

ZENworks 2017

Mobile Management Reference

December 2016

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.novell.com/company/legal/>).

Copyright © 2016 Micro Focus Software Inc. All Rights Reserved.

Contents

About This Guide	7
1 Supported Devices for Mobile Management	9
2 ZENworks Mobile Management Workflow Tasklist	11
3 Overview	13
3.1 Using the Mobile Management Getting Started Page	13
3.2 Prerequisites	14
4 Configuring User Sources	15
4.1 Adding an LDAP Directory as a User Source	15
4.1.1 Prerequisites	15
4.1.2 Procedure	15
4.2 Enabling a User Source for Mobile Device Enrollment	16
4.2.1 Procedure	16
5 Configuring MDM Servers	19
5.1 Adding an MDM Server	19
5.1.1 Procedure	20
5.2 Testing the Outbound Capability of MDM Servers	20
5.3 Securing MDM Servers	20
5.4 MDM Servers and APNs Configuration	21
5.5 Removing MDM Servers	21
5.6 Configuring a Default DNS Name	22
6 Enabling Push Notifications	23
6.1 Enabling Push Notifications for Android Devices	23
6.1.1 Prerequisites	23
6.1.2 Procedure	23
6.2 Enabling Push Notifications for iOS Devices	26
6.2.1 Prerequisites	27
6.2.2 Creating and Importing an APNs Certificate	27
6.2.3 Renewing an Expired APNs Certificate	28
7 Securing a Device	29
7.1 Creating a Mobile Device Control Policy	29
7.1.1 Procedure	29
7.2 Editing Mobile Device Control Policy Settings	30
7.2.1 Procedure	30
7.3 Assigning a Mobile Device Control Policy	34
7.3.1 Procedure	35
7.4 Creating a Mobile Security Policy	35
7.4.1 Procedure	35

7.5	Editing Mobile Security Policy Settings	36
7.5.1	Procedure	36
7.6	Assigning a Mobile Security Policy	40
7.6.1	Procedure	40
8	Provisioning Apps	43
8.1	Creating an iOS Bundle	43
8.1.1	Prerequisites	43
8.1.2	Procedure	43
8.2	Assigning an iOS Bundle	45
8.2.1	Procedure	45
8.3	Installing a Bundle using Quick Task	46
8.3.1	Procedure	47
8.4	Viewing Bundle Information	47
8.4.1	Understanding the Bundle Information	47
8.4.2	Bundle Summary Page	47
8.4.3	Bundles Relationship Page	50
8.4.4	Bundles Details Page	51
9	Subscribing to Apple VPP	53
9.1	Linking ZENworks to the Apple VPP Account	53
9.1.1	Prerequisites	53
9.1.2	Procedure	53
9.2	Creating VPP Bundles	55
9.3	Distributing VPP Bundles	56
9.4	Viewing Volume Purchase Program License Summary	57
9.5	Updating License Summary	59
9.6	Renewing the VPP Token	60
9.7	Revoking App Licenses	60
9.8	Viewing or Editing Apple VPP Subscription	60
9.8.1	Procedure	61
9.9	Deleting a Subscription	62
10	Configuring Email Access	63
10.1	Connecting to a New ActiveSync Server	63
10.1.1	Prerequisites	63
10.1.2	Procedure	63
10.2	Linking a User Source to an ActiveSync Server	64
10.2.1	Procedure	65
10.3	Creating a Mobile Email Policy	65
10.3.1	Procedure	65
10.4	Assigning a Mobile Email Policy	66
10.4.1	Procedure	67
11	Enrolling a Device	69
11.1	Types of Enrollment	69
11.2	Modes of Enrollment	70
11.3	Creating a Mobile Enrollment Policy	71
11.3.1	Procedure	72
11.4	Assigning a Mobile Enrollment Policy	73
11.4.1	Procedure	73
11.5	Prerequisites to Enroll a Device to the ZENworks Management Zone	73

11.6	Enrolling an Android Device	74
11.6.1	Procedure	74
11.7	Enrolling an iOS Device	82
11.7.1	Procedure	82
11.8	Enrolling an Email Only Device	87
11.8.1	Procedure	87
11.9	Allowing Manual Reconciliation by User	91

12 Managing a Device **95**

12.1	Status Messages	95
12.2	Viewing Device Information	96
12.3	Organizing Devices into Dynamic Mobile Device Groups	97
12.4	Creating a Device Refresh and Removal Schedule	97
12.4.1	Configuring Mobile Device Refresh Schedule	98
12.4.2	Configuring Mobile Device Removal Schedule	98
12.5	Refreshing a Device	98
12.5.1	Procedure	99
12.6	Locking a Device	99
12.6.1	Procedure	99
12.7	Unlocking a Device	99
12.7.1	Procedure	100
12.8	Sending a Message to a Device	100
12.8.1	Procedure	100
12.9	Unenrolling a Device	100
12.9.1	Procedure	101

A Troubleshooting **103**

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:

- ◆ Chapter 1, “Supported Devices for Mobile Management,” on page 9
- ◆ Chapter 2, “ZENworks Mobile Management Workflow Tasklist,” on page 11
- ◆ Chapter 3, “Overview,” on page 13
- ◆ Chapter 4, “Configuring User Sources,” on page 15
- ◆ Chapter 5, “Configuring MDM Servers,” on page 19
- ◆ Chapter 6, “Enabling Push Notifications,” on page 23
- ◆ Chapter 7, “Securing a Device,” on page 29
- ◆ Chapter 8, “Provisioning Apps,” on page 43
- ◆ Chapter 9, “Subscribing to Apple VPP,” on page 53
- ◆ Chapter 10, “Configuring Email Access,” on page 63
- ◆ Chapter 11, “Enrolling a Device,” on page 69
- ◆ Chapter 12, “Managing a Device,” on page 95
- ◆ Appendix A, “Troubleshooting,” on page 103

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 2017 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.

1 Supported Devices for Mobile Management

Mobile Management capabilities are supported on the following devices:

Device	Functionality
Android, versions 4.1 and newer	<p>Security policy enforcement, device inventory, email synchronization for Exchange ActiveSync accounts and device management (such as refresh, send message and unenroll).</p> <p>Users enroll their Android devices by installing the ZENworks Agent App on their devices.</p>
iOS, versions 8 and newer	<p>Security and device control policy enforcement, email policy enforcement, device inventory, email synchronization for Exchange ActiveSync accounts, app installation using Bundles, install configuration profiles, subscribing to Apple VPP and device management (such as refresh, unenroll and locking the device).</p> <p>Users enroll their iOS devices by installing an MDM (Mobile Device Management) profile on iOS devices.</p>
Devices using ActiveSync 12.1 and newer	<p>Enrollment, email synchronization for Exchange ActiveSync accounts, and security and device control policy enforcement via ActiveSync 12.1. ActiveSync enrollment is supported on the following devices:</p> <ul style="list-style-type: none">◆ Android version 4.1 and newer◆ iOS version 8 and newer◆ Windows version 8 and newer◆ Blackberry 10.0 and newer

2 ZENworks Mobile Management Workflow 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 13.
<input type="checkbox"/> Configure a user source in the ZENworks Management Zone.	For instructions, see “Configuring User Sources” on page 15.
<input type="checkbox"/> Configure an MDM Server to enable communication with mobile devices.	For instructions, see “Configuring MDM Servers” on page 19.
<input type="checkbox"/> Enable push notifications on Android and iOS devices.	For instructions see “Enabling Push Notifications” on page 23.
<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 29.
<input type="checkbox"/> Provision and manage apps or configuration profiles on iOS devices.	For instructions, see “Provisioning Apps” on page 43.
<input type="checkbox"/> Subscribe to the Apple Volume Purchase Program.	For instructions, see “Subscribing to Apple VPP” on page 53.
<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 Email Access” on page 63.
<input type="checkbox"/> Create and assign an enrollment policy and enroll a mobile device in the ZENworks Management Zone.	For instructions, see “Enrolling a Device” on page 69.
<input type="checkbox"/> Manage and maintain mobile devices in the ZENworks Management Zone.	For instructions, see “Managing a Device” on page 95.

3 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 Control Center, 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 and 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, Windows, and Blackberry devices.
- ♦ **Enforce security and mobile control policies** on Android, iOS and devices with Exchange ActiveSync (EAS) capabilities (that include Windows and Blackberry 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.
- ♦ **Synchronize email** from ActiveSync servers on Android, iOS and devices with Exchange ActiveSync (EAS) capabilities (that include Windows and Blackberry devices). You can also remotely configure the default email client on iOS devices.
- ♦ **Install Apps** on iOS devices. You can distribute free App Store Apps to iOS devices using the bundles workflow in ZENworks.
- ♦ **Distribute and manage Apple VPP apps** purchased with your organization's Volume Purchase Program (VPP) account, by using the existing Bundles and Subscription workflow in ZENworks.
- ♦ **Distribute Configuration Profiles** to iOS devices to manage certain features on the device such as access to VPN and Wi-Fi.

3.1 Using the Mobile Management Getting Started Page

ZENworks Control Center includes a [Getting Started with Mobile Management](#) page that guides you through the tasks that you need to complete in order to enroll and manage mobile devices in your zone.


To access the [Getting Started with Mobile Management](#) page:

- 1 In ZENworks Control Center, click **Mobile Management** (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.

You can refer to the following sections within this guide to understand the procedure to complete each configuration task:

- ◆ **User Sources:** [“Configuring User Sources” on page 15](#)
- ◆ **Enrollment Policy:** [“Enrolling a Device” on page 69](#)
- ◆ **MDM Servers:** [“Configuring MDM Servers” on page 19](#)
- ◆ **Android Devices:** [“Enabling Push Notifications” on page 23](#)
- ◆ **Apple Devices:** [“Enabling Push Notifications” on page 23](#)
- ◆ **ActiveSync Servers:** [“Configuring Email Access” on page 63](#)
- ◆ **Email Policy:** [“Configuring Email Access” on page 63](#)
- ◆ **Apple VPP Subscription:** [“Subscribing to Apple VPP” on page 53](#)

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

- 2 Complete the **Configuration** tasks that are required to enroll the devices to the zone. Subsequently, you can complete the tasks listed in the **What’s Next** section to manage these devices.

You can refer to the following sections within this guide to understand the procedure to complete each **What’s New** task:

- ◆ **Mobile Security and Control:** [“Securing a Device” on page 29](#)
- ◆ **Deploy Mobile Applications:** [“Provisioning Apps” on page 43](#)

3.2 Prerequisites

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

- ◆ **Install and Configure ZENworks:** The Mobile Management feature is integrated with ZENworks Configuration Management. To install and configure ZENworks Configuration Management, see [ZENworks 2017 Server Installation Guide](#).

4 Configuring User Sources

User-based management is an important facet of mobile 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.

- ♦ [Section 4.1, “Adding an LDAP Directory as a User Source,” on page 15](#)
- ♦ [Section 4.2, “Enabling a User Source for Mobile Device Enrollment,” on page 16](#)

4.1 Adding an LDAP Directory as a User Source

4.1.1 Prerequisites

Your ZENworks Management Zone must be connected to the LDAP directory that is your mobile device users' primary authentication source and the connection must be configured to allow username/password authentication.

4.1.2 Procedure

- 1 On the Getting Started with Mobile Management page, click **User Sources** to display the Configuration page. Alternatively, from the left hand side navigation pane of ZCC, click **Configuration** and navigate to the **User Sources** section.
- 2 In the User Sources panel, click **New** to launch the Create New User Source Wizard.
- 3 On the Connection Information page, define the following connection information, then click **Next**:
 - ♦ **Connection Name:** Specify a descriptive name for the connection to the LDAP directory.
 - ♦ **Address:** Specify the IP address or DNS hostname of the server on which the LDAP directory resides.
 - ♦ **Use SSL:** By default, this option is enabled. Disable the option if the LDAP server is not using the SSL (Secure Socket Layer) protocol.
 - ♦ **Port:** This field defaults to the standard SSL port (636) or non-SSL port (389) depending on whether the **Use SSL** option is enabled or disabled. If your LDAP server is listening on a different port, specify that port number.
 - ♦ **Root LDAP Context:** Displays the root context for the LDAP directory. The root context establishes the point in the directory where you can begin to browse for user containers. Specifying a root context can enable you to easily navigate to the directory, but it is optional. If you do not specify a root context, the directory's root container becomes the entry point.

- ♦ **Ignore Dynamic Groups in eDirectory:** This option allows you to select whether or not to display the dynamic groups in a user's page. If you choose to select **Ignore Dynamic Groups in eDirectory**, then administrators cannot assign a policy or a bundle to a dynamic user group and the dynamic group membership will not be computed while calculating the effective assignments for any user.
- 4 (Optional) On the Certificate page (which is displayed only if the connection is using SSL), review the certificate information, then click **Next**.
 - 5 On the Credentials page, specify a username and password to access the directory, then click **Next**.
 - ♦ **Username:** Specify the username for a user that has read-only access to the directory. The user can have more than read-only rights, but read-only rights is all that is required and recommended.
For Novell eDirectory access, use standard LDAP notation. For example:
`cn=admin_read_only,ou=users,o=mycompany`
For Microsoft Active Directory, use standard domain notation. For example:
`AdminReadOnly@mycompany.com`
For DSfW, use standard LDAP notation. For example:
`cn=admin_read_only,ou=users,dc=mycompany, dc=com`
 - ♦ **Password:** Specify the password for the user you specified in the **Username** field.
 - 6 On the Authentication Mechanisms page, select **Username/Password**, then click **Next**.
 - 7 On the User Containers page, add all containers that have user accounts of users to whom you want to provide mobile management access, then click **Next**.
 - 8 Complete the wizard.

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.

4.2 Enabling a User Source for Mobile Device Enrollment

4.2.1 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. For fully managed iOS devices, the updated Mobile Email policy will automatically re-configure

the email account. However, for fully managed Android devices, based on the updated Mobile Email policy, the email settings are sent to the device and the user needs to manually re-configure the email account.

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

Domain Alias: If you do not use simple enrollment, you must add at least one registration domain. To add a domain, 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.

If you have multiple user sources, you cannot use the same domain name in more than one user source. Domain names must be unique across user sources. Also, if you change this setting from one user source to another, then the email accounts on mobile devices enrolled using the earlier user source might not work properly. For fully managed iOS devices, the updated Mobile Email policy will automatically re-configure the email account. However, for fully managed Android devices, based on the updated Mobile Email policy, the email settings are sent to the device and the user needs to manually re-configure the email account.

For more information on the existing Users feature of ZENworks, see [ZENworks User Source and Authentication Reference](#).

5 Configuring MDM Servers

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 the 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.

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.

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, ZENworks MDM Server faces the Internet from within the DMZ. This lets the enterprise firewall protect the MDM Server from external attacks.

- ♦ [Section 5.1, “Adding an MDM Server,” on page 19](#)
- ♦ [Section 5.2, “Testing the Outbound Capability of MDM Servers,” on page 20](#)
- ♦ [Section 5.3, “Securing MDM Servers,” on page 20](#)
- ♦ [Section 5.4, “MDM Servers and APNs Configuration,” on page 21](#)
- ♦ [Section 5.5, “Removing MDM Servers,” on page 21](#)
- ♦ [Section 5.6, “Configuring a Default DNS Name,” on page 22](#)

5.1 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 2017 version or newer deployed on it.

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

5.1.1 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**.


5.2 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 Google Cloud Messaging (GCM). If the configuration is valid, both these options will test connection to APNs and GCM respectively, from each of the MDM Servers. If 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 MDM Servers fails, check the zcc.log, services-messages.log, and the loader-messages.log.

5.3 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 2017 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.

5.4 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.

5.5 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. 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 in the zone, then you can add it back only after 30 minutes from the time the role was removed.

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. Also, if you delete all the MDM Servers, then the push notifications configuration (APNs and GCM) will be automatically deleted.

5.6 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. 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.

6 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 6.1, “Enabling Push Notifications for Android Devices,” on page 23](#)
- ♦ [Section 6.2, “Enabling Push Notifications for iOS Devices,” on page 26](#)

6.1 Enabling Push Notifications for Android Devices

Google Cloud Messaging (GCM) enables a ZENworks MDM Server to notify an Android device when the server requires information from the device or has changes for the device. The ZENworks MDM Server communicates with the Google Cloud Messaging 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 receive the changes.

6.1.1 Prerequisites

- ♦ **Firestore Console:** For Google Cloud Messaging, you must use the Firestore Console, which is the latest version of GCM. In this console, you need to create a Firestore project and obtain a project API Key (server key) and a Project Number (sender ID) that allows your ZENworks Primary Server to send notifications to Android mobile devices. The Project Number and API Key are then used to configure ZENworks access to the GCM service.

However, if you have already created a GCM project, then the steps to retrieve the API key and Project Number are detailed in the following procedure.

- ♦ **MDM Server:** An MDM role is assigned to a Primary Server. For more information, see [Configuring MDM Servers](#).

6.1.2 Procedure

- 1 **Create a Firestore Project:** Follow these steps if you want to create a Firestore project. However, if you have already created a GCM project, then go to [Step 2](#):

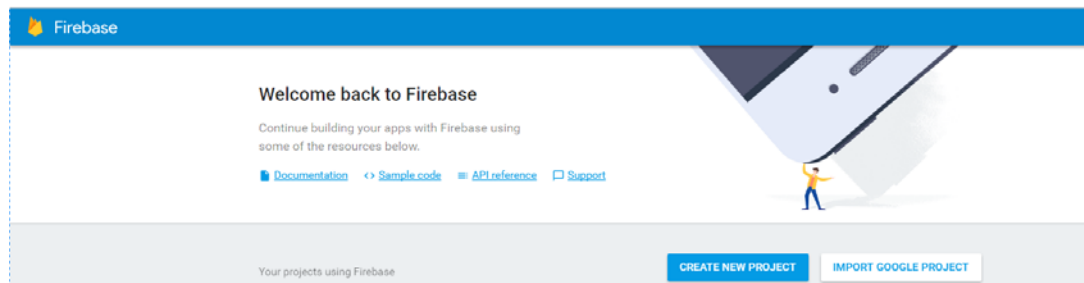
- 1a On the Getting Started with Mobile Management page, navigate to the **Android Devices** section, click **Configure GCM** to display the Google Cloud Messaging page. Alternatively, from the left hand side navigation pane of ZCC, navigate to **Configuration > Push Notification > Google Cloud Messaging**.

- 1b Click **Google Developers Console**, which will direct you to the Firestore console at <https://console.firebase.google.com>.


- 1c Sign in using your Google account credentials.

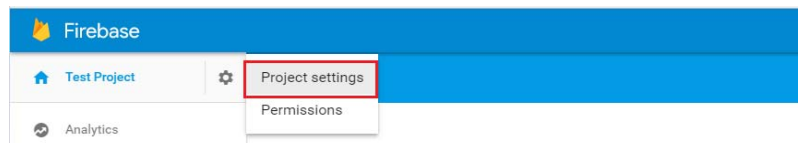
As a best practice, we recommend that this should be a Google account created specifically for managing your corporate Google Cloud Messaging service and not a personal Google account.

- 1d Click **Create New Project**.

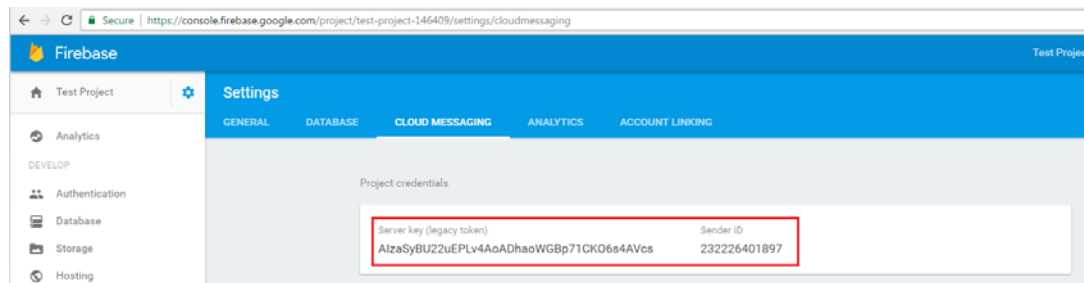


1e Specify a **Project Name** and click **Create Project**.

1f After the project is created, click  appearing next to your project and click **Project Settings**.



1g Select the **Cloud Messaging** tab. You can now view the **Server Key**, which is the same as the **API key**, and the **Sender ID**, which is the same as the **Project Number**.

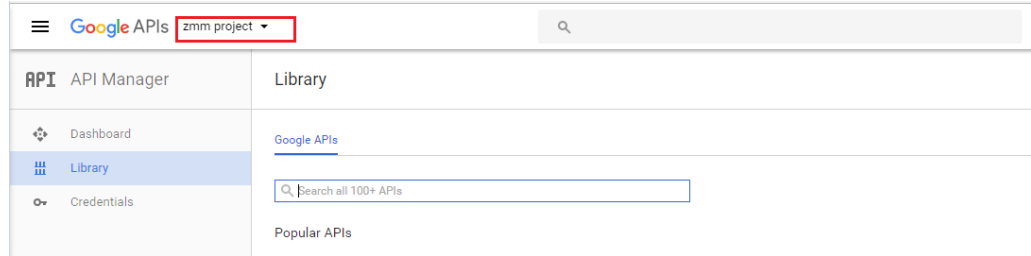


1h Exit the Firebase Console, then continue with [Step 3](#).

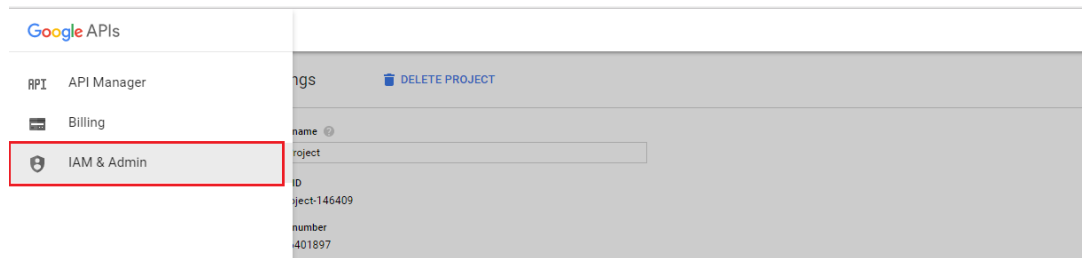
2 Existing GCM Project: If you have already created a GCM project, then refer to the following steps to retrieve the API Key and Project Number:

2a Navigate to the link <https://console.developers.google.com> and sign in using your Google account credentials.

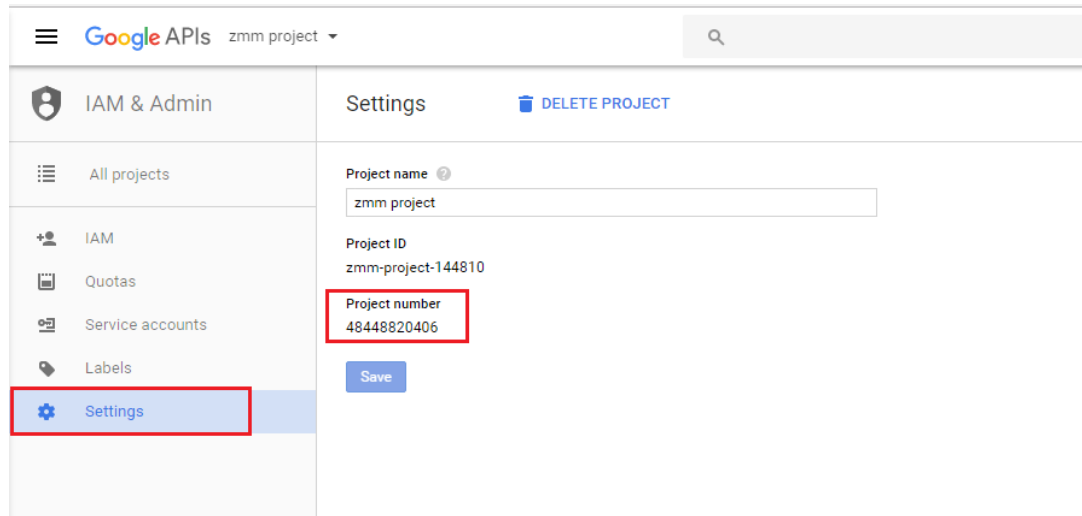
2b Select the existing GCM project from the drop-down menu appearing on the top-left corner of the page.



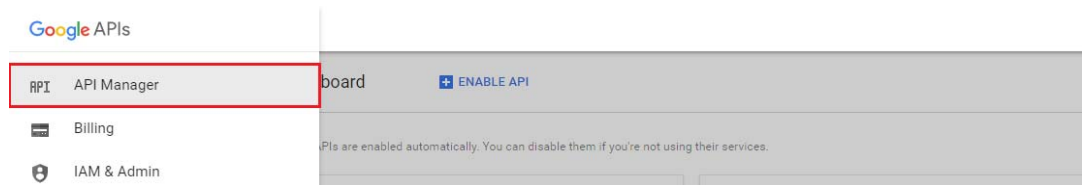
2c To retrieve the project number, click the Hamburger menu appearing on the top-left corner and select **IAM & Admin**, to view the IAM & Admin page.



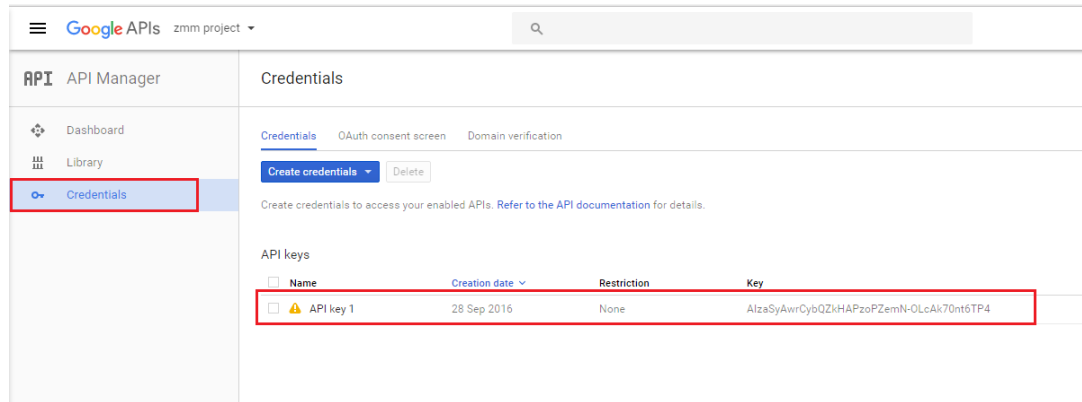
2d On the IAM & Admin page, click **Settings**. You can now view and make a note of the **Project Number**.



2e To retrieve the API key, click the Hamburger menu and click **API Manager** to view the API Manager page.



2f On the API Manager page, click **Credentials** to view the API key.



2g Exit the Google Developers Console, then continue with [Step 3](#).

3 In ZCC, on the Getting Started with Mobile Management page, navigate to the Android Devices section, click **Configure GCM** to display the Google Cloud Messaging page. Alternatively, from the left hand side navigation pane of ZCC, navigate to **Configuration > Push Notification > Google Cloud Messaging**. Configure ZENworks with the Project Number and API Key:

3a Click the **Enable Google Cloud Messaging** check box to turn on the option.

3b Fill in the following fields with the information you generated in the Google Developers Console:

- ♦ **Project number:** Specify the project number generated for your ZENworks project.
- ♦ **API key:** Specify the API server key generated for your ZENworks project.
- ♦ **Key activation date:** Specify the key's activation date.
- ♦ **Google user ID:** Specify the Google account ID used to log in to the Google Developers Console and create the ZENworks project.

3c Click **Test API Key** to validate that the information is entered correctly and the key is active. This option will test the connection to GCM 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.

3d Click **OK** to save your Google Cloud Messaging configuration.

6.2 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.

6.2.1 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 MDM Servers](#). To enable both internal and external access to the MDM server, certain firewall ports must be open. Most MDM servers accept inbound connections using HTTPS on port 443. Both the MDM server and the iOS clients must communicate with the Apple Push Notification service. For outbound connections, the MDM server uses ports 2195 and 2196 with APNs, while clients use port 5223. Port 5223 must be open in the firewall to enable mobile devices to communicate with the MDM server at all times.

6.2.2 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.

6.2.3 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.

7 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:** 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.
- ♦ **Mobile Security Policy:** configures the password restrictions, encryption settings, and device inactivity settings.
- ♦ [Section 7.1, "Creating a Mobile Device Control Policy," on page 29](#)
- ♦ [Section 7.2, "Editing Mobile Device Control Policy Settings," on page 30](#)
- ♦ [Section 7.3, "Assigning a Mobile Device Control Policy," on page 34](#)
- ♦ [Section 7.4, "Creating a Mobile Security Policy," on page 35](#)
- ♦ [Section 7.5, "Editing Mobile Security Policy Settings," on page 36](#)
- ♦ [Section 7.6, "Assigning a Mobile Security Policy," on page 40](#)

7.1 Creating a Mobile Device Control Policy

7.1.1 Procedure

- 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 > 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, disables voice assistant Siri, removes the device camera, and disables pop-up tabs in Safari.
- 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 Mobile Device Control Policy Settings](#).

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

7.2 Editing Mobile Device Control Policy Settings

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. However, these settings vary based on the platform. Also, you can configure these settings for a personal or a corporate owned device.

7.2.1 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.

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.

Apple: The settings that can be enabled or disabled for iOS devices are as follows:

Tab	Settings	Description
Device	Allow Camera	Determines whether to enable or disable the device camera. If set to No , the camera icon is removed from 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 .

Tab	Settings	Description
	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.
	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.
	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.
	Allow screenshots	Determines whether the user can capture images of the device's display screen.
	Allow sending diagnostic and usage data to Apple	Determines whether automatic submission of diagnostic and usage reports to Apple should be enabled.
	Allow users to accept untrusted TLS certificate	Determines whether the user can accept Transport Layer Security (TLS) certificates that cannot be verified.
	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.
	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.
	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
	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.

Tab	Settings	Description
Apps	Allow enterprise app trust	Determines whether the user is allowed to install or use enterprise apps that are not distributed by ZENworks.
	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.
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.
iTunes	Require iTunes Store password for each purchase	Determines whether or not the user needs to enter the password for each purchase on the iTunes Store.
iCloud	Allow My Photo Stream	Determines whether a copy of any photo taken on the managed iOS device should be synced with the user's other iOS devices.
	Allow iCloud Keychain	Determines whether Keychain data such as accounts, passwords, and credit card information, should be synced with iCloud.
	Allow iCloud Photo Library	Determines whether photos on iCloud can be accessed on the managed device.
	Allow iCloud Photo Sharing	Determines whether the user can publish and share photos with other iOS users through the iCloud website. Default value is Yes .
	Allow iCloud backup	Determines whether data can be backed up or restored on iCloud.
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.
	Accept cookies	<p>Determines the cookie policy that should be enabled in the Safari web browser. The accepted values are:</p> <ul style="list-style-type: none"> ◆ Block all websites, third parties, and advertisers from storing cookies on the device. ◆ Allow all websites, third parties, and advertisers to store cookies on the device. ◆ 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. ◆ 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>The default value is to allow cookies from all websites, third parties, and advertisers.</p>

Tab	Settings	Description
	Allow pop-ups	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 .
	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 .
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.
	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.
	Show Notification Center in Lock screen	Determines whether Notification Center can be accessed from the Lock screen.
	Show Today View in Lock screen	Determines whether the Today View in Notification Center should be displayed on Lock screen.
Media Content	Allow Bookstore Erotica	Determines the user is permitted to download media that is tagged as erotica from the iBooks store.
	Ratings Region	Determines the region that needs to be selected to populate the allowed ratings for media content defined for that region.
	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.
	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.
	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.
Security	Allow Touch ID to unlock device	Determines whether the user can unlock the device by using fingerprint.

Android: The settings that can be enabled or disabled for Android devices are as follows:

Settings	Description
Allow Camera	Determines whether the device camera should be enabled. If set to No , the camera is disabled and a warning message is displayed if the user tries to access it.

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

- ◆ ActiveSync Only devices
- ◆ Fully Managed devices, that is, iOS and ActiveSync (iOS MDM + ActiveSync) or Android and ActiveSync (Android App + ActiveSync).

If a setting is applicable for both Android and ActiveSync, or iOS and ActiveSync, then the stricter setting of the two is applied. For example: the mode in which a device is enrolled is iOS MDM + ActiveSync. 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.

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.

7.3 Assigning a Mobile Device Control Policy

Most mobile policies 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 device.

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

7.3.1 Procedure

- 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.

7.4 Creating a Mobile Security Policy

7.4.1 Procedure

- 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. 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. 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 Mobile Security Policy Settings](#).

Click **Finish** to complete the policy.

7.5 Editing Mobile Security Policy Settings

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.

7.5.1 Procedure




- 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.

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









- ◆  Android
- ◆  iOS
- ◆  ActiveSync

Password: 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. Using the example values provided in the table below, the following settings would be applied:




- ◆ **Android:** The **Require numeric complex password** setting for Android 5.0 and higher.
- ◆ **iOS:** The **Require simple password** setting.
- ◆ **ActiveSync:** The **Require simple password** setting.

Setting	Description	Example	Platform Support
Require password	Requires a password to unlock the device.	Yes	  
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).	No	
Require simple password	Allows the password to include repeating characters such as (0000) or sequential characters such as (abcd). 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.	Yes	  
Minimum password length	Specifies the minimum number of characters required for the password.	8	  
Require numeric password	Requires the password to contain numbers. Other characters (letters and symbols) are optional.	No	
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.	Yes	
Require alphabetic password	Requires the password to contain letters (or symbols). Other characters (numbers) are optional.	No	







Setting	Description	Example	Platform Support
Require alphanumeric password	Requires the password to contain letters (or symbols) and numbers.	No	 iOS 
Require complex password	Requires the password to contain letters, numbers, and symbols.	Inherit	 iOS 
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 	2	
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>	2	 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>	1	
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>	1	
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>	1	
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>	1	
Minimum nonletters required	<p>Applies only if Require complex password is set to Yes or Inherit.</p> <p>Specifies the minimum number of numbers or symbols that must be included in the complex password.</p>	2	




Setting	Description	Example	Platform Support
Require password expiration	Requires the password to expire within a specified number of days.	Yes	 iOS 
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.	30	 iOS 
Require password history	Requires a history of used passwords to be stored in order to prevent immediate reuse of passwords.	Yes	 iOS 
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.	3	 iOS 

Encryption: Not all Encryption settings apply to all device platforms. In addition, the setting support can vary from version to version within a platform.

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

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.

Setting	Description	Platform Support
Require inactivity lock	Requires the device to be locked after it has been inactive for a specified period of time.	 iOS 
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.	 iOS 
Wipe device on failed number of unlock attempts	Wipes the device data after a specified number of failed attempts to unlock the device.	 iOS 

Setting	Description	Platform Support
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.	  
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

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.

7.6 Assigning a Mobile Security Policy

Most mobile policies 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 policies to user groups, user folders, device groups, and device folders. Each member of the group or folder receives the assignment.

7.6.1 Procedure

- 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](#).

8 Provisioning Apps

ZENworks lets you provision apps or an iOS configuration profile to mobile devices by using the existing Bundles feature in ZENworks Control Center. A bundle consists of all the configuration settings and installation instructions required to deploy and manage applications or profiles on a device. In ZENworks Mobile Management, bundles are currently supported for only iOS devices. There are two types of bundles that can be created:

- ♦ **App Store App:** Allows you to distribute apps available in the Apple App Store.
- ♦ **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 to restrict certain device features.
- ♦ [Section 8.1, “Creating an iOS Bundle,” on page 43](#)
- ♦ [Section 8.2, “Assigning an iOS Bundle,” on page 45](#)
- ♦ [Section 8.3, “Installing a Bundle using Quick Task,” on page 46](#)
- ♦ [Section 8.4, “Viewing Bundle Information,” on page 47](#)

8.1 Creating an iOS Bundle

8.1.1 Prerequisites

- ♦ Ensure that you remain connected to your iTunes account, 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.

8.1.2 Procedure

- 1 On the Getting Started with Mobile Management page, navigate to the **Deploy Mobile Applications** section and click **Create New 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 **App Store App** or **iOS Profile**.
- 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 If **App Store App** is selected in [Step 3](#), then follow these steps:
 - 5a On the Search iOS App page:
 - 5a1 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.

5a2 Click **Search** to view the search result.

5a3 (Optional) Click **Reset** to clear the search and search result.

5a4 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.

5a5 Select an app. Click **Next**.

5b 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** to 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.

5c 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.
- 6 If **iOS Profile** was selected in [Step 3](#), then in the Import Profile page browse and upload the configuration profile that you have created using Apple Configurator. For more information on creating and importing iOS profiles, refer to the Apple Configurator documentation. Click **Create Sandbox**, if you want to create a Sandbox only version of the bundle.
 - 7 Click **Finish** to complete the activity.

8.2 Assigning an iOS Bundle

ZENworks lets you assign bundles to users as well as devices. These bundles can be assigned directly to a user, a device, a user group, a device group, a user folder, or a device folder.

8.2.1 Procedure

- 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	Select one of the following: <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.

Option	Steps
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. Based on this selection, the app will 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 Review the summary page and click **Finish** to complete the assignment.

When the device to which the bundle is assigned syncs with the ZENworks Server, then a notification to install the app is sent to the device. Based on the user's response, the app is installed on the device. In the subsequent refresh, the status of the bundle is marked as **Success** or **Failure**.

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 2017 Management Zone Settings Reference](#).

8.3 Installing a Bundle using Quick Task

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

8.3.1 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.

8.4 Viewing Bundle Information

When you create a bundle, the bundle is listed on the Bundles page of the ZENworks Control Center.

8.4.1 Understanding the Bundle Information

The Bundles page displays the following information:

- ♦ **Status:** Provides a quick indication of the message logging and enforcement status of the bundle. The status icons are:
 -  - No warning or error messages;
 -  - Warning messages;
 -  - Error messages;
- ♦ **Name:** Displays the object's (bundle, bundle group, or the bundle folder) name. Click the name to view or edit the object's information.
- ♦ **Type:** Displays the type of object. For example, an iOS bundle.
- ♦ **Category:** Displays the bundle category selected during the creation of the bundle. For example, App Store App.
- ♦ **Enabled:** Displays whether the bundle is enabled to be deployed on a device or not. The possible values are **Yes** and **No**.
- ♦ **Version:** Displays the latest published version of the bundle. However, if the bundle is a sandbox-only bundle, it displays **Sandbox**.
- ♦ **Has Sandbox:** Displays whether the bundle has a sandbox or not.

8.4.2 Bundle Summary Page

The Summary page of the bundle displays the general information, bundle status, generated messages, and scheduled events for the specified version of the bundle. This page can be viewed when you click a specific bundle on the Bundles page.

Displayed Version

Lists all existing versions of the bundle and the latest version of the bundle is selected by default. Select the version of the bundle whose details you want to view or edit. If a Sandbox version of the bundle exists, this option displays the Sandbox version. However, if a Sandbox version of the bundle does not exist, this option displays the published version.

General

The General panel provides a summary of the bundle's general settings.

- ◆ **Bundle Type:** Displays the type of bundle.
- ◆ **Volume Purchase Program Account:** Displays the Apple VPP account, if the bundle is an Apple VPP bundle.
- ◆ **Version:** Displays the bundle's version number.
- ◆ **Enabled:** Displays whether or not the bundle can be deployed to iOS devices. If a bundle is enabled, it can be deployed to iOS devices. When you disable a bundle, the app is uninstalled from the device. However, if the **Retain app on the device if the bundle is deleted or unassigned, or if the device is removed from the zone** setting is enabled as part of the app configuration settings, then this bundle will not be uninstalled from the device. If the bundle is disabled and if the app is installed on the device, then the app will be uninstalled from the device. You can click **Enable** to allow it to be deployed.
- ◆ **Number of Errors not Acknowledged:** An error is anything that causes the deployment or installation of the bundle to fail. The number displayed indicates the number of unacknowledged warnings, which are errors that you have not specifically marked as acknowledged. Unacknowledged errors are displayed in the Message Log section.
- ◆ **Number of Warnings not Acknowledged:** A warning is anything that does not cause the deployment or installation of the bundle to fail, but indicates minor problems with the bundle. The number displayed indicates the number of unacknowledged warnings, which include warnings that you have not specifically marked as acknowledged. Unacknowledged warnings are displayed in the Message Log section.
- ◆ **GUID:** Lists the bundle's GUID (global unique identifier), a randomly generated string that provides a unique identifier for the bundle. You cannot edit the GUID.
- ◆ **Display Name:** Displays the bundle's name as it appears in ZENworks Control Center (ZCC). Click **Edit** to change the name. Changing the name does not cause the bundle to be redeployed.
- ◆ **Description:** Displays the bundle's description, if one was provided when the bundle was created. The description appears in ZCC. Click **Edit** to change the description.
- ◆ **Administrator Notes:** Displays any information that has been added specifically for ZENworks administrators to view. The notes are displayed only in ZCC.
Click **Edit** to change the notes, add notes, or delete notes. Editing the note does not create a sandbox. You can edit the administrator notes for any version of a bundle.

Bundle Status

The Bundle Status panel displays a summary of the bundle's assignment and deployment status. The **User** row displays the status of the bundle through assignment to users; the **Device** row displays the status of the bundle through assignment to devices. A bundle can be directly assigned or assigned

through membership in a folder or group. You can click an underlined link in any column to view the status of the individual users and devices to which the bundle is assigned or export the data to a CSV file. To export a bundle, select the bundle and click **Actions > Export**.

A bundle's status is calculated using the status of many events. For example, a device might indicate that the bundle failed when the distribution was successful, but the installation failed. The numbers in the various columns represent an overall view of the bundle's status.

The bundle status information is separated into the following groups listed below, which are independent of each other.

Assignment Status

The following status information is available:

Targeted: Displays the number of users and devices to which the bundle is assigned.

Devices Effective: Displays the number of devices on which the bundle is effective through a user or device assignment. A bundle is effective for a device if the device meets the system requirements of the bundle. The number of users or devices in the **Devices Effective** column might be less than the number in the **Targeted** column because the bundle might be assigned to a device that does not meet the bundle's system requirements.

Devices Not Effective: Displays the number of devices on which the bundle is not effective through a user or device assignment. If a bundle is not effective for the device, it means that the device does not meet the bundle's system requirements.

Pending: The pending status for the device displays the number of devices on which the bundle is not yet distributed or installed, such as devices that are switched off. Click the underlined link to display the list of such devices.

Blocked/Targeted: Displays the number of users or devices on which the bundle is blocked from being used, versus the targeted number of users or devices. Click the underlined link to display the list of such users or devices.

Deployment Status

The following status information is available:




Devices Pending: Displays the number of devices on which the bundle is pending to be deployed. A bundle's status is pending if the bundle has met the device's system requirements, but the bundle has not been distributed to the device or the bundle has been distributed to the device but the bundle has not been installed.

Devices Succeeded: Displays the number of devices on which the bundle was successfully distributed and installed.

Devices Failed: Displays the number of devices on which the bundle's distribution or installation failed.

Message Log

The Message Log panel displays all unacknowledged messages generated for the object. An unacknowledged message is one that you have not yet reviewed and marked as acknowledged.

- ♦ **Status:** Displays an icon indicating the type of message:  critical,  warning, and  normal.
- ♦ **Message:** Displays a brief description of the event that occurred.

- ♦ **Date:** Displays the date and time the event occurred.

A message remains in the Message Log list until you acknowledge it. You can acknowledge individual messages, acknowledge all messages at one time, or view more information about both acknowledged and unacknowledged messages. The following table explains how to do these tasks:

Task	Steps	Additional Details
Acknowledge a message	<ol style="list-style-type: none"> 1. Click the message to display the Message Detail Information dialog box. 2. Click Acknowledge. 	If you decide that you do not want to acknowledge the message, click Cancel to dismiss the dialog box. This causes the message to remain in the Message Log list.
Acknowledge all messages	<ol style="list-style-type: none"> 1. In the Tasks list located in the left navigation pane, click Acknowledge All Messages. 	
View all acknowledged or unacknowledged messages	<ol style="list-style-type: none"> 1. Click the Advanced button to display the Edit Message Log page. 	<p>In addition to viewing all acknowledged and unacknowledged messages, you can also view only those messages with a specific status or date, view more details about messages, and acknowledge messages.</p> <p>Click the Help button on the Edit Message Log page for specific information about performing tasks on that page.</p>
Delete a message	<ol style="list-style-type: none"> 1. Click the relevant messages to display the Message Log dialog box. 2. Click Delete. 	Deleting a message completely removes the message from your ZENworks system.

App Details

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:

- ♦ **Size:** Displays the size of the app.
- ♦ **Categories:** Displays the Apple App Store categories in which the app is included. For example: Games, Education and Business.
- ♦ **iTunes Store ID:** Displays the App Store ID that is linked to the iTunes Store. Click the ID to access the app on the iTunes Store.
- ♦ **Cost:** Displays the cost associated with the app.
- ♦ **App Region:** Displays the region selected while creating the new bundle.
- ♦ **Device Compatibility:** Displays the supported devices that can run the app.
- ♦ **OS version compatibility:** Displays the supported operating system versions for the app.
- ♦ **Supported Languages:** Displays the supported languages for the app.

8.4.3 Bundles Relationship Page

The Relationships page of the bundle lets you view and manage the assignments that the bundle has for devices, users, and groups.

Displayed Version: Lists all existing versions of the bundle, and the latest version of the bundle is selected by default. Select the version of the bundle whose details you want to view or edit. If a Sandbox version of the bundle exists, this option displays the Sandbox version. However, if a Sandbox version of the bundle does not exist, this option displays the published version.

Device Assignments: Lists the devices, device folders, or device groups to which the bundle is assigned. You can add and remove assignments.

User Assignments: Lists the users, user folders, or user groups to which the bundle is assigned. You can add and remove assignments.

Bundle Groups: Displays the groups in which the bundle is a member. You can add the bundle to groups or remove it from groups.

8.4.4 Bundles Details Page

For App Store App Bundles:

The Details page of the bundle lets you view or edit the app settings:

- ♦ **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 backup 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 deploying it.

For iOS Profile Bundles:

You can click the download button to view or edit the configuration profile XML file. Subsequently, you can replace the previously uploaded file with the modified file by clicking the browse icon.

If you have modified the settings on the Bundle Details page, then click **Publish** to display the Publish Options page. In this page, you can publish the bundle to assigned devices or users as a new bundle or as a new version of the same bundle.

For more information on the existing Bundles feature of ZENworks, see the [ZENworks 2017 Software Distribution Reference](#) guide.

9 Subscribing to Apple VPP

The Apple Volume Purchase Program (VPP) allows organizations to purchase apps in volume to distribute to their managed devices. After registering with the Apple VPP and on purchasing apps, ZENworks enables distribution of these purchased apps to the devices or to the users who have enrolled their 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.

- ♦ [Section 9.1, “Linking ZENworks to the Apple VPP Account,” on page 53](#)
- ♦ [Section 9.2, “Creating VPP Bundles,” on page 55](#)
- ♦ [Section 9.3, “Distributing VPP Bundles,” on page 56](#)
- ♦ [Section 9.4, “Viewing Volume Purchase Program License Summary,” on page 57](#)
- ♦ [Section 9.5, “Updating License Summary,” on page 59](#)
- ♦ [Section 9.6, “Renewing the VPP Token,” on page 60](#)
- ♦ [Section 9.7, “Revoking App Licenses,” on page 60](#)
- ♦ [Section 9.8, “Viewing or Editing Apple VPP Subscription,” on page 60](#)
- ♦ [Section 9.9, “Deleting a Subscription,” on page 62](#)

9.1 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 this 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 MDM Servers](#).

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

9.1.1 Prerequisites

- ♦ **VPP Enrollment:** VPP is part of the Apple Deployment Programs. To get started, the organization must enroll in the program and create an Apple Deployment Programs account.

9.1.2 Procedure

- 1 On the Getting Started with Mobile Management page, navigate to **Apple VPP Subscription** and click **New 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:** Click **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.
 - 4b **Link ZENworks to the Volume Purchase Program server:** 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.
 - ◆ **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 through 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 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. For more information on each schedule type, see “[Schedule Types](#)” in *ZENworks 2017 Primary Server and Satellite Reference*

Irrespective of the **Schedule Type** selected, ZENworks syncs with Apple on a daily basis, to retrieve the latest apps. However, bundles are not created as a part of this sync. For details, see [Updating License Summary](#).

You can also select the **Launch the Apple Volume Purchase Program Summary page immediately after saving** checkbox, which will re-direct you to the Apple VPP License Summary 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.

9.2 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. This action initiates a sync between Apple and ZENworks to retrieve the latest apps. Subsequently, bundles are created for these apps. For details, see [Viewing or Editing Apple VPP Subscription](#).
- ♦ Click **Create Bundle** on the Apple VPP License Summary page for specific apps. For details, see [Viewing Volume Purchase Program License Summary](#).

NOTE: ZENworks supports distribution of iOS apps only. Also, the assigned app installs on a device only if it is compatible on it. For example: an iOS app that is not compatible with iPhones will not be installed on them.

If the app metadata changes after a bundle is created in ZCC, then the bundle does not reflect the updated metadata. However, if this app is assigned to a device, then the latest version of the app is installed on the device.

Bundle Creation Failure Scenarios

If at any point in time bundle creation fails, then check the logs for details on this failure. Bundle creation might fail due to one of the following reasons:

- ♦ The Apple Server is busy and not responding.

- ◆ Apple is unable to provide the latest app metadata as Apple might have discontinued support for the app.
- ◆ Apple has extended VPP support to a new country, which is not supported by ZENworks. Contact the Micro Focus tech support team to include this country in ZENworks.

9.3 Distributing 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 Apple VPP License Summary page. For details, see [Viewing Volume Purchase Program License Summary](#).

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.

Procedure to Assign Bundles

To assign a bundle, in ZENworks Control Center, click **Bundles** (in the left navigation pane). Select the relevant folder within which the VPP bundles reside.

For more information on assigning bundles, see [Assigning an iOS Bundle](#).

Bundle Distribution Failure Scenarios

If at any point in time bundle assignment or distribution fails, then you need to check the bundle **Deployment Status** to identify the reason for failure. For details, see [Viewing Bundle Information](#). Bundle distribution might fail due to the following reasons:



- ◆ A VPP bundle is assigned to a device with iOS version prior to 9.0. Apple supports device assignments on iOS versions 9.0 or newer.
- ◆ A VPP bundle is assigned to a user and the invite to associate with the Apple VPP is not accepted by the user.
- ◆ A VPP bundle is assigned to a user and the Apple ID on the user's device is different from the Apple ID that the user has used to associate with the Apple VPP.
- ◆ The app is not compatible with the device.
- ◆ Deficit in the number of licenses.
- ◆ The Apple VPP subscription is disabled or deleted.
- ◆ The VPP token ownership has changed and is being used by another MDM solution.
- ◆ Apple is unable to validate the iTunes Store ID of the specific app.
- ◆ The app has discontinued in the iTunes Store.


9.4 Viewing Volume Purchase Program License Summary

The Volume Purchase Program License Summary page provides a single view of all the apps purchased using the VPP accounts associated with all the VPP subscriptions created within your management zone. This page helps you in managing the app licenses as it displays the number of licenses purchased as against the number of licenses consumed and installed. You can also create bundles for any purchased apps in this page. To view this page, navigate to the **Mobile Management** section in ZCC and click the **Apple VPP** tab. You can perform the following tasks on this page:

- ◆ **Create Bundles:** You can create bundles by selecting one or more apps (for each app an individual iOS 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 subscription name is suffixed with the name of the app. For subsequent bundles of the same app, a random GUID number is suffixed.

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.
- ◆ **Filter:** You can filter the data displayed on this page by specifying either the **App Name**, **Publisher**, or the **Subscription Name** in the **Search** field. You can also filter the data to view apps that have bundles or no bundles associated with it. 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:
 - ◆ **App:** Displays the name of the app purchased using the VPP account. You will be unable to hide this column.
 - ◆ **Publisher:** Displays the name of the app publisher.
 - ◆ **Cost:** Displays the cost of the app.
 - ◆ **Subscription Name:** Displays the name of the subscription.
 - ◆ **Purchased:** Displays the number of app licenses purchased using the VPP account.
 - ◆ **Available:** Displays the number of unused licenses that are available for consumption.
 - ◆ **Consumed:** Displays the number of user or 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.
 - ◆ **User License 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 with him/her and if the app is installed on only two devices, then the **User License Installed** count will be 2. 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.
 - ◆ **User License Consumed:** Displays the number of user licenses that are consumed from Apple. 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 user has installed the app 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 License Consumed:** 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.
 - ◆ **Total Apps Installed:** Displays the sum of the user licenses installed and device licenses installed.
 - ◆ **App Size:** Displays the size of the app.
 - ◆ **iTunes ID:** Displays the iTunes Store ID of the associated app.

- ◆ **Total Bundles:** Displays the number of bundles created for the specific app.
- ◆ **Update View:** Click  to initiate a sync between the ZENworks Server and Apple to update this page with the latest apps.

This option also revokes unused app 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.


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.

9.5 Updating 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. For details, see [Viewing or Editing Apple VPP Subscription](#).
- ◆ Click  on the Apple VPP License Summary page. For details, see [Viewing Volume Purchase Program License Summary](#).
- ◆ **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 Apple VPP License Summary 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 Volume Purchase Program License Summary page.

9.6 Renewing the VPP Token

The validity of a VPP token is one year from the time the token is downloaded using the Apple VPP account. 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 page of the Apple VPP Subscription. For details, see [Viewing or Editing Apple VPP Subscription](#).


9.7 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 these actions are 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 2017 Software Distribution Reference](#).

If the device cannot sync with the ZENworks Server, then you can click  on the Apple VPP License Summary 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.

9.8 Viewing or Editing Apple VPP Subscription

You can view or edit the contents of an Apple VPP Subscription. While editing a subscription you can perform tasks such as, renew the linked VPP token or initiate a sync between the ZENworks Server and the Apple Server.

9.8.1 Procedure

- 1 In ZENworks Control Center, navigate to the **Subscribe and Share** section.
- 2 Click the Apple VPP Subscription, for which the content needs to be edited.
- 3 You can edit or view the Apple VPP Subscription in the Summary tab:

General: This panel lets you add information to describe the subscription, enable or disable the subscription, and to view the subscription log details.

- ◆ **Name:** Displays the name of the subscription.
- ◆ **Type:** Displays the type of subscription.
- ◆ **Created By:** Displays who created the subscription.
- ◆ **GUID:** Displays the subscription's GUID (Global Unique Identifier), which is a randomly generated string that provides a unique identifier for the subscription.
- ◆ **Description:** Displays the subscription's description if it was provided when the subscription was created. Click **Edit** to change the description.
- ◆ **Enabled:** Displays **Yes** if the subscription is enabled, or displays **No** if the subscription is disabled. Click the link next to the field to enable or disable the subscription.
- ◆ **Subscription Logs:** Displays messages associated with the last run of the subscription. Click the **View Log** link to view the subscription logs in the Subscription Log Details dialog box.

VPP Token Details: The VPP Token Details panel lets you view information retrieved from the linked Apple VPP token. You can also test the linked token or renew the token.

- ◆ **Organization:** Displays the name of the organization that has subscribed for the Apple VPP.
- ◆ **Country Code:** Displays the country code of the organization that has subscribed for the Apple VPP.
- ◆ **Apple ID:** Displays the Apple ID associated with the Apple VPP token.
- ◆ **Email ID:** Displays the email address associated with the Apple VPP token.
- ◆ **Token Expiry:** Displays the expiry date of the Apple VPP token. You can validate the token by clicking **Test**. If the token has expired, click **Renew** to upload the renewed token.

NOTE: If the existing token or the renewed token is managed by another MDM solution, then an appropriate message will be displayed and you will be unable to use the subscription. You need to delete this subscription and create a new subscription. If you want to continue using the same token in the new subscription, you need to claim management of the token.

Bundle Details: The Bundle Details panel lets you edit information related to iOS bundles configured for the subscription.

- ◆ **ZENworks Bundle Location:** Displays the folder location in which you want the iOS bundle to reside. Within this folder location, another folder with the name of the subscription is created, within which bundles will reside. To change the folder, browse and select a different folder.
- ◆ **Bundle Settings:** Displays the app settings configured while creating the subscription.
 - ◆ **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 and cannot be modified.
- ♦ **Prevent backup of app data to iCloud:** Prevents the backup data 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.

Schedule: The Schedule panel displays details of the bundle creation schedule.

- ♦ **Status:** Displays the bundle creation schedule status. Click **Run Now** to initiate a sync between ZENworks and Apple to retrieve the latest apps and to create bundles for these apps. You can view the **Subscription Logs** for any messages that might have been logged while initiating this sync.
- ♦ **Last Run:** Displays the date on which the bundle creation event was last run.
- ♦ **Bundle Creation Schedule:** Displays the schedule that you set while creating the Apple VPP Subscription. You can select a different schedule type from the drop-down list or edit the existing schedule. For more information on each schedule type, see “[Schedule Types](#)” in [ZENworks 2017 Primary Server and Satellite Reference](#).

9.9 Deleting a Subscription

To delete a subscription or a subscription folder:

- 1 In ZENworks Control Center, click the **Subscriptions** tab.
- 2 In the Subscriptions list, select the check box next to the subscription that you want to delete.
- 3 Click **Delete**. The Delete Subscriptions dialog box is displayed.
- 4 If you want to delete the bundles created by the subscription, select the **Delete the replicated objects created by the subscriptions** check box.
- 5 Click **OK**.

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.

If a token that was previously linked to a deleted subscription (but the bundles are retained), is now linked to a new subscription, 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.

10 Configuring Email Access

ZENworks can relay email and PIM (calendar, contacts, and tasks) traffic between ActiveSync Servers and mobile devices. This requires you to connect your ZENworks Server to the ActiveSync Servers through which your mobile device users receive their email. ZENworks supports ActiveSync Servers running Microsoft Exchange Activesync 12.1 and newer.

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, Blackberry and Windows devices enrolled to the ZENworks Server through the ActiveSync Server to send or receive corporate data.

ZENworks supports both Microsoft Exchange and GroupWise Mobility Servers.

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](#).

- ♦ [Section 10.1, “Connecting to a New ActiveSync Server,” on page 63](#)
- ♦ [Section 10.2, “Linking a User Source to an ActiveSync Server,” on page 64](#)
- ♦ [Section 10.3, “Creating a Mobile Email Policy,” on page 65](#)
- ♦ [Section 10.4, “Assigning a Mobile Email Policy,” on page 66](#)

10.1 Connecting to a New ActiveSync Server

10.1.1 Prerequisites

A backend Exchange Server should be configured with user mailboxes.

10.1.2 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. The standard non-SSL port is 80 and the standard SSL port is 443.
 - ♦ **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.

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.

10.2 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.

10.2.1 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**.

10.3 Creating 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 a Device” on page 69](#)

- ♦ **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.
- ♦ **Android device enrolled as a fully managed device:** If a Mobile Email Policy is assigned to a fully managed Android device, then an email is sent with the account settings (through the SMTP server) to the user who has enrolled the device. Subsequently, this user needs to manually configure the email account 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 the user will be unable to send or receive corporate emails on the device.

10.3.1 Procedure

- 1 On the Getting Started with Mobile Management page, navigate to the **Email Policy** section and click **New 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.
 - ◆ **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) devices 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.

10.4 Assigning a Mobile Email Policy

Most mobile policies 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 policies to user groups, user folders, device groups, and device folders. Each member of the group or folder receives the assignment.

NOTE: 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 **ActiveSync > Mobile Management > Email Notifications**. Click the relevant email and edit its contents.

10.4.1 Procedure

- 1 On the Getting Started with Mobile Management page, 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.

11

Enrolling a Device

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. These enrollment options can be configured in the Mobile Device Enrollment policy that needs to be assigned to the users before their devices are enrolled.

IMPORTANT: Before enrolling the devices, you need to ensure that the ZENworks 2017 release version is deployed on all the Primary Servers within your management zone.

- ◆ [Section 11.1, “Types of Enrollment,” on page 69](#)
- ◆ [Section 11.2, “Modes of Enrollment,” on page 70](#)
- ◆ [Section 11.3, “Creating a Mobile Enrollment Policy,” on page 71](#)
- ◆ [Section 11.4, “Assigning a Mobile Enrollment Policy,” on page 73](#)
- ◆ [Section 11.5, “Prerequisites to Enroll a Device to the ZENworks Management Zone,” on page 73](#)
- ◆ [Section 11.6, “Enrolling an Android Device,” on page 74](#)
- ◆ [Section 11.7, “Enrolling an iOS Device,” on page 82](#)
- ◆ [Section 11.8, “Enrolling an Email Only Device,” on page 87](#)
- ◆ [Section 11.9, “Allowing Manual Reconciliation by User,” on page 91](#)

11.1 Types of Enrollment

ZENworks lets you enroll your devices in either of the following ways:

- ◆ **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.

To enable ZENworks to manage the Exchange ActiveSync capabilities on these devices, you need to ensure that a Mobile Email Policy is assigned to these devices or users. This policy should use the ZENworks Server as the proxy server between the configured ActiveSync Server and the enrolled device.

In the assigned Mobile Email Policy, you also have the option to directly relay mails from the configured ActiveSync Server, however in this case, ZENworks will not manage the corporate email account configured on the device. For more information on configuring email access, see [Configuring Email Access](#).

- ◆ **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, Blackberry, 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, the device will be unable to send or receive emails. ZENworks can only 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. 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.

For more information on configuring an ActiveSync Server and a Mobile Email Policy, see [Configuring Email Access](#).

11.2 Modes of Enrollment

As soon as you enroll your device, the mode in which the device is enrolled is displayed on the Device Information page. To access 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 enrolled mode of the device.

The screenshot shows the ZENworks console interface. The left sidebar contains navigation options like Home, Deployment, Devices, Users, Policies, Bundles, Asset Management, Patch Management, Subscribe and Share, Mobile Management, Reports, Audit and Messages, Diagnostics, Configuration, and Mobile Device Tasks. The main content area displays the 'Device Information' page for a device with ID 'user1-20BUA0KHIG'. The device status is 'Active'. Key details include: Manufacturer: MSFT, Serial number: 411e2ae0ca2d98d2db0797c6b0d9874b, GUID: 411e2ae0ca2d98d2db0797c6b0d9874b, Device ID, Current time zone, Last boot time, and User enrolled: /Users/ravadjst.com/ravadjst.com/RAVmail/Mailusers/user1. The 'Enrolled Mode' is explicitly set to 'ActiveSync' and is highlighted with a red box. Other details include Ownership: Corporate, Network information (Bluetooth MAC, Wi-Fi MAC, IP Address), Last Connections (Oct 25, 2016 01:01 PM), ActiveSync Version (14.1), ActiveSync ID, User Agent, Administrative owner, and Test Device status (No).

For more information on this page, see [Viewing Device Information](#).

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, 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.
- ♦ **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.

11.3 Creating 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.

11.3.1 Procedure

- 1 On the Getting Started with Mobile Management 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 > 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 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 enable the **Allow the device user to select ownership type** option to allow users who are enrolling their devices 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.

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.
- 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.

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.

NOTE: While editing the policy, you can 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 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.

11.4 Assigning a Mobile Enrollment Policy

Mobile Enrollment policy should be assigned to only users.

11.4.1 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.

11.5 Prerequisites to Enroll a Device to the ZENworks Management Zone

Before enrolling a mobile device as a fully managed device or an email only device, you need to ensure that the following prerequisites are met:

- ♦ ZENworks supports devices running on Android 4.1 and newer, and devices running iOS version 8 and newer. Also, ZENworks supports devices running ActiveSync 12.1 and newer.
- ♦ A user source is configured and enabled for mobile device enrollment. For details, see [“Configuring User Sources” on page 15](#)
- ♦ An enrollment policy is created and assigned to the user. For details, see [“Creating a Mobile Enrollment Policy” on page 71](#).
- ♦ An MDM role is assigned to a Primary Server. For details, see [“Configuring MDM Servers” on page 19](#)

- ◆ Push notifications for either Android or iOS devices are enabled. For details, see [“Enabling Push Notifications”](#) on page 23
- ◆ To enable ZENworks to synchronize emails for Exchange ActiveSync accounts, an ActiveSync server should be configured. Also, create and assign a Mobile Email Policy with the ZENworks Server configured as the proxy server for the ActiveSync Server. This will enable ZENworks to manage the corporate emails sent and received on the device. For details, see [“Configuring Email Access”](#) on page 63.

11.6 Enrolling an Android Device

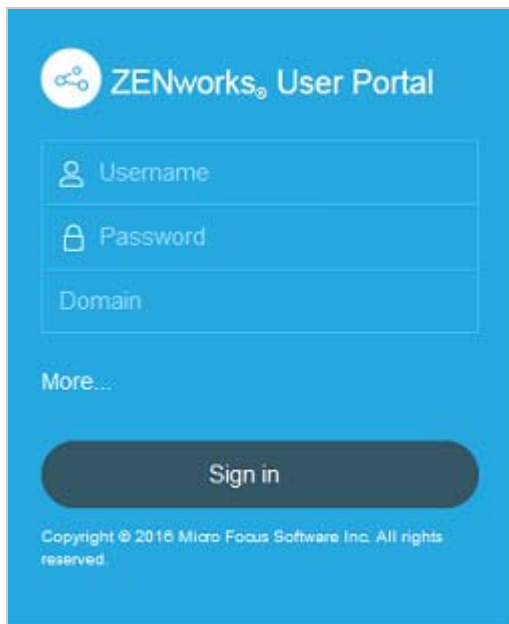
This scenario shows you how to enroll an Android device as a fully managed device in your ZENworks Management Zone.

11.6.1 Procedure

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

NOTE: You must use Google Chrome. The built-in Internet browser is not supported.

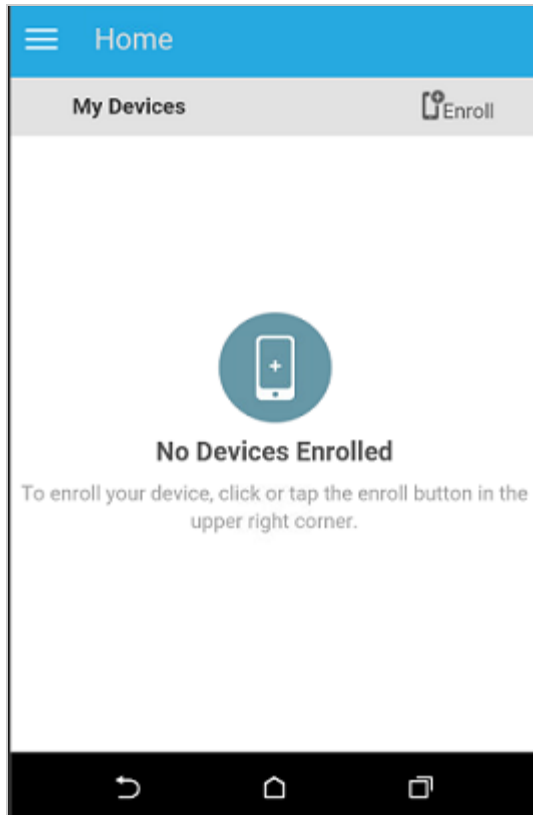
The login screen for the ZENworks User Portal is displayed. You use the user portal to enroll devices to the zone.



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

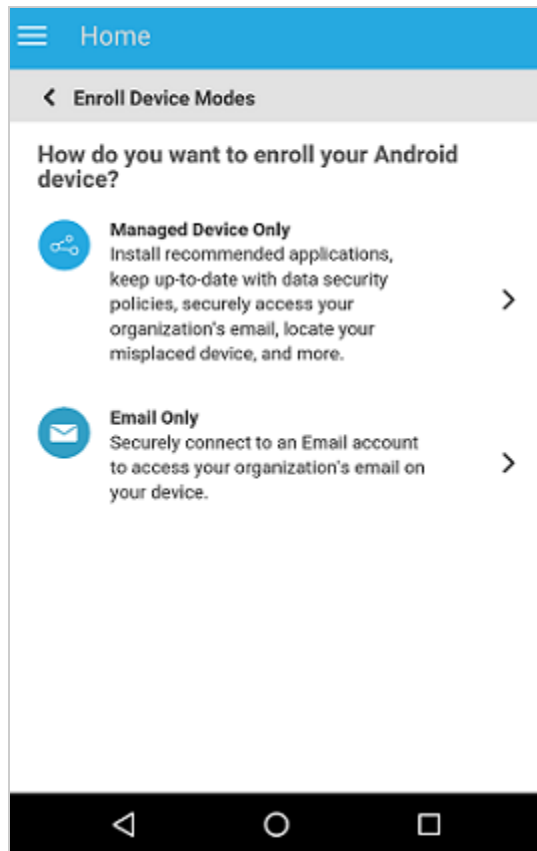
- 2 Enter the user's user name and password. If **Allow Simple Enrollment** option is selected for the user source to which the user belongs, then the registration domain need not be specified or else specify the registration domain. For information, see [Section 4.2, "Enabling a User Source for Mobile Device Enrollment,"](#) on page 16. 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.

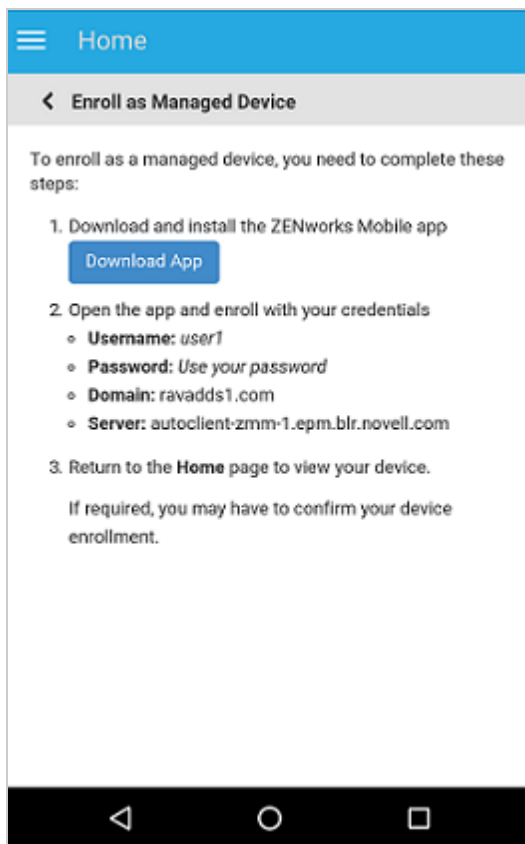


3 Tap **Enroll** in the upper-right corner to display the enrollment options for the device.

The enrollment options are determined by the Mobile Enrollment policy assigned to the user. For details, see [“Creating a Mobile Enrollment Policy” on page 71](#).

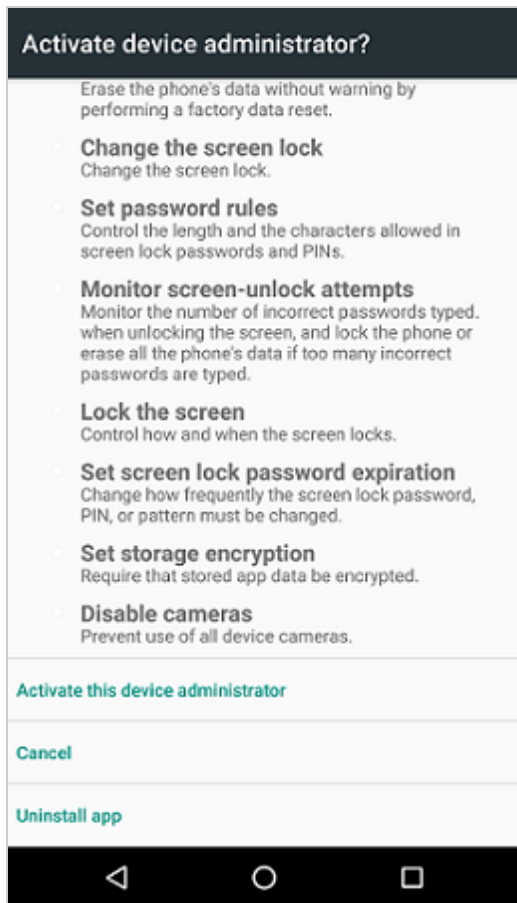


4 Tap **Managed Device Only**.



- 5 Tap **Download App**. The user will be directed to the Google Play Store, where the user needs to click **Install** to install the ZENworks Agent app. After installation, click **Open**.

- 6 Click **Activate this Device Administrator** to enable you to manage the device by performing the operations listed in this screen.



NOTE: For Android Marshmallow and subsequent versions, ensure that the user accepts the `READ_WRITE_PHONE` permission and `WRITE_EXTERNAL_STORAGE` permission after downloading and launching the app. Contrary to the statement mentioned in the dialog box, the `READ_WRITE_PHONE` permission does not make any calls and does not collect phone logs. This permission is required to identify the device's information such as the serial number and IMEI number. The `WRITE_EXTERNAL_STORAGE` permission is required to access the device storage to create logs that can be used for troubleshooting.

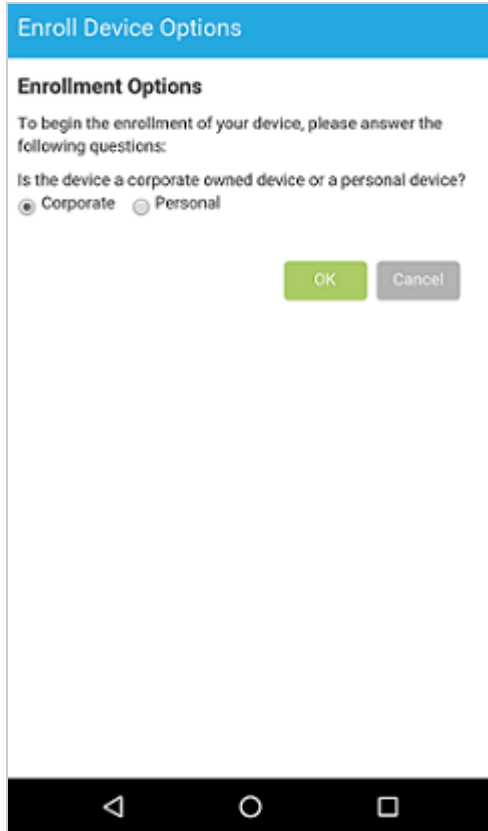
7 The ZENworks Agent app login screen is displayed.



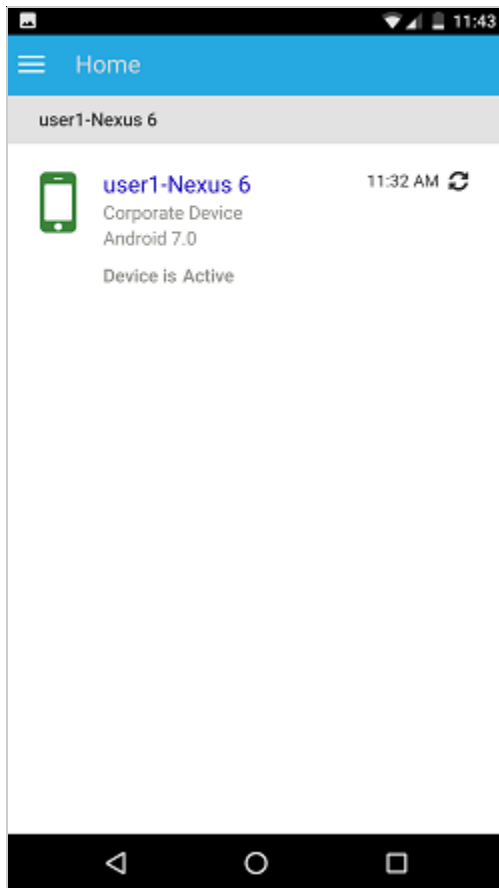
8 Fill in the fields, then tap **Sign In**.

- ◆ **User name, Password, Domain, Server URL:** Use the same user name, password, and registration domain (if required) that you had initially used to log in to the ZENworks User Portal along with the server URL of the ZENworks MDM Server. You can obtain this information from the ZENworks User Portal as displayed in [Step 4](#).

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. Tap **OK**. The device will be automatically enrolled to the zone.



- 9 The ZENworks Agent App Home screen is displayed, showing that the device is enrolled and active.



After the device is enrolled to the ZENworks Management Zone, you can view the device information 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 mode will be displayed as **Android App**.

- 10 After ZENworks Agent app enrollment, based on the assigned Mobile Email Policy, an email is sent to the user with the corporate email account settings. This email can be accessed from the email client's web application or from any other device. With this information, the user needs to manually configure the email account on the device to send or receive corporate emails. You need to configure an SMTP server, to enable ZENworks to send these email notifications. For more information on configuring an SMTP server, see [Event and Messaging Settings](#) in the [ZENworks 2017 Management Zone Settings Reference](#) guide.
- 11 After configuring the corporate email account, the device will enroll and automatically reconcile to the device object that was initially created when the ZENworks Agent app enrollment was completed. The enrollment mode changes to **Android App + ActiveSync** on the Device Information page in ZCC. For more information, see ["Viewing Device Information" on page 96](#).

NOTE: After configuring an ActiveSync account, if the device is unable to auto reconcile to the device object that was created after ZENworks Agent app enrollment and if **Allow Manual Reconciliation by User** is checked in the assigned Device Enrollment Policy, the user will be prompted to manually reconcile the device. For details, see [Allowing Manual Reconciliation by User](#).

If a Mobile Email Policy is unassigned from the device that is enrolled to the ZENworks Management Zone, 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 ZCC by navigating to **Configuration > Mobile Management > Email Notifications**. Click the relevant email and edit its contents.

11.7 Enrolling an iOS Device

This scenario shows you how to enroll an iOS device as a fully managed device in your ZENworks Management Zone.

11.7.1 Procedure

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

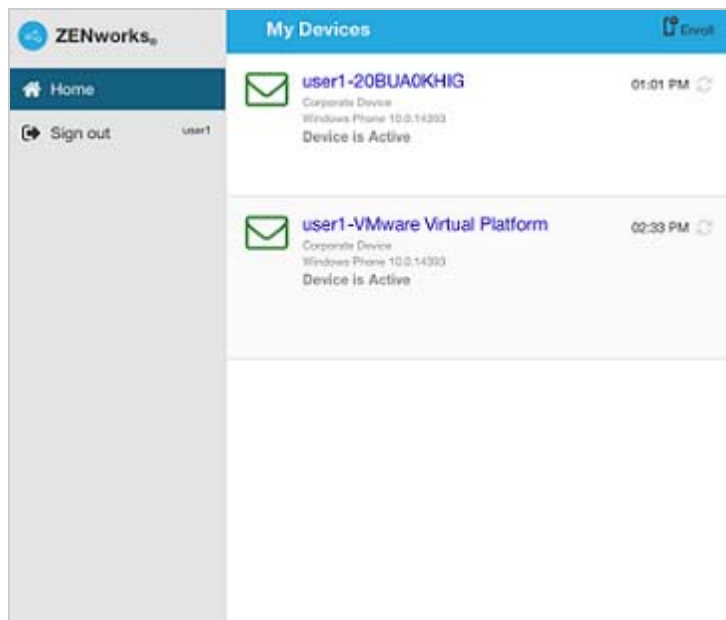
The login screen for the ZENworks User Portal is displayed. You use the ZENworks User Portal to enroll devices to the zone.



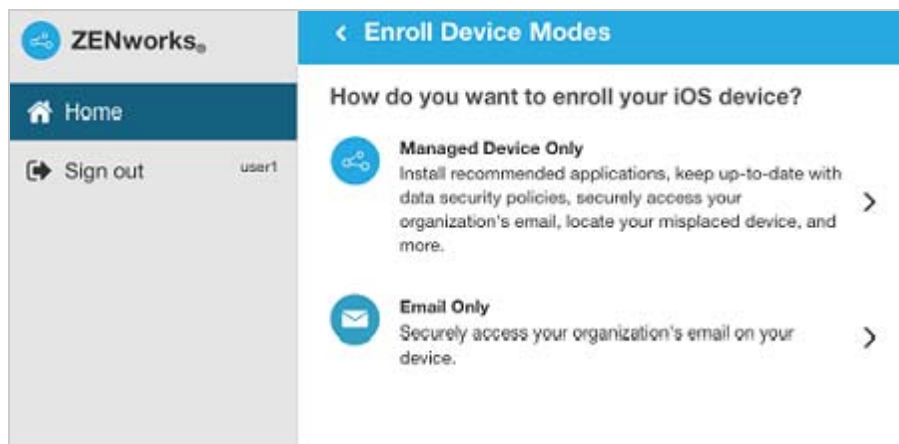
- 2 Enter the user's user name and password. If **Allow Simple Enrollment** option is selected for the user source to which the user belongs, then the registration domain need not be specified or else specify the registration domain. For information, see [Section 4.2, "Enabling a User Source for Mobile Device Enrollment,"](#) on page 16. 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.

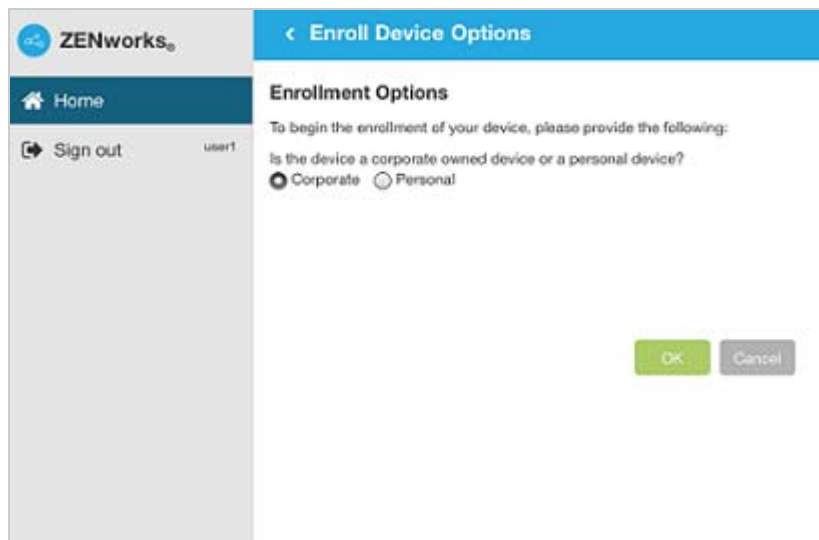
All devices associated with the user, are displayed in the ZENworks User Portal.



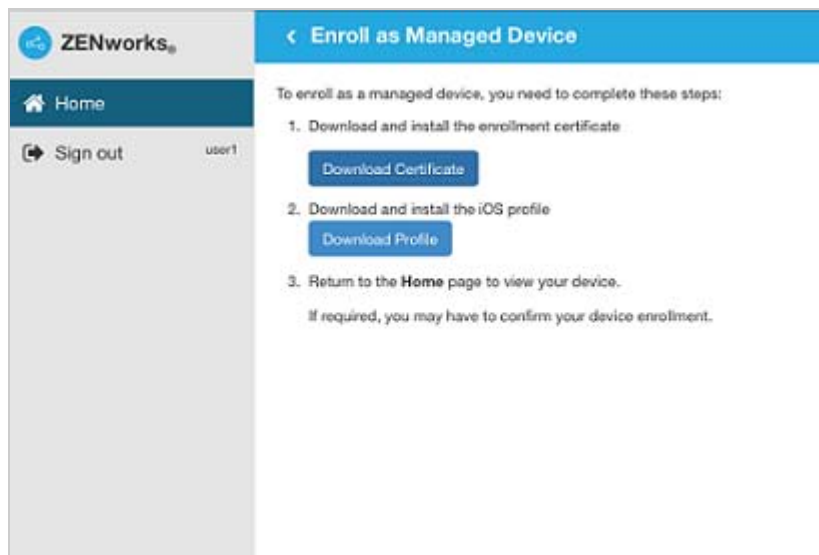
- 3 Tap **Enroll** in the upper-right corner to display the enrollment options for the device. The enrollment options are determined by the user's Mobile Enrollment policy. For details, see [“Creating a Mobile Enrollment Policy” on page 71](#).



- 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**.

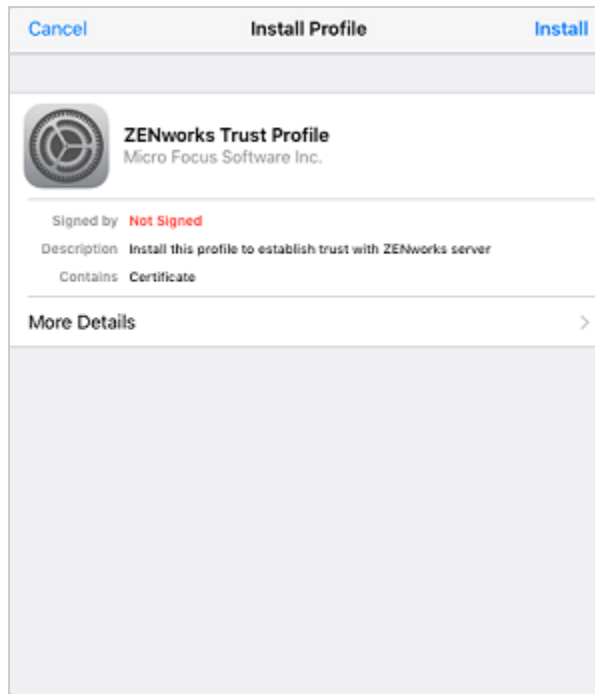


5 Tap **Download Certificate** to display the **Install Profile** screen.



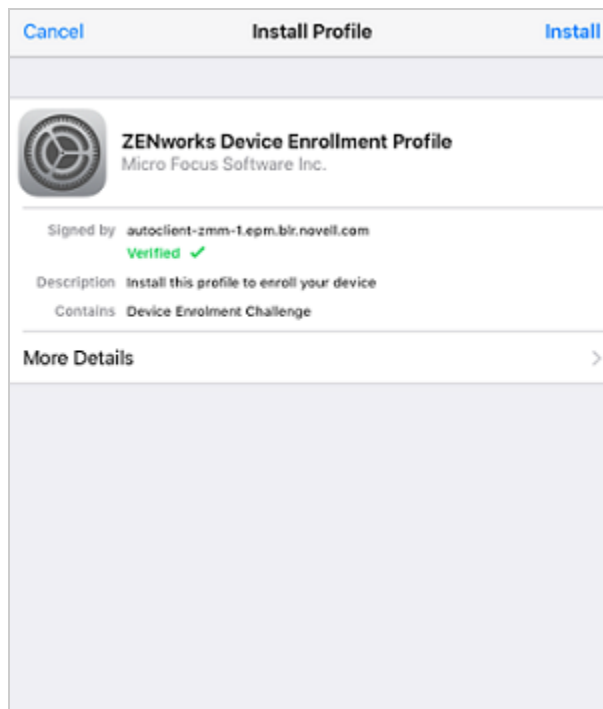
- 6 Tap **Install** and follow the prompts to install the certificate and return to the Enroll as Managed Device screen.

The ZENworks Trust Profile contains the certificate required for secure communication between the device and the ZENworks Primary Server.



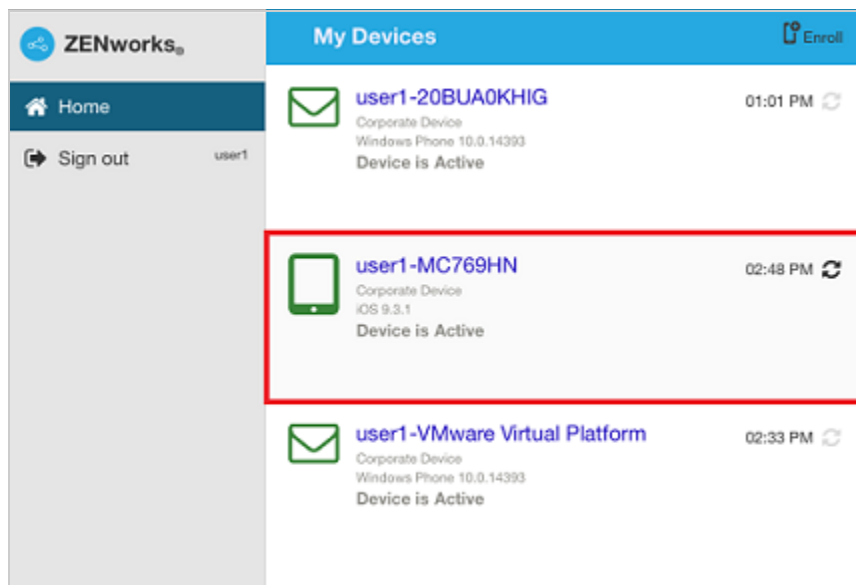
- 7 Tap **Download Profile** in the Enroll as Managed Device screen, to display the profile install screen. Tap **Install** and follow the prompts to install the profile and return to the Enroll as Managed Device screen.

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



- 8 Tap **Home** to return to the Home 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.

11.8 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.

11.8.1 Procedure

- 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.

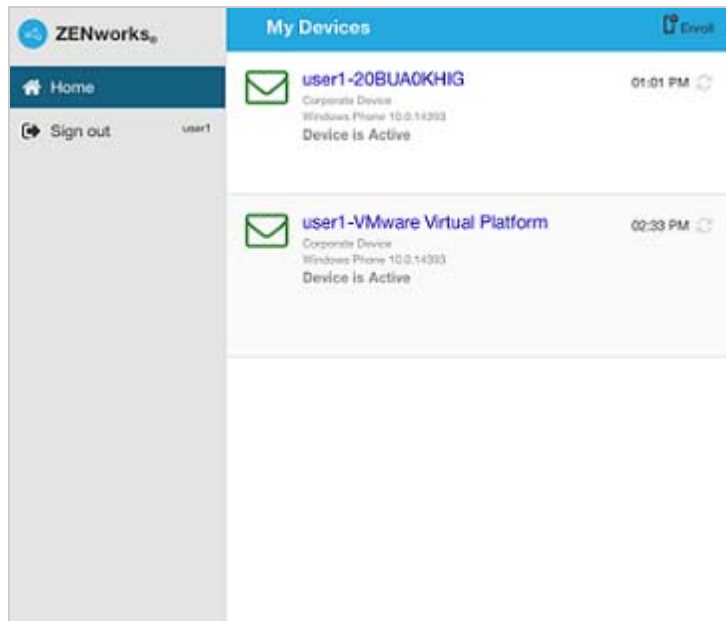
The login screen for the ZENworks User Portal is displayed. You use the ZENworks User Portal to enroll the device.



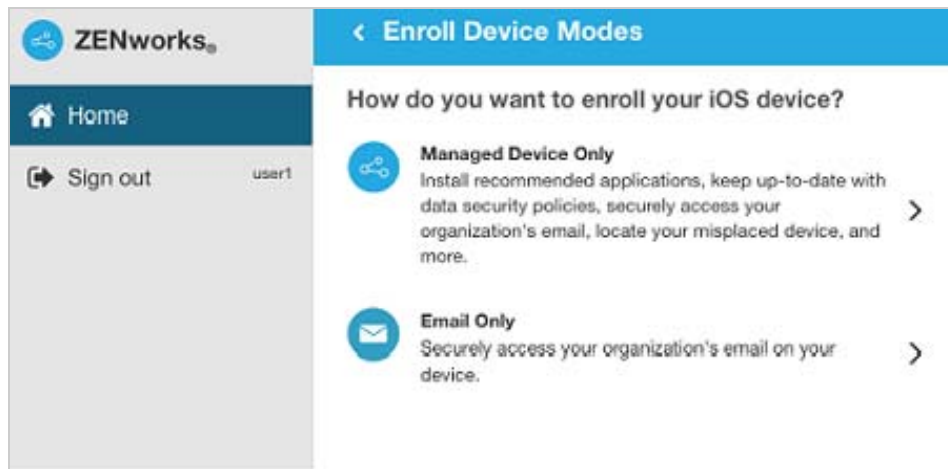
- 2 Enter the user's user name and password. If **Allow Simple Enrollment** option is selected for the user source to which the user belongs, then the registration domain need not be specified or else specify the registration domain. For information, see [Section 4.2, "Enabling a User Source for Mobile Device Enrollment,"](#) on page 16. 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.

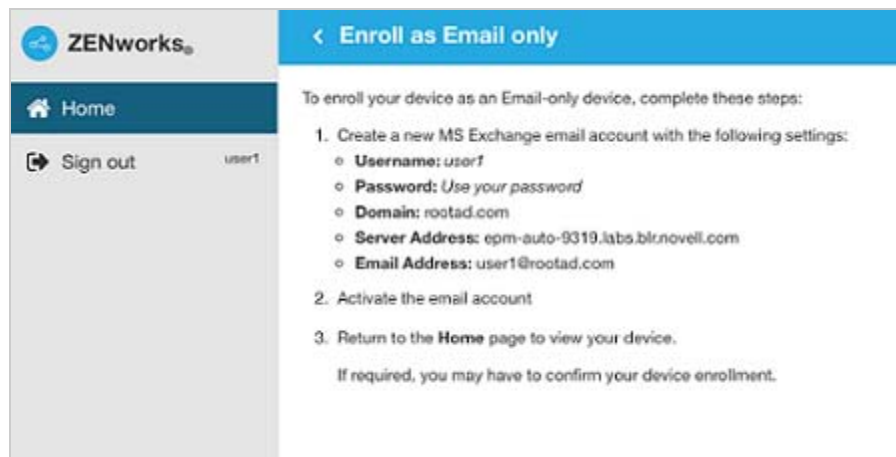
All devices associated with the user, are displayed in the ZENworks User Portal.



- 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 a Mobile Enrollment Policy" on page 71](#).



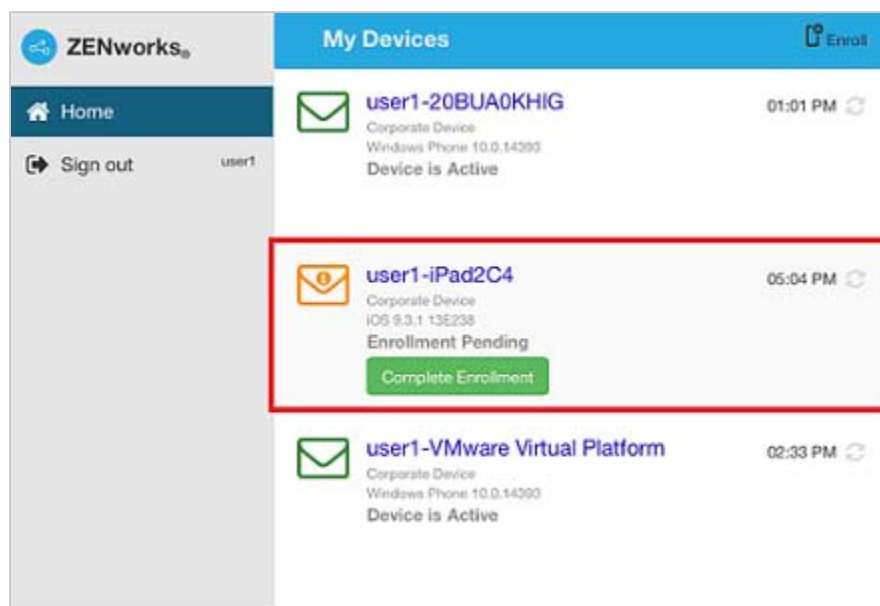
- 4 Tap **Email Only** to display the **Enroll as Email Only** screen. Use the displayed information to create an email account for the user.



- 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 > ActiveSync > Email Notifications**. Click the relevant email and edit its contents.

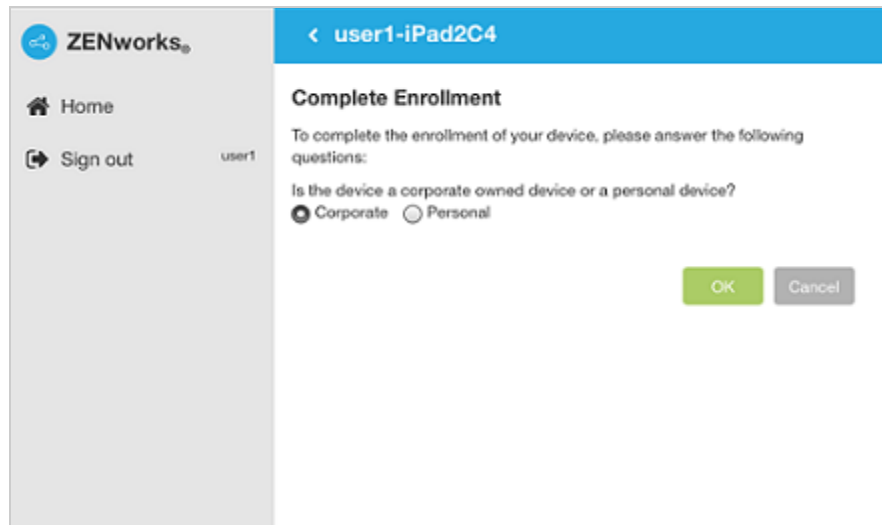
To complete the enrollment process, click the link to the ZENworks End User Portal provided in the email or visit the ZENworks End User Portal as described in [Step 1](#).

- 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.

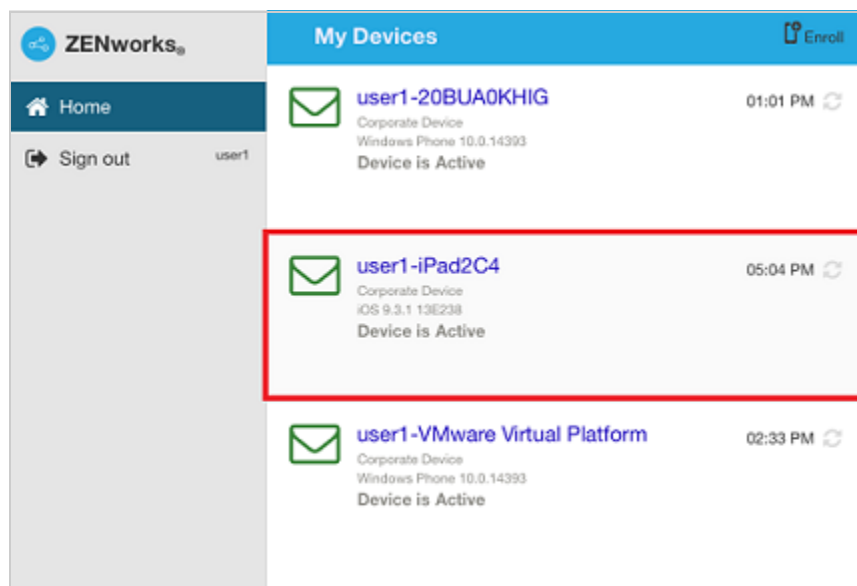


7 On the device, tap **Complete Enrollment**.

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 > ActiveSync > 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.

11.9 Allowing Manual Reconciliation by User

When users attempt to enroll their devices that 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 reconciliation. However, for certain devices auto reconciliation might fail due to the following reasons:

- ♦ ZENworks is unable to access the IMEI number of certain non-cellular Android devices.
- ♦ 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. This feature will enable the user to manually reconcile the device to an existing device object or to enroll as a new device. If **Allow manual reconciliation by user** option is not selected, then the device automatically enrolls 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.

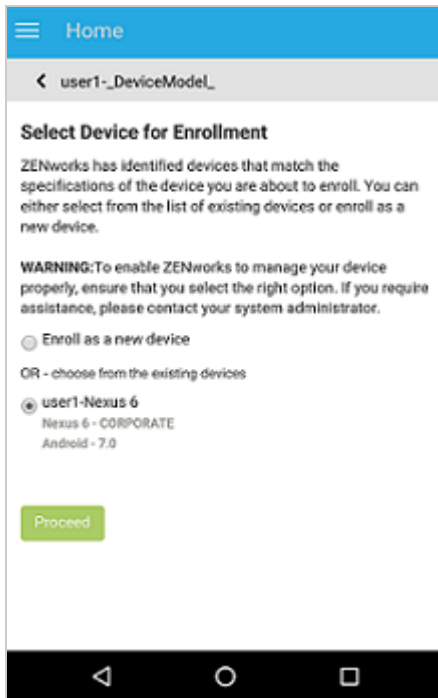
IMPORTANT: During manual reconciliation, it is important that the user selects the right option. If an incorrect option is selected, then ZENworks will be unable to manage the device properly.

Consider the following scenarios:

For Android Devices: A user has downloaded the ZENworks Agent app and completed the enrollment procedure as elaborated from [Step 1](#) to [Step 9](#) 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**.

☰ Home

◀ user1-iPhone5C2

Select Device for Enrollment

ZENworks has identified devices that match the specifications of the device you are about to enroll. You can either select from the list of existing devices or enroll as a new device.

WARNING: To enable ZENworks to manage your device properly, ensure that you select the right option. If you require assistance, please contact your system administrator.

Enroll as a new device

OR - choose from the existing devices

user1-MD298HN
MD298HN - CORPORATE
iOS - 9.2.1

Proceed










12 Managing a Device

The following scenarios show you how to use the device management features available in ZENworks Control Center.

- ◆ [Status Messages \(page 95\)](#)
- ◆ [Viewing Device Information \(page 96\)](#)
- ◆ [Organizing Devices into Dynamic Mobile Device Groups \(page 97\)](#)
- ◆ [Creating a Device Refresh and Removal Schedule \(page 97\)](#)
- ◆ [Refreshing a Device \(page 98\)](#)
- ◆ [Locking a Device \(page 99\)](#)
- ◆ [Unlocking a Device \(page 99\)](#)
- ◆ [Sending a Message to a Device \(page 100\)](#)
- ◆ [Unenrolling a Device \(page 100\)](#)

12.1 Status Messages

Status messages give a quick indication of the status of the device. To view these messages, 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 are as follows:

- ◆  - 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 bundle and policy status by clicking the device name and viewing the bundle or policy information on the device's Relationship page.

12.2 Viewing Device Information

After a device is enrolled to the ZENworks Management Zone, you can view the details of your enrolled device. 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, Network, Operating System, and Cellular:** Provides general information about the device, its hardware, operating system, network configuration, and cellular network information.
- ♦ **Last Connections:** Shows when the device was last connected with the ZENworks system. 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:** Displays information about the administrative owner and 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. This section also provides additional information about the department to which the device belongs, the site, and the location of the device. Click **Edit** to change the information in any of the fields.
- ♦ **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.
- ♦ **Locater Service Enabled (iOS only)** Indicates that the device allows certain apps to determine the users' approximate location.
- ♦ **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.

12.3 Organizing Devices into Dynamic Mobile Device Groups

Using ZENworks Control Center, you can manage devices by performing tasks directly on individual device objects. However, to optimize management of a large number of devices, ZENworks lets you organize devices into dynamic groups; you can then perform tasks on these groups to manage its devices. With a dynamic group, you define criteria that a device must meet to be a member of the group, and then devices that meet the criteria are automatically added.

- 1 In ZENworks Control Center, click the **Devices** tab.
- 2 Click the **Mobile Devices** folder.
- 3 Click **New > Dynamic Mobile Device Group** to launch the Create New Group Wizard.
- 4 On the Basic Information page, type a name for the new group in the **Group Name** field, then click **Next**.
- 5 On the Define Filter for Group Members page, select the group on which the filters are to be applied and then define the criteria that a device must meet to become a member of the group, then click **Next**.

For example: you can add a filter to specify that the mobile device platform should be Android and you can add another filter to specify the owner of the Android device.

- 6 On the Summary page, click **Finish** to create the group.

ZCC automatically refreshes the group members based on the settings configured in **Configuration > Device Management > Dynamic Group Refresh Schedule**. However, you can manually update the dynamic group by selecting the group and navigating to **Group > Actions > Update Group Membership**.

12.4 Creating a Device Refresh and Removal Schedule

The Device Refresh schedule lets you define how often a device contacts the ZENworks Server to update information such as policies and bundles. The Device Removal schedule lets you take an appropriate action on a device if it has not contacted the ZENworks Server within a certain number of days. 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 > 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: The removal schedule can be set on the Management Zone and Device Folder levels only. Also, 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.

12.4.1 Configuring Mobile Device Refresh Schedule

You can configure a manual refresh schedule or a timed refresh schedule.

NOTE: This schedule is not applicable for devices enrolled as ActiveSync Only (Email Only) devices.

Manual Refresh

If you want a device refreshed only when its user manually initiates the refresh, select **Manual Refresh**, then click **Apply**. Users can initiate a refresh by clicking the refresh icon located on the ZENworks Agent app on the device or by clicking the refresh icon in the ZENworks End User Portal.

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:

- 1 Fill in the following fields to define the schedule:

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.

- 2 Click **Apply** to save the settings.

12.4.2 Configuring Mobile Device Removal Schedule

The Mobile Device Lost Schedule panel lets you flag any devices that have not contacted a ZENworks Server within a specified period of time. You can specify the maximum number of days without contact based on which the device is flagged as a lost device.


12.5 Refreshing a 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.

IMPORTANT: During a device refresh, data from the ZENworks Server cache is read and delivered to the device. Therefore, if an action is assigned to a device, before executing the **Refresh Device** quick task, 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 2017 Management Zone Settings Reference](#).

For example: If a bundle is assigned to a device and the **Refresh Device** quick task is executed immediately, then the bundle might not deploy on the device. If you want to install the bundle immediately, you can instead execute the **Install Bundle** quick task.

12.5.1 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 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” on page 96](#).

12.6 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.

12.6.1 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 Android or iOS 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 the 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.

12.7 Unlocking a Device

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. For iOS devices, you only need to specify the reason for unlocking the device. This quick task is applicable for Android and iOS devices that are enrolled as fully managed devices in the management zone.

12.7.1 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 Android or iOS 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.

12.8 Sending a Message to a Device

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.

12.8.1 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 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.

12.9 Unenrolling a Device

You can unenroll devices through ZENworks Control Center. You can choose whether the unenrolled device is to be deleted from the ZENworks Management Zone or to be retired (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).

NOTE: The Selective Wipe action is not performed on devices enrolled as ActiveSync Only devices. For a fully managed iOS device, this option removes the fully managed profile along with the remotely configured ActiveSync profile. However, if the ActiveSync profile was manually configured, then this option retains it. For Android devices, the **Selective Wipe** option removes the app and retains the ActiveSync configuration.

Therefore, if you want to delete or retire a device that is enrolled as **iOS MDM + ActiveSync** or **Android App + ActiveSync**, then you need to perform a full wipe of the device.


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 iOS App Store App bundles) the apps are uninstalled based on the configured app settings (**Retain App on Unenrollment**).

12.9.1 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 > 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 Leave the quick task options set to the defaults and click **Start** to send the task to the device.
- 5 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.

- 6 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: If a device is in **Retired** or **Wipe Pending** status 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.

A Troubleshooting

The following sections provide solutions to the problems you might encounter while using the Mobile Management feature.

- ◆ “Status of a newly enrolled iOS device is displayed as **Pending Enrollment in ZENworks User Portal, until the browser is refreshed**” on page 103
- ◆ “Quick task to unlock device does not reset existing password on Android N devices” on page 104
- ◆ “If the time on the ZENworks Server lags behind the actual enrollment time of a mobile device, then any quick task that is sent to this device within this time period is not processed and its status will remain as **Initiated**” on page 104
- ◆ “Purchased license count is not updated, if sync to retrieve latest VPP apps is initiated immediately after purchasing an app” on page 104
- ◆ “Max Grace Period and Max Inactivity Timeout restriction settings might display incorrect values on the device” on page 104
- ◆ “Mobile Security policies might not apply automatically on a few Android devices” on page 105
- ◆ “Windows mobile devices do not accept alphanumeric or complex characters even if they are enabled in the assigned Mobile Security policy” on page 105
- ◆ “Simple passwords are accepted by a few Android devices even if the setting is disabled in the assigned Mobile Security policy” on page 105
- ◆ “If the time on an Android device lags behind the time on the ZENworks Server, then device enrollment will be unsuccessful” on page 105
- ◆ “Email accounts on some devices might stop functioning and an authentication error is displayed” on page 105
- ◆ “While configuring access controls to secure an MDM Server, Administration access is denied for all” on page 106
- ◆ “APNs certificate import fails” on page 106
- ◆ “After configuring access controls to secure an MDM Server, an IP address of a device that is denied access is still able to contact the ZENworks Server” on page 106
- ◆ “Push notifications does not behave as expected on a newly added MDM Server.” on page 106
- ◆ “Push notifications to enrolled devices will not work as expected, if the APNs certificate has expired and a new certificate is imported” on page 107

Status of a newly enrolled iOS device is displayed as Pending Enrollment in ZENworks User Portal, until the browser is refreshed

Explanation: The status of a newly enrolled iOS device is displayed as **Pending Enrollment** in the ZENworks User Portal even though the device object has moved from the **Pending Enrollment** folder to **Devices > Mobile Devices** folder in ZCC. Tapping the Home icon or the Sync Now icon in the ZENworks User Portal does not update the status of the enrolled device.

Action: Refresh the ZENworks User Portal browser to view the updated status of the device as **Active**.

Quick task to unlock device does not reset existing password on Android N devices

Explanation: If the Unlock Device quick task is performed on an Android N device that already has a password set, the password does not reset with the new password configured in the quick task. However, if a password is not set on the device, then the Unlock Device quick task will set the new password on the device.

Action: None.

If the time on the ZENworks Server lags behind the actual enrollment time of a mobile device, then any quick task that is sent to this device within this time period is not processed and its status will remain as **Initiated**

Explanation: When a mobile device is enrolled to the zone and the ZENworks Server time lags behind the enrollment time of this device, then any quick task that is sent during this time period, is not processed and the status of the quick task remains as **Initiated**.

Action: You need to wait until the ZENworks Server time is equal to or exceeds the device enrollment time, before sending a push notification, such as quick tasks, to the device.

Purchased license count is not updated, if sync to retrieve latest VPP apps is initiated immediately after purchasing an app

Explanation: If a sync between the ZENworks Server and the Apple Server is initiated immediately after purchasing an app using the Apple VPP account credentials, then the purchased license count might not be updated with these latest app purchases. Subsequently, bundle assignments might fail.

Action: Ensure that you verify the purchased license count for that specific app in the Apple VPP License Summary page, before assigning that app to a device or a user. Wait for the next sync or re-initiate the sync to update the purchased license count.

Max Grace Period and Max Inactivity Timeout restriction settings might display incorrect values on the device

Explanation: The **display the passcode screen on unlock** (max grace period) and **maximum inactivity timeout** values specified in the mobile security policy that is assigned to an iOS device, might display incorrect values when viewed on the device. However, this does not affect the behavior of the device lock feature as the values specified while defining the mobile security policy in ZENworks Control Center (ZCC) are applied.

Action: None

Mobile Security policies might not apply automatically on a few Android devices

Explanation: Mobile Security policies assigned to devices might not apply automatically on a few Android devices.

Action: Initiate a Refresh action on these devices.

Windows mobile devices do not accept alphanumeric or complex characters even if they are enabled in the assigned Mobile Security policy

Explanation: When a Mobile Security policy, which has alphanumeric or complex characters enabled as a part of the Password settings, is assigned to a Windows device, the device keeps prompting for Personal Identification Number (PIN) and does not accept alphanumeric or complex characters.

Action: None. This is a Microsoft limitation.

Simple passwords are accepted by a few Android devices even if the setting is disabled in the assigned Mobile Security policy

Explanation: When a Mobile Security policy, in which the simple password setting is disabled, is assigned to Android devices, a few of the Android devices might still accept a simple password.

Action: None.

If the time on an Android device lags behind the time on the ZENworks Server, then device enrollment will be unsuccessful

Explanation: The time on an Android device lags behind the time on the ZENworks Server. During device enrollment, when the user logs into the ZENworks mobile app, the enrollment process does not advance to the next stage.

Action: Ensure that the time on the device and the ZENworks Server is the same and then try re-enrolling the device.

Email accounts on some devices might stop functioning and an authentication error is displayed

Explanation: On a few devices, the configured ActiveSync accounts might stop functioning and an **Authentication Error** notification is displayed. In some cases, this notification recurs even if the user has specified the account credentials and in some cases the device does not respond on clicking this notification.

Action: Delete and re-create the email account.

While configuring access controls to secure an MDM Server, Administration access is denied for all

Explanation: While configuring access controls to secure an MDM Server, Administration access is denied for all and ZCC remains inaccessible except from the server in which the access was allowed or denied.

Action: Change the configuration by accessing ZCC from the MDM Server in which the access was denied. You can access ZCC in the following ways:

- ◆ Enter the Server IP.
- ◆ Enter `https://localhost` (applicable for IPv4 addresses only)
- ◆ Enter the loopback address.

If you are still unable to access ZCC, then delete the configuration file `access-filters.json` from the directory available at `%ZENWORKS_HOME%/share/tomcat/conf`. Restart the MDM server. Administration access will be allowed for all. You need to navigate back to ZCC and re-configure the access controls.

APNs certificate import fails

Explanation: While configuring the Apple Push Notification service in ZENworks, APNs certificate import fails.

Action: Check the `ZCC.log` or the `service-messages.log` of the MDM Servers. If the failure is due some issue with the APNs Keystore, try restarting the server and then import the certificate. If `CertificateNotYetValidException` is displayed as the reason for failure, then this indicates that the MDM Server time is ahead of the certificate creation time. You need to wait for a while and then try importing the certificate.

After configuring access controls to secure an MDM Server, an IP address of a device that is denied access is still able to contact the ZENworks Server

Explanation: While securing an MDM Server, a specific IP address of a device is denied access to the server. However, this device is still able to contact the MDM Server.

Action: Enable the Tomcat valve logging to check the logs. For more information, see [Tomcat Valve Logging](#) in *ZENworks Configuration Management - Best Practices Guide*.

Also, check whether the device is communicating with the ZENworks Server using a proxy server. If so, you need to deny access to the IP address of the proxy server, if other devices are not using this proxy server.

Push notifications does not behave as expected on a newly added MDM Server.

Source: ZENworks Mobile Management

Explanation: An MDM Server that contains the APNs keystore is not connected to the network. Another MDM Server is added in the same zone, which tries to pull the APNs keystore from the existing MDM Server. However, since the existing MDM Server is not connected to the network, the APNs keystore fails to replicate in the new MDM Server, due to which this server does not function appropriately.

Action: You need to ensure that the MDM Server that contains the APNs keystore, is online at all times. After you ensure that the existing MDM Server is online, remove the MDM role from the newly added MDM Server and re-assign it to the same server.

Push notifications to enrolled devices will not work as expected, if the APNs certificate has expired and a new certificate is imported

Source: ZENworks Mobile Management

Explanation: When the existing APNs certificate has expired and you create a new certificate in the Apple Push Certificates portal and import it to ZENworks, then the push notifications to mobile devices, which were enrolled using the earlier certificate, will not work as expected.

Action: Re-enroll the devices. As a best practice, if the APNs certificate has expired, it is recommended that you **Renew** the certificate in the Apple Push Certificates portal instead of creating a new certificate. For details, see [Renewing an Expired APNs Certificate](#).

