

opentext™

ZENworks Mac MDM Reference

Legal Notices

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

© Copyright 2008 - 2024 Open Text

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

Contents

About This Guide	5
Part I Getting Started	7
1 Supported Devices for Mac MDM	9
2 Overview	11
3 Creating Registration Rules	13
Part II Enrolling Mac MDM Devices	15
4 Enrolling Mac MDM using ADE/DEP	17
5 Enrolling Mac MDM using the OTA Profile	19
Part III Managing Mac Devices	27
6 Viewing Device Information	29
7 Viewing Device Status	31
8 Provisioning Applications	33
8.1 Distributing macOS MDM Bundles	33
8.2 Distributing VPP Apps	34
8.3 Linking ZENworks to the Apple VPP Account	34
8.4 Creating VPP Bundles	34
8.5 Assigning VPP Bundles	34
9 Refreshing a Device	37
Initiating a Scheduled Refresh	37
Timed Refresh	38
Manually Triggered Refresh	38
Refresh Device Quick Task	38
10 Account Configuration	39
11 Managing the DEP Settings	41
General and Skip Setup Item Settings	41

General	41
Skip Setup Items	43
Skip Setup Items - Mac	43
12 Device Removal and Retirement	45
Deleting Devices from Your ZENworks System	45
Retiring or Unretiring Devices	45
Unregister Mac MDM Device	46
13 Unenrolling Mac MDM Devices using Quick Task	47
A Troubleshooting Scenarios	49
A.1 Devices respond as NotNow when a Mac device is locked	49
A.2 A new CA is activated when a device is in the lost state	49

About This Guide

This *ZENworks Mac MDM* guide includes information about configuration and use the Mac MDM feature in ZENworks. The information in this guide is organized as follows:

- ♦ [Part I, “Getting Started,” on page 7](#)
- ♦ [Part II, “Enrolling Mac MDM Devices,” on page 15](#)
- ♦ [Part III, “Managing Mac Devices,” on page 27](#)
- ♦ [Appendix A, “Troubleshooting Scenarios,” on page 49](#)

Audience

This guide is intended for ZENworks administrators.

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 Configuration Management 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 [ZENworks documentation Web site](#).

Getting Started

The following sections provide information on how to get started with the Mac MDM in ZENworks Configuration Management. You should already have installed your ZENworks system. If not, see the [ZENworks Server Installation](#).

- ◆ Chapter 1, “Supported Devices for Mac MDM,” on page 9
- ◆ Chapter 2, “Overview,” on page 11
- ◆ Chapter 3, “Creating Registration Rules,” on page 13

1 Supported Devices for Mac MDM

Mac MDM is supported on the following devices:

Device	Functionality
Macintosh 11.x (Big Sur)	◆ Enrollment through the Apple Device Enrollment Program/OTA
Macintosh 12.x (Monterey)	◆ Installation of Configuration Profile
Macintosh 13.x (Ventura)	◆ Device Management: Refresh Device
Macintosh 14.x (Sonoma)	◆ Distribute and manage apps purchased using the Apple Volume Purchase Program (VPP)
	◆ Retiring and Unretiring of Devices
	◆ Deleting Devices
	◆ Unenrolling Mac MDM Device via Quick Task

2 Overview

Limited Support for Mac MDM

In the current ZENworks release, Mac MDM support is limited. The features which are documented should work as expected, but there may be issues with undocumented aspects of device management. For some issues, a fix may only be available in a later release.

Mac MDM provides a management solution to help IT administrators to manage devices, without compromising users' privacy on their devices. The ZENworks Mac MDM document includes information that is required to configure and use the Mac MDM feature in ZENworks. By leveraging the features of ZENworks, you can perform multiple management operations on Mac devices:

- ◆ **Enroll (register) devices** to your ZENworks Management Zone. Users can enroll their devices as:
 - ◆ **Managed:** Management of a Mac device is enabled using the ZENworks Agent and Mac MDM that is installed on the device. When a Mac MDM device is enrolled via DEP or OTA, those devices are managed by ZENworks.
- ◆ **Utilize Apple Device Enrollment Program (DEP)** to streamline deployment of multiple corporate owned Mac MDM devices.
- ◆ **Distribute Configuration Profile** to Managed Mac devices to manage certain features on the device such as access to VPN and to run enterprise apps.

NOTE: The Provisioning Profile type is not supported when creating the macOS MDM bundle.

- ◆ **Distributing VPP Apps:** Distribute and manage apps purchased using the Apple Volume Purchase Program (VPP).
- ◆ **Unenrolling Mac MDM Device via Quick Task:** You can initiate the **Unenroll MDM Device Now** quick task to unenroll devices from ZENworks that you no longer want to manage.
- ◆ **Retiring and Unretiring Devices:** You can now retire or unretire Mac MDM devices. If you retire a workstation device, the selected device is retired from the ZENworks zone. If you unretire the device in the future, its assignments are restored.
- ◆ **Registration Rules:** A registration rule is a set of predefined criteria (for example, operating system type, CPU, or IP address) that you define. Using Registration Rules, you can manage a large number of devices and automatically add them to the correct folders and groups during registration.

3 Creating Registration Rules

When you enroll a Mac MDM device via DEP or OTA, the device is registered in your Management Zone and becomes a managed device.

By default, a device's hostname is used as its ZENworks name, it is added to the /Servers or /Workstations folder, and it is not given membership in any groups. You can manually move devices to other folders and add them to groups, but this can be a burdensome task if you have a large number of devices or if you are consistently adding new devices. The best way to manage a large number of devices is to have them automatically added to the correct folders and groups during registration.

To add devices to folders and groups during registration, you can use registration rules. Registration rules let you assign folder and group memberships to a device.

NOTE: The Registration Keys feature does not apply to Mac MDM devices.

For more information, see [Registration Rules](#).



Enrolling Mac MDM Devices

You can enroll Mac MDM devices to a zone either via ADE/DEP or OTA. Any Mac device that already exists in zone as a ZENworks Agent only device, can be enrolled again via MDM and it reconciles to the existing device present in the zone.

NOTE:

- ◆ To enroll any Mac MDM device via DEP which is already enrolled as ZENworks Agent then the device has to be reset.
 - ◆ The Mac MDM devices can be enrolled using either the Apple Device Enrollment Program (DEP) or Over The Air (OTA). Do NOT use both DEP and OTA enrollment methods on the same device.
-

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

- ◆ [Chapter 4, “Enrolling Mac MDM using ADE/DEP,” on page 17](#)
- ◆ [Chapter 5, “Enrolling Mac MDM using the OTA Profile,” on page 19](#)

4 Enrolling Mac MDM using ADE/DEP

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

Prerequisites:

Before enrolling a Mac device to ZENworks, you need to ensure that the prerequisites are met in the following order:

Task	Details
In the Apple Business Manager Portal, add an MDM Server	For more information, refer to the Apple documentation
MDM Servers and APNs	For more information, see MDM Servers and APNs Configuration
Configure the ZENworks MDM Server	For more information, see Configuring an MDM Server
Enable Push Notifications	For more information, see Enabling Push Notifications
Configure a DEP Server in ZENworks. The workflow associated with enrolling DEP devices are as follows: <ul style="list-style-type: none">◆ Linking ZENworks to the Apple Deployment Programs Account◆ Assigning Devices◆ Syncing Devices◆ Viewing DEP Devices	For more information, see Linking ZENworks to the Apple Deployment Programs Account, Assigning Devices, Syncing Devices, Viewing DEP Devices
Setup DEP Attributes - including Skip Panes / Mac Accounts	For more information, see “General and Skip Setup Item Settings” on page 41.
Configure the Administrator and Primary User Accounts	For more information, see “Account Configuration” on page 39.

NOTE: Account configuration is required only for ADE or DEP and not required for OTA.

For information on enrolling any existing Mac OS device as DEP, see the following Apple documentation sections:

- ◆ [Apple Configurator User Guide](#)
- ◆ [Apple Configurator for Mac](#)

Procedure:

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

Turn on the device and follow the setup prompts to enroll the device after powering on the device for the first time or after device reset. Once the wizard is finished, the Mac device will be enrolled into ZENworks via MDM.

If the User account is configured (Admin or local user account) then those accounts will be created on the Mac device.

After the device enrolls, you can view the Deployment Status of the device in ZCC, which should have changed from Discovered to Managed. You can view this status on **Device > Discovered > Apple DEP Devices**. For more information, see [Chapter 6, “Viewing Device Information,” on page 29](#). The enrolled device object is also created within the Workstations folder (**Devices > Workstations**).

For more information, see [Enrolling a DEP Device](#).

5 Enrolling Mac MDM using the OTA Profile

You can now securely enroll non-DEP devices into ZENworks using the OTA (over-the-air) Profile which deploys the enrollment profile without a reset of the device.

- ◆ Devices that already have ZENAgent deployed, can onboard MDM without having to reset the device and go through ADE enrollment.
- ◆ Devices in use can enroll in ZENworks without having to reset the device and go through ADE enrollment.

NOTE: To enroll Mac devices as MDM using OTA, you need to have Mac administrator permissions.

Before enrolling a macOS device, you need to ensure that the following prerequisites are met:

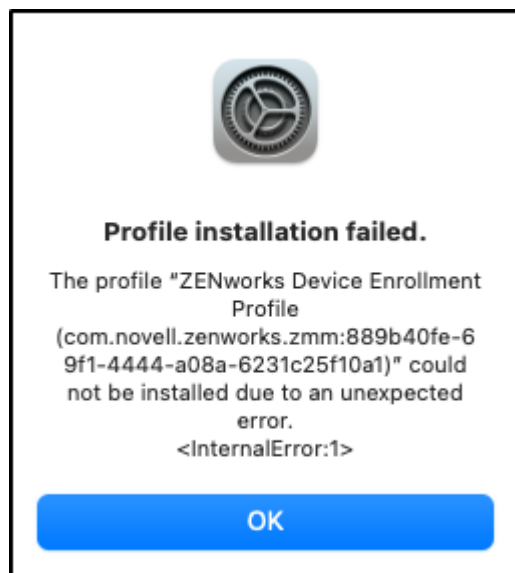
Prerequisites:

Task	Details
Enable Push Notifications	For more information, see Enabling Push Notifications
Configure MDM Servers and APNs	For more information, see MDM Servers and APNs Configuration

IMPORTANT:

- ◆ To enroll a Mac device as MDM via OTA Profile in ZENworks, the device should be pre-approved in ZENworks either with its Serial Number or Mac Address or both for authenticating the device. For more information, see [Adding Pre-approved Devices](#).
- ◆ If the device is not pre-approved, the following error will be displayed on the device.

Figure 5-1



- ◆ Pre-approval check will fail in case if the value is specified in the DNS Name device attribute and in the Device Matching Setting if both DNS Name and Enable Differentiation are selected.
-

- ◆ As part of the MDM Enrollment Profile, the consent text can be set which is displayed to the user on the Mac device during profile installation. You can modify the default consent text in `com.novell.zenworks.apple.plist.profileinfo.consent.text`

The file is available in the following location:

On Windows Server:

```
C:/Program Files/microfocus/zenworks/resources/properties/com/novell/zenworks/apple/plist/profileinfo/ios_profile_<Locale>.properties
```

On Linux Server:

```
/opt/microfocus/zenworks/resources/properties/com/novell/zenworks/apple/plist/profileinfo/ios_profile_<Locale>.properties
```

Restart the `microfocus-zenclient-mgmt` service after updating the consent text.

- ◆ Once the OTA profile enrolled, the following message is displayed:

“This Mac is supervised and managed by: IT Organization”

If you want to customize the organization before enrolling through OTA Profile, you should add a system variable in **Configuration > Device Management > System Variables** screen with value as “organization.name” (case-sensitive).

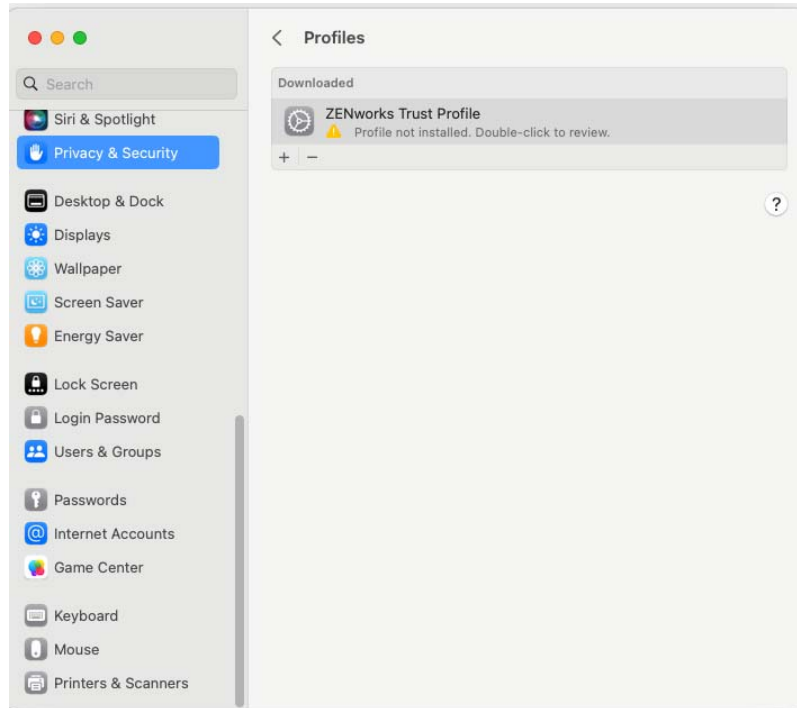
NOTE:

- ◆ The macOS devices running Macintosh 11.x (Big Sur) or later versions can be enrolled as supervised devices.
 - ◆ If the DNS attribute is selected to uniquely identify a pre-approved device, the Mac enrollment using the OTA profile might fail.
-

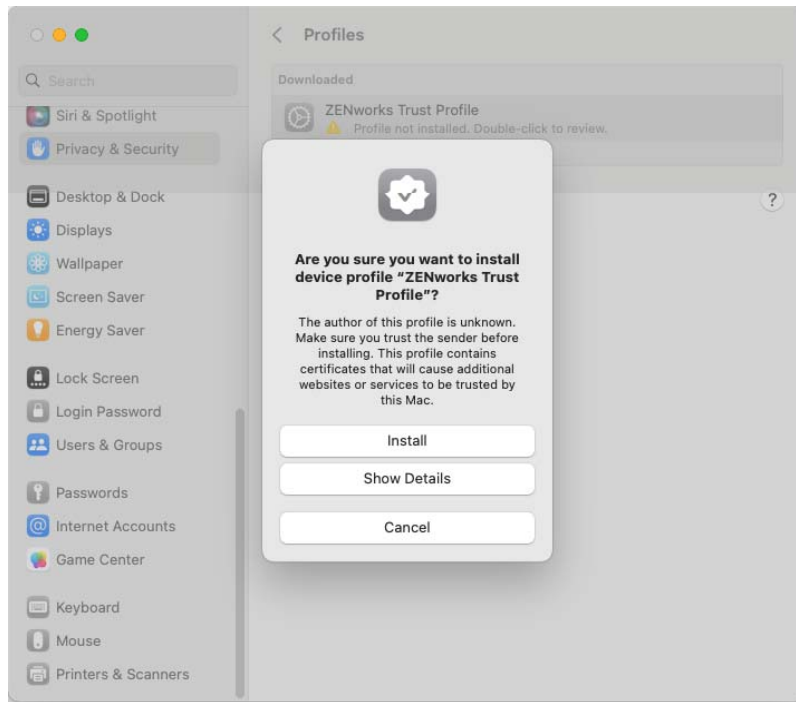
Procedure:

- 1 In the Safari browser on a Mac device, specify the URL to download the ZENworks Trust Profile. The URL should be specified in the following format, for example: `https://<ZENworks_server_address>/endpoint/apple/trust`
`ZENworks_server_address` is the DNS name or IP address of the ZENworks MDM Server.
- 2 Navigate to the **System Settings** menu on the device and select **Privacy & Security > Profiles**.
- 3 Click **ZENworks Trust Profile**.

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



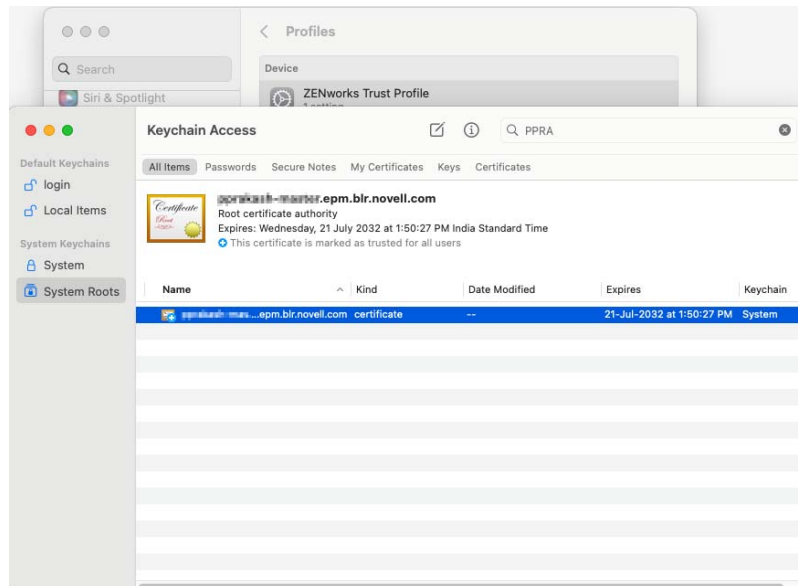
- 4 Double-click the profile and click **Install...**
- 5 Install the profile.



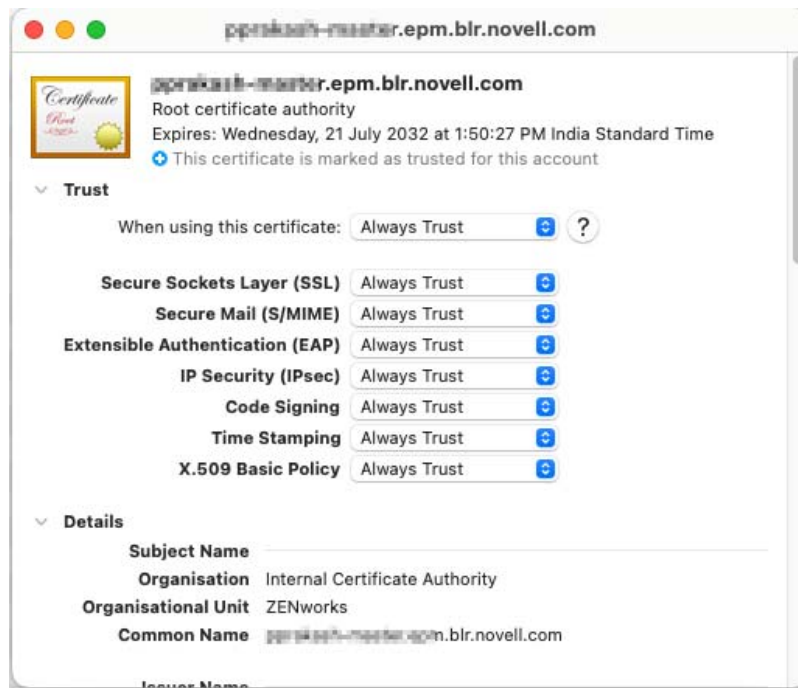
6 Specify the administrator password and click **OK**.

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

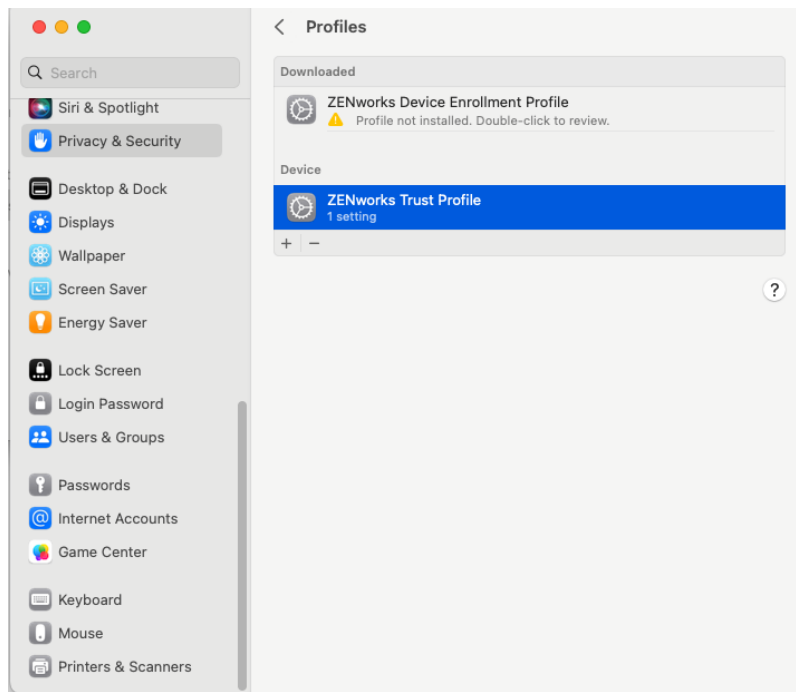
- ◆ Navigate to **Keychain Access > System Roots > Certificates**.
- ◆ Search for the ZENworks CA certificate and double-click the certificate.



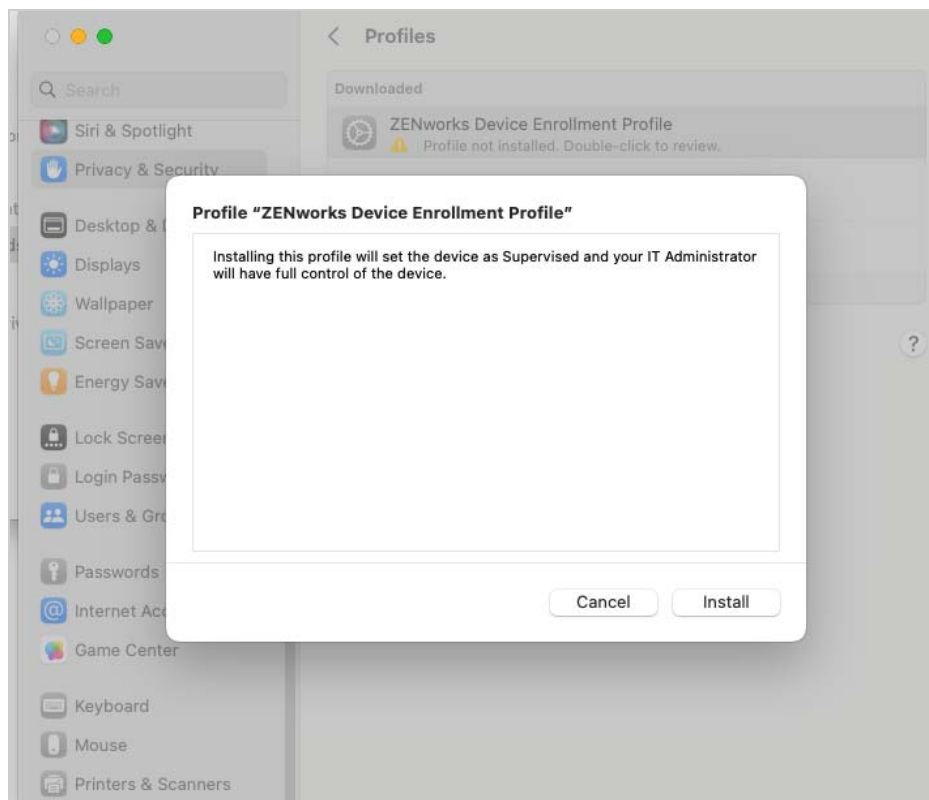
- ◆ Expand the **Trust** details.
- ◆ Select **Always Trust** from the **Secure Sockets Layer (SSL)** drop-down list.



- ◆ Click **Continue**.
 - ◆ Specify the administrator password and click **Update Settings**.
- 8 Next, in the Safari browser on a MAC device, enter `https://<ZENworks_server_address>/endpoint/apple/userlessOTAEnroll`, where `ZENworks_server_address` is the DNS name or IP address of the ZENworks MDM Server. The ZENworks Enrollment Profile will be downloaded.
 - 9 Navigate to **System Settings > Privacy & Security > Profiles**.
 - 10 Double-click **ZENworks Device Enrollment Profile**. The ZENworks Device Enrollment Profile contains the MDM profile required for ZENworks to manage the device.



- 11 Click **Install...** and follow the prompts to install the profile. Once the profile is successfully installed, the device will be supervised and managed by ZENworks.



12 Specify the administrator password and click **Enrol**.





Managing Mac Devices

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

- ♦ [Chapter 6, “Viewing Device Information,” on page 29](#)
- ♦ [Chapter 7, “Viewing Device Status,” on page 31](#)
- ♦ [Chapter 8, “Provisioning Applications,” on page 33](#)
- ♦ [Chapter 9, “Refreshing a Device,” on page 37](#)
- ♦ [Chapter 10, “Account Configuration,” on page 39](#)
- ♦ [Chapter 11, “Managing the DEP Settings,” on page 41](#)
- ♦ [Chapter 12, “Device Removal and Retirement,” on page 45](#)
- ♦ [Chapter 13, “Unenrolling Mac MDM Devices using Quick Task,” on page 47](#)

6 Viewing Device Information

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

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





The Device Information page displays the following details:

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

The various enrollment modes are as follows:


- ◆ **macOS MDM + ZENAgent:** Indicates that as a part of full management of a Mac device, the device is enrolled via the MDM, and the ZENAgent is installed on the Mac device. After the device reconciles the enrollment mode is displayed as macOS MDM + ZENAgent.
- ◆ **macOS MDM:** Indicates that as a part of full management of a Mac device, the device is enrolled via MDM.
- ◆ **Network:** Displays network information such as the Wi-Fi MAC address and the IP address.
- ◆ **Operating System:** Displays information on the Operating System installed on the device.
- ◆ **Last Connections:** Displays the last time the ZENworks Agent or macOS MDM contacted the ZENworks Server. If the device is not enrolled as macOS MDM, this field displays when the Agent last contacted with the ZENworks Server.
- ◆ **Administration:** This section displays the following information. Click **Edit** to change the information in any of the fields.
 - ◆ **Administrative Owner:** Indicates the administrator of the device.
 - ◆ **Test Device:** Indicates if the device is a test device. If the device is not a test device, you can click **Set** to set the device as a test device. If the device is a test device, you can click **Reset** to reset the device to a non-test device.
 - ◆ **Enrolled MDM Server:** Indicates the MDM Server to which the device is enrolled.
 - ◆ **Department:** Indicates the department to which the device belongs.
 - ◆ **Site:** Indicates the site to which the department belongs.
 - ◆ **Location:** Indicates the location of the department.
- ◆ **ZENworks Agent Details:**
 - ◆ **Last Contact:** Displays the last time the agent contacted the ZENworks Server.
 - ◆ **Last Full Refresh:** Displays the last time that the device refreshed its information (bundles, policies, configuration information, registration information, and so forth). A refresh can be manually initiated by the device's user, manually initiated by an administrator using the


Refresh Device Quick Task or scheduled. The refresh schedule is determined by the Device Refresh Schedule configuration setting available on devices, device folders, and the Management Zone.


- ◆ **Reboot Pending Since:** Displays the date and time since when the device reboot is pending. This field will be displayed only when you have postponed the device reboot after applying a patch, update, or any other action that requires a device reboot. The value will be unavailable if the server reboot is already completed, if the server is at ZENworks 2020 Update 2 or lower versions, or if the server OS is Linux or Macintosh.
- ◆ **Network Location:** Displays the network location name to which the device was connected. Along with the name, time and date of connection will also be displayed. The value will be unavailable if the server is at ZENworks 2020 Update 2 or lower versions.
- ◆ **Network Environments:** Displays the name of the network environment.
- ◆ **ZENworks Agent Version:** Displays the version of the ZENworks Agent software on the device. Click View to display a list of the ZENworks Agent modules that are installed on the device along with their version numbers.
- ◆ **ZENworks Agent Last Contact:** Displays the last time the ZENworks Agent contacted the ZENworks Server.
- ◆ **ZENworks Agent Status:** Monitors and displays the status of the ZENworks Updater Service (ZeUS) and the ZENworks Agent. It might take a while for the status to be displayed.
 - ◆  Indicates that both ZeUS and ZENworks Agent are reachable.
 - ◆  Indicates that ZeUS is up but the ZENworks Agent is not reachable.
 - ◆  Indicates that ZeUS is not reachable.
 - ◆  Unknown; indicates that status determination is in progress


7 Viewing Device Status


The following icons give a quick indication of the status of the device. To view the status, click **Devices** on the left navigation pane of ZENworks Control Center and click **Workstations**. The status icons that appear beside a device indicate the following:


 - No warning or error messages;


 - Warning messages;


 - Error messages;

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

 - Warning messages, bundle or policy assignment has failed.

 - Error messages; bundle or policy assignment has failed.

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

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

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

8

Provisioning Applications

8.1 Distributing macOS MDM Bundles

You can deploy a Configuration Profile using the macOS MDM bundle.

Prerequisite

To upload an Configuration Profile or command, an XML file with the configuration settings should be exported from Apple Configurator. For more information on creating and importing profiles or commands, refer to the Apple Configurator documentation or [Cool Solution on the Mac MDM Profiles and Commands](#).

Procedure

- 1 In ZENworks Control Center, click the **Bundles** tab.
- 2 In the **Bundle** list, click **New**, then click **Bundle** to display the Select Bundle Type page.
- 3 Select **macOS MDM Bundle**, then click **Next** to display the Select Bundle Category page.
- 4 Select the **macOS Profile** bundle category.
- 5 Click **Next** to display the Define Details page, then fill in the fields:
- 6 On the Define Details page, specify a name for the bundle, select the folder in which to place the bundle, then click **Next**.
- 7 On the Select Profile Type page, select the following **Configuration Profile** to deploy to macOS MDM device:
 - ♦ **Configuration Profile:** Select a Configuration Profile consisting of payloads that will enable you to deploy configuration settings and commands.

NOTE: The Provisioning Profile type is not supported when creating the macOS MDM bundle.

- 8 Based on the option selected in the previous page, browse and upload a configuration profile or command on the Import Configuration Profile/Command page.

IMPORTANT: Currently, you can configure profiles and commands only for device channels and not for user channels.

- 9 Review the information, making any changes to the bundle settings by using the **Back** button as necessary.
- 10 Click **Finish** to create the bundle as configured per settings.

For information on the viewing the bundle information, see [Viewing the Bundle Information](#) .

When you create a bundle, the bundle is listed on the Bundles page of the ZENworks Control Center. For more information on the created bundle, review the following sections:

- ♦ [Understanding the Bundle Page](#)
- ♦ [Bundle Summary Page](#)

After the macOS bundle is created, bundle is assigned to devices, device groups, or device folders and the summary of bundle assignment and distribution is displayed on the Bundle Dashboard page. You can continue to assign this bundle to an Mac device. For more information, see [Assigning VPP Bundles](#) and [Distributing VPP Apps](#).

NOTE: For macOS MDM bundle, the user assignment is not supported.

After enforcing the profile on the device, on your Mac device, go to **System Settings > Privacy & Security > Profiles**.

The profile you have assigned from ZENworks will be available. You can double-click the profile to view the restrictions and configurations that are applied to the device.

8.2 Distributing VPP Apps

The Apple Volume Purchase Program (VPP) allows organizations to purchase apps in volume to distribute to their managed devices. Using ZENworks, administrators can easily distribute, reclaim, and reassign apps using the existing Bundles workflow. Your organization might possess multiple VPP accounts. ZENworks can distribute licenses from multiple such VPP accounts to Apple devices. For more information, see [Distributing VPP Apps](#).

8.3 Linking ZENworks to the Apple VPP Account

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

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

While creating a subscription, you can also define a schedule based on which bundles for these purchased apps will be automatically created by ZENworks. For more information, see [Linking ZENworks to the Apple VPP Account](#)

8.4 Creating VPP Bundles

ZENworks creates VPP bundles based on the Schedule Type selected while creating the Apple VPP Subscription. For more information, see [Creating VPP Bundles](#).

8.5 Assigning VPP Bundles

You can distribute apps purchased through the Apple Volume Purchase Program (VPP), by assigning VPP bundles to the devices that have enrolled their devices to the zone. For more information, see [Assigning VPP Bundles](#).

NOTE: For the macOS MDM bundle, the user assignment is not supported.

For additional information, see the following sections:

- ◆ [Updating VPP License Summary](#)
- ◆ [Renewing a VPP Token](#)
- ◆ [Revoking App Licenses](#)
- ◆ [Deleting VPP Subscription](#)

9 Refreshing a Device

A device refresh can be initiated in the following ways:

- ◆ **Scheduled Refresh**
- ◆ **Manually Triggered Refresh**
 - ◆ Quick Task Refresh initiated by the Administrator.
- ◆ [“Initiating a Scheduled Refresh” on page 37](#)
- ◆ [“Manually Triggered Refresh” on page 38](#)

Initiating a Scheduled Refresh

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

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

This schedule can be defined at three levels:

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

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

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

NOTE: ◆ If you are configuring this setting at a Device Folder or at Device level, then you need to click [Override](#) or else the default setting will apply.

- ◆ The macOS MDM devices are excluded from the Server/Workstation Removal Schedule.
 - ◆ Manual Refresh and Partial Refresh does not update the bundle information.
 - ◆ The full refresh schedule defines how often you want a device to update all of its information (bundle, registration) from the ZENworks Server.
 - ◆ Full Refresh schedule¹ for macOS MDM bundle
-

Timed Refresh

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

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

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

Manually Triggered Refresh


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

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

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

Refresh Device Quick Task

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

- 1 In ZENworks Control Center, click **Devices > Workstations** to display your enrolled devices.
- 2 Select the check box in front of the Mac 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 [Chapter 6, "Viewing Device Information," on page 29](#).

10 Account Configuration

This page provides information about configuring the administrator and primary user accounts created on Mac devices during the DEP enrollment.

NOTE: ♦ It is mandatory to create at least one administrator account when configuring Mac MDM. The administrator account is used to manage the device and its settings.

- ♦ If both the administrator and the primary user accounts are not configured, then the user will be prompted to create an administrator account.
 - ♦ It is recommended to configure a unique primary user account against each discovered device as this name is used to configure the hostname of the device.
-

Table 10-1

Setting	Description
Create Admin Account	Select Yes to create an administrator account on the macOS device.
Hide Account from end user	Select Yes to hide the admin account on the macOS device to non-administrator accounts. Hidden accounts are not visible in the Login Window to end-users. Select No to make the admin account visible when a user logs in.
Admin Account Display Name	Enter the full name for the admin account. This name is displayed when logging on to the device.
Admin Account Short Name	Enter the short name for the admin account. The short name is used to create the user's Home folder.
Admin Account Password	Specify the password for the admin account. The admin account password should not be more than 80 characters.

Setting	Description
Primary User Account	<p>The primary user account provides access to a local user on the macOS device.</p> <p>Choose any of the following options:</p> <ul style="list-style-type: none"> ♦ Don't create the account: Select this option if you do not want to create a primary user account. ♦ Create as Local User: Select this option to create a local user account. This option is displayed only when the Create Admin Account is set to Yes. ♦ Create as Local Admin: Select this option to create an account for the primary user with administrator privileges.
User Information	<p>Choose any of the following options:</p> <ul style="list-style-type: none"> ♦ Not pre-populated: The end user should specify the display name, short name, and password. The values are not pre-populated. ♦ Pre-populated and Editable by end user: The display name and short name is displayed, and the end user can modify the details if required. ♦ Pre-populated and non-Editable by end user: The primary user account is created with the specified User Account Display Name, User Account Short Name, and User Account Password. The end user cannot modify these values. ♦ Pre-populated, Non-editable and Reserved for end user: Only the Reserved user of the discovered device can configure the User Account Display Name and User Account Short Name. The reserved user's full name is used as display name and Reserved user's login name is used as short name. <p>NOTE: Ensure that the Reserved User is available for the DEP device. If the Reserved user is not available, account configuration will fail.</p>
User Account Display Name	Enter the full name for the primary account. This name is displayed when logging on to the device.
User Account Short Name	Enter the short name for the primary account. The short name is used to create the user's Home folder.
User Account Short Name	Specify the password for the primary account. The primary account password should not be more than 80 characters.

11 Managing the DEP Settings

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

- ◆ **General and Skip Item Settings:** Lets you modify the initial setup process of the device. For more information, see [“General and Skip Setup Item Settings” on page 41.](#)

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

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

NOTE: Ensure that you do not modify the settings while the users are enrolling their devices.

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

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

General and Skip Setup Item Settings

The General and Skip Setup Item Settings page consists of the following panels:

[General](#)

[Skip Setup Items](#)

- ◆ [Skip Setup Items - Mac](#)

General

This page lets you modify the DEP settings to enhance the enrollment process. You can modify the settings at the device folder level or for a specific device. The modified settings are applicable for devices that are to be newly enrolled or are reset to their factory settings.

The general profile settings are as follows:

- ◆ **Allow pairing of devices with a host computer:** Enables the user to pair a device. If set to **Yes** then the device can pair with any device. If set to **No**, then the device can pair with only those host devices that have their certificate configured in the DEP settings.
- ◆ **Set device as supervised:** Enables supervision of devices.

- ♦ **Allow user to remove the MDM profile from the device:** Enables the user to remove the configured MDM profile. This setting is enabled if the device is set as Supervised.

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

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

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

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

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

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

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

Skip Setup Items

Skip Setup Items allow you to skip certain setup steps or configuration options during the initial device setup process. This helps streamline the setup process and ensures devices are quickly ready for deployment. This can even be configured if you want to prevent users from making changes to their devices during setup.

This page consists of the following panels:

- ◆ [Skip Setup Items - Mac](#)

Skip Setup Items - Mac

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

NOTE: The skip settings seen on the Mac devices during ADE enrollment might vary depending on the architecture and the macOS version.

Select **Auto Advance** to skip the setup assistance panes during the initial setup of Mac. This feature is available for devices that are managed by MDM. It does not require any user interaction and allows automated setups.

Select **Select All** to skip the setup panes. This feature may still require user intervention.

- ◆ The **Location Services** screen, which helps in determining the user's current location.
- ◆ The **Restore apps and data** options screen, which enables the user to restore data from backup.
- ◆ The **Apple ID** screen, which enables the user to specify the Apple ID.
- ◆ The **Terms and Conditions** screen. If this option is selected, these Terms and Conditions are automatically accepted by the device.
- ◆ The **Touch ID/Face ID** screen, which enables the user to use biometrics to unlock the device or authenticate to apps.
- ◆ The **Apple Pay** setup screen, which enables the user to make digital payments.
- ◆ The **Siri** screen, which enables the user to setup Siri.
- ◆ The **Diagnostics** screen, which enables the user to send diagnostic data to Apple.
- ◆ The **Display Tone** options screen, which enables the user to adjust the white balance on the device display.
- ◆ The **Privacy** screen that controls which apps can access information stored on the device.
- ◆ The **Screen Time** screen, which provides information on the time spent by users on their devices.
- ◆ The **Appearance** screen, which enables users to access the Choose your Look screen.
- ◆ The **Accessibility** screen, which skips the Accessibility pane, only if the Mac is connected to Ethernet and the cloud config is downloaded.
- ◆ The **App Store** screen, which enables users to skip the App Store pane.
- ◆ The **FileVault** screen, disables FileVault Setup Assistant screen in macOS.
- ◆ The **iCloud Diagnostics** screen, which enables users to skip to iCloud Analytics screen.

- ♦ The **iCloud Storage** screen, which enabled users to skip iCloud Documents and Desktop screen in macOS.
- ♦ The **Unlock With Watch** screen, which enabled users to skip Unlock Your Mac with your Apple Watch pane.

12 Device Removal and Retirement

The following sections provide information and instructions to help you delete or retire devices from your ZENworks system.

If you delete a device, the selected device is removed from your ZENworks system; however, the MDM profile is not removed from the device. The MDM profile has to be manually removed.

Retiring a device is different from deleting a device. When you retire a device, its GUID is retained (as opposed to when you delete a device, which also deletes its GUID). A retired device is in a holding state until you unretire or delete the device. If you unretire the device in the future, its assignments are restored. You can retire only the managed devices.

- ♦ [“Deleting Devices from Your ZENworks System” on page 45](#)
- ♦ [“Retiring or Unretiring Devices” on page 45](#)
- ♦ [“Unregister Mac MDM Device” on page 46](#)

Deleting Devices from Your ZENworks System

If you delete a macOS MDM device, the selected device is removed from your ZENworks system, its GUID is deleted and bundle assignments are removed.

1. In ZENworks Control Center, click the **Devices** tab.
2. Click the underlined link next to the Workstations folder to display the list of workstations in your ZENworks system.
3. Select the check box in front of workstation (you can select multiple devices).

NOTE: In ZENworks Control Center, if you delete Mac MDM devices, the devices are not registered after the next refresh.

To delete a device using `zman`, follow the procedure in the [workstation-delete \(wd\) workstation object path](#) [...] [options] section of the [ZENworks Command Line Utilities Reference](#) guide.

To delete a device using dashlet, see [Device Distribution](#) and [Device Last Contact](#)

Retiring or Unretiring Devices

If you retire a workstation device, the selected device is retired from the ZENworks zone. Retiring a device is different from deleting a device. When you retire a device, the device GUID is retained. However, when you delete a device, the device GUID is also deleted. Also when a device is retired, all bundle assignments are retained. A retired device is in a holding state until you unretire or delete the device. If you unretire the device in the future, its assignments are restored. You can retire only the managed devices. For more information, see [Retiring or Unretiring Devices](#).

NOTE: If you select **Action > Unregister Device** on a Mac MDM enrolled device, no action is performed on the MDM profile, but the device is deleted. To remove the MDM profile, you can use the **Unenroll MDM Device Now** quick task.

Unregister Mac MDM Device

If you select **Action > Unregister Device** on a Mac MDM enrolled device, no action is performed on the MDM profile, but the device is deleted. To remove the MDM profile, you can use the **Unenroll MDM Device Now** quick task.

13 Unenrolling Mac MDM Devices using Quick Task

You can initiate the Unenroll quick task to unenroll devices from ZENworks that you no longer want to manage.

To unenroll Mac MDM devices, perform the following steps:

1. In ZCC, click **Devices > Workstations**.
2. Select the required Mac MDM enrolled devices, and then click **Quick Task**.
3. Select the **Unenroll MDM Device Now** option.
4. In the Quick Start Status window, select **Start**.

The device will be unenrolled after the Quick Task status changes to Done.

Based on the enrollment modes, the following actions are performed if unenroll is selected:

Table 13-1

Enrollment Mode	Unenroll
Mac MDM	Remove the MDM Profile and the device is deleted from the zone
Mac MDM+ZENAgent	Remove the MDM Profile and the MDM data is deleted from the ZENworks system
ZENAgent	No action performed

NOTE: Unenrolling of Mac MDM devices via dashlets is not supported.

A Troubleshooting Scenarios

The following sections provide solutions to the problems you might encounter with Mac Devices:

A.1 Devices respond as NotNow when a Mac device is locked

When a schedule sync is attempted on Mac devices, a device may not execute commands, but instead respond with a `NotNow` status during these conditions:

- ♦ The device is running on battery power in Power Nap and the server sends any command other than `DeleteUserCommand`, `DeviceLockCommand`, `EraseDeviceCommand`, `RestartDeviceCommand`, `ShutDownDeviceCommand`, `UserListCommand`, `ActivationLockBypassCodeCommand`, `ClearActivationLockBypassCodeCommand`, or `UnlockUserAccountCommand`.
- ♦ The server sends an `InstallProfile` or `RemoveProfile` command on the user connection and the user's keychain is locked.
- ♦ The device is blocking the user's login while it contacts the server and the server sends a request that can take a long time to process; for example, `InstalledApplicationList`.

Workaround: The commands will be executed when the device reaches the server once the device is unlocked (No manual step will be required by the administrator).

A.2 A new CA is activated when a device is in the lost state

When the device is in a lost state during the CA remint process, a new CA is activated the Mac MDM devices will not be able to communicate with the server.

Workaround:

1. Download the trust profile by visiting <https://<server address>/endpoint/apple/trust>.
2. Perform steps 1 through 7 mentioned in [Chapter 5, "Enrolling Mac MDM using the OTA Profile," on page 19](#)
3. Initiate the **Refresh Device** quick task for the device.

