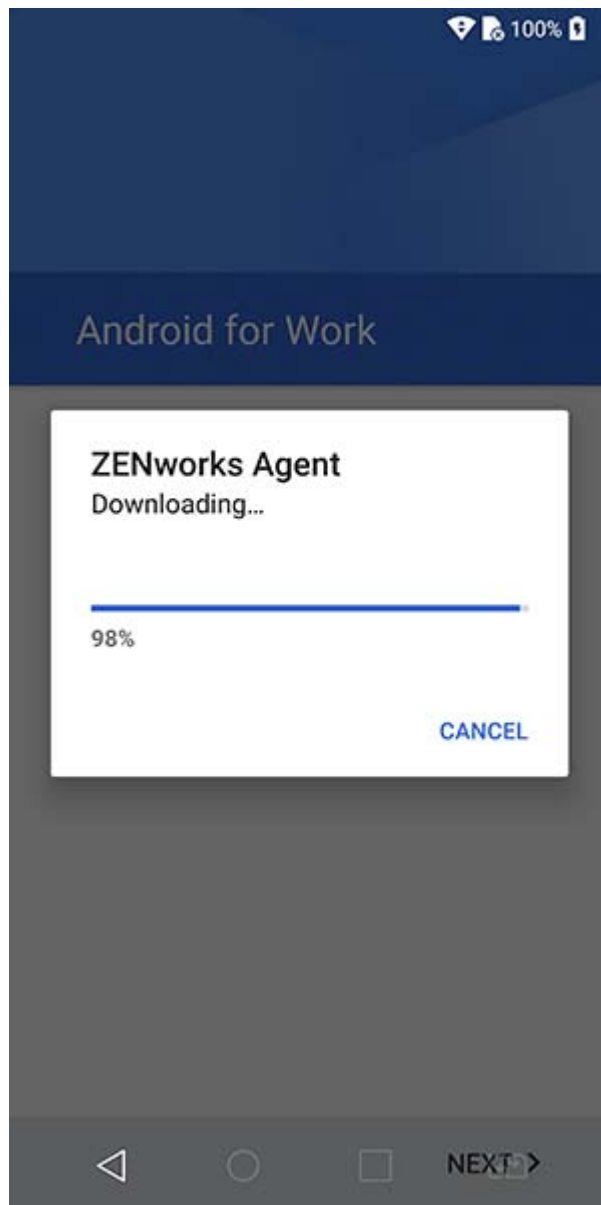
- 1 Follow the initial setup screens such as language setup and Wi-Fi configuration.
- 2 Specify the AFW identifier (afw#zenworks) in the Email field in the Add your Account setup screen.



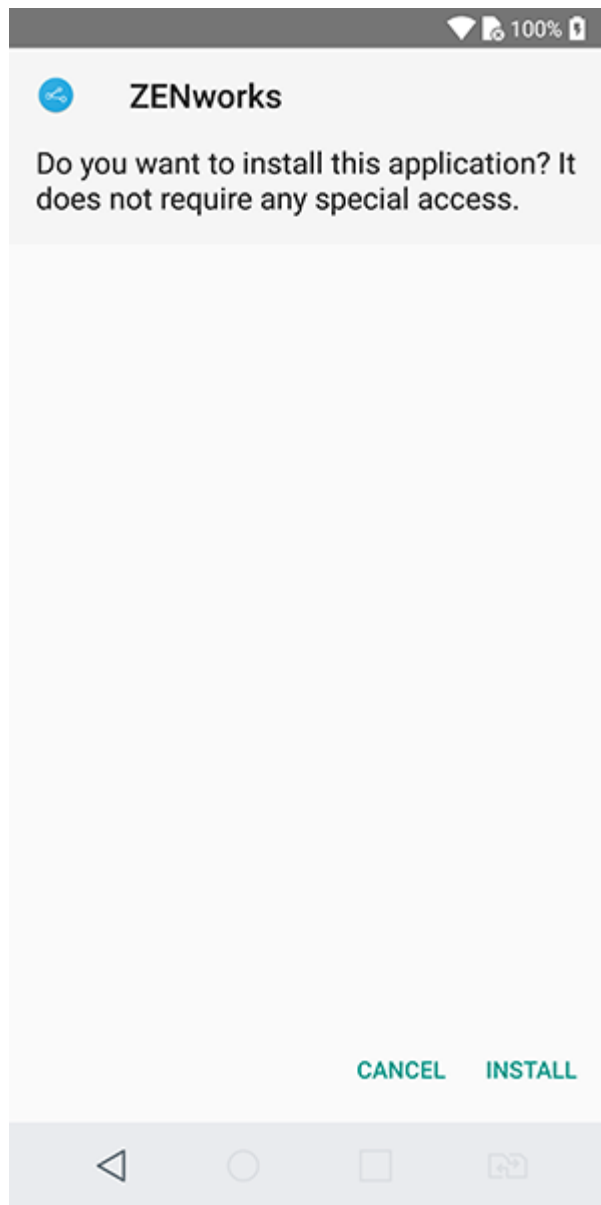
- 3 Click **Next** in the Android for Work page to proceed with the ZENworks App installation.



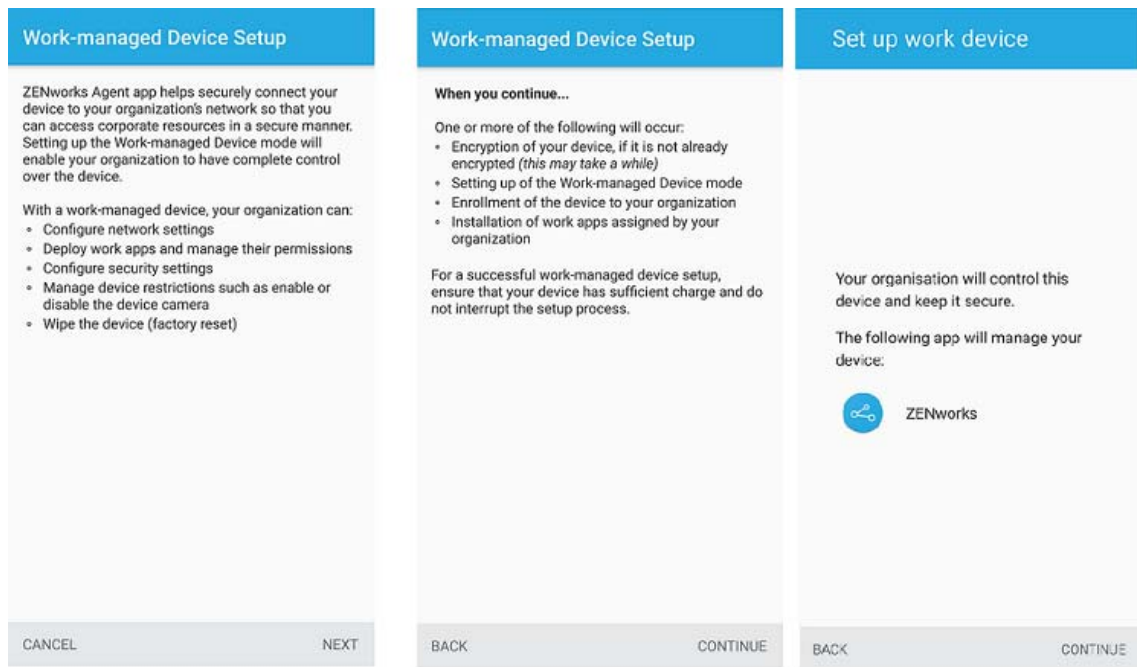
The ZENworks agent app will be automatically downloaded on the device.



- 4 Click **Install** to install the app on the device and follow the prompts to complete setting up the device.



- 5 Follow the prompts appearing in the remaining screens to set up a work-managed device. The following screens are displayed:

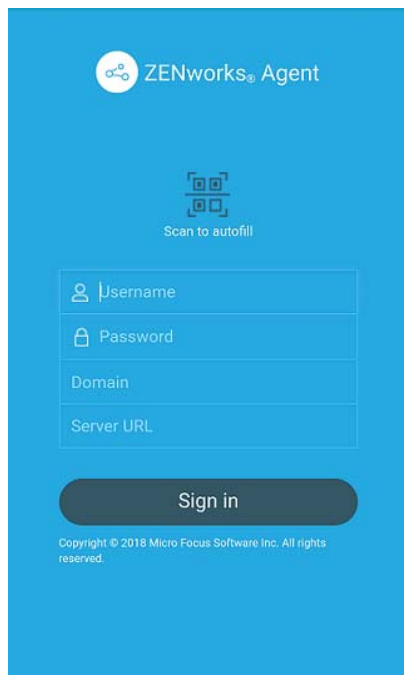


- 6 The device is now setup but is yet to be enrolled as a work-managed device. Search for the ZENworks Agent app on the device and log in with the following details to start the enrollment: *Username, Password, Domain, Server URL*: Specify the username, password, and registration domain (if **Allow Simple Enrollment** is disabled for the user) along with the server URL of the ZENworks MDM Server.

NOTE

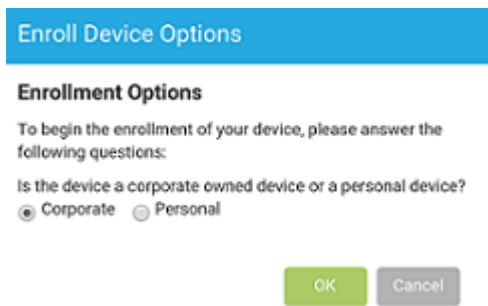
- ◆ If instead of the login screen, the device’s home screen is displayed, then open the ZENworks Agent App from the Applications Menu on your device.

Alternatively, the user can also scan the QR code in the Invite Email to autofill the login credentials. To do this, tap **Scan to autofill** in the ZENworks Agent app. If the user has enabled the permission to allow ZENworks to access the device camera, then the camera will automatically open and the user needs to point the camera to the QR code appearing in the **To enroll an iOS, Blackberry or Windows mobile devices** section of the default Invite Email. After scanning the QR code, the user is redirected to the ZENworks Agent App, in which all the login details are automatically filled and the user has to only specify the login password.



The work-managed device is automatically setup on the device.

- 7 If you have configured the Mobile Enrollment policy to allow the user to specify the device ownership (corporate or personal), the user is prompted for that information. Tap **OK**.



- 8 The device information can now be viewed in ZCC. Click **Devices > Mobile Devices** (or navigate to the folder as configured in the Mobile Enrollment Policy) from the left hand navigation pane in ZCC. Click the appropriate device and view its details in the **Summary** page. The enrollment mode is displayed as **Android App** and **Work-managed Device Mode** is also enabled.

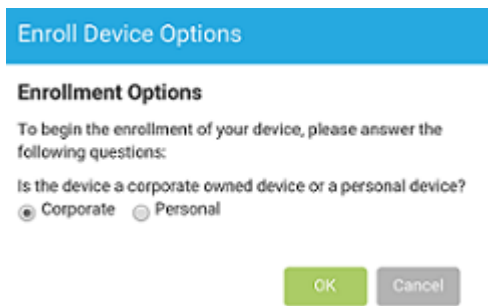
NOTE: On an Android 8.0+ device that has a device password already enabled, ZENworks will send a notification to confirm the existing device credentials (PIN, pattern or passcode), immediately after enrollment. When the user confirms the device credentials, the **Reset Password Enabled** status displayed on the Device Information page in ZCC, is activated. This will enable you to send the **Unlock Device** quick task, if the user forgets the device’s credentials. For more information on this quick task, see [Unlocking a Device](#)

You can now distribute work apps, such as Gmail, to the device. Unlike in the work profile mode, a badge icon will be not be attached to work apps distributed to work-managed devices.

Enroll using a QR code

Procedure

- 1 Perform the steps in the [“Enroll Managed Device using a QR code”](#) on page 109 section and then continue with the steps here.
- 2 If you have configured the Mobile Enrollment policy to allow the user to specify the device ownership (corporate or personal), the user is prompted for that information. Tap **OK**.



- 3 The device information can now be viewed in ZCC. Click **Devices > Mobile Devices** (or navigate to the folder as configured in the Mobile Enrollment Policy) from the left hand navigation pane in ZCC. Click the appropriate device and view its details in the **Summary** page. The enrollment mode is displayed as **Android App** and **Work-managed Device Mode** is also enabled.

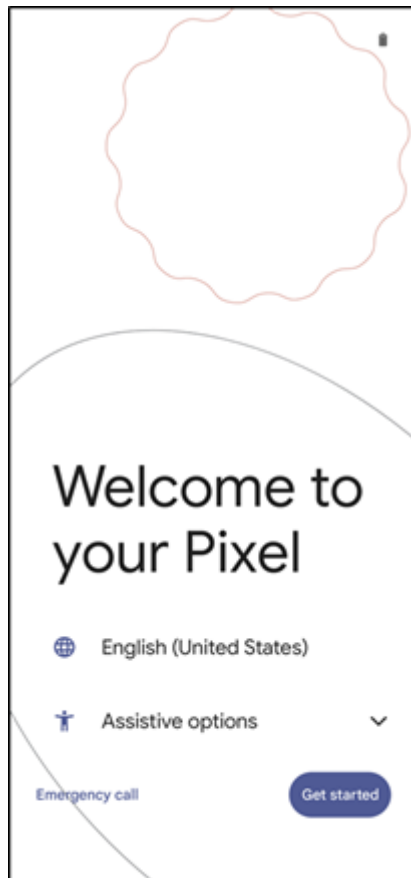
NOTE: On an Android 8.0+ device that has a device password already enabled, ZENworks will send a notification to confirm the existing device credentials (PIN, pattern or passcode), immediately after enrollment. When the user confirms the device credentials, the **Reset Password Enabled** status displayed on the Device Information page in ZCC, is activated. This will enable you to send the **Unlock Device** quick task, if the user forgets the device's credentials. For more information on this quick task, see [Unlocking a Device](#)

You can now distribute work apps, such as Gmail, to the device. Unlike in the work profile mode, a badge icon will not be attached to work apps distributed to work-managed devices.

Enroll Managed Device using a QR code

To enroll devices in the work-managed device mode, perform these steps on your Android device:

- 1 In the **Welcome** screen, tap the screen six times in the same spot.

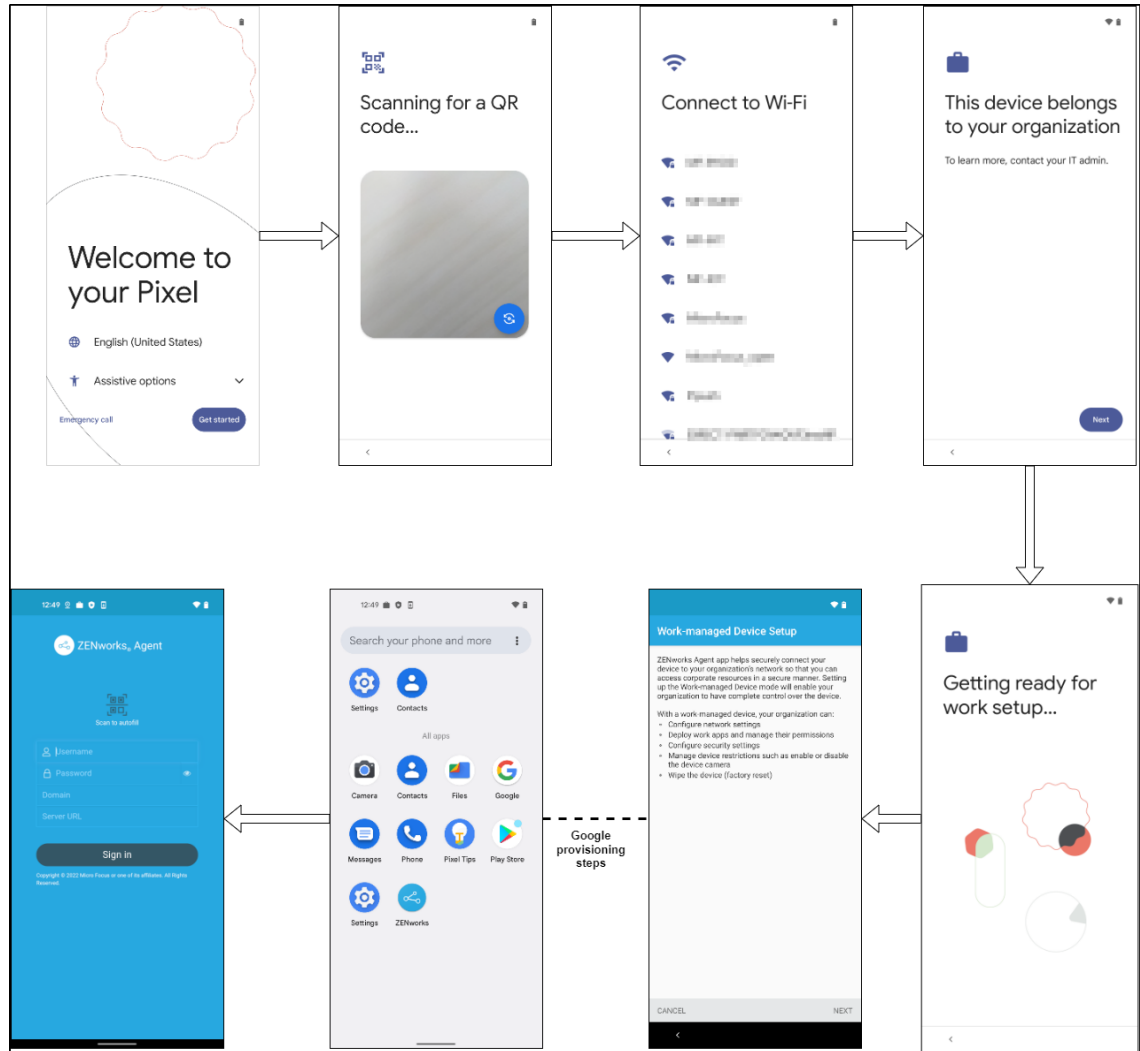


- 2 Download the ZENworks Agent apk to a local machine.
- 3 Calculate the checksum of the downloaded apk using the below command:

```
cat '<ZENworks Agent APK path>' | openssl dgst -binary -sha256 | openssl  
base64 | tr '+/' '-_' | tr -d '='
```
- 4 Upload the APK to any HTTP server and copy the URL to download this apk.
- 5 Using the below data generate the QR code

```
{  
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME":  
  "com.novell.zapp/  
  .framework.content.broadcastreceivers.DeviceAdminEnablementReceiver",  
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM":  
  "<apk checksum>",  
  
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION  
  ": "<apk download url>"  
}
```
- 6 Scan the QR code.
- 7 Google will provision the device.
Once the provisioning is done, search and open the ZENworks App.

8 Log in to the ZENworks app.



16 Enrolling an Email Only Device

This scenario shows you how to enroll a device as an Email Only device in your ZENworks Management Zone. This scenario details the procedure to enroll an iOS device as an Email Only Device.

- 1 In a browser on the device, enter `ZENworks_server_address/zenworks-eup`, where `ZENworks_server_address` is the DNS name or IP address of the ZENworks MDM Server.

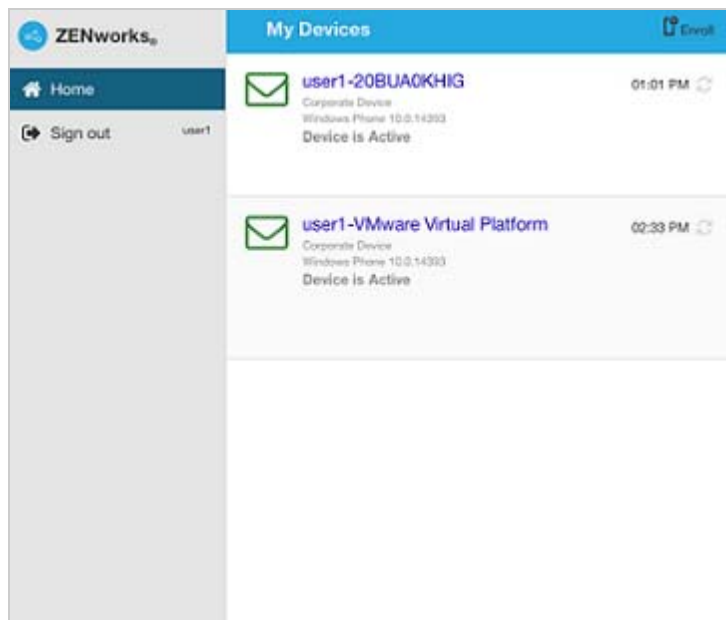
The login screen for the ZENworks User Portal is displayed. You use the ZENworks User Portal to enroll the device.



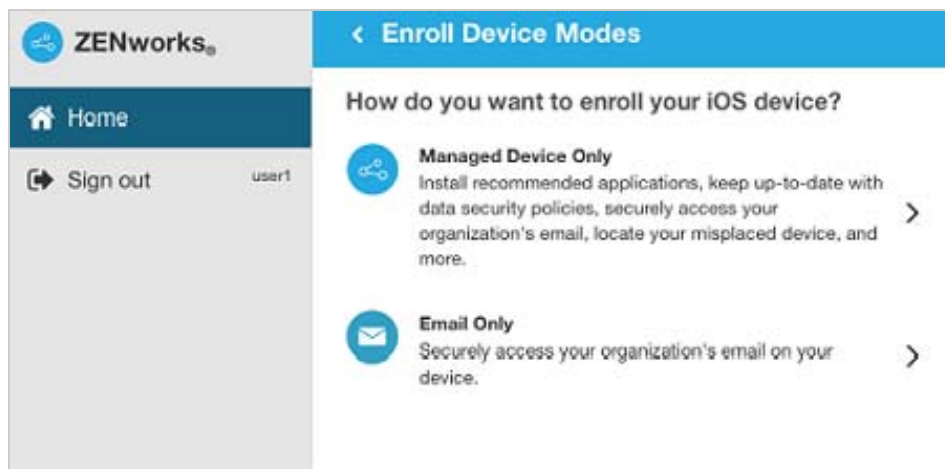
- 2 Enter the user's user name and password. If **Allow Simple Enrollment** option is selected for the user source to which the user belongs, then the registration domain need not be specified or else specify the registration domain. For information, see [Section 6.1, "Enabling a User Source for Mobile Device Enrollment,"](#) on page 25. Tap **Sign In**.

NOTE: If the **Allow Simple Enrollment** option is not enabled or the registration domain name is not configured, then you can specify the configured user source name in the **Domain** field while enrolling a device.

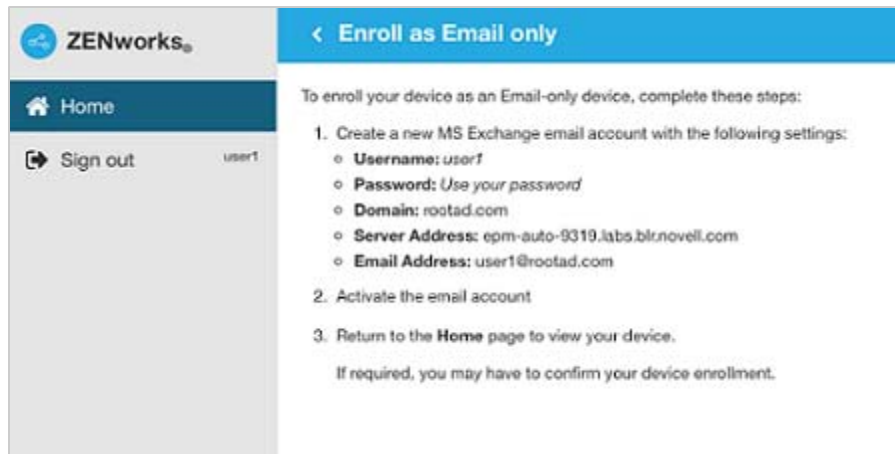
All devices associated with the user, are displayed in the ZENworks User Portal.



- 3 Tap **Enroll** on the upper-right corner, to display the enrollment options for the device. The enrollment options are determined by the user's Mobile Enrollment policy. For details, see [Creating and Assigning a Mobile Enrollment Policy](#).



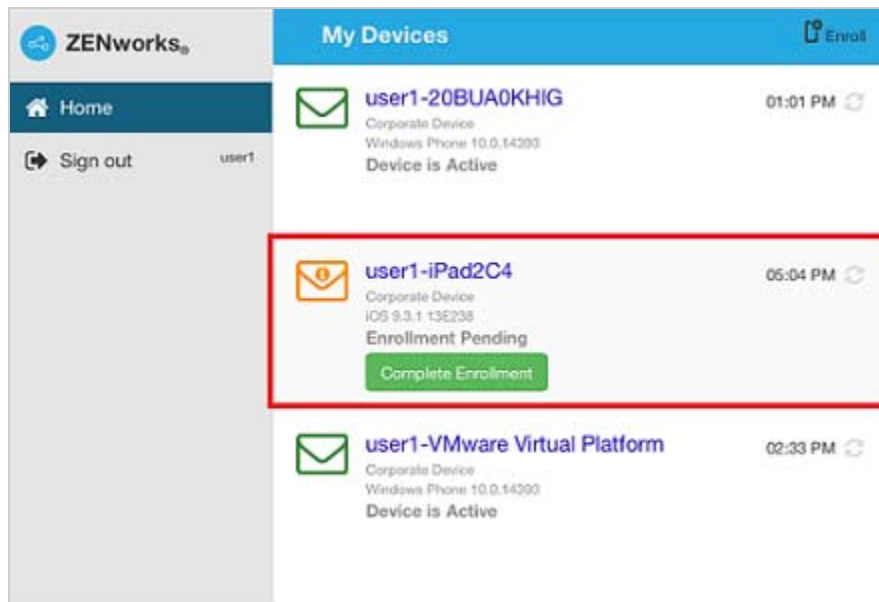
- 4 Tap **Email Only** to display the **Enroll as Email Only** screen. Use the displayed information to create an email account for the user.



- 5 After the user configures the email account, an email is sent to the user stating that the enrollment process needs to be completed. You can edit the contents of this email in ZCC, by navigating to **Configuration > Management Zone Settings > Event and Messaging > Email Notifications**. Click the relevant email and edit its contents.

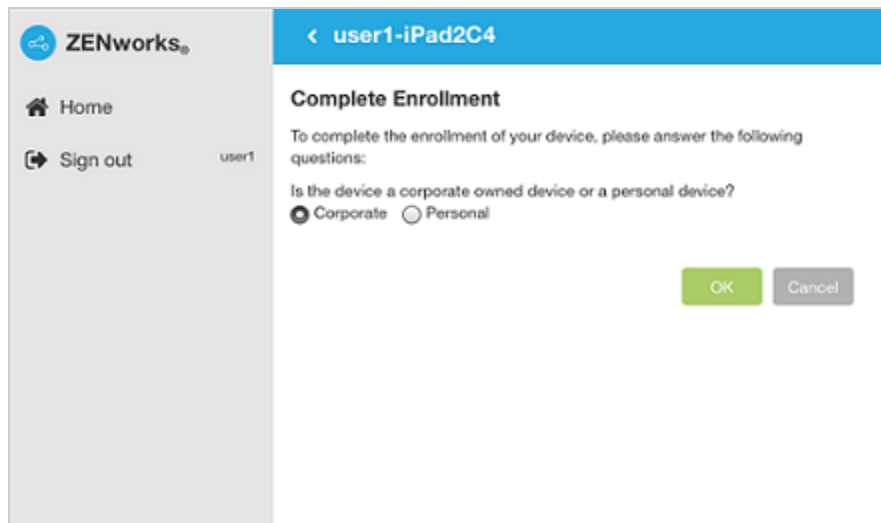
To complete the enrollment process, click the link to the ZENworks End User Portal provided in the email or visit the ZENworks End User Portal as described in [Step 1](#).

- 6 On the ZENworks User Portal, the device is displayed in the My Devices list. At this point, the device has been added to the ZENworks Management Zone but is pending enrollment.

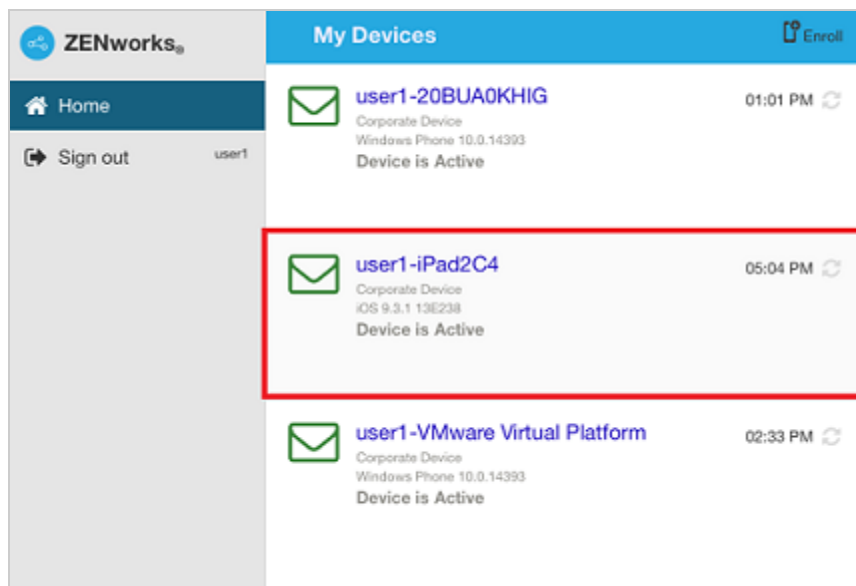


7 On the device, tap **Complete Enrollment**.

If you configured your Mobile Enrollment policy to allow the user to specify the device ownership (corporate or personal), you are prompted for that information. On the device, provide the required enrollment information, then tap **OK**.



8 The My Devices list is updated to show that the device is enrolled and active.



9 Verify that the device is receiving emails, by sending an email to the user from another account.

NOTE: If a Mobile Email policy is not assigned to the enrolled Email Only device or is unassigned from the already enrolled Email Only device, then an email is sent to the device stating that the user will be unable to send or receive corporate emails. You can edit the contents of this email in ZENworks Control Center by navigating to **Configuration > Management Zone Settings > Event and Messaging > Email Notifications**. Click the relevant email and edit the contents.

Also, if a Mobile Email policy is not assigned to the device enrolled as an Email Only device, the device can still be managed by the ZENworks Control Center wherein you can apply policies applicable for Email Only devices.

- 10 After the device is enrolled to the ZENworks Management Zone, the enrollment mode of the device is displayed as **ActiveSync** on the Device Information page in ZCC. To view the device information, from the left hand side navigation pane in ZCC, click **Devices > Mobile Devices** (or navigate to the folder as configured in the Mobile Enrollment Policy) and select the appropriate device.

17 Allowing Manual Reconciliation by the User

When users attempt to enroll their devices, which they have previously enrolled, using the same enrollment mode or a different enrollment mode, ZENworks will update the existing device object in the management zone through auto reconciliation. However, for certain devices auto reconciliation might fail due to the following reasons:

- ◆ ZENworks is unable to access the IMEI number of certain Android devices, as the IMEI number is masked.
- ◆ The ActiveSync ID of iOS devices change if they are reset to factory settings before re-enrolling.

Taking these scenarios into account, you can select the **Allow manual reconciliation by user** option while editing the Mobile Enrollment Policy.

If this feature is turned on and ZENworks is unable to reconcile with the existing device object, then a page is displayed that lets the user manually reconcile to the existing device object.

If the feature is turned off and ZENworks is unable to reconcile with the existing device object, then the device is automatically enrolled as a new device.

To enable this option:

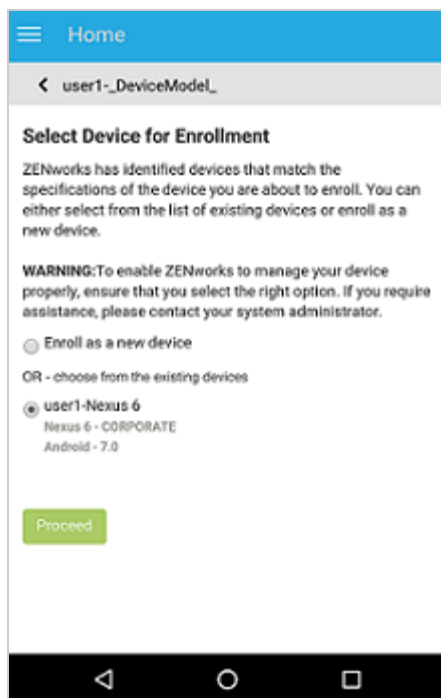
- 1 Navigate to the **Policies** section in ZCC.
- 2 Click the relevant Mobile Enrollment Policy.
- 3 Click the **Details** tab.
- 4 Click **Advanced Settings**.
- 5 Click **Allow Manual Reconciliation by User**.
- 6 Click **Apply**.
- 7 Publish as a new policy or as a new version of the policy.

IMPORTANT: During manual reconciliation, it is important that the user selects the right option. If an incorrect option is selected, then ZENworks will be unable to manage the device properly. If the user has reconciled to an incorrect device object, then both the devices will have to be unenrolled from the ZENworks Management Zone.

Consider the following scenario:

For Android Devices: A user has downloaded the ZENworks Agent app and completed the enrollment procedure for a non-cellular Android device. Subsequently, a device object is created in the ZENworks Management Zone. Later, to enable ZENworks to manage corporate emails on the device, the user configures an ActiveSync account on the same device. After configuring the ActiveSync account, since the IMEI number of this device is not available, ZENworks will be unable to reconcile the device with the existing device object that was created during the ZENworks Agent app enrollment.

In such a scenario, if **Allow Manual Reconciliation by User** is allowed in the Mobile Enrollment policy and if reconciliation fails, ZENworks sends a mail to the user to complete the enrollment process. When the user re-visits the ZENworks User Portal to complete ActiveSync enrollment, the user needs to select the appropriate device ownership type. Subsequently, the ZENworks User Portal will list all active Android devices associated with the user that are enrolled to the ZENworks Management Zone. The user can select the appropriate device to manually reconcile it to the existing device object. The user also has the option to select **Enroll as New Device**. Click **Proceed**.



NOTE: If for any reason, platform related information of the device could not be obtained by ZENworks, then the ZENworks User Portal will initially list all the platforms before listing all devices for manual reconciliation. The user needs to select the relevant platform of the device before proceeding further. This page will be displayed regardless of whether the **Allow manual reconciliation by user** option is selected or not.

In a scenario, wherein an Android device is already enrolled via the ActiveSync mode and the user is about to re-enroll the same device by downloading the ZENworks App, then as a part of manual reconciliation, the ZENworks App will display all active Android devices that are enrolled as Email Only (ActiveSync Only) devices and are associated with the same user.

For iOS devices: An iOS device that was initially enrolled via Email Only mode is fully wiped and retired. You have now unretired the device for the user to re-enroll the device back to the zone using the same enrollment mode. Since the ActiveSync IDs of the re-enrolled device changes, auto reconciliation fails.

In such a scenario, enable **Allow Manual Reconciliation by User** in the Mobile Enrollment Policy. When the user re-visits the ZENworks User Portal page to complete ActiveSync Only enrollment of the unretired device (see [Enrolling an Email Only Device](#)) and after selecting the device ownership type, the ZENworks User Portal will list all active iOS devices associated with the user that are

enrolled to the ZENworks Management Zone. The user can select the appropriate device to manually reconcile the device to the existing device object. The user also has the option to select **Enroll as New Device**. Click **Proceed**.



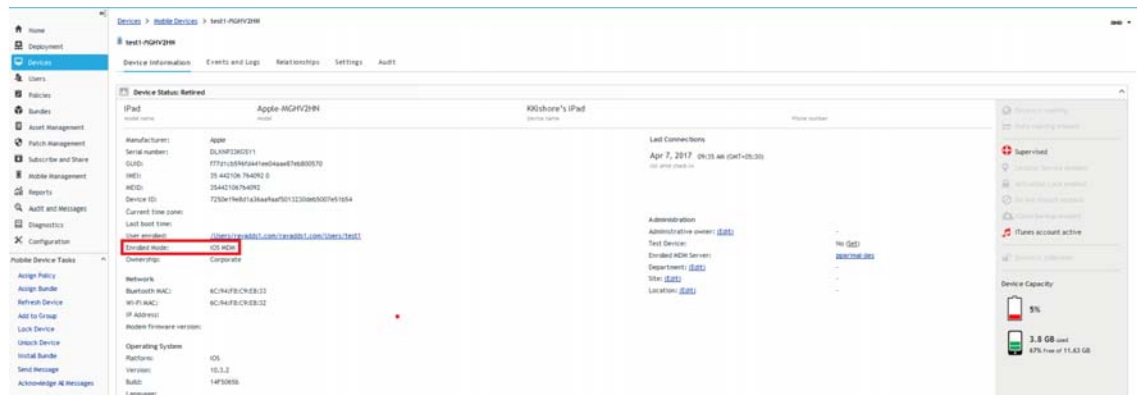
18 Viewing Device Information

After a device is enrolled to the ZENworks Management Zone, you can view the details of your enrolled device in ZCC. To view this page:

- 1 Navigate to the **Devices** section in ZCC.
- 2 Click **Mobile Devices**.
- 3 Click the relevant device.

The Device Information page displays the following details:

- ◆ **General Information:** Provides general information about the device such as the device manufacturer, the IMEI number and the GUID. This also displays information on the mode of enrollment and ownership type of the device (personal or corporate). As soon as you enroll your device, the mode in which the device is enrolled is displayed on the Device Information page.



The various enrollment modes are as follows:

- ◆ **Android App:** Indicates that as a part of full management of an Android device, the ZENworks Agent app enrollment is complete.
- ◆ **Android App + ActiveSync:** Indicates that as a part of full management of an Android device, the ZENworks Agent app enrollment is complete and the corporate email account configured on the device is managed by ZENworks that acts as a proxy server for the configured ActiveSync Server.
- ◆ **iOS MDM:** Indicates that as a part of full management of an iOS device, the device is enrolled via the MDM client but the corporate email account on the device is not managed by ZENworks due to any one of the following reasons:
 - ◆ A Mobile Email Policy is not assigned to the device.
 - ◆ The assigned Mobile Email Policy does not use ZENworks as the proxy server between the configured ActiveSync Server and the device. The policy directly connects to the configured ActiveSync Server.

- ◆ The ActiveSync server is not linked to the associated user source.
- ◆ The ActiveSync server is not valid for the user.
- ◆ **iOS MDM + ActiveSync:** Indicates that as a part of full management of an iOS device, the device is enrolled via the MDM client and the corporate email account configured on the device is managed by ZENworks that acts as a proxy server for the configured ActiveSync Server.
- ◆ **ActiveSync:** Indicates that as a part of Email Only enrollment, ZENworks manages only the corporate email account on the device and certain policies that are enforceable through the ActiveSync protocol, such as the Mobile Device Control Policy and Mobile Security Policy, can be applied on this device.
- ◆ **Unknown:** Indicates that the device is in a retired state.
- ◆ **Network:** Displays network information such as the Wi-Fi MAC address and the IP address.
- ◆ **Operating System:** Displays information on the Operating System installed on the app. For Android devices, it also displays the latest Security Patch Level that is installed on the device. Security patch level refers to all security vulnerabilities and bugs that have been fixed by Android.
- ◆ **Cellular:** Displays information on the cellular network used by the device.
- ◆ **Last Connections:** Shows when the device was last connected with the ZENworks system. It also displays the last inventory scan time. If ZENworks also manages the device's ActiveSync connection, the date and time of the last ActiveSync connection is also displayed.
- ◆ **ZENworks Mobile App:** Displays the version of the ZENworks Agent App that is installed on the device. This is applicable for Android devices only.
- ◆ **ActiveSync:** Displays the ActiveSync Server version, the ActiveSync ID, and the User Agent that identifies the email client on the device.
- ◆ **Administration:** This section displays the following information. Click **Edit** to change the information in any of the fields.
 - ◆ **Administrative Owner:** Indicates the administrator of the device.
 - ◆ **Test Device:** Indicates if the device is a test device. If the device is not a test device, you can click **Set** to set the device as a test device. If the device is a test device, you can click **Reset** to reset the device to a non-test device.
 - ◆ **DEP Device (iOS only)** Indicates if the device is a DEP device.

NOTE: ZENworks will identify a device as a DEP device, only if this device is assigned to the relevant virtual MDM Server in the Apple portal. If a DEP enabled device is enrolled to ZENworks (using ZENworks User Portal) but is not assigned to the virtual MDM Server in the Apple portal, this device will not be identified as a DEP device.

- ◆ **Activation Lock Bypass Code (iOS only):** Indicates the 16 digit activation lock bypass code of the device. Click **Show** to view the code.
- ◆ **Factory Reset Protection Unlock Accounts (Android only):** Indicates the corporate accounts that are authorized to provision a device that has undergone a hard factory reset. Click **Show**, to view these accounts.
- ◆ **Department:** Indicates the department to which the device belongs.
- ◆ **Site:** Indicates the site to which the department belongs.
- ◆ **Location:** Indicates the location of the department.

- ◆ **MDM Server:** Indicates the MDM Server to which the device is enrolled.
- ◆ **Device is Roaming:** Indicates if the device is connecting through a network other than its home carrier network, as indicated by the **Home carrier network** field in the **Network** section. The “roaming” network is identified in the **Current carrier network** field, which is also displayed in the **Network** section.
- ◆ **Data Roaming Enabled:** Indicates if the device is allowed to use data while roaming.
- ◆ **Device is Rooted (Android Only):** Indicates if the device is configured for root access. This is applicable for Android devices only.
- ◆ **Device Capacity:** Provides information about the device’s battery, internal storage, external storage, and RAM.
- ◆ **Supervised (iOS only)** Indicates that the device is in a supervised mode allowing extra restrictions to be imposed.
- ◆ **Find My iPhone Enabled (iOS only)** Indicates that the device allows certain apps to determine the users’ approximate location. When enabled, this feature helps users in locating their devices and protecting them, if the devices are lost or stolen.
- ◆ **Activation Lock Enabled (iOS only)** Indicates that unauthorized access to a user’s device is restricted.
- ◆ **Do Not Disturb enabled (iOS only)** Indicates that notifications, alerts, and calls on a user’s device are silenced while it is locked.
- ◆ **iCloud Backup enabled (iOS only)** Indicates that the device information is backed up on a daily basis to iCloud.
- ◆ **iTunes Account Active (iOS only)** Indicates that the iTunes account associated with the device is active.
- ◆ **Device is Jailbroken (iOS only)** Indicates that the software restrictions imposed by Apple are removed.
- ◆ **Device Permissions (Android only)** Provides information on the permissions that are enabled for the ZENworks Agent App to access certain features of the device. The check mark against each of these permissions, indicates that the permission is enabled on the device. These permissions are required for the following reasons:
 - ◆ **Access Device Camera:** To scan the QR code in the Invite Email to autofill the login credentials in the app.
 - ◆ **Access Device Location:** To identify the current location of the device, in case it is lost or stolen.
 - ◆ **Read Phone State:** To identify the device’s information such as the serial number and IMEI number.
 - ◆ **Write External Storage:** To access the device storage to create logs that can be used for troubleshooting.




Managing Mobile Devices


This section provides information on all the administration tasks that can be performed related to the Mobile Management feature in ZENworks.


- ♦ [Chapter 19, “Viewing Device Status,” on page 129](#)
- ♦ [Chapter 20, “Securing a Device,” on page 131](#)
- ♦ [Chapter 21, “Monitoring Device Compliance,” on page 167](#)
- ♦ [Chapter 22, “Provisioning Applications,” on page 169](#)
- ♦ [Chapter 23, “Viewing Apps Catalog,” on page 193](#)
- ♦ [Chapter 24, “Refreshing a Device,” on page 197](#)
- ♦ [Chapter 25, “Collecting Mobile Device Inventory,” on page 201](#)
- ♦ [Chapter 26, “Initiating Quick Tasks,” on page 205](#)
- ♦ [Chapter 27, “Bypassing Activation Lock,” on page 209](#)
- ♦ [Chapter 28, “Locating a Device,” on page 213](#)
- ♦ [Chapter 29, “Enabling Factory Reset Protection on Android Work-Managed Devices,” on page 215](#)
- ♦ [Chapter 30, “Protecting Intune Apps,” on page 217](#)
- ♦ [Chapter 31, “Managing Email Notifications,” on page 237](#)
- ♦ [Chapter 32, “Unenrolling Devices,” on page 239](#)
- ♦ [Chapter 33, “Unenrolling the Organization from Android Enterprise,” on page 241](#)


19 Viewing Device Status


The following icons give a quick indication of the status of the device. To view the status, click **Devices** on the left navigation pane of ZENworks Control Center and click **Mobile Devices** (or navigate to the folder as configured in your Mobile Enrollment policy). The status icons that appear beside a device indicate the following:


 - No warning or error messages;


 - Warning messages;


 - Error messages;


 - No warning or error messages, bundle or policy assignment has failed.

 - Warning messages, bundle or policy assignment has failed.

 - Error messages; bundle or policy assignment has failed.

 - Retired device; inventory information is retained, but no policies or bundles are applied

 - Wipe Pending; unenroll device action is initiated from the ZENworks Management Zone and is waiting for response from the user's device.

 - Enrollment Pending; device object has been created in the ZENworks Management Zone and is waiting for enrollment to be completed on the device.

You can get more information about the warning and error messages by clicking the device and viewing the **Message Log** by navigating to the **Events and Logs** tab. You can get more information about the bundle and policy status by clicking the device name and viewing the bundle or policy information on the device's Relationship page.

20 Securing a Device

To secure all mobile devices in your ZENworks Management Zone, you can configure policies that consist of a set of rules to control a range of hardware and software configuration settings on your mobile devices. The various policies present within the Mobile Management feature that help secure a mobile device, are as follows:

- ♦ [Mobile Device Control Policy](#)
- ♦ [Mobile Security Policy](#)

20.1 Mobile Device Control Policy

This policy enables you to allow or restrict users from accessing the various features of a mobile device. For example, through this policy you can restrict access to applications such as the device's camera, the device's web browser, and voice assistant.

- ♦ [Section 20.1.1, "Creating a Mobile Device Control Policy," on page 131](#)
- ♦ [Section 20.1.2, "Editing a Mobile Device Control Policy Setting," on page 132](#)
- ♦ [Section 20.1.3, "Assigning a Mobile Device Control Policy," on page 153](#)

20.1.1 Creating a Mobile Device Control Policy

- 1 On the **Modern Management > Getting Started > Managing iOS/iPadOS Devices** page, navigate to the **Security and Control Policies** section and click **Create Policies**. Alternatively, from the left hand side navigation pane of ZCC, navigate to **Policies > New > Policy**.
- 2 On the **Select Platform** page, select **Mobile** and click **Next**.
- 3 On the **Select Policy Category** page, select **General Mobile Policies** and then click **Next**.
- 4 On the **Select Policy Type** page, select **Mobile Device Control Policy** and then click **Next**.
- 5 On the **Define Details** page, specify a name for the policy, select the folder in which to place the policy, then click **Next**.
- 6 On the **Configure Mobile Device Control Settings** page, assign different security levels to corporate-owned devices and personally-owned devices, and click **Next**:
 - ♦ **None**: Inherits the setting value from other Mobile Device Control policies assigned higher in the policy hierarchy. For example, if you assign this policy to a device, the setting value is inherited from any Mobile Device Control policy assigned to groups and folders of which the device is a member. If a setting value is not inherited from another Mobile Device Control policy, the device's default value is used.
 - ♦ **Low**: No restrictions are enforced on the device. However, some settings are assigned a default value and for the remaining settings no value is assigned.
 - ♦ **Moderate**: A few restrictions are imposed. For example, in the case of iOS devices, in-app purchases are disabled, background data fetch while roaming is disabled, access to documents from managed sources in unmanaged destinations and vice versa are disabled.

- ♦ **Strict:** Some restrictions are enforced on the device. For example, in the case of iOS devices, backup of data to iCloud is prevented, display of notification on the Lock screen is disabled, submission of diagnostic reports to Apple is disabled.
 - ♦ **High:** This level is similar to strict security level however with higher restrictions. For example, in the case of iOS devices, voice assistant Siri is disabled, the device camera is removed, and pop-up tabs in Safari is disabled.
- 7 On the **Summary** page, you can perform the following actions:
- ♦ **Create as Sandbox:** Creates a Sandbox-only version of the policy. A Sandbox version of a policy enables you to test it on your device before actually deploying it
 - ♦ **Define Additional Properties:** Enables you to edit the default device control settings configured in the policy. For more information, see [Editing a Mobile Device Control Policy Setting](#).

Click **Finish** to complete creating the policy.

20.1.2 Editing a Mobile Device Control Policy Setting

Based on the security level selected while creating the Mobile Device Control Policy, the settings that are predefined by ZENworks can be viewed or edited by performing the steps elaborated in this section. The Mobile Device Control policy settings can be configured for iOS, , Android, and ActiveSync devices.

Procedure

- 1 In ZENworks Control Center, navigate to the **Policies** section.
- 2 Click the Mobile Device Control policy for which the content needs to be configured.
- 3 Click the **Details** tab and edit the settings for the relevant device platform.

NOTE: If while creating the policy, the **Define Additional Properties** checkbox was selected, then you will be automatically redirected to the **Details** tab of the policy.

Corporate/Personal: The settings in the **Corporate** column are applied to devices whose ownership is defined as Corporate. The settings in the **Personal** column are applied to devices whose ownership is defined as Personal. The settings use the following values:

- ♦ **Yes:** Enables the setting.
- ♦ **No:** Disables the setting.
- ♦ **Inherit:** Inherits the setting value from other Mobile Device Control policies assigned higher in the policy hierarchy. For example, if you assign this policy to a device, the setting value is inherited from any Mobile Device Control policy assigned to groups and folders of which the device is a member. If there is no value to inherit, then ZENworks does not set the restriction.
- ♦ **Not Set (--):** Indicates that a value is not set by ZENworks.
- ♦ **Work Managed (Applicable for Android):** Indicates that a setting is applicable for Android devices enrolled in the work-managed device mode.
- ♦ **Work Profile (Applicable for Android):** Indicates that a setting is applicable for Android devices enrolled in the work profile mode.

4 Click **Apply**.

5 Click **Publish** to display the Publish Option page. In this page you can publish the modified policy as a new version of the same policy or as a new policy.

Apple

The settings that can be enabled or disabled for iOS devices are as follows. Some of these restrictions are applicable for supervised devices only, which can be identified based on the check mark under the **Supervised Only** column:

Tab	Settings	Description	Applicable from
Device	Allow camera	Determines whether to enable or disable the device camera. If set to No , the camera icon is removed from the home screen on the device.	
	Allow FaceTime	Determines whether to enable or disable FaceTime. This setting is enabled if the Allow camera setting is configured as Yes or Inherit .	
	Allow global background fetch while roaming	Determines whether the latest app data should be fetched from the network for apps running in the background, while the device is roaming.	
	Allow Handoff	Determines whether a user is allowed to resume an existing task or is allowed to access content from any device, which is logged into the same iCloud account.	
	Allow Siri	Determines whether Apple's voice assistant should be enabled.	
	Allow Siri while device is locked	Determines whether the user can access Siri while the device is locked. This setting is enabled if the Allow Siri setting is set to Yes or Inherit . Also, this option is ignored if a passcode is not set on the device.	iOS 5.1+

Tab	Settings	Description	Applicable from
	Allow automatic updates to certificate trust settings	Determines whether automatic updates to certificate trust settings should be enabled.	
	Allow documents from managed sources in unmanaged destinations	Determines whether a document can be opened in an unmanaged app or account if the document was created or downloaded from a managed app or account.	iOS 7.0+
	Allow managed apps to write contacts to unmanaged apps	Determines whether managed apps can write contacts to unmanaged contacts accounts. This field is enabled, if Allow documents from managed sources in unmanaged destinations is enabled.	iOS 12.0+
	Allow documents from unmanaged sources in managed destinations	Determines whether a document can be opened in a managed app or account if the document was created or downloaded from an unmanaged app or account.	iOS 7.0+
	Allow unmanaged apps to access contacts in managed apps	Determines whether unmanaged apps can access managed contacts accounts. This field is enabled, if Allow documents from unmanaged sources in managed destinations is enabled	iOS 12.0+
	Allow screenshots	Determines whether the user can capture images of the device's display screen. If disabled, this setting will prevent the classroom app from observing remote screens.	iOS 9.0+

Tab	Settings	Description	Applicable from
	Allow Bluetooth setting modification	Determines whether the user can modify the bluetooth settings on the device.	iOS 10+
	Allow host pairing	Determines whether an iOS device can pair with other devices. If No is selected, then these devices can only pair with their supervision host or with hosts having a Supervising Host Certificate. If a Supervision Host Certificate is not configured, all pairing is disabled.	iOS 7.0+
	Allow ScreenTime	Determines whether the user can use the Screen Time setting on the device.	iOS 7+
	Allow Find My Friends setting modification	Determines whether the user can modify the Find my Friend settings on the device.	
	Allow sending diagnostic and usage data to Apple	Determines whether automatic submission of diagnostic and usage reports to Apple should be enabled.	iOS 6.0+
	Allow users to accept untrusted TLS certificate	Determines whether the user can accept Transport Layer Security (TLS) certificates that cannot be verified.	iOS 5.0+
	Force encrypted backup	Determines whether the device backup process should be encrypted.	
	Force limited ad tracking	Determines whether advertisers' tracking of a user's activities across apps should be limited. If set to Yes , then ad tracking is not eliminated but reduced to some extent.	iOS 7.0+

Tab	Settings	Description	Applicable from
	Request passcode for incoming AirPlay requests	Determines whether a pairing passcode restriction should be enforced for all incoming AirPlay requests coming from another device to a managed device.	Apple TV 6.1 to tvOS 10.1
	Request passcode for outgoing AirPlay requests	Determines whether a pairing passcode restriction should be enforced for all outgoing AirPlay requests sent from a managed device to another device.	iOS 7.1+
	Treat Airdrop as unmanaged destination	Determines whether Airdrop should be considered as an unmanaged drop target. If set to Yes , then the user will be unable to share managed data through Airdrop.	iOS 9.0+
	Allow Dictation	Determines whether or not the user can enable the dictation option present in the keyboard.	iOS 10.3+
	Allow Wi-Fi whitelisting	Determines whether or not the user can connect to the Wi-Fi service that is setup using the configuration profile.	iOS 10.3+
	Allow VPN creation	Determines whether or not the user can configure a VPN connection using their devices.	iOS 11.0+
	Allow setting up of new devices within proximity	Determines whether the device is allowed to identify other devices that are within its proximity to share password and settings.	iOS 12.0+
	Allow automatic update of date and time	Determines whether the date and time can be automatically set based on the current location and network.	iOS 12.0+

Tab	Settings	Description	Applicable from
	Allow enterprise app trust	<p>Determines whether custom apps can be provisioned using universal provisioning profiles. If No is selected, it removes the Trust Enterprise Developer button in Settings-> General-> Profiles & Device Management.</p> <p>This restriction applies to free developer accounts but it does not apply to enterprise app developers who are trusted because their apps were pushed via MDM, nor does it revoke previously granted trusts.</p>	iOS 9.0+
	Allow backup of enterprise books	Determines whether the user can back up books distributed by the organization to iCloud or iTunes.	
	Allow in-app purchase	Determines whether the user can make in-app purchases.	
	Allow managed apps to store data in iCloud	Determines whether managed app data should sync with iCloud.	
	Allow notes and highlights sync for enterprise books	Determines whether metadata, which includes notes and highlights of books that are distributed by the user's organization, should be synced with iCloud.	
	Allow System App Removal	Determines whether the user can remove system apps from the device.	iOS 11.0+
Apple Watch	Force Apple Watch wrist detection	Determines whether an Apple Watch should display the time and the latest alerts when the user's wrist is raised.	iOS 8.2+

Tab	Settings	Description	Applicable from
iTunes	Allow iTunes	Determines whether the user can access the iTunes music store app. If disabled, the icon will be removed from the Home screen.	
	Require iTunes Store password for each purchases	Determines whether or not the user needs to enter the password for each purchase on the iTunes Store.	iOS 5.0+
iCloud	Allow My Photo Stream	Determines whether a copy of any photo taken on the managed device should be synced with the user's other iOS devices.	iOS 6.0+
	Allow iCloud Keychain	Determines whether Keychain data such as accounts, passwords, and credit card information, should be synced with iCloud.	iOS 7.0+ and macOS 10.12+
	Allow iCloud Photo Library	Determines whether photos on iCloud can be accessed on the managed device. If disabled, any photos that are not fully downloaded from the Photo Library to the device, will be removed from local storage.	iOS 9.0+ and macOS 10.12+
	Allow iCloud Photo Sharing	Determines whether the user can publish and share photos with other iOS users through the iCloud website.	
	Allow iCloud backup	Determines whether data can be backed up or restored on iCloud.	iOS 5.0+
Safari	Allow use of Safari	Determines whether the user is allowed to use the Safari web browser on the device. If set to No , then the Safari icon is removed from the Home screen of the device.	

Tab	Settings	Description	Applicable from
	Accept cookies	<p data-bbox="870 218 1146 365">Determines the cookie policy that should be enabled in the Safari web browser. The accepted values are:</p> <ul data-bbox="894 407 1146 1352" style="list-style-type: none"> <li data-bbox="894 407 1146 554">◆ Block all websites, third parties, and advertisers from storing cookies on the device. <li data-bbox="894 575 1146 722">◆ Allow all websites, third parties, and advertisers to store cookies on the device. <li data-bbox="894 743 1146 995">◆ Allow cookies to be stored from only those websites that the user is currently visiting and not from third parties that embed content in the website. <li data-bbox="894 1016 1146 1352">◆ Allow cookies to be stored from only those websites that the user visits. With this option you can prevent websites that have embedded content in other websites that you visit from storing cookies. <p data-bbox="870 1373 1146 1499">The default value is to allow cookies from all websites, third parties, and advertisers.</p>	
	Allow pop-ups	<p data-bbox="870 1520 1146 1751">Determines whether pop-ups should be blocked in the Safari web browser. This setting is enabled, if Allow use of Safari is configured as Yes or Inherit.</p>	

Tab	Settings	Description	Applicable from
	Enable autoFill	Determines whether Safari should remember the data entered by users on web entry forms. This setting is enabled, if Allow use of Safari is configured as Yes or Inherit .	
	Enable JavaScript	Determines whether JavaScript should be enabled in the Safari web browser. This setting is enabled, if Allow use of Safari is configured as Yes or Inherit .	
	Force fraud warning	Determines whether Safari should warn users about refraining from visiting websites that are fraudulent. This setting is enabled, if Allow use of Safari is configured as Yes or Inherit .	

Tab	Settings	Description	Applicable from
Lock Screen	Allow passbook notifications in lock screen	Determines whether notifications on the passbook app can be displayed on the lock screen. The passbook app allows users to store their coupons, tickets, and so on.	iOS 6.0+
	Allow voice dialing while device is locked	Determines whether voice dialing should be enabled while the device is locked.	
	Show Control Center in lock screen	Determines whether Control Center can be accessed from the Lock screen. The Control Center gives the user quick access to the apps and controls on the device.	iOS 7.0+
	Show Notification Center in lock screen	Determines whether users can view past notifications on the lock screen. If enabled, the users can still view notifications on the lock screen, when they arrive.	iOS 7.0+
	Show Today View in lock screen	Determines whether the Today View in Notification Center should be displayed on Lock screen.	iOS 7.0+
	Allow USB connections when device is locked	Determines whether the device can connect to USB accessories while locked.	iOS 12.0+
Media Content	Allow bookstore erotica	Determines whether the user is permitted to download media that is tagged as erotica from the iBooks store.	iOS and tvOS 11.3+
	Ratings region	Determines the region that needs to be selected to populate the allowed ratings for media content defined for that region.	iOS and tvOS 11.3+

Tab	Settings	Description	Applicable from
	Apps	Determines the maximum allowed rating for apps. These values are populated based on the selected Ratings region . If a rating is enabled, items that do not conform to the rating restrictions cannot be downloaded or installed on the device.	iOS 5.0+ and tvOS 11.3+
	Movies	Determines the maximum allowed rating for movies. The values in this field are populated based on the selected Ratings region . If a rating is enabled, items that do not conform to the rating restrictions cannot be downloaded on the device.	iOS and tvOS 11.3+
	TV Shows	Determines the maximum allowed rating for TV shows. The values in this field are populated based on the selected Ratings region . If a rating is enabled, items that do not conform to the rating restrictions cannot be downloaded on the device.	iOS and tvOS 11.3+
Security	Allow Touch ID to unlock device	Determines whether the user can unlock the device by using fingerprint.	iOS 7+ and macOS 10.12.4+
	Force authentication before using autofill	Determines whether users need to authenticate using Touch ID or Face ID before entering passwords or credit card information in Safari and Apps.	iOS 12.0+

Tab	Settings	Description	Applicable from
	Allow password autofill	Determines whether users can use the Autofill Passwords feature and will be prompted to use saved passwords in Safari or in apps. If disabled, Automatic Strong Password will not be applicable and strong passwords will not be suggested to users.	iOS 12.0+
	Allow password sharing	Determines whether users can share their passwords using the Airdrop Passwords feature.	iOS 12.0+
	Allow password proximity request	Determines whether the device can request passwords from nearby devices.	iOS 12.0+
AirPrint	Allow AirPrint	Determines whether or not a user can connect to the AirPrint feature to print documents or pictures wirelessly using any AirPrint enabled printer.	iOS 11.0+
	Allow AirPrint Credentials Storage	Determines whether or not AirPrint credentials can be stored in Keychain.	iOS 11.0+
	Force AirPrint Trusted TLS Requirement	Determines whether or not devices can connect to AirPrint enabled devices only using the trusted TLS certificates.	iOS 11.0+
	Allow AirPrint iBeacon Discovery	Determines whether or not devices can discover the printer beacons. Using these i Beacons, printers can broadcast connection information, and devices can discover it to reduce setup time.	iOS 11.0+
OS Update	Allow delay in OS updates	Determines whether user visibility of software updates should be delayed.	iOS 12.0+

Tab	Settings	Description	Applicable from
	Select number of days for delay	Select for how many days the software update should be delayed, after which the software update is visible to the user. The maximum number of days is 90 days and the default value is 30 days.	iOS 12.0+
Classroom App	Force users to automatically join Classroom	Determines whether permission to join classes is automatically granted without prompting the student.	iOS 12.0+
	Allow teacher to lock apps and devices	Determines whether a teacher can lock apps or the entire device without prompting the student.	iOS 12.0+
	Force request for teacher consent before leaving Classroom	Determines whether a student enrolled in an unmanaged course needs to request for permission before leaving the course.	iOS 12.0+
	Allow teacher to observe device screen	Determines whether the device of a student enrolled in a managed course, can automatically give permission to that course's teacher's request to observe the student's device screen, without prompting the student.	iOS 12.0+

NOTE: The settings that are applicable for only supervised devices are subject to change.

Android

The settings that can be enabled or disabled for Android devices are as follows. Each of these restrictions are either applicable for work profile or work-managed device modes of enrollment, which can be identified based on the check mark under the respective columns:

	Settings	Description	Applicable from
Devices	Allow camera	Determines whether the device camera should be enabled. If disabled on devices enrolled in the work profile mode, the camera can still be accessed from the device's personal space. This setting does not remove the camera app. The camera app when opened, the camera will be blocked and the user cannot click photos or videos.	Android 5.0+
	Allow install from unknown sources	Determines whether or not the user can install apps from outside the managed Google Play Store.	Android 5.0+
	Allow debugging features	Determines whether or not debugging of the device can be enabled. USB debugging is often used by developers or IT support to connect/debug using Android studio and transfer data from an Android device to a computer. While this feature is useful, a device is not as secure when connected to a computer.	Android 5.0+
	Allow screenshots	Determines whether the user can capture images of the device's display screen.	Android 5.0+
	Allow cross-profile copy and paste	Determines whether the user can copy and paste data between the work profile and the personal space on the device.	Android 7.0+
	Allow user to factory reset the device	Determines whether the user can factory reset the device from the settings menu of the device.	Android 5.1+
	Allow factory reset protection	Determines whether devices need to be protected from an unauthorized (hard) factory reset. If enabled, this setting provides the ability to whitelist one or more corporate unlock accounts which can be used to provision devices after unauthorized factory resets such as from bootloader or fast boot.	Android 5.1+
	Specify corporate unlock accounts	This setting is enabled if Allow factory reset protection is enabled. Specify the corporate accounts of users who are authorized to provision devices that have undergone a hard factory reset. For more information, see Enabling Factory Reset Protection on Android Work-Managed Devices .	Android 5.1+

Settings	Description	Applicable from
Allow mounting of physical external media	Determines whether the user can connect their devices to external physical media.	Android 5.1+
Allow sharing data using NFC beam	Determines whether the user can share data from their devices using the NFC beam.	Android 5.1+
Allow USB file transfer	Determines whether the user can transfer files over USB.	Android 5.1+
Allow USB storage	Determines whether USB storage is enabled or disabled.	Android 5.1+
Allow cross-profile contact search	Determines whether the telephony or messaging apps in the personal space of a device can access work profile contacts.	Android 7.0+
Allow cross-profile caller ID lookup	Determines whether caller ID information of work profile contacts should be displayed in the personal space of a device during incoming calls.	Android 7.0+
Allow contact sharing with other bluetooth devices	Determines whether the user can share work contacts to other connected bluetooth devices such as hands-free calling in cars or headsets.	Android 7.0+
Allow location configuration	Determines whether the user can turn the location on or off. If disabled, the user will not be able to turn on the Location setting on the device and you will not be able to determine the location of the device.	Android 9.0+
Set location services mode	Set the location services mode to any one of the following to estimate the device location faster and more accurately: <ul style="list-style-type: none"> ◆ High Accuracy uses GPS, Wi-Fi, mobile network and sensors to determine the most accurate location. ◆ Battery saving uses sources that use less battery, like Wi-Fi and mobile networks. ◆ Sensor only uses only GPS (not including network-provided location). This mode consumes more battery and takes time in determining location. 	Android 5.0+

	Settings	Description	Applicable from
Apps	Allow Printing	Determines whether users can print data from their devices.	Android 9.0+
	Allow data sharing from personal to work profile	Determines whether users can share data from the personal profile to the work profile. If enabled, users can share data from apps in the personal profile to work profile apps. Also, work profile apps can pick items from the personal profile, such as files or pictures.	Android 9.0+
	Runtime permissions	Select the default response for any runtime permissions requested by apps. For more information, see the Android Developer Documentation (https://developer.android.com/training/permissions/requesting.html) . You can select any one of the following values: <ul style="list-style-type: none"> ◆ Prompt: Allows the user to grant or deny permissions to the apps in profile or those distributed by the organization. ◆ Auto Grant: Automatically grant permissions to the apps in profile or those distributed by the organization. ◆ Auto Deny: Automatically denies permission to the apps in profile or those distributed by the organization. 	Android 6.0+
	Allow adding accounts	Determines whether the user can add or remove accounts to access work apps. However, this setting should be used with caution, as by enabling it users can also add their personal accounts to access work apps, which might make it difficult to contain corporate data within the workspace.	Android 5.0+
	Allow public play store access	Determines whether the user can access play store using the newly added account. This field will be enabled, if the Allow adding accounts field is enabled. This setting does not restrict user from adding accounts to personal side from the Play store.	

	Settings	Description	Applicable from
	Allow Verify Apps enforcement	Determines whether Verify Apps can be enabled on the device. This feature scans apps for malware before and after the apps are installed, thereby securing corporate data from malicious apps.	Android 5.0+
	Allow apps to be uninstalled	Determines whether users can uninstall apps in profile or those distributed by the organization.	Android 5.0+
	Allow modifying of app data	Determines whether users can modify app data from the Settings menu such as uninstalling of apps, disabling of apps, clearing of app data and cache, force stopping apps, clearing app defaults and so on.	Android 5.0+
Network	Allow cell broadcasts	Determines whether users can configure cell broadcasts.	Android 7.0+
	Allow editing of mobile network settings	Determines whether users can modify the mobile network settings from the Settings menu.	Android 7.0+
	Allow resetting of all network settings	Determines whether users can reset network settings such as current cellular and Wi-Fi settings, VPN settings and so on.	Android 7.0+
	Allow cellular data while roaming	Determines whether device permits cellular data while roaming.	Android 7.0+
	Allow outgoing calls	Determines whether the users can make calls on their devices.	Android 7.0+
	Allow sending and receiving of SMS messages	Determines whether the device can receive text messages or whether users can send text messages.	Android 7.0+
	Allow tethering and configuring portable hotspots	Determines whether users can use their device as a portable hotspot by tethering.	Android 7.0+
	Set Wi-Fi timeout	Determines whether the device should disconnect from the connected Wi-Fi network, when the device is not in use. If the Not when plugged in option is selected, then the Wi-Fi will not timeout if the device is plugged-in.	Android 7.0+
	Allow bluetooth configuration	Determines whether users can configure bluetooth on their devices.	Android 7.0+

	Settings	Description	Applicable from
	Allow editing of ZENworks-provisioned Wi-Fi settings	Determines whether the user can modify the Wi-Fi settings that are provisioned by ZENworks.	Android 6.0+
	Allow changing of Wi-Fi network	Determines whether the user can connect to different Wi-Fi access points.	Android 6.0+
	Allow airplane mode	Determines whether users can set their devices in the airplane mode.	Android 9.0+
Audio	Mute master volume	Determines whether the master volume is remotely muted or not.	Android 5.0+
	Allow editing of volume settings	Determines whether users can modify the device volume settings.	Android 5.0+
	Allow muting of device microphone	Determines whether users can mute the device microphone.	Android 5.0+
Date	Allow configuration of date, time and time zone	Determines whether the user can configure the date, time and timezone settings, either manually or automatically.	Android 9.0+
	Allow configuration of date and time	Determines whether the users can configure the date and time on their devices either automatically or manually. If disabled, the date and time settings are disabled.	Android 5.0+
	Allow automatic update of date and time	Determines whether the date and time should be automatically fetched from the network. If enabled, the user will not be able to set the date and time manually.	Android 5.0+
	Allow automatic update of time zone	Determines whether the time zone should be automatically fetched from the network. If enabled, the user will not be able to set the time zone manually.	Android 5.0+

	Settings	Description	Applicable from
OS Update	Select OS update type	<p>Select from any one of the following options to configure and apply over-the-air system updates for devices:</p> <ul style="list-style-type: none"> ♦ Automatic indicates that the devices will receive the update as soon as it is available. ♦ Postpone indicates that the update can be postponed to up to 30 days. ♦ Windowed indicates that the update can be scheduled within a daily maintenance window. You can set the start time and the end time (based on a 24 hour format) in the Daily maintenance window start time and Daily maintenance window end time, respectively. The system update will install at any time between the start and the end time. If the start time is later than the end time, then the end time will be considered as a time on the next day. 	Android 6.0+
Keyguard Features	Allow device keyguard features	Determines whether features such as Trust Agents and Fingerprint Unlock are made available to users before unlocking the device lock screen.	Android 5.0+
	Allow trust agents	Determines whether trust agents such as Smart Lock can be enabled by the user to unlock the device keyguard. If you select Configure , then you can enable or disable specific Google Smart Lock trustlets in the Smart Lock field. If you select All , then all the Trust Agents will be automatically enabled for the user to configure on the device.	Android 5.0+

Settings	Description	Applicable from
Smart Lock	<p>The Smart Lock feature lets users keep their Android devices unlocked when any of the following options are enabled:</p> <ul style="list-style-type: none"> ◆ Bluetooth: When enabled, this option lets the user add a bluetooth device such as a bluetooth watch to the Trusted Devices setting on the device. The user's device remains unlocked as long as it is connected to one of these trusted devices. ◆ NFC: When enabled, this option lets the user add an NFC device to the Trusted Devices setting on the device. The user's device remains unlocked based on the NFC tags on the trusted devices. ◆ Places: When enabled, this option lets the user add a safe location such as the user's home or office, in the Trusted Places setting. The user's device unlocks and remains unlocked as long as the current location of the user is one of the configured Trusted Places. ◆ Faces: When enabled, this option lets the user set his or her face as a Trusted Face. The user's device unlocks when it recognizes the user's face. ◆ On Body: When enabled, this option lets the user configure On Body Detection on the device. Based on this setting, the device will unlock and will remain unlocked until it is being carried in the user's hand, bag, or pocket, which is detected based on the device's motion sensors such as the accelerometer or gyroscope. ◆ Voice: This option enables the device to unlock when the user uses the voice command "OK Google". 	Android 5.0+
Allow fingerprint unlock	Determines whether users can unlock their devices using their fingerprints.	Android 5.0+

	Settings	Description	Applicable from
Display	Allow redacted notifications	Determines whether the user can enable all notifications, including redacted (containing sensitive information) notifications, on the lock screen. If disabled, the user has the option to disable redacted notifications on the lock screen.	Android 5.0+
	Allow secure camera	Determines whether the camera can be accessed from the lock screen.	Android 5.0+
	Allow all notifications	Determines whether all notifications are displayed on the lock screen.	Android 5.0+
	Allow ambient display	Determines whether the user can configure ambient display on their devices.	Android 9.0+
	Allow screen brightness	Determines whether the users can configure screen brightness on their devices.	Android 9.0+
	Set screen brightness mode	Determines whether the screen brightness mode should be set to automatic.	Android 9.0+
	Configure screen brightness percentage	Determines whether a specific backlight brightness percentage should be enforced. If enabled, you can set the percentage in the Set screen brightness percentage field. The brightness value on an Android device ranges from 0 to 255. When you define a percentage in the Set screen brightness percentage field, then the equivalent value is set on the device. For example, if 50% is set as the brightness percentage, then the brightness value is set as 127.5.	Android 9.0+
	Allow user to configure screen timeout	Determines whether the user can configure when the device screen should timeout.	Android 9.0+

ActiveSync

These settings can be applied on devices that are enrolled as:

- ◆ ActiveSync Only devices

- ◆ If a setting is applicable for both iOS and ActiveSync, then the stricter restriction of the two is applied. For example, if **Allow Camera** is enabled as a part of the iOS settings and if **Allow Camera** is disabled as a part of the ActiveSync settings, then the camera icon is removed from the device, as disabling of the camera is a strict setting.

Settings	Description
Allow Bluetooth	Determines whether bluetooth connections are allowed to and from the device. You also have the option of allowing only a hands free configuration on the device.
Allow browser	Determines whether the user is allowed to use the default web browser on the device.
Allow camera	Determines whether the device camera should be enabled.
Allow infrared	Determines whether infrared connections are allowed to and from the device.
Allow text messaging	Determines whether the user can send or receive text messages on the device.
Allow storage card	Determines whether the device can access a removable storage card.

20.1.3 Assigning a Mobile Device Control Policy

The Mobile Device Control Policy can be assigned to users or devices. User-assigned policies apply to all devices enrolled by the user. Device-assigned policies apply only to the explicitly assigned devices.

In addition to assigning policies directly to users and devices, you can assign this policy to user groups, user folders, device groups, and device folders. Each member of the group or folder receives the assignment.

- 1 To assign the policy to users, from the **Policies** list, select the check box in front of the policy and click **Action > Assign to User**. To assign the policy to devices, from the **Policies** list, select the checkbox in front of the policy and then click **Action > Assign to Device**.
- 2 In the Select Object dialog box, browse and select the users or devices to whom you want to assign the policy, click **OK** to add them to the list and then click **Next**.
- 3 If the policy is assigned to a device, then the Policy Conflict Resolution page is displayed. In this page you can set the precedence for device-associated policies and user-associated policies for resolving conflicts that arise when policies of the same type are associated to both devices and users. Define any of the following and click **Next**:
 - ◆ **User Precedence:** User-associated policy will override the device-associated policy. Select this option to apply policies that are associated to the users first, and then to the devices.
 - ◆ **Device Precedence:** Device-associated policy will override the user-associated policy. Select this option to apply policies that are associated to the devices first, and then to the users.
 - ◆ **Device Only:** Select this option to apply policies that are associated to devices alone.

- ♦ **User Only:** Select this option to apply policies that are associated to users alone.
- 4 Review the summary page and click **Finish** to complete the assignment.

20.2 Mobile Security Policy

This policy configures the password restrictions, encryption settings, and device inactivity settings.

20.2.1 Creating a Mobile Security Policy

- 1 On the Getting Started with Mobile Management page, navigate to the **Mobile Security and Control** section and click **Create New Policies**. Alternatively, from the left hand side navigation pane of ZCC, navigate to **Policies > New > Policies**.
- 2 On the Select Platform page, select **Mobile** and then click **Next**.
- 3 On the Select Policy Category page, select **General Mobile Policies** and then click **Next**.
- 4 On the Select Policy Type page, select **Mobile Security Policy** and then click **Next**.
- 5 On the Define Details page, specify a name for the policy, select the folder in which to place the policy, then click **Next**.
- 6 On the **Select Security Levels** page you can assign different security levels to corporate-owned devices and personally-owned devices. There are five security levels. Each security level provides pre-configured defaults for the password, encryption, and device inactivity settings. After the policy is created, you can edit the policy to customize individual settings, if needed.

Select from the following security levels and click **Next**:

- ♦ **None:** All settings are inherited from other Mobile Security policies applied to the device. If no other policies are applied to the device, the device's default settings are used.

The None security level is useful for creating exceptions for devices. For example, you might have a corporate Mobile Security policy that applies a Moderate security level to all devices. However, you have a few devices on which you want to enforce storage card encryption, which is not enforced by the Moderate security level. You create a policy with the None security level, edit the policy to turn on storage card encryption, and then assign the policy to the appropriate devices.

The None security level is also useful for overriding a few default settings on devices. For example, you might want to retain all of the default settings of the device with the exception that you want to enable the Require Encryption setting. In this scenario, you need to create a policy with the None security level, edit the policy to turn on device encryption, and then assign the policy to the appropriate devices. The devices will retain all default settings except for the device encryption setting enforced through the policy.

- ♦ **Low:** Enforces a password on the device. The password can be a simple password with a minimum of 4 characters.
- ♦ **Moderate:** Enforces a password and inactivity lockout restrictions. The password must be an alphanumeric password with a minimum of 6 characters. A 30 day password expiration is enforced, and the last 5 passwords cannot be reused. After 5 minutes of inactivity, the device is locked; after 10 failed attempts to unlock the device, it is wiped.

- ♦ **Strict:** Enforces a password, encryption, and inactivity lockout restrictions. The password must be a complex password with a minimum of 8 characters. A 30 day password expiration is enforced, and the last 7 passwords cannot be reused. The device and its storage card are encrypted. After 1 minute of inactivity, the device is locked; after 7 failed attempts to unlock the device, it is wiped.
- ♦ **High:** Same as the Strict security level with higher restrictions for each complex password setting. The password must be a strong complex password with a minimum of 8 characters. A 30 day password expiration is enforced, and the last 10 passwords cannot be reused. The device and its storage card are encrypted. After 1 minute of inactivity, the device is locked; after 5 failed attempts to unlock the device, it is wiped.

7 On the **Summary** page.

- ♦ **Create as Sandbox:** Creates a Sandbox-only version of the policy. A Sandbox version of a policy enables you to test it on your device before actually deploying it
- ♦ **Define Additional Properties:** Enables you to edit the default security settings configured in the policy. For more information, see [Editing a Mobile Security Policy Setting](#).

Click **Finish** to complete the policy.

20.2.2 Editing a Mobile Security Policy Setting



Based on the security level selected while creating a Mobile Security policy, the settings as predefined by ZENworks can be viewed or edited by performing the steps elaborated in this section.

- 1 In ZENworks Control Center, navigate to the **Policies** section.
- 2 Click the Mobile Security Policy whose content you want to edit.
- 3 Click the **Details** tab, and edit the settings.

Corporate/Personal: The settings in the **Corporate** column are applied to devices whose ownership is defined as Corporate. The settings in the **Personal** column are applied to devices whose ownership is defined as Personal. The settings use the following values:

- ♦ **Yes:** Enables the setting.
- ♦ **No:** Disables the setting.
- ♦ **Inherit:** Inherits the setting value from other Mobile Security Policies assigned higher in the policy hierarchy. For example, if you assign this policy to a device, the setting value is inherited from any Mobile Security Policy assigned to groups and folders of which the device is a member. If a setting value is not inherited from another Mobile Security Policy, the device's default value is used.
- ♦ **Numeric value:** Configures the setting with the numeric value provided by you.
- ♦ **None, Low, Medium, High:** These values apply only to the Password Quality setting for Android 12 or higher only.

Platform Support: The platform columns show support for a setting. The platforms are:

- ♦ Android 12 or higher
- ♦ Android 11 or lower
- ♦  iOS
- ♦  ActiveSync

The **Password**, **Device Inactivity** and **Encryption** tabs are applicable for the following devices:

- ◆ iOS devices
- ◆ Android devices enrolled in the work-managed device.
- ◆ ActiveSync Only devices

The **Profile Security** tab is for Android devices enrolled in the work profile mode.

4 Click **Apply**.

5 Click **Publish** to display the Publish Option page. In this page you can publish the modified policy as a new version of the same policy or as a new policy.

Password

NOTE

- ◆ After updating to ZENworks 2020 Update 3, by default, for the existing policies, the value for Password Quality will be set as Inherit. Ensure to set the password for the Android 12 devices.
- ◆ For Android 12 devices, the existing mobile password requirements are not supported. Existing password requirements of both the Device and Profile side will be mapped to the complexity levels that Android 12 supports. Password mapping will be done as below:

Table 20-1

Existing Password Requirements	Mapped Value
Require Simple Password	Low
Require Numeric Password	Medium
Require Numeric Complex Password	Medium
Require Complex Password	High
Require BioMetric Weak Password	Low
Require Alphanumeric Password	High
Require Alphabetic Password	High

The Password settings are listed in increasing order of complexity (strictness). If more than one setting applies to a device, the more complex (strict) setting is enforced. The platform for which these restrictions apply are mentioned in the Platform Support column. For Android devices (fully managed) these restrictions are applicable for work-managed devices only. To set password restrictions for the work profile, see [Profile Security](#).

Setting	Description	Platform Support
Require password	Requires a password to unlock the device.	Android 12 or higher, Android 11 or lower, iOS, ActiveSync

Setting	Description	Platform Support
Password Quality	<p>Requires setting the password complexity for Android 12 devices.</p> <ul style="list-style-type: none"> ◆ None: No password is required ◆ Low: <ul style="list-style-type: none"> ◆ Pattern ◆ PIN with repeating (4444) or ordered (1234, 4321, 2468) sequences ◆ Medium: <ul style="list-style-type: none"> ◆ PIN with no repeating (4444) or ordered (1234, 4321, 2468) sequence and length of at least 4 ◆ Alphabetic, length at least 4 ◆ Alphanumeric, length at least 4 ◆ High: <ul style="list-style-type: none"> ◆ PIN with no repeating (4444) or ordered (1234, 4321, 2468) sequence and length of at least 8 ◆ Alphabetic, length at least 6 ◆ Alphanumeric, length at least 6 	Android 12 or higher
Require biometric weak password	Requires at least low-security biometric recognition technology that can recognize the identity of an individual to about a 3 digit PIN (false detection is less than 1 in 1,000).	Android 11 or lower
Require simple password	<p>Allows the password to include repeating characters such as (0000) or sequential characters such as (abcd).</p> <p>This setting behaves differently on Android and iOS devices. For Android devices, the strictest rule gets applied. However, for iOS devices, the rule that is applied is cumulative of all the set rules.</p>	Android 11 or lower, iOS, ActiveSync
Minimum password length	Specifies the minimum number of characters required for the password.	Android 11 or lower, iOS, ActiveSync
Require numeric password	Requires the password to contain numbers. Other characters (letters and symbols) are optional.	Android 11 or lower
Require numeric complex password	Requires the password to contain numbers, with no repeating numbers (4444) or sequential numbers (1234). Other characters (letters and symbols) are optional.	Android 11 or lower

Setting	Description	Platform Support
Require alphabetic password	Requires the password to contain letters (or symbols). Other characters (numbers) are optional.	Android 11 or lower
Require alphanumeric password	Requires the password to contain letters (or symbols) and numbers.	Android 11 or lower, iOS, ActiveSync
Require complex password	Requires the password to contain letters, numbers, and symbols.	Android 11 or lower, iOS, ActiveSync
Minimum complex character types	<p>Applies only if Require complex password is set to Yes or Inherit.</p> <p>Specifies the minimum number of character types the complex password must contain. Character types are defined as:</p> <ul style="list-style-type: none"> ◆ Lowercase alphabetical characters ◆ Uppercase alphabetical characters ◆ Numbers ◆ Non-alphanumeric characters 	ActiveSync
Minimum complex characters required	<p>Applies only if Require complex password is set to Yes or Inherit.</p> <p>Specifies the minimum number of characters required for the complex password.</p>	Android 11 or lower, iOS,
Minimum letters required	<p>Applies only if Require complex password is set to Yes or Inherit.</p> <p>Specifies the minimum number of letters that must be included in the complex password.</p>	Android 11 or lower
Minimum numbers required	<p>Applies only if Require complex password is set to Yes or Inherit.</p> <p>Specifies the minimum number of numbers that must be included in the complex password.</p>	Android 11 or lower
Minimum lowercase letters required	<p>Applies only if Require complex password is set to Yes or Inherit.</p> <p>Specifies the minimum number of lowercase letters (abcd) that must be included in the complex password.</p>	Android 11 or lower
Minimum uppercase letters required	<p>Applies only if Require complex password is set to Yes or Inherit.</p> <p>Specifies the minimum number of uppercase letters (ABCD) that must be included in the complex password.</p>	Android 11 or lower

Setting	Description	Platform Support
Minimum nonletters required	Applies only if Require complex password is set to Yes or Inherit . Specifies the minimum number of numbers or symbols that must be included in the complex password.	Android 11 or lower
Require password expiration	Requires the password to expire within a specified number of days.	Android 12 or higher, Android 11 or lower, iOS, ActiveSync
Password expiration (days)	Applies only if Require device password expiration is set to Yes . Specifies the number of days after which the password expires and must be changed. For example, if set to 30, the password expires after 30 days and must be changed.	Android 12 or higher, Android 11 or lower, iOS, ActiveSync
Require password history	Requires a history of used passwords to be stored in order to prevent immediate reuse of passwords.	Android 12 or higher, Android 11 or lower, iOS, ActiveSync
Number of passwords stored	Applies only if Require device password history is set to Yes . Specifies the number of passwords stored in the history. For example, if set to 5, the last 5 passwords cannot be reused.	Android 12 or higher, Android 11 or lower, iOS, ActiveSync

NOTE: In this policy, even when you specify the minimum password length as a value that is less than 6, an iOS device (version 11 or newer), to which this policy is assigned, prompts for a password length of minimum 6 characters. However, the device accepts a password length that is less than 6 characters, as specified in the policy.

Encryption

Not all Encryption settings apply to all device platforms. In addition, the setting support can vary from version to version within a platform. For Android devices (fully managed) these restrictions are applicable for work-managed devices only. Encryption settings for the work profile cannot be set.

Setting	Description	Platform Support
Require encryption on the device	Requires content stored on the device to be encrypted.	Android, ActiveSync
Require encryption on the storage card	Requires content on the storage card to be encrypted.	ActiveSync

Device Inactivity

Not all Device Inactivity settings apply to all device platforms. In addition, setting support can vary from version to version within a platform. For Android devices (fully managed) these restrictions are applicable for work-managed devices only. To set inactivity restrictions for the work profile, see [Profile Security](#).

Setting	Description	Platform Support
Require inactivity lock	Requires the device to be locked after it has been inactive for a specified period of time.	Android, iOS, ActiveSync
Maximum inactivity timeout (minutes)	Applies only if Require inactivity lock is set to Yes . Specifies the maximum number of minutes the user can set for the inactivity lock. For example, if set to 5, the user can set the inactivity timeout up to 5 minutes.	Android, iOS, ActiveSync
Wipe device on failed number of unlock attempts	Wipes the device data after a specified number of failed attempts to unlock the device.	Android, iOS, ActiveSync
Maximum number of unlock attempts	Applies only if Wipe device on failed number of unlock attempts is set to Yes . Specifies the number of failed attempts to unlock the device that is allowed before the device data is wiped. For example, if set to 10, the device is wiped after the 10th failed attempt.	Android, iOS, ActiveSync
Configure time period after which passcode is required	Enables you to define when a passcode is required after a period of inactivity.	iOS
Display the passcode screen on unlock	Displays the passcode at the specified time period, after a period of inactivity. For example, if set to After 5 minutes , the passcode is displayed after 5 minutes of inactivity.	iOS

Profile Security

This setting is applicable for Android devices enrolled in the work profile mode. To enable the **Profile Security** settings, select **Yes** from the **Secure Work Profile** drop-down list for the ownership type with which the devices are enrolled (Corporate or Personal).

NOTE: If you have assigned the profile security password settings to a device and the *Use one lock* feature is enabled on the same device (under *Settings > Security*), then the password setting with a stricter restriction is applied both on the device as well as the work profile. For example, if the configured work profile password is more complex than the configured device password, then the work profile password is used to unlock the device as well.

Section	Setting	Description	Platform Support
Password	Require password	Requires a password to unlock the device.	Android 12 or higher, Android 11 or lower
	Password Quality	<p>Requires setting the password complexity for Android 12 devices.</p> <ul style="list-style-type: none"> ◆ None: No password is required ◆ Low: <ul style="list-style-type: none"> ◆ Pattern ◆ PIN with repeating (4444) or ordered (1234, 4321, 2468) sequences ◆ Medium: <ul style="list-style-type: none"> ◆ PIN with no repeating (4444) or ordered (1234, 4321, 2468) sequence and length of at least 4 ◆ Alphabetic, length at least 4 ◆ Alphanumeric, length at least 4 ◆ High: <ul style="list-style-type: none"> ◆ PIN with no repeating (4444) or ordered (1234, 4321, 2468) sequence and length of at least 8 ◆ Alphabetic, length at least 6 ◆ Alphanumeric, length at least 6 	Android 12
	Require biometric weak password	Requires at least low-security biometric recognition technology that can recognize the identity of an individual to about a 3 digit PIN (false detection is less than 1 in 1,000).	Android 11 or lower
	Require simple password	Allows the password to include repeating characters such as (0000) or sequential characters such as (abcd).	Android 11 or lower
	Minimum password length	Specify the minimum number of characters required for the password.	Android 11 or lower

Section	Setting	Description	Platform Support
	Require numeric password	Requires the password to contain numbers. Other characters (letters and symbols) are optional.	Android 11 or lower
	Require numeric complex password	Requires the password to contain numbers, with no repeating numbers (4444) or sequential numbers (1234). Other characters (letters and symbols) are optional.	Android 11 or lower
	Require alphabetic password	Requires the password to contain letters (or symbols). Other characters (numbers) are optional.	Android 11 or lower
	Require alphanumeric password	Requires the password to contain letters (or symbols) and numbers.	Android 11 or lower
	Require complex password	Requires the password to contain letters, numbers, and symbols.	Android 11 or lower
	Minimum complex characters required	Applies only if Require complex password is set to Yes or Inherit . Specify the minimum number of characters required for the complex password.	Android 11 or lower
	Minimum letters required	Applies only if Require complex password is set to Yes or Inherit . Specify the minimum number of letters that must be included in the complex password.	Android 11 or lower
	Minimum numbers required	Applies only if Require complex password is set to Yes or Inherit . Specify the minimum number of numbers that must be included in the complex password.	Android 11 or lower
	Minimum lowercase letters required	Applies only if Require complex password is set to Yes or Inherit . Specify the minimum number of lowercase letters (abcd) that must be included in the complex password.	Android 11 or lower
	Minimum uppercase letters required	Applies only if Require complex password is set to Yes or Inherit . Specify the minimum number of uppercase letters (ABCD) that must be included in the complex password.	Android 11 or lower

Section	Setting	Description	Platform Support
	Minimum non-letters required	Applies only if Require complex password is set to Yes or Inherit . Specify the minimum number of numbers or symbols that must be included in the complex password.	Android 11 or lower
	Require password expiration	Requires the password to expire within a specified number of days.	Android 12 or higher, Android 11 or lower
	Password expiration (days)	Applies only if Require device password expiration is set to Yes . Specifies the number of days after which the password expires and must be changed. For example, if set to 30, the password expires after 30 days and must be changed.	Android 12 or higher, Android 11 or lower
	Require password history	Requires a history of used passwords to be stored in order to prevent immediate reuse of passwords.	Android 12 or higher, Android 11 or lower
	Number of passwords stored	Applies only if Require device password history is set to Yes . Specifies the number of passwords stored in the history. For example, if set to 5, the last 5 passwords cannot be reused.	Android 12 or higher, Android 11 or lower

Section	Setting	Description	Platform Support
Profile Inactivity	Require inactivity lock	Confirms that the device should be locked if the work profile has been inactive for a specified period of time.	Android 12 or higher, Android 11 or lower
	Maximum inactivity timeout (minutes)	Applies only if Require inactivity lock is set to Yes . Specifies the maximum number of minutes the user can set for the inactivity lock. For example, if set to 5, the user can set the inactivity timeout up to 5 minutes.	Android 12 or higher, Android 11 or lower
	Wipe profile on failed number of unlock attempts	Wipes the work profile after the specified number of failed attempts to unlock the device.	Android 12 or higher, Android 11 or lower
	Maximum number of unlock attempts	Applies only if Wipe profile on failed number of unlock attempts is set to Yes . Specifies the number of failed attempts to unlock the work managed app that is allowed before the work profile is wiped. For example, if set to 10, the profile is removed after the 10th failed attempt.	Android 12 or higher, Android 11 or lower

20.2.3 Assigning a Mobile Security Policy

A Mobile Security Policy can be assigned to users or devices. User-assigned policies apply to all devices that the user enrolls. Device-assigned policies apply only to the assigned device.

In addition to assigning policies directly to users and devices, you can assign this policy to user groups, user folders, device groups, and device folders. Each member of the group or folder receives the assignment.

- 1 To assign the policy to users, from the **Policies** list, select the check box in front of the policy, then click **Action > Assign to User**. To assign the policy to devices from the **Policies** list, select the check box in front of the policy, then click **Action > Assign to Device**.
- 2 In the Select Object dialog box, browse for and select the users or devices to whom you want to assign the policy, click **OK** to add them to the list and then click **Next**.
- 3 If the policy is assigned to a device, then the Policy Conflict Resolution page is displayed. In this page, you can set the precedence for device-associated policies and user-associated policies for resolving conflicts that arise when policies of the same type are associated to both devices and users. Define any of the following and click **Next**:
 - ♦ **User Precedence:** The user-associated policy will override the device-associated policy. Select this option to apply policies that are associated to the users first, and then to the devices.

- ♦ **Device Precedence:** The device-associated policy will override the user-associated policy. Select this option to apply policies that are associated to the devices first, and then to the users.
 - ♦ **Device Only:** Select this option to apply policies that are associated to devices alone.
 - ♦ **User Only:** Select this option to apply policies that are associated to users alone.
- 4 Review the summary page and click **Finish** to complete the assignment.
- For more information on the existing Policies section of ZENworks, see [ZENworks Configuration Policies Reference](#).

21 Monitoring Device Compliance

To ensure that devices are compliant with the assigned rules and policies, you can create and assign a Mobile Compliance Policy to the Android devices enrolled in the work profile and work-managed device mode. The Mobile Compliance Policy contains a pre-defined event based on which the compliance of a device is monitored. Using the Compliance Dashboard you can view the compliance status of the devices.

- ♦ [“Creating and Assigning a Mobile Compliance Policy” on page 167](#)
- ♦ [“Viewing the Compliance Dashboard” on page 168](#)

Creating and Assigning a Mobile Compliance Policy

To create a Mobile Compliance Policy:

- 1 Click **Policies** in the left hand pane in ZCC.
- 2 Click **New > Policies** and click **Next**.
- 3 Click **Mobile** and click **Next**.
- 4 Click **General Mobile Policies** and click **Next**.
- 5 Click **Mobile Compliance Policy** and click **Next**.
- 6 Specify a policy name, policy folder and a short description.
- 7 Click the pre-defined event **Non-compliance with Security Policy** to configure the audit, restrict, and remediate settings for non-compliant devices. This event is applicable for devices that do not comply with the assigned Mobile Security Policy. Configure the following:
 - ♦ **Audit:** You can enable auditing for this event for devices that become non-compliant with the assigned Mobile Security Policy.
 - ♦ **Restrict:** You can enforce the following restrictions on non-compliant devices that will be applied after the specified number of days defined in the **Restrict After** field.
 - ♦ **Restrict Work Apps** on Android devices.
 - ♦ **Remediate:** You can enforce remediation actions, that is, **Remove work profile** or **Factory reset the work-managed device**, on non-compliant devices that will be applied after the specified number of days defined in the **Remediate After** field. The device will be unenrolled from ZENworks and retired.

For example, if the number of days specified in the **Restrict After** field (appearing in the **Restrict** tab) is 1 and in the **Remediate After** field (appearing in the **Remediate** tab) is 2 for a device that was reported as non-compliant on January 1st, then the device will be allowed 1 day (24 hours) to become compliant again, failing which device restrictions will be applied on January 2nd. If the device does not become compliant even after 2 days (48 hours) of being non-compliant, the device remediation actions will be applied on January 3rd. The remediation actions will be applied irrespective of whether restrictions are applied on the device or not.

NOTE: The restriction and remediation actions are applied only when the device syncs with the ZENworks server.

You can also configure the event logging and notification settings for each of the **Audit**, **Restrict**, and **Remediate** settings:

- ◆ **Event Logging:** To view the audit logs navigate to **Audit and Messages > Events > Agent Events > Mobile > Compliance**
 - ◆ **Event Classification:** Based on the nature of the event, classify the event as **Critical**, **Major** or **Informational**.
 - ◆ **Days to Keep:** Specify the number of days to keep the audit log before purging it.
- ◆ **Event Notification:** You can notify the user of device non-compliance by sending a message to the user's device. On enabling, you can configure a custom message, which will be sent to the device.

8 Review the summary page and click **Finish**.

Viewing the Compliance Dashboard

The compliance dashboard provides a single view of the compliance status of the devices in the zone.

For more information on the Compliance Dashboard feature, see [Dashboard](#).

22 Provisioning Applications

A bundle consists of all the configuration settings and installation instructions required to deploy and manage applications or profiles on a device. Based on the device platform, ZENworks lets you provision the following types of apps or configuration information, using the existing Bundles feature in ZENworks:

iOS

- ♦ **App Store App:** Allows you to distribute apps available in the Apple App Store. For more information, see [Distributing iOS App Store Apps](#).
- ♦ **iOS Profile:** Allows you to distribute configuration information to iOS devices. This configuration information allows you to manage certain features such as Wi-Fi settings, VPN settings, and restricts certain other device features.
- ♦ **iOS Enterprise:** Allows you to distribute in-house apps that are not meant for public distribution. For more information, see [Distributing iOS Enterprise Apps](#).
- ♦ **VPP Apps:** Allows you to distribute bundles related to apps purchased using the Apple Volume Purchase Program. These bundles are automatically created as soon as an Apple VPP subscription is created. For more information, see [Distributing VPP Apps](#).
- ♦ **iOS Update:** Allows you to distribute an OS update to iOS devices. For more information, see [Distributing iOS Update Bundles](#).

Android and iOS

- ♦ **Wi-Fi Bundle:** Allows you to distribute Wi-Fi configuration to devices. This bundle can be assigned to Android, iOS, devices. For more information on Wi-Fi Profile bundle, see [Distributing Corporate Wi-Fi Settings](#).
- ♦ [Section 22.1, “Distributing iOS App Store Apps,” on page 170](#)
- ♦ [Section 22.2, “Distributing iOS Enterprise Apps,” on page 172](#)
- ♦ [Section 22.3, “Distributing VPP Apps,” on page 172](#)
- ♦ [Section 22.4, “Distributing iOS Update Bundles,” on page 179](#)
- ♦ [Section 22.5, “Distributing Android Apps,” on page 180](#)
- ♦ [Section 22.6, “Distributing Corporate Wi-Fi Settings,” on page 182](#)
- ♦ [Section 22.7, “Assigning Bundles,” on page 186](#)
- ♦ [Section 22.8, “Specifying App Configuration Parameters,” on page 188](#)
- ♦ [Section 22.9, “Installing a Bundle using a Quick Task,” on page 190](#)
- ♦ [Section 22.10, “Viewing Information of Apps Installed on Devices,” on page 191](#)

22.1 Distributing iOS App Store Apps

To distribute apps from the Apple App Store, you need to create an **App Store App** bundle and assign these bundles to users or devices. On distributing the bundle to the device, the device will connect with the Apple store and install the app on the device.

22.1.1 Prerequisites

- ◆ Ensure that the device has an iTunes account in place, so that the iOS devices to which these bundles are distributed, can receive and install the apps.
- ◆ Creating an iOS bundle involves choosing the app to be installed from the Apple App Store. For this, you need to use ZCC of an MDM Server or any other server that has outbound connectivity.

22.1.2 Procedure

- 1 On the Modern Management > Getting Started > Managing iOS/iPadOS Devices, navigate to the **Deploy Applications** section and click **Create Bundles**. Alternatively, from the left hand side navigation pane of ZCC, click **Bundles > New > Bundle**.
- 2 On the Select Bundle Type page, click **iOS/iPadOS Bundle**.
- 3 On the Select Bundle Category page, click **App Store App**.
- 4 On the Define Details page, specify a name for the bundle, select the folder in which to place the bundle, then click **Next**.
- 5 On the Search iOS App page:
 - 5a Specify the following information to search for an app from the Apple store:
 - ◆ **Search for:** You can search the app by specifying the app name, publisher name, or App description.
 - ◆ **Region:** Select the country. The app is displayed only if it is available in the specified country.
 - ◆ **Compatibility:** Select a device such as iPhone, iPad, or All Devices. Apps that are compatible with these devices are displayed in the search results.

NOTE: You can search and create bundles only for apps that have no cost associated with it.

- 5b Click **Search** to view the search result.
- 5c (Optional) Click **Reset** to clear the search and search result.
- 5d Specify a filter to further narrow down the app results in the search results. The search result displays the following:
 - ◆ **Bundle Name:** The application name. Mouse over the icon to view the app description.
 - ◆ **Publisher:** The app publisher name.
 - ◆ **Cost:** The cost associated with the app.
 - ◆ **Size:** Size of the app (KB, MB, or GB).
 - ◆ **Devices:** Displays whether the app is compatible on iPhone, iPad or both.

NOTE: Sorting is supported on the Name, Publisher, Cost, and Size columns.

- 5e Select an app. Click **Next**.
- 6 On the Bundle Details page, the following details are displayed. View or specify the relevant details and click **Next**.
- ◆ **Name:** Displays the default name of the app. You can edit the app name.
 - ◆ **Folder:** Displays the default folder in which the bundle will be created. You can edit the folder location by clicking the search icon.
 - ◆ **Description:** Specify a description for the new bundle. Alternatively, you can select **Use App Description**, which will populate the default description of the app as displayed in the App Store.
 - ◆ **App Details:** The App Details page displays additional information on the chosen app:
 - ◆ **Publisher:** The name of the entity that has published the app.
 - ◆ **Size:** The size of the app.
 - ◆ **Categories:** The App Store categories in which the app is included. For example: Games, Education, Business.
 - ◆ **iTunes Store ID:** The App Store ID which is linked to the App Store. Click the ID to view the app in the iTunes Store.
 - ◆ **Cost:** The cost associated with the app.
 - ◆ **App Region:** The country associated with the app.
 - ◆ **Device Compatibility:** The supported devices that can run the app.
 - ◆ **OS version compatibility:** The supported operating system versions of iOS.
 - ◆ **Supported Languages:** The supported languages for the app.
- 7 On the **App Settings** page, you can configure additional settings for the app:
- ◆ **Allow ZENworks to take ownership of the app, if the app is already installed on the device:** If the app is already installed on the device, this option allows ZENworks to manage the app on the device. If this option is selected, then the ownership will be retained by ZENworks even if it is unchecked in the subsequent versions of the bundle.
 - ◆ **Retain app on the device if the bundle is deleted or unassigned, or if the device is removed from the zone:** Retains the app on the device if the bundle is deleted, unassigned, blocked, or disabled, or if the device is removed from the zone. Subsequently, ZENworks will no longer manage the app on the device.
 - ◆ **Prevent backup of app data to iCloud:** Prevents the app data from getting synced with iCloud. You will not be able to retrieve the app data if the device has unenrolled from the ZENworks Management Zone.
 - ◆ **Create Sandbox:** Creates a Sandbox-only version of the bundle. A Sandbox version of a bundle enables you to test it on your device before actually deploying it.
- 8 Click **Finish** to complete the activity.

You can continue to assign this bundle to an iOS device. For more information, see [Assigning Bundles](#).

22.2 Distributing iOS Enterprise Apps

This bundle lets you distribute an enterprise app or an in-house app that is not meant to be available for the general public and is not published in the app store.

22.2.1 Procedure

- 1 On the Modern Management > Getting Started > Managing iOS/iPadOS Devices, navigate to the **Deploy Applications** section and click **Create Bundles**. Alternatively, from the left hand side navigation pane of ZCC, click **Bundles > New > Bundle**.
- 2 On the Select Bundle Type page, click **iOS Bundle**.
- 3 On the Select Bundle Category page, click **iOS Enterprise**.
- 4 On the Define Details page, specify a name for the bundle, select the folder in which to place the bundle, then click **Next**.
- 5 In the Import App Information page, you can import the enterprise app information by performing any of the following operations:
 - ♦ **IPA File:** Upload a .IPA file which contains the app information. Ensure that the app name, the app identifier and the minimum OS version parameters are specified in the info.plist (within the uploaded .IPA file), without which you will be unable to proceed further.
 - ♦ **Manifest URL:** Specify the URL of the manifest file that will be used by the device to find, download and install the app. If the manifest file is hosted on an external server whose server certificate is not trusted by a well-known CA, then you will be required to trust the SSL certificate of this external server to enable ZENworks to securely access the server. This server certificate should also be trusted by the device, failing which the device will be not be able to read the app information in the specified manifest URL.

Click **Next**.

- 6 In the summary page, click **Create Sandbox**, if you want to create a Sandbox only version of the bundle.
- 7 Click **Finish** to complete the activity.

You can continue to assign this bundle to an iOS device. For more information, see [Assigning Bundles](#).

22.3 Distributing VPP Apps

The Apple Volume Purchase Program (VPP) allows organizations to purchase apps in volume to distribute to their managed devices. Using ZENworks, administrators can easily distribute, reclaim, and reassign iOS apps using the existing Bundles workflow. Your organization might possess multiple VPP accounts. ZENworks can distribute licenses from multiple such VPP accounts to both iOS devices.

ZENworks lets you purchase and distribute VPP apps using the Apple Deployment Programs account and Apple Business Manager. In Apple Deployment Programs all licenses are linked to the email ID of the VPP purchaser and it uses an account-based token (hereafter referred to as legacy token within this document). Whereas, in Apple Business Manager all licenses are linked to a location and it uses

a location-based token. ZENworks lets you associate a location-based token to an existing subscription and ensures that all existing bundle assignments work seamlessly with Apple Business Manager.

If you have already enrolled in the Apple Deployment Programs account and want to upgrade to Apple Business Manager, then before migrating, it is recommended that you review the best practices for migration by referring to both the [Apple Support](#) documentation (for general information on the migration process) and the [Migrating to Apple Business Manager](#) section (for information on migrating to a location-based token in ZENworks) within this guide. This will ensure that Apple Business Manager works seamlessly with ZENworks and the existing bundle assignments are not affected.

IMPORTANT: If you are purchasing VPP apps using Apple School Manager, ensure that the Content Manager role is assigned to your Apple School Manager account. For more information, see the [Apple School Manager Help](#).

22.3.1 Linking ZENworks to the Apple VPP Account

To help ZENworks distribute the apps purchased through the Apple VPP, you need to create an Apple VPP Subscription in ZCC. This will enable you to link your ZENworks Server to the VPP account to retrieve all apps purchased through the VPP account.

NOTE: Before creating an Apple VPP Subscription, ensure that an MDM role is assigned to at least one of the ZENworks Primary Servers. For details, see [Configuring an MDM Server](#).

While creating a subscription, you can also define a schedule based on which bundles for these purchased apps will be automatically created by ZENworks.

Prerequisites

You can enroll in either of the following programs

- ♦ **Apple Deployment Programs account:** Navigate to deploy.apple.com and create your program agent account. For more information, see the [Apple Documentation](#).
- ♦ **Apple Business Manager:** Navigate to business.apple.com to create your Apple Business Manager account. For more information, see the [Apple Documentation](#).

Procedure

- 1 On the Modern Management > Getting Started > Managing iOS/iPadOS Devices page, navigate to **Apple VPP Subscription** and click **Create VPP Subscription**. Alternatively, click **Subscribe and Share > New > Subscription**.
- 2 Select **Apple VPP Subscription** and click **Next**.
- 3 Fill in the fields:
 - Subscription Name:** Specify a unique name for the subscription.
 - Folder:** Browse to the folder in which the subscription will be created. By default, the subscription will be created in the `/Subscriptions` folder.

Description: Provide a short description for the subscription. This description is displayed on the subscription's Summary page. Click **Next**.

4 On the Configure Apple Volume Purchase Program page, perform the following:

4a Download the Apple Volume Purchase Program Token: You can download and link either of the following tokens:

- ◆ For legacy tokens, click Apple **Volume Purchase Program Enrollment Web Portal** to sign in to the Apple VPP portal using the Apple Deployment Programs account. Download the VPP token from the Account Summary page of the Apple VPP portal.
- ◆ For location-based tokens, click Apple **Business Manager Web portal** and sign in using your VPP account credentials. Download the specific location-based VPP token by navigating to Settings > Apps and Books section.

4b Link ZENworks to the Volume Purchase Program server: In ZCC, browse and upload the VPP token. The following information that is associated with the token is retrieved:

- ◆ **Organization:** The name of the organization that has subscribed for the Apple VPP.
- ◆ **Country Code:** The country code associated with the Apple VPP token.
- ◆ **Apple ID:** The Apple ID associated with the Apple VPP token.
- ◆ **Email:** The email address associated with the Apple VPP token.
- ◆ **Location ID:** The unique code associated with the location-based token. This is applicable only for Apple Business Manager accounts.
- ◆ **Location Name:** The name of the location associated with the location-based token. This is applicable only for Apple Business Manager accounts.
- ◆ **Token Expiry:** The expiry date of the Apple VPP token.

After the token is successfully uploaded and linked to ZENworks, any existing licenses associated with the token are reset and the associated users, if any, are also retired. If the token is already in use by another MDM solution, then ZENworks will notify with an appropriate message, after which you can click **Claim Management** to link the token with ZENworks.

If the token was previously used by a subscription (that is deleted but its bundles are retained) within the ZENworks zone, then the new subscription will reflect the licenses already consumed. This is achieved by reconciling the VPP account of the new subscription with the one of the deleted subscription.

Click **Next**.

5 For each app purchased using the Apple VPP, ZENworks retrieves the app details from Apple and creates iOS bundles, which can then be distributed to users or devices. On the Bundle Creation Settings page, click the browse icon to select a folder location where you want the iOS VPP bundles to reside. Within this folder location, another folder with the name of the subscription is created, within which bundles will reside.

You can also configure additional app settings for these bundles:

- ◆ **Allow ZENworks to take ownership of the app, if the app is already installed on the device:** If the app is already installed on the device, this option allows ZENworks to now manage the app. This option is checked by default for all VPP bundles and cannot be modified.

- ♦ **Retain app on the device after unenrolling the device from the ZENworks Management Zone:** Retains the app on the device if the bundle is unassigned or deleted, or if the device is removed from the zone. This option is unchecked by default for all VPP bundles and cannot be modified.
- ♦ **Prevent backup of app data to iCloud:** Prevents the backup data of apps from getting synced with iCloud. You will not be able to retrieve the app data if the device has unenrolled from the zone.
- ♦ **Create Bundle as Sandbox:** Creates a Sandbox-only version of the bundle. A Sandbox version of a bundle enables you to test it on your device before actually deploying it. This option is selected by default for all VPP bundles.

Click **Next**.

- 6 From the **Schedule Type** drop-down list, choose one of the schedule types. Based on the specified schedule, ZENworks retrieves the latest apps associated with the VPP account. Subsequently, bundles are created for only those apps for which bundles are yet to be created.

You can also select the **Launch the Apple Volume Purchase Program Summary page immediately after saving** checkbox, which will re-direct you to the Apps Catalog page. Click **Finish** to complete creating the subscription.

After creating the subscription, you can view its status in the **Subscribe and Share** section of ZCC. **Claim in Progress** and **Claim Failed** statuses indicate that the process to claim management of the VPP account from another MDM solution is either in progress or has failed. If the claim fails, ZENworks will retry until the claim is successful. However, if for any reason the status remains as **Claim Failed** for a substantial period of time, then it is recommended that you delete the subscription along with its bundles and create a new subscription. Until the claim is successful, you will be unable to perform actions such as creating bundles, with this subscription.

IMPORTANT: Any replicated content objects, such as bundles that are associated with Apple VPP Subscriptions should not be shared across multiple zones.

22.3.2 Creating VPP Bundles

ZENworks creates VPP bundles based on the **Schedule Type** selected while creating the Apple VPP Subscription. However, if you have not specified a schedule or if you want to create bundles immediately, then you can perform any of the following actions:

- ♦ Click **Run Now** by navigating to **Subscribe and Share > <Select a Subscription> > Quick Tasks > Run Now** or by navigating to the Summary page of the Apple VPP Subscription. These actions initiate a sync between Apple and ZENworks to retrieve the latest apps. Subsequently, bundles are created for these apps.
- ♦ Click **Create Bundle** on the Apps Catalog page for specific apps. For more information, see [Viewing Apps Catalog](#).

22.3.3 Assigning VPP Bundles

You can distribute apps purchased through the Apple Volume Purchase Program (VPP), by assigning VPP bundles to either the devices or to the users who have enrolled their devices to the zone.

- ◆ [Distribute Bundles to Users](#)
- ◆ [Distribute Bundles to Devices](#)

When a bundle is assigned to a user or a device and the associated device syncs with the ZENworks Server, the app license is **Consumed** from Apple. Subsequently, the user is prompted to confirm the app installation. Based on the user's response, the app is **Installed** on the device. The license consumption and installation count is updated on the Apps Catalog page. For details, see [Viewing Apps Catalog](#).

NOTE: If a bundle is assigned to multiple devices, device groups or folders, or multiple users, user groups or folders, then the app licenses are distributed based on the order in which the devices sync with the ZENworks Server.

Distribute Bundles to Users

VPP Bundles can be distributed to users, user groups, or user folders.

If a VPP bundle is assigned to a user for the first time, then as soon as the first device associated with the user syncs with the ZENworks Server, an invitation is sent to the user to join the Apple VPP.

To accept the invitation, users need to sign-in on their devices with their personal Apple ID. The Apple ID is registered with the Apple VPP, but remains private and is unknown to ZENworks. As soon as the users agree to the invitation and accept the iTunes Store terms and conditions, they are associated with ZENworks. In the next sync, the app license is consumed from Apple and a message is sent to the device prompting the user to confirm whether to install the app or not. Based on the user's response, the app is installed on the device.

NOTE: When the user associates with the Apple VPP, these invites are not re-sent to the user for subsequent assignments.

The Apple ID with which the user has associated for the Apple VPP, should be used across all the user's devices to enable successful installation of VPP apps. Also, it is important that the Apple ID does not change, so that all bundle assignments are successful and all assigned apps are retained on the device. If the user logs into the iTunes account using a different Apple ID, then the apps distributed to the user are revoked.

NOTE: The terms Apple ID and iTunes ID are used interchangeably in ZENworks.

Distribute Bundles to Devices

VPP bundles can be distributed to devices, device groups, or device folders.

VPP bundles can be distributed to only those iOS devices that are running on iOS versions 9.0 or newer.



When a bundle is assigned to the device and the device syncs with the ZENworks Server, the server consumes app license for the device from Apple. If the license consumption is successful, the user is prompted to install the app on the device.

For more information on assigning bundles, see [Assigning Bundles](#).


22.3.4 Updating VPP License Summary

- ♦ **Updating Apps:** Based on the schedule selected while creating the Apple VPP Subscription, ZENworks syncs with Apple to retrieve the latest apps. However, irrespective of the schedule selected, ZENworks automatically syncs with Apple on a daily basis to retrieve the latest apps. Bundles are not created for any newly purchased apps during this sync.

You can also initiate this sync immediately by performing either of the following:

- ♦ Click **Run Now** by navigating to **Subscribe and Share** > **<Select a Subscription>** > **Quick Tasks** > **Run Now** or by navigating to the Summary page of the Apple VPP Subscription. This option also creates bundles for any newly purchased apps.
- ♦ Click  on the Apps Catalog page.
- ♦ **Updating Distributed Licenses:** If an app license is assigned to a device or a user, then the license consumed and installed count is updated when the associated devices syncs with the ZENworks Server. Subsequently, the app is installed on the device.
- ♦ **Revoking Licenses:** Unused app licenses are revoked when the device syncs with the ZENworks Server. To revoke licenses from devices that cannot sync with the ZENworks Server, click  on the Apps Catalog page. This option can be used to revoke licenses in the following scenarios:
 - ♦ Mobile device management on the device is disabled.
 - ♦ The device is in a **Retired** or **Wipe Pending** state. In case of a device assignment, all apps assigned to the device are revoked. In case of a user assignment, if the device is the last device associated with the user, then the app licenses are revoked from the user.
 - ♦ Bundle assignment is removed.
 - ♦ User does not exist anymore.

Alternatively, ZENworks periodically (every two hours) revokes unused licenses from devices that cannot sync with the ZENworks Server. However, if you do not want to wait for the device

to sync or for the periodic schedule to revoke licenses, then clicking  helps in revoking licenses instantaneously.


If any of these tasks fail, then the relevant error messages are displayed when you visit the Apps Catalog page.

22.3.5 Renewing a VPP Token

The validity of a VPP token is one year from the time the token is downloaded. As soon as you upload the token while creating a new subscription in the ZENworks Management Zone, the expiry date of the token is displayed. You can also view the expiry date of token by visiting the **Summary** page of the Apple VPP Subscription. To renew this token, download the token again from the Apple VPP portal and upload it in the **Summary** tab of the Apple VPP Subscription, which can be accessed by clicking the subscription.


22.3.6 Revoking App Licenses

To revoke unused app licenses assigned to a user or a device, you can **Block** the bundle assignment, **Remove** the bundle assignment, or **Disable** the bundle. When any one of these actions is performed and the device syncs with the ZENworks Server, an uninstall command is sent to the device and the app license is revoked. For details on the **Block**, **Remove** and **Disable** options, see [Bundle Tasks](#) in [ZENworks Software Distribution Reference](#).

If the device cannot sync with the ZENworks Server, then you can click  on the Apps Catalog page. This option can be used to revoke licenses in the following scenarios:

- ◆ Mobile device management on the device is disabled.
- ◆ The device is in a **Retired** or **Wipe Pending** state. In case of a device assignment, all apps assigned to the device are to be revoked. In case of a user assignment, if the device is the last device associated with the user, then the app licenses are to be revoked from the user.
- ◆ Bundle assignment is removed.
- ◆ User does not exist anymore.

As stated earlier, unused app licenses are revoked when the device syncs with the ZENworks Server. Also, every two hours ZENworks automatically revokes unused licenses from devices that cannot sync with the ZENworks Server. However, if you do not want to wait for the device to sync or for

ZENworks to automatically revoke licenses, then clicking  helps in revoking licenses instantaneously.

22.3.7 Deleting VPP Subscription

If you delete a subscription, all of its associated bundles are retained in the zone. If a token that was previously linked to a deleted subscription (but the bundles are retained), is now linked to a new subscription within the same zone, then the VPP account of the new subscription reconciles with the one of the deleted subscription. The new subscription will reflect the licenses that are already consumed. However, if after deleting the subscription from Zone 1, a new subscription is created with the same token in Zone 2, then while creating a new subscription with the same token in Zone 1 you will have to associate a new VPP account with the subscription and all existing bundles that were retained in zone 1 will be deleted.

NOTE: If you want to delete the subscription successfully, including all its bundles, then you need to have the relevant Bundle rights assigned to you. For details, see [Bundle Rights](#) in the [ZENworks Administrator Accounts and Rights Reference](#) guide.

22.4 Distributing iOS Update Bundles

An OS update for mobile devices are vital as it provides a whole lot of feature improvements and vulnerability fixes. However, if the devices are not updated with the latest OS update, then the device might be vulnerable to critical enterprise risks.

This Update feature enables ZENworks administrators to enforce the OS update on all supervised devices in the zone. To enforce the OS update on mobile devices, you need to create an iOS Update bundle and then assign the bundle to the devices.

1. In ZENworks Control Center, click **Bundles**.
2. In the Bundles page, click **New**, and then select **Bundles**.
3. Select **iOS Bundle** and click **Next**.
4. Select **iOS Update** and click **Next**.
5. In the Define Details page, perform the following steps, and then click Next:
 - ◆ Specify a bundle name.
 - ◆ Select a folder for the bundle.
 - ◆ Specify a description for the bundle.
6. In the Available update versions page, the Available update versions drop-down lists all the available OS update. Select the available update.

NOTE

- ◆ Depending on the iOS update versions available for the iOS devices in your Management Zone, the Available update versions list is populated.
- ◆ If the iOS update is not listed, then none of the devices in the zone has reported the version as an available OS update.

After selecting the update version, following information is displayed:

- ◆ Product Name
 - ◆ Product Key
 - ◆ Version
 - ◆ Build
 - ◆ Is Update Critical
 - ◆ Is Restart Required
7. Review the OS update information, and then click Next.
 8. In the Summary page, review the information, and then click Finish.

IMPORTANT

- ◆ Ensure that you assign the iOS Update bundles only to supervised devices.
- ◆ If a passcode is enabled on the device, the OS update is downloaded, but the update will not be installed on the device. To install the update, you need to perform the following steps:
 1. Create and assign the bundle to the device.

2. Assign the Unlock Device quick task.

As soon as the device is unlocked, the OS update is initiated on the device.

- ◆ After the update is downloaded, it will be installed as part of the next device refresh and the device will reboot automatically.
-

NOTE: If the passcode is disabled for updating the device, then after the device is updated, ensure that the users enable the passcode again. You can also assign the Mobile Security Policy to enforce the users to set the passcode on their devices.

For more information, see [Mobile Security Policy](#).

22.4.1 Assigning the iOS Update Bundle

After creating the iOS update bundle you need to assign the bundle to the devices. For information on assigning the bundle, see the [Assigning iOS App Store App, Enterprise, Profile, and Corporate Bundle](#) section.

NOTE: The OS update will be downloaded to the device from the Apple server, and then it will be installed on the device during the next device sync.

22.5 Distributing Android Apps

ZENworks lets you distribute Android work apps to Android devices enrolled in the work-managed or work profile modes. ZENworks distributes work apps to users through managed Google Play, which is Android's app management platform for enterprise users. Subsequently, all app licenses are managed by ZENworks through managed Google Play.

ZENworks also lets you distribute the System App bundles and Android Enterprise App bundles to enable or disable apps on Android devices.

22.5.1 Distributing Android Enterprise Apps

To distribute apps from the Google Play Store, you need to create an Android Enterprise App bundle and assign these bundles to users or devices. On assigning the bundle to a mobile device, the assigned app will be distributed to the device based on the assignment schedule.:

- 1 In ZENworks Control Center, click **Bundles**.
- 2 In the Bundles page, click **New**, and then select **Bundles**.
- 3 In the Select Bundle type page, select **Android Bundle**, and then select **Android Enterprise App**.
- 4 Specify the bundle details, and then click **Next**.
- 5 On the Search for an App in Google Play Store page.
 - ◆ Specify the app name in the search field and click the Search icon.
 - ◆ Choose the app. You can view additional details of the app on this page.
 - ◆ Click **Select** and then click **Next**.

Click **Select** and then click **Next**.

The bundle details page displays additional information about the new bundle. Review the information on this page and proceed further.

The following details of the new bundle are displayed:

- ◆ **Bundle Name:** Displays the default name of the app; however, you can edit the app name.
- ◆ **Folder:** Displays the default folder in which the bundle will be created. You can edit the folder location by clicking the browse icon.
- ◆ **Description:** Displays the default description of the app as displayed in the Google Play Store.

The App Details Panel displays additional information about the app. The name of the app and the publisher is displayed along with the following information:

- ◆ **Android Package Name:** Unique identifier of the app in Google Play Store. On clicking this link, you will be directed to the app's page on the Google Play Store.
- ◆ **App version, Track:** All the published app versions along with the track that indicates whether the app is published in the Alpha, Beta or Production version.
- ◆ **Categories:** Google Play Store categories in which the app is included. For example, Games, Education, and Business.
- ◆ **Distribution channel:** Android apps can be published as public apps.
- ◆ **Cost:** Cost associated with the app.
- ◆ **Content rating:** The rating of the app content that is provided by the rating authority, which denotes for what type of audience the app is suitable. The possible values are All, Mature, PreTeen, and Teen.
- ◆ **Last published on:** The timestamp to indicate when the app was last published.

You can configure additional settings of the app, before creating a bundle:

- ◆ **Create as Sandbox:** (Optional) Select the Create as Sandbox option to create a sandbox-only version of the bundle. A Sandbox version of a bundle enables you to test it on your device before deploying it.
- ◆ **Define Additional Properties:** (Optional) Select the Define Additional Properties option to display the bundle's Action page after the wizard completes. You can use the various tabs to edit the bundle's assignments, system requirements, actions, settings, and content replication settings.


6 Click **Finish** to complete creating the bundle.

22.5.2 Updating Android Apps

NOTE: The option to update Android apps is only available if you are using ZENworks 2020 Update 2 - FTF 1008 and above.

Based on the schedule selected while creating the Android Enterprise Subscription, ZENworks syncs with Google to retrieve the latest apps. However, irrespective of the schedule selected, ZENworks automatically syncs with Google on a daily basis to retrieve the latest apps. Bundles are not created for any newly purchased apps during this sync.

You can also initiate this sync immediately by performing either of the following:

- ◆ Click **Run Now** by navigating to **Subscribe and Share > Quick Tasks > Run Now** or by navigating to the Summary page of the subscription.
- ◆ Click  on the App Catalog page.

22.6 Distributing Corporate Wi-Fi Settings

A Wi-Fi Profile bundle enables deployment of wireless network settings to managed devices or users. Deploying these Wi-Fi configurations makes it easier for users to connect to the corporate Wi-Fi. The Wi-Fi Profile bundle enables devices to connect to corporate networks, even if the Wi-Fi is hidden, encrypted or password protected.

For example, if you have a corporate Wi-Fi network that should connect only to Android devices, then create a Wi-Fi Profile bundle, which includes all the necessary settings to connect to the wireless network. Deploy the bundle to all Android devices in your management zone. Users with Android devices can readily connect to the corporate network.

- ◆ [Section 22.6.1, “Creating a Wi-Fi Profile bundle,” on page 182](#)
- ◆ [Section 22.6.2, “Managing the Wi-Fi Profile Bundle,” on page 185](#)

22.6.1 Creating a Wi-Fi Profile bundle

IMPORTANT

- ◆ In an Android device, if a Wi-Fi profile with an SSID is already installed by another user or a third-party app, then another profile with the same SSID cannot be installed on the device. As a workaround, you need to remove the existing Wi-Fi profile, and then reassign the Wi-Fi Profile bundle to the device.
- ◆ In an iOS device, multiple bundles with the same SSID can be installed.

-
- 1 In ZENworks Control Center, click **Bundles**.
 - 2 In the Bundles page, click **New**, and then select **Bundles**.
 - 3 In the Select Bundle type page, select **Corporate Bundle**, and then select **Wi-Fi Profile**.
 - 4 Specify the bundle details, and then click **Next**.
 - 5 In the Specify Network Identity page, specify the required network details, and then click **Next**. For more information on the settings on this page, see [Network Identity](#).
 - 6 In the Specify Security information page, select the **Security Type**. Specify the required information, and then click **Next**. For more information on the settings on this page, see [Security Information](#).
 - 7 In the Trust Certificates page, you can upload a certificate that will be used for communication between the devices and the Wi-Fi router. Specify the required information, and then click **Next**. For more information on the settings on this page, see [Trust Certificates](#).
 - 8 In the Summary page, review all the updated information and then click **Finish**.

- 9 (Optional) Select the **Create as Sandbox** option to create a sandbox-only version of the bundle.
- 10 (Optional) Select the **Define Additional Properties** option, which will display additional details of the bundle. For more information on the Details page, see [Managing the Wi-Fi Profile Bundle](#).

Network Identity

Specify the following network identifiers:

- ◆ **Service Set Identified (SSID):** Specify a unique identifier that the wireless networking devices use to establish and maintain wireless connectivity.
- ◆ **Hidden Network:** Select this option if the network access is not broadcast.
- ◆ **Auto Join:** Select this option if devices should automatically join the Wi-Fi network. If this option is not selected, users must select the network name on the device to join the network.
- ◆ **Disable Captive Network Detection:** Select this option to bypass the Captive network detection when the device connects to the network.

Security Information

Depending on the selected Security Type, the relevant fields are displayed. The Security Type field has the following options:

- ◆ **None:** Select this option, if you do not want to specify any security information for the Wi-Fi profile.
- ◆ **Enterprise:** Select this option, if you are configuring an Wi-Fi profile for an enterprise. For more information see [Enterprise](#).
- ◆ **Personal:** Select this option, if you are configuring an Wi-Fi profile for personal use. For more information see [Personal](#).

Enterprise

If Enterprise is selected as the Security Type, then following fields are displayed:

- ◆ **Encryption Type:** Select the encryption type that can be used to encrypt this network. Possible values are WEP, WPA, and WPA2. Depending on the network access point, select the required encryption type.
- ◆ **EAP Type:** Select the EAP types that can be used to access this network. Depending on your network configuration, select any one EAP Type.

Following are the available EAP Types:

- ◆ TTLS
- ◆ EAP-FAST
- ◆ PEAP
- ◆ LEAP
- ◆ EAP-SIM
- ◆ EAP-AKA
- ◆ PWD
- ◆ AKA-PRIME

Depending on the selected EAP type, one of the following fields are displayed:

- ◆ **User Name:** Specify the user name required to access the network. If the user name field is not specified, then the user will be prompted for the user name while accessing the network.
- ◆ **Password:** : Specify the password to access the network. If the password field is not specified, the device user will be prompted for the password.
- ◆ **Use Per-Connection Password:** Select this option to prompt the user for a password for each connection. When the device rejoins the same network, the device user will be prompted to re-authenticate.
- ◆ **Inner Authentication:** Select the protocol used to authenticate the user name and password (None, CHAP, MSCHAP, MSCHAPv2, PAP, EA or GTC). The None option is valid only for Android devices.
- ◆ **Outer Identity:** Specify an alternate user name to be used outside the encrypted tunnel to conceal the user's identity.
- ◆ **Minimum TLS Version:** Specify the minimum TLS version. By default, Minimum TLS Version is 1.0.
- ◆ **Maximum TLS Version:** : Specify the maximum TLS version. By default, Maximum TLS Version is 1.2.
- ◆ **Use PAC:** Select this option to use Protect Access Credentials (PAC).
PACs are strong shared secrets that enable EAP-FAST end-user clients to authenticate each other and establish a TLS tunnel.
- ◆ **Provision PAC:** If this option is selected, then a new PAC is sent to the end-user client over a secured network connection. Automatic PAC provisioning requires no intervention of the network user or administrator, provided the server and the end-user client are configured to support automatic provisioning.
- ◆ **Provision PAC Anonymously:** If this option is selected, the administrator should generate PAC files, which must then be distributed to the applicable network users. Users must configure end-user clients with the PAC files.
- ◆ **Allow two RANDs:** Number of expected RANDs for EAP-SIM. Select the check box to use 2 RANDs for network security.

Personal

If Personal is selected as the Security Type, then the following fields are displayed:

- ◆ **Password:** Specify the password to access the network. If the password field is not specified, then the device user will be prompted for the password.

IMPORTANT: : Based on the Android versions of the devices, ensure that you specify a password that meets the minimum requirements:

- ◆ Android 6, 7 and 8 (Oreo): Minimum password length is 7 characters.
- ◆ Android 9 (Pie): Minimum password length is 8 characters.

If the password length does not meet the Android operating system requirements, the bundle installation might fail on the device.

Trust Certificates

In this section, you can either upload a trust certificate, or add a certificate name that is already approved by the Certificate Authority.

Trust Certificate

In this section, you can upload any number of certificates that will be used to communicate between devices and the Wi-Fi router.

To upload a trust certificate:

1. Click **Add**, in the **Add Trust Certificate** pop-up, and then click **Browse**.
2. In the **File Upload** dialog box, select the required certificate file.

Trusted Server Certificate Names

In this section, you can add a trusted certificate that is already approved by the Certificate Authority.

- ◆ To add a trusted certificate name, click **Add**, specify the certificate name, and then click **OK**.

IMPORTANT: On Android 5 (Lollipop) and 6 (Marshmallow) devices:

- ◆ Only one certificate can be installed on the device.
- ◆ The binary encoded certificate (DER format) is not supported.

If a certificate is installed on the device, it cannot be removed, but can be replaced with another certificate.

22.6.2 Managing the Wi-Fi Profile Bundle

After creating a bundle, based on requirements, you can modify the bundle. For more information, see [Viewing the Bundle Information](#) in the [ZENworks Software Distribution Reference](#).

Details

In the Details tab, you can modify the following settings:

- ◆ [Network Identity](#)
- ◆ [Security Information](#)
- ◆ [Trust Certificates](#)
- ◆ [Proxy](#)

Proxy

In this section, configure the proxy server that should be used with this network. Depending on the selected Proxy Setup, the relevant fields are displayed.

- ◆ **None:** If the Proxy Setup is selected as None, then no field is displayed.

- ♦ **Manual:** If the Proxy Setup is selected as Manual, then following fields are displayed:
 - ♦ **Server and Port:** Specify the proxy server address and port number.
 - ♦ **User Name:** Specify the user name to access the proxy server.
 - ♦ **Password:** Specify the password for the proxy server.
- ♦ **Automatic:** If the Proxy Setup is selected as Automatic, then the following fields are displayed:
 - ♦ **Proxy URL:** Specify the fully-qualified URL to retrieve proxy settings.
- ♦ **Allow direct connection if PAC is unreachable:** Select this option if you want to allow users to connect directly to the destination when the PAC file is unreachable.

IMPORTANT

- ♦ On Android 5 (Lollipop), 6 (Marshmallow), and 7 (Nougat) devices, proxy is not supported.
 - ♦ On Android 8 and above, Manual proxy is not supported.
-

22.7 Assigning Bundles

22.7.1 Assigning iOS App Store App, Enterprise, Profile, and Corporate Bundle

- 1 In ZENworks Control Center, click **Bundles** (in the left navigation pane).
- 2 To assign the bundle to users, from the **Bundles** list, select the check box in front of the bundle, then click **Action > Assign to User**. To assign the bundle to devices, select the check box in front of the bundle, then click **Action > Assign to Device**.
- 3 In the **Select Object** dialog box, browse and select the users or devices to whom you want to assign the bundle, click **OK** to add them to the list, then click **Next**.
- 4 On the App Installation Schedule page, specify a schedule based on which the ZENworks Server triggers a notification to install the app on the device. You can select from one of the following schedules and click **Next**:

Now: indicates that a notification to install the app is sent to the device immediately. On selecting this schedule, you can select any of the following options:

NOTE: This is applicable for device assignments only.

Option	Steps
Quick Task Notification Options	<p>Select one of the following:</p> <ul style="list-style-type: none"> ◆ Notify all the devices immediately: Select this option to send the quick task notification to all the devices, immediately. ◆ Notify all the devices within _ mins: Select this option to send the quick task notification to all the devices within the specified time. The minimum time that can be set is 1 min. By default, the notification time is set to 10 minutes. You can choose to specify the notification time according to your requirements.
Quick Task Expiry Option	<p>Select one of the following:</p> <ul style="list-style-type: none"> ◆ Never Expires: Select this option if you never want the quick task to expire. ◆ Expires after _ mins of the quick task creation: Select this option to specify in minutes, the time at which the quick task should expire after it is created. By default, the expiry time is set to 20 minutes. You can choose to specify the expiration time according to your requirement.

Event: Select when the app should be installed on the device:

- ◆ **Next Refresh:** Indicates that a notification to install the app will be sent on the subsequent refresh of the device. On refresh, a dialog box is displayed on the device to either accept or decline the request to install the app. This is a one time notification and will not be re-sent by the ZENworks Server if the user declines to install the app.
 - ◆ **Every Refresh:** Indicates that a notification to install the app will be sent to the device each time a refresh action is performed on the device. On refresh, a dialog box is displayed on the device to either accept or decline the request to install the app on the device. If the user declines the request to install the app on the device, then the ZENworks Server will continue sending these notifications till the user accepts the request. Also, if the user has uninstalled the bundle, this notification will be re-sent to the device when it syncs with the ZENworks Server.
- 5 If a bundle is assigned to a device, then on the Bundle Conflict Resolution page, set the priority between device-associated bundles and user associated bundles to resolve conflicts that arise when the same bundle is associated with devices and users. Select any one of the following and click **Next**
- ◆ **User Precedence:** The user-associated bundle will override the device-associated bundle. Select this option to apply bundles that are associated to the users first, and then to the devices.
 - ◆ **Device Precedence:** The device-associated bundle will override the user-associated bundle. Select this option to apply bundles that are associated to the devices first, and then to the users.
- 6 Click **Finish** to complete creating the bundle.

NOTE

- ◆ Before a bundle is sent to the device, to ensure that the right bundle is assigned to the device, precomputed effective assignments are calculated. For details, see [Infrastructure Management Settings](#) in the [ZENworks Management Zone Settings Reference](#).

During the installation of an App Store App bundle, ZENworks sends the iTunes ID of the app to the device. The device then downloads the app from the Apple App Store using this iTunes ID.

- ◆ If you are assigning an app through the iOS app store and if you have not logged into the iTunes store, then you will be prompted to log in to the app store for the first time and the subsequent app assignment will not prompt you to log in and app assignment will be seamless.
-

22.8 Specifying App Configuration Parameters

As a part of the setup process, many apps require users to specify their email addresses, the port and other configuration settings. The app configuration parameters feature helps in providing the configuration information for apps that support this feature. ZENworks lets you pre-configure this information that become effective as soon as the app is installed on the device. The users are not required to specify these values manually. For each app, the configuration parameters are published in the specific app documentation.



This feature is applicable for the following bundles:

- ◆ App Store App
- ◆ iOS Enterprise
- ◆ VPP Apps
- ◆ Android Bundle

ZENworks also supports app configuration of Micro Focus' in-house apps, such as Micro Focus Filr, Novell Messenger, and Micro Focus iPrint. For each of these apps, you can obtain their configuration parameters by clicking the following links:

- ◆ **Micro Focus Filr:** see [Key-Value pairs](#) in the [Maintenance Best Practices Guide](#).
- ◆ **Micro Focus iPrint:** see [Key-Value pairs](#) in the [Micro Focus iPrint Appliance 3 Administration Guide](#).

22.8.1 Procedure

To navigate to the [App Configuration Parameters](#) page, select **Bundles**, select a bundle and click the **Details** tab. Alternatively, for Android apps, you can visit **Modern Management > Apps Catalog** and identify the app against which the  icon is displayed. This icon indicates that either app permissions or managed configuration parameters require your attention. You can then click the bundle count appearing beside this app and select the bundle against which the  icon is displayed and navigate to the **Details** tab.

Pre-configuring iOS Apps

You can pre-configure App Store apps, VPP apps or Enterprise apps by selecting either one of the following options:

- ◆ **Key-value pairs:** Click **Add** and specify the **Key** and its corresponding **Value**. You can specify the value as a string, integer, or as a boolean value. You can also specify built-in variables or custom variables as the **Value**. The following built-in system variables can be used:
 - ◆ **\${LoginName}:** Retrieves the user login name in the configured user source.
 - ◆ **\${Email}:** Retrieves the first email address associated with the user from the user source.
 - ◆ **\${ActiveSyncLogonName}:** Retrieves the ActiveSync logon attribute from the user source. This attribute is used to authenticate to the ActiveSync Server, while configuring an email account on the device.

To specify custom variables, you first need to define these variables by navigating to **Configuration > Device Management > System Variables**. For more information, see [Using System Variables](#).

- ◆ **Configuration File:** Click **Upload** to browse and import a configuration file that contains the configuration information of the app. You can also directly specify the file parameters or edit the parameters of the uploaded file in the displayed text box. The configuration file can be obtained from the app vendor.

You need to ensure that a valid configuration file is imported. A sample format of the configuration file is provided below:

```
<key>Configuration</key>
<dict>
  <key>username</key>
  <string>username@example.com</string>
  <key>server</key>
  <string>exampleserver.com</string>
</dict>
```

Built-in or custom variables can also be added as string values within this configuration file. For example:

```
<key>com.ibm.mobile.connections.user</key>
<string>${LoginName}</string>
```

The application configuration will be pushed to the device when the application is distributed.

Pre-configuring Android Apps

Select a parameter and click **Edit**. The following are displayed in the **Edit App Configuration Parameter** dialog box.

- ◆ A **Title** and a **Key** are displayed.
- ◆ The **Type** of value that needs to be specified is displayed. The supported value types include boolean, string, integer with a value from MIN_VALUE (-2147483648) to MAX_VALUE (2147483647), choice, multi-select list and bundle array. For the bundle array type, to edit a parameter within a bundle, you need to click the bundle array appearing in the **App**

Configuration Parameters section and drill-down to its parameters. You can also click **Add** to configure multiple bundles within a bundle array that will include the same parameters as the existing bundle.


NOTE: The Bundles and bundle arrays feature used within Managed App Configurations is specific to Google and are not related to the Bundles feature in ZENworks. Also, this feature is only supported on Android M (6.0) and later versions. On versions older than Android 6.0, these properties are silently dropped on the devices.

Also, if the configuration parameters of an app is not in accordance with Google's guidelines, then these parameters will not be displayed by ZENworks. For more information, see [Table 1: Restriction entry types and usage](#).

- ◆ A short description of the parameter is displayed as provided by the app developer.
- ◆ Specify the corresponding value for the key. You can also specify custom or built-in system variables such as:
 - ◆ `#{LoginName}`: Retrieves the user login name in the configured user source.
 - ◆ `#{Email}`: Retrieves the first email address associated with the user from the user source.
 - ◆ `#{ActiveSyncLogonName}`: Retrieves the ActiveSync logon attribute from the user source. This attribute is used to authenticate to the ActiveSync Server while configuring an email account on the device.

NOTE: If an incorrect built-in or custom variable is specified, then the bundle will not deploy to the device.

You can also restore the default values set by the app developers for any of the parameters. To do this, select a parameter and click **Default** on the top panel. The app configuration will be pushed to the device when the app is distributed.

Click  to immediately initiate a sync between the Google server and ZENworks to retrieve the latest Android apps.

22.9 Installing a Bundle using a Quick Task

The **Install Bundle** quick task lets you immediately install a bundle to one or more devices.

22.9.1 Procedure

- 1 In ZENworks Control Center, click **Devices > Mobile Devices** to display your enrolled mobile devices.
- 2 Select the check box in front of the mobile device, click **Quick Tasks > Install Bundle** to display the Install Bundle dialog box.
- 3 Browse to the folder location in which the bundle you want to install resides. You can also include additional devices by clicking **Add**. Click **Ok** to display the quick task options.
- 4 Retain the default options and click **Start** to send the message.
- 5 Click **Hide** to close the quick task.



22.10 Viewing Information of Apps Installed on Devices

The list of apps installed on the device, can be viewed in the Apps tab of a specific device in ZCC. The Apps page lists all the apps which are inventoried and assigned to a device.

To view the Apps page:

- 1 In ZCC, click **Devices**.
- 2 In the Devices page, click **Mobile Devices**.
- 3 In the Mobile Devices page, select a device and click **Apps**.

Following are some of the tasks that you can perform in the Apps page.

Task	Description
Export	You can export all the app information displayed in this page as a CSV file. Click Export > As CSV , which creates a ZIP folder. This ZIP folder contains a CSV file, which contains all the app information that are displayed in the Apps page.
Search/Filter	You can filter the data displayed on this page by specifying either the App Name, Publisher, Bundle or the Package Name in the search field. You can further filter the data based on the App Type. To filter the data, click  and select the appropriate option.
Show/Hide Columns	To arrange the columns in the summary page, click  and select the columns that need to be displayed in the summary page.

Following are the columns available for display:

- ♦ **Name:** Displays the name of the app.
- ♦ **Version:** Displays the version of the app.
- ♦ **Publisher:** Displays the name of the app publisher.
- ♦ **Package Name:** Displays the package name that is associated with the app.
- ♦ **Cost:** Displays the cost associated with the app. The app can be free, free with in-app purchases or paid.
- ♦ **App Size:** Displays the size of the app in MBs.
- ♦ **App Store ID:** Displays the app store ID. This is displayed only for iOS devices.
- ♦ **Region:** Displays the name of the geographical location from where the app was installed.
- ♦ **App Type:** Displays the type of app. The app type can be any one of the following:
 - ♦ **System:** Apps that are either a part of the operating system or installed on the device by the device manufacturer. System apps are displayed only for Android devices.
 - ♦ **Managed:** Apps that are managed through ZENworks. A managed app is one that was deployed through ZENworks to a device.

- ♦ **Non-managed:** Apps that are installed by the user that are not managed through ZENworks. A non-managed app is an app that was installed on the device before enrolling with ZENworks, or an app that was downloaded directly from the device without being deployed through ZENworks.
- ♦ **Installation Status:** Displays the installation status of the app. The status can either be **installed** or **not installed**. The status is not installed when the app is assigned, but not installed on the device.
- ♦ **Trusted App:** Displays whether the app is trusted or not. If the app is not installed from Google Play Store (Android) or App Store (iOS), then it is considered as a not trusted app.
- ♦ **App Store Type:** Displays whether the app is downloaded from Google Play (Android) or App Store (iOS).
- ♦ **Apple VPP App:** Displays **Yes** if the app is managed by the Apple Volume Purchase Program (VPP).
- ♦ **Enterprise App:** Displays **Yes** if the app is distributed through Self-hosted private apps or Google-hosted private apps.
- ♦ **Bundle Name:** Displays the name of the bundle through which the app was installed on the device. If the app was installed through one bundle, then the bundle name link is displayed. If multiple bundles were assigned for the same app, the **View Bundles** link is displayed instead of the bundle name link. Click the link to access the bundles page that displays the list of bundles.

23 Viewing Apps Catalog

For a single view of all the iOS and Android apps that are being managed by ZENworks, you can visit the Apps Catalog page. This page lets you view the details of the following apps:



- ♦ **iOS Apps:** Apps that are either purchased using the Apple Volume Purchase Program or obtained from the Apple App Store.
- ♦ **Android Apps:** Apps that are approved using the Android Enterprise program.
- ♦ [“Overview of the Apps Catalog Page” on page 193](#)
- ♦ [“Editing App Permissions” on page 195](#)


Overview of the Apps Catalog Page

Click the **Modern Management** panel and click the Apps Catalog tab. Using this page, you can do the following:

- ♦ **Create Bundles (applicable for Android and iOS VPP apps only):** You can create bundles by selecting one or more apps (for each app an individual iOS or Android bundle is created) by clicking **Action > Create Bundle**. If a bundle for the same app already exists, then for the newly created bundle, the VPP or the Android Enterprise Subscription name is suffixed to the name of the app. For subsequent bundles of the same app, a random GUID number is suffixed to the name of the app.

NOTE: If the sync between ZENworks and Apple is initiated immediately after purchasing an app, then the **Purchased** license count might not display the correct number. Therefore, ensure that you verify the **Purchased** license count before assigning bundles or else distribution of these bundles might fail.

- ♦ **Export as CSV:** You can export all app information displayed on this page as a CSV file. Click **Export > As CSV** to create a .ZIP folder. This .ZIP folder contains two files; a **Summary** file which will display all the app information that is already displayed on the summary page and a **Details** file with detailed information such as to which users or on which devices the app has been installed.
- ♦ **Search/Filter:** You can filter the data displayed on this page by specifying either the **App Name**, **Publisher**, **VPP Account**, or the **Android enterprise** account in the search field. You can further filter the data to view apps based on the platform or based on the bundles associated with the apps. For this, click  and select the appropriate option.
- ♦ **Show/Hide Columns:** To arrange the columns on the summary page, click  and select the columns that need to be displayed on the summary page. The columns available for display are as follows:
 - ♦ **Publisher:** Displays the name of the app publisher.
 - ♦ **Cost:** Displays the cost of the app. The cost is displayed as free for apps, which do not have a cost associated with it.

- ◆ **Platform:** Displays whether the app is an Android or iOS app.
- ◆ **Subscription Name (applicable for iOS VPP and Android apps only):** Displays the name of the Apple VPP Subscription or the Android Enterprise Subscription using which the app is either purchased or approved.
- ◆ **Purchased (applicable for iOS VPP and Android apps only):** Displays the number of Android or iOS VPP app licenses approved or purchased.
- ◆ **Consumed:** Displays the number of app licenses that are consumed from Apple (Apple VPP or the App Store) or Google Play (Android enterprise). This indicates that the device has synced with the ZENworks Server and the app is sent to the device but might not necessarily mean that the app is installed on the device.
- ◆ **Available (applicable for iOS VPP and Android apps only):** Displays the number of unused licenses that are available for consumption.
- ◆ **User Licenses Installed:** Displays the number of devices on which an app, having a user license, is installed. For example: if a specific app is assigned to a user having three devices associated and if the app is installed on only two devices, then the **User License Installed** count will be 2. You can select the **Export** option and view the **Details** file to identify the devices on which the app is installed.
- ◆ **User Licenses Consumed (applicable for iOS VPP and Android apps only):** Displays the number of user licenses that are consumed from Apple or Google Play. This indicates that the device associated with the user has synced with the ZENworks Server and the app is sent to the device but might not necessarily mean that the app is installed on the device.
- ◆ **Device License Installed:** Displays the number of devices on which an app, having a device license, is installed. If the user rejects the installation of an app on the device, then this count will not be incremented. You can view the devices on which the app is installed by viewing the **Details** file, which is generated if you select the **Export** option.
- ◆ **Device Licenses Installed:** Displays the number of devices on which an app, having a device license, is installed. You can select the **Export** option and view the **Details** file to identify the devices on which the app is installed. This field is not applicable for Android apps, as these apps can be assigned to users only.
- ◆ **Device Licenses Consumed (applicable for iOS VPP and Android apps only):** Displays the number of device licenses that are consumed from Apple. This indicates that the device has synced with the ZENworks Server and the app is sent to the device but might not necessarily mean that the app is installed on the device. This field is not applicable for Android apps, as these apps can be assigned to users only.
- ◆ **Total Apps Installed:** In the case of iOS apps, displays the sum of installed device licenses and user licenses. In the case of Android, displays the user licenses installed.
- ◆ **App Size:** Displays the size of the app. Applicable only for iOS apps.
- ◆ **Package Name:** Displays the iOS app identifier or Android app package name.
- ◆ **Total Bundles:** Displays the number of bundles created for the specific app. You can click the number to view the bundles. To view these bundles you need to have the relevant Bundle Rights assigned to you.
- ◆ **Update View:** Click  to initiate the following:
 - ◆ a sync between the ZENworks Server and the Apple server to update this page with the latest apps and license information for VPP apps.

- ◆ a sync between the ZENworks Server and the Google server to update the license information for Android Apps.


NOTE: The option to sync to Google server is available only if you are using ZENworks 2020 Update 2 - FTF 1008 and above.

- ◆ update the app information, if a new App Store App bundle is created.


This option also revokes unused app licenses in the following scenarios:

- ◆ Mobile device management on the device is disabled.
- ◆ Device enrolled as **Managed Device Only** is unenrolled from the zone. In case of a device assignment, all apps assigned to the device are revoked. In case of a user assignment, if the device is the last device associated with the user, then the app licenses are revoked from the user.
- ◆ User does not exist anymore. This is applicable for Apple VPP apps only. For Android enterprise apps, this check is performed only during the LDAP server refresh.

Unused app licenses are revoked when the device syncs with the ZENworks Server. Also, every two hours ZENworks automatically revokes unused licenses from devices that cannot sync with the ZENworks Server. However, if you do not want to wait for the device to sync or for ZENworks


to automatically revoke licenses, then click  to revoke licenses immediately.

Editing App Permissions

ZENworks lets you edit the default runtime permissions of the approved Android work apps in the Apps Catalog page. Runtime permissions are a set of dangerous permissions as defined by Google. You can edit permissions for apps against which the  icon is displayed. This icon indicates that either the runtime permissions or managed configurations require your attention.

To edit the permissions, in the Apps Catalog page, select the app and click **Action > Edit Permissions**. The **Edit Permissions** dialog lists all the permissions used by the app. You can edit the **Runtime State** against each runtime permission. Any customized permissions created by the app developer that does not have a name associated with it, is displayed as a Custom Permission and its value cannot be edited. You can set the following values for the **Runtime State**:

- ◆ **Denied:** Automatically denies the permission and the user cannot edit the permission on the device.
- ◆ **Granted:** Automatically grants the permission and the user cannot edit the permission on the device.
- ◆ **Default:** Users can manage the permission through the device UI.

If the permissions are not edited in this dialog box, then the permissions as set in the assigned Mobile Device Control Policy will apply. After applying your changes, it will reflect on the device as soon as it syncs with the server. In the future, if the app developer updates the permissions, then these updates will be indicated by the  icon.

24 Refreshing a Device

A device refresh can be initiated in the following ways:

- ◆ **Scheduled Refresh**
- ◆ **Manually Triggered Refresh**
 - ◆ Quick Task Refresh initiated by the Administrator.
 - ◆ ZENworks User Portal or ZENworks Agent App refresh initiated by the end user.
- ◆ [“Initiating a Scheduled Refresh” on page 197](#)
- ◆ [“Manually Triggered Refresh” on page 198](#)

Initiating a Scheduled Refresh

The Device Refresh schedule lets you define how often a device contacts the ZENworks Server to update information such as policies and bundles.

During a scheduled device refresh, data from the ZENworks Server cache is read and delivered to the device. Therefore, if an action is assigned to a device you need to wait until the server cache is updated with the assignment, which is determined by the value specified in **Assignment Optimization Settings**. For more information on **Assignment Optimization Settings**, see [Infrastructure Management Settings](#) in [ZENworks Management Zone Settings Reference](#).

This schedule can be defined at three levels:

Management Zone: The schedule is inherited by all device folders and devices. To configure this setting, navigate to **Configuration > Management Zone Settings > Device Management > Device Refresh and Removal Schedule**.

Device Folder: The schedule is inherited by all devices contained within the folder or its subfolders. Overrides the Management Zone refresh schedule. To configure this setting, navigate to **Devices > <Folder (Details)> > Settings > Device Management > Device Refresh and Removal Schedule**.

Device: The schedule applies only to the device for which it is configured. Overrides the refresh schedules set at the Management Zone and folder levels. To configure this setting, navigate to **Devices > <Select a Device> > Settings > Device Management > Device Refresh and Removal Schedule**

NOTE: If you are configuring this setting at a Device Folder or at Device level, then you need to click **Override** or else the default setting will apply.

Timed Refresh

This option ensures that for multiple devices that have the same refresh schedule, the ZENworks Server does not initiate their refresh at the same time. The default value is 120 minutes and the minimum value that you need to set is 60 minutes. For example, if you have 1000 devices with the same refresh schedule, you might overburden your ZENworks Server. By selecting this option, the server waits a randomly generated amount of time before initiating the refresh on these devices.

To define the refresh schedule, fill in the following fields and click **Apply** to save the settings:

Days, Hours, Minutes: Specifies the maximum amount of time within which the mobile devices should refresh. For example, to set the refresh time as 8.5 hours, you would specify 0 Days, 8 Hours, 30 Minutes.

Manually Triggered Refresh


If you do not want to specify a refresh schedule, then select **Manual Refresh** on the Device Refresh and Removal Schedule page (**Configuration > Device Management > Device Refresh and Removal Schedule**). This option lets users manually initiate a refresh. Manual refresh can be initiated by:

- ♦ Using the Refresh Device quick task.
- ♦ Using the Refresh icon on the ZENworks Agent App or the ZENworks User Portal.

During a device refresh initiated manually, ZENworks bypasses the server cache and it retrieves the latest updates and send these updates to the devices.

Refresh Device Quick Task

You can initiate a device refresh through a ZENworks Control Center quick task. The quick task sends a synchronization request to the device. When the device connects to the ZENworks Primary Server, it uploads updated device information and receives configuration changes (for example, policy changes) that have not already been sent to the device. This quick task is applicable for Android, iOS devices that are enrolled as fully managed devices in the management zone.

- 1 In ZENworks Control Center, click **Devices > Mobile Devices** to display your enrolled mobile devices.
- 2 Select the check box in front of the Android, or iOS device you want to refresh, click **Quick Tasks > Refresh Device** to display the Refresh Device quick task.
- 3 Retain the default values of the quick task options and click **Start** to initiate the device refresh.
- 4 Click **Hide** to close the quick task, after the quick task is initiated.
- 5 Click  in the upper-right corner of the **Devices** list to refresh the list.
The device's Last Contact time is updated to show the refresh time.
- 6 (Optional) Click the device to show its properties, then review the Device Information page for any updated device information. For more information, see [Viewing Device Information](#).

Refresh Device on the User Portal or the ZENworks App

Click the Refresh icon on the ZENworks User Portal for iOS devices or the ZENworks Agent app for Android Devices. When a refresh is initiated from the device, the device connects to the ZENworks server, it uploads updated device information and receives configuration changes (for example, policy changes) that have not already been sent to the device.

25 Collecting Mobile Device Inventory

An inventory scan of your mobile devices provides you with a detailed report of each device’s hardware and software information. The topics addressed in this chapter are:

- ♦ “Mobile Inventory Scan” on page 201
- ♦ “Viewing Mobile Inventory” on page 202

The following table lists software and hardware information that is collected from mobile devices:

Table 25-1 Mobile Inventory details

Data	Inventoried Information
Software	<p>Operating System details, system apps, managed and non-managed app details.</p> <ul style="list-style-type: none">♦ Managed Apps: Information related to apps that are installed through ZENworks. This information is collected by default.♦ Non-managed Apps: Information related to apps that are installed using an app store or any other source besides ZENworks.♦ System Apps: Information related to built-in apps. This information is collected for Android devices only. <p>App details such as app name, app version, publisher name, package name and app size are collected.</p>
Hardware	<p>System information such as device serial number, MAC address, LAN adapter, RAM, memory modules, free space and total disk space details are collected. This information is collected by default.</p>

Mobile Inventory Scan

By default, mobile inventory details are collected once in 24 hours. However, you can configure this schedule in ZCC. The scan settings can be configured at three levels:

- ♦ **Management Zone:** The settings are inherited by all the device folders and devices. To enable inventory scan at the Management Zone level, click **Configuration > Management Zone Settings > Inventory > Mobile Device Inventory**.
- ♦ **Device Folder:** The settings are inherited by all the devices contained within the folder and the subfolders. Override the management zone settings. To configure the device folder level settings, click **Devices > <Device Folder> (Details) > Settings > Inventory > Mobile Device Inventory**. Click **Override Settings** to enable you to configure the setting for the folder.

- ♦ **Device:** The settings apply only to the device for which they are configured. Overrides the Management Zone and Device Folder level settings. To configure the device level settings, click [Devices > <Click a device> Settings > Inventory > Mobile Device Inventory](#). Click [Override Settings](#) to enable you to configure the setting for the device.

To begin collecting these inventory details, navigate to the Mobile Device Inventory page and click [Enable Inventory Scan](#). If this option is disabled, then you also cannot initiate the Inventory Scan quick task.

Select either one of the following scheduling options:

- ♦ **No Schedule:** This indicates that the inventory scan will not be performed unless an Inventory Scan quick task is initiated. For more information, see [Initiating Quick Tasks](#).
- ♦ **Recurring Schedule:** Specify the schedule in days or hours to indicate how often the inventory scan should be run on the device. If **Hours** is selected, then you need to specify any value between 1 and 24. If **Days** is selected, then you need to specify any value between 1 and 30. The inventory information will be populated in ZCC only when the device syncs with the ZENworks server.

Consider a scenario, where the inventory collection and device refresh is scheduled for every 3 and 2 hours, respectively. The first device refresh is performed at 12:00 PM based on which the inventory details are collected. The subsequent refreshes occur at 2:00 PM and 4:00 PM. Since the inventory scan is scheduled for every 3 hours, the inventory information will be collected during the device refresh that occurs at 4:00 PM as 3 hours would have elapsed from the time the first refresh (12:00 PM) had occurred.

In the [Apps Inventory](#) section, select the type of inventory information you want to collect, that is, non-managed apps or system apps. Managed apps and hardware information is collected by default and cannot be disabled.

NOTE: If in the previous releases, you had configured the inventory scan schedule in the properties file, then from the current release onwards, re-configure the inventory collection details using this page as the properties file will no longer be effective.

Viewing Mobile Inventory

Mobile inventory details can be viewed in the Apps page or in the Reports page.

For more information, see [Section 22.10, “Viewing Information of Apps Installed on Devices,” on page 191](#) and [Using Reports](#) in the [ZENworks Asset Inventory Reference](#).

Like servers and workstations, you can view standard or create a custom report.

- ♦ [“Viewing Standard Reports for Mobile Devices” on page 203](#)
- ♦ [“Creating Custom Reports for Mobile Devices” on page 203](#)

IMPORTANT: While creating custom report of type Software applications for mobile devices, ensure that you select Mobile Applications in the Focus section.

Viewing Standard Reports for Mobile Devices

Viewing an inventory report for a mobile device is similar to viewing an inventory report for a Workstation or a Servers. The existing standard reports are modified to display mobile device information along with servers and workstation reports.

The standard report includes mobile device details retrieved from mobile devices in a zone.

To view a standard reports:

1. In ZCC, click **Reports**,
2. In the Inventory Standards Reports panel, click any Group folder, and then click the required report.

For more information, see [Using Inventory Standard Reports](#) in the [ZENworks Asset Inventory Reference](#)

Creating Custom Reports for Mobile Devices

In ZCC, you can create a custom report to collect mobile application data.

To create a custom report of type Software Application as part of the Mobile apps:

- 1 In ZCC, click **Reports**.
- 2 Select or create an Inventory Custom Reports folder.
- 3 In the folder, click **New**.
- 4 In the Custom Report Definition page, perform the following and click **Continue**:
 - ◆ Specify the name for the report
 - ◆ In the **Type** section, select Software Applications.
 - ◆ In the **Focus** section, select Mobile Applications.
- 5 Fill in the following fields:
 - ◆ **Name**: Specify the name of the report.
 - ◆ **Folder**: Select a folder where you want to save the report.
 - ◆ **Description**: Specify a description for your report.
 - ◆ **Type**: This field is display only. It shows the report type you selected.
 - ◆ **Columns**: From the list on the left, select what data you want to include in your report. Use the arrow icons to move the selected data to the list on the right. Use Ctrl+click to select more than one option at a time. Use the up and down icons to arrange how you want the data displayed.

Some of the newly added columns for mobile devices include Application Package Name, Application Platform, Application ID, Application Type, Story Type, Application Size (MB) and Enterprise Application.
 - ◆ **Criteria**: Select your filter criteria in the Field, Operator, and Value fields. Use the + icons to add filters; click the - icon to delete a filter. Click OR or AND to toggle back and forth between the two operators.

- ◆ **Summary Criteria:** Select your summary filter criteria in the Field, Operator, and Value fields. Use the + icons to add filters; click the - icon to delete a filter. Click OR or AND to toggle back and forth between the two operators.

6 Click **Save**.

For more information, see [Using Inventory Custom Reports](#) in the [ZENworks Asset Inventory Reference](#).


26 Initiating Quick Tasks

Quick Tasks are the tasks that you can quickly perform on one or more devices through ZENworks Control Center. This topic discusses the quick tasks that can be performed on mobile devices.

- ♦ “Refresh Device” on page 205
- ♦ “Install Bundle” on page 205
- ♦ “Reboot or Shutdown Devices” on page 206
- ♦ “Lock Device and Unlock Device” on page 206
- ♦ “Unenrolling a Device” on page 207
- ♦ “Send Message” on page 207

Refresh Device

You can initiate a device refresh through a ZENworks Control Center quick task. The quick task sends a synchronization request to the device. When the device connects to the ZENworks Primary Server, it uploads updated device information and receives configuration changes (for example, policy changes) that have not already been sent to the device. This quick task is applicable for Android, and iOS devices that are enrolled as fully managed devices in the management zone.

- 1 In ZENworks Control Center, click **Devices** > **Mobile Devices** to display your enrolled mobile devices.
- 2 Select the check box in front of the Android, or iOS device you want to refresh, click **Quick Tasks** > **Refresh Device** to display the Refresh Device quick task.
- 3 Retain the default values of the quick task options and click **Start** to initiate the device refresh.
- 4 Click **Hide** to close the quick task, after the quick task is initiated.
- 5 Click  in the upper-right corner of the **Devices** list to refresh the list.
The device’s Last Contact time is updated to show the refresh time.
- 6 (Optional) Click the device to show its properties, then review the Device Information page for any updated device information. For more information, see [Viewing Device Information](#).

Install Bundle

The **Install Bundle** quick task lets you immediately install a bundle to one or more devices.

Procedure

- 1 In ZENworks Control Center, click **Devices > Mobile Devices** to display your enrolled mobile devices.
- 2 Select the check box in front of the mobile device, click **Quick Tasks > Install Bundle** to display the Install Bundle dialog box.
- 3 Browse to the folder location in which the bundle you want to install resides. You can also include additional devices by clicking **Add**. Click **Ok** to display the quick task options.
- 4 Retain the default values and click **Start** to send the message.
- 5 Click **Hide** to close the quick task.

Reboot or Shutdown Devices

Using this quick task feature, you can restart and shutdown devices. The reboot action is applicable for both iOS supervised devices (10.3 and newer) and Android devices enrolled in the work-managed device mode. The shutdown action is applicable for iOS supervised devices only. To perform this quick task:

- 1 In ZENworks Control Center, click **Devices > Mobile Devices** to display your enrolled mobile devices.
- 2 Select the device, click **Quick Tasks > Reboot/Shutdown**.
- 3 Select Reboot or Shutdown in the Reboot and Shutdown Settings section. The remaining settings in this dialog box are not applicable for mobile devices.
- 4 Click **Next** to display the quick task options.
- 5 Retain the default options and click **Start** to send the message.
- 6 Click **Hide** to close the quick task, after the quick task is initiated.

Lock Device and Unlock Device

Locking a Device

You can remotely lock a lost or a stolen device from ZENworks Control Center by using the **Lock Device** quick task. If passcode restriction is already enabled on the device, then the user can unlock the device by only entering the set passcode. This quick task is applicable for Android, and iOS devices that are enrolled as fully managed devices in the management zone.

- 1 In ZENworks Control Center, click **Devices > Mobile Devices** to display your enrolled mobile devices.
- 2 Select the check box in front of the device, click **Quick Tasks > Lock Device** to display the Lock Device quick task.
- 3 Specify a reason for locking the device. Additionally, for iOS devices, you can specify a call back phone number that can be called back when the device is found, along with a message. The call back phone number and the message are displayed on the lock screen of a device on which a passcode is enabled.

- 4 Click **Next** to display the quick task options.
- 5 Retain the default values of the quick task options and click **Start**.
- 6 Click **Hide** to close the quick task after the quick task is initiated.

Unlocking a Device

This quick task is applicable for Android, and iOS devices that are enrolled as fully managed devices in the management zone. The Unlock Device quick task removes the passcode restriction on devices. This task can be performed on only a single device at any given point in time. For Android devices, you need to specify the reason for unlocking the device along with the new passcode. The new passcode will be set immediately after the previous passcode is cleared on the device.

On Android 8.0+ devices that already have an existing device passcode set, the Unlock Device Quick Task can be initiated only if the **Reset Password Enabled** status, displayed on the right pane of the Device Information page, is active. This status is activated when the user confirms the existing device passcode credentials after the device is enrolled to the zone. For the user to confirm these credentials, ZENworks automatically sends a notification to the device when it syncs with the ZENworks server immediately after enrollment. For devices that do not have a passcode set, on initiating this quick task, ZENworks will automatically set the new passcode on the device.

For iOS devices, you only need to specify the reason for unlocking the device.

- 1 In ZENworks Control Center, click **Devices > Mobile Devices** to display your enrolled mobile devices.
- 2 Select the check box in front of the device, click **Quick Tasks > Unlock Device** to display the Unlock Device quick task.
- 3 For Android devices, specify the reason for unlocking the device along with the new passcode. The new passcode will be set immediately after the previous passcode is cleared on the device. In the case of an iOS device, you only need to specify the reason for unlocking the device.
- 4 Click **Next** to display the quick task options.
- 5 Retain the default values of the quick task options and click **Start**.
- 6 Click **Hide** to close the quick task after the quick task is initiated.

Unenrolling a Device

While unenrolling a device, you can choose to delete the device from the ZENworks Management Zone or to retire the device (remains in the zone but is inactive). You can also choose to fully wipe the data and reset the device to its factory settings or selectively wipe the data on the device (corporate data and email only). For more information on this task, see [Unenrolling Devices](#).

Send Message

You can send a message from ZENworks Control Center to an Android device that is enrolled as a fully managed device. The message consists of a subject and a body (140 character limit). It shows up as a notification on the device, if notifications are turned on for the ZENworks Agent app.

Procedure

- 1 In ZENworks Control Center, click **Devices > Mobile Devices** to display your enrolled mobile devices.
- 2 Select the check box in front of the Android device you want to refresh, click **Quick Tasks > Send Message** to display the Send Message dialog box.
- 3 Provide a subject and message, then click **Next** to display the quick task options.
- 4 Leave the quick task options set to the defaults and click **Start** to send the message.
- 5 Click **Hide** to close the quick task, after the quick task is initiated.
- 6 On the Android device, open the Notification area to view the message.

27 Bypassing Activation Lock

Activation Lock is a security feature on Apple devices that runs on iOS 7 or later versions. Using this feature you can prevent the reactivation of lost or stolen devices.

Activation Lock is enabled automatically when you turn on the Find My Device feature on a device. To enable Find My Device, log into iCloud account on the device. If you sign out of the iCloud account on your device, Find My Device and Activation Lock will be disabled.

If Find My Device is enabled on a device, iCloud credentials are required to:

- ◆ Erase the device
- ◆ Reactivate the device
- ◆ Turn off the Find My Device feature

If Activation Lock is enabled on a corporate-owned fully managed iOS supervised device, iCloud credentials are required to reset the device and assign it to another user. If iCloud credentials of the user are not available, then administrators can use the Activation Lock Bypass feature to bypass the Activation Lock on the device.

- ◆ [“Enabling Activation Lock Bypass” on page 209](#)
- ◆ [“Disabling Activation Lock Bypass” on page 209](#)
- ◆ [“Retrieving the Activation Lock Bypass Code” on page 210](#)
- ◆ [“Viewing the Activation Lock Bypass Code in ZCC” on page 210](#)
- ◆ [“Activating the Device Using the Activation Lock Bypass Code” on page 211](#)

Enabling Activation Lock Bypass

To enable Activation Lock Bypass:

- 1 In ZENworks Control Center, click **Configuration**.
- 2 In the Management Zone Settings panel, click **Device Management**, and then click **iOS Device Settings**.
- 3 In the iOS Device Settings page, select the **Enable Activation Lock Bypass** checkbox, and then click **Apply**.

NOTE: By default, Activation Lock Bypass will be enabled on all devices in the Management Zone.

Disabling Activation Lock Bypass

To disable Activation Lock Bypass, uncheck the **Enable Activation Lock Bypass** checkbox in the iOS device Settings page.

NOTE: You can reactivate the device using the Activation Lock Bypass code only if the Activation Lock Bypass feature is enabled on the device. Hence, it is recommended that you always enable the setting in ZCC.

Retrieving the Activation Lock Bypass Code

When an iOS supervised device is enrolled to a zone, the Activation Lock Bypass code is automatically retrieved from the device. The retrieved bypass code is encrypted and stored in the ZENworks database.

NOTE

- ◆ After enrolling the device to a ZENworks zone, the activation lock bypass code is automatically deleted from the device.
 - ◆ Whenever a device is reset, a new Activation Lock Bypass code is generated. Hence, it is recommended that you reset the device before enrolling the device to a zone.
-

Viewing the Activation Lock Bypass Code in ZCC

After enrolling a device to a zone, perform the following steps to view the Activation Lock Bypass code:

- 1 In ZENworks Control Center, click **Devices**.
- 2 In the Devices page, click **Mobile Devices**, and then select the device for which you want to view the bypass code.
- 3 In the Device Information page, under the Administration section, click **Show**, adjacent to Activation Lock Bypass Code.

The 16 digit Activation Lock Bypass code for the selected device is displayed.

NOTE: Administrators with *View Activation Lock Bypass Code* rights can view the bypass code.

Exporting the Activation Lock Bypass Code

The Activation Lock Bypass codes in the zone can be exported by running the `zman malbetf` command. The command exports the Activation Lock Bypass codes of all supervised iOS devices in the zone to a ZIP file.

NOTE: Only super admins have rights to execute the command.

For more information, see the [ZENworks Command Line Utilities Reference](#).

Activating the Device Using the Activation Lock Bypass Code

If Activation Lock is enabled on the device, iCloud credentials are required to reset the device. To reactivate the device, you should provide the iCloud credentials that was used to enable the activation lock. If iCloud credentials are not available, then the Activation Lock Bypass code can be used to reactivate the device.

To reactivate the device using the Activation Lock Bypass code:

1. Either unenroll the device from ZCC by selecting **Fully wipe the devices, resetting them to factory setting** or reset the device by using Apple Configurator.

For more information, see [Unenrolling Devices](#).

2. When prompted for Apple ID and password, leave the Apple ID field empty and enter the 16 digit bypass code in the password field without specifying the dashes.

NOTE: You can reactivate the device using the Activation Lock Bypass code only if Activation Lock Bypass is enabled on the device.

28 Locating a Device

Use the Geolocation feature in ZENworks to identify the current geographic location of an enrolled mobile device. It is recommended that this feature be used on a need-only basis and not to continuously monitor the device location. While identifying the device location, only the last known location of the device is retrieved and populated by ZENworks.

- ♦ [“Prerequisites” on page 213](#)
- ♦ [“Procedure” on page 214](#)
- ♦ [“Notifying Users of Device Location” on page 214](#)

Prerequisites

For ZENworks to determine the device location successfully, ensure that the following prerequisites are met:

- ♦ This feature is applicable for iOS supervised devices and Android devices that are enrolled as fully managed devices.
- ♦ For an Android device, turn on the device’s location services. To enable the device’s location services:
 - ♦ Navigate to the Settings app on the device.
 - ♦ Tap Location.
 - ♦ Enable Location.

NOTE: For a device enrolled in the work-profile mode, even if the location is turned on at the device level, the user can turn it off at the work profile level (applicable on Android 7.0 and newer versions). In such cases, ZENworks will not be able to determine the location of the device.

- ♦ For an Android device, ensure that the Location permission for the ZENworks Agent app is turned on.
- ♦ For an Android 8.0 and older device, the location mode selected by the end-user will enable ZENworks to accurately identify the location of the device. When the **Device only** mode is set as the location mode, then the device might not be able to report its current location. The Device only mode works better when the user is outdoors. To ensure that the device is able to report its current location, it is recommended that the end user sets the location mode as **High Accuracy**.
- ♦ For an Android 9.0 device, ensure that location accuracy is on. When this setting is turned on, ZENworks will be able to obtain the most accurate location of the device using resources such as GPS, Wi-Fi, Mobile networks, and Sensors.
- ♦ For an Android device, ensure that the device is not in Doze mode.
- ♦ Associate the Geolocation right to your admin account. To enable this right:
 1. Click **Configuration**.

2. Click **Administrators**.
3. Click **New** appearing under the **Roles** panel.
4. Click **Add** appearing under the **Rights** section.
5. Select **Device Rights**.
6. Retain the default selection **Allow** appearing next to the **Geolocation** right.

Procedure

- 1 In ZENworks Control Center, navigate to the **Devices** tab.
- 2 Click a device that you want to locate.
- 3 Click the **Geolocation** tab.
- 4 Click **Locate Now**.

On clicking **Locate Now**, a quick task is sent to the device and only the last known location of the device is identified and populated in ZENworks. The location details such as the address, the longitude and latitude along with the time stamp are displayed. You can also click **View on map** to view the location on Google Maps.

If the device does not respond within a minute of the quick task initiation, then the operation is timed out. Subsequently, whenever a new location request is sent to the device, the previous location details stored by ZENworks are overwritten with the latest location details.

Notifying Users of Device Location

To ensure that end users are aware that their administrator has obtained the current location of their devices, notifications are sent to the user as email notifications (applicable for iOS, and Android devices) and device notifications (applicable only for Android devices), which are sent after the devices are located successfully. Also, while the device location is in the process of being identified, an additional notification is sent to Android 8.0 or newer devices, informing the users that their administrator is attempting to locate their devices.

You can customize the contents of the email notification by navigating to **Configuration > Management Zone Settings > Event and Messaging > Email Notifications > Device Located**. For more information, see [Managing Email Notifications](#).

29 Enabling Factory Reset Protection on Android Work-Managed Devices

Factory Reset Protection (FRP) is a security feature that prevents unauthorized users from using a device that has been hard factory reset. This feature is applicable in a situation where a malicious user is in possession of a lost or stolen device and has performed a hard reset from the bootloader. If FRP is enabled, then the account credentials of only an authorized user can be specified on the device, without which the device is rendered unusable.

NOTE: This feature is not applicable for Android 6 (Marshmallow) devices.

- ◆ “[Specifying corporate accounts to provision devices](#)” on page 215
- ◆ “[Wiping Factory Reset Protection Data](#)” on page 216

Specifying corporate accounts to provision devices

To enable FRP, you need to create a Mobile Device Control policy and enable the **Allow factory reset protection** setting in the policy. On enabling this setting, you can specify the corporate accounts of users that are authorized to provision devices that have undergone a hard factory reset. While configuring the corporate account, you need to specify the email address and the corresponding ID of the authorized user. To obtain the ID, you need to:

1. Navigate to <https://developers.google.com/people/api/rest/v1/people/get> and login with your Google account credentials.
2. Specify `people/me` in the **resourceName** field appearing in the right pane of the page.
3. Specify `metadata` in the **personFields** field appearing in the right pane of the page.
4. Click **Execute**.
5. Select the Google account for which you want to obtain the ID and accept the permission.

The ID is displayed as an integer string.

For more information on enabling FRP setting in the Mobile Device Control policy, see [Editing a Mobile Device Control Policy Setting](#)

Wiping Factory Reset Protection Data

If a device on which FRP is enabled, needs to be unenrolled from the zone, then to remove the FRP data from the device as well as from the ZENworks database, you need select the **Wipe Factory Reset Protection data** option while initiating the Unenroll quick task. For more information on this quick task, see [Unenrolling Devices](#).

If the device has already unenrolled and is deleted from the zone and if the FRP data is not wiped during unenrollment, then you can execute the `zman mfrpr` command to remove the FRP data for these devices from the ZENworks database. These details will be removed only from the database and not from the device. Therefore, before running this command, it is recommended that you run the `zman mfebf` command to take a backup of the FRP details.



30 Protecting Intune Apps

Mobile Application Management or MAM enables administrators to manage only specific apps on users' devices without having to manage the entire device. Leveraging on these capabilities, ZENworks enables you to secure apps built using the Intune Software Development Kit (for example, Office 365 apps). To secure these apps, ZENworks lets you create an app protection policy that can be enforced on both managed and unmanaged devices. Using the app protection policy, you can enforce restrictions such as disabling the option to copy and paste content from Intune apps and mandating the need of a PIN to access an Intune app.

The topics covered in this chapter are as follows:

- ◆ [Section 30.1, "Prerequisites," on page 217](#)
- ◆ [Section 30.2, "Configuring Microsoft Graph API," on page 218](#)
- ◆ [Section 30.3, "Policy Sync Schedule," on page 220](#)
- ◆ [Section 30.4, "Creating the App Protection Policy," on page 221](#)
- ◆ [Section 30.5, "Editing the App Protection Policy Settings," on page 223](#)
- ◆ [Section 30.6, "Assigning the App Protection Policy," on page 233](#)
- ◆ [Section 30.7, "Disabling or Enabling the App Protection Policy," on page 233](#)
- ◆ [Section 30.8, "Viewing and Wiping Intune Protected Apps," on page 234](#)

For more information on protecting Intune apps using ZENworks, you can also watch the following videos:

 <http://www.youtube.com/watch?v=2q6yjB3S1H4>  http://www.youtube.com/watch?v=9Mm_nq-ka-o

30.1 Prerequisites

Before proceeding with the configuration, ensure that you have the following in place:

Intune

- ◆ The Azure administrator and end users should have a Microsoft Enterprise mobility + Security license.
- ◆ The Azure Administrator should have an Application Administrator role along with Intune Administrator role or a Privileged Role Administrator linked to the Azure Account. For more information, see the [Microsoft Documentation](#).

ZENworks

- ◆ Enable the following admin rights in ZENworks:
 - ◆ **Configure Intune App Management** under Zone Rights.

- ◆ **Modify Settings** under Zone Rights.
- ◆ **Modify** under User Rights.
- ◆ Ensure that the ZENworks server that will be used to configure Microsoft Graph API and manage Intune apps, has outbound connectivity to contact the Azure portal.
- ◆ Ensure that you always allow pop-ups for the ZCC page from which Microsoft Graph API is being configured.
- ◆ Ensure that the local Active Directory user context (to which this configuration will be associated) is synced with Azure Active Directory (AD). You also need to ensure that the following attributes present in the local user source are synced with the Azure AD:
 - ◆ *objectsid*
 - ◆ *userprincipalname*

30.2 Configuring Microsoft Graph API

To enable ZENworks to apply the protection policies, you need to first configure Microsoft Graph API, which acts as a gateway to Microsoft Azure services. Microsoft exposes Azure services through REST endpoints. Using this REST endpoint, ZENworks can send requests to Azure to perform specific operations related to Intune App Management.

To configure Microsoft Graph API in ZENworks, you need to navigate to **Configuration > Management Zone Settings > Intune App Management**. On the **Intune App Management** page, you need to perform the following tasks to configure Microsoft Graph API:

- ◆ **Registering an application:** Register your app to obtain an application ID along with other relevant data required to authenticate to Azure Active Directory. A registered application is unique to a tenant. By registering an app, ZENworks can authenticate to Azure Active Directory to obtain an access token required to manage Intune apps related to your tenant. For more information on tenant, see the [Microsoft Documentation](#).
- ◆ **Generating an access token:** Generate an access token using the details obtained while registering your app. Using this token, ZENworks can make REST calls with Microsoft Graph, which in turn validates the entity (in this case ZENworks) and ensures that ZENworks has the relevant permissions to perform the requested operations.
- ◆ **Associating users:** Associate the user contexts (that contains one or more user groups) within ZENworks that should be a part of this configuration. ZENworks can apply protection policies to only those user groups that are part of the associated user context.

NOTE: When you choose to manage Intune Apps using ZENworks, it is recommended to use only ZENWorks to perform any further management operations. Any edits made to the Intune App Protection policy directly in the Azure portal, will not be synced back to ZENworks. Also, these modifications might be overwritten, when the policy is re-published in ZENworks.

30.2.1 Application Registration

To register your application with the Microsoft App Registration Portal:

1. Navigate to **Configuration > Management Zone Settings > Intune App Management**
2. Click the [Microsoft Application Registration portal link](#) to register your app.

3. Sign in to the registration portal using your Microsoft account.
4. Select **All Services** in the left pane and select **App Registrations**. Alternatively, you can also search for app registrations in the search field.
5. Click **New Registrations**.
6. Specify the application **Name**.
7. Select **Accounts in any organizational directory** as **Supported account types**.
8. Paste the callback URL that you had copied earlier, in the **Redirect URI** field and click **Register**.
9. Copy the **Application (client) ID** displayed on the page that shows the details of the app. This Application ID, which is the unique identifier for your app, is required to generate an access token in ZCC.
10. Click **Authentication** in the left hand pane and select **Access tokens** and **ID tokens** in the **Implicit Grants** section.
11. Click **Certificates and Secrets** in the left hand navigation pane and click **New client secret** to generate the application secret.
12. In the **Add a client secret** dialog box, specify a description and a time period for which the **Client Secret** should be valid. Click **Add**.
13. Copy the generated **Client Secret**.

30.2.2 Access Token

1. In ZCC, navigate to **Configuration > Management Zone Settings > Intune App Management**
2. Click **Generate Token**.
3. Specify the **Application ID** and the **Application Password** that you had copied from the Microsoft Application Registration portal. Click **OK**.

You will be navigated to the Microsoft portal where you need to sign in using the same credentials that were used to register the app. After signing-in, accept the requested permissions. After generating the token, you will be redirected to ZCC and the token details will be populated.

After the token is generated, you can perform the following tasks, whenever required.

- ♦ **Test token:** You need to perform this task if you want to validate the token and ensure that it is active.
- ♦ **Renew Token:** You need to perform this task when any of the Intune app management related operations fail due to token expiry.

NOTE: If the tenant ID in the renewed token is different from the tenant ID used in the existing configuration, then all the associated policies in ZENworks will become ineffective. However, the policy will be retained both in ZENworks and Azure. You can continue to create new policies using the new tenant ID. However, if you want to remove the existing policies in ZENworks and in Azure, then you need to remove the Microsoft Graph API configuration and re-configure it by generating the token with the new tenant ID.

- ♦ **Remove Configuration:** If you remove this configuration, the associated user contexts and all existing app protection policies are removed from ZENworks and Azure.

30.2.3 User Association

You can associate one or more user contexts with this configuration. You need to ensure that these selected user contexts are synced with Azure Active Directory. The Intune app management operations can only be performed on the user groups present in the selected user context:

1. Click **Add**.
2. Select the user context and then click **OK**.

After configuring Microsoft Graph API, click **OK** to save the updated configuration.

30.3 Policy Sync Schedule

Configure the schedule to enable ZENworks to sync the Intune App Protection policy with Azure. When the sync schedule is configured, ZENworks ensures that all policies and assignments are replicated in Azure. If any error occurs during the creation or assignment of policies in Azure, the sync provides an auto correction mechanism that will retry these actions during the next sync.

To configure a sync schedule:

1. In ZENworks Control Center, click **Configuration**.
2. In the Configuration page, click **Intune App Management**, and then click **Policy Sync Schedule**.
3. In the Policy Sync Schedule page, perform the following:
 - a. Click the browse icon and select a Primary Server that should perform the sync operation.
 - b. The Status panel displays the current status of the sync operation with Azure.
Click **Run Full Sync** to perform a full sync with Azure.

NOTE: The **Last sync with Azure** field displays the time stamp of the last sync with Azure.

- c. In the Schedule section, configure a schedule to sync with Azure.
 - i. In the **Schedule Type** field, select one of the following schedules and fill in the fields:
 - ♦ **No Schedule:** Select this option if you do not want the event to run automatically. The sync operation should be performed manually to get the latest changes from Azure.
 - ♦ **Recurring:** Depending on the configured schedule, ZENworks syncs with Azure on the specified days. For more information on the options that can be configured for this schedule, see [Recurring in ZENworks Primary Server and Satellite Reference](#).
 - ii. Click **OK** or **Apply**.

30.4 Creating the App Protection Policy

The Intune App Protection policy lets you apply protection settings on apps that are installed on iOS, devices. After creating this policy, ZENworks establishes a connection with Azure and creates the policy with the same settings in the Azure portal. Subsequently, any changes made to the policy in ZCC will be replicated in Azure.

- ◆ [Section 30.4.1, “Creating iOS Intune App Protection Policy,” on page 221](#)
- ◆ [Section 30.4.2, “Creating Android Intune App Protection Policy,” on page 222](#)

NOTE: With an Intune App Protection policy, you cannot:

- ◆ Create a Sandbox version of the policy
 - ◆ Add the policy within a policy group.
 - ◆ Assign the policy to individual users. This policy can be assigned to only user groups. This is a Microsoft limitation.
-

It is recommended that you use ZCC to create and edit this protection policy. Any edits made to the policy directly in the Azure portal will not be synced back to ZENworks.

30.4.1 Creating iOS Intune App Protection Policy

To create this policy:

- 1 Click **Policies** in the left hand pane in ZCC.
- 2 On the **Select Platform** page, select **Mobile** and click **Next**.
- 3 On the **Select Policy Category** page, select **iOS** and click **Next**.
- 4 On the **Select Policy Type** page, retain the default selection **iOS Intune App Protection Policy** and click **Next**.
- 5 On the **Define Details** page, specify the Policy Name, the folder in which the policy should reside, and short description of the policy.
- 6 On Microsoft Intune Apps page, select the apps on which the restrictions should be applied. You can also click **Add** to include a custom app. A custom app is an in-house app that is not published on the Azure app portal. While adding a custom app, you need to specify the name of the app and its package ID. Click **Next**.
- 7 On the App Protection Settings page, assign a security level. Based on the security level selected, the pre-defined values for each setting is populated. However, these values can be customized to suit your requirement:
 - ◆ **Low:** A few restrictions are enforced on the device. Some of the values pre-configured with this security level are:
 - ◆ The default value for **Recheck the access requirements after offline grace period** is 12 hours.
 - ◆ The default value for **Offline interval before app data is wiped** is 90 days.
 - ◆ The default value for **Restrict web content to display in managed browser** is No.

- ♦ **Moderate:** Some restrictions are enforced on the device. Some of the values pre-configured with this security level are:
 - ♦ The default value for **Recheck the access requirements after offline grace period** is 6 hours.
 - ♦ The default value for **Offline interval before app data is wiped** is 30 days.
 - ♦ The default value for **Restrict web content to display in managed browser** is Yes.
 - ♦ **High:** Most restrictions are enforced on the device. Some of the values pre-configured with this security level are:
 - ♦ The default value for **Recheck the access requirements after offline grace period** is 1 hour.
 - ♦ The default value for **Offline interval before app data is wiped** is 7 days.
 - ♦ The default value for **Allow simple PIN** is No.
 - ♦ The default value to **Disable contact sync** is Yes.
- 8 On the Summary page, review the information. You can also click **Define Additional Properties**, if you want to edit the values of the settings. Click **Finish**.

On clicking Finish, ZENworks calls the Azure REST APIs and creates the same policy in Azure. At times, policy creation might fail in Azure. You can identify the reason for failure by navigating to the summary page of policy in ZCC (click the policy in the **Policies** panel in ZCC) and checking the message logs. For more information on the possible reasons for failure, see [Protecting Intune Apps](#).

30.4.2 Creating Android Intune App Protection Policy

To create this policy:

- 1 Click **Policies** in the left hand pane in ZCC.
- 2 On the **Select Platform** page, select **Mobile** and click **Next**.
- 3 On the **Select Policy Category** page, select **Android** and click **Next**.
- 4 On the **Select Policy Type** page, click **Android Intune App Protection Policy** and click **Next**.
- 5 On the **Define Details** page, specify the Policy Name, the folder in which the policy should reside, and short description of the policy.
- 6 On Microsoft Intune Apps page, select the apps on which the restrictions should be applied. You can also click **Add** to include a custom app. A custom app is an in-house app that is not published on the Azure app portal. While adding a custom app, you need to specify the name of the app and its package ID. Click **Next**.
- 7 On the App Protection Settings page, assign a security level. Based on the security level selected, the pre-defined values for each setting is populated. However, these values can be customized to suit your requirement:
 - ♦ **Low:** A few restrictions are enforced on the device. Some of the values pre-configured with this security level are:
 - ♦ The default value for **Recheck the access requirements after offline grace period** is 12 hours.
 - ♦ The default value for **Offline interval before app data is wiped** is 90 days.
 - ♦ The default value for **Restrict web content to display in managed browser** is No.

- ♦ **Moderate:** Some restrictions are enforced on the device. Some of the values pre-configured with this security level are:
 - ♦ The default value for **Recheck the access requirements after offline grace period** is 6 hours.
 - ♦ The default value for **Offline interval before app data is wiped** is 30 days.
 - ♦ The default value for **Restrict web content to display in managed browser** is Yes.
 - ♦ **High:** Most restrictions are enforced on the device. Some of the values pre-configured with this security level are:
 - ♦ The default value for **Recheck the access requirements after offline grace period** is 1 hour.
 - ♦ The default value for **Offline interval before app data is wiped** is 7 days.
 - ♦ The default value for **Allow simple PIN** is No.
 - ♦ The default value to **Disable contact sync** is Yes.
- 8 On the Summary page, review the information. You can also click **Define Additional Properties**, if you want to edit the values of the settings. Click **Finish**.

On clicking Finish, ZENworks calls the Azure REST APIs and creates the same policy in Azure. At times, policy creation might fail in Azure. You can identify the reason for failure by navigating to the summary page of policy in ZCC (click the policy in the **Policies** panel in ZCC) and checking the message logs. For more information on the possible reasons for failure, see [Protecting Intune Apps](#).

30.5 Editing the App Protection Policy Settings

Based on the security level selected while creating the Intune App Protection Policy, the settings that are predefined by ZENworks can be viewed or edited by performing the steps elaborated in this section. As this policy, does not support creation of a Sandbox version, when you edit any of the settings within this policy, the policy needs to be published as a new version. For more information, see [Publishing the App Protection Policy](#).

30.5.1 Procedure

- 1 In ZENworks Control Center, navigate to the **Policies** section.
- 2 Click the App Protection Policy for which the content needs to be configured.
- 3 Click the **Details** tab and edit the settings.

NOTE: If you had selected **Define Additional Properties** while creating this policy, after clicking the **Finish** button you will be directly navigated to the **Details** tab.

Apps

You can edit the list of apps that you had selected in the policy. You can also click **Add** to include custom apps to this list.

Settings

There are two categories of Intune App Protection Policy settings: **Data Relocation** settings and **App Access** settings.

Data Relocation

Setting Name	Supported Platforms	Description
Prevent iTunes and iCloud backups	iOS,	Prevents the back up of data to iCloud or iTunes.
Prevent Android backups	Android	Restricts backup of the app information.

Setting Name	Supported Platforms	Description
Allow app to transfer data to other apps	iOS, and Android	<p>Enables the app to transfer the corporate data to selected apps.</p> <p>Following are the available options:</p> <ul style="list-style-type: none"> ◆ All Apps: Sends the corporate data to any apps. ◆ Policy Managed apps Sends the data only to the managed apps. ◆ None Restricts sending data to other apps. ◆ (Only iOS) Policy Managed apps with OS sharing: Sends the data to other policy managed apps and sends documents to other MDM managed apps on enrolled devices. This setting is applicable only for iOS and devices. ◆ (Only iOS) Policy Managed apps with Open-In/Share filtering: Sends data to other policy managed apps and filter OS open-in or share dialogs to only display policy managed apps. This setting is applicable only for iOS devices. <p>Select exempted apps: Click Add/Edit to include app that should be exempted from the data transfer.</p> <p>If you need to allow data to be transferred to specific apps that do not support Intune APP, you can add the apps in the exempted list. Exemptions allow applications managed by Intune to transfer data to unmanaged applications based on URL protocol (iOS) or package name (Android). By default, Intune adds vital native applications to this list of exceptions.</p>

Setting Name	Supported Platforms	Description
Allow app to receive data from other apps	iOS, and Android	To specify from which app, data can be received: <ul style="list-style-type: none"> ♦ All apps: Allow data to be received from all apps. ♦ Policy Managed apps: Allow data to be received from other policy-managed apps. ♦ None: Do not allow data to be received from any app.
Allow app to transfer data to other apps	iOS, and Android	To specify to which app, data can be transferred. <ul style="list-style-type: none"> ♦ All apps: Allow data to be transferred to all apps. ♦ Policy Managed apps: Allow data to be transferred to other policy-managed apps. ♦ None: Do not allow data to be transferred to any app.
Prevent "Save As"	iOS, and Android	Disables the Save As option on the app.
Select the storage services to which the corporate data can be saved	iOS, and Android	This field will be enabled if the Prevent "Save As" option is enabled. This field enables you to select the specific storage services to which the app data can be saved, such as Sharepoint, Onedrive or the local storage. Use CTRL + Click to select multiple values in the field.

Setting Name	Supported Platforms	Description
Restrict cut, copy, and paste with other apps:		<p>Restricts the cut, copy, and paste operations for the selected apps:</p> <ul style="list-style-type: none"> ◆ Any apps: Allow cut, copy, and paste actions between this app and any app. ◆ Policy managed apps: Allow cut, copy, and paste actions only between this app and any other policy-managed app. ◆ Policy managed with paste in: Allow cut, copy, and paste actions between this app and any other policy-managed app. Allow data from any app to be pasted into this app. ◆ Blocked: Do not allow cut, copy, and paste actions between this app and any other app.
Restrict web content to display in the Managed Browser	iOS, and Android	Restricts the opening of web links displayed in the app to the Managed Browser app.
Block screen capture and Android Assistant	Android	Disables both screen capture and Android Assistant app scanning capabilities.
Encrypt app data	iOS,	Select if the app data should be encrypted. When a PIN is required, the data is encrypted according to the settings in this policy. If a device PIN is not set and if these encryption settings are enabled, then the user will be prompted to set a PIN.
Encrypt app data	Android	Specify whether the app data should be encrypted.
Disable app encryption when device encryption is enabled	Android	<p>If the device encryption is enabled, then this option automatically disables the app encryption.</p> <p>If Encrypt app data is enabled only then this field can be modified.</p>

Setting Name	Supported Platforms	Description
Disable contact sync	iOS, and Android	Prevents the app from saving data to the native Contacts app on the device.
Disable printing	iOS, and Android	Prevents the app from printing protected data.
Disable third-party Keyboards	iOS,	Disable the usage of third-party keyboards with the app.

App Access

Setting Name	Supported Platforms	Description
Require PIN for access	iOS, and Android	Enforces the creation of a PIN for this app. The user will be prompted to setup a PIN the first time they run the app. The following fields will also be enabled: <ul style="list-style-type: none"> ◆ PIN Type ◆ Number of attempts before PIN reset ◆ Allow simple PIN ◆ PIN length ◆ Allow fingerprint instead of PIN ◆ Allow facial recognition instead of PIN ◆ Disable app PIN when device PIN is managed
PIN Type	iOS, and Android	Enforces the format of the PIN. For example: a numeric PIN or a passcode type PIN.
Number of attempts before PIN reset	iOS, and Android	Defines the number of times the users can attempt to enter the PIN before they must reset it. Only a positive whole number can be specified.
Allow simple PIN	iOS, and Android	Enables users to specify a simple PIN sequence such as 1111 and 1234. NOTE: If a Passcode type PIN is configured, and Allow simple PIN is set to Yes at least 1 letter or 1 special character must be specified. If Passcode type PIN is configured, and Allow simple PIN is set to No , at least 1 number, 1 letter and 1 special character must be specified.
PIN length	iOS, and Android	Defines the required number of digits in the PIN. Only a positive whole number can be specified.

Setting Name	Supported Platforms	Description
Allow fingerprint instead of PIN	iOS, and Android	Enables the user to use fingerprint identification instead of a PIN to access the app. This is applicable only on iOS 8.0 and newer versions.
Allow facial recognition instead of PIN	iOS,	Enables the user to use facial recognition instead of a PIN to access the app. This is applicable only on iOS 11.0 and newer versions.
Disable app PIN when device PIN is managed	iOS, and Android	Disables the app PIN when a device lock is detected on an enrolled device.
Require corporate credentials for access	iOS, and Android	Enforces the users to use their corporate credentials instead of entering a PIN for app access.
Block managed apps from running on jailbroken or rooted devices	iOS, and Android	Prevents this app from running on jailbroken or rooted devices.
Offline interval before app data is wiped (days)	iOS, and Android	Defines the number of days after which the app that is running offline will require the user to connect to the network to re-authenticate. When the user successfully authenticates, the user will be able to continue to access data and the offline interval will reset. If the user fails to authenticate, the app will perform a selective wipe of the users account and data.
Recheck the access requirements after timeout (minutes)	iOS, and Android	Defines the time (in minutes) after which the access requirements are rechecked.
Recheck the access requirements after offline grace period (minutes)	iOS, and Android	Allows the app to run offline for the specified time, after which the access requirements are rechecked.
Require minimum iOS operating system	iOS,	Enforces the requirement for a minimum iOS operating system to use the app. The user's access to the app will be blocked if the minimum OS requirement is not met. The value should be specified in the iOS operating system field.

Setting Name	Supported Platforms	Description
Require minimum iOS operating system (Warning only)	iOS,	Sends a notification to the user if the specified minimum iOS operating system requirements needed to use the app are not met. The notification can be dismissed. The value should be specified in the iOS operating system field.
Require minimum app version	iOS,	Enforces the requirement for a minimum app version to use the app. The user's access to the app will be blocked if the minimum app version requirement is not met. The value should be specified in the App version field.
Require minimum app version (Warning only)	iOS,	Sends a notification to the user if the specified minimum app version requirement is not met. The notification can be dismissed. The value should be specified in the app version field.
Require minimum Intune app protection policy SDK version	iOS,	Enforces the requirement for a minimum Intune app protection policy SDK version to access the app. The user is blocked from access if the SDK version does not meet the requirement.
Require minimum Android version	Android	Restricts app access to the specified minimum Android version. The value should be specified in the Android version field.
Require minimum Android version (Warning only)	Android	Sends a notification to the user if the specified minimum Android version needed to use the app are not met. The notification can be dismissed. The value should be specified in the Android version field.

Setting Name	Supported Platforms	Description
Require minimum app version	Android	Enforces the requirement for a minimum app version to use the app. The user's access to the app will be blocked if the minimum app version requirement is not met. The value should be specified in the App version field.
Require minimum app version (Warning only)	Android	Sends a notification to the user if the specified minimum app version requirement is not met. The notification can be dismissed. The value should be specified in the app version field.
Require minimum Android patch version	Android	Enforces the requirement for a minimum Android security patch level to securely access the app. The value should be specified in the Patch version field.
Require minimum Android patch version (Warning only)	Android	Sends a notification to the user if the specified minimum patch version requirement is not met. The notification can be dismissed. The value should be specified in the Patch version field.

- 4 Click **Publish** to display the Publish Option page. In this page you can publish the modified policy as a new version of the same policy or as a new policy.

30.5.2 Publishing the App Protection Policy

Unlike other policies in ZCC, you cannot create a Sandbox version of the Intune App Protection policy. When you edit the settings of the latest version of the policy, you can only publish the policy as a new version. To edit the older version of a policy:

1. Click **Policies** in the left hand pane in ZCC.
2. Click an Intune App Protection Policy.
3. From the **Displayed Version** drop-down menu select a version of the policy that you want to edit.
4. Click **Publish** and publish the policy to its latest version.
5. Edit the settings of the policy and click **Publish** to apply the latest changes.

Consider a scenario, where version 0 is selected of the two published versions (version 0 and version 1) of the policy. After selecting version 0, click **Publish** to publish the policy to its latest version, that is Version 2. You can now edit the settings of the policy and publish the policy again as Version 3.

30.6 Assigning the App Protection Policy

As mandated by Microsoft, the Intune App Protection policy can be assigned to only user groups. This policy cannot be assigned to individual users or to devices. You also need to ensure that the selected user group is part of the same user context associated while configuring Microsoft Graph API. For more information, see [User Association](#). When the policy is assigned, ZENworks calls the Azure REST APIs and the same policy assignment is replicated in Azure, after which the protection settings are enforced on the users' devices. The user group in Azure is identified based on the *OnPremisesSecurityIdentifier* value, which is matched with the *objectsid* attribute value of the user group selected in ZENworks.

After assigning the policy, it is recommended that you review the policy message logs to identify any errors that might have occurred while replicating the policy assignment in Azure. To view the policy logs, navigate to the summary page of the policy (click the policy in the **Policies** panel) and view the message logs to identify the reason for failure, if any. For more information on the possible reasons for failure, see [Protecting Intune Apps](#).

30.6.1 Procedure

- 1 To assign the policy to the user group, from the **Policies** list, select the check box in front of the policy, then click **Action > Assign to User**.
- 2 In the Select Object dialog box, browse for and select the user group to whom you want to assign the policy, click **OK** to add them to the list and then click **Next**.
- 3 Review the summary page and click **Finish** to complete the assignment.

30.7 Disabling or Enabling the App Protection Policy

By default the Intune App Protection policy is enabled during creation. When the policy that is enforced on users' devices is disabled, the user assignment is retained in the ZENworks Database but removed in the Azure portal. Subsequently, the policy is removed from the devices. Also, you will not be able to enforce a disabled policy to a user's device.

To disable a policy:

1. Click the **Policies** tab.
2. Select the checkbox next to the policy that you want to enable.
3. Click **Action > Disable Policies**.

When a disabled policy is enabled, the user assignment of the policy in ZENworks is restored. To enable the disabled policy:

1. Click the **Policies** tab.
2. Select the checkbox next to the policy that you want to enable.
3. Click **Action > Enable Policies**.

30.8 Viewing and Wiping Intune Protected Apps

In the Intune App Protection panel, you can view the devices belonging to a specific user who has logged into the Intune apps installed on the device. The panel displays the user's devices if the user is logged into at least one Intune app regardless of whether an app protection policy is applied to the app or not. You can also remove app data from the logged-in apps by initiating a wipe. The information displayed in this panel is directly obtained from Azure.

To view the Intune App Protection panel:

1. In ZENworks Control Center, click the **Users** section in the left hand panel.
2. Navigate to the user whose Intune apps you want to view or wipe and click the user to open the **Details** page.
3. Click the link to view the list of devices that belong to the user, in the **Intune App Protection** panel. The user should be directly associated with the user context linked with the Microsoft Graph API configuration. If the user of another user context is only referenced from the associated user context, then the Intune App Protection information will not be populated for the user.

The information displayed in this panel is obtained from Azure. ZENworks uses the *userprincipalname* object attribute to map the user in the local user source with that in Azure AD.

To wipe the protected app data, select a device and click **Action > Wipe App Data**. On clicking **Wipe App Data**, and on confirming the Wipe action, ZENworks initiates a request with Azure to wipe the app data. Hence, the time taken to wipe the data from the app is dependent on when the app syncs with Azure. On performing wipe, corporate data is removed from all the logged-in apps on that particular device and the user is logged off from the apps.

The **Intune App Protection** panel displays the following information:

- ♦ **Device Name:** The name of the device that belongs to the user.
- ♦ **Platform:** The device platform, that is, iOS, or Android.
- ♦ **Operating System Version:** The version of the operating system on the device.
- ♦ **Logged-in Apps:** Displays the number of apps that the user is logged into. The count includes both protected as well as unprotected apps. Protected apps are those on which an app protection policy is applied. Whereas, unprotected apps are those on which an app protection policy is not applied.

You can also view the status of the wipe action and other information for each logged-in app, by clicking the link appearing against each device in the **Logged-in apps** column. On clicking the link, the following information is displayed:

- ♦ **App Name:** Name of the app.
- ♦ **Intended Policies:** Names of the app protection policies assigned to the app. These include policies that are already enforced and are yet to be enforced on the app.
- ♦ **Applied Policies:** Names of the app protection policies enforced on the app when it last synced with Azure.

NOTE: Policies that are created directly in Azure and those configured using ZENworks are displayed in the intended or applied policies section. Policies that are configured in ZENworks are displayed with a link that will redirect you to the policy's summary page in ZENworks.

- ◆ **Status:** The status of the app are displayed, which are out of sync, synced, not synced, wipe pending and unprotected. The **Unprotected** status indicates that the app is not included in the assigned app protection policy.
- ◆ **Last Sync:** The date and time that the logged-in app last synced with Azure.

31 Managing Email Notifications

Email notifications are pre-configured mails that ZENworks sends to notify users about specific activities. Currently, the following email notifications are sent to the user:

- ♦ **Device pending enrollment:** Notification is sent when the device is registered to the ZENworks Management Zone but the enrollment process is not complete. The user needs to complete the enrollment process by logging in to the ZENworks end-user portal. When this notification is sent to the device, the term <HOSTNAME> in the default message, will be replaced with the server address to which the device is registered.
- ♦ **Email account not provisioned:** Notification is sent when the user is unable to send or receive organizational emails on the device due to one of the following reasons:
 - ♦ Mobile Email Policy is not yet assigned to a device that has enrolled to the ZENworks Management Zone.
 - ♦ Mobile Email Policy is unassigned from a device that is enrolled to the ZENworks Management Zone.

To edit the content within each of these notifications, navigate to **Configuration > Management Zone Settings > Event and Messaging > Email Notifications**.

ZENworks lets you send these email notifications in multiple languages. You need to specify the language in which the email notification is to be sent, in the Mobile Enrollment Policy. For more information, see [Editing Mobile Enrollment Policy](#).

To edit the email messages in these languages, click any of these notifications, select the language from the drop-down menu, and edit the contents of the email in that language. The **Custom** option will display the notification content that was created in the previous releases. Also, if a particular language is not listed in the drop-down menu, then you can select **Custom** and edit the email message.

32 Unenrolling Devices

You can initiate the Unenroll quick task to unenroll devices from ZENworks that you no longer want to manage. You can delete the device from the zone or retire it (remains in the zone but is inactive). You can also choose to fully wipe the device by resetting it to factory settings, or to selectively wipe the device by removing only corporate data and email.

Based on the enrollment modes, the following actions are performed if selective wipe or full wipe is selected:

Enrollment Mode	Selective Wipe	Full Wipe
Android App	Removes the ZENworks Agent app	Resets Device
Android App (in work profile mode)	Removes the app and the work profile	No action performed
Android App + ActiveSync (in work profile mode)	Removes the app, ActiveSync account and the work profile	No action performed
ActiveSync	No action performed	Resets Device
Android App (in work-managed device mode)	No action performed	Resets Device
Android App + ActiveSync (in work-managed device mode)	No action performed	Resets Device
iOS MDM Profile	Removes the MDM Profile	Resets Device
iOS MDM Profile + ActiveSync	Removes the MDM Profile and the ActiveSync account	Resets Device

NOTE: The ActiveSync account will be deleted only if it is remotely configured by ZENworks. If the ActiveSync account is manually configured on the device, then only the MDM profile is removed. In this case, the device remains active and the enrollment mode will change to ActiveSync.


Procedure

- 1 In ZENworks Control Center, click **Devices > Mobile Devices** to display your enrolled mobile devices.
- 2 Select the check box in front of the mobile device, click **Quick Tasks > Unenroll Device** to display the Unenroll dialog box.

- 3 Select the data removal option for the device, that is, **Selectively Wipe the devices, by removing only corporate data and email** or **Fully wipe the devices, resetting them to factory setting**. Select **Delete the devices from the zone** or select **Retire the devices (devices remain in the zone)**. Enter a reason for unenrolling the device, then click **Next** to display the quick task options.
- 4 (Conditional) If the Full Wipe option is selected, then select **Wipe Factory Reset Protection data** to wipe the FRP details from the device as well as the ZENworks database. These FRP details are the corporate accounts that can provision the device after a hard factory reset.
- 5 Leave the quick task options set to the defaults and click **Start** to send the task to the device.
- 6 Click **Hide** to close the quick task after the quick task is initiated.

The quick task will not complete if the ZENworks Primary Server is unable to contact the device. In this case, you can close the quick task, refresh the **Devices** list, select the mobile device, and click **Delete** to remove the device from the management zone.

NOTE: If the device is offline and the **Delete** option is selected, then the status of the device changes to **Wipe Pending**. Subsequently, the device will be deleted when it is online. However, if **Retire** is selected, then the device status changes to **Retired** irrespective of whether the device is online or offline.

- 7 Click  in the upper-right corner of the **Devices** list to refresh the list.

If the **Delete the devices from the zone** option was selected, then the device is no longer listed. However, if the **Retire the devices** option was selected, then the device will be listed with the status as retired.

NOTE: During unenrollment, if VPP apps are installed on the device, then these apps are automatically uninstalled from the device. However, for App Store Apps (distributed using App Store App bundles) the apps are uninstalled based on the configured app settings (**Retain App on Unenrollment**).

If a device is in **Retired** or **Wipe Pending** state and if an iOS bundle created through an Apple VPP subscription is assigned to the device, then the app will be uninstalled and the license will be revoked. However, if the VPP related iOS bundle is assigned to the user, then the app will be uninstalled and the license revoked, if the device is the only device associated with the user.

If you unretire a device in ZCC using the **Unretire Device** action, then the device will not automatically sync with the ZENworks server and reconcile with the unretired device object in ZCC. You need to re-enroll the device again using one of the enrollment methods, after which the device reconcile with the unretired device object. For more information on these enrollment methods, see [Enrolling Mobile Devices](#).

If a device is in **Retired** or **Wipe Pending** state, then to remove this device from the ZENworks system, select the device and click **Delete**.

33

Unenrolling the Organization from Android Enterprise

The organization can unenroll from Android Enterprise Management by deleting the Android Enterprise Subscription from ZCC.

You can also remotely remove the work profile from devices or factory reset a work-managed device by initiating the Unenroll quick task. For more information on this quick task, see [Unenrolling Devices](#).

Unenrolling the Organization

To unenroll from Android enterprise management, you should delete the Android Enterprise Subscription from ZENworks Control Center.

Before deleting the Android Enterprise Subscription, administrators should be aware of the following:

- ◆ NCC credentials are required to delete the subscription.
- ◆ By deleting the Android Enterprise Subscription, your enterprise will be unenrolled from managed Google Play. However, data associated with this subscription will be deleted only after 30 days. Within the next 30 days, if you create a new Android Enterprise Subscription using the same email ID, ZENworks might be able to recognize the enterprise details and restore the subscription data.
- ◆ The user context associated with the deleted subscription, cannot be associated with the new subscription. You can select an alternate user context. If you still want to use the same user context then either wait for 30 days or run the `zman subscription-clear-ae` command.
- ◆ You can also delete the organization from managed Google Play. The subscription and its data will be deleted from ZENworks only after 24 hours. To delete the organization from managed Google Play:
 1. Navigate to [Managed Google Play](#) and log in using the credentials that you had used to create the Android Enterprise Subscription.
 2. On the left hand panel, click **Admin Settings**.
 3. In the Organization Information panel, click the hamburger menu and click **Delete Organization**.
 4. Confirm your action in the Delete Organization pop-up.

To delete the Android Enterprise Subscription:

- 1 In ZCC, click **Subscribe and Share**.
- 2 In the Subscription panel, select the subscription, and click **Delete**.
- 3 In the **Delete Subscription** pop-up, specify the NCC credentials, and then click **OK**.

NOTE: To delete the data associated with unenrolled subscription, run the `zman sca` command. All data including bundles, apps, users and other data associated with unenrolled subscription will be deleted from ZENworks.

A Best Practices

In this section you will learn the best practices for managing mobile devices using ZENworks Configuration Management.

- ♦ [“Migrating to Apple Business Manager” on page 243](#)

Migrating to Apple Business Manager

Best Practices

This section is applicable for VPP purchasers who have already upgraded or are planning to upgrade to Apple Business Manager from the Apple Deployment Programs account. This section details the best practices to migrate to a location-based token in ZENworks.

If you want to migrate an existing VPP subscription (that uses a legacy token) to a location-based token (provided by Apple Business Manager) and associate all the existing bundle assignments to this new location-based token, then as a best practice it is recommended that you renew the subscription to the location-based token. This ensures that all existing bundle assignments work seamlessly with the new location-based token. However, you can renew the subscription only if the VPP account (associated with the subscription) is mapped to a unique location. As recommended by Apple, it is advisable to migrate one VPP purchaser to one location in Apple Business Manager, which makes a location unique. This ensures that all the licenses (assigned or unassigned) are automatically migrated to the Apps and Books section of Apple Business Manager.

For example: if you have an existing subscription XYZ in your ZENworks zone, then in Apple Business Manager, you can migrate the account of this subscription to location XYZ.

If in ZENworks, instead of renewing the subscription, you create a new subscription using the location-based token while retaining the existing subscription, then it might lead to duplication and VPP licenses might be reset.

Procedure to migrate to location-based token in ZENworks

Before migrating to a location-based token in ZENworks, ensure that you have migrated the existing VPP account to the unique location. For more information, see the [Apple Support](#) documentation.

1. Login to [Apple Business Manager](#) using your VPP account credentials.
2. Navigate to Settings > Apps and Books.
3. Download the token of a specific unique location (example: location XYZ).
4. Navigate back to ZCC.
5. Click the existing subscription (example: subscription XYZ).
6. Click **Renew Token** and select the location-based token that you had just downloaded.

IMPORTANT: After migrating all the VPP accounts to Apple Business Manager, ensure that you use only location-based tokens to manage VPP licenses in ZENworks and not a combination of both account-based and location-based tokens. If both account-based and location-based tokens are used to create subscriptions in the zone, then you might face license-related issues, such as resetting of assigned licenses and it can also result in duplicate subscriptions in the zone that might lead to confusion.

Troubleshooting Scenarios

When assigned licenses do not transfer:

If the location in Apple Business Manager is not a unique location, then only the unassigned licenses are transferred to this location. A location is considered as non-unique if:

- ◆ A location already has licenses in it before the VPP purchaser migrates to that location.
- ◆ The location's token is downloaded before the first VPP purchaser migrates to that location.
- ◆ A new content manager is created in the location after another user opts into Apps and Books.
- ◆ Multiple VPP purchasers migrate to the same location.

For example: in Apple Business Manager, you have migrated subscription XYZ to a location that is non-unique, then only the unassigned licenses (available licenses) will migrate to the new location-based account. The assigned licenses (consumed) will still be associated with the legacy account. In this case, in ZENworks, all bundle assignments related to the existing subscription (that uses the legacy account) should be unassigned and transferred to the non-unique location. Thereafter, you need to create a new subscription in ZENworks to distribute the transferred licenses.

Procedure to migrate to location-based token in ZENworks if the location is non-unique

1. In ZENworks, unassign all the bundles assignments associated with the subscription to which the legacy token is associated. Thereafter, refresh all devices and verify that all licenses are revoked and the **Consumed License** count for all apps is 0.

or

Delete the associated subscription and ensure that you select the **Delete the replicated objects created by the subscription(s)** checkbox. Re-create the subscription in ZENworks using the same legacy token, which will reset all licenses.

2. Delete the subscription (existing or the new subscription created by linking the same legacy token) and ensure that you select the **Delete the replicated objects created by the subscription(s)** checkbox.
3. In Apple Business Manager, navigate to Settings > Apps and Books. Transfer the unassigned licenses to the specific location.
4. Download the token for that specific location.
5. In ZENworks, create a new Apple VPP subscription and upload the newly downloaded location-based token.

When the new subscription is created, ZENworks syncs with Apple and all licenses transferred to this location will be identified and populated as available licenses in ZENworks. You can now create bundles and assign these licenses to specific devices or users.

When there are multiple subscriptions in the zone:

If there are multiple subscriptions in the zone, then based on the scenario, you can refer to the relevant procedure to migrate to location-based tokens:

- ◆ Each associated subscription account is migrated to non-unique locations, then for each account follow the steps documented in [Procedure to migrate to location-based token in ZENworks if the location is non-unique](#).
- ◆ All associated subscription accounts are migrated to a single non-unique location, then for each account follow the steps documented in [Procedure to migrate to location-based token in ZENworks if the location is non-unique](#). However, instead of creating multiple subscriptions for each account, create only one subscription and map the location token with this subscription.
- ◆ If the first account is migrated to a unique location and all other accounts are migrated to non-unique locations, then for the first account follow the steps documented in [Procedure to migrate to location-based token in ZENworks](#) and for the remaining accounts follow the steps documented in [Procedure to migrate to location-based token in ZENworks if the location is non-unique](#).
- ◆ If the first account is migrated to a unique location and subsequently the second account is migrated to the same location, then for the first account follow the steps documented [Procedure to migrate to location-based token in ZENworks](#) and for the second account follow the steps documented in [Procedure to migrate to location-based token in ZENworks if the location is non-unique](#). However, you do not need to create a new subscription with the second account. The renewed subscription can be utilized to distribute licenses.

The 'Account Deactivated' notification is displayed

The 'Account Deactivated' notification is displayed when your work account is disabled. To resolve this issue, you need to manually remove the work account from the Account Settings page of your Android device and then re-enroll the device.

