iOS Supervised Devices

ZENworks® Mobile Management 3.1.x

August 2015

Novell.

Legal Notices

Novell, Inc., makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc., makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. See the Novell International Trade Services Web page (http://www.novell.com/info/exports/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Copyright © 2012-15 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

Novell, Inc.
1800 South Novell Place
Provo, UT 84606
U.S.A.
www.novell.com

Online Documentation: To access the latest online documentation for this and other Novell products, see the Novell Documentation Web page (http://www.novell.com/documentation).

Novell Trademarks

For Novell trademarks, see the Novell Trademark and Service Mark list (http://www.novell.com/company/legal/trademarks/tmlist.html).

Third-Party Materials

All third-party trademarks are the property of their respective owners.

Table of Contents

iOS Device Deployment Options

You can deploy iOS devices in education or business environments using Apple Configurator or the Apple Device Enrollment Program (DEP). Both offer the ability to configure devices as supervised and are ideal for managing corporate owned devices.

A decision on which deployment method to use should be based on how the devices will ultimately be used.

Apple Configurator

- Apple Configurator is the recommended tool for deploying iOS devices that will be shared between many users over the course of a day or week.

Apple Device Enrollment Program (DEP)

- DEP devices are the best fit when a device will be used by one user for an extended period of time.

- DEP is a good solution for organizations that distribute corporate owned devices for personal use.

- The Device Enrollment Program is available to qualifying businesses, public and private schools, colleges, and universities in the United States that purchase iPad, iPhone, or Mac directly from Apple.

Apple Configurator

Description

Apple Configurator is a tool that assists administrators in the deployment and management of iOS devices in business or education settings. It is well suited to environments where devices are often reassigned or where they are shared by multiple users.

When integrated with *ZENworks Mobile Management*, the application is useful as a deployment tool since it provisions multiple devices quickly, enrolling them with the *ZENworks Mobile Management* server and staging each device with the appropriate MDM profiles. As a management tool, Apple Configurator makes reassigning devices quick and simple. Configurator can reassign a device allowing the next user to start with a clean slate of content. If needed, Configurator can back up and store user-specific data in its database for use on another device in the future.

ZENworks Mobile Management provides the administrative component of an organization's mobile strategy. After deployment via Apple Configurator, devices are secured and monitored to protect valuable content and the devices themselves. Updates can be made as a user's role or needs change. Administrators can also easily manage devices from the *ZENworks Mobile Management* dashboard if issues arise or devices are compromised.

Requirements: Mac OS X 10.5   iTunes version 11.1 or greater

Overview

Outlined below are steps that illustrate how *ZENworks Mobile Management* and Apple Configurator integrate to seamlessly deploy and administer devices.

1) Establish a Policy Suite and Device Connection Schedule in *ZENworks Mobile Management* that you will use to govern the devices.

2) From *ZENworks Mobile Management*, create the iOS Configurator Group using the designated Policy Suite and Device Connection Schedule and export the profile.

3) Prepare devices in Apple Configurator, setting them to the *Supervised* mode.

4) Import the profile into Apple Configurator.

5) Configurator enables mass deployment of the *ZENworks Mobile Management* profile to any device formatted with the application. In doing so, each connected device is silently enrolled with *ZENworks Mobile Management*.

From this point on, the device can be tracked and administered from the *ZENworks Mobile Management* dashboard.

Preparing for Integration

Considerations

If you are supporting devices with the *ZENworks Mobile Management* app that have been deployed via *ZENworks Mobile Management,* along with supervised Configurator devices, consider creating a separate organization for the Configurator devices.

Configurator devices do not have the *ZENworks Mobile Management* app or an ActiveSync profile. If you set up restrictions with *ZENworks Mobile Management* and ActiveSync related compliance rules for other devices, they will affect Configurator devices as well. Creating exceptions for the Configurator devices, to the *ZENworks Mobile Management* and ActiveSync related compliance rules, can prevent this. Another option, however, is to segregate the Configurator devices in a separate organization that does not impose these particular compliance rules.

Before you Integrate

Before creating a Configurator group in *ZENworks Mobile Management* and exporting it for use in Apple Configurator, you will need to determine which Policy Suite and Device Connection Schedule you will use to govern the Configurator devices.

These settings are components of the MDM profile that is delivered to each device via Apple Configurator.

If you want to create a new policy suite or connection schedule specifically for the Configurator devices, use the wizards available in the *ZENworks Mobile Management* dashboard:

- Organization > Policy Suites
- Organization > Device Connection Schedules

With these tasks completed, you can create a Configurator group in *ZENworks Mobile Management* and export the MDM profile.

Integrating with Apple Configurator

Preparing Devices

Since it can take some time, start by preparing devices in Apple Configurator.

Set devices to the *Supervised* mode. Supervised mode is recommended for devices that users will share. Supervised devices cannot be synced with iTunes or with Apple Configurator on a different Mac. An unsupervised device will give the user the freedom to personalize the device, syncing any content they want.

Setting a device to Supervised Mode allows you to load the preferred iOS version, apply sync and backup restrictions, set each device's lock screen image and message, and wipe the device to a clean template state.

1. Connect the device(s) through the USB port(s).
2. Select the **Prepare** page in Configurator.

3. Enter a **Name** for the device(s). When multiple devices will be associated with this name, check the **Number sequentially** box. Numbers will be appended to the name to distinguish each connected device.
4. Set the **Supervision** option to *ON*. The checkbox for *Erase before installing* will automatically be enabled. Old data on Supervised devices will be erased.
5. **iOS** version defaults to *Latest*. If needed, you can select an older version from the drop-down list.
6. The **Restore** option defaults to *Don't Restore Backup*. Accept the default unless you are restoring data on connected devices.

Note: When restoring a backup, only like devices should be prepared at the same time. For example, if restoring from an iPad mini backup when preparing devices for Supervision, only connected iPad minis get the Supervision profile. If an iPhone is connected, it would not get the Supervision profile. To properly supervise the device when restoring a backup, only like devices should be prepared at the same time to avoid issues.

7. You can leave the **Profiles** box empty for now. You will have another opportunity to import the MDM profile on the Configurator *Supervise* page.

8. Click the **Prepare** button at the bottom of the window to prepare the connected devices. Connect more devices, if necessary, clicking the *Prepare* button to initiate the formatting of each batch.

Creating the Configurator Group and Exporting a Profile

1. Navigate to **System** and select **Organization** from the left panel.

2. Locate the **iOS Configurator Groups** field and click the **Export Profile for Configurator** button.

iOS Configurator Groups: [Export Profile for Configurator]
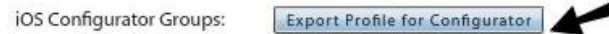
3. Enter a **Configurator Group Name** and select the **Policy Suite**, **Device Connection Schedule,** and **Liability** and **Ownership** status for the group.

4. Click **Next**.

| Export Profile for Configurator ✖	Export Profile for Configurator ✖
Configurator Group Name: ✱ Classroom 102A	Click the Finish button to complete the export.
Policy Suite: ✱ default ▾	
Device Connection Schedule: ✱ default ▾	
Device Liability: ◉ Corporate ○ Individual	
Device Ownership: ◉ Company ○ Personal	
[Cancel] [Next]	[Cancel] [Finish]

5. Click **Finish** to export the profile. Select a location in which to save the mobile.config file that is created. Click **Save**.

Importing a Profile into Apple Configurator

Import the profile into Apple Configurator and apply it to the connected device(s) that have been prepared as *Supervised*.

>   **Note:** Devices must have a Wi-Fi or cellular connection in order to install the profile properly.

1. Connect devices and select the **Supervise** page in Configurator. Verify that the devices have a Wi-Fi or cellular connection.

2. Import the MDM profile. Click the plus sign under the **Profiles** box and browse to the mobile.config file you want to import, or drag and drop the file into the box.
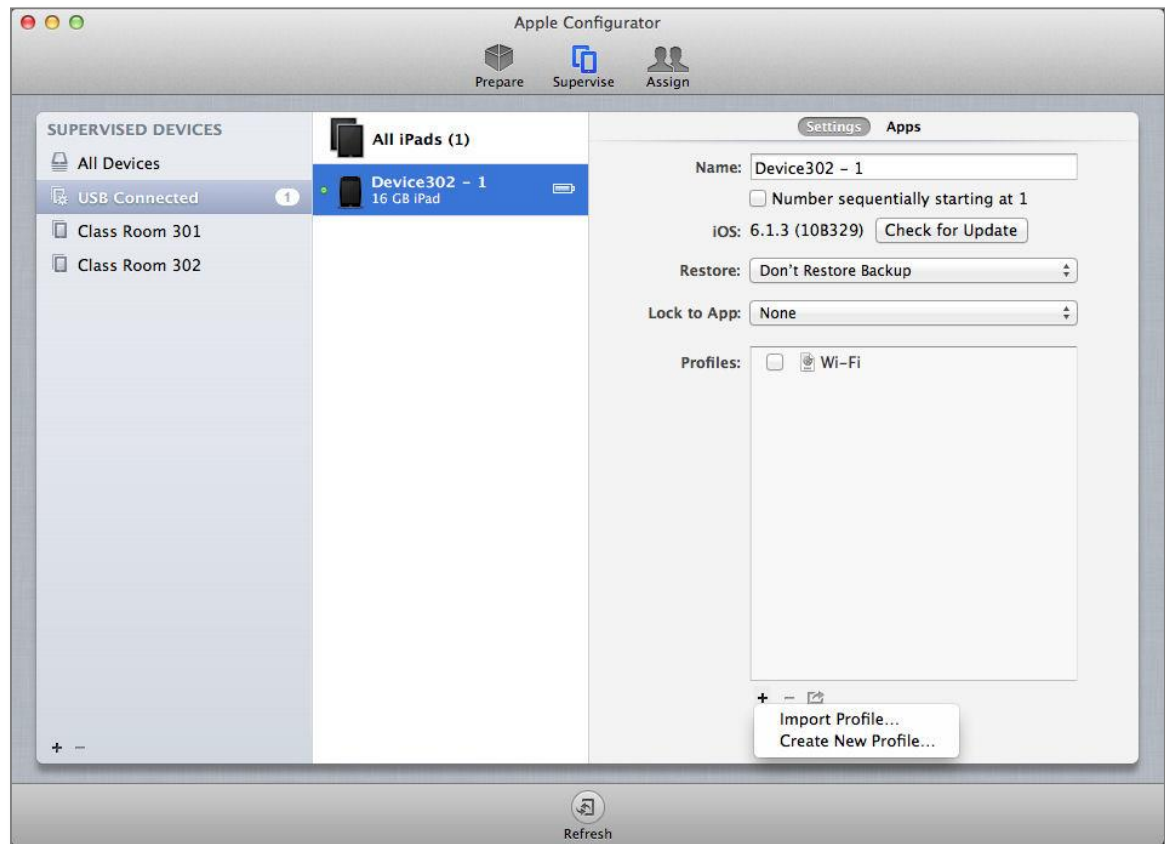
3. (Optional) Use the plus sign under the *SUPERVISED DEVICES* column to create a category in which to group devices. Move devices listed in the middle column into the categories.

4. Select one or more devices from the device list in the middle panel or a category of devices from the left panel, then select a profile from the *Profiles* box.
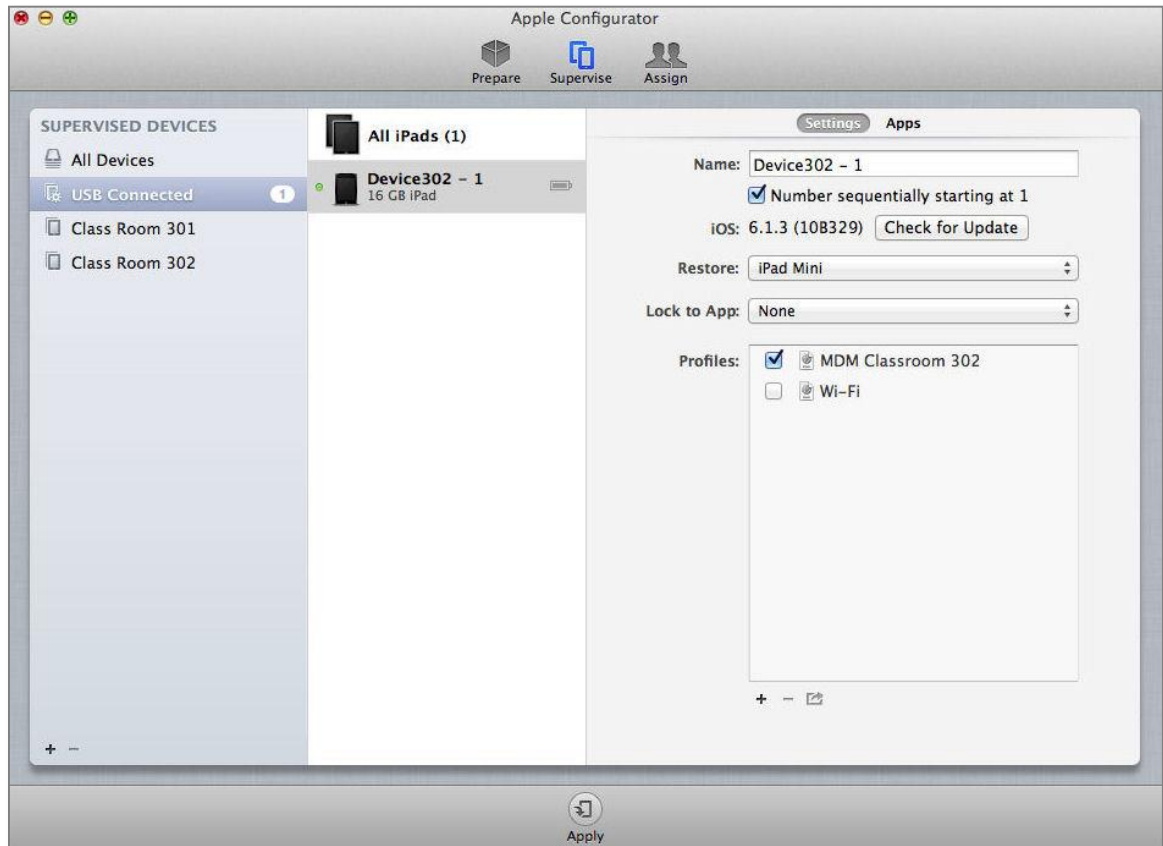
5. Click the **Apply** button at the bottom of the window and your devices will be enrolled with the *ZENworks Mobile Management* server and staged with the appropriate MDM profile. The profiles appear on the device under *Settings > General*.

From this point on, you can manage device settings and features from the *ZENworks Mobile Management* dashboard.

Managing Configurator Devices

Devices deployed via Apple Configurator can be managed from the *ZENworks Mobile Management* dashboard like any other device. Functionality on Configurator devices may be different from iOS devices deployed through *ZENworks Mobile Management*, since Configurator devices do not have the *ZENworks Mobile Management* app or an ActiveSync profile. See the [Device Platform Functionality](#) matrix for details.

Configurator devices appear in the user grid and share the same username when they belong to the same iOS Configurator Group.

Active	User Name	First Name	Last Name	Liability	Ownership	Device Platform	Device Model
Yes	Classroom 302	Device302 - 1		Corporate	Company	iOS	iPad Mini
Yes	Classroom 302	Device302 - 2		Corporate	Company	iOS	iPhone 4S
Yes	jdoe	John	Doe	Corporate	Company		Unknown

Device Reassignment

When it is time to reassign a device to another user, Apple Configurator makes the process simple. When connected to the Configurator the device is wiped so that the next user starts with a clean slate of content.

From the *ZENworks Mobile Management* User Grid, you should either issue a command to un-enroll the device (*Stop Managing Device*) or use the *Reset for Enrollment* command before you repurpose the device via Configurator.

Apple Device Enrollment Program

Description

The Device Enrollment Program (DEP) is part of the Apple Deployment Programs and provides administrators with a streamlined way to deploy multiple corporate owned iOS devices. The program is available to qualifying businesses, public and private schools, colleges, and universities in the United States that purchase iPad, iPhone, or Mac directly from Apple.

Enroll in the program at: https://deploy.apple.com   See also: Apple's DEP Guide

A DEP token, issued from Apple, is uploaded to the *ZENworks Mobile Management* server. Information for each device associated with the token populates the User Grid.

Upon device activation, enrollment with the MDM server is automatic and over-the-air configuration of account settings, apps, and IT services is immediate. There is no need for IT administrators to physically access each device to complete the setup.

Like configurator devices, a DEP device does not install the *ZENworks Mobile Management* app unless the administrator configures the server to push the app to iOS devices, however, each device is associated with an individual user when it is enrolled on the *ZENworks Mobile Management* server. The server communicates updates to the DEP devices via the Apple Push Notification service (APNs).

DEP devices that have been enrolled with user credentials can be managed like any other device enrolled on the *ZENworks Mobile Management* server.

Apple DEP Token Upload

You must link the *ZENworks Mobile Management* server to your Apple DEP account. The MDM server will generate a Public Key which you will upload to the Apple web portal. Apple will then issue a token that is associated with the DEP devices your organization has purchased directly from Apple. When this token is uploaded to the *ZENworks Mobile Management* server, information for each device associated with the token populates the User Grid.

Helpful Hints:

- The APNs certificate must be uploaded before managing the DEP token.

- The DEP token will be deleted if the APNs certificate is removed.

- You cannot use a single token for multiple organizations. Each organization must have its own token.

1. From the dashboard, navigate to **System Management** > **Organization**. Click the **Upload** button next to the *Apple DEP Token* field. A pop-up appears.


2. Click the **Download** button next to the *Public Key* field.

3. The MDM server generates the Public Key (a .PEM file labeled *MDM_DEP_Public_Key.PEM* by default). Save the file somewhere on your server.

4. Click the link to Apple's Deployment Program web portal and follow the directions to upload the .PEM file you stored. Apple will issue a DEP token.

5. Download the DEP token and save it somewhere on your server.

6. Click the **Browse** button next to the *Choose Apple DEP Token* field to choose the DEP token you stored.

7. Enter the email address you used to enroll in and sign into the DEP web portal (*optional*).

8. Click the **Submit** button. Devices associated with the token are retrieved from the Apple server and will populate the User Grid.

DEP Profile

The *ZENworks Mobile Management* server generates a default profile for devices associated with the token. The profile is applied to each device as it is activated by a user. The default profile settings are illustrated here.

See also Managing the DEP Profile.
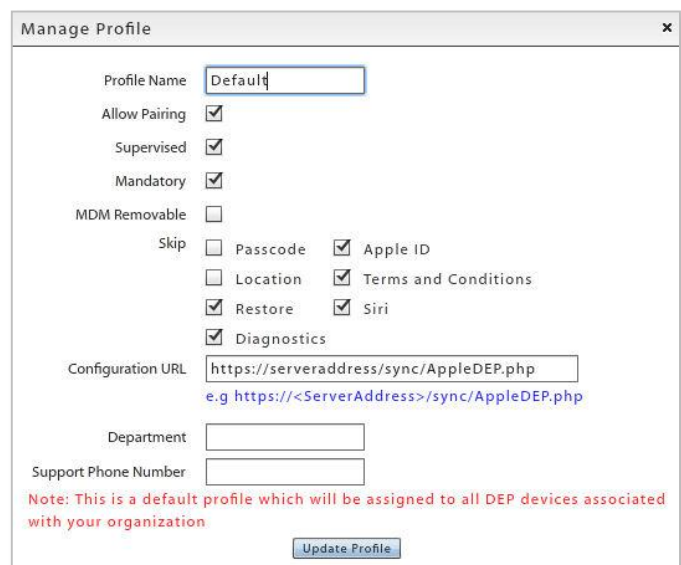
Default Profile Settings

Apple DEP Token Management

Once the Apple DEP token has been uploaded, there are several options for managing it.

Edit	Click *Edit* to upload a new token or edit/add the E-mail address associated with the DEP account.	Apple DEP Token: [Edit] [Remove] [Sync Now]
Remove	Removes the token from the server. Devices remain intact on the User Grid. Automatic discovery of devices, however, no longer functions.	Confirm Delete — MDM will no longer be able to manage DEP devices associated with this token. Are you sure you want to remove this token? [Yes] [No]
Sync Now	Initiates a connection with the Apple server to retrieve the latest information about devices associated with the DEP token. An automatic check is done each time the token is uploaded or edited and each time the *DEP Device Grid* is accessed. You can also initiate a sync from the User Grid.	Syncing DEP Devices ✕ — Please wait while we retrieve devices associated with the DEP token from Apple server.

Managing the DEP Profile

DEP devices can be viewed on a grid separate from the *User/Device Grid*. From the dashboard, select **Smart Devices and Users** and click the **Apple DEP Devices** button in the upper right corner of the grid.
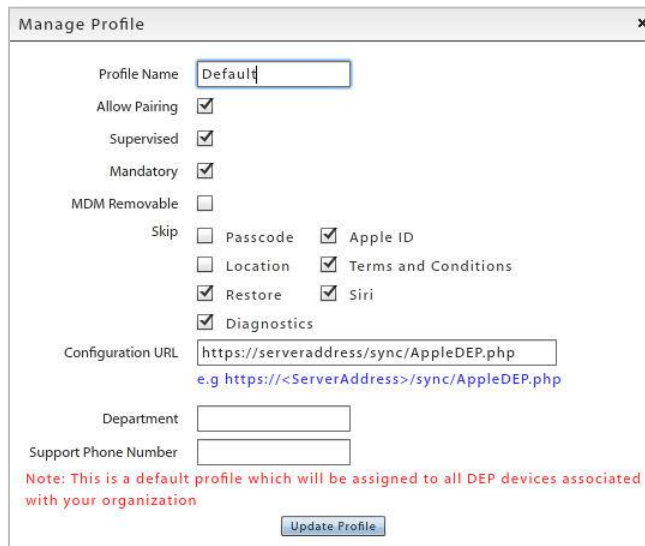
On the DEP device grid, click the **Manage Profile** button to view or edit the default DEP profile that is applied to each device as it is activated by a user.

User Name	Domain	Status	Serial Number	Device Model	Description	Profile Status	D
gcochenour@ex07.notify		Enrolled	DMQMC1WUF182	iPad Wi-Fi With Retina Display	IPAD WI-FI 16GB BLACK-USA	assigned	
N/A		Not Enrolled	C37LXDT2FF9R	iPhone 5S	IPHONE 5S SPACE GRAY 16GB-USA	assigned	SF
N/A		Not Enrolled	F78LFZ7RFFHG	iPhone 5C	IPHONE 5C WHITE 16GB-USA	assigned	
N/A		Not Enrolled	F7NLX9A4FP84	iPad Mini Wi-Fi	IPAD MINI WI-FI 16GB SPACE GRAY-US	assigned	SF

The *ZENworks Mobile Management* server generates a default profile for devices associated with the token. The profile is applied to each device as it is activated by a user. The profile allows several parts of the standard iOS Setup Assistant to be skipped.

The profile can be edited. However, in order to receive the updated profile, any device that has already been enrolled must be wiped and re-enrolled. The default profile settings are illustrated below.

Default Profile Settings

To Edit the DEP Profile:

1. From the dashboard, select the **Smart Devices and Users** view and click the **Apple DEP Devices** button in the upper right corner of the User/Device Grid. This flips the view to a list of the DEP devices.

2. Click the **Manage Profile** button.

3. Edit any of the fields in the profile, then click the **Update Profile** button.

Options	Default	Description
Allow Pairing	Enabled	Determines whether device can exchange a passkey with another device to allow automatic authentication for communication between the devices.
Supervised	Enabled	Determines whether the device must be in Supervised mode.
Mandatory	Enabled	Determines whether the user can skip applying the profile returned by the MDM server.
MDM Removable	Disabled	Determines whether user can remove the MDM payload delivered by the configuration URL.
Configuration URL	Auto-populated	This field is automatically populated with the server address of the *ZENworks Mobile Management* server.
Department	Blank	A department or location name (*optional*).
Support Phone Number	Blank	If defined, this will display on the device (*optional*).
Skip Options		
Passcode	Not skipped	If skipped, hides the passcode pane during setup.
Location	Not skipped	If skipped, disables location services.
Restore	Skipped	If skipped, disables restoring from backup.
Diagnostics	Skipped	If skipped, disables the automatic sending of diagnostic information.
Apple ID	Skipped	If skipped, disables signing in to Apple ID and iCloud.
Terms and Conditions	Skipped	If skipped, skips the Terms and Conditions during setup.
Siri	Skipped	If skipped, disables Siri.

Any existing DEP device that is already enrolled must be wiped and re-enrolled in order to receive an updated profile.

Enrolling a DEP Device

Enrolling a DEP device is simple for an end user since the DEP profile skips most of the native device activation prompts. A DEP device does not install the *ZENworks Mobile Management* device agent at enrollment unless the administrator configures the server to push the app to iOS devices.

After entering a Wi-Fi code, the user will be prompted for user credentials.

- If an administrator has entered users on the server prior to enrollment, an MDM account username and password can be entered.

- Users can also enroll if they have not been added to the server. In these cases, they must authenticate against an ActiveSync or LDAP server that is associated with the *ZENworks Mobile Management* server. They will use either domain\username and password or email address and password as their enrollment credentials.

Enrolling DEP Devices when a DEP User is Set

It is possible to select a shared user as the user for enrolling DEP devices. When a DEP user is set, enrollment of DEP devices proceeds without prompting for user authentication credentials.

During enrollment, the DEP profile skips most of the native device activation prompts. When Wi-Fi connects and the server is contacted, the device retrieves the shared user assignment instead of prompting for user credentials. Once the device is activated, it functions as any other DEP device would.

To set a DEP user:

1. From the dashboard, select the **Smart Devices and Users** view and click the **Apple DEP Devices** button in the upper right corner of the User/Device Grid.

2. On the DEP device grid, click the **Set DEP User** button. *Note:* This button is only displayed when shared users have been added to the organization.
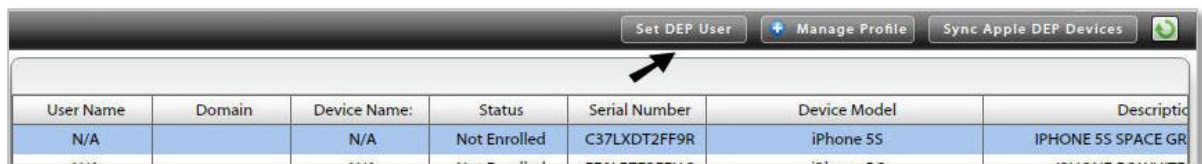
3. Make a selection from the list of available shared users. Click **Finish** to save your selection.

ZENworks Mobile Management 3.1.x Integrating Configurator with ZENworks Mobile Management   Apple Device Enrollment Program ● 17
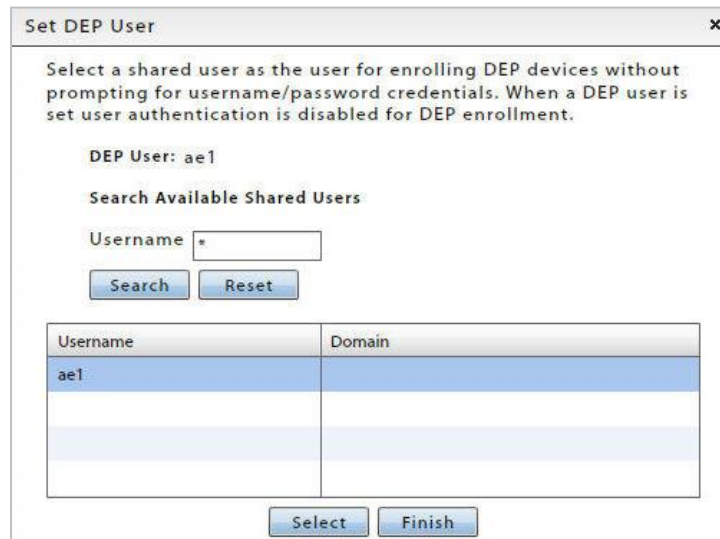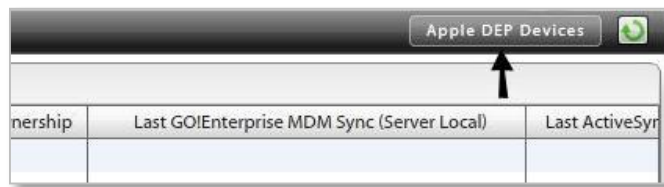
Managing DEP Devices

Like configurator devices, a DEP device does not install the *ZENworks Mobile Management* device agent, however, each device is associated with an individual user when it is enrolled on the *ZENworks Mobile Management* server. DEP devices that have been activated with user credentials can be managed like any other device enrolled on the server. The server communicates updates to the DEP devices via the Apple Push Notification service (APNs).

The Apple DEP User Grid

If your organization has deployed devices through the Apple Device Enrollment Program (DEP) you can view these devices on a grid separate from the standard User Grid.

From the dashboard, select the **Smart Devices and Users** view. Click the **Apple DEP Devices** button in the upper right corner of the User Grid page. This flips the view to a list of the DEP devices. Devices that have already been enrolled with user credentials, appear on the standard User Grid as well.

Double-click a DEP user/device on the grid to access the *User Profile*. From the *User Profile* the administrator can manage the device by updating account settings, making app assignments, giving access to IT services, etc.

Apple DEP User Grid

The **Status** column on the DEP Device Grid indicates whether a device is enrolled on the *ZENworks Mobile Management* server. The Username and Domain (if applicable) fields are populated only when the device has enrolled with the server. Devices that have already been enrolled with user credentials, appear on the standard User Grid as well as on the DEP Device Grid. A column can be added to the standard grid to identify DEP devices (from *Choose Visible Columns*, select **Apple DEP Device**).

User Name	Domain	Status	Serial Number	Device Model	Description	Profile Status	De
gcochenour@ex07.notify		Enrolled	DMQMC1WUF182	iPad Wi-Fi With Retina Display	IPAD WI-FI 16GB BLACK-USA	assigned	
N/A		Not Enrolled	C37LXDT2FF9R	iPhone 5S	IPHONE 5S SPACE GRAY 16GB-USA	assigned	SF
N/A		Not Enrolled	F78LFZ7RFFHG	iPhone 5C	IPHONE 5C WHITE 16GB-USA	assigned	
N/A		Not Enrolled	F7NLX9A4FP84	iPad Mini Wi-Fi	IPAD MINI WI-FI 16GB SPACE GRAY-US	assigned	SF

The **Disown Device** option in the administrator panel to the left of the DEP or standard User Grid should only be used if you want to permanently remove a device from the grid and notify the Apple servers that your organization no longer owns the device.

Disowning a device is a *permanent* action. Once it is disowned, a device cannot be reassigned to the server as an Apple DEP device. Disowning removes the DEP profile from the device.

> **Note**: Issue a Selective Wipe prior to disowning a device. *(In a future release, disowning a device will initiate a Selective Wipe automatically, as well as remove the DEP profile from the device.)*

← Back to Grid
Search ▼
Display by User Categories ▼
Device Panel ▲
Serial Number: C37LXDT2FF9R
Device Model: iPhone 5S
Administration: Disown Device

Synchronize DEP Device Information

Click the **Sync Apple DEP Devices** button. This action initiates a connection with the Apple server to retrieve the latest information about devices associated with the DEP token. An automatic check is done each time the *DEP Device Grid* is accessed.

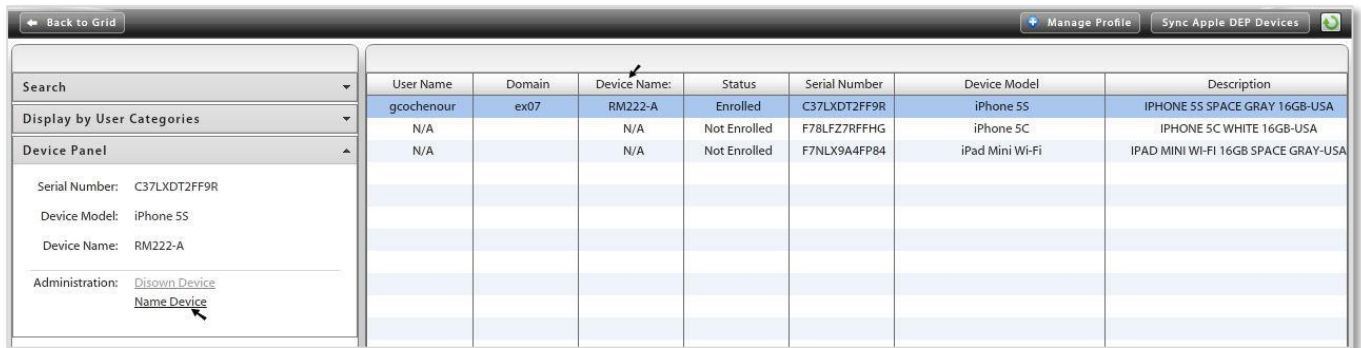| User Name	Domain	Status	Serial Number	Device Model	Description	Profile Status	De
gcochenour@ex07.notify		Enrolled	DMQMC1WUF182	iPad Wi-Fi With Retina Display	IPAD WI-FI 16GB BLACK-USA	assigned	
N/A		Not Enrolled	C37LXDT2FF9R	iPhone 5S	IPHONE 5S SPACE GRAY 16GB-USA	assigned	SF
N/A		Not Enrolled	F78LFZ7RFFHG	iPhone 5C	IPHONE 5C WHITE 16GB-USA	assigned	
N/A		Not Enrolled	F7NLX9A4FP84	iPad Mini Wi-Fi	IPAD MINI WI-FI 16GB SPACE GRAY-US	assigned	SF

Name a DEP Device

Supervised DEP devices running iOS 8.0+ can be named for easy identification on the device and in the dashboard. A column in the DEP Device Grid will display the names assigned to supervised devices. The name can be viewed on the device by navigating to *General > About > Name*. The name can be enter or changed from the device as well.

1. Select a supervised device from the grid and click the **Name Device** option on the *Device Panel*.

2. Name or edit the name of the device in the pop-up box and click **Save**.

The **Device Name** will appear in the grid once it synchronizes to the device and the device reports its statistics.

Return to the Standard User Grid

Click the **Back to Grid** button to return to the standard User Grid.