ZENworks 2020
Configuration Management
Evaluator’s Guide

August 2021

Legal Notice

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/.

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

1 Welcome to ZENworks 2020 Configuration Management!

Some endpoint management solutions can manage your organization's servers. ***Others*** can manage your workstations and laptops. And ***still others*** can manage your mobile devices.

However, ***few can do what ZENworks 2020 Configuration Management does***—unify the management of your organization's server, workstation, and mobile devices into one system under a single management console. And ***none*** can do it with the simplicity, uniformity, and control provided by ZENworks.

But don't take our word for it. Use this *Evaluator's Guide* to check out ZENworks yourself. We'll help you look at how ZENworks performs on two of the most common endpoint tasks an organization faces: ***delivering applications to devices*** and ***securing those devices***. And we'll help you do it on not one but three of the major device platforms: ***iOS***, ***Android***, and ***Windows***.

1.1 How to Evaluate ZENworks

1. What You'll Need for the Evaluation (page 5): Learn about the resources you'll need for the evaluation.
2. Install and Configure ZENworks (page 7): Install the ZENworks software and perform the configuration tasks needed to use the product.
3. Managing Windows Devices via the ZENworks Agent (page 33): Windows devices can be managed using the ZENworks Agent, native Windows MDM, or both. We'll help you install the ZENworks Agent on a Windows device and register it in your ZENworks zone, secure that device, and then distribute applications to the device.
4. Manage Windows Devices via Windows MDM (page 49): Windows devices can be managed using the ZENworks Agent, native Windows MDM, or both. We'll help you MDM enroll a Windows device in your ZENworks zone, secure that device, and then distribute an application to the device.
5. Manage Mobile Devices (page 73): ZENworks manages iOS and Android devices using the native MDM capabilities of those platforms. We'll help you enroll iOS and Android devices in your ZENworks zone, secure the devices, and distribute apps to them.
6. Explore Other Areas (page 125): Learn about other areas of the product that aren't covered in the evaluation.

1.2 What You'll Need for the Evaluation

Here's a heads up on some of the resources you'll need in order to run through this evaluation. More information about these requirements is provided as needed in the sections that follow.

1.2.1 ZENworks System

- ❐ **A ZENworks server.** This can be either a supported hypervisor where you can run the ZENworks Virtual Appliance or a server (physical or virtual) where you can install the ZENworks software.
- ❐ **An LDAP directory.** ZENworks user authentication and user-based management requires access to an LDAP user directory.

1.2.2 iOS Device Management

- ❐ **An iOS device.** This is a test device for you to see how ZENworks manages policies on the device and distributes apps to the device. It needs to be running a minimum of iOS version 10. You're going to play with settings so we recommend it be a clean device that you can reset when finished.
- ❐ **An Apple Business Manager account or Apple School Manager account.** Required if you want to see how ZENworks manages enrollment of iOS devices purchased through the Device Enrollment Program (DEP) or how ZENworks supports distribution of apps purchased through the Apple Volume Purchase Program (VPP).
- ❐ **Two Apple ID accounts.** One ZENworks-dedicated account to link ZENworks to the Apple Push Notification Service. A second individual account to receive apps distributed through ZENworks. Required for managing iOS devices.

1.2.3 Android Device Management

- ❐ **An Android device.** This is a test device for you to see how ZENworks manages policies on the device and distributes apps to the device. It needs to be running a minimum of Android 5. You're going to play with settings so we recommend it be a clean device that you can reset when finished.
- ❐ **A Firebase account.** This is a Google account you can use to access Firebase to set up Firebase Cloud Messaging services for ZENworks. We recommend that you use a ZENworks-dedicated Google account.
- ❐ **An Android Enterprise account.** This is a Google account you can use to register with the Android Enterprise program. This is required to enroll Android devices in ZENworks and distribute managed Google Play Store apps to the devices. It can be the same account you use for Firebase.

1.2.4 Windows Device Management

- ❐ **A Windows device.** This is a traditional Windows 10 desktop or laptop. As with the mobile devices, you'll use it to test policies and apps.
- ❐ **A Microsoft Partner Center account.** This is a paid Microsoft subscription that you can use to set up Windows Notification Service. This is required if you want ZENworks to use the Windows modern management (MDM) capabilities to manage Windows 10 devices.

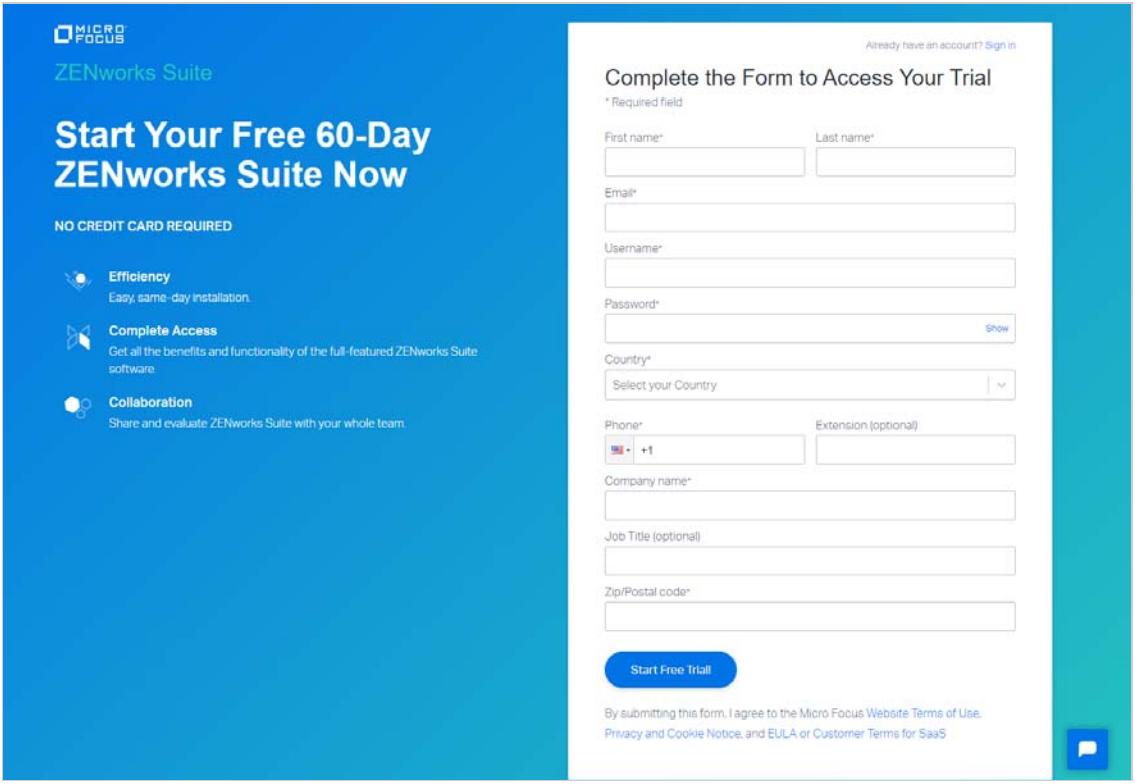
2 Install and Configure ZENworks

As a Unified Endpoint Management and Protection solution, all ZENworks Suite products (Asset Management, Configuration Management, Endpoint Security, Full Disk Encryption, and Patch Management) use the same ZENworks infrastructure. This means that when you complete the ZENworks installation, not only can you evaluate ZENworks Configuration Management but you can also evaluate any of the other products. The products can then be licensed individually or as a Suite.

2.1 Download ZENworks Software

To download the ZENworks software, you need a Micro Focus account. If you don’t already have an account, no worries, we’ll help you easily create one through our free trial website. Not only does your Micro Focus account let you access the ZENworks software, it also gives you access to trials for other Micro Focus products and membership in the Micro Focus product communities.

1 Go to the ZENworks 2020 Suite Trial Registration page (https://www.microfocus.com/products/zenworks/free-trial).



ZENworks Suite

Start Your Free 60-Day ZENworks Suite Now

NO CREDIT CARD REQUIRED

Efficiency
Easy, same-day installation.

Complete Access
Get all the benefits and functionality of the full-featured ZENworks Suite software.

Collaboration
Share and evaluate ZENworks Suite with your whole team.

Already have an account? Sign in

Complete the Form to Access Your Trial

* Required field

First name*

Last name*

Email*

Username*

Password*

Country*

Select your Country

Phone*

+1

Extension (optional)

Company name*

Job Title (optional)

Zip/Postal code*

Start Free Triall

By submitting this form, I agree to the Micro Focus Website Terms of Use, Privacy and Cookie Notice, and EULA or Customer Terms for SaaS

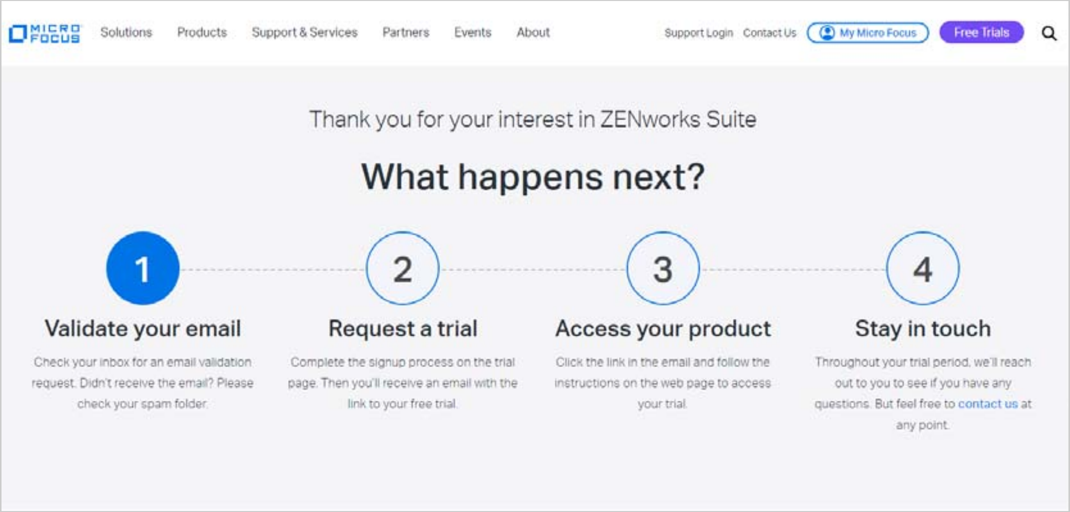
2 If you already have a Micro Focus account, click the **Sign In** link in the top right corner of the form and sign in to your account. Then continue with Step 3 below.

or

If you don't have a Micro Focus account:

2a Fill in the form to provide information for your account, then click **Start Free Trial**.

Your account is created and the following page is displayed.



Thank you for your interest in ZENworks Suite

What happens next?

1 Validate your email

Check your inbox for an email validation request. Didn't receive the email? Please check your spam folder.

2 Request a trial

Complete the signup process on the trial page. Then you'll receive an email with the link to your free trial.

3 Access your product

Click the link in the email and follow the instructions on the web page to access your trial.

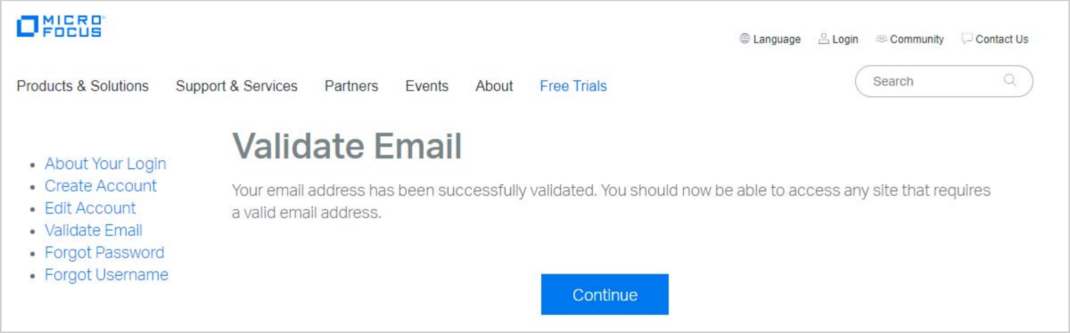
4 Stay in touch

Throughout your trial period, we'll reach out to you to see if you have any questions. But feel free to contact us at any point.

2b In your email account, open the Micro Focus Account email and click the **Validate Email** link.

2c Sign in with your Micro Focus account username and password.

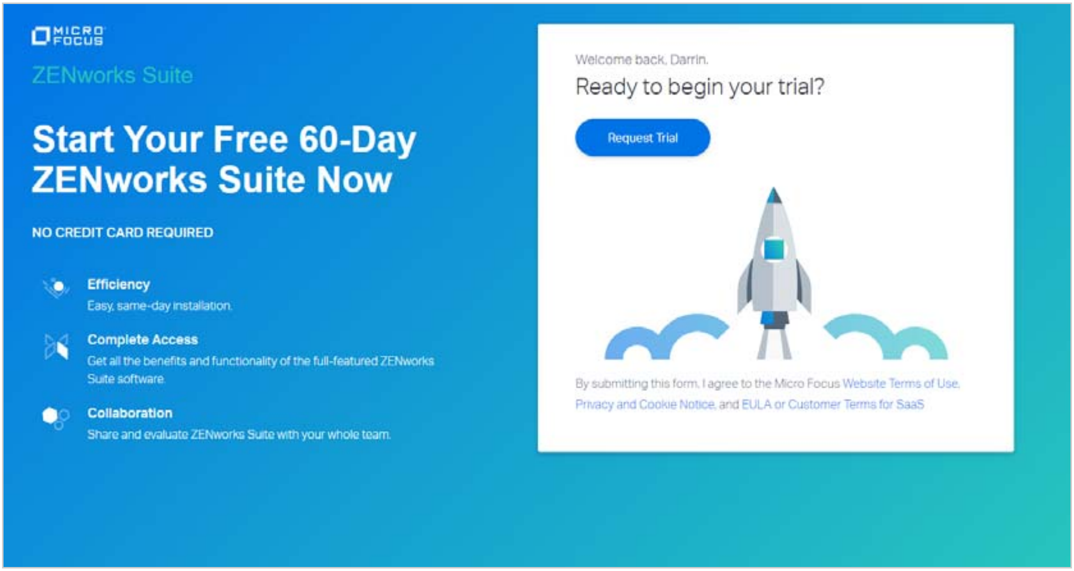
After successful login, your email is validated and your Micro Focus account is activated.



Validate Email

Your email address has been successfully validated. You should now be able to access any site that requires a valid email address.

2d Click **Continue** to return to the ZENworks Suite trial page.



Start Your Free 60-Day ZENworks Suite Now

NO CREDIT CARD REQUIRED

Efficiency
Easy, same-day installation.

Complete Access
Get all the benefits and functionality of the full-featured ZENworks Suite software.

Collaboration
Share and evaluate ZENworks Suite with your whole team.

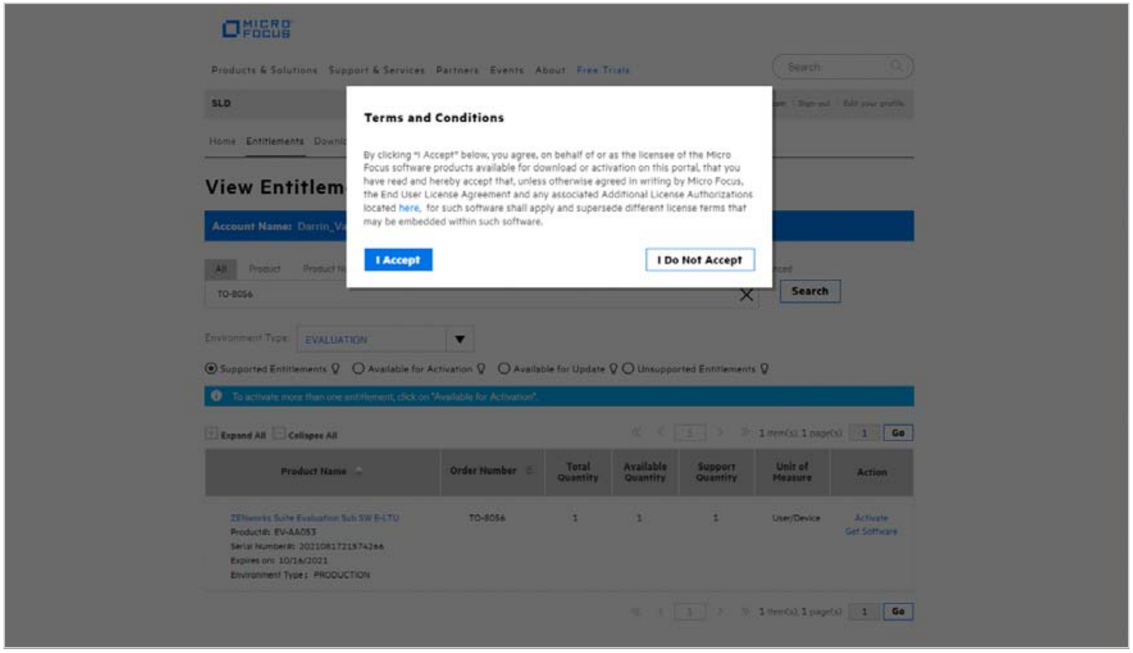
Welcome back, Darrin.

Ready to begin your trial?

By submitting this form, I agree to the Micro Focus Website Terms of Use, Privacy and Cookie Notice, and EULA or Customer Terms for SaaS

3. Click the **Request Trial** link.
4. In your email account, open the MFI Trials and Eval email and click the **Sign in** link.
5. If prompted, sign in with your Micro Focus account username and password.

   Your Micro Focus Software and License Distribution (SLD) portal is displayed.



Terms and Conditions

By clicking "I Accept" below, you agree, on behalf of or as the licensee of the Micro Focus software products available for download or activation on this portal, that you have read and hereby accept that, unless otherwise agreed in writing by Micro Focus, the End User License Agreement and any associated Additional License Authorizations located here, for such software shall apply and supersede different license terms that may be embedded within such software.

I Accept   I Do Not Accept

View Entitlem

Account Name: Darrin_V

TO-8056

Environment Type: EVALUATION

● Supported Entitlements ○ Available for Activation ○ Available for Update ○ Unsupported Entitlements

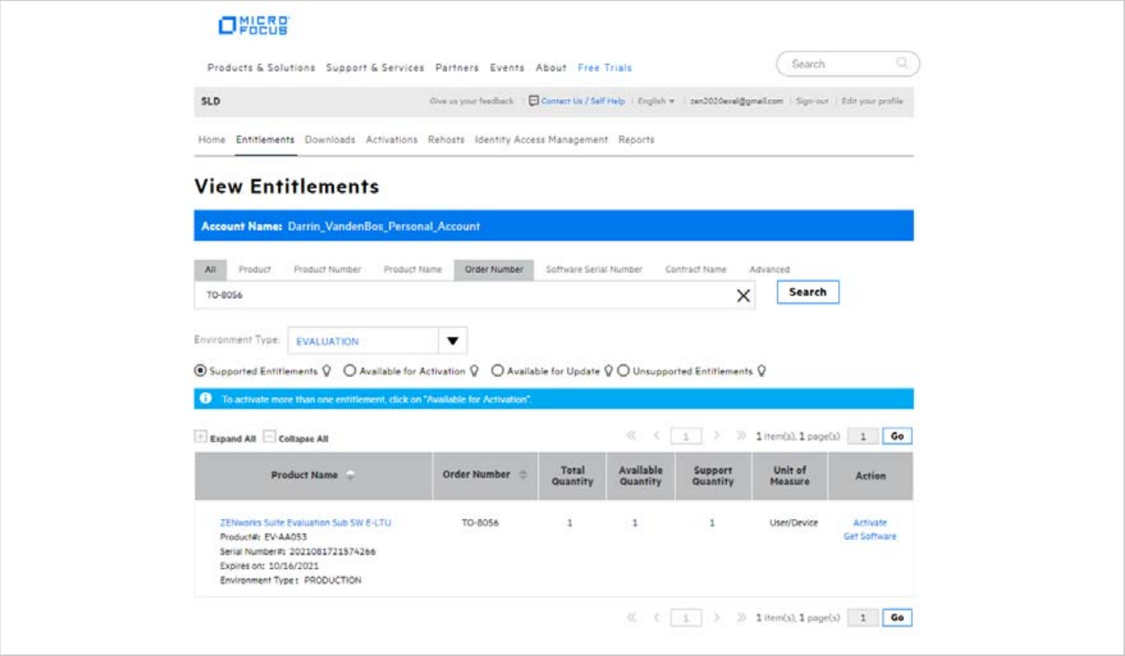
To activate more than one entitlement, click on "Available for Activation".

1 item(s), 1 page(s)

Product Name	Order Number	Total Quantity	Available Quantity	Support Quantity	Unit of Measure	Action
ZENworks Suite Evaluation Sub SW E-LTU Product#: EV-AA053 Serial Number#: 2021081721574266 Expires on: 10/16/2021 Environment Type: PRODUCTION	TO-8056	1	1	1	User/Device	Activate Get Software

1 item(s), 1 page(s)

6. Click **I Accept** to agree to the terms and conditions for Micro Focus software products.
7. Click **OK** to dismiss the *How to access your License Entitlements and Software Downloads* dialog.



View Entitlements

Account Name: Darrin_VandenBos_Personal_Account

All | Product | Product Number | Product Name | Order Number | Software Serial Number | Contract Name | Advanced

TO-8056 | Search

Environment Type: EVALUATION

● Supported Entitlements ○ Available for Activation ○ Available for Update ○ Unsupported Entitlements

To activate more than one entitlement, click on "Available for Activation".

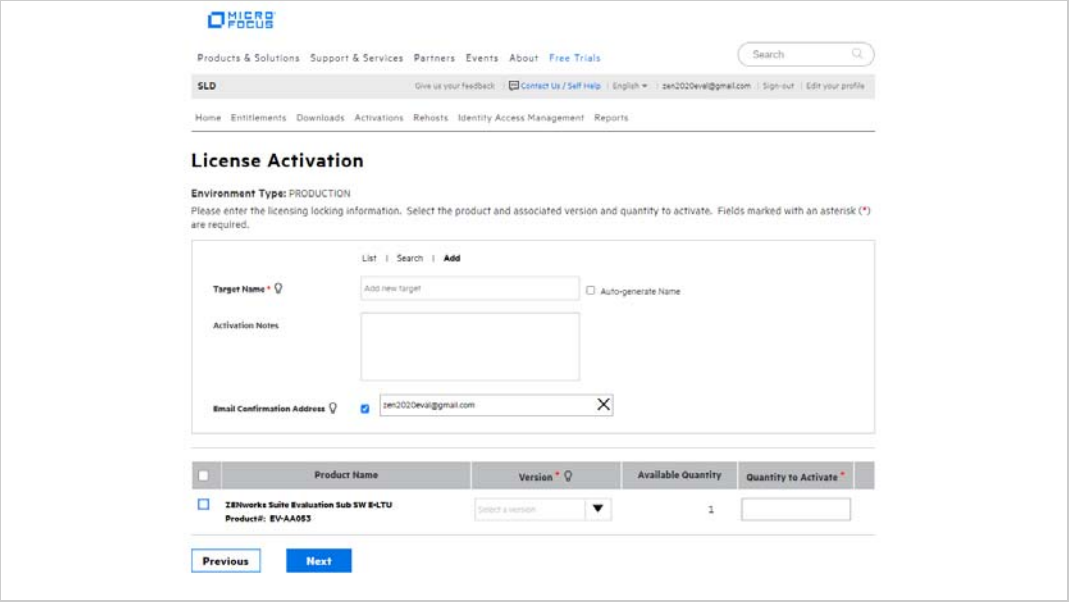
Expand All | Collapse All — 1 item(s), 1 page(s) 1 Go

Product Name	Order Number	Total Quantity	Available Quantity	Support Quantity	Unit of Measure	Action
ZENworks Suite Evaluation Sub SW E-LTU Product#: EV-AA053 Serial Number#: 2021081721574266 Expires on: 10/16/2021 Environment Type: PRODUCTION	TO-8056	1	1	1	User/Device	Activate Get Software

1 item(s), 1 page(s) 1 Go

8 Activate the product:

8a In the product list, click the **Activate** link for the *ZENworks Suite Evaluation Sub SW-E-LTU* entry to display the License Activation page.



License Activation

Environment Type: PRODUCTION

Please enter the licensing locking information. Select the product and associated version and quantity to activate. Fields marked with an asterisk (*) are required.

List | Search | **Add**

Target Name * : Add new target ☐ Auto-generate Name

Activation Notes:

Email Confirmation Address: ☑ zen2020eval@gmail.com

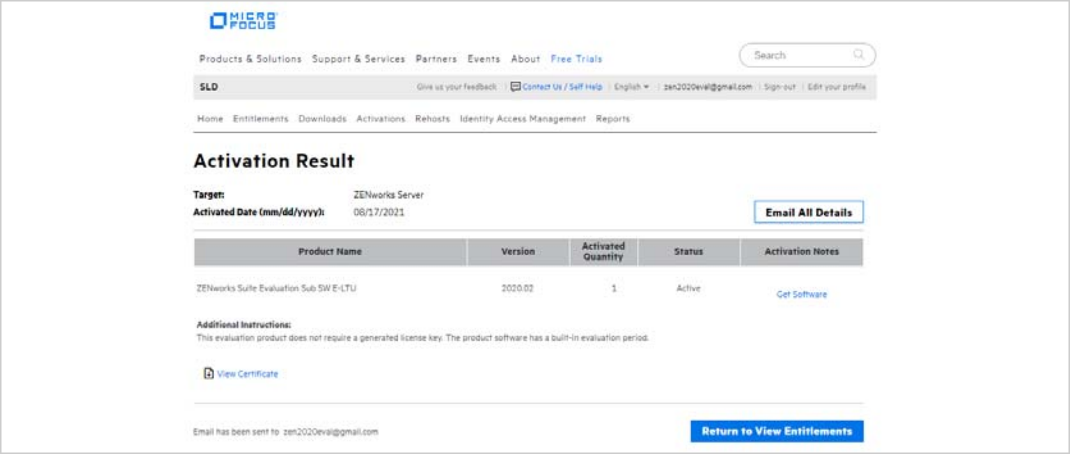
☐	Product Name	Version *	Available Quantity	Quantity to Activate *
☐	ZENworks Suite Evaluation Sub SW E-LTU Product#: EV-AA053	Select a version	1	

Previous | Next

8b In the Target Name field, enter `ZENworks Server.`

8c In the list, select **ZENworks Suite Evaluation Sub SW E-LTU**, select **2020.02** for the version, enter 1 as the quantity to activate, then click **Next**.

8d Click **Submit** to confirm the activation details and display the Activate Results page.



Activation Result

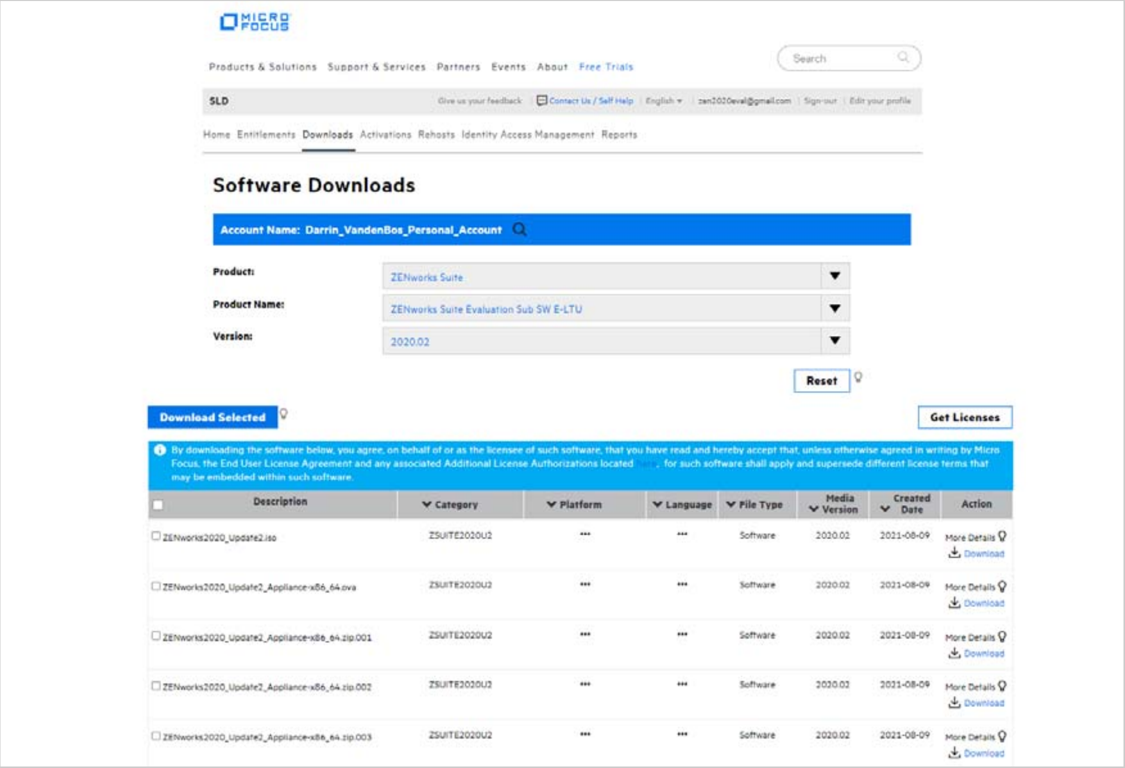
Target: ZENworks Server
Activated Date (mm/dd/yyyy): 08/17/2021

Product Name	Version	Activated Quantity	Status	Activation Notes
ZENworks Suite Evaluation Sub SW E-LTU	2020.02	1	Active	Get Software

Additional Instructions:
This evaluation product does not require a generated license key. The product software has a built-in evaluation period.

Email has been sent to zen2020eval@gmail.com

9 Click **Get Software** to display the Software Downloads page.



Software Downloads

Account Name: Darrin_VandenBos_Personal_Account

Product: ZENworks Suite
Product Name: ZENworks Suite Evaluation Sub SW E-LTU
Version: 2020.02

By downloading the software below, you agree, on behalf of or as the licensee of such software, that you have read and hereby accept that, unless otherwise agreed in writing by Micro Focus, the End User License Agreement and any associated Additional License Authorizations located here, for such software shall apply and supersede different license terms that may be embedded within such software.

□ Description	Category	Platform	Language	File Type	Media Version	Created Date	Action
□ ZENworks2020_Update2.iso	ZSUITE2020U2	•••	•••	Software	2020.02	2021-08-09	More Details Download
□ ZENworks2020_Update2_Appliance-x86_64.ova	ZSUITE2020U2	•••	•••	Software	2020.02	2021-08-09	More Details Download
□ ZENworks2020_Update2_Appliance-x86_64.zip.001	ZSUITE2020U2	•••	•••	Software	2020.02	2021-08-09	More Details Download
□ ZENworks2020_Update2_Appliance-x86_64.zip.002	ZSUITE2020U2	•••	•••	Software	2020.02	2021-08-09	More Details Download
□ ZENworks2020_Update2_Appliance-x86_64.zip.003	ZSUITE2020U2	•••	•••	Software	2020.02	2021-08-09	More Details Download

You'll quickly notice that there are a bunch of different download files. The files you need depend on whether you want to use the ZENworks Virtual Appliance or perform a traditional install.

Virtual Appliance: ZENworks is available as a virtual appliance that can be deployed to a supported virtual infrastructure. The appliance is built on a customized SUSE Linux Enterprise Server (64-bit) and comes pre-installed with ZENworks.

We strongly recommend that you use the appliance for the evaluation. Why? Because the appliance is convenient, easy to use, and doesn't require you to supply an operating system license.

The appliance is supported on the following hypervisors.

Hypervisor	File to Download
VMware ESXi 6.x VMware Workstation 6.5 and newer (use in non-production environments only)	ZENworks2020_Update2_Appliance-x86_64.ova
Microsoft Hyper-V Server Windows 2012 | 2012 R2 | 2016 | 2019	ZENworks2020_Update2_Appliance-x86_64.vhd.zip ZENworks2020_Update2_Appliance-x86_64.vhdx.zip
XEN on SLES 12.x |15.x	ZENworks2020_Update2_Appliance-x86_64.xen.tar.gz
Citrix XenServer 7.x and Citrix Hypervisor 8.x	ZENworks2020_Update2_Appliance-x86_64.xva.tar.gz

Traditional Install: You can install the software on a server listed below.

Operating System	File to Download
Windows 2012 Server x86_64 Windows 2012 Server R2 x86_64 Windows 2016 Server x86_64 Windows 2019 Server x86_64	ZENworks_2020_Update2.iso
SLES 12 SP4 | SP5 x86_64 SLES 15 | SP1 | SP2 x86_64	ZENworks_2020_Update2.iso

10 Click the **Download** link for the files you want to download.

2.2 Create a ZENworks System

After you've downloaded the ZENworks software, you are ready to install the ZENworks Primary Server and establish a management zone. The Primary Server manages the devices that register in the zone. For example, application and policy configurations are distributed by the Primary Server to the managed devices.

Refer to the appropriate section for installation instructions:

- Deploy the ZENworks Virtual Appliance (page 12)
- Install the ZENworks Software (page 13)

2.2.1 Deploy the ZENworks Virtual Appliance

1 Make sure the host machine has at least 16 GB RAM and 130 GB free disk space, and has a static IP address or a permanently leased dynamic (DHCP) IP address.

2 Import the ZENworks Virtual Appliance into your hypervisor to create a new virtual machine.

3. After the virtual machine has been created, add a second hard disk of size 40 GB. The first disk (90 MB) is used for the Appliance while the second disk (40 GB) will be used to store the ZENworks data.
4. Power on the new virtual machine.
5. Follow the prompts to configure the virtual machine and then the ZENworks Server and zone.

   For this evaluation, we recommend the following:

   - Create a new ZENworks Management Zone.
   - Use the embedded PostgreSQL database. Even if you use Oracle or MSSQL database in your environment, using the embedded PostgreSQL database is more convenient and quicker.
   - Use the internal Certificate Authority. Even if you use an external CA in your environment, using the internal CA is more convenient and quicker.

If you need more details, refer to the *ZENworks Appliance Deployment and Administration Reference (https://www.novell.com/documentation/zenworks-2020-update-2/zen_ca_appliance)*.

2.2.2 Install the ZENworks Software

1. Make sure the target server has at least 16 GB RAM and 80 GB free disk space, and has a static IP address or a permanently leased dynamic (DHCP) IP address.
2. Log in to the server as a user with administrative rights.
3. Mount the ZENworks ISO and run the installation program:
   - **Windows:** Run `setup.exe`.
   - **Linux:** Run `setup.sh`.
4. Complete the installation wizard.

   For this evaluation, we recommend the following:

   - Create a new ZENworks Management Zone.
   - Use the embedded PostgreSQL database. Even if you use Oracle or MSSQL database in your environment, using the embedded PostgreSQL database is more convenient and quicker.
   - Use the internal Certificate Authority. Even if you use an external CA in your environment, using the internal CA is more convenient and quicker.

If you need more details, refer to the *ZENworks 2020 Server Installation Guide (https://www.novell.com/documentation/zenworks-2020-update-2/zen_installation)*.

2.3 Connect to a User Source

ZENworks ties into your LDAP user directory (Microsoft Active Directory or NetIQ eDirectory) in order to provide user-based management of devices.

For mobile devices, a user source is required because device authentication and enrollment are both associated with the device’s user, not the device.

For workstations and laptops, a user source is not required; however, connecting to a user source provides device management based on both the device and the logged-in user.

- Select an Evaluation User (page 14)
- Connect to an LDAP Directory (page 14)

2.3.1 Select an Evaluation User

You need an LDAP user account that you can use for the evaluation. To enroll mobile devices with the user, you'll need to know the account credentials (username and password). You can use an existing account, or you can create an account. Throughout this evaluation, we use *ZENUser*.

2.3.2 Connect to an LDAP Directory

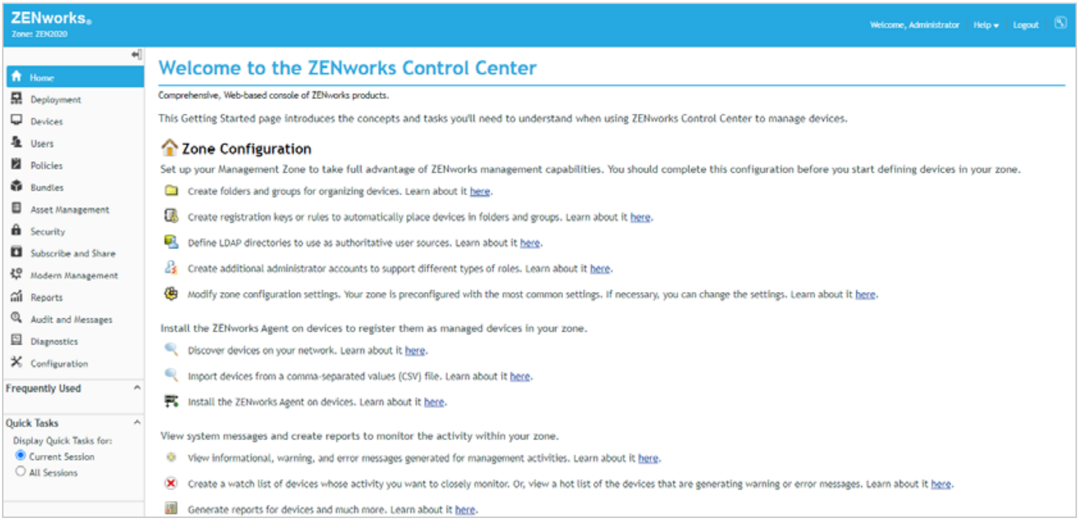
1 Log in to ZENworks Control Center:

1a In a web browser, enter the following URL:

```
https://ZENworks_Server_Address
```

Replace `ZENworks_Server_Address` with the IP address or DNS name of the ZENworks Primary Server.

1b Specify *Administrator* as the username, specify the password you defined during installation, then click **Login** to display the Welcome page.



Welcome to the ZENworks Control Center

Comprehensive, Web-based console of ZENworks products.

This Getting Started page introduces the concepts and tasks you'll need to understand when using ZENworks Control Center to manage devices.

Zone Configuration

Set up your Management Zone to take full advantage of ZENworks management capabilities. You should complete this configuration before you start defining devices in your zone.

Create folders and groups for organizing devices. Learn about it here.

Create registration keys or rules to automatically place devices in folders and groups. Learn about it here.

Define LDAP directories to use as authoritative user sources. Learn about it here.

Create additional administrator accounts to support different types of roles. Learn about it here.

Modify zone configuration settings. Your zone is preconfigured with the most common settings. If necessary, you can change the settings. Learn about it here.

Install the ZENworks Agent on devices to register them as managed devices in your zone.

Discover devices on your network. Learn about it here.

Import devices from a comma-separated values (CSV) file. Learn about it here.

Install the ZENworks Agent on devices. Learn about it here.

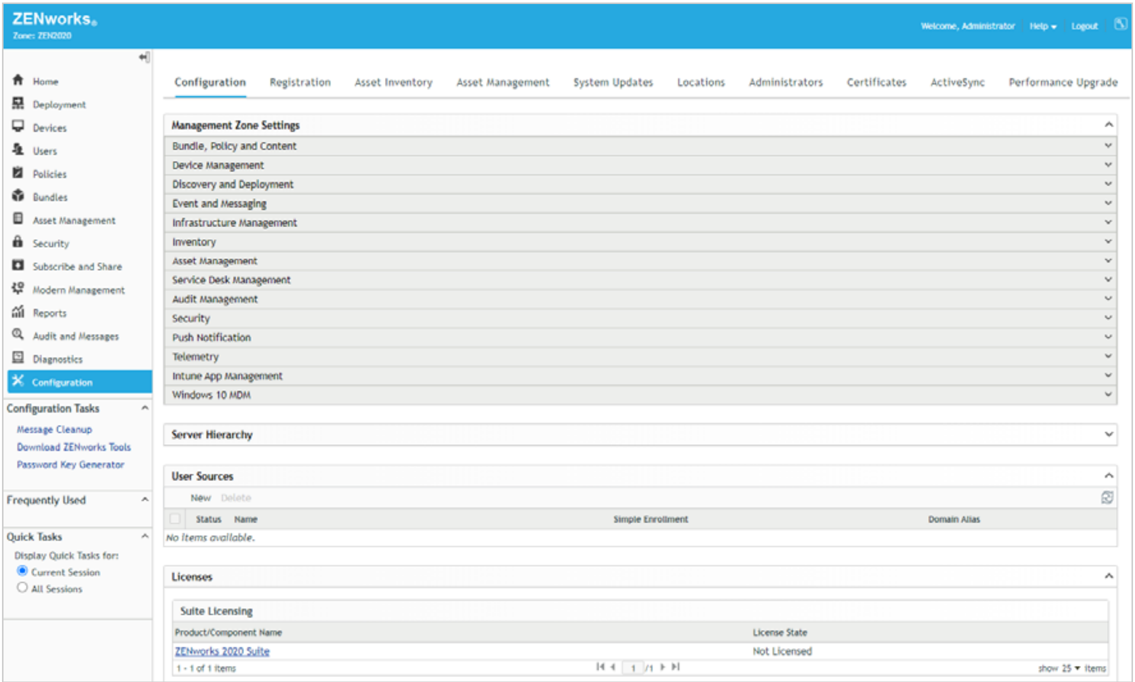
View system messages and create reports to monitor the activity within your zone.

View informational, warning, and error messages generated for management activities. Learn about it here.

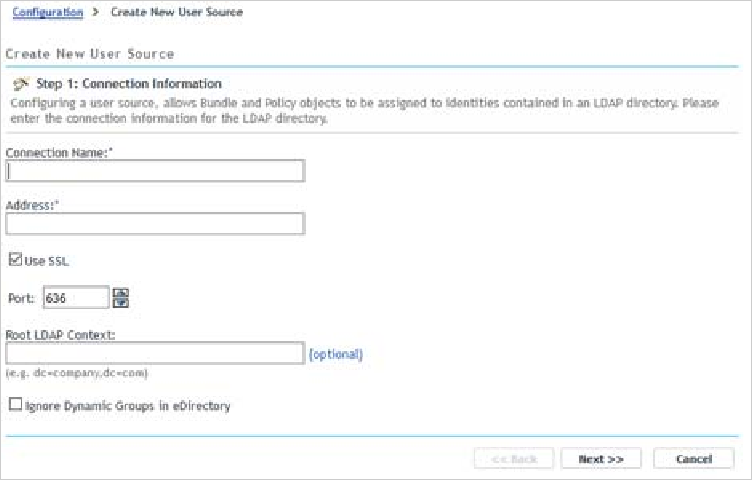
Create a watch list of devices whose activity you want to closely monitor. Or, view a hot list of the devices that are generating warning or error messages. Learn about it here.

Generate reports for devices and much more. Learn about it here.

2 Click **Configuration** (in the left navigation pane).



3 In the User Sources panel, click **New** to launch the Create New User Source wizard.


Configuration > Create New User Source
Create New User Source
Step 1: Connection Information

Configuring a user source, allows Bundle and Policy objects to be assigned to identities contained in an LDAP directory. Please enter the connection information for the LDAP directory.

Connection Name:*

Address:*

☑ Use SSL

Port: 636

Root LDAP Context: (optional)

(e.g. dc=company,dc=com)

☐ Ignore Dynamic Groups in eDirectory

4 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 LDAP directory server.
- **Use SSL:** Disable the option if the LDAP server is not using the Secure Socket Layer protocol.
- **Port:** If your LDAP server is not listening on a default port (636 or 389), select the correct port number.
- **Root LDAP Context:** The root context establishes the ZENworks entry point into the directory. If you don't specify a root context, the directory's root container is used.

- **Ignore Dynamic Groups in eDirectory:** Leave this option unchecked.

5 (Conditional) On the Certificate page (which is displayed only if the connection is using SSL), verify the certificate information, then click **Next**.

6 On the Credentials page, specify a Read-only username and password that ZENworks can use to access the directory, then click **Next**.

7 On the Authentication Mechanisms page, select **Username/Password**, then click **Next**.

8 On the User Containers page, add the container where your evaluation user resides, then click **Next**.

9 Complete the wizard.

2.4 Enable MDM Communication

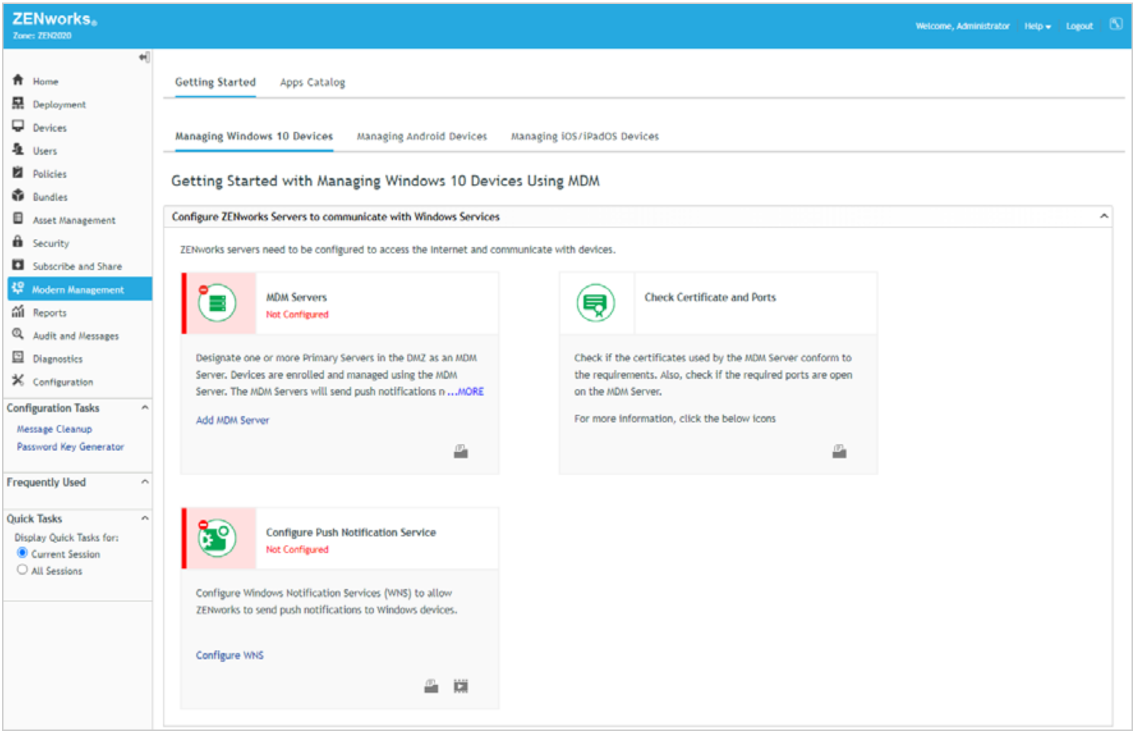
You need to complete several system configuration tasks to enable ZENworks to communicate with devices via their native push notification services. This includes defining your ZENworks Primary Server as a Mobile Device Management (MDM) Server and then connecting the MDM Server to the Windows, Apple, and Google push notification services.

- Designate an MDM Server (page 17)
- Enabling Push Notifications for Windows Devices (page 19)
- Enabling Push Notifications for iOS Devices (page 25)
- Enabling Push Notifications for Android Devices (page 28)

2.4.1 Designate an MDM Server

A ZENworks Management Zone must have at least one ZENworks Primary Server that is designated as an MDM Server. For this evaluation, you only have one ZENworks Primary Server, so you need to designate it as your MDM Server:

1 In ZENworks Control Center, click **Modern Management** (in the left navigation pane).



Getting Started with Managing Windows 10 Devices Using MDM

Configure ZENworks Servers to communicate with Windows Services

ZENworks servers need to be configured to access the internet and communicate with devices.

MDM Servers
Not Configured

Designate one or more Primary Servers in the DMZ as an MDM Server. Devices are enrolled and managed using the MDM Server. The MDM Servers will send push notifications n ...MORE

Check Certificate and Ports

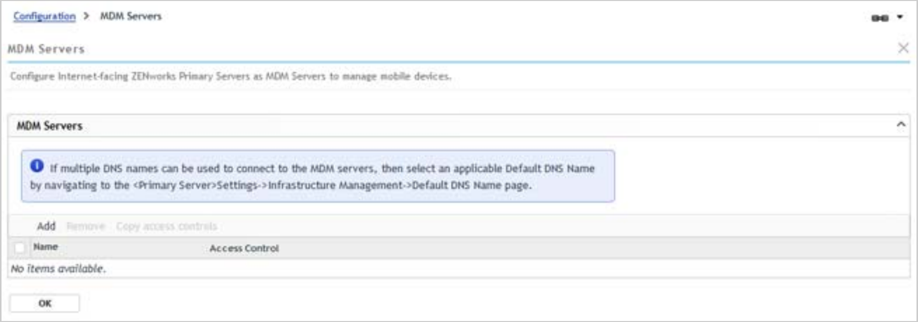
Check if the certificates used by the MDM Server conform to the requirements. Also, check if the required ports are open on the MDM Server.

For more information, click the below icons

Configure Push Notification Service
Not Configured

Configure Windows Notification Services (WNS) to allow ZENworks to send push notifications to Windows devices.

2 In the MDM Servers panel, click **Add MDM Server** to display the MDM Servers page.



MDM Servers

Configure Internet-facing ZENworks Primary Servers as MDM Servers to manage mobile devices.

MDM Servers

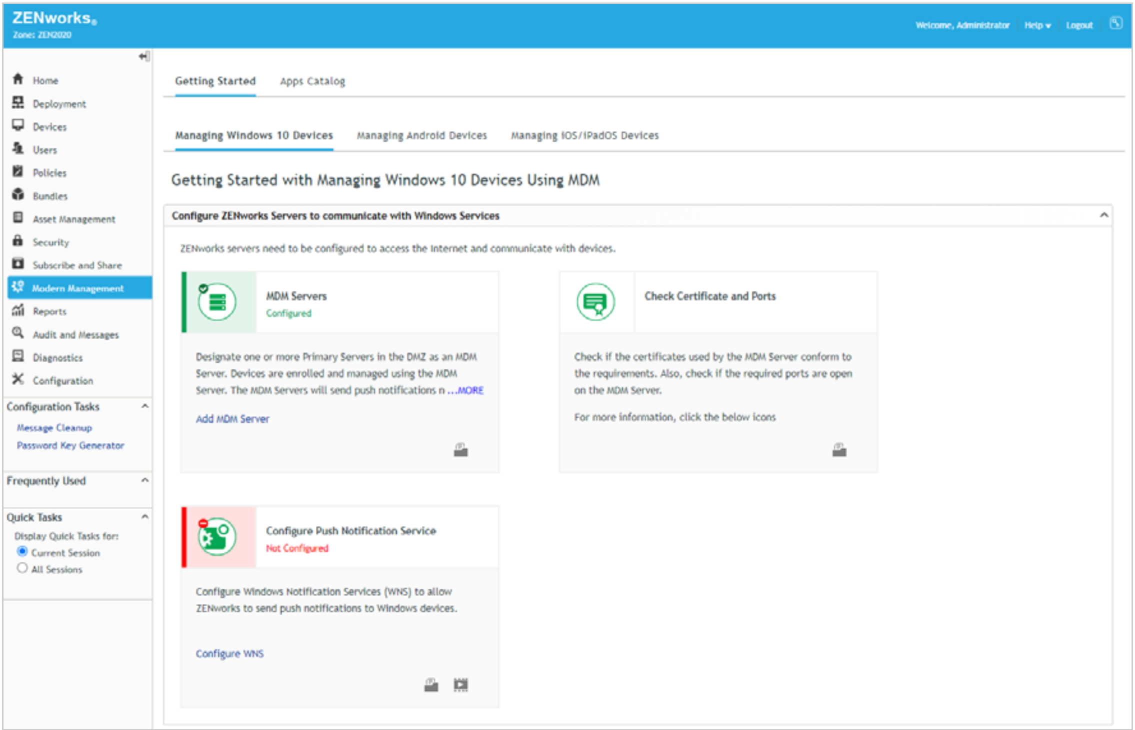
If multiple DNS names can be used to connect to the MDM servers, then select an applicable Default DNS Name by navigating to the <Primary Server>Settings->Infrastructure Management->Default DNS Name page.

☐	Name	Access Control
No items available.		

3 In the MDM Servers list, click **Add**, select your ZENworks Primary Server, then click **OK** to add it to the list.

4 Click **OK** to save the MDM Servers list.

You are returned to the Modern Management Getting Started and the MDM Servers panel shows that an MDM Server is configured.



Getting Started with Managing Windows 10 Devices Using MDM

Configure ZENworks Servers to communicate with Windows Services

ZENworks servers need to be configured to access the Internet and communicate with devices.

MDM Servers
Configured

Designate one or more Primary Servers in the DMZ as an MDM Server. Devices are enrolled and managed using the MDM Server. The MDM Servers will send push notifications n ...MORE

Add MDM Server

Check Certificate and Ports

Check if the certificates used by the MDM Server conform to the requirements. Also, check if the required ports are open on the MDM Server.

For more information, click the below icons

Configure Push Notification Service
Not Configured

Configure Windows Notification Services (WNS) to allow ZENworks to send push notifications to Windows devices.

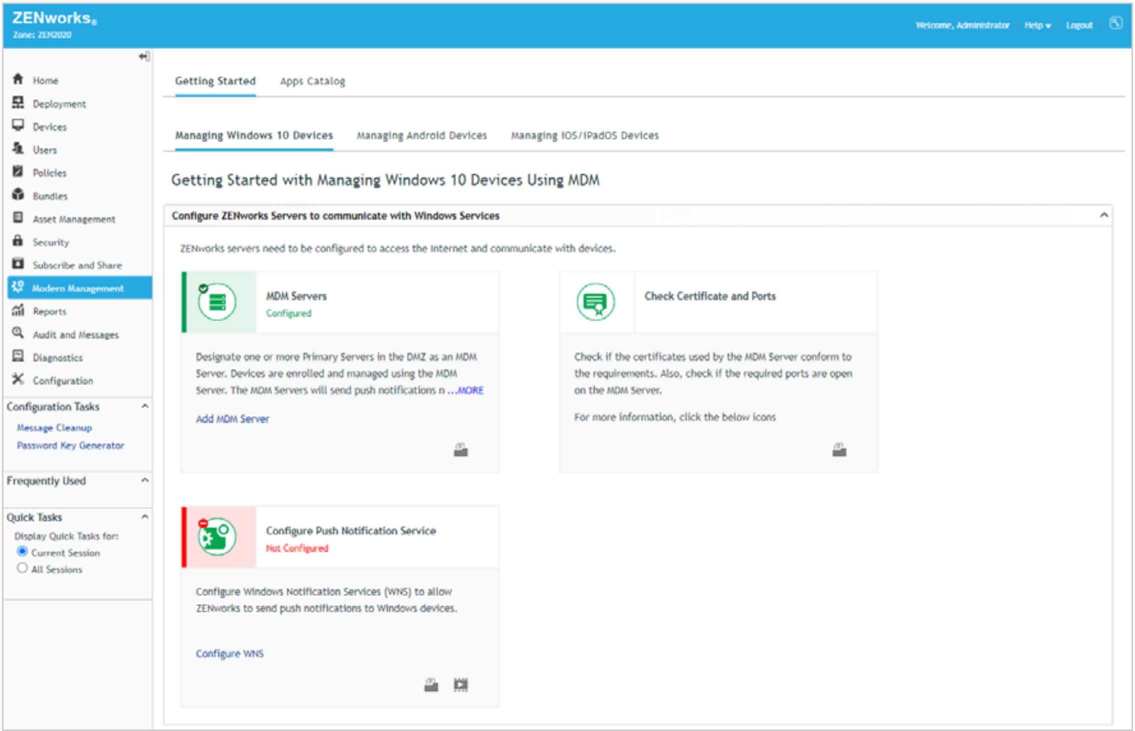
Configure WNS

2.4.2 Enabling Push Notifications for Windows Devices

Windows Notification Services (WNS) enables the ZENworks MDM Server to enroll and manage a Windows device. The ZENworks MDM Server authenticates to the Windows Notification Services which routes ZENworks notifications to the device.

In order to use Windows Notification Services, you must create a Windows app in the Microsoft Partner Center.

1 In ZENworks Control Center, make sure you are on Getting Started with Managing Windows 10 Devices Using MDM.



Getting Started with Managing Windows 10 Devices Using MDM

Configure ZENworks Servers to communicate with Windows Services

ZENworks servers need to be configured to access the Internet and communicate with devices.

MDM Servers
Configured

Designate one or more Primary Servers in the DMZ as an MDM Server. Devices are enrolled and managed using the MDM Server. The MDM Servers will send push notifications n ...MORE

Add MDM Server

Check Certificate and Ports

Check if the certificates used by the MDM Server conform to the requirements. Also, check if the required ports are open on the MDM Server.

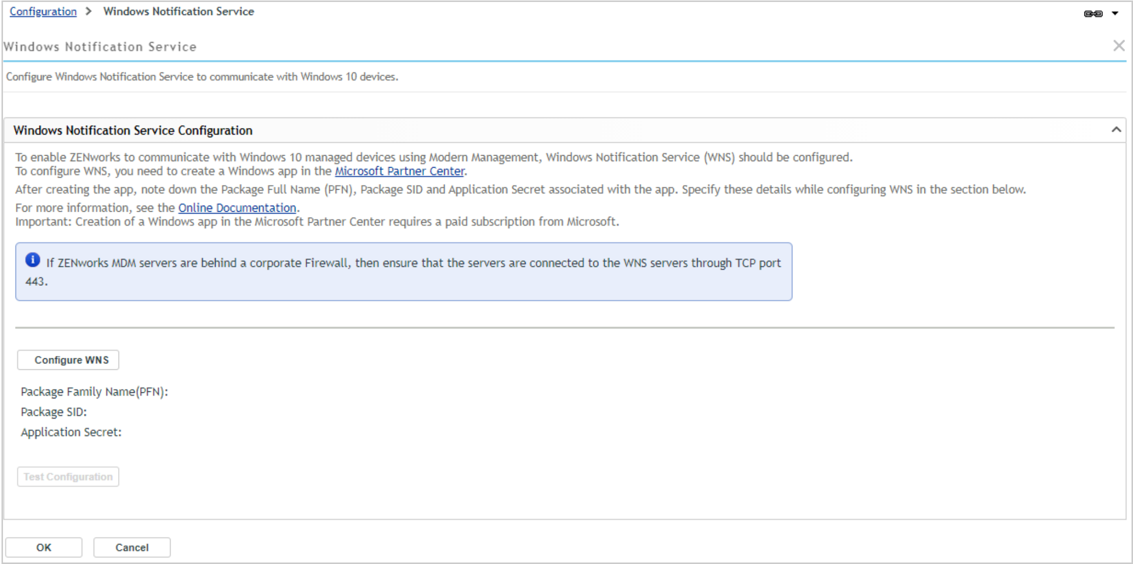
For more information, click the below icons

Configure Push Notification Service
Not Configured

Configure Windows Notification Services (WNS) to allow ZENworks to send push notifications to Windows devices.

Configure WNS

2 In the Configure Push Notification Services panel, click **Configure WNS** to display the Windows Notification Service settings.



Windows Notification Service

Configure Windows Notification Service to communicate with Windows 10 devices.

Windows Notification Service Configuration

To enable ZENworks to communicate with Windows 10 managed devices using Modern Management, Windows Notification Service (WNS) should be configured.
To configure WNS, you need to create a Windows app in the Microsoft Partner Center.
After creating the app, note down the Package Full Name (PFN), Package SID and Application Secret associated with the app. Specify these details while configuring WNS in the section below.
For more information, see the Online Documentation.
Important: Creation of a Windows app in the Microsoft Partner Center requires a paid subscription from Microsoft.

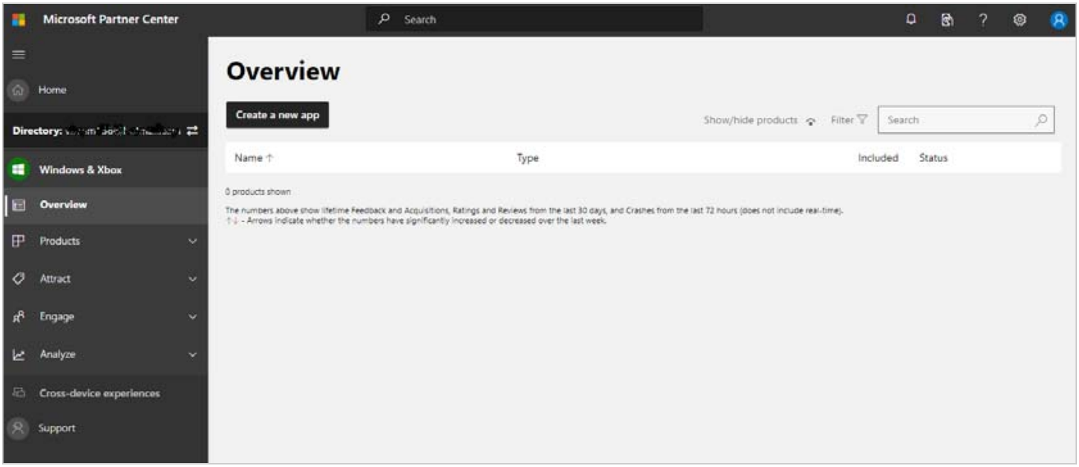
If ZENworks MDM servers are behind a corporate Firewall, then ensure that the servers are connected to the WNS servers through TCP port 443.

Package Family Name(PFN):
Package SID:
Application Secret:

3 Create a Windows app in Microsoft Partner Center:

3a Click **Microsoft Partner Center**.

3b Sign in with your account username and password to display the Overview.



Directory: [redacted]

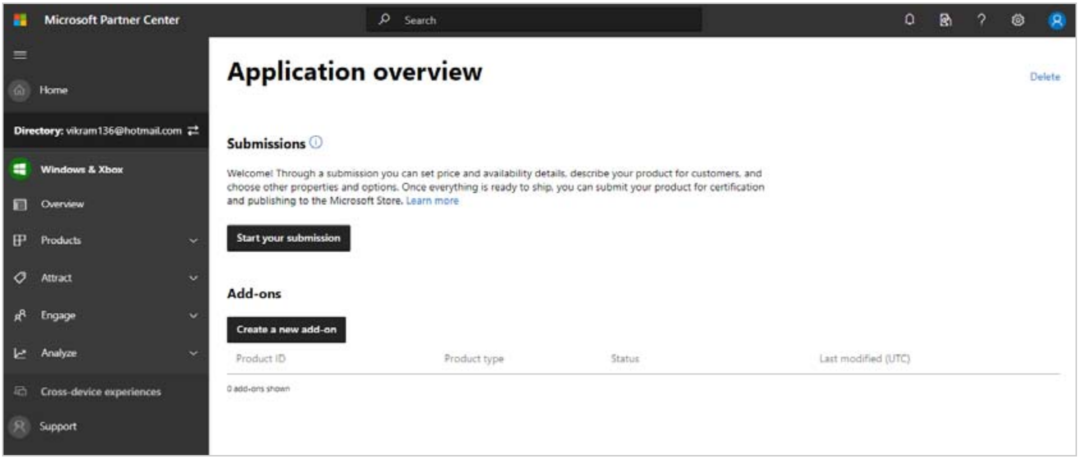
Name ↑	Type	Included	Status

0 products shown

The numbers above show lifetime Feedback and Acquisitions, Ratings and Reviews from the last 30 days, and Crashes from the last 72 hours (does not include real-time).
↑↓ - Arrows indicate whether the numbers have significantly increased or decreased over the last week.

3c Click **Create a new app**.

3d Enter a name (such as ZEN2020Eval), check its availability, then click **Reserve product name** to display the Application Overview.



Application overview

Submissions

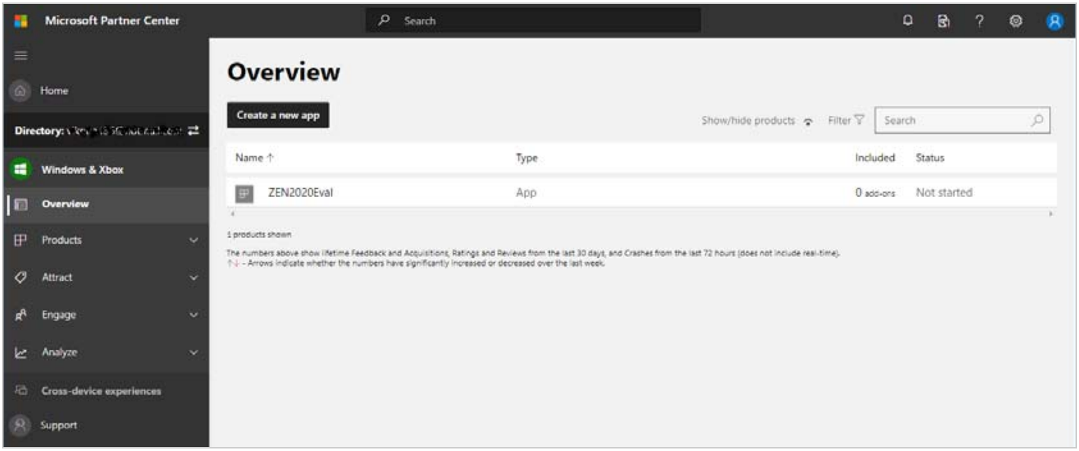
Welcome! Through a submission you can set price and availability details, describe your product for customers, and choose other properties and options. Once everything is ready to ship, you can submit your product for certification and publishing to the Microsoft Store. Learn more

Add-ons

Product ID	Product type	Status	Last modified (UTC)

0 add-ons shown

3e Click **Overview** (in the left navigation pane) to display the Overview list with the application you reserved.



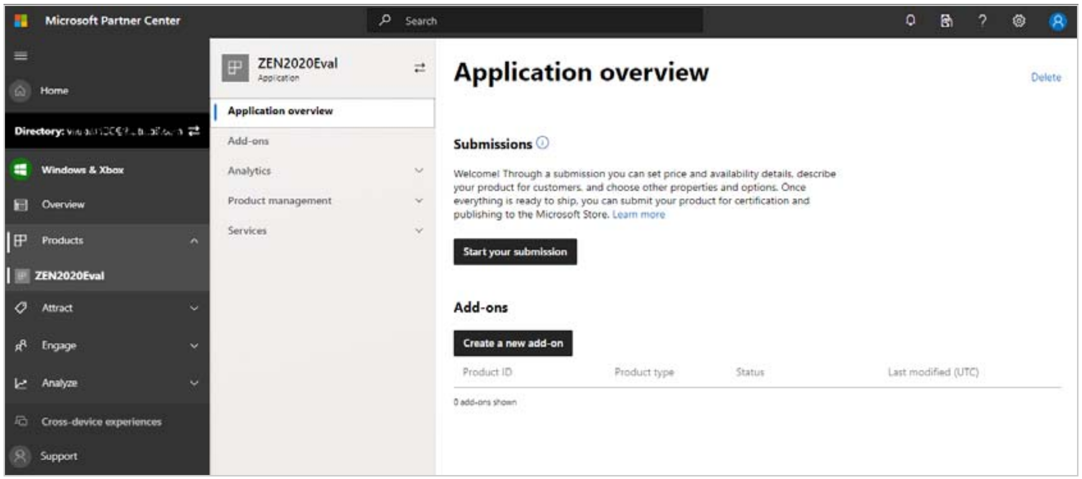
Overview

Name ↑	Type	Included	Status
ZEN2020Eval	App	0 add-ons	Not started

1 products shown

The numbers above show lifetime Feedback and Acquisitions, Ratings and Reviews from the last 30 days, and Crashes from the last 72 hours (does not include real-time).
↑↓ - Arrows indicate whether the numbers have significantly increased or decreased over the last week.

3f Click the application name to display the Application Overview.



Application overview

Submissions

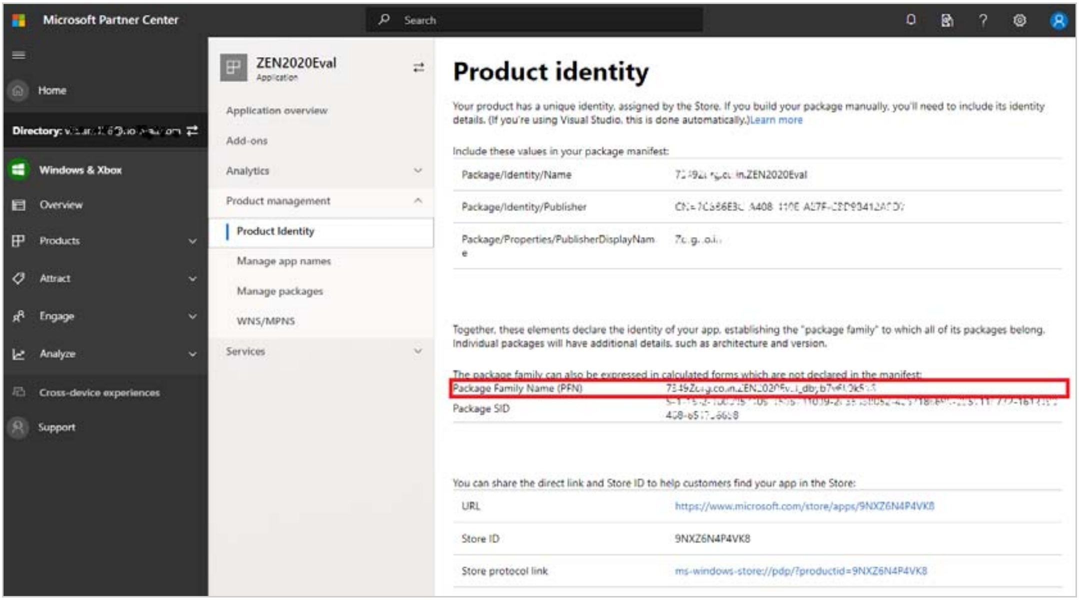
Welcome! Through a submission you can set price and availability details, describe your product for customers, and choose other properties and options. Once everything is ready to ship, you can submit your product for certification and publishing to the Microsoft Store. Learn more

Add-ons

Product ID	Product type	Status	Last modified (UTC)

0 add-ons shown

3g Click **Product management** > **Product Identity** to display the Product Identity.



Product identity

Your product has a unique identity, assigned by the Store. If you build your package manually, you'll need to include its identity details. (If you're using Visual Studio, this is done automatically.)Learn more

Include these values in your package manifest:

Package/Identity/Name	[redacted]
Package/Identity/Publisher	[redacted]
Package/Properties/PublisherDisplayName	[redacted]

Together, these elements declare the identity of your app, establishing the "package family" to which all of its packages belong. Individual packages will have additional details, such as architecture and version.

The package family can also be expressed in calculated forms which are not declared in the manifest:

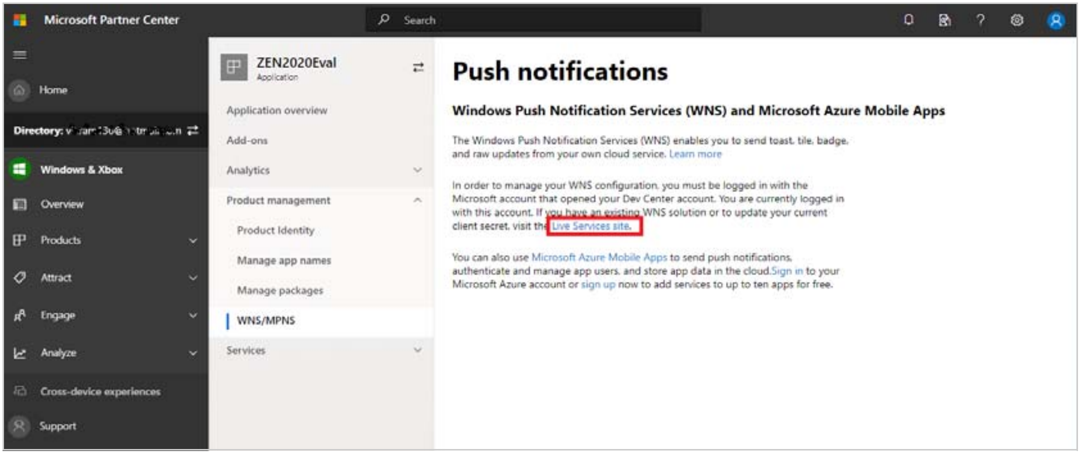
Package Family Name (PFN)	[redacted]
Package SID	[redacted]

You can share the direct link and Store ID to help customers find your app in the Store:

URL	https://www.microsoft.com/store/apps/9NXZ6N4P4VK8
Store ID	9NXZ6N4P4VK8
Store protocol link	ms-windows-store://pdp/?productid=9NXZ6N4P4VK8

3h Copy the Package Family Name (PFN) to a text editor. You'll copy two additional pieces of information to the text editor in the next few steps so label the PFN to identify it.

3i Click **WNS/MPNS** to display the Push Notifications.



Push notifications

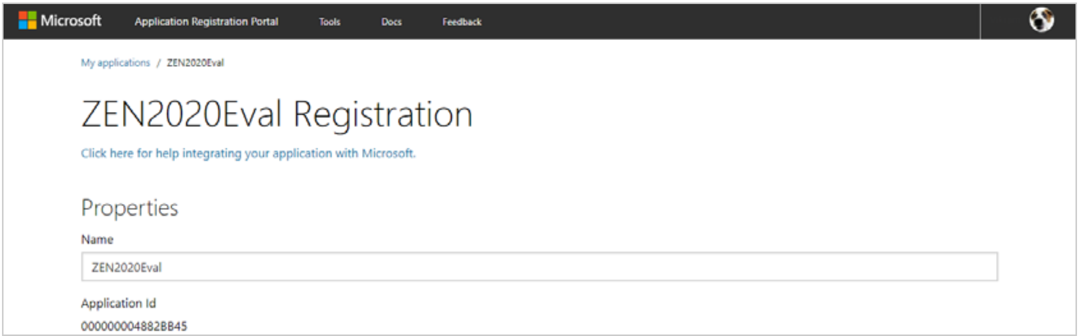
Windows Push Notification Services (WNS) and Microsoft Azure Mobile Apps

The Windows Push Notification Services (WNS) enables you to send toast, tile, badge, and raw updates from your own cloud service. Learn more

In order to manage your WNS configuration, you must be logged in with the Microsoft account that opened your Dev Center account. You are currently logged in with this account. If you have an existing WNS solution or to update your current client secret, visit the Live Services site.

You can also use Microsoft Azure Mobile Apps to send push notifications, authenticate and manage app users, and store app data in the cloud.Sign in to your Microsoft Azure account or sign up now to add services to up to ten apps for free.

3j Click the **Live Services Site** link to display the following page.


Microsoft
Application Registration Portal
Tools
Docs
Feedback
My applications / ZEN2020Eval

ZEN2020Eval Registration

Click here for help integrating your application with Microsoft.

Properties

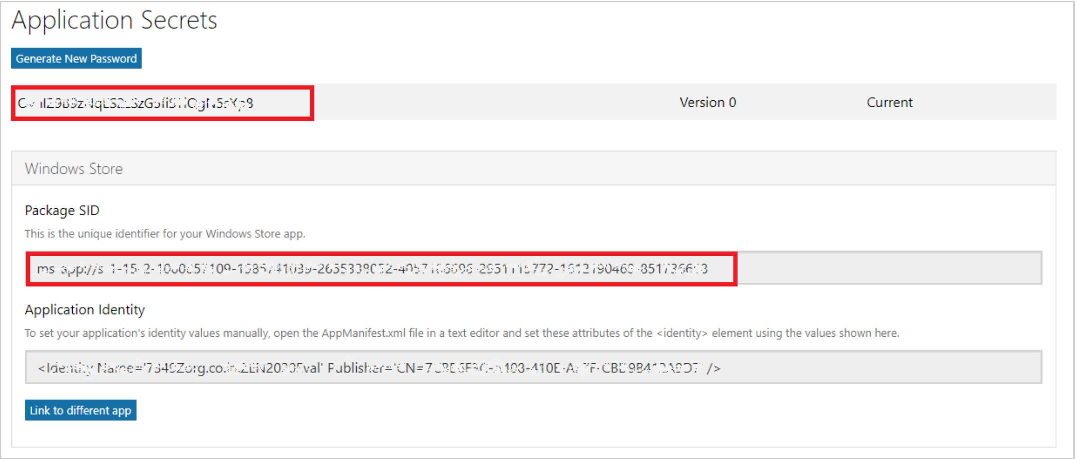
Name

ZEN2020Eval

Application Id

000000004882BB45

3k Copy the Application Secrets and the Package SID to a text editor and label them to identify them.



Application Secrets

C~ilZ9B9zNqLS2LSzGoliS1QgI.5rXp8	Version 0	Current

Windows Store

Package SID

This is the unique identifier for your Windows Store app.

ms-app://s-1-15-2-1000857109-1385741039-2655339052-4057106096-2951115772-1512190460-3517356613

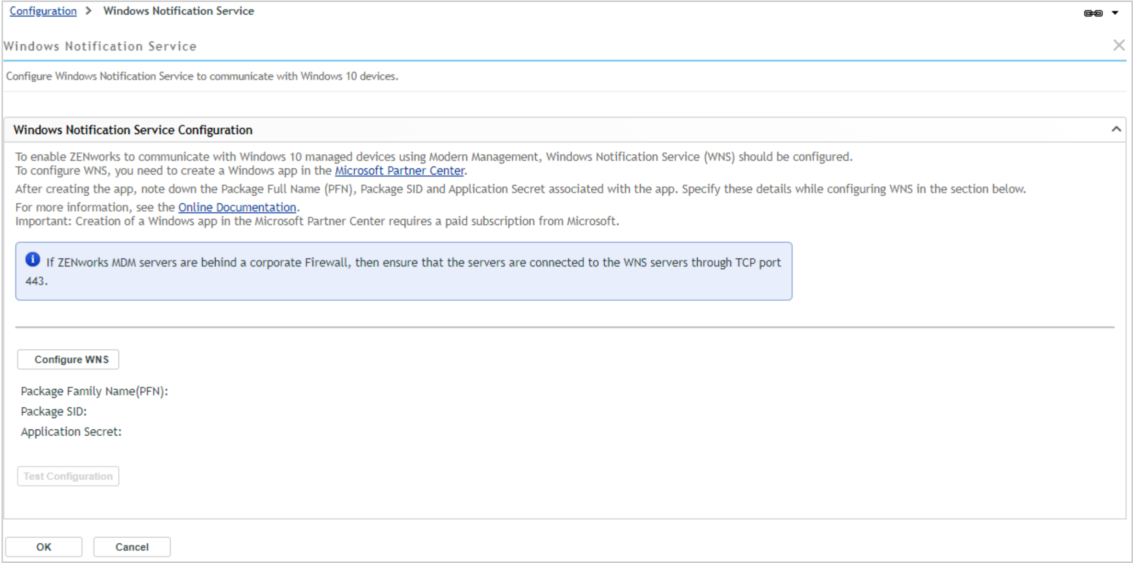
Application Identity

To set your application's identity values manually, open the AppManifest.xml file in a text editor and set these attributes of the <identity> element using the values shown here.

<Identity Name='7349Zorg.co.in.ZEN2020Eval' Publisher='CN=7[illegible]BE3F8C-[illegible]103-410E-A[illegible]7F-CBD9B412A9D7' />

3l Log out of Microsoft Partner Center.

4 In ZENworks Control Center, return to the Windows Notification Service settings.



Configuration > Windows Notification Service

Windows Notification Service

Configure Windows Notification Service to communicate with Windows 10 devices.

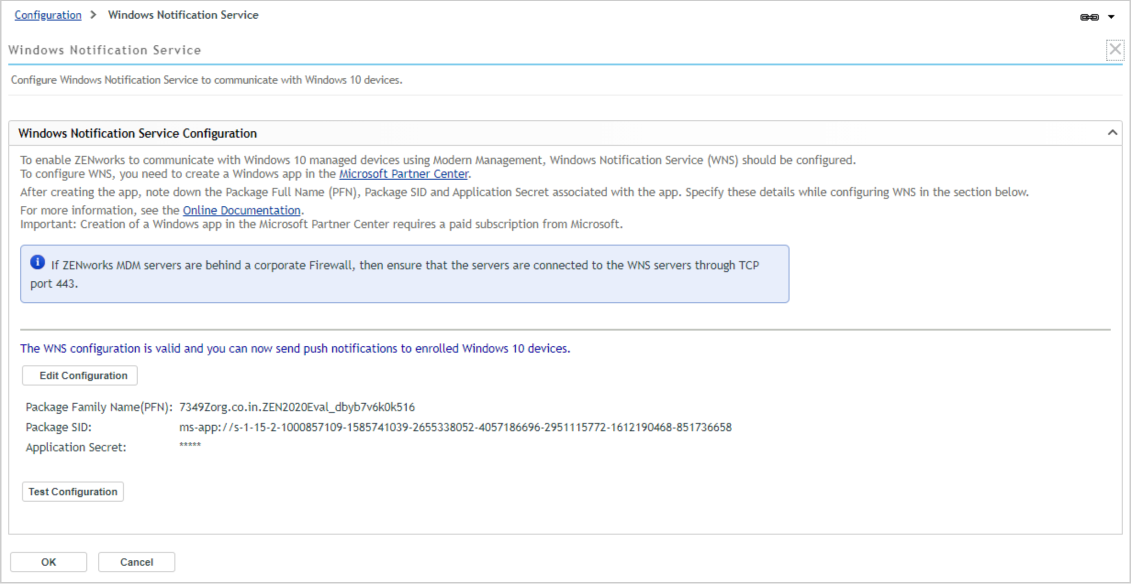
Windows Notification Service Configuration

To enable ZENworks to communicate with Windows 10 managed devices using Modern Management, Windows Notification Service (WNS) should be configured.
To configure WNS, you need to create a Windows app in the Microsoft Partner Center.
After creating the app, note down the Package Full Name (PFN), Package SID and Application Secret associated with the app. Specify these details while configuring WNS in the section below.
For more information, see the Online Documentation.
Important: Creation of a Windows app in the Microsoft Partner Center requires a paid subscription from Microsoft.

If ZENworks MDM servers are behind a corporate Firewall, then ensure that the servers are connected to the WNS servers through TCP port 443.

Package Family Name(PFN):
Package SID:
Application Secret:

5 Click **Configure WNS**, provide the Package Family Name (PFN), Package SID, and Application Secret from your Windows app, then click **OK**.



Windows Notification Service

Configure Windows Notification Service to communicate with Windows 10 devices.

Windows Notification Service Configuration

To enable ZENworks to communicate with Windows 10 managed devices using Modern Management, Windows Notification Service (WNS) should be configured.
To configure WNS, you need to create a Windows app in the Microsoft Partner Center.
After creating the app, note down the Package Full Name (PFN), Package SID and Application Secret associated with the app. Specify these details while configuring WNS in the section below.
For more information, see the Online Documentation.
Important: Creation of a Windows app in the Microsoft Partner Center requires a paid subscription from Microsoft.

If ZENworks MDM servers are behind a corporate Firewall, then ensure that the servers are connected to the WNS servers through TCP port 443.

The WNS configuration is valid and you can now send push notifications to enrolled Windows 10 devices.

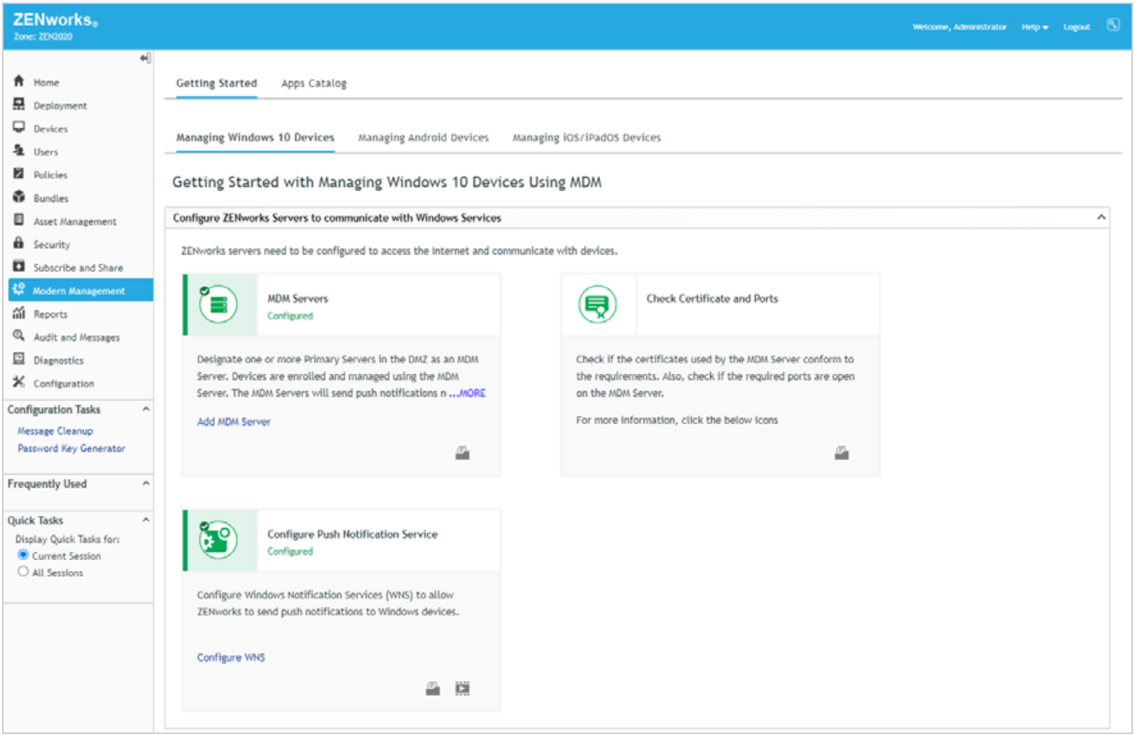
Package Family Name(PFN): 7349Zorg.co.in.ZEN2020Eval_dbyb7v6k0k516
Package SID: ms-app://s-1-15-2-1000857109-1585741039-2655338052-4057186696-2951115772-1612190468-851736658
Application Secret: *****

6 Click **Test Configuration** to validate the configuration.

7 Click **OK** to close the Windows Notification Services page.

8 Return to the Getting Started with Managing Windows 10 Devices Using MDM.

Windows Push Notification Service shows as successfully configured.



Display Quick Tasks for:
● Current Session
○ All Sessions

Getting Started with Managing Windows 10 Devices Using MDM

Configure ZENworks Servers to communicate with Windows Services

ZENworks servers need to be configured to access the internet and communicate with devices.

MDM Servers
Configured

Designate one or more Primary Servers in the DMZ as an MDM Server. Devices are enrolled and managed using the MDM Server. The MDM Servers will send push notifications n ...MORE

Check Certificate and Ports

Check if the certificates used by the MDM Server conform to the requirements. Also, check if the required ports are open on the MDM Server.

For more information, click the below icons

Configure Push Notification Service
Configured

Configure Windows Notification Services (WNS) to allow ZENworks to send push notifications to Windows devices.

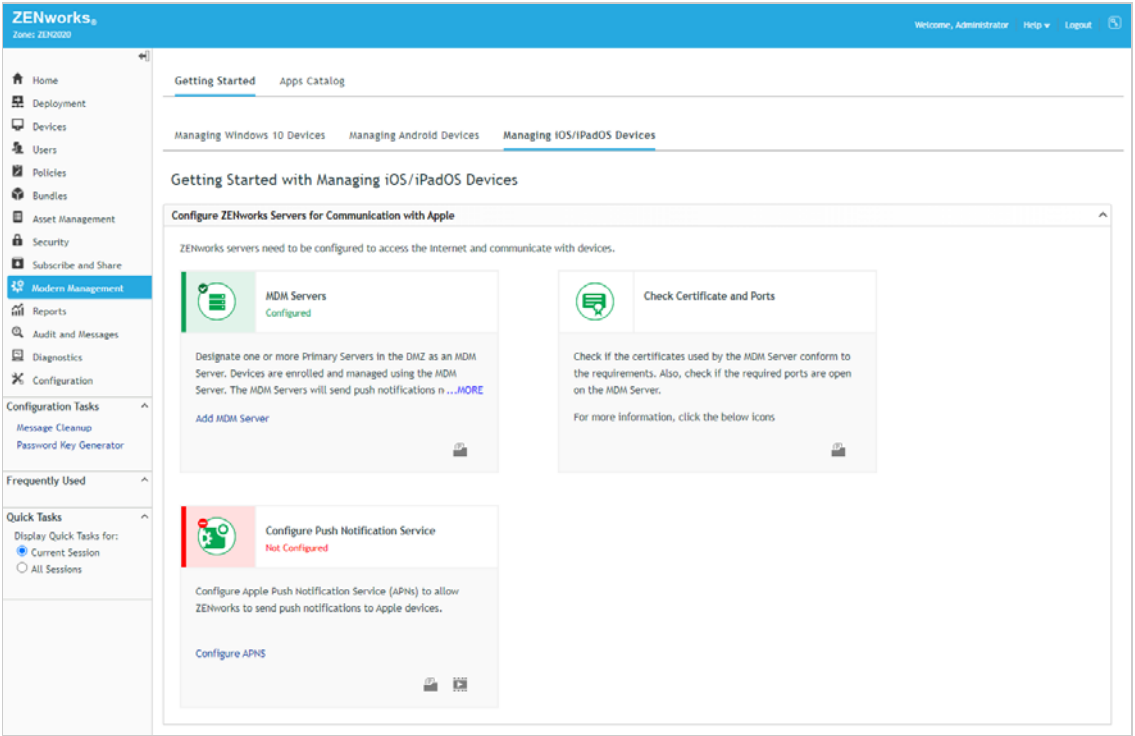
2.4.3 Enabling Push Notifications for iOS Devices

Apple Push Notification service (APNs) enables the ZENworks MDM Server to notify an iOS device when the server requires information from the device or has changes for the device. The ZENworks Primary 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 MDM Server directly to provide the requested information or receive the changes.

In order to use the Apple Push Notification service, an Apple Push Notification service certificate is required. The APNs certificate allows the ZENworks MDM Server and iOS devices to authenticate securely to the service.

Apple Push Notification service certificates are issued by Apple. The following steps help you create the Certificate Signing Request (CSR), submit the request to Apple, and import the Apple-issued APNs certificate into your ZENworks zone.

1 In ZENworks Control Center, go to Getting Started with Managing iOS/iPadOS Devices.



Getting Started with Managing iOS/iPadOS Devices

Configure ZENworks Servers for Communication with Apple

ZENworks servers need to be configured to access the internet and communicate with devices.

MDM Servers
Configured

Designate one or more Primary Servers in the DMZ as an MDM Server. Devices are enrolled and managed using the MDM Server. The MDM Servers will send push notifications n ...MORE

Add MDM Server

Check Certificate and Ports

Check if the certificates used by the MDM Server conform to the requirements. Also, check if the required ports are open on the MDM Server.

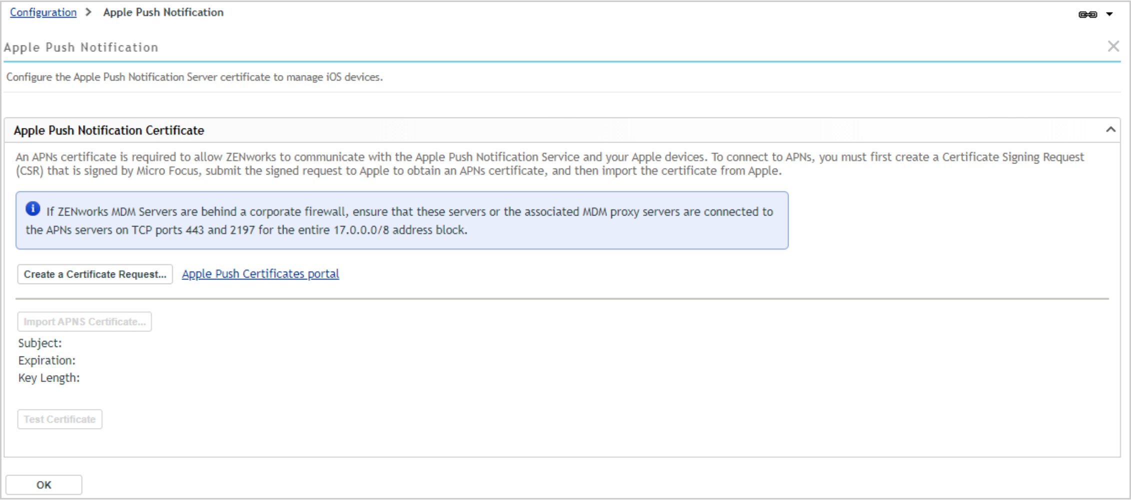
For more information, click the below icons

Configure Push Notification Service
Not Configured

Configure Apple Push Notification Service (APNs) to allow ZENworks to send push notifications to Apple devices.

Configure APNS

2 In the Configure Push Notification Service panel, click **Configure APNS** to display the Apple Push Notification service settings.



Configuration > Apple Push Notification

Apple Push Notification

Configure the Apple Push Notification Server certificate to manage iOS devices.

Apple Push Notification Certificate

An APNs certificate is required to allow ZENworks to communicate with the Apple Push Notification Service and your Apple devices. To connect to APNs, you must first create a Certificate Signing Request (CSR) that is signed by Micro Focus, submit the signed request to Apple to obtain an APNs certificate, and then import the certificate from Apple.

If ZENworks MDM Servers are behind a corporate firewall, ensure that these servers or the associated MDM proxy servers are connected to the APNs servers on TCP ports 443 and 2197 for the entire 17.0.0.0/8 address block.

Create a Certificate Request...
Apple Push Certificates portal
Import APNS Certificate...

Subject:
Expiration:
Key Length:

3 Create a Certificate Signing Request:

3a Click **Create a Certificate Request**.

3b Fill in the certificate details needed in the request:

Organization Apple ID: Specify a valid Apple ID in email format (for example, *apns@microfocus.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 personal account.

Organization Unit: Specify the 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: Specify the name of your organization. For example, *Micro Focus*.

City or Locality/State/Country: Specify the location information for your organization.

Key Length: Specify the key length that satisfies your corporate policy.

3c For the Micro Focus (Novell) Customer Center credentials, use **ZENeval** as the username and **zeneval!** as the password).

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

3d Click **Submit for Signing**.

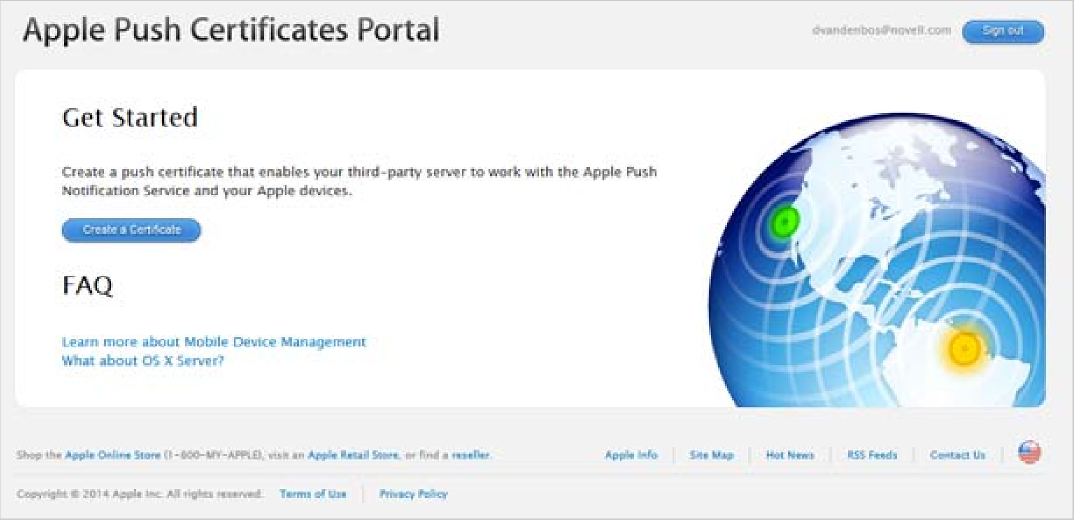
3e After the Certificate Signing Request file is signed by Micro Focus, save the signed CSR file to a location of your choice.

If desired, you can change the default filename, `apns-novell.csr`, before saving the file.

4 Submit the Certificate Request to Apple:

4a Click **Apple Push Certificates Portal** to open the Apple Push Certificates Portal web site.

4b Sign in with your Apple ID and password.



Apple Push Certificates Portal

dvandenbos@novell.com Sign out

Get Started

Create a push certificate that enables your third-party server to work with the Apple Push Notification Service and your Apple devices.

Create a Certificate

FAQ

Learn more about Mobile Device Management
What about OS X Server?

Shop the Apple Online Store (1-800-MY-APPLE), visit an Apple Retail Store, or find a reseller. Apple Info | Site Map | Hot News | RSS Feeds | Contact Us |

Copyright © 2014 Apple Inc. All rights reserved. Terms of Use | Privacy Policy

4c Click **Create a Certificate**, then follow the prompts to upload your Certificate Signing Request file and create an APNs certificate.

4d After the APNs certificate is created, download the certificate.

5 Import the APNs Certificate:

5a Click **Import APNs Certificate**.

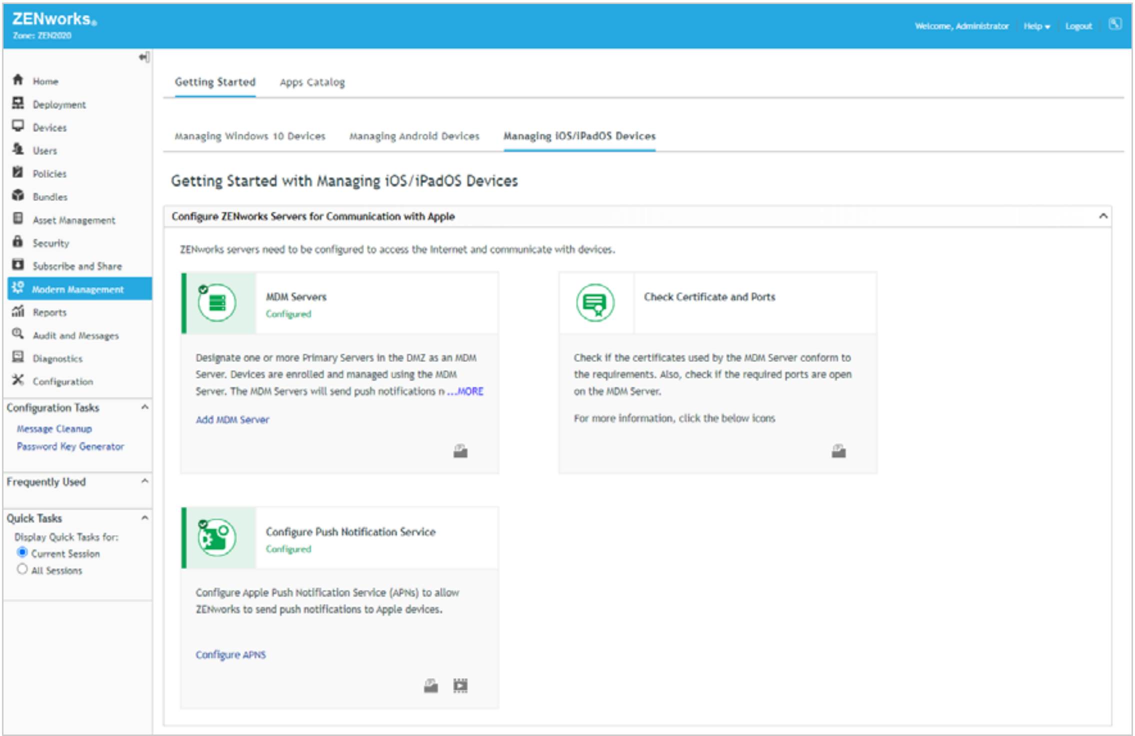
5b Browse for and select the APNs certificate file, then click **OK**.

The default name for the certificate file is `MDM_ Novell Inc_Certificate.pem`. The certificate is imported into your zone and the certificate’s subject, expiration date, and key length are displayed.

5c To check that the certificate is valid and that your ZENworks MDM Server can communicate with the Apple Push Notification service, click **Test Certificate**.

6 Click **OK** to save your Apple Push Notification changes.

You are returned to the Getting Started and the Configure Push Notification Service panel shows that an Apple Push Notification services is configured.



Display Quick Tasks for:
● Current Session
○ All Sessions

Getting Started with Managing iOS/iPadOS Devices

Configure ZENworks Servers for Communication with Apple

ZENworks servers need to be configured to access the Internet and communicate with devices.

MDM Servers
Configured

Designate one or more Primary Servers in the DMZ as an MDM Server. Devices are enrolled and managed using the MDM Server. The MDM Servers will send push notifications n ...MORE

Check Certificate and Ports

Check if the certificates used by the MDM Server conform to the requirements. Also, check if the required ports are open on the MDM Server.

For more information, click the below icons

Configure Push Notification Service
Configured

Configure Apple Push Notification Service (APNs) to allow ZENworks to send push notifications to Apple devices.

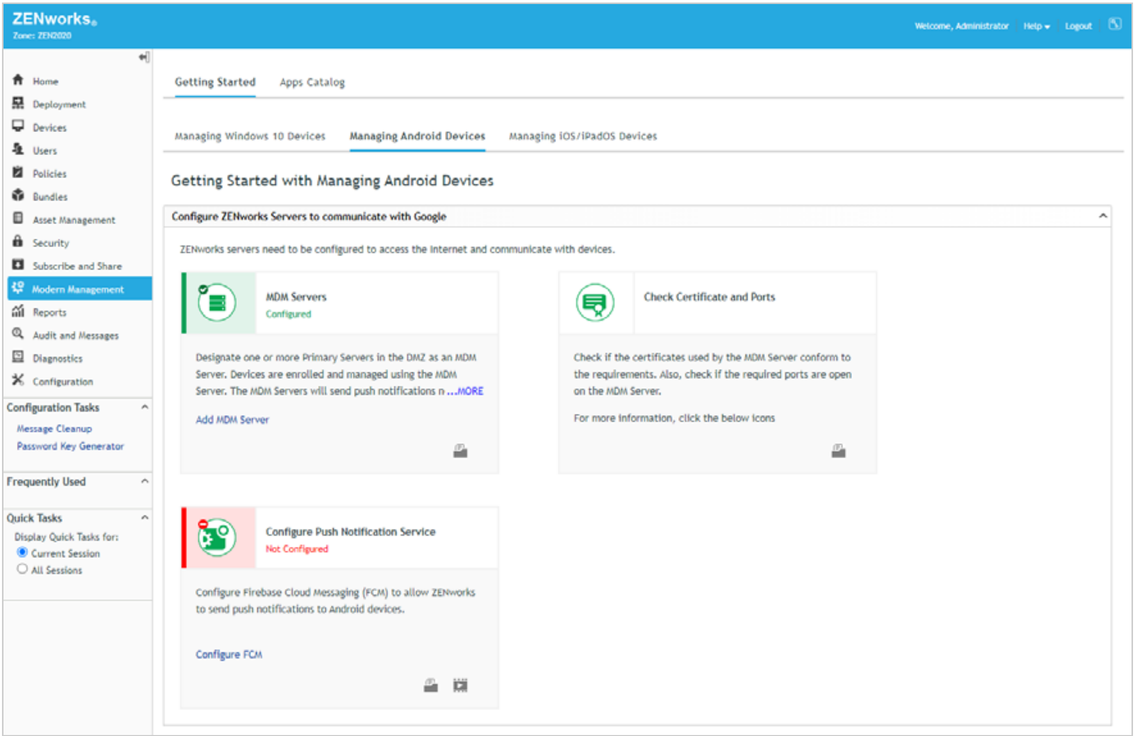
2.4.4 Enabling Push Notifications for Android Devices

Firebase Cloud Messaging (FCM) 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 MDM Server communicates with the Firebase Cloud Messaging service, which then pushes the notification to the device. After receiving the push notification, the device contacts the MDM Server directly to provide the requested information or receive the changes.

In order to use Firebase Cloud Messaging, you must have an existing Firebase project or use the Firebase Console to create a Firebase project. The Firebase project provides the api/server key and project/sender ID used by your MDM Server to send notifications to Android devices.

1 In ZENworks Control Center, go to Getting Started with Managing Android Devices.



Getting Started with Managing Android Devices

Configure ZENworks Servers to communicate with Google

ZENworks servers need to be configured to access the internet and communicate with devices.

MDM Servers
Configured

Designate one or more Primary Servers in the DMZ as an MDM Server. Devices are enrolled and managed using the MDM Server. The MDM Servers will send push notifications n ...MORE

Add MDM Server

Check Certificate and Ports

Check if the certificates used by the MDM Server conform to the requirements. Also, check if the required ports are open on the MDM Server.

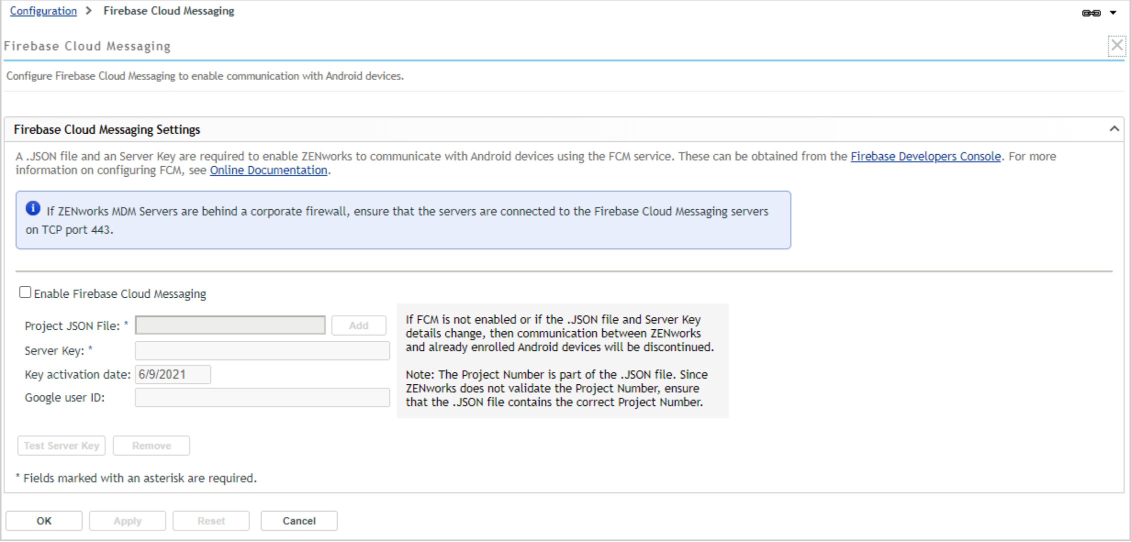
For more information, click the below icons

Configure Push Notification Service
Not Configured

Configure Firebase Cloud Messaging (FCM) to allow ZENworks to send push notifications to Android devices.

Configure FCM

2 In the Configure Push Notification Service panel, click **Configure FCM** to display the Firebase Cloud Messaging settings.



Configuration > Firebase Cloud Messaging

Firebase Cloud Messaging

Configure Firebase Cloud Messaging to enable communication with Android devices.

Firebase Cloud Messaging Settings

A .JSON file and an Server Key are required to enable ZENworks to communicate with Android devices using the FCM service. These can be obtained from the Firebase Developers Console. For more information on configuring FCM, see Online Documentation.

If ZENworks MDM Servers are behind a corporate firewall, ensure that the servers are connected to the Firebase Cloud Messaging servers on TCP port 443.

□ Enable Firebase Cloud Messaging

Project JSON File: *
Server Key: *
Key activation date: 6/9/2021
Google user ID:

If FCM is not enabled or if the .JSON file and Server Key details change, then communication between ZENworks and already enrolled Android devices will be discontinued.

Note: The Project Number is part of the .JSON file. Since ZENworks does not validate the Project Number, ensure that the .JSON file contains the correct Project Number.

* Fields marked with an asterisk are required.

3 Create a Firebase Project:

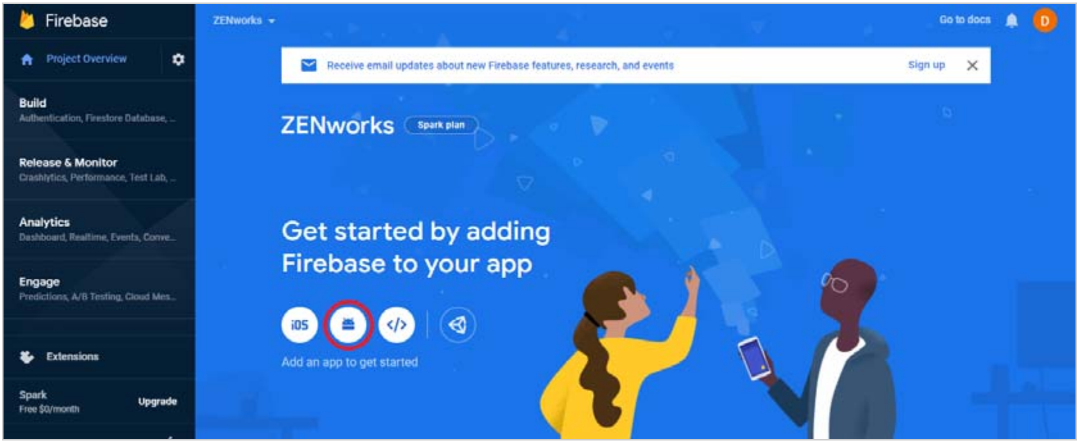
3a Click **Firebase Developers Console**.

3b Sign in using your Google account credentials.

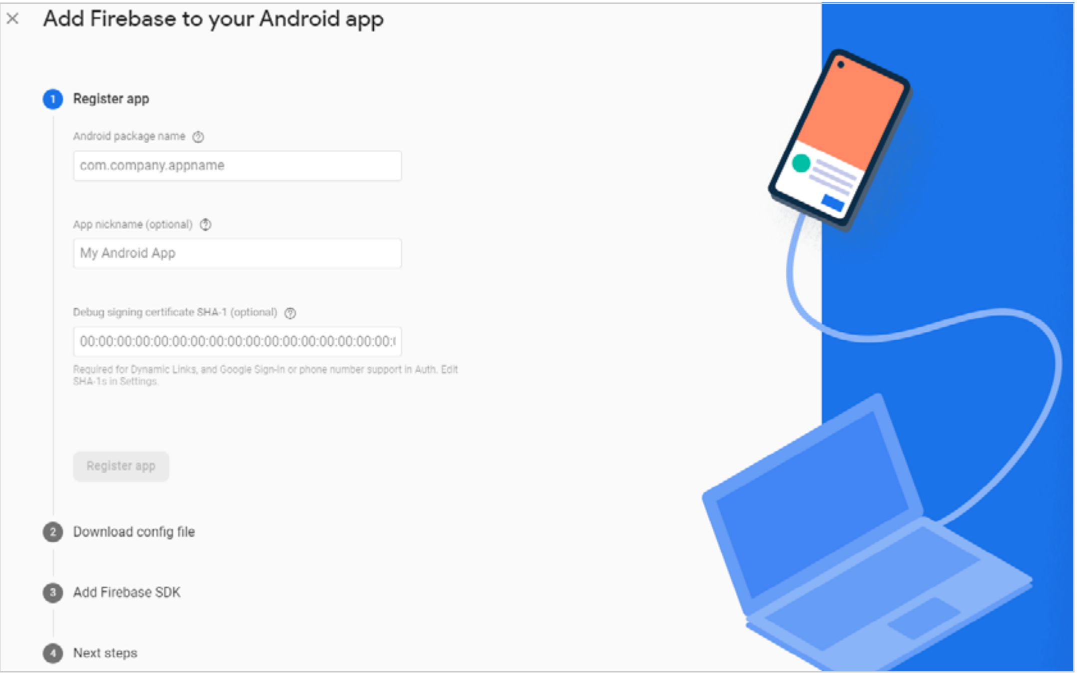
Best practice dictates that this should be Google account created specifically for managing your corporate Firebase projects and not a personal Google account.

3c Click **Create a Project**, supply a name for your project (such as ZENworks) and follow the remaining prompts to create the project.

3d After the project is created, the Firebase Console is displayed.


Firebase
Project Overview
Build
Authentication, Firestore Database, ...
Release & Monitor
Crashlytics, Performance, Test Lab, ...
Analytics
Dashboard, Realtime, Events, Conve...
Engage
Predictions, A/B Testing, Cloud Mes...
Extensions
Spark
Free $0/month
Upgrade
ZENworks
Go to docs
D
Receive email updates about new Firebase features, research, and events
Sign up
ZENworks
Spark plan
Get started by adding Firebase to your app
iOS
</>
Add an app to get started

3e Click the Android app icon (circled in red above) to display the app registration page.



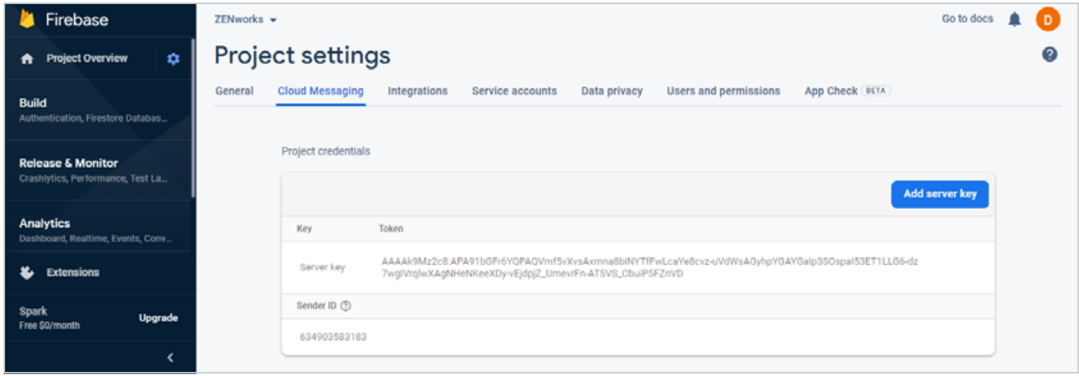
3f In the *Android package name* field, enter `com.novell.zapp`, then click **Register app**.

3g Click **Download google-services.json** to download the .JSON file.

3h Click **Next**, click **Next** in the Add Firebase SDK section to skip it, then click **Continue to console** to the Firebase console.

3i In the console's upper-left corner, click the ⚙ icon, then click **Project Settings**.

3j Click Cloud Messaging.



Project credentials

Key	Token
Server key	AAAAk9Mz2c8:APA91bGFr6YQPAQVmf5vXvsAxmna8biNYTfFwLcaYe8cvz-uVdWsAGyhpYGAYGalp3SOspal53ET1LLG6-dz 7wglVrqlwXAgNHeNKeeXDy-vEjdpjZ_UmevrFn-AT5VS_CbuiP5FZnVD

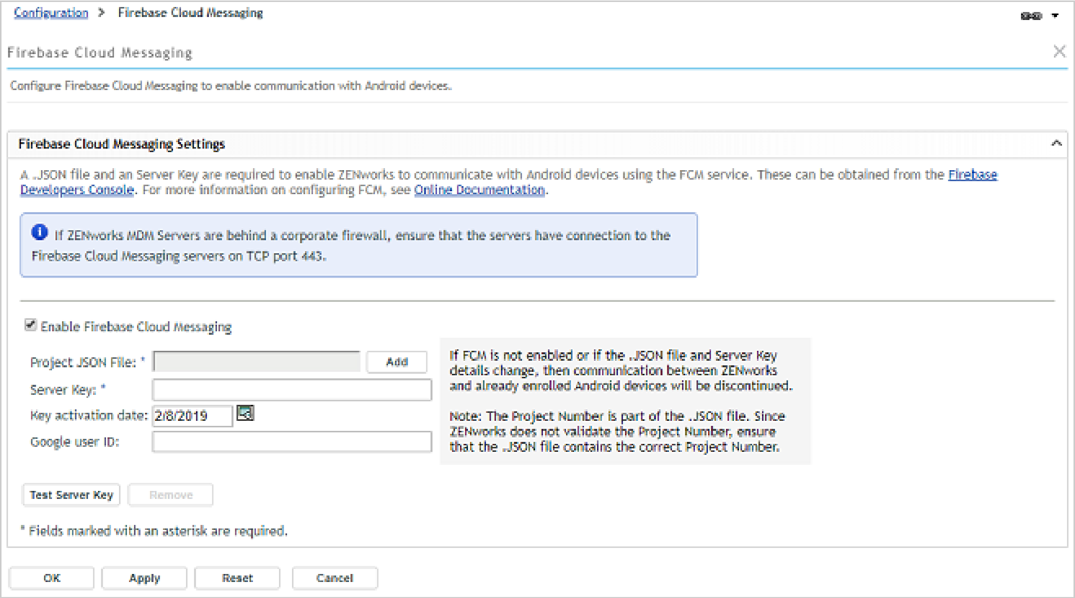
Sender ID

634903583183

3k Copy the Server Key so that you can paste it into ZENworks Control Center.

4 Configure ZENworks with the JSON file and Server Key:

4a In ZENworks Control Center (in the Firebase Cloud Messing settings), click the Enable Firebase Cloud Messaging check box to turn on the option.



Firebase Cloud Messaging

Configure Firebase Cloud Messaging to enable communication with Android devices.

Firebase Cloud Messaging Settings

A .JSON file and an Server Key are required to enable ZENworks to communicate with Android devices using the FCM service. These can be obtained from the Firebase Developers Console. For more information on configuring FCM, see Online Documentation.

If ZENworks MDM Servers are behind a corporate firewall, ensure that the servers have connection to the Firebase Cloud Messaging servers on TCP port 443.

☑ Enable Firebase Cloud Messaging

Project JSON File: *

Server Key: *

Key activation date: 2/8/2019

Google user ID:

If FCM is not enabled or if the .JSON file and Server Key details change, then communication between ZENworks and already enrolled Android devices will be discontinued.

Note: The Project Number is part of the .JSON file. Since ZENworks does not validate the Project Number, ensure that the .JSON file contains the correct Project Number.

* Fields marked with an asterisk are required.

4b Configure the following:

Project JSON File: Add the `google-services.json` file you downloaded from Firebase.

Server Key: Add the Server Key.

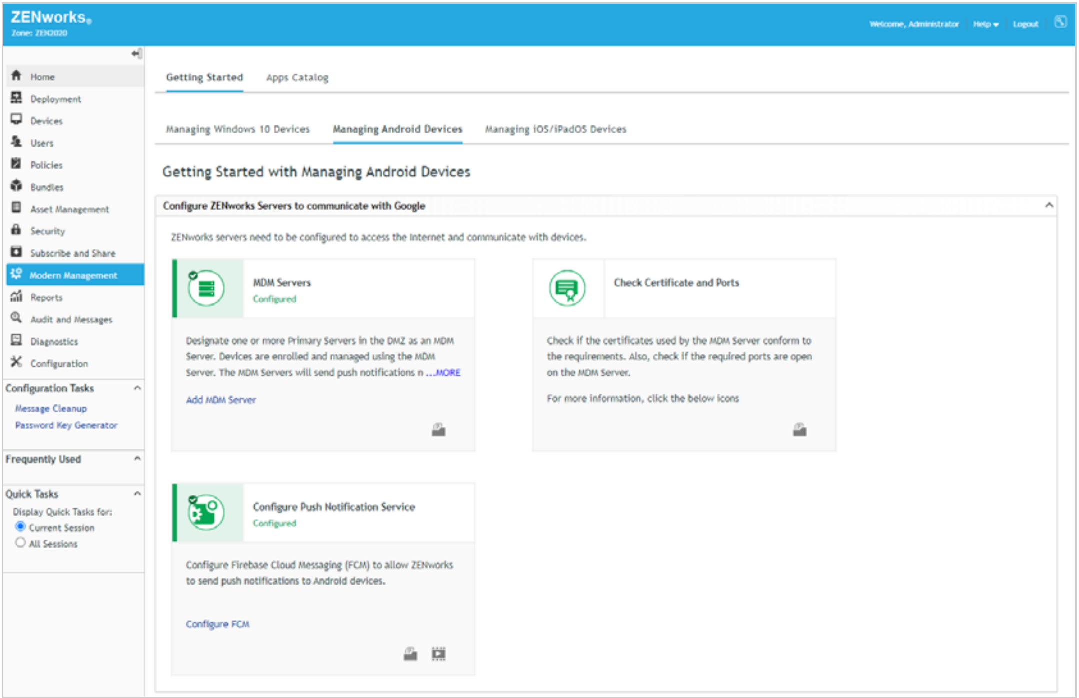
Key activation date: Specify the key's activation date.

Google user ID: Specify the Google account ID used to create the project.

4c Click Test Server Key to validate that the information is entered correctly and the key is active.

4d Click OK to save your Firebase Cloud Messaging configuration.

You are returned to the Getting Started and the Configure Push Notification Service panel shows that Firebase Cloud Messaging is configured.



Getting Started with Managing Android Devices

Configure ZENworks Servers to communicate with Google

ZENworks servers need to be configured to access the Internet and communicate with devices.

MDM Servers
Configured

Designate one or more Primary Servers in the DMZ as an MDM Server. Devices are enrolled and managed using the MDM Server. The MDM Servers will send push notifications n ...MORE

Add MDM Server

Check Certificate and Ports

Check if the certificates used by the MDM Server conform to the requirements. Also, check if the required ports are open on the MDM Server.

For more information, click the below icons

Configure Push Notification Service
Configured

Configure Firebase Cloud Messaging (FCM) to allow ZENworks to send push notifications to Android devices.

Configure FCM

3 Managing Windows Devices via the ZENworks Agent

Windows devices can be managed using the ZENworks Agent, native Windows MDM, or both. This part of the evaluation explains how to use the ZENworks Agent. To explore how to use Windows MDM capabilities see Chapter 4, “Manage Windows Devices via Windows MDM,” on page 49.

Of the two methods, the ZENworks Agent provides the most comprehensive management of Windows devices. This includes distributing software, enforcing policies, collecting inventory data, enabling remote management, and more. The follow sections explain how to install the ZENworks Agent on a Windows device and register it in the zone, secure that device, and then distribute applications to the device. For information about other management tasks you can perform with ZENworks, see Chapter 6, “Explore Other Areas,” on page 125.

- Section 3.1, “Register a Windows 10 Device,” on page 33
- Section 3.2, “Secure Your Windows Device,” on page 38
- Section 3.3, “Distribute an Application,” on page 41
- Section 3.4, “Unregister Your Windows Devices,” on page 47

3.1 Register a Windows 10 Device

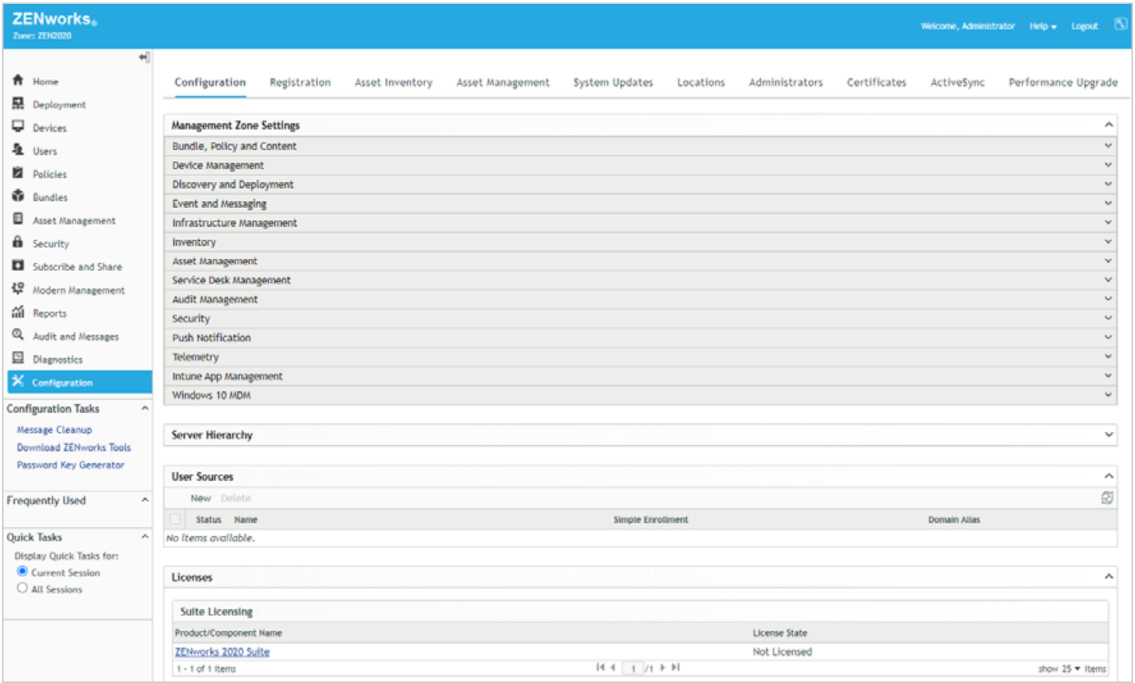
A device must register with the ZENworks management zone in order for it to be managed. To register a Windows device, you install the ZENworks Agent on the device. The agent then contacts the ZENworks Primary Server and completes the registration process.

- Section 3.1.1, “Create an Authorization Key,” on page 33
- Section 3.1.2, “Install the ZENworks Agent and Register the Device,” on page 35

3.1.1 Create an Authorization Key

When you install the ZENworks Agent on a device, the agent has the information required to connect back to your ZENworks Primary Server and register in your zone. To secure your ZENworks system against access by rogue devices, ZENworks allows only authorized devices to register. One way to authorize a device is to issue an authorization key that must be entered during installation of the ZENworks Agent on the device. This is the method we'll have you use, which means you first need to create an authorization key.

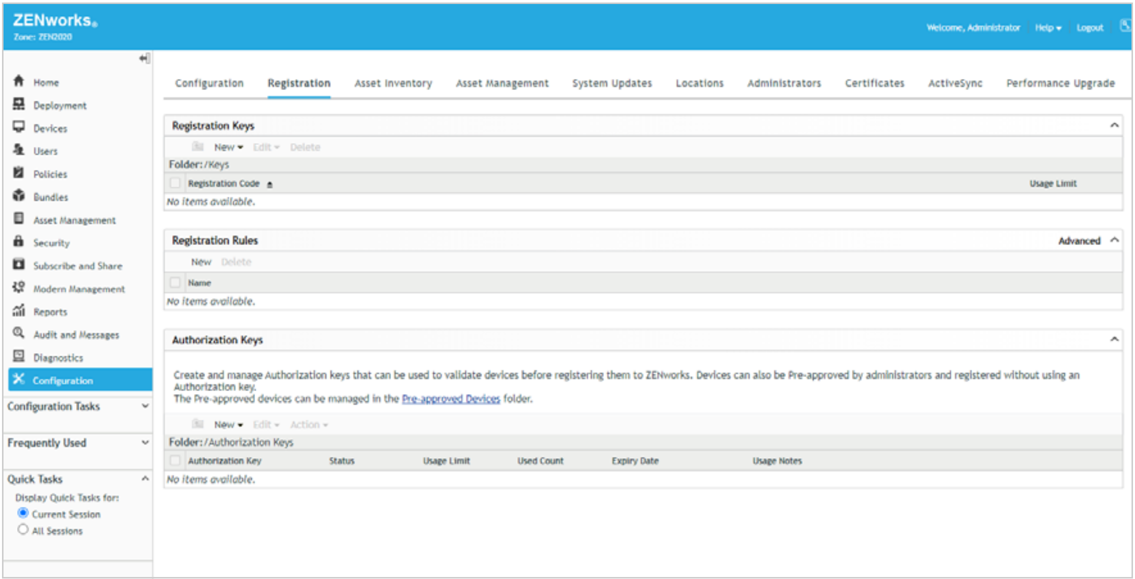
1 In ZENworks Control Center, click **Configuration** (in the left navigation pane).



Status	Name	Simple Enrollment	Domain Alias
No items available.			

Product/Component Name	License State
ZENworks 2020 Suite	Not Licensed

2 Click the **Registration** tab (top of page).



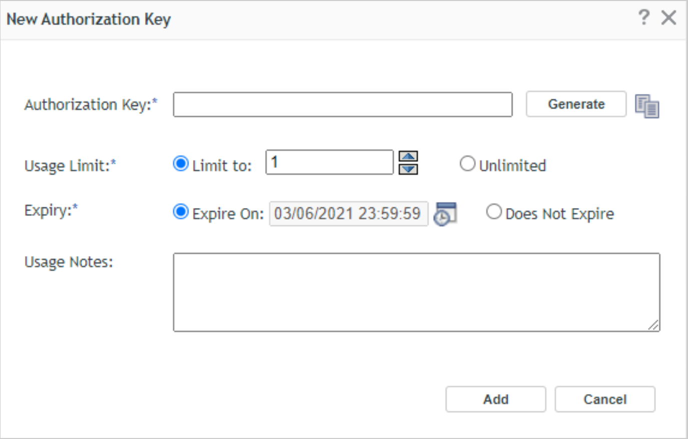
Registration Code	Usage Limit
No items available.	

Name
No items available.

Create and manage Authorization keys that can be used to validate devices before registering them to ZENworks. Devices can also be Pre-approved by administrators and registered without using an Authorization key.
The Pre-approved devices can be managed in the Pre-approved Devices folder.

Authorization Key	Status	Usage Limit	Used Count	Expiry Date	Usage Notes
No items available.					

3 In the Authorization Keys panel, click **Configure > Authorization Key** to display the New Authorization Key dialog box.



New Authorization Key

Authorization Key:*

Usage Limit:* ● Limit to: 1 ○ Unlimited

Expiry:* ● Expire On: 03/06/2021 23:59:59 ○ Does Not Expire

Usage Notes:

4 Configure the settings as follows, then click Add to create the key.

- **Authorization Key:** Enter an 8 - 10 character key of your choice, or click Generate to automatically generate one. You'll need to remember the key so write it down if necessary.
- **Usage Limit:** Select the limit for the number of times this key can be used, or select Unlimited to remove the usage limit for this evaluation. Security best practices dictate that you not allow unlimited uses in a production environment.
- **Expiry:** Select an expiration date for the key, or select Does Not Expire for this evaluation. As with the usage limit, security best practice in a production environment would be to use an expiration date.

5 Click Add to create the key and add it to the list.

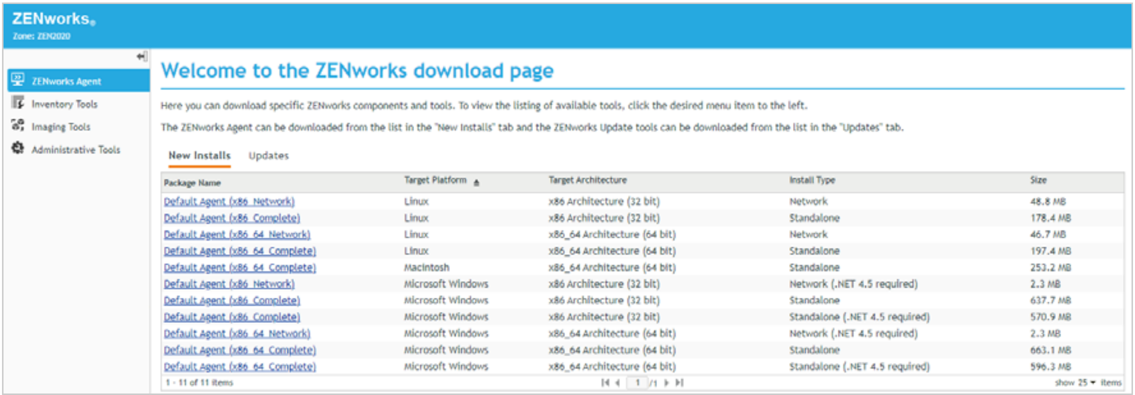
3.1.2 Install the ZENworks Agent and Register the Device

There are several ways you can distribute the ZENworks Agent to the device, including using discovery and deployment tasks in ZENworks Control Center to push the agent to devices, but we'll just have you manually download the agent from your ZENworks Primary Server and start the installation.

1 On the Windows 10 device, enter the following URL:

`https://ZENworks_Server_Address/zenworks-setup`

The ZENworks Agent download list is displayed.



Welcome to the ZENworks download page

Here you can download specific ZENworks components and tools. To view the listing of available tools, click the desired menu item to the left.

The ZENworks Agent can be downloaded from the list in the "New Installs" tab and the ZENworks Update tools can be downloaded from the list in the "Updates" tab.

Package Name	Target Platform	Target Architecture	Install Type	Size
Default Agent (x86 Network)	Linux	x86 Architecture (32 bit)	Network	48.8 MB
Default Agent (x86 Complete)	Linux	x86 Architecture (32 bit)	Standalone	178.4 MB
Default Agent (x86 64 Network)	Linux	x86_64 Architecture (64 bit)	Network	46.7 MB
Default Agent (x86 64 Complete)	Linux	x86_64 Architecture (64 bit)	Standalone	197.4 MB
Default Agent (x86 64 Complete)	Macintosh	x86_64 Architecture (64 bit)	Standalone	253.2 MB
Default Agent (x86 Network)	Microsoft Windows	x86 Architecture (32 bit)	Network (.NET 4.5 required)	2.3 MB
Default Agent (x86 Complete)	Microsoft Windows	x86 Architecture (32 bit)	Standalone	637.7 MB
Default Agent (x86 Complete)	Microsoft Windows	x86 Architecture (32 bit)	Standalone (.NET 4.5 required)	570.9 MB
Default Agent (x86 64 Network)	Microsoft Windows	x86_64 Architecture (64 bit)	Network (.NET 4.5 required)	2.3 MB
Default Agent (x86 64 Complete)	Microsoft Windows	x86_64 Architecture (64 bit)	Standalone	663.1 MB
Default Agent (x86 64 Complete)	Microsoft Windows	x86_64 Architecture (64 bit)	Standalone (.NET 4.5 required)	596.3 MB

1 - 11 of 11 items

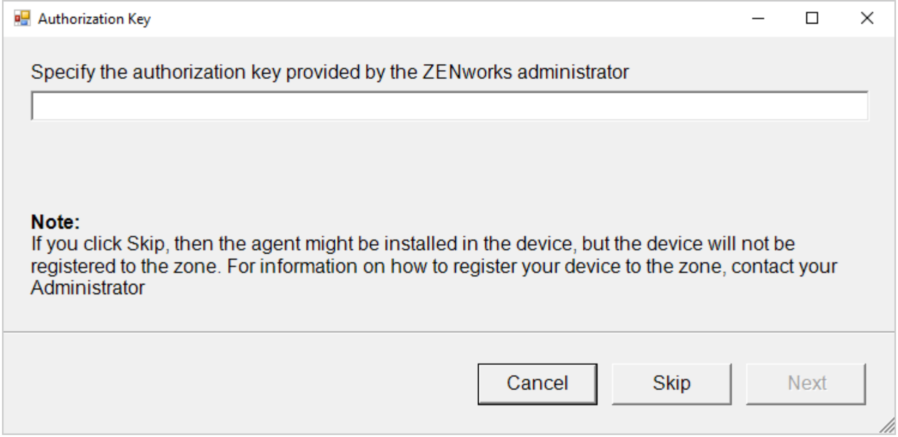
2 In the list, click the correct installation package for the device, then follow the prompts to download it.

You want the Microsoft Windows package that is the **Standalone** install type. If you know that the target device has .NET 4.5 or newer installed, you can use the **Standalone (.NET 4.5 required)** install type instead.

- **32 bit:** *Default Agent (x86_Complete)* Microsoft Windows x86 Architecture (32 bit) Standalone package
- **64 bit:** *Default Agent (x86_64_Complete)* Microsoft Windows x86_64 Architecture (64 bit) Standalone package

3 After the ZENworks Agent download completes, double-click the agent to start the installation.

4 When prompted, enter the authorization key you created, then click **Next** to continue the installation.



Specify the authorization key provided by the ZENworks administrator

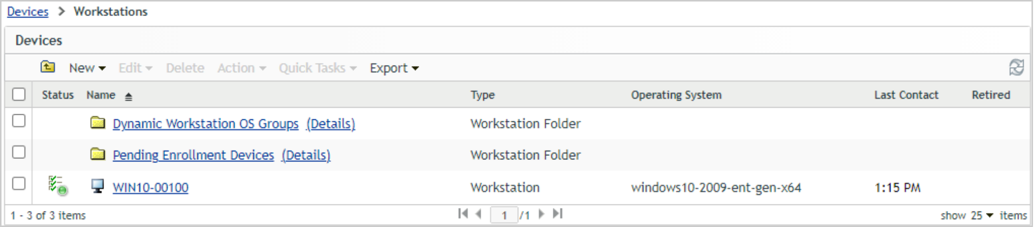
Note:
If you click Skip, then the agent might be installed in the device, but the device will not be registered to the zone. For information on how to register your device to the zone, contact your Administrator

The installation can take a few minutes. You can track the progress through the ZENworks icon located in the notification area.

5 When installation is complete, reboot the device as prompted.

6 In ZENworks Control Center, go to the **Devices** > **Workstations** list to confirm that the device registered in the zone.

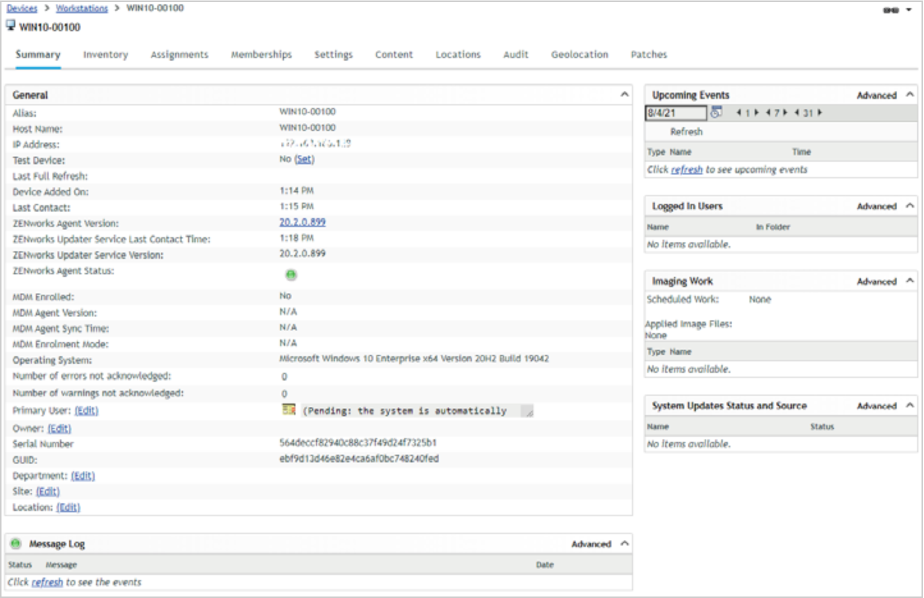
The Windows device is listed after the predefined device folders. In this example, we enrolled a Windows device named *WIN10-00100*.



□	Status	Name	Type	Operating System	Last Contact	Retired
□		Dynamic Workstation OS Groups (Details)	Workstation Folder			
□		Pending Enrollment Devices (Details)	Workstation Folder			
□		WIN10-00100	Workstation	windows10-2009-ent-gen-x64	1:15 PM	

7 (Optional) In the list, click the Windows device to display its Summary page.

The Summary page provides details about the device.



Devices > Workstations > WIN10-00100

WIN10-00100

General

Alias:	WIN10-00100
Host Name:	WIN10-00100
IP Address:	[illegible]
Test Device:	No (Set)
Last Full Refresh:	
Device Added On:	1:14 PM
Last Contact:	1:15 PM
ZENworks Agent Version:	20.2.0.899
ZENworks Updater Service Last Contact Time:	1:18 PM
ZENworks Updater Service Version:	20.2.0.899
ZENworks Agent Status:	●
MDM Enrolled:	No
MDM Agent Version:	N/A
MDM Agent Sync Time:	N/A
MDM Enrolment Mode:	N/A
Operating System:	Microsoft Windows 10 Enterprise x64 Version 20H2 Build 19042
Number of errors not acknowledged:	0
Number of warnings not acknowledged:	0
Primary User: (Edit)	(Pending: the system is automatically
Owner: (Edit)	
Serial Number	564deccf82940c88c37f49d24f7325b1
GUID:	ebf9d13d46e82e4ca6af0bc748240fed
Department: (Edit)	
Site: (Edit)	
Location: (Edit)	

Message Log Advanced

Status	Message	Date
Click refresh to see the events		

Upcoming Events Advanced

8/4/21 ◂ 1 ▸ ◂ 7 ▸ ◂ 31 ▸

Refresh

Type	Name	Time
Click refresh to see upcoming events		

Logged In Users Advanced

Name	In Folder
No items available.	

Imaging Work Advanced

Scheduled Work: None

Applied Image Files:
None

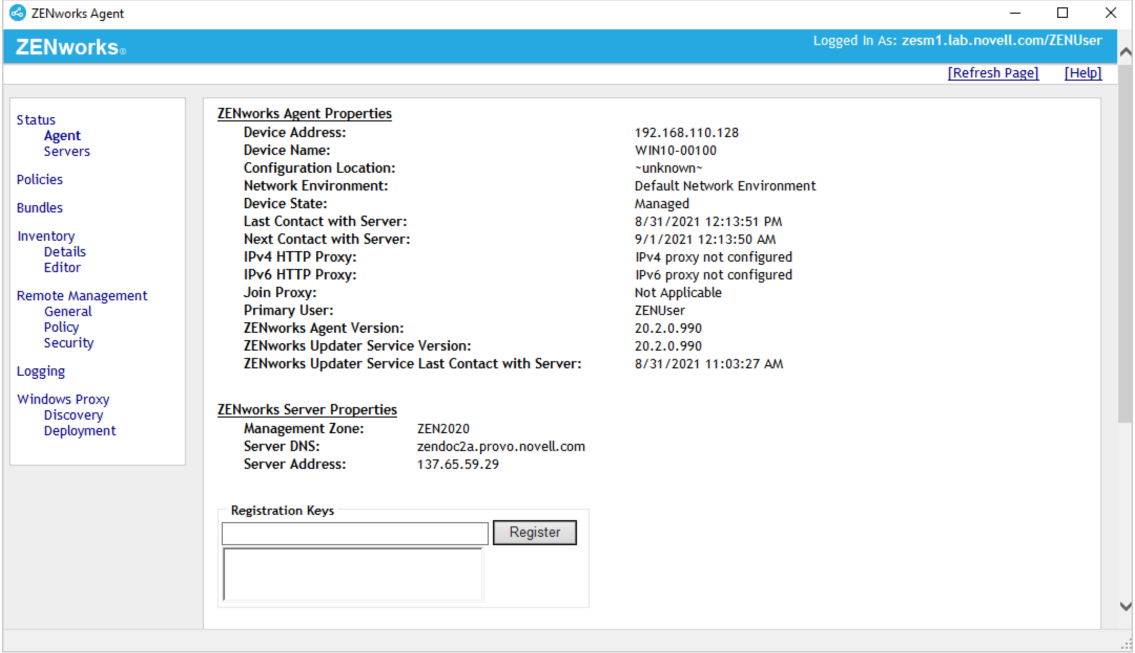
Type	Name
No items available.	

System Updates Status and Source Advanced

Name	Status
No items available.	

8 On the device, right-click the ZENworks icon in the Notification area, then click Technician Application to display the ZENworks Agent window.

The ZENworks Agent window provides details about the agent and the ZENworks server to which it is connected. It also provides information such as assigned polices and bundles. Typically, users don't need to access the ZENworks Agent windows, but we wanted to introduce it to you as an administrative tool.



ZENworks Agent

ZENworks

Logged In As: zesm1.lab.novell.com/ZENUser

[Refresh Page] [Help]

ZENworks Agent Properties

Device Address:	192.168.110.128
Device Name:	WIN10-00100
Configuration Location:	~unknown~
Network Environment:	Default Network Environment
Device State:	Managed
Last Contact with Server:	8/31/2021 12:13:51 PM
Next Contact with Server:	9/1/2021 12:13:50 AM
IPv4 HTTP Proxy:	IPv4 proxy not configured
IPv6 HTTP Proxy:	IPv6 proxy not configured
Join Proxy:	Not Applicable
Primary User:	ZENUser
ZENworks Agent Version:	20.2.0.990
ZENworks Updater Service Version:	20.2.0.990
ZENworks Updater Service Last Contact with Server:	8/31/2021 11:03:27 AM

ZENworks Server Properties

Management Zone:	ZEN2020
Server DNS:	zendoc2a.provo.novell.com
Server Address:	137.65.59.29

Registration Keys

You now have a device that you can use for the rest of this evaluation. One device is sufficient, but you can register additional Windows 10 devices if you'd like.

3.2 Secure Your Windows Device

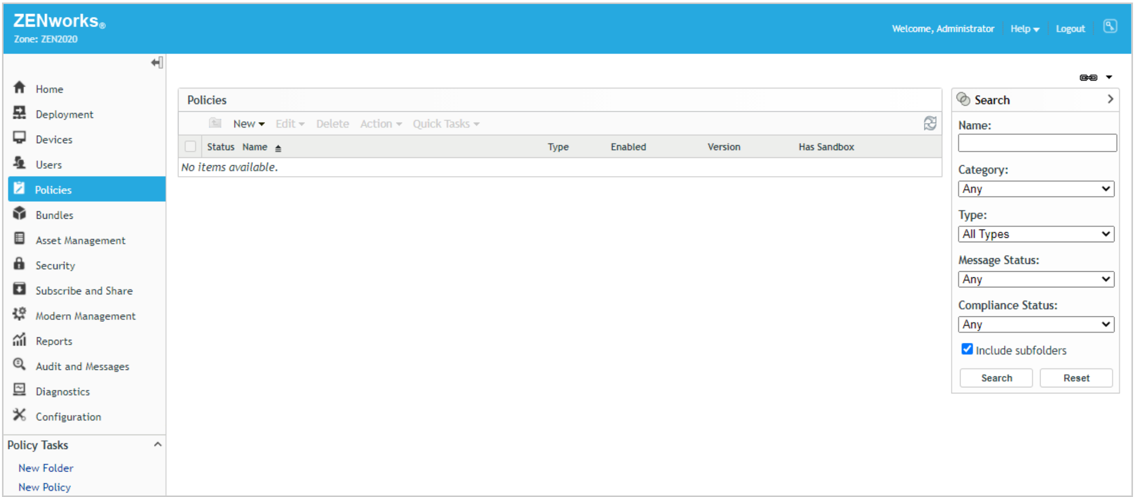
ZENworks lets you control the Windows Group policy to secure devices. In this evaluation, we'll use the Windows Group policy to enforce a complex password on your Windows device.

When creating the Windows Group policy, you need to run ZENworks Control Center on a device that has the same Windows version and architecture as the managed Windows device. For example, if you registered a Windows 10 64-bit device, you need to run ZENworks Control Center on a Windows 10 64-bit device.

- Create the Windows Group Policy (page 38)
- Test the Policy (page 40)

3.2.1 Create the Windows Group Policy

1 In ZENworks Control Center, click **Policies** (in the left navigation pane).



No items available.

2 Click **New** > **Policy** to display the Create New Policy wizard.

3 On the Select Platform page, select **Windows**, then click **Next**.

4 On the Select Policy Category page, select **Windows Configuration Policies**, then click **Next**.

5 On the Select Policy Type page, select **Windows Group Policy**, then click **Next**.

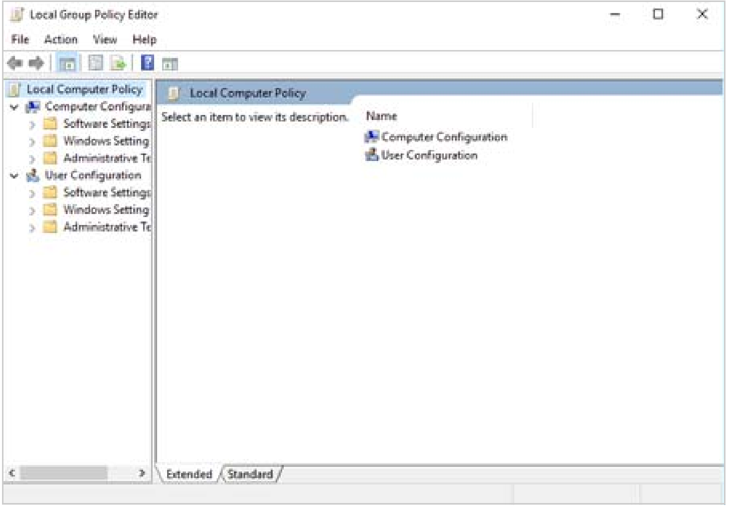
6 On the Define Details page, specify *Windows Group Policy* for the policy name, then click **Next**.

7 On the Windows Group Policy Settings page, configure the policy settings:

7a Leave **Local Group Policy** selected, then click **Configure**.

7b Follow the prompts to install the ZENworks ZCC Helper.

When the ZCC Helper is finished installing, the Windows Local Group Policy Editor is displayed:



Sometimes, depending on browser settings, the Local Group Policy Editor is not launched after the ZCC Helper is installed. If this happens, simply click **Configure** again and follow the prompts to launch it.

7c In the Local Group Policy Editor, edit the Password Policy to enable the **Password must meet complexity requirements** option.

This option forces the user's password to be at least six characters consisting of at least three of the following character types: uppercase, lowercase, number, and non-alphabetic.

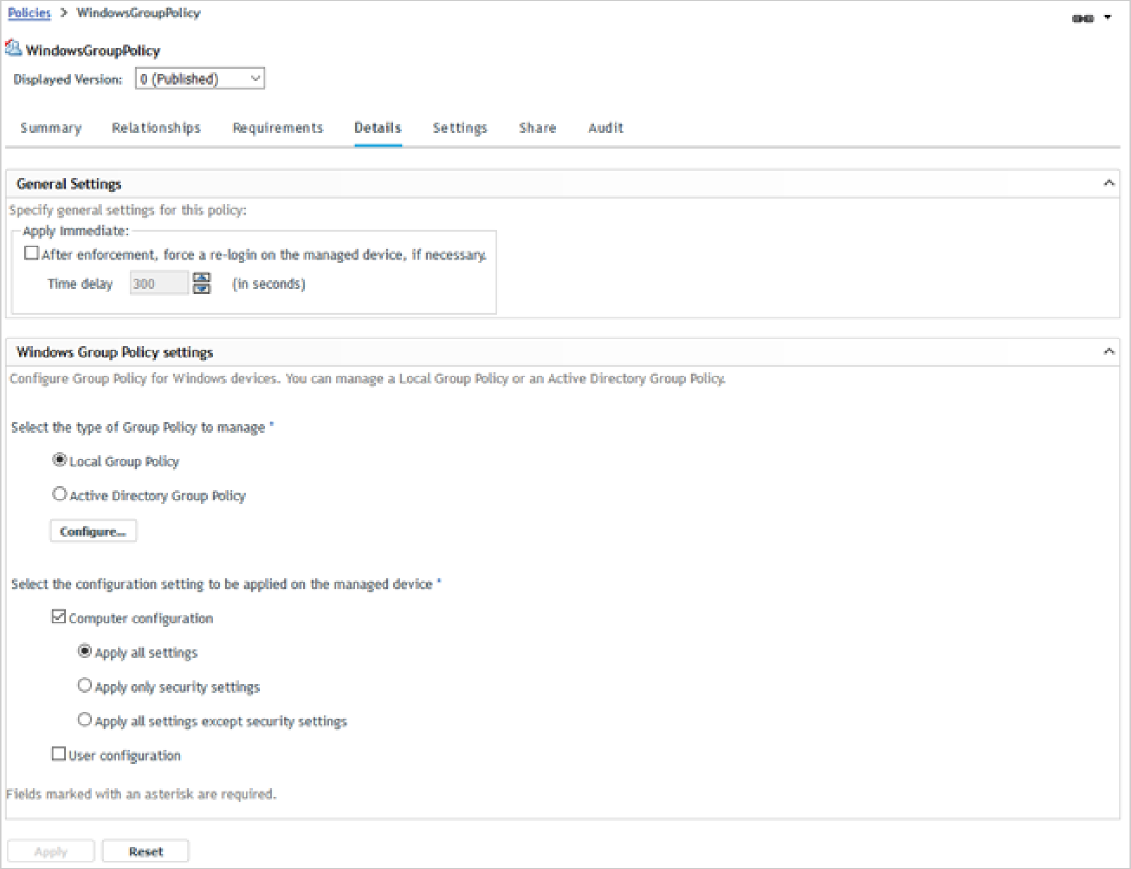
The path to the Password Policy is:

Computer Configuration > Windows Settings > Security Settings > Account Policies

7d When you've finished editing the Password Policy, exit the Local Group Policy Editor and upload the policy (when prompted).

7e Click **Next** to display the Summary page.

8 On the Summary page, deselect **Create as Sandbox**, select **Define Additional Properties**, then click **Finish** to create the policy and display it.



Policies > WindowsGroupPolicy

WindowsGroupPolicy

Displayed Version: 0 (Published)

General Settings

Specify general settings for this policy:

Apply Immediate:

□ After enforcement, force a re-login on the managed device, if necessary.

Time delay 300 (in seconds)

Windows Group Policy settings

Configure Group Policy for Windows devices. You can manage a Local Group Policy or an Active Directory Group Policy.

Select the type of Group Policy to manage *

● Local Group Policy

○ Active Directory Group Policy

Select the configuration setting to be applied on the managed device *

☑ Computer configuration

● Apply all settings

○ Apply only security settings

○ Apply all settings except security settings

□ User configuration

Fields marked with an asterisk are required.

9 The Windows Group policy can be assigned to either users or devices. We'll have you assign it to the evaluation user:

9a Click **Relationships**.

9b In the User Assignments list, click **Add**.

9c Select the evaluation user, then click **OK** to add the user to the assignment list.

9d Complete the assignment wizard.

3.2.2 Test the Policy

1 On the Windows device, make sure you are logged in to ZENworks as the evaluation user.

If you are not logged in as the user, you can right-click the ZENworks icon (in the Notification area) and then click **Sign in**. A gray ZENworks icon indicates that a user is not logged in while a blue ZENworks icon indicates a logged-in user.

2 Right-click the ZENworks icon (in the Notification area) and then click **Refresh** to make sure the Windows Group policy has been applied to the device.

3 Change the local Windows account password.

You'll be required to enter a password that is at least six characters consisting of at least three of the following character types: uppercase, lowercase, number, and non-alphabetic.

3.3 Distribute an Application

ZENworks lets you distribute anything from single file applications such as Calculator to complex Microsoft Installer (.msi) packages such as Microsoft Office.

For this evaluation, you'll distribute the free Evernote application. ZENworks will deliver the Evernote installation package to the device, let you install the application, and then delete the installation package when the installation is complete.

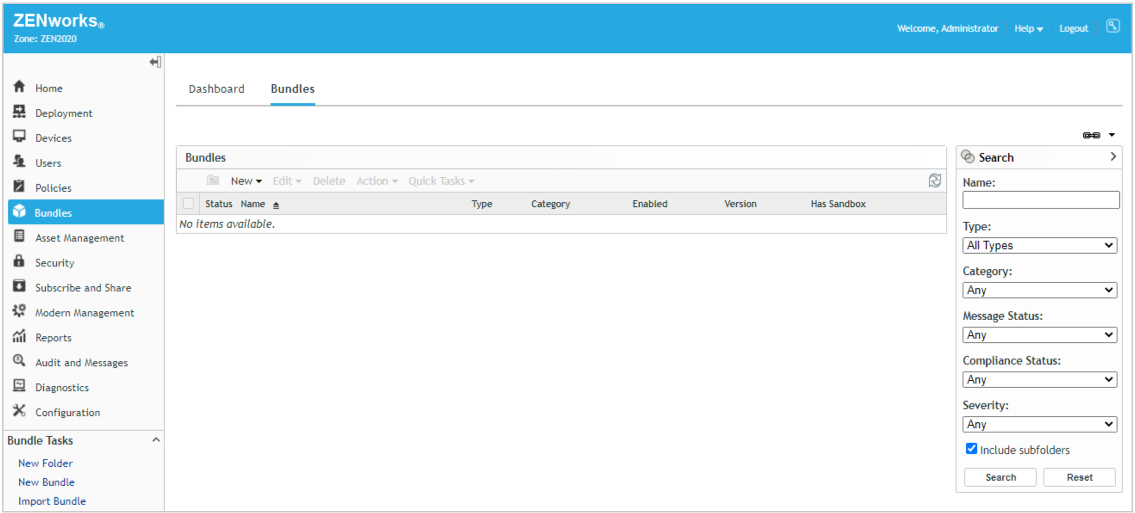
- Section 3.3.1, "Create the Windows Bundle," on page 41
- Section 3.3.2, "Test the Bundle," on page 44
- Section 3.3.3, "View the Bundle Status," on page 45

3.3.1 Create the Windows Bundle

1 Download the Evernote installation package from https://evernote.com/download/.

The installation package is a self-extracting executable such as `Evernote-10.20.4-win-ddl-ga-2893.exe`.

2 In ZENworks Control Center, click **Bundles** (in the left navigation pane).



3 Click **New** > **Bundle** to display the Create New Bundle wizard.

4 On the Select Bundle Type page, select **Windows Bundle**, then click **Next**.

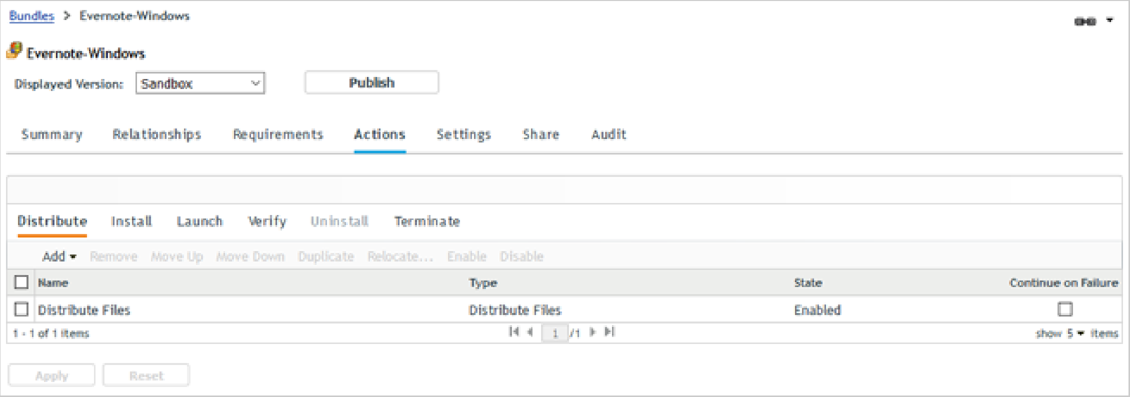
5 On the Select Bundle Category page, select **(Empty Bundle)**, then click **Next**.

This option lets you create a bundle and then add the actions, or instructions, that are needed to copy the installation package to your Windows device, install the package, and then remove the package from the device.

6 On the Define Details page, enter *Evernote-Windows* as the bundle name, then click **Next**.

7 One the Summary page, select both **Create as Sandbox** and **Define Additional Properties**, then click **Finish**.

The bundle's Actions page is displayed.



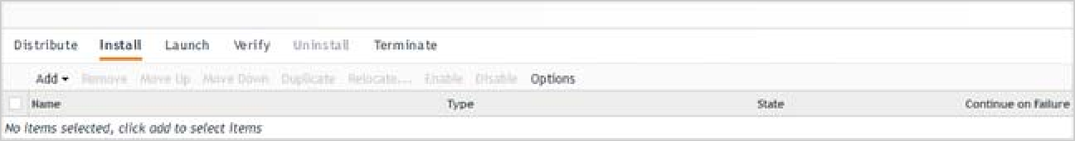
Displayed Version: Sandbox

□ Name	Type	State	Continue on Failure
□ Distribute Files	Distribute Files	Enabled	□

1 - 1 of 1 items

8 Configure the bundle to install the Evernote application:

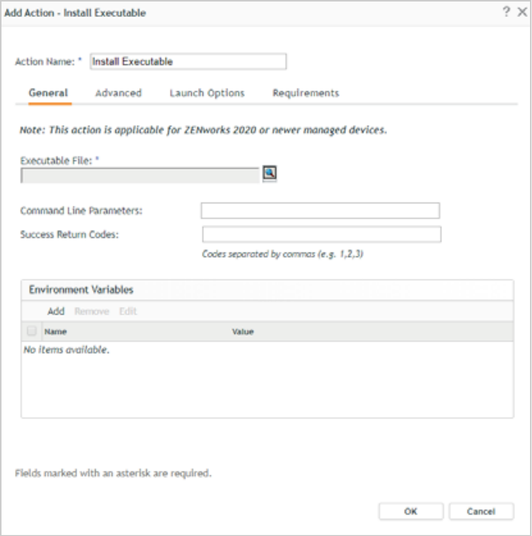
8a In the Actions list, click **Install**.



□ Name	Type	State	Continue on Failure

No items selected, click add to select items

8b Click **Add** > **Install Executable** to display the Add Action - Install Executable dialog.



Action Name: * Install Executable

Note: This action is applicable for ZENworks 2020 or newer managed devices.

Executable File: *

Command Line Parameters:

Success Return Codes:

Codes separated by commas (e.g. 1,2,3)

□ Name	Value

No items available.

Fields marked with an asterisk are required.

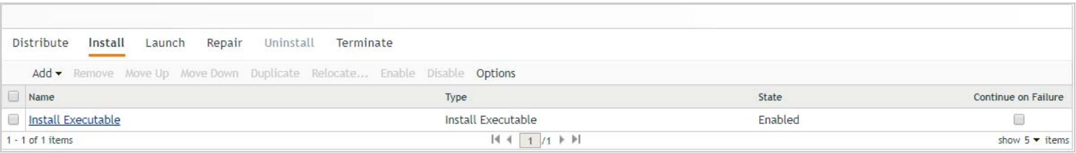
8c Change the Action Name to *Install Evernote*.

8d For the Executable File, browse to select the Evernote installation package and upload it.

If you are prompted to first download and install the ZCC Helper, do so.

The file is uploaded to the ZENworks server's content repository. It can then be distributed from the repository to the Windows device.

8e Click **OK** to add the action to the Install list.



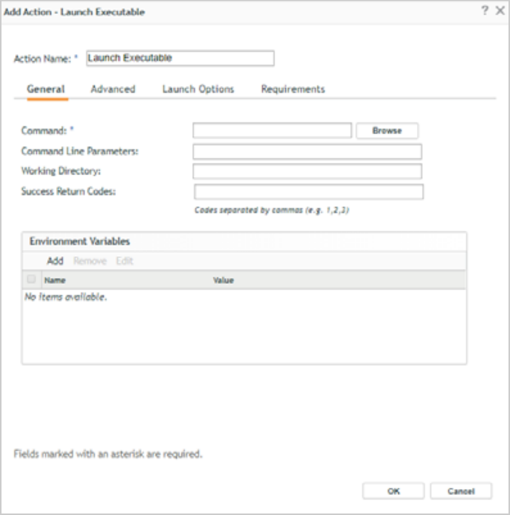
□	Name	Type	State	Continue on Failure
□	Install Executable	Install Executable	Enabled	□

1 - 1 of 1 items

9 Configure the bundle to launch the Evernote application immediately after installation:

9a In the Actions list, click **Launch**.

9b Click **Add** > **Launch Executable** to display the Add Action - Launch Executable dialog.



Action Name: * Launch Executable

Command: *

Command Line Parameters:

Working Directory:

Success Return Codes:

Codes separated by commas (e.g. 1,2,3)

□	Name	Value

No Items available.

Fields marked with an asterisk are required.

9c Change the Action Name to *Launch Evernote*.

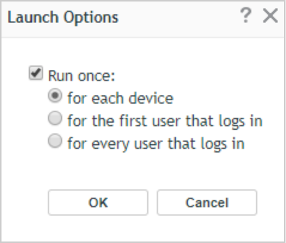
9d In the Command field, enter:

```
%USERPROFILE%\AppData\Local\Programs\Evernote\Evernote.exe
```

9e Click **OK** to add the action to the Launch list.

9f In the Launch list, click **Options** to display the Launch Options dialog.

The bundle installs the Evernote application, including a shortcut on the desktop, and then launches it. This option instructs the bundle to run one time and then no longer be available on the Windows device, alleviating confusion as to which shortcut should be used to launch the application.



☑ Run once:

● for each device

○ for the first user that logs in

○ for every user that logs in

9g Click **Run once**, select the **for each device** option, then click **OK**.

10 Click **Apply** to save the changes you've made to the bundle's actions.

11 Assign the bundle to your managed Windows device:

11a Click the **Relationships** tab.

11b In the Device Assignments list, click **Add**, then follow the prompts to assign the bundle.

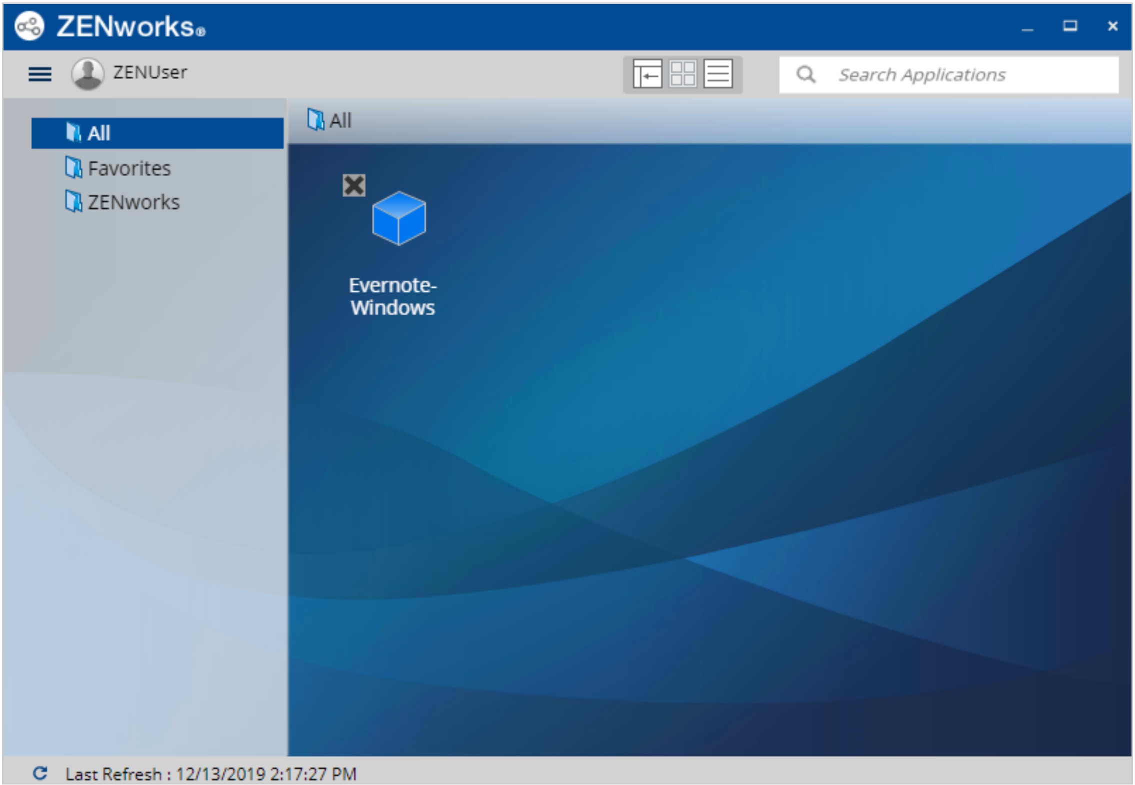
As you go through the assignment wizard, keep the default settings.

12 After you've assigned the bundle, click **Publish**, then follow the prompts to publish the bundle.

The bundle was created as a Sandbox version. A sandboxed app is not available to users or devices until it is published.

3.3.2 Test the Bundle

1 On the Windows device, click the ZENworks icon in the Notification area to display the ZENworks application window.



2 If the Evernote bundle is not displayed in the window, click the menu in the upper-left corner, then click **Refresh**.

3 Double-click the Evernote bundle to download the installation package and start the installation process.

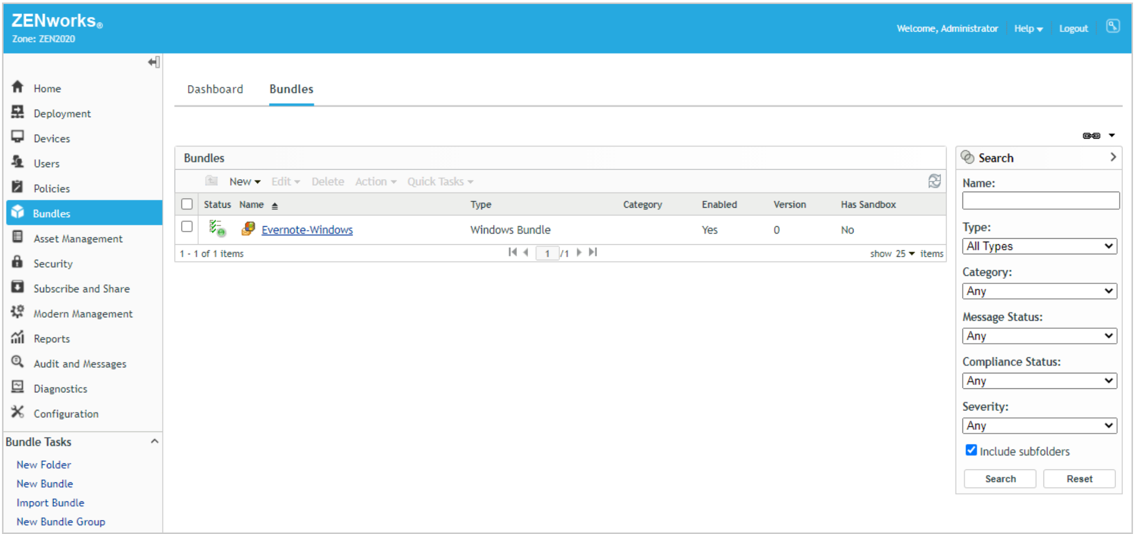
4 Follow the prompts to install the application.

When the installation is complete, an Evernote shortcut is added to the desktop, the Evernote bundle is removed from the ZENworks application window, and the Evernote application is launched.

3.3.3 View the Bundle Status

ZENworks Control Center makes it easy for you to know the status of the bundle on your Windows device, including whether it has been assigned, distributed, installed, and launched on the device.

1 In ZENworks Control Center, click **Bundles** (in the left navigation pane).



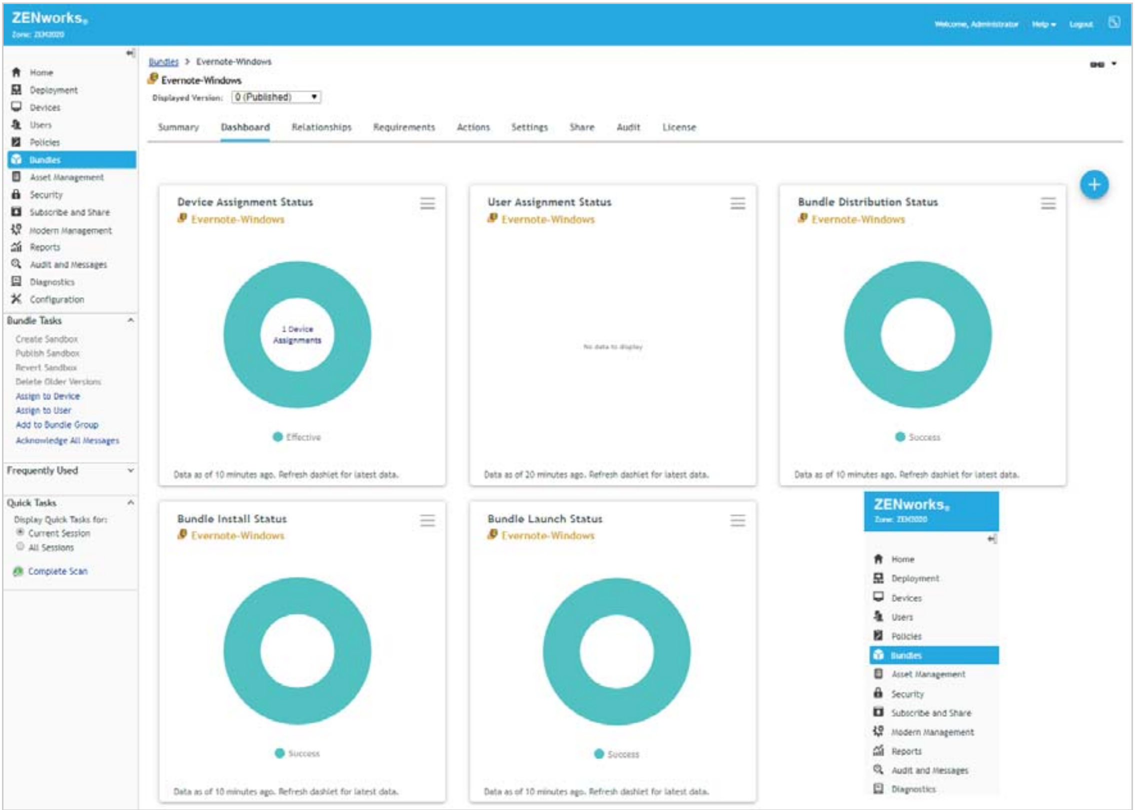
□	Status	Name	Type	Category	Enabled	Version	Has Sandbox
□		Evernote-Windows	Windows Bundle		Yes	0	No

1 - 1 of 1 items   1 /1   show 25 items

2 In the Bundles list, click the Evernote-Windows bundle to display its properties.

3 Click the Dashboard tab.

The Dashboard displays a set of dashlets that shows the assignment, distribution, installation, and launch status of the bundle for every device to which the bundle is assigned. For this evaluation, we installed the bundle to one Windows device so the dashlets only reflect the bundle status for that one device.



No data to display

Data as of 10 minutes ago. Refresh dashlet for latest data.

Data as of 20 minutes ago. Refresh dashlet for latest data.

Data as of 10 minutes ago. Refresh dashlet for latest data.

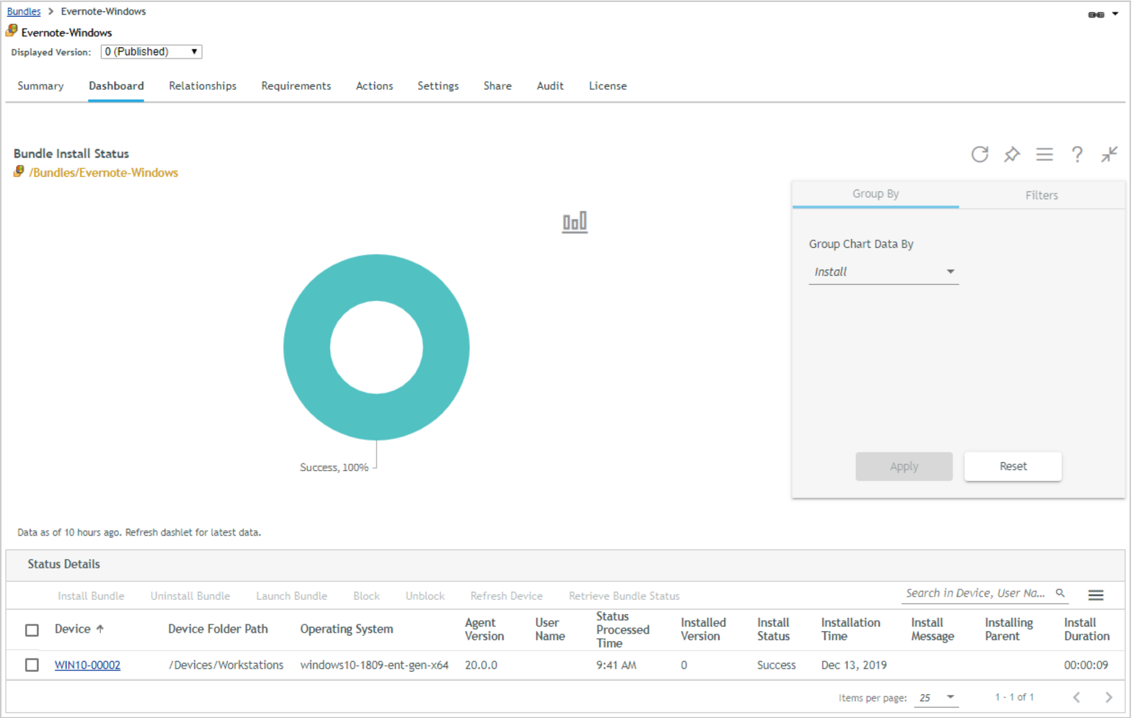
Data as of 10 minutes ago. Refresh dashlet for latest data.

Data as of 10 minutes ago. Refresh dashlet for latest data.

When you hover over the Device Assignment, Distribution, Install, and Launch Status charts, each dashlet shows success for the device. The User Assignment Status bundle has no data to display because the bundle is assigned to the device and not any users.

4 Click the Bundle Installation Status dashlet.

The expanded dashlet gives installation information for each device on which the bundle is installed. Go ahead and play around with the filters and columns to see how you can customize the dashlet. You can save any changes by clicking the menu icon ≡ above the Filters box and then selecting **Save As**.



Bundles > Evernote-Windows

Evernote-Windows

Displayed Version: 0 (Published)

Bundle Install Status

/Bundles/Evernote-Windows

Data as of 10 hours ago. Refresh dashlet for latest data.

Status Details

□	Device ↑	Device Folder Path	Operating System	Agent Version	User Name	Status Processed Time	Installed Version	Install Status	Installation Time	Install Message	Installing Parent	Install Duration
□	WIN10-00002	/Devices/Workstations	windows10-1809-ent-gen-x64	20.0.0		9:41 AM	0	Success	Dec 13, 2019			00:00:09

Items per page: 25 1 - 1 of 1

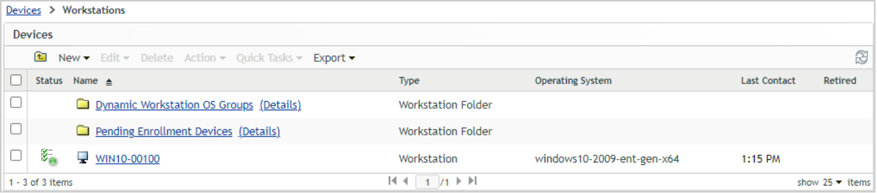
5 Become familiar with the other dashlets if desired.

3.4 Unregister Your Windows Devices

If you no longer want ZENworks to manage a device, you can unregister the device from the zone or you can retire it. Unregistering a device removes all assignments from the device and deletes the device from the ZENworks databases. Retiring a device removes all assignments but leaves the device, including its inventory data, in the database.

For this evaluation, we'll have you unregister and uninstall the device.

1 In ZENworks Control Center, click **Devices** > **Workstations** to display your enrolled Windows device.



Devices > Workstations

Devices

□	Status	Name ▲	Type	Operating System	Last Contact	Retired
□		Dynamic Workstation OS Groups (Details)	Workstation Folder			
□		Pending Enrollment Devices (Details)	Workstation Folder			
□		WIN10-00100	Workstation	windows10-2009-ent-gen-x64	1:15 PM	

1 - 3 of 3 items 1 /1 show 25 items

2 Select the check box in front of the Windows device, click **Actions** > **Unregister Device**, then click **OK** when prompted.

The device is removed from the list.

3 On the device, use the Apps and Features setting to uninstall Micro Focus ZENworks.

4 Manage Windows Devices via Windows MDM

Windows devices can be managed using the ZENworks Agent, the native Windows MDM capabilities, or both. This part of the evaluation explains how to use native Windows MDM. To explore how to use the ZENworks Agent see Chapter 3, “Managing Windows Devices via the ZENworks Agent,” on page 33.

ZENworks provides modern management of Windows devices via native Windows MDM. This includes enrolling the devices as MDM-managed devices in the ZENworks zone, deploying Configuration Service Providers (CSPs) to manage configuration settings, and deploying MSI applications.

IMPORTANT: At this time, ZENworks management via Windows MDM is experimental and should be used for evaluation purposes only. Future releases will include full support as the capabilities are fleshed out.

The follow sections explain how to enroll a Windows device, secure that device, and then distribute an application to the device. For information about other management tasks you can perform with ZENworks, see Chapter 6, “Explore Other Areas,” on page 125.

- Section 4.1, “Enroll a Windows 10 Device,” on page 49
- Section 4.2, “Secure the Device,” on page 59
- Section 4.3, “Distribute an MSI Application,” on page 63
- Section 4.4, “Unenroll Your Windows Devices,” on page 70

4.1 Enroll a Windows 10 Device

A device must enroll with the ZENworks management zone in order for it to be managed via native Windows MDM. There are multiple ways to MDM enroll a device, including using a provisioning package, Azure AD, and Windows AutoPilot. In this evaluation, we’ll enroll using a provisioning package. However, if you are interested in using Azure AD or Windows AutoPilot, see the ZENworks Windows 10 MDM Reference (https://www.novell.com/documentation/zenworks-2020-update-2/zen_win_mdm/data/zen_win_mdm.html#).

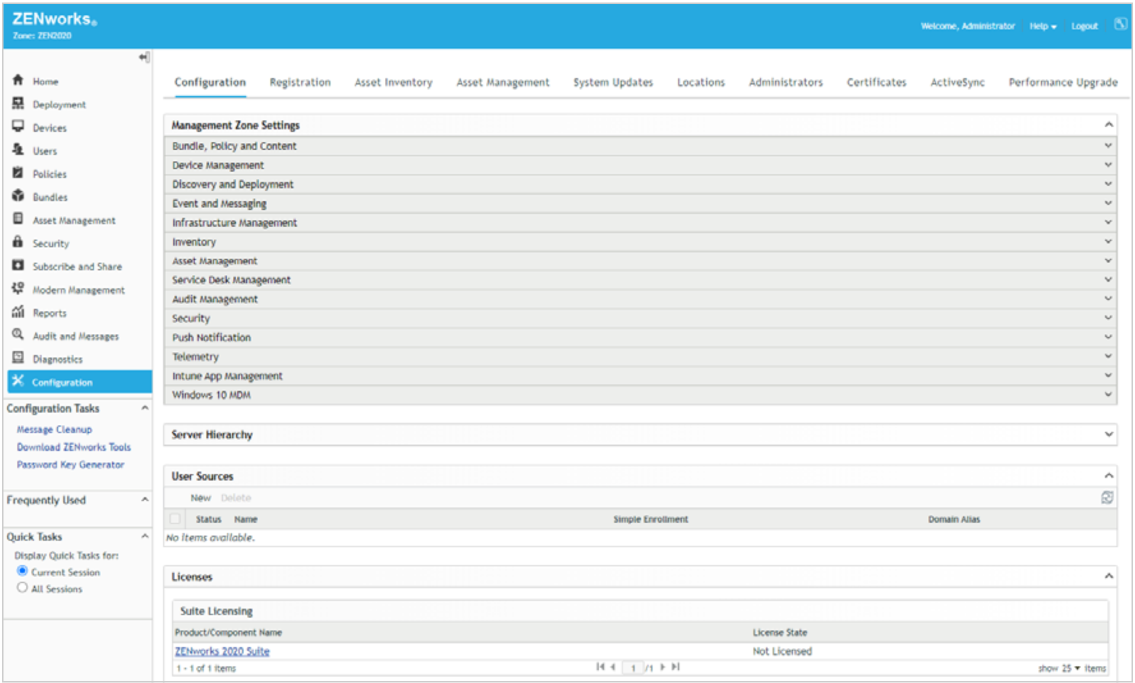
IMPORTANT: If desired, you can use the same Windows 10 device you used in Chapter 3, “Managing Windows Devices via the ZENworks Agent,” on page 33. Because ZENworks supports dual enrollment and management via both the ZENworks Agent and Windows MDM, the device can have the ZENworks Agent installed or not—it does not matter for this part of the evaluation.

- Section 4.1.1, “Prepare for Provisioning Package Creation,” on page 50
- Section 4.1.2, “Create the Provisioning Package,” on page 52
- Section 4.1.3, “Enroll a Device,” on page 56

4.1.1 Prepare for Provisioning Package Creation

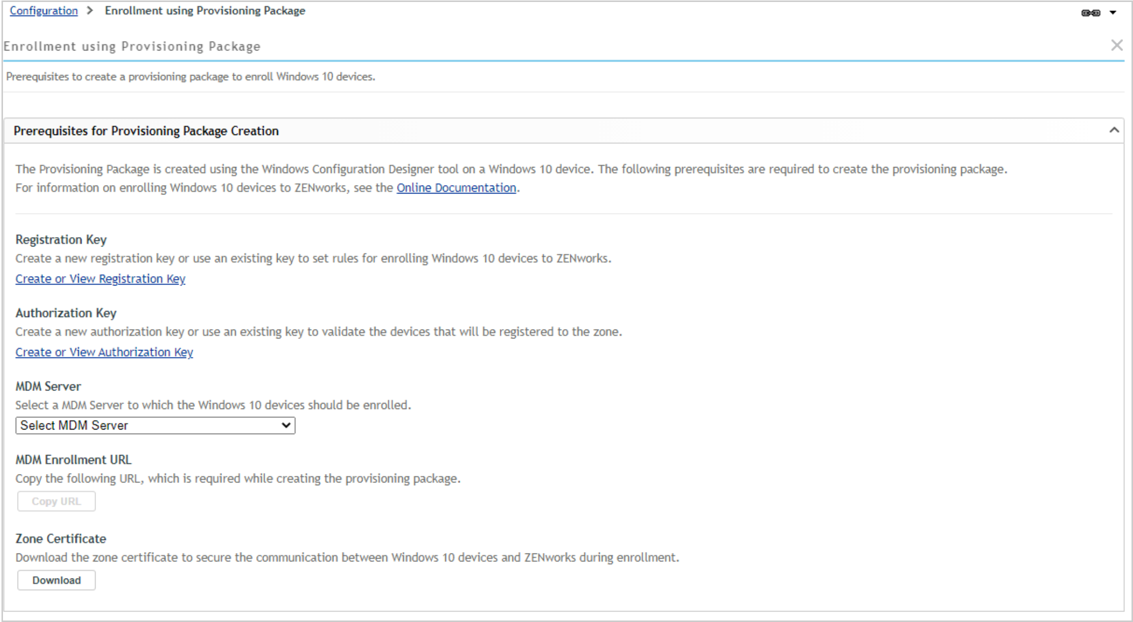
You use Windows Configuration Designer to create a provisioning package. The tool requires you to supply information gathered from ZENworks. To gather the information:

1 In ZENworks Control Center, click **Configuration** (in the left navigation pane).



2 In the Management Zone Settings, click **Windows 10 MDM**, then click **Enrollment using Provisioning Package** to display the prerequisites page.

This page walks you through gathering (and creating if necessary) the ZENworks information required for the provisioning package.


Configuration > Enrollment using Provisioning Package
Enrollment using Provisioning Package

Prerequisites to create a provisioning package to enroll Windows 10 devices.

Prerequisites for Provisioning Package Creation

The Provisioning Package is created using the Windows Configuration Designer tool on a Windows 10 device. The following prerequisites are required to create the provisioning package.
For information on enrolling Windows 10 devices to ZENworks, see the Online Documentation.

Registration Key
Create a new registration key or use an existing key to set rules for enrolling Windows 10 devices to ZENworks.
Create or View Registration Key

Authorization Key
Create a new authorization key or use an existing key to validate the devices that will be registered to the zone.
Create or View Authorization Key

MDM Server
Select a MDM Server to which the Windows 10 devices should be enrolled.
Select MDM Server

MDM Enrollment URL
Copy the following URL, which is required while creating the provisioning package.
Copy URL

Zone Certificate
Download the zone certificate to secure the communication between Windows 10 devices and ZENworks during enrollment.
Download

3 Create a registration key:

3a Click **Create or View Registration Key**.

3b In the Registration Keys list, click **New** > **Registration Key** to launch the Create New Registration Key wizard.

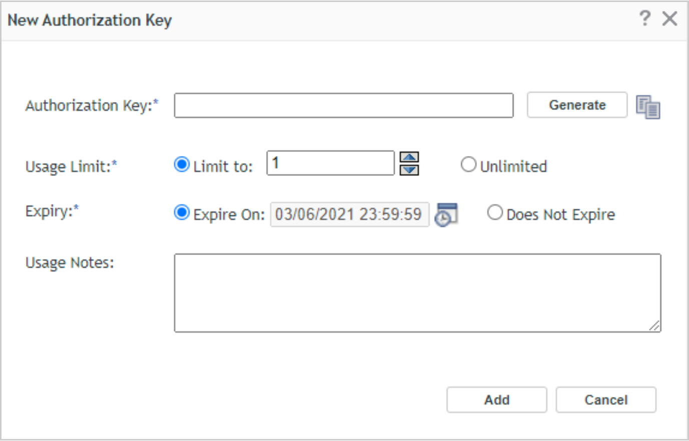
3c Complete the wizard using the following information:

- **Step 1: Basic Information:** Click **Generate** to generate the key, then copy it to text file to use during creation of the provisioning package. Leave the key usage set to Unlimited.
- **Step 2: Device Folder:** Keep the default folder (/Devices/Workstations). This is where the enrolled device will be placed in ZENworks Control Center.
- **Step 3: Device Fields:** Ignore these fields.
- **Step 4: Group Membership:** Ignore this option.
- **Step 5: Reconcile Settings:** Keep the default settings. These settings are used if a device ever needs to be re-enrolled. It enables the enrolling device to be matched to its device record in ZENworks.
- **Step 6: Summary:** Click **Finish** to add the key to the Registration Key list.

3d Stay on the Registration page and continue with the next step.

4 In the Authorization Keys list, copy the authorization key you created in Chapter 3, "Managing Windows Devices via the ZENworks Agent," on page 33. If haven't done that part of the evaluation, create an authorization key now:

4a In the Authorization Keys list, click **New > Authorization Key** to display the New Authorization Key dialog box.



New Authorization Key

Authorization Key:*

Usage Limit:* ● Limit to: 1 ○ Unlimited

Expiry:* ● Expire On: 03/06/2021 23:59:59 ○ Does Not Expire

Usage Notes:

4b Configure the settings as follows:

- **Authorization Key:** Enter an 8 - 10 character key of your choice, or click **Generate** to automatically generate one. You'll need to remember the key so write it down if necessary.
- **Usage Limit:** Select the limit for the number of times this key can be used, or select **Unlimited** to remove the usage limit for this evaluation. Security best practices dictate that you not allow unlimited uses in a production environment.

- **Expiry:** Select an expiration date for the key, or select **Does Not Expire** for this evaluation. As with the usage limit, security best practice in a production environment would be to use an expiration date.

4c Click **Add** to create the key and add it to the list.

4d Return to the provisioning package prerequisites page.

5. On the Enrollment using Provisioning Package page, select your MDM Server.
6. Copy the MDM Enrollment URL.
7. Download the zone certificate.

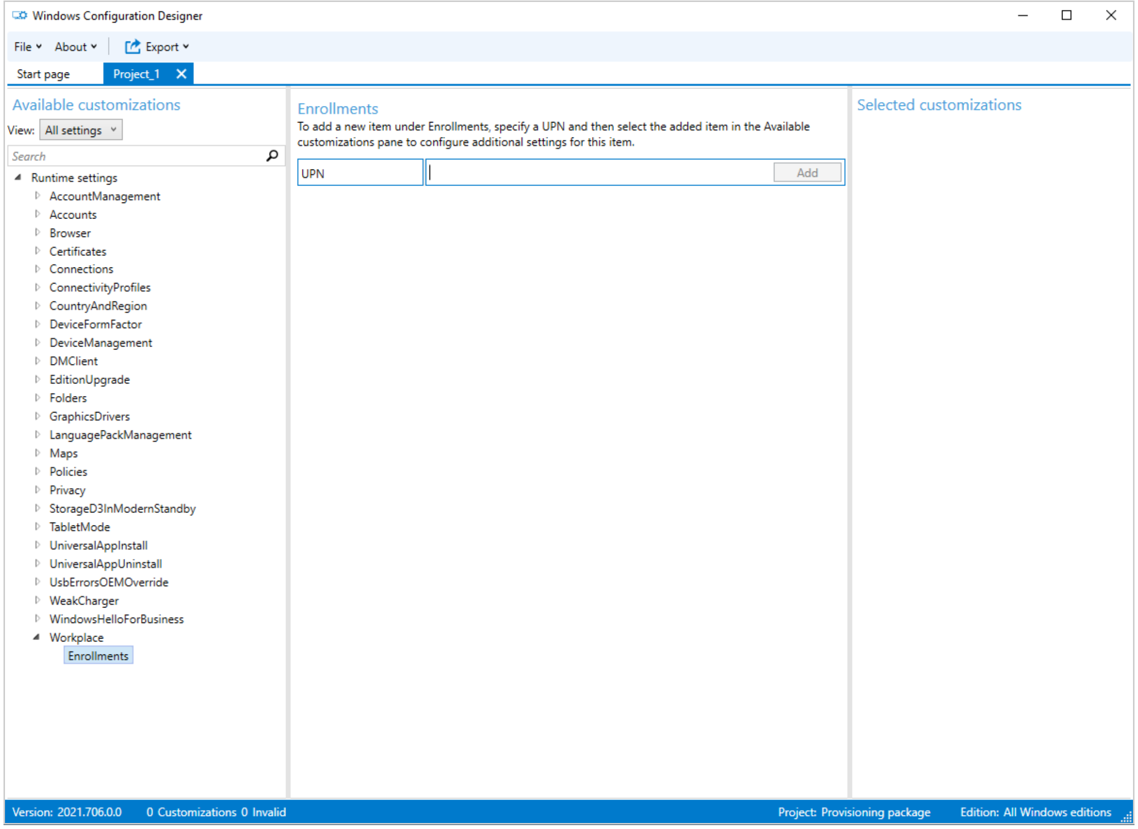
4.1.2 Create the Provisioning Package

At this point, you should have recorded your registration key, authorization key, and MDM enrollment URL key for use when creating the provisioning package. You should have also downloaded the zone certificate.

To create the package:

1. On a Windows 10 device, download Windows Configuration Designer (https://www.microsoft.com/en-us/p/windows-configuration-designer/9nblggh4tx22?rtc=1#activetab=pivot:overviewtab) from the Microsoft Store.
2. Open Windows Configuration Designer, click **File** > **New Project**.
3. Enter a name for the project (for example, ZENworks MDM Enrollment), change the project folder if desired, then click **Next**.
4. Keep **Provisioning package** as the selected workflow, then click **Next**.
5. Select **All Windows desktop editions**, then click Next.
6. Ignore the provisioning package import and click **Finish**.

7 In the Available Customizations section, expand **Runtime settings**, expand **Workplace**, then click **Enrollments** to display the UPN field.

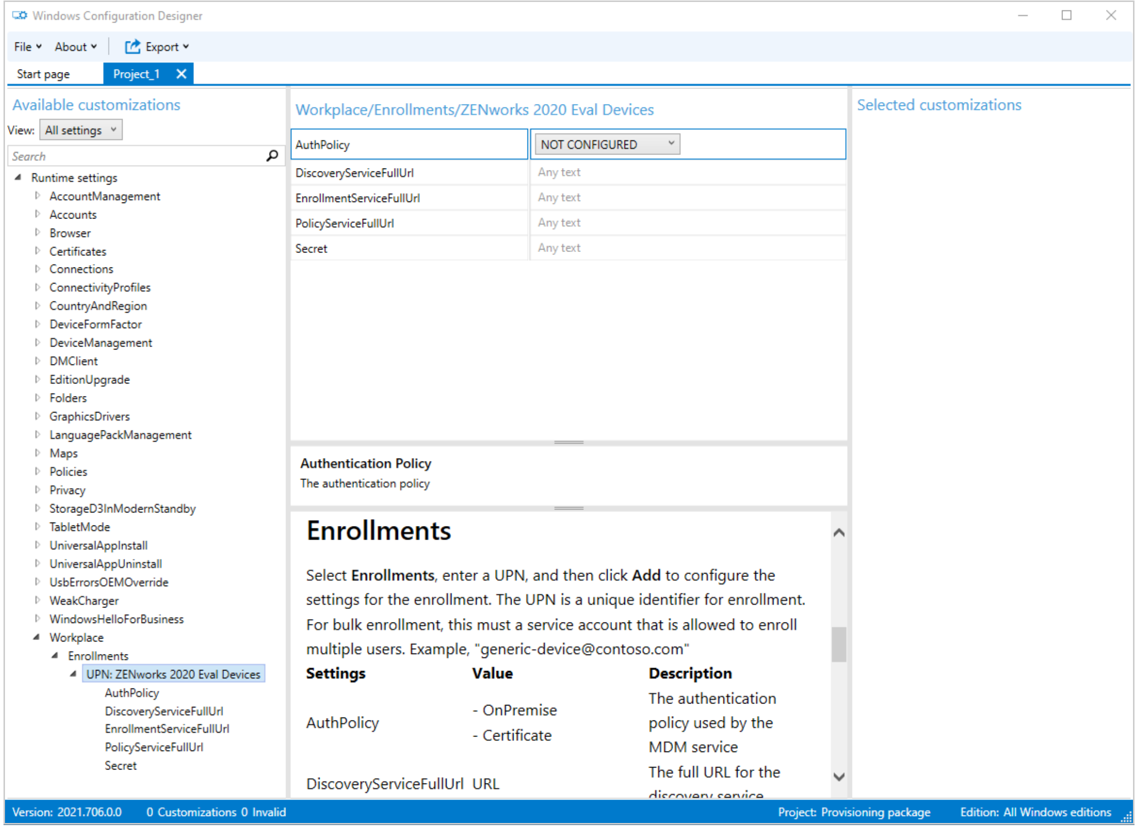


Enrollments

To add a new item under Enrollments, specify a UPN and then select the added item in the Available customizations pane to configure additional settings for this item.

8 In the UPN field, enter an enrollment name (such as ZENworks 2020 Eval Devices), then click **Add**.

9 In the left navigation, click the UPN that was just added under Enrollments to display the enrollment settings.



Workplace/Enrollments/ZENworks 2020 Eval Devices

AuthPolicy	NOT CONFIGURED
DiscoveryServiceFullUrl	Any text
EnrollmentServiceFullUrl	Any text
PolicyServiceFullUrl	Any text
Secret	Any text

Authentication Policy

The authentication policy

Enrollments

Select **Enrollments**, enter a UPN, and then click **Add** to configure the settings for the enrollment. The UPN is a unique identifier for enrollment. For bulk enrollment, this must a service account that is allowed to enroll multiple users. Example, "generic-device@contoso.com"

Settings	Value	Description
AuthPolicy	- OnPremise - Certificate	The authentication policy used by the MDM service
DiscoveryServiceFullUrl	URL	The full URL for the discovery service

10 Fill in the following fields:

- **AuthPolicy:** Select **OnPremise**.
- **DiscoveryServiceFullUrl:** Enter your ZENworks MDM enrollment URL. It will be:

  `https://<ZEN_Server>/zenworks-win-mdm/registration/discoveryservice`

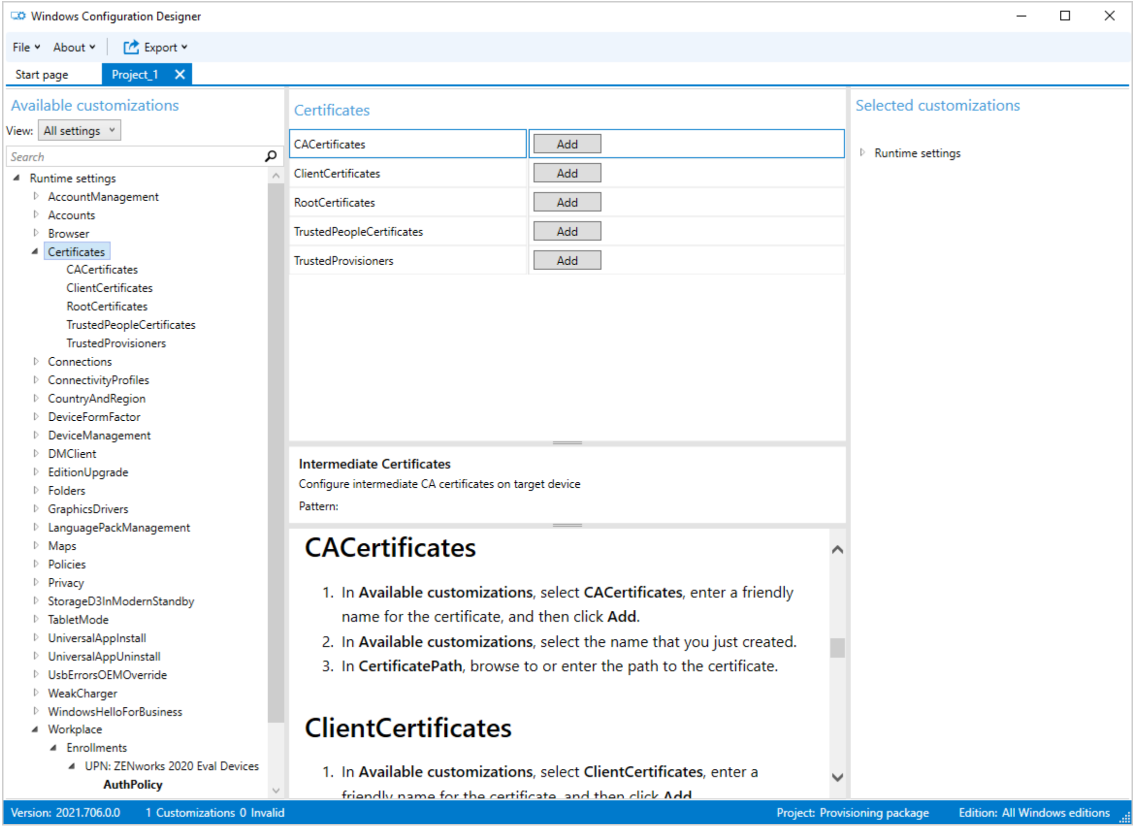
  where `<ZEN_Server>` is the IP address or hostname of your ZENworks Primary Server.
- **Secret:** Enter your ZENworks registration and authorization keys in the following format. Make sure to leave a space between the two entries:

  `regkey:<key> authkey:<key>`

  For example:

  `regkey:ec9f48d8-91e8-b60c-2842-7a5756bf6531 authkey:bf84-e37c6`

11 In the left navigation, click **Certificates** (under Runtime settings) to display the Certificates page.



Certificates

CACertificates	Add
ClientCertificates	Add
RootCertificates	Add
TrustedPeopleCertificates	Add
TrustedProvisioners	Add

Intermediate Certificates

Configure intermediate CA certificates on target device

Pattern:

CACertificates

1. In **Available customizations**, select **CACertificates**, enter a friendly name for the certificate, and then click **Add**.
2. In **Available customizations**, select the name that you just created.
3. In **CertificatePath**, browse to or enter the path to the certificate.

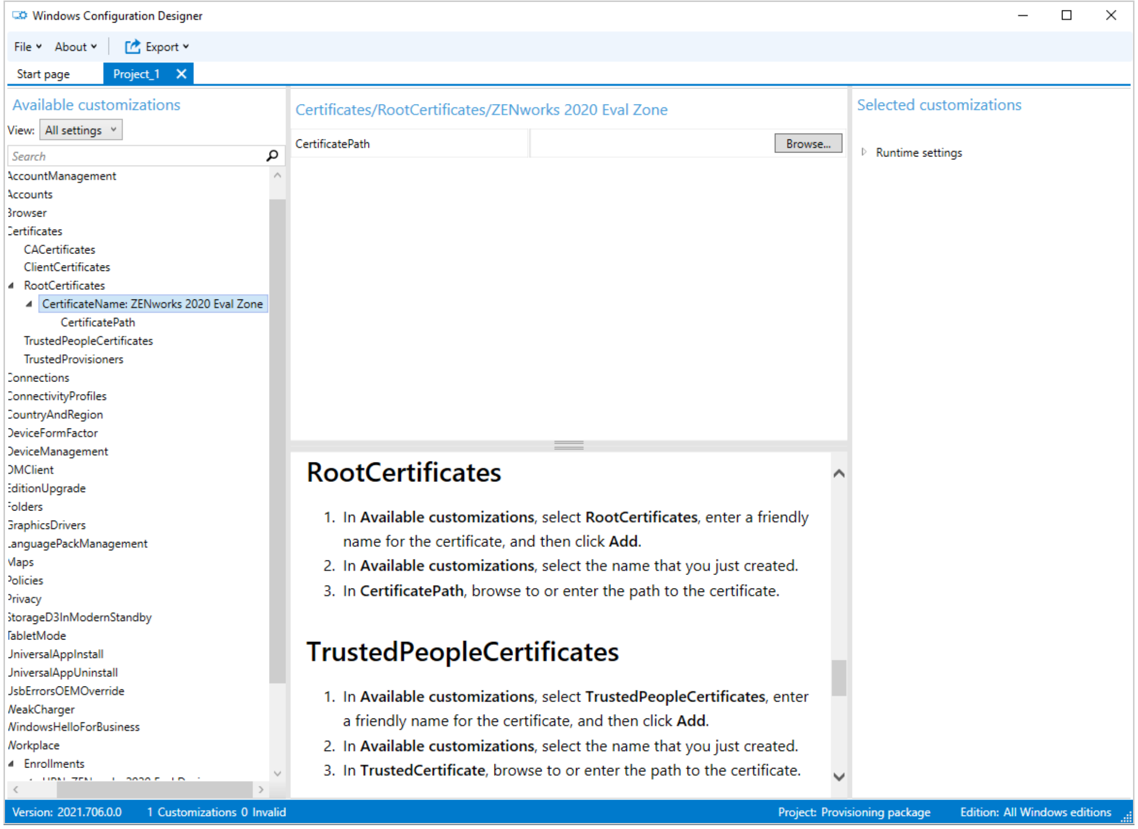
ClientCertificates

1. In **Available customizations**, select **ClientCertificates**, enter a friendly name for the certificate, and then click **Add**

12 In the RootCertificates field, click **Add**.

13 Enter a certificate name (such as ZENworks 2020 Eval Zone), then click **Add**.

14 In the left navigation, click the **CertificateName** you just added to display the CertificatePath field.



RootCertificates

1. In **Available customizations**, select **RootCertificates**, enter a friendly name for the certificate, and then click **Add**.
2. In **Available customizations**, select the name that you just created.
3. In **CertificatePath**, browse to or enter the path to the certificate.

TrustedPeopleCertificates

1. In **Available customizations**, select **TrustedPeopleCertificates**, enter a friendly name for the certificate, and then click **Add**.
2. In **Available customizations**, select the name that you just created.
3. In **TrustedCertificate**, browse to or enter the path to the certificate.

15 In the CertificatePath field, click **Browse**, then select the ZENworks zone certificate you downloaded.

16 At this point, click **File** > **Save** to save your project.

17 Click **Export** > **Provisioning Package** and follow the prompts to create the package.

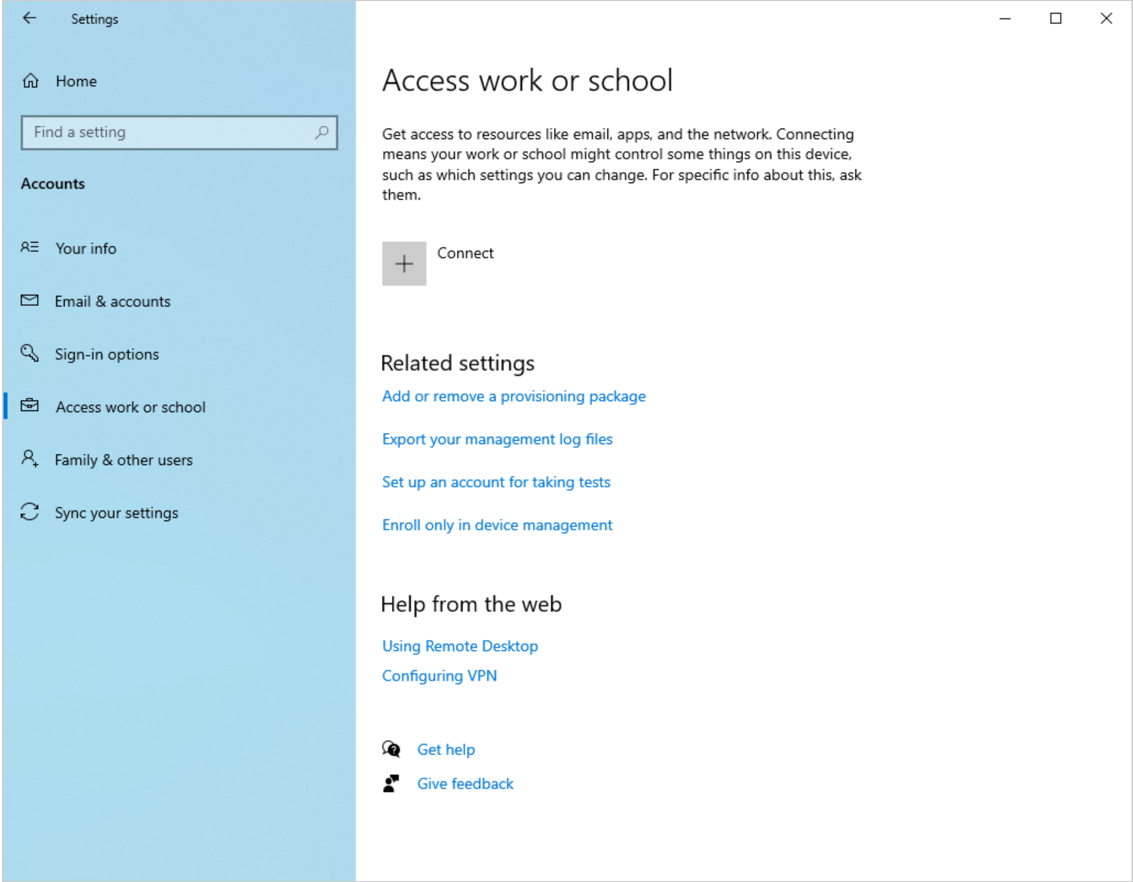
18 Copy the provisioning package to a USB drive.

4.1.3 Enroll a Device

1 On the Windows 10 device, log in through an account with Administrator privileges.

2 Insert the USB drive containing the provisioning package you created.

3 Click **Start** > **Settings** > **Accounts** > **Access work or school**.



Access work or school

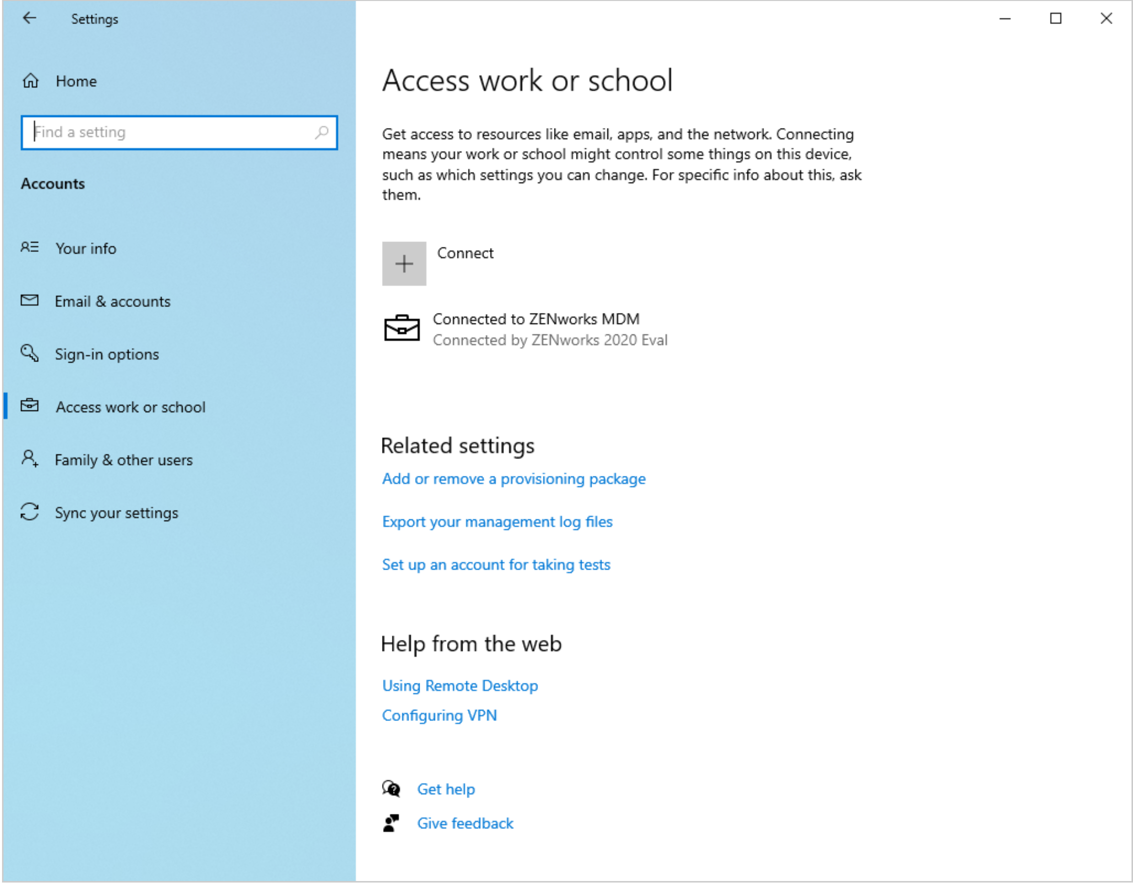
Get access to resources like email, apps, and the network. Connecting means your work or school might control some things on this device, such as which settings you can change. For specific info about this, ask them.

Connect
Related settings
Add or remove a provisioning package
Export your management log files
Set up an account for taking tests
Enroll only in device management
Help from the web
Using Remote Desktop
Configuring VPN
Get help
Give feedback

4 Click **Add or remove a provisioning package**.

5 Click **Add a package**, select the provisioning package and click **Add**, then follow the prompts to install the package.

6 Return to the Access work or school page to verify that the device is enrolled.



Access work or school

Get access to resources like email, apps, and the network. Connecting means your work or school might control some things on this device, such as which settings you can change. For specific info about this, ask them.

Connect

Connected to ZENworks MDM
Connected by ZENworks 2020 Eval

Related settings

Add or remove a provisioning package

Export your management log files

Set up an account for taking tests

Help from the web

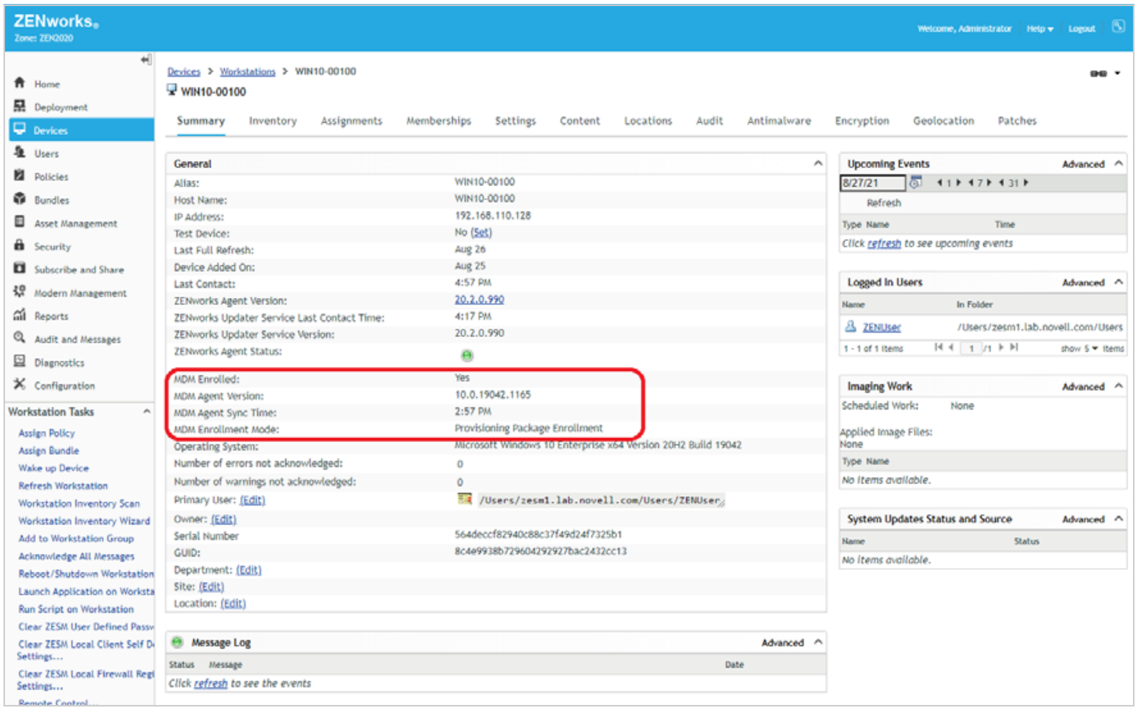
Using Remote Desktop

Configuring VPN

Get help

Give feedback

7 In ZENworks Control Center, click **Devices** > **Workstations**, then click the device to display its details and verify that it is MDM enrolled.



Devices > Workstations > WIN10-00100

WIN10-00100

General

Alias:	WIN10-00100
Host Name:	WIN10-00100
IP Address:	192.168.110.128
Test Device:	No (Set)
Last Full Refresh:	Aug 26
Device Added On:	Aug 25
Last Contact:	4:57 PM
ZENworks Agent Version:	20.2.0.990
ZENworks Updater Service Last Contact Time:	4:17 PM
ZENworks Updater Service Version:	20.2.0.990
ZENworks Agent Status:	●
MDM Enrolled:	Yes
MDM Agent Version:	10.0.19042.1165
MDM Agent Sync Time:	2:57 PM
MDM Enrollment Mode:	Provisioning Package Enrollment
Operating System:	Microsoft Windows 10 Enterprise x64 Version 20H2 Build 19042
Number of errors not acknowledged:	0
Number of warnings not acknowledged:	0
Primary User: (Edit)	/Users/zesm1.lab.novell.com/Users/ZENUser
Owner: (Edit)	
Serial Number	564deccf82940c88c37f49d24f7325b1
GUID:	8c4e9938b729604292927bac2432cc13
Department: (Edit)	
Site: (Edit)	
Location: (Edit)	

Message Log Advanced

Status	Message	Date
Click refresh to see the events		

Upcoming Events Advanced

8/27/21 ◀ 1 ▶ ◀ 7 ▶ ◀ 31 ▶

Refresh

Type	Name	Time
Click refresh to see upcoming events		

Logged In Users Advanced

Name	In Folder
ZENUser	/Users/zesm1.lab.novell.com/Users

1 - 1 of 1 items | 1 /1 | show 5 items

Imaging Work Advanced

Scheduled Work: None

Applied Image Files:
None

Type	Name
No items available.	

System Updates Status and Source Advanced

Name	Status
No items available.	

4.2 Secure the Device

ZENworks lets you deploy Configuration Service Providers (CSPs) to set, modify, or delete configuration settings on Windows 10 devices. The extensive list of configuration settings you can control is documented in the Microsoft Configuration Server Provider Reference (https://docs.microsoft.com/en-us/windows/client-management/mdm/configuration-service-provider-reference).

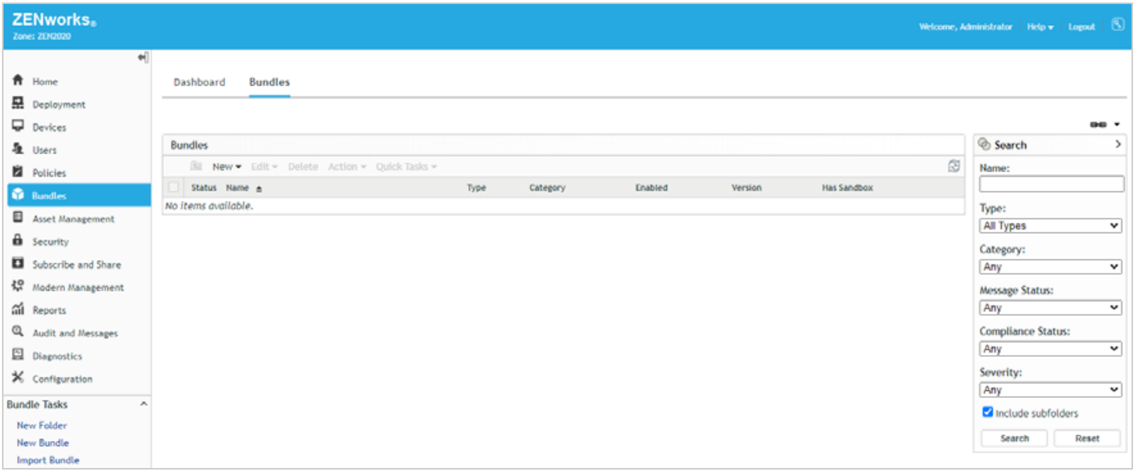
We'll use the Policy CSP to change the device's minimum password length from the standard 4 characters to 12 characters.

- Create a Windows 10 MDM CSP Bundle (page 59)
- Test the Bundle (page 60)

4.2.1 Create a Windows 10 MDM CSP Bundle

ZENworks uses its bundle system to distribute CSPs to devices. We'll have you create a Windows 10 MDM CSP bundle to distribute the Policy CSP to the device and change its minimum password length requirement to 12 characters.

1 In ZENworks Control Center, click **Bundles** (in the left navigation pane).



2 Click **New** > **Bundle** to display the Create New Bundle wizard.

3 On the Select Bundle Type page, select **Windows MDM Bundle**, then click **Next**.

4 On the Select Bundle Category page, select **Windows 10 MDM CSP**, then click **Next**.

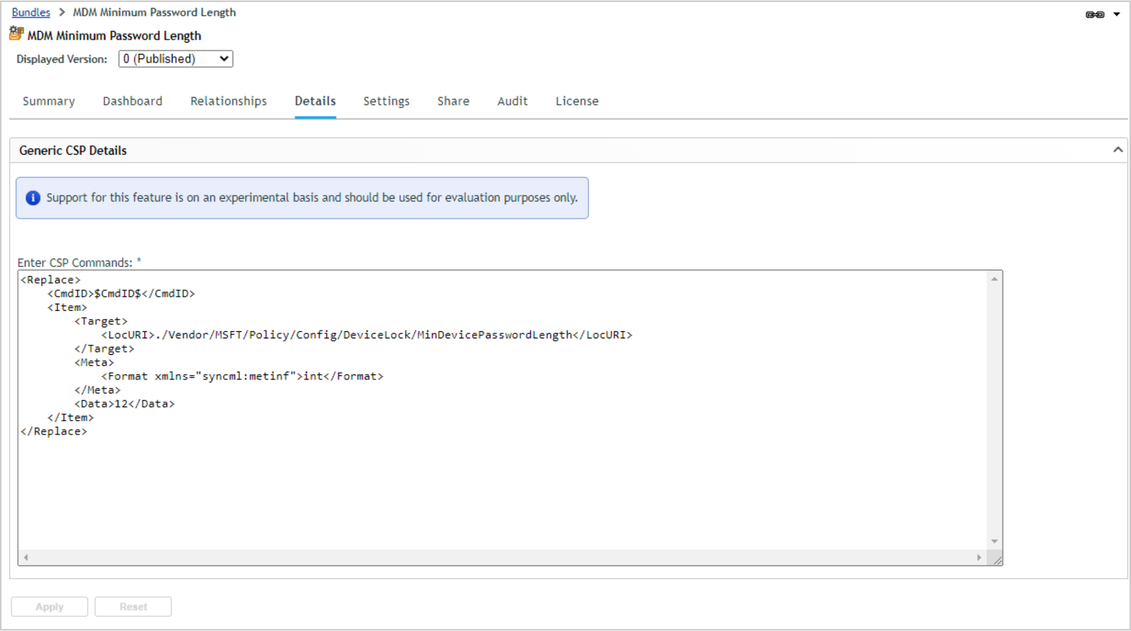
5 On the Define Details page, specify *MDM Minimum Password Length* for the bundle name, then click **Next**.

6 On the Enter CSP Commands page, copy and paste the following XML, then click **Next**.

```
<Replace>
    <CmdID>$CmdID$</CmdID>
    <Item>
        <Target>
        <LocURI>./Vendor/MSFT/Policy/Config/DeviceLock/
MinDevicePasswordLength</LocURI>
        </Target>
        <Meta>
           <Format xmlns="syncml:metinf">int</Format>
         </Meta>
         <Data>12</Data>
          </Item>
</Replace>
```

IMPORTANT: The <LocURI> line is broken above because it is too long for the PDF page, but you must add it as one line (i.e. no line break) in the policy.

7 On the Summary page, deselect **Create as Sandbox**, select **Define Additional Properties**, then click **Finish** to create the policy and display it.



Displayed Version: 0 (Published)

Support for this feature is on an experimental basis and should be used for evaluation purposes only.

Enter CSP Commands: *

```
<Replace>
    <CmdID>$CmdID$</CmdID>
    <Item>
        <Target>
            <LocURI>./Vendor/MSFT/Policy/Config/DeviceLock/MinDevicePasswordLength</LocURI>
        </Target>
        <Meta>
            <Format xmlns="syncml:metinf">int</Format>
        </Meta>
        <Data>12</Data>
    </Item>
</Replace>
```

8 Assign the bundle to the Windows 10 device:

8a Click **Relationships**.

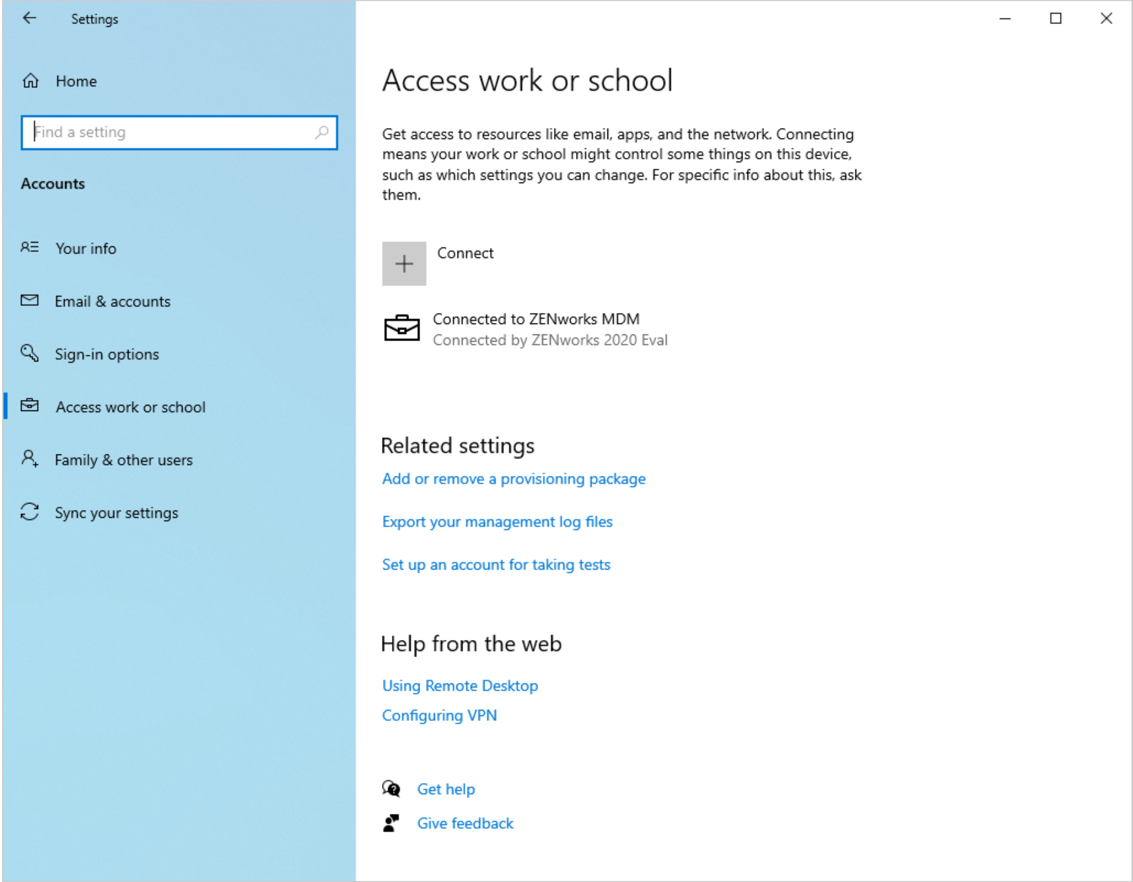
8b In the Device Assignments list, click **Add**.

8c Select the Windows 10 device, click **OK** to add the device to the Devices to be Assigned list.

8d Complete the assignment wizard keeping all of the defaults.

4.2.2 Test the Bundle

1 On the Windows 10 device, click **Start** > **Settings** > **Accounts** > **Access work or school**.



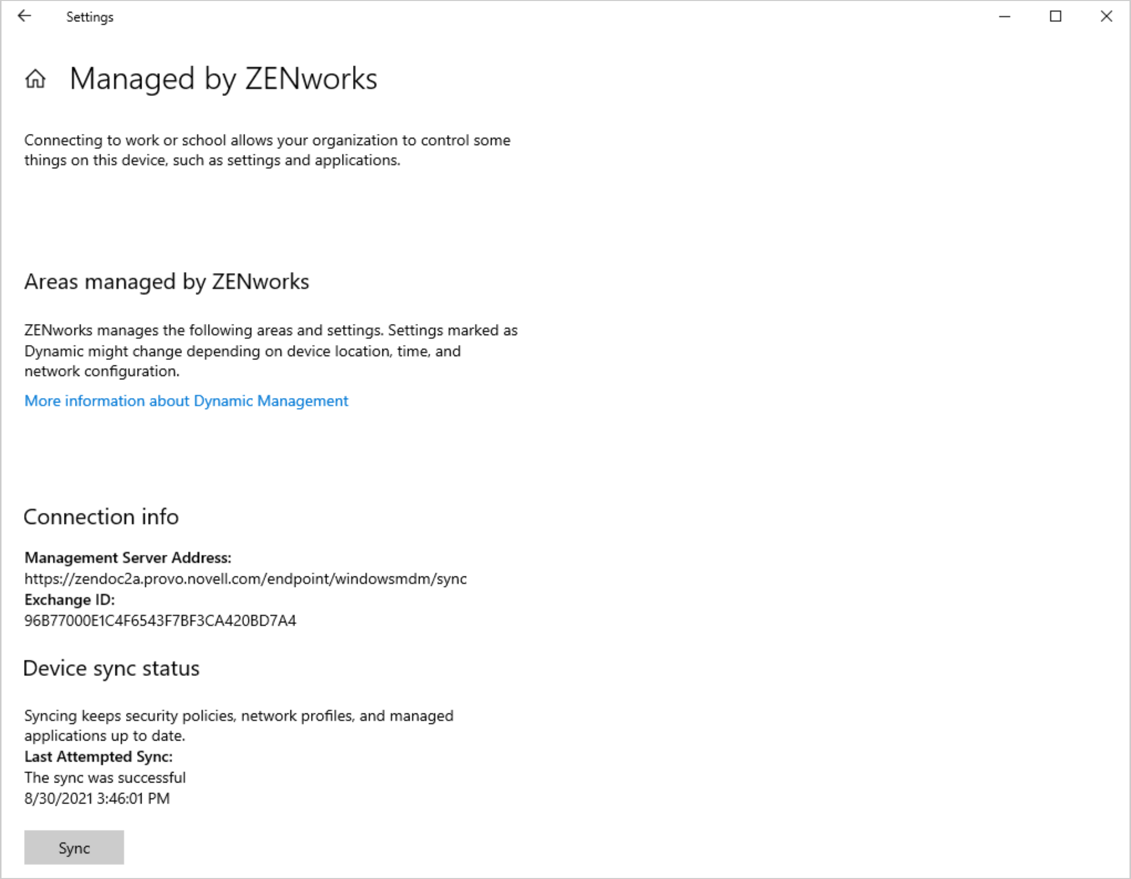
Access work or school

Get access to resources like email, apps, and the network. Connecting means your work or school might control some things on this device, such as which settings you can change. For specific info about this, ask them.

Connected to ZENworks MDM
Connected by ZENworks 2020 Eval

Related settings
Add or remove a provisioning package
Export your management log files
Set up an account for taking tests
Help from the web
Using Remote Desktop
Configuring VPN
Get help
Give feedback

2 Click **Connected to ZENworks MDM**, then click **Info** to display the Managed by ZENworks page.



Managed by ZENworks

Connecting to work or school allows your organization to control some things on this device, such as settings and applications.

Areas managed by ZENworks

ZENworks manages the following areas and settings. Settings marked as Dynamic might change depending on device location, time, and network configuration.

More information about Dynamic Management

Connection info

Management Server Address:
https://zendoc2a.provo.novell.com/endpoint/windowsmdm/sync
Exchange ID:
96B77000E1C4F6543F7BF3CA420BD7A4

Device sync status

Syncing keeps security policies, network profiles, and managed applications up to date.
Last Attempted Sync:
The sync was successful
8/30/2021 3:46:01 PM

3 Click **Sync** to download the bundle and update the DeviceLock policy with the new minimum password length requirement.

By default, ZENworks initiates an MDM sync automatically every 125 minutes. We did a manual sync only to avoid waiting for the next auto sync.

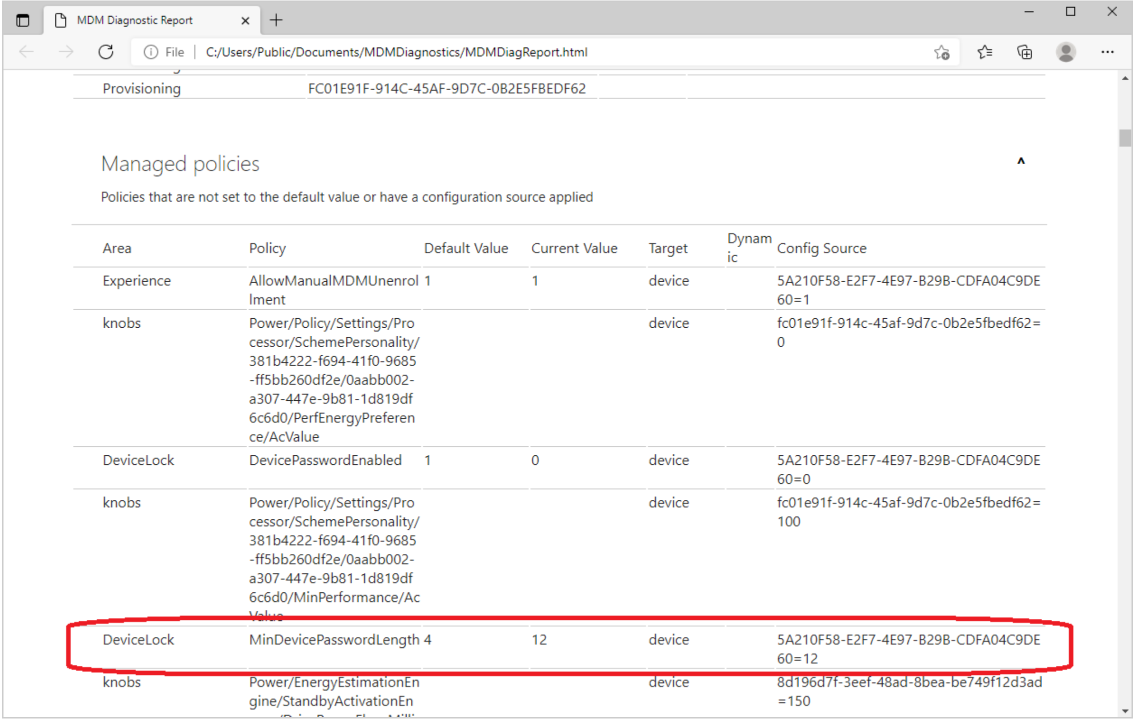
4 On the same page under Advanced Diagnostic Report, click **Create Report**.

An `MDMDiagReport.html` file is created in the following directory:

`C:\Users\Public\Documents\MDMDiagnostics`

5 Open the file in a web browser and locate the DeviceLock MinDevicePasswordLength entry in the Managed Policies section.

You'll notice that the Current Value for the policy is 12.



Provisioning	FC01E91F-914C-45AF-9D7C-0B2E5FBEDF62

Managed policies

Policies that are not set to the default value or have a configuration source applied

Area	Policy	Default Value	Current Value	Target	Dynamic	Config Source
Experience	AllowManualMDMUnenrollment	1	1	device		5A210F58-E2F7-4E97-B29B-CDFA04C9DE60=1
knobs	Power/Policy/Settings/Processor/SchemePersonality/381b4222-f694-41f0-9685-ff5bb260df2e/0aabb002-a307-447e-9b81-1d819df6c6d0/PerfEnergyPreference/AcValue			device		fc01e91f-914c-45af-9d7c-0b2e5fbedf62=0
DeviceLock	DevicePasswordEnabled	1	0	device		5A210F58-E2F7-4E97-B29B-CDFA04C9DE60=0
knobs	Power/Policy/Settings/Processor/SchemePersonality/381b4222-f694-41f0-9685-ff5bb260df2e/0aabb002-a307-447e-9b81-1d819df6c6d0/MinPerformance/AcValue			device		fc01e91f-914c-45af-9d7c-0b2e5fbedf62=100
DeviceLock	MinDevicePasswordLength	4	12	device		5A210F58-E2F7-4E97-B29B-CDFA04C9DE60=12
knobs	Power/EnergyEstimationEngine/StandbyActivationEn			device		8d196d7f-3eef-48ad-8bea-be749f12d3ad=150

6 Restart the device and log in.

After entering your Windows password, you’ll be prompted to change it to meet the new minimum password length requirement.

This is just one simple example of the configuration settings you can manage via MDM on Windows 10 devices. You’ll want to refer to the Microsoft Configuration Server Provider Reference to see what else you can manage as well as how to create the code required in the Windows 10 MDM CSP policy.

IMPORTANT: Removing the Windows 10 MDM CSP bundle will not revert the configuration setting to its previous value. To change the configuration setting value again, you’ll need to modify the Windows 10 MDM CSP bundle and sync the device.

4.3 Distribute an MSI Application

ZENworks lets you distribute applications that use the Microsoft Installer (MSI) package. The MSI package is deployed using the EnterpriseDesktopAppManagement CSP.

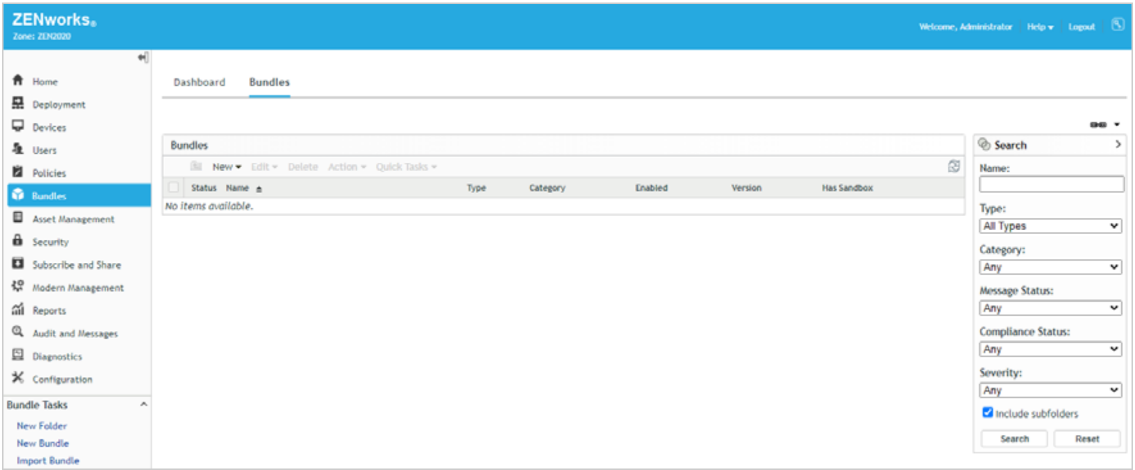
For this evaluation, we’ll distribute the free Notepad++ application.

- Section 4.3.1, “Create a Windows 10 MDM Bundle,” on page 64
- Section 4.3.2, “Test the Bundle,” on page 66

4.3.1 Create a Windows 10 MDM Bundle

1 Download the Notepad++ MSI package from https://notepad-plus-plus.org/downloads/.

2 In ZENworks Control Center, click **Bundles** (in the left navigation pane).



	Status	Name	Type	Category	Enabled	Version	Has Sandbox
No items available.							

Name:

Type: All Types

Category: Any

Message Status: Any

Compliance Status: Any

Severity: Any

☑ Include subfolders

3 Click **New** > **Bundle** to display the Create New Bundle wizard.

4 On the Select Bundle Type page, select **Windows MDM Bundle**, then click **Next**.

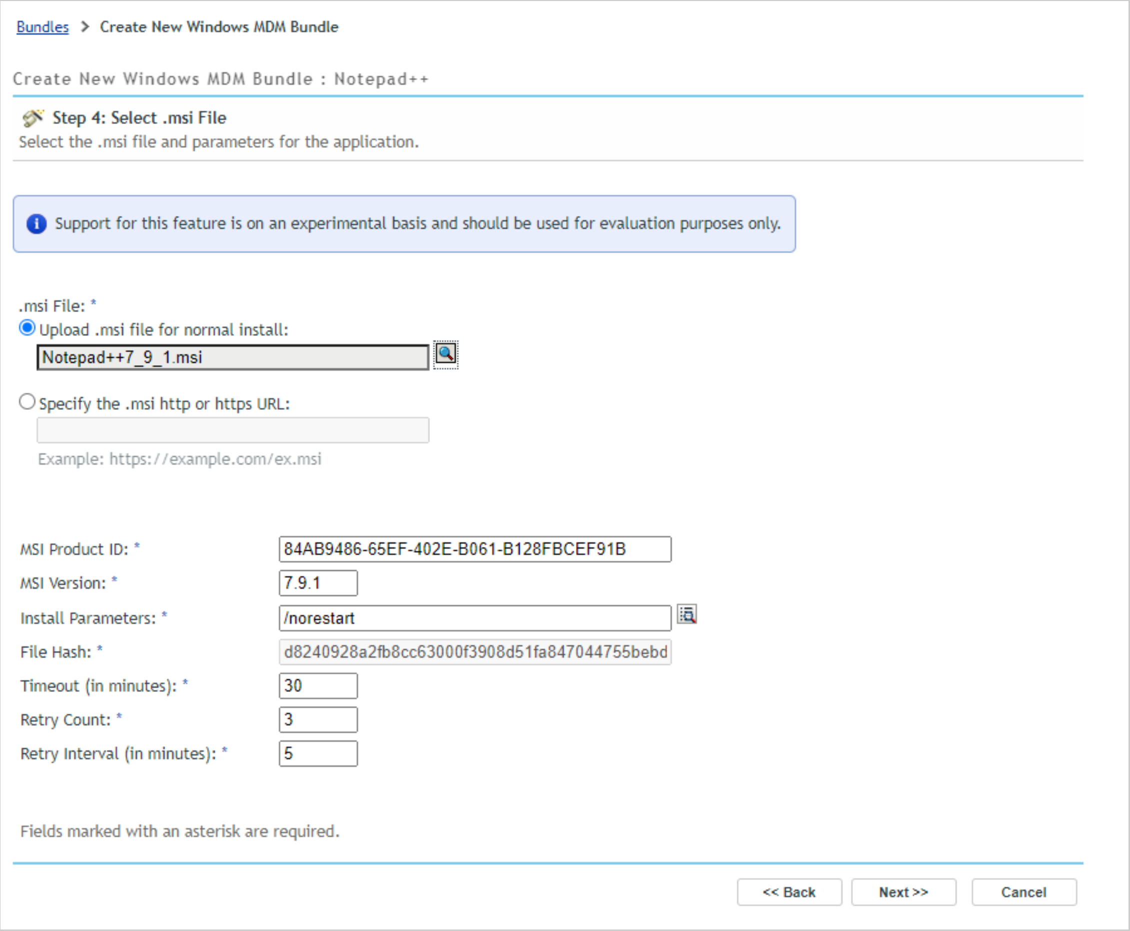
5 On the Select Bundle Category page, select **Windows 10 MDM - Install MSI**, then click **Next**.

6 On the Define Details page, enter *Notepad++* as the bundle name, then click **Next**.

7 On the Select .msi File page, click the Browse icon 🔍 for the **Upload.mis file for normal install** field, then use the ZCC Helper to upload the Notepad++ MSI file, then click **Next**.

If you are prompted to download and install the ZCC Helper, do so. Once it is installed, click **Launch** and then select the MSI package to upload.

After the Notepad++ MSI file is uploaded, the MSI details are populated automatically.



Bundles > Create New Windows MDM Bundle

Create New Windows MDM Bundle : Notepad++

Step 4: Select .msi File

Select the .msi file and parameters for the application.

Support for this feature is on an experimental basis and should be used for evaluation purposes only.

.msi File: *

● Upload .msi file for normal install:

Notepad++7_9_1.msi

○ Specify the .msi http or https URL:

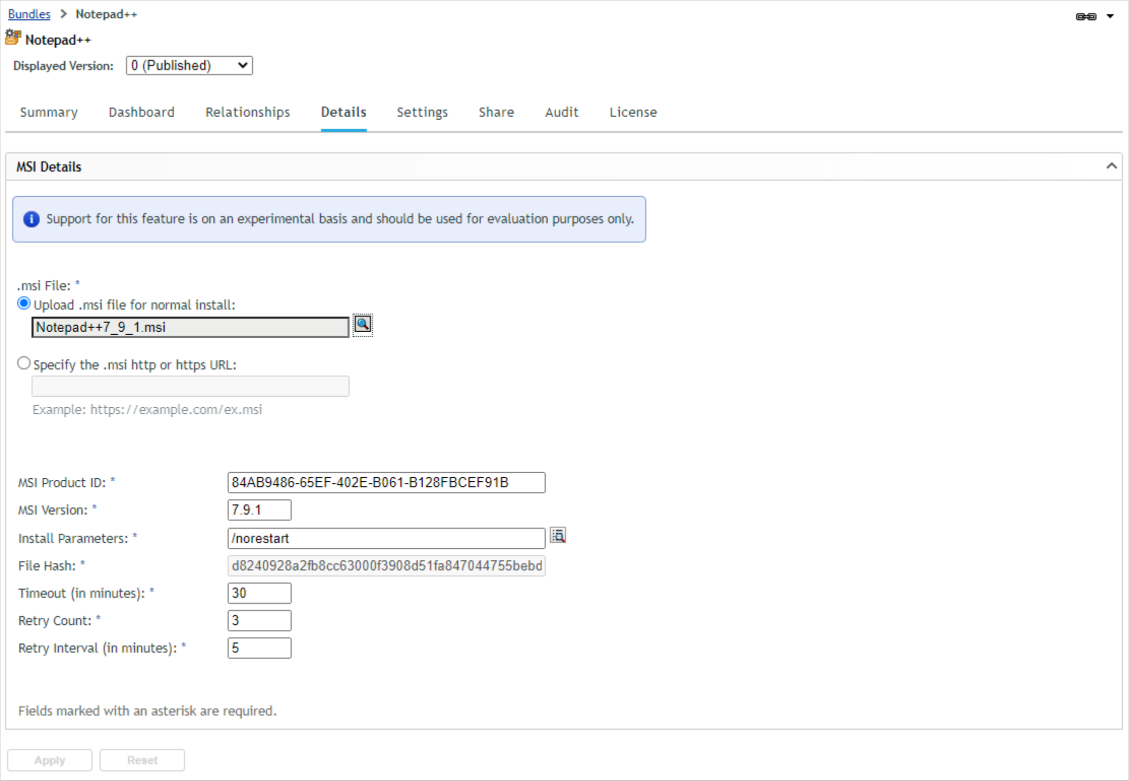
Example: https://example.com/ex.msi

MSI Product ID: *	84AB9486-65EF-402E-B061-B128FBCEF91B
MSI Version: *	7.9.1
Install Parameters: *	/norestart
File Hash: *	d8240928a2fb8cc63000f3908d51fa847044755bebd
Timeout (in minutes): *	30
Retry Count: *	3
Retry Interval (in minutes): *	5

Fields marked with an asterisk are required.

8 On the Summary page, deselect **Create as Sandbox** and select **Define Additional Properties**, then click **Finish**.

The bundle's Details page is displayed.



Displayed Version: 0 (Published)

Support for this feature is on an experimental basis and should be used for evaluation purposes only.

.msi File: *

● Upload .msi file for normal install: Notepad++7_9_1.msi

○ Specify the .msi http or https URL:

Example: https://example.com/ex.msi

MSI Product ID: *	84AB9486-65EF-402E-B061-B128FBCEF91B
MSI Version: *	7.9.1
Install Parameters: *	/norestart
File Hash: *	d8240928a2fb8cc63000f3908d51fa847044755bebd
Timeout (in minutes): *	30
Retry Count: *	3
Retry Interval (in minutes): *	5

Fields marked with an asterisk are required.

9 Assign the bundle to your Windows device:

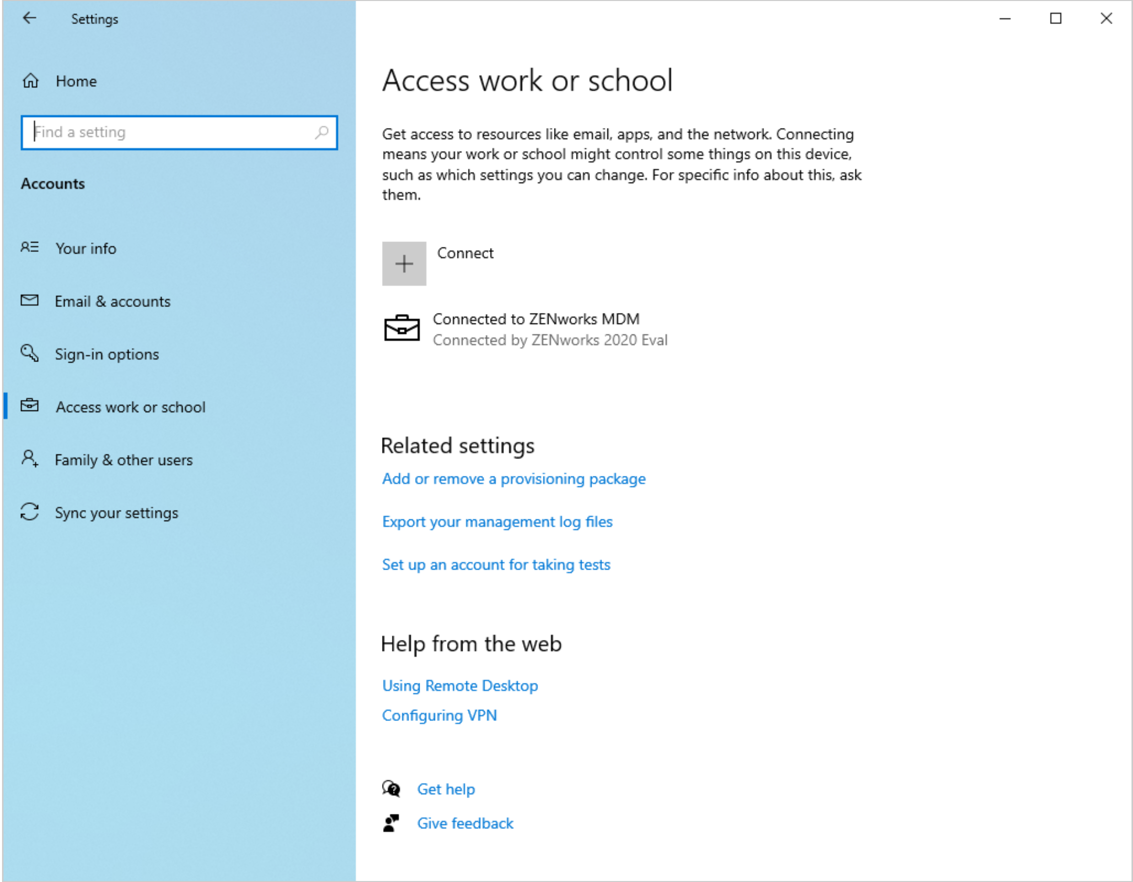
9a Click the **Relationships** tab.

9b In the Device Assignments list, click **Add**, then follow the prompts to assign the bundle.

As you go through the assignment wizard, keep the default settings.

4.3.2 Test the Bundle

1 On the Windows 10 device, click **Start** > **Settings** > **Accounts** > **Access work or school**.



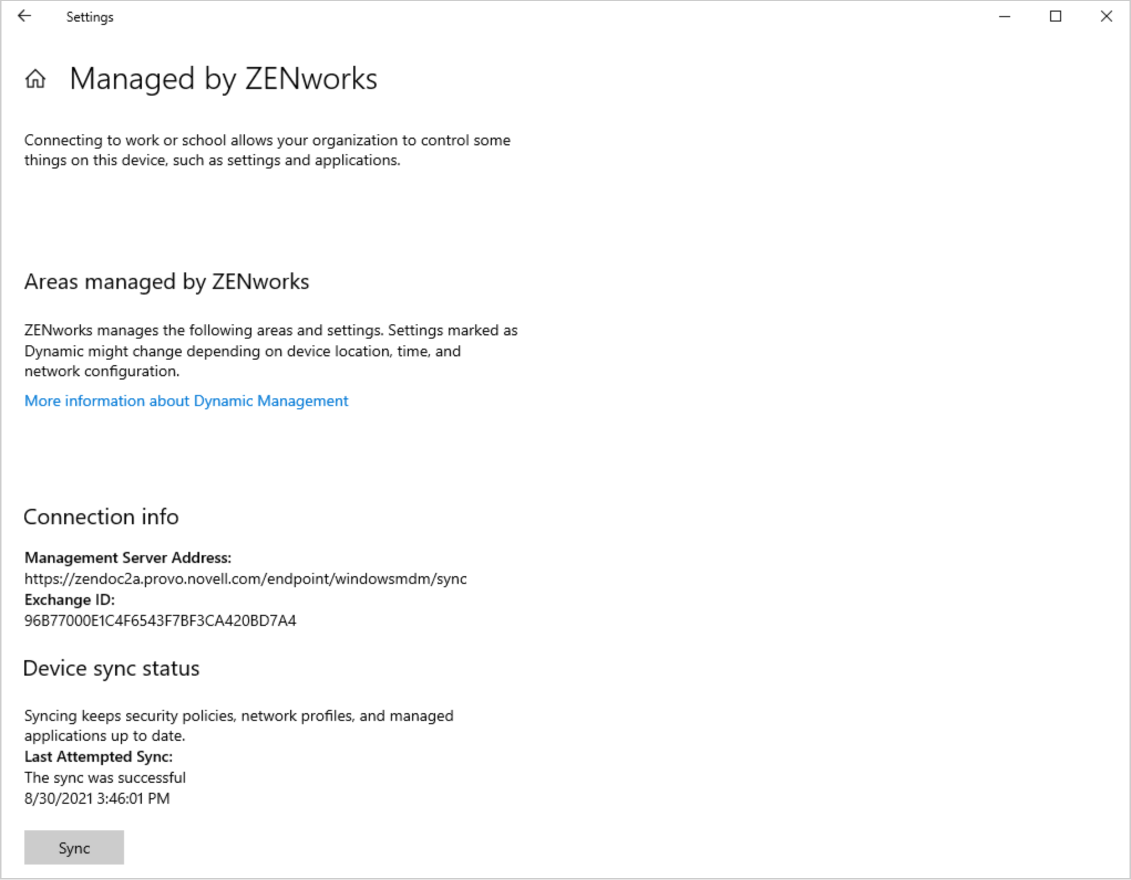
Access work or school

Get access to resources like email, apps, and the network. Connecting means your work or school might control some things on this device, such as which settings you can change. For specific info about this, ask them.

Connected to ZENworks MDM
Connected by ZENworks 2020 Eval

Related settings
Add or remove a provisioning package
Export your management log files
Set up an account for taking tests
Help from the web
Using Remote Desktop
Configuring VPN
Get help
Give feedback

2 Click **Connected to ZENworks MDM**, then click **Info** to display the Managed by ZENworks page.



Managed by ZENworks

Connecting to work or school allows your organization to control some things on this device, such as settings and applications.

Areas managed by ZENworks

ZENworks manages the following areas and settings. Settings marked as Dynamic might change depending on device location, time, and network configuration.

More information about Dynamic Management

Connection info

Management Server Address:
https://zendoc2a.provo.novell.com/endpoint/windowsmdm/sync
Exchange ID:
96B77000E1C4F6543F7BF3CA420BD7A4

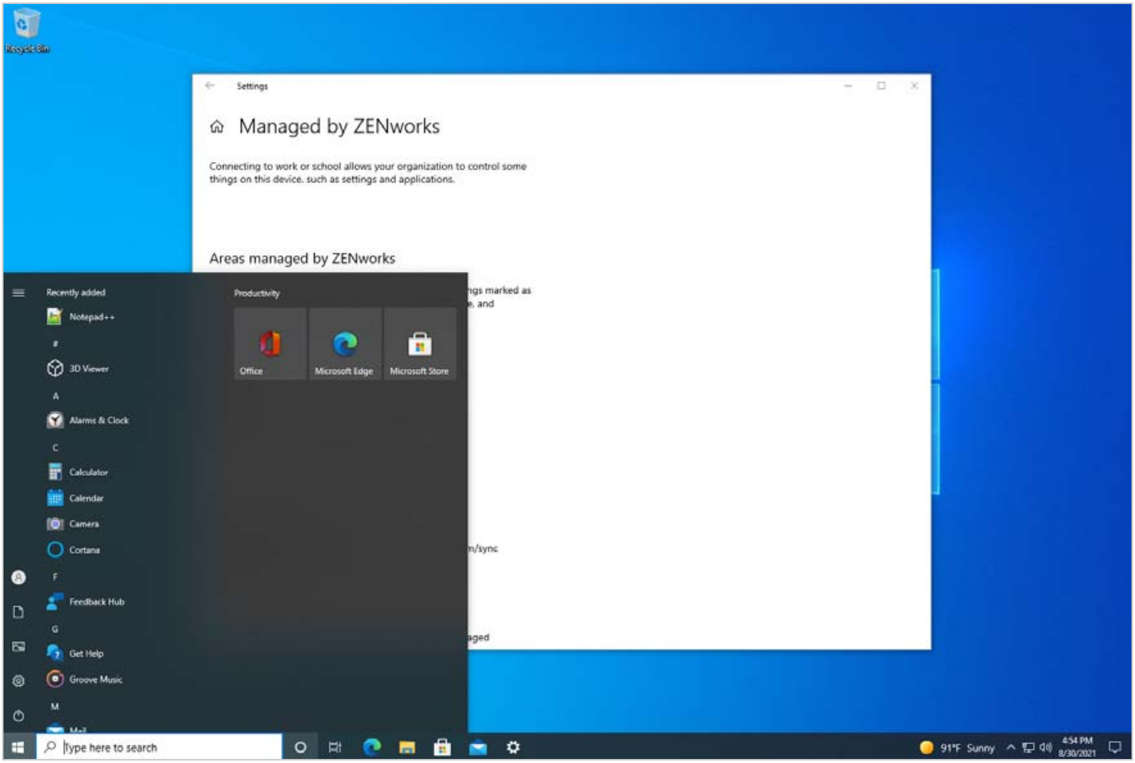
Device sync status

Syncing keeps security policies, network profiles, and managed applications up to date.
Last Attempted Sync:
The sync was successful
8/30/2021 3:46:01 PM

3 Click **Sync** to download and install the bundle.

By default, ZENworks initiates an MDM sync automatically every 125 minutes. We did a manual sync only to avoid waiting for the next auto sync.

After a minute or two, Notepad++ is installed and you can see it as a recently added app on the Start menu.

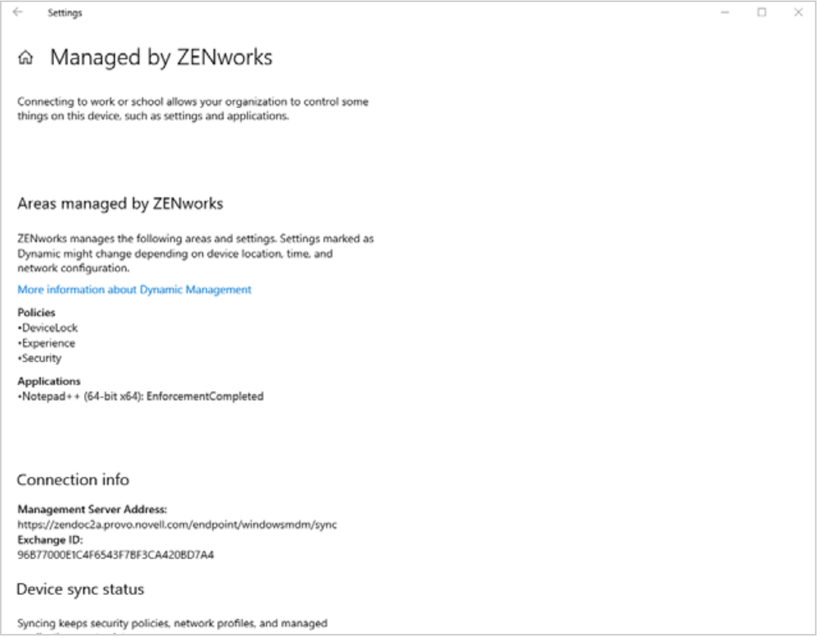


Managed by ZENworks

Connecting to work or school allows your organization to control some things on this device, such as settings and applications.

Areas managed by ZENworks

4 Refresh the Managed by ZENworks page and Notepad++ is displayed under the managed applications.



Managed by ZENworks

Connecting to work or school allows your organization to control some things on this device, such as settings and applications.

Areas managed by ZENworks

ZENworks manages the following areas and settings. Settings marked as Dynamic might change depending on device location, time, and network configuration.

More information about Dynamic Management

Policies
•DeviceLock
•Experience
•Security

Applications
•Notepad++ (64-bit x64): EnforcementCompleted

Connection info

Management Server Address:
https://zendoc2a.provo.novell.com/endpoint/windowsmdm/sync
Exchange ID:
96B77000E1C4F6543F7BF3CA420BD7A4

Device sync status

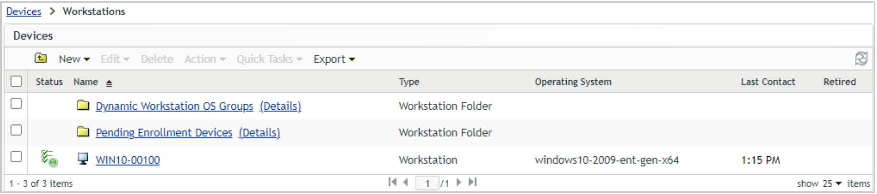
Syncing keeps security policies, network profiles, and managed

4.4 Unenroll Your Windows Devices

If you no longer want your device MDM enrolled with ZENworks, you can unenroll the device from the zone. Unregistering a device removes all assignments from the device and deletes the device from the ZENworks databases. Retiring a device removes all assignments but leaves the device, including its inventory data, in the database.

For this evaluation, we'll have you unregister and uninstall the device.

1 In ZENworks Control Center, click **Devices** > **Workstations** to display your enrolled Windows device.



Devices > Workstations

Devices

□	Status	Name	Type	Operating System	Last Contact	Retired
□		Dynamic Workstation OS Groups (Details)	Workstation Folder			
□		Pending Enrollment Devices (Details)	Workstation Folder			
□		WIN10-00100	Workstation	windows10-2009-ent-gen-x64	1:15 PM	

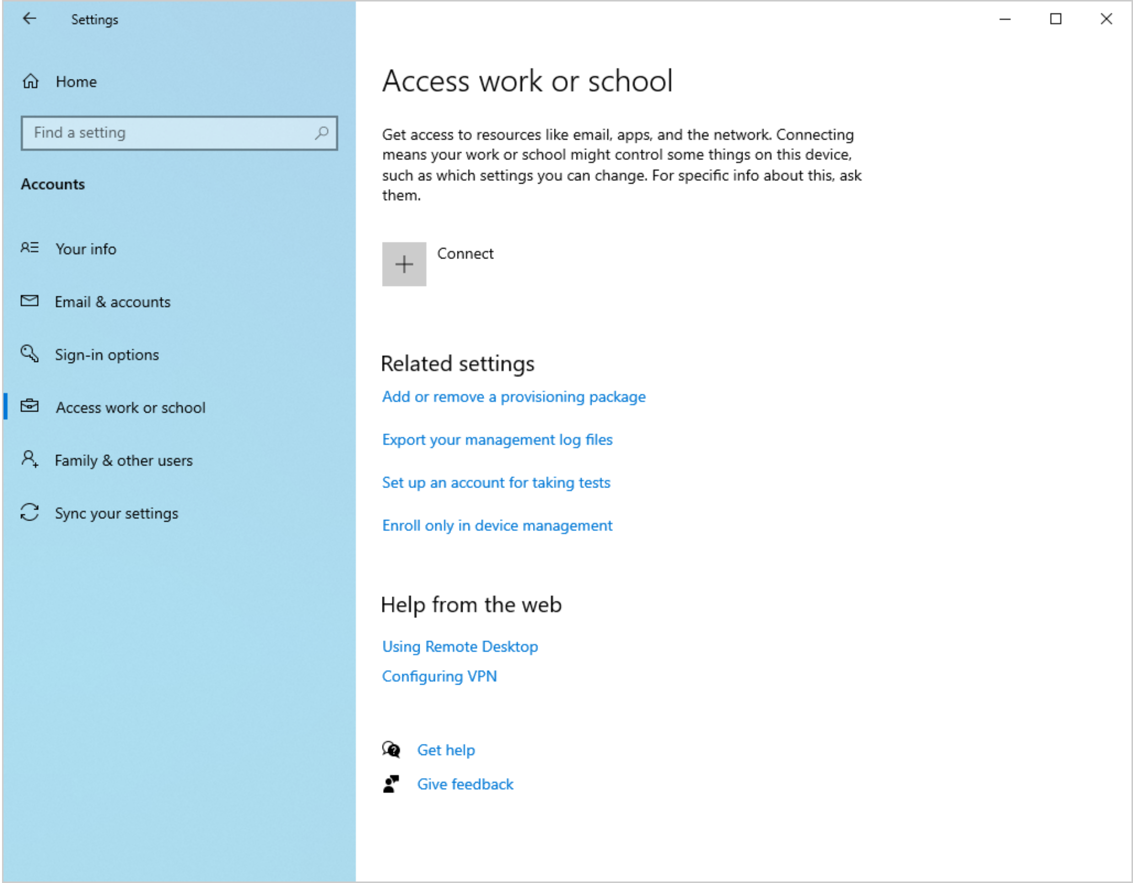
1 - 3 of 3 items 1 /1 show 25 items

2 Select the check box in front of the Windows device, click **Quick Tasks** > **Unenroll MDM Device Now**, then click **Start** when the Quick Task displays.

The Quick Task initiates the MDM unenrollment which can take several minutes.

3 After the Quick Task completes, go to the Windows 10 device, click **Start** > **Settings** > **Accounts** > **Access work or school**.

The page shows that the device is no longer managed by ZENworks.



Access work or school

Get access to resources like email, apps, and the network. Connecting means your work or school might control some things on this device, such as which settings you can change. For specific info about this, ask them.

Related settings

Add or remove a provisioning package
Export your management log files
Set up an account for taking tests
Enroll only in device management

Help from the web

5 Manage Mobile Devices

ZENworks manages iOS and Android devices using the native MDM capabilities of those platforms. We'll help you enroll iOS and Android devices in your ZENworks zone, secure the devices, and distribute apps to them.

- Section 5.1, "Enroll Mobile Devices," on page 73
- Section 5.2, "Secure Your Mobile Devices," on page 99
- Section 5.3, "Distribute an App to Your Mobile Devices," on page 106
- Section 5.4, "Unenroll Your iOS and Android Devices," on page 122

5.1 Enroll Mobile Devices

In order for mobile devices to be enrolled in your ZENworks Management Zone, you must create a Mobile Enrollment policy and assign it to any users who will enroll devices. The following sections help you create a Mobile Enrollment policy and then enroll iOS devices and Android devices:

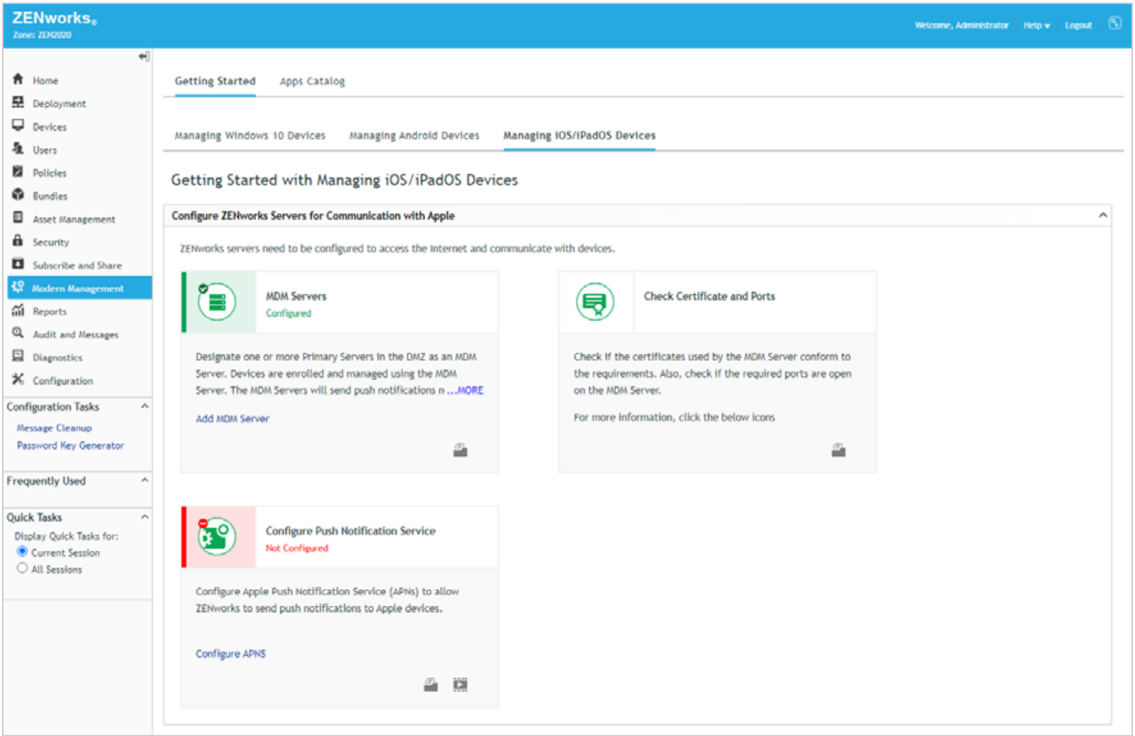
- Create a Mobile Enrollment Policy (page 74)
- Enroll an iOS Device (page 77)
- Enroll an Apple DEP iOS Device (page 80)
- Enroll an Android Device (page 89)

5.1.1 Create a Mobile Enrollment Policy

The Mobile Enrollment policy not only allows users to enroll devices but also assigns specific management settings to the device. For example, the policy determines the ZENworks name and group memberships assigned to the device, whether the device is designated as corporate owned or personal, and what happens to the device when it is unenrolled.

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. For the purpose of this evaluation, we'll have you create a single policy.

1 In ZENworks Control Center, go to Getting Started with Managing iOS/iPadOS Devices.



Getting Started with Managing iOS/iPadOS Devices

Configure ZENworks Servers for Communication with Apple

ZENworks servers need to be configured to access the Internet and communicate with devices.

MDM Servers
Configured

Designate one or more Primary Servers in the DMZ as an MDM Server. Devices are enrolled and managed using the MDM Server. The MDM Servers will send push notifications n ...MORE

Add MDM Server

Check Certificate and Ports

Check if the certificates used by the MDM Server conform to the requirements. Also, check if the required ports are open on the MDM Server.

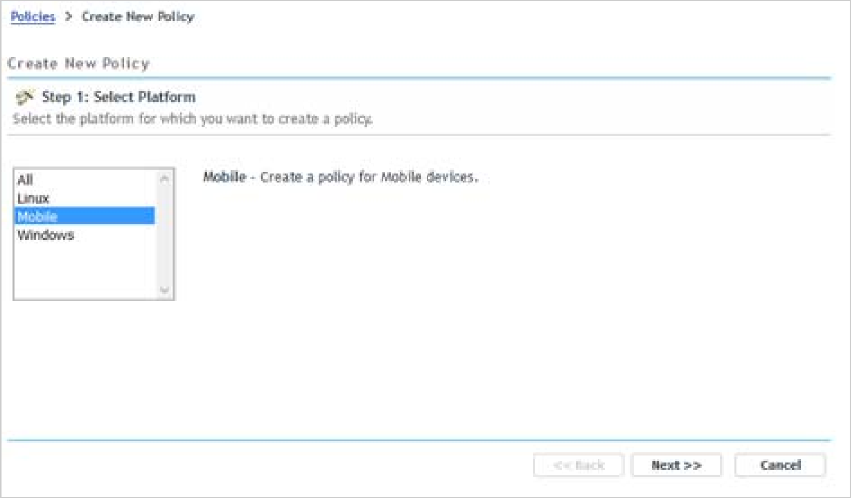
For more information, click the below icons

Configure Push Notification Service
Not Configured

Configure Apple Push Notification Service (APNs) to allow ZENworks to send push notifications to Apple devices.

Configure APNS

2 Scroll to the Enroll Users section, then click **Create Enrollment Policy** in the Enrollment Policy panel to display the Create New Policy wizard.



Policies > Create New Policy

Create New Policy

Step 1: Select Platform

Select the platform for which you want to create a policy.

Mobile - Create a policy for Mobile devices.

3 On the Select Platform page, select **Mobile**, then click **Next**.

4 On the Select Policy Category page, select **General Mobile Policies**, then click **Next**.

5 On the Select Policy Type page, select **Mobile Enrollment Policy**, then click **Next**.

6 On the Define Details page, specify a name for the policy (for example, *Mobile Enrollment*), then click **Next**.

7 On the Configure Device Ownership page:

7a Leave the Default Ownership set to **Corporate** for both enrollment methods.

Every mobile policy includes two groups of settings, one group that is applied to corporate devices and a second group that is applied to personal devices.

For example, the Mobile Security policy lets you configure different password, encryption, and lockout settings for corporate devices versus personal devices. When the Mobile Security policy is applied to a device, the device's ownership type determines which group of settings is applied

7b Under the *Enrollment using the ZENworks User Portal or the ZENworks Agent app* method, enable the **Allow the device user to select ownership type** option.

In a production environment, your corporate policy might dictate that you don't allow users to select the ownership type during enrollment. For this evaluation, however, we suggest that you enable the option so that you experience this enrollment method.

This option is not available for the *Enrollment through the Apple Device Enrollment Program (DEP) or Apple Configurator (during initial device setup)* method because these are silent enrollments; no options are displayed to the user.

7c Click **Next**

8 On the Configure Device Management Level page:

8a Review the differences between a fully managed device and an ActiveSync-only device:

- **Fully managed:** ZENworks can perform various device management operations such as apply policies to the device, deploy applications on the device, synchronize email from Exchange ActiveSync accounts, and capture device information (inventory). Only iOS or Android devices can be enrolled as managed devices. Full management of an

Android device is performed through the ZENworks App that is hosted on the Google Play Store. Full management of an iOS device is performed through the device's native MDM client.

- **ActiveSync only:** ZENworks can manage corporate emails on the device. Also, certain policies that are enforceable through the ActiveSync protocol, such as the Device Control Policy and Mobile Security Policy, can be applied to these device. Android, iOS, Blackberry, and Windows devices can be enrolled as ActiveSync only devices.

The default setting prompts the user to enroll as a fully managed device but allows the change from fully managed to ActiveSync-only. In a production environment, your corporate policy might dictate that you don't allow users to select the management level during enrollment. For this evaluation, however, we suggest that you allow the choice so that you can see what the option looks like when enrolling devices.

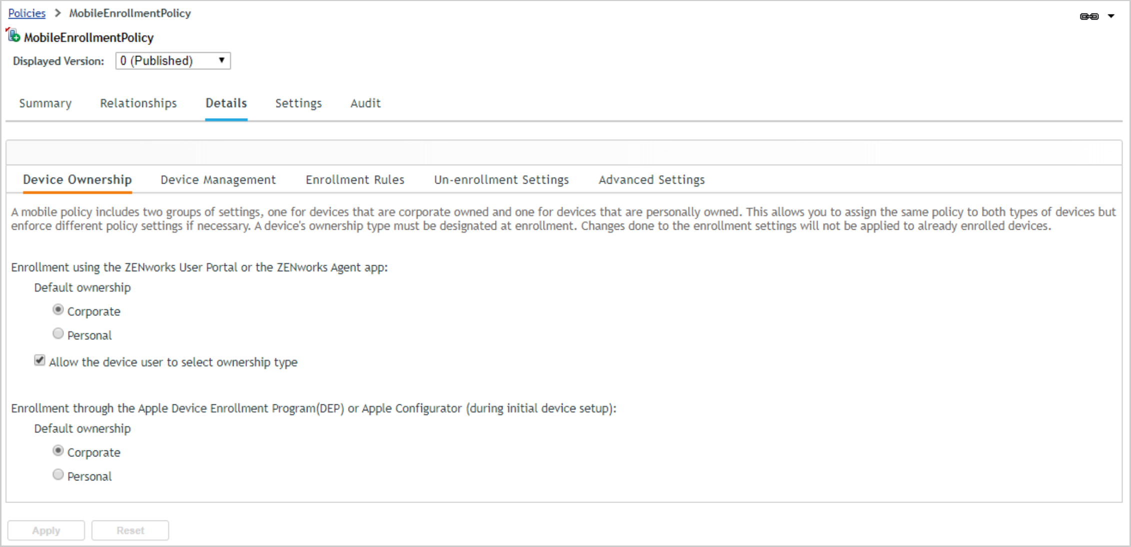
8b Keep the default setting so that devices are enrolled as fully managed, then click **Next**.

9 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 establish the criteria that a user's device must meet in order to enroll, and determines the enrolling device's display name, folder placement, and group assignments in ZENworks Control Center.

10 On the Configure the Un-enrollment Settings page, keep the default settings, then click **Next**.

11 On the Summary page, deselect **Create as Sandbox**, select **Define Additional Properties**, then click **Finish** to create the policy.



Displayed Version: 0 (Published)

A mobile policy includes two groups of settings, one for devices that are corporate owned and one for devices that are personally owned. This allows you to assign the same policy to both types of devices but enforce different policy settings if necessary. A device's ownership type must be designated at enrollment. Changes done to the enrollment settings will not be applied to already enrolled devices.

Enrollment using the ZENworks User Portal or the ZENworks Agent app:

Default ownership

● Corporate

○ Personal

☑ Allow the device user to select ownership type

Enrollment through the Apple Device Enrollment Program(DEP) or Apple Configurator (during initial device setup):

Default ownership

● Corporate

○ Personal

12 Assign the policy to your evaluation user:

12a Click **Relationships**.

12b In the User Assignments list, click **Add**.

12c Select the evaluation user, then click **OK** to add the user to the assignment list.

12d Click **Next** > **Finish** to complete the assignment.

5.1.2 Enroll an iOS Device

You can enroll any device running iOS version 10 or newer. We used an iPhone running iOS version 14.7.1. The screens and steps might vary slightly on other iOS devices and versions.

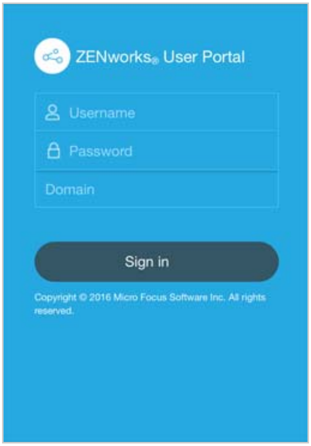
If the device you want to enroll is factory fresh and was purchased through the Apple Device Enrollment Program or has been added to the program via Apple Configurator (available for Apple devices running iOS version 11 or newer), use the instructions in "Enroll an Apple DEP iOS Device" on page 80 instead.

1 In the Safari browser on the iOS device, enter the following URL:

`*ZENworks_server_address*/zenworks-eup`

Replace *`ZENworks_server_address`* with the DNS name or IP address of your ZENworks Primary Server.

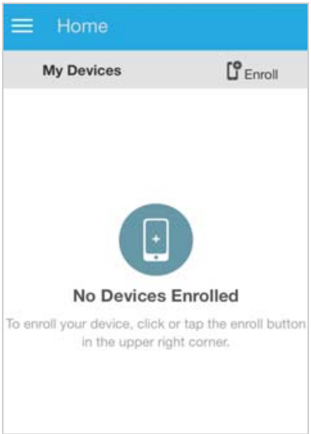
The login screen for the ZENworks User Portal is displayed.



Copyright © 2016 Micro Focus Software Inc. All rights reserved.

2 Enter the evaluation user's username and password, skip the Domain field, then tap **Sign In** to display the My Devices screen.

The Domain name field is not needed because the system is configured for simple enrollment, which allows users to log in with only their username rather than their full domain name.

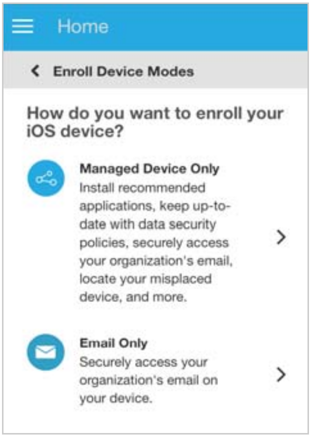


No Devices Enrolled

To enroll your device, click or tap the enroll button in the upper right corner.

3 Tap **Enroll** in the upper-right corner to display the **Enroll Device Modes** screen.

The available enrollment options are determined by the Mobile Enrollment policy. If you configured the policy as recommended in "Create a Mobile Enrollment Policy" on page 74, both options are available as shown below. Otherwise, only one of the two options is available.



Home

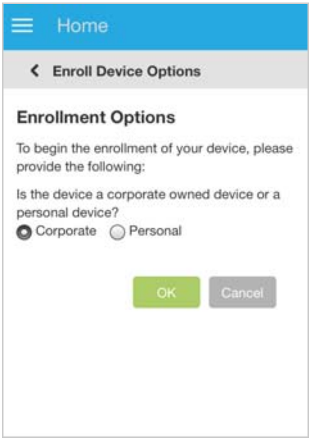
Enroll Device Modes

How do you want to enroll your iOS device?

Managed Device Only
Install recommended applications, keep up-to-date with data security policies, securely access your organization's email, locate your misplaced device, and more.

Email Only
Securely access your organization's email on your device.

4 Tap **Managed Device Only** to display the **Enroll Device Options** screen.



Home

Enroll Device Options

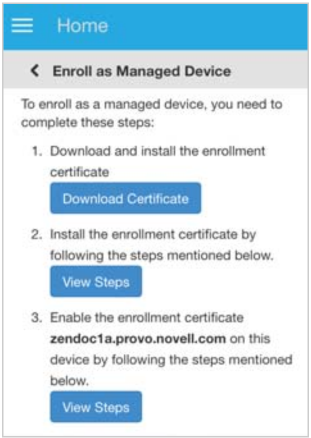
Enrollment Options

To begin the enrollment of your device, please provide the following:

Is the device a corporate owned device or a personal device?
● Corporate ○ Personal

OK Cancel

5 Click **OK** to enroll the device as a corporate device and display the **Enroll as Managed Device** screen.



Home

Enroll as Managed Device

To enroll as a managed device, you need to complete these steps:

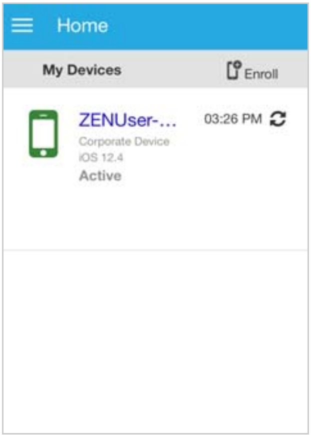
1. Download and install the enrollment certificate
   Download Certificate
2. Install the enrollment certificate by following the steps mentioned below.
   View Steps
3. Enable the enrollment certificate **zendoc1a.provo.novell.com** on this device by following the steps mentioned below.
   View Steps

6 Complete the steps to enroll the device.

Note: If you enroll multiple devices, the steps might not be the same on all devices. This is because of differences in iOS versions. ZENworks displays only the steps required to complete enrollment on the current device.

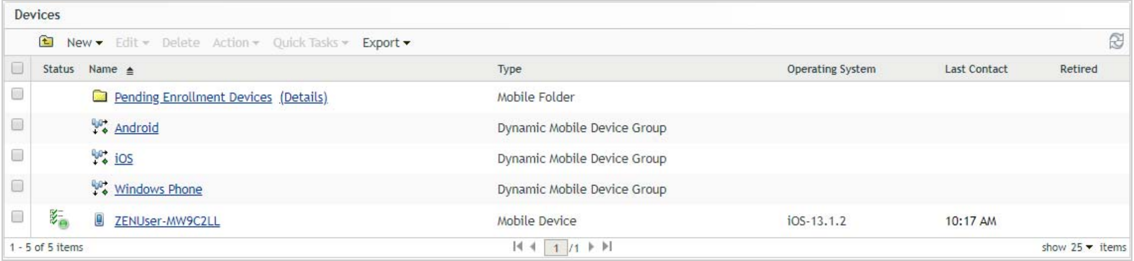
7 After you've finished enrollment, tap **Home** to return to the Home page.

The enrolled device is displayed in the My Devices list.



ZENUser-... 03:26 PM
Corporate Device
iOS 12.4
Active

8 In ZENworks Control Center, go to the **Devices** > **Mobile Devices** list to confirm that the device is enrolled in the zone.

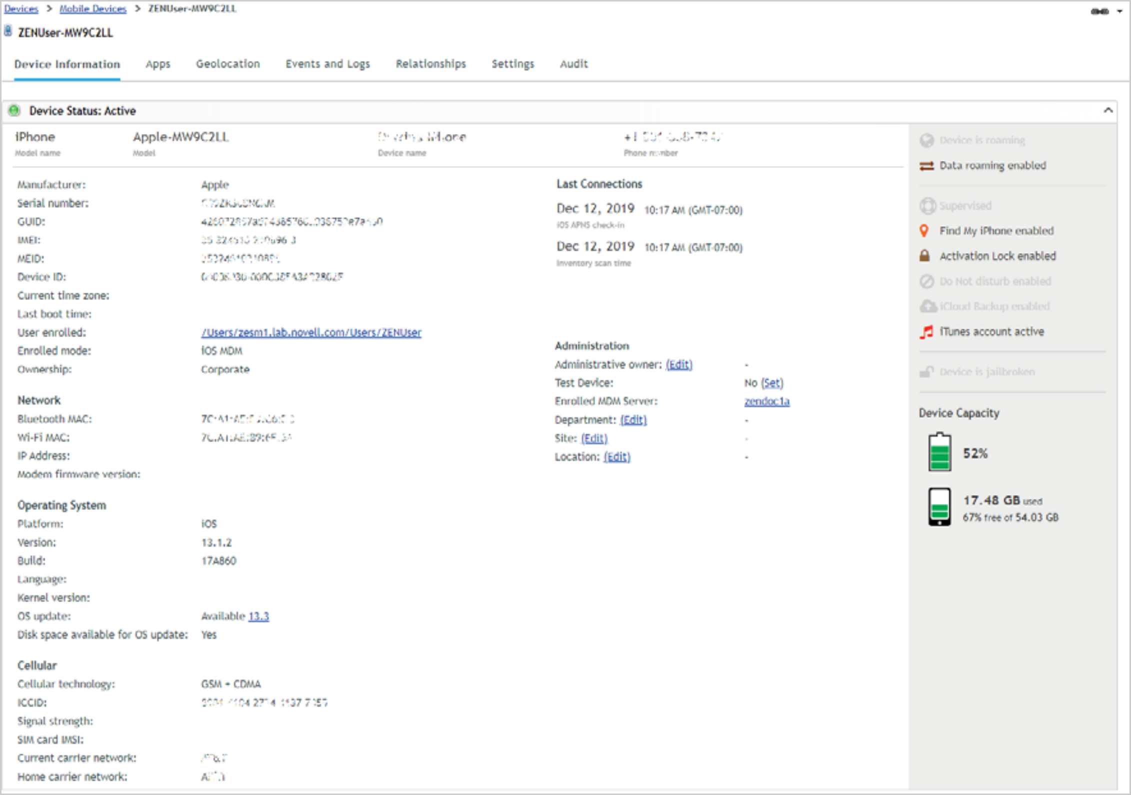


Status	Name	Type	Operating System	Last Contact	Retired
	Pending Enrollment Devices (Details)	Mobile Folder			
	Android	Dynamic Mobile Device Group			
	iOS	Dynamic Mobile Device Group			
	Windows Phone	Dynamic Mobile Device Group			
	ZENUser-MW9C2LL	Mobile Device	iOS-13.1.2	10:17 AM	

1 - 5 of 5 items 1 /1 show 25 items

9 (Optional) In the list, click the iOS device to display its Device Information page.

The Device Information page provides inventory details collected from the device.



Devices > Mobile Devices > ZENUser-MW9C2LL

ZENUser-MW9C2LL

Device Status: Active

iPhone	Apple-MW9C2LL	[redacted]	[redacted]
Model name	Model	Device name	Phone number

Manufacturer:	Apple
Serial number:	[redacted]
GUID:	[redacted]
IMEI:	[redacted]
MEID:	[redacted]
Device ID:	[redacted]
Current time zone:	
Last boot time:	
User enrolled:	/Users/zesm1.lab.novell.com/Users/ZENUser
Enrolled mode:	iOS MDM
Ownership:	Corporate

Network

Bluetooth MAC:	[redacted]
Wi-Fi MAC:	[redacted]
IP Address:	
Modem firmware version:	

Operating System

Platform:	iOS
Version:	13.1.2
Build:	17A860
Language:	
Kernel version:	
OS update:	Available 13.3
Disk space available for OS update:	Yes

Cellular

Cellular technology:	GSM + CDMA
ICCID:	[redacted]
Signal strength:	
SIM card IMSI:	
Current carrier network:	[redacted]
Home carrier network:	[redacted]

Last Connections

Dec 12, 2019 10:17 AM (GMT-07:00)
iOS APNS check-in

Dec 12, 2019 10:17 AM (GMT-07:00)
Inventory scan time

Administration

Administrative owner: (Edit)	-
Test Device:	No (Set)
Enrolled MDM Server:	zendoc1a
Department: (Edit)	-
Site: (Edit)	-
Location: (Edit)	-

Device is roaming
Data roaming enabled

Supervised
Find My iPhone enabled
Activation Lock enabled
Do Not disturb enabled
iCloud Backup enabled
iTunes account active

Device is jailbroken

Device Capacity

52%

17.48 GB used
67% free of 54.03 GB

5.1.3 Enroll an Apple DEP iOS Device

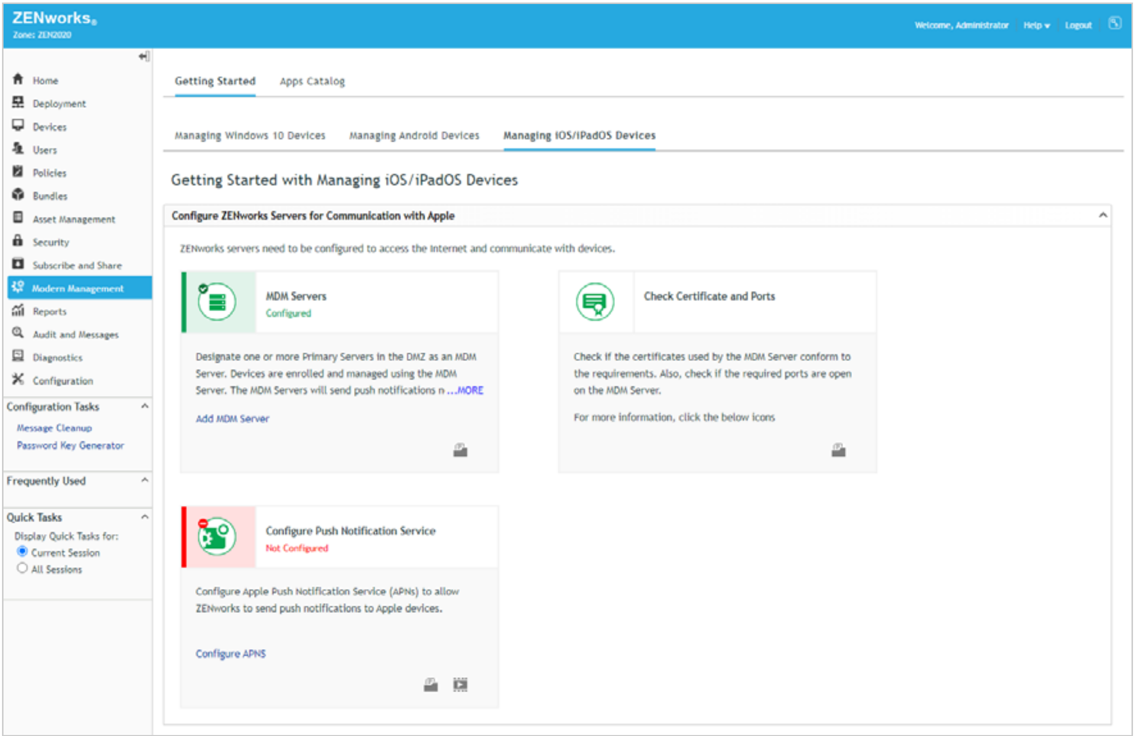
If you use the Apple Device Enrollment Program (DEP), you can use ZENworks to simplify the initial setup and enrollment of your DEP devices. This applies to devices purchased through the program. It also applies to devices (iOS version 11 or newer) that you add to the program via Apple Configurator.

Using ZENworks Control Center, you configure setup options such as whether or not a device is supervised and what features (Location Services, Passcode, and so forth) are required to be configured at initial setup. Then, during the initial setup of a device, the device is configured according to your setup options and enrolled in the ZENworks Management Zone for continued management.

Linking Your MDM Server to the Apple Device Enrollment Program

You need to link your MDM Server to the Apple Device Enrollment Program. This allows you to assign DEP devices to the MDM Server so that it can manage the devices' initial setup and enrollment.

1 In ZENworks Control Center, go to Getting Started with Managing iOS/iPadOS Devices.



Getting Started with Managing iOS/iPadOS Devices

Configure ZENworks Servers for Communication with Apple

ZENworks servers need to be configured to access the internet and communicate with devices.

MDM Servers
Configured

Designate one or more Primary Servers in the DMZ as an MDM Server. Devices are enrolled and managed using the MDM Server. The MDM Servers will send push notifications n ...MORE

Add MDM Server

Check Certificate and Ports

Check if the certificates used by the MDM Server conform to the requirements. Also, check if the required ports are open on the MDM Server.

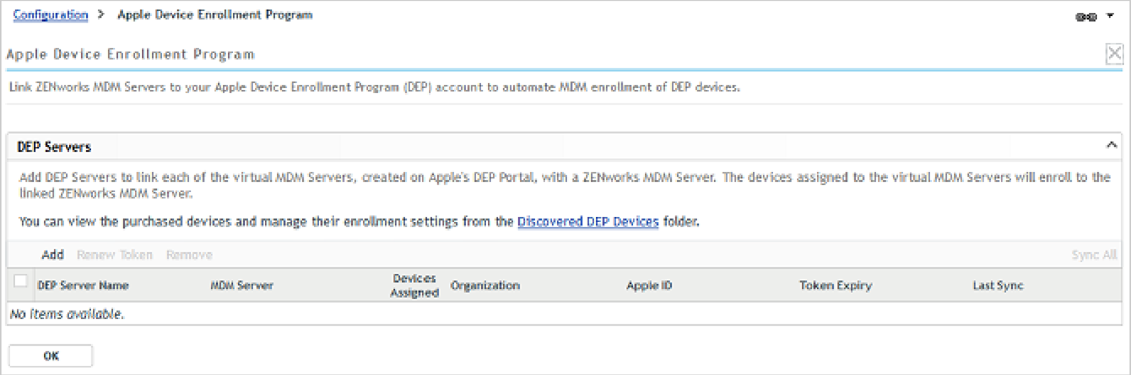
For more information, click the below icons

Configure Push Notification Service
Not Configured

Configure Apple Push Notification Service (APNs) to allow ZENworks to send push notifications to Apple devices.

Configure APNS

2 In the Setup Apple Business or School Manager section, click **Add DEP Server** to display the following page.



Apple Device Enrollment Program

Link ZENworks MDM Servers to your Apple Device Enrollment Program (DEP) account to automate MDM enrollment of DEP devices.

DEP Servers

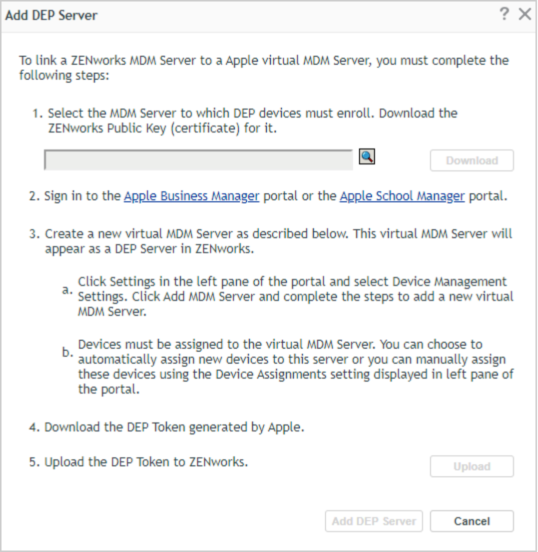
Add DEP Servers to link each of the virtual MDM Servers, created on Apple's DEP Portal, with a ZENworks MDM Server. The devices assigned to the virtual MDM Servers will enroll to the linked ZENworks MDM Server.

You can view the purchased devices and manage their enrollment settings from the Discovered DEP Devices folder.

□	DEP Server Name	MDM Server	Devices Assigned	Organization	Apple ID	Token Expiry	Last Sync
No items available.							

You can link one or more MDM Servers to your Apple Device Enrollment Program. The MDM Servers that you link are referred to as ZENworks DEP Servers and end up being displayed in the DEP Servers list shown in the screenshot.

3 In the DEP Servers list, click **Add** to display the Add DEP Server dialog box.



Add DEP Server

To link a ZENworks MDM Server to a Apple virtual MDM Server, you must complete the following steps:

1. Select the MDM Server to which DEP devices must enroll. Download the ZENworks Public Key (certificate) for it.

2. Sign in to the Apple Business Manager portal or the Apple School Manager portal.

3. Create a new virtual MDM Server as described below. This virtual MDM Server will appear as a DEP Server in ZENworks.

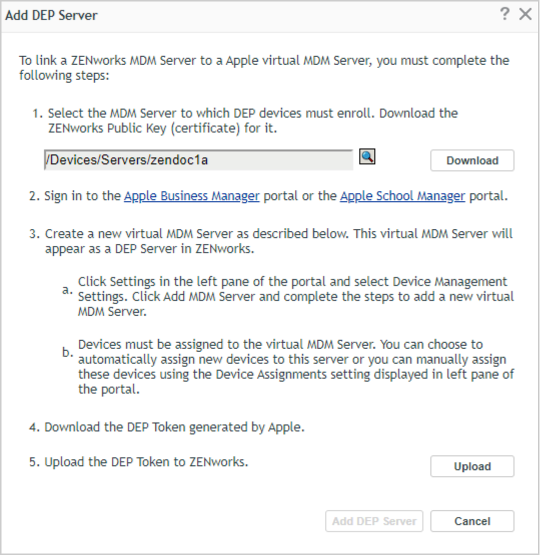
   a. Click Settings in the left pane of the portal and select Device Management Settings. Click Add MDM Server and complete the steps to add a new virtual MDM Server.

   b. Devices must be assigned to the virtual MDM Server. You can choose to automatically assign new devices to this server or you can manually assign these devices using the Device Assignments setting displayed in left pane of the portal.

4. Download the DEP Token generated by Apple.

5. Upload the DEP Token to ZENworks.

4 To select the MDM Server you want to designate as the DEP Server, click 🔍, then browse for and select the server.



Add DEP Server

To link a ZENworks MDM Server to a Apple virtual MDM Server, you must complete the following steps:

1. Select the MDM Server to which DEP devices must enroll. Download the ZENworks Public Key (certificate) for it.

   /Devices/Servers/zendoc1a

2. Sign in to the Apple Business Manager portal or the Apple School Manager portal.

3. Create a new virtual MDM Server as described below. This virtual MDM Server will appear as a DEP Server in ZENworks.

   a. Click Settings in the left pane of the portal and select Device Management Settings. Click Add MDM Server and complete the steps to add a new virtual MDM Server.

   b. Devices must be assigned to the virtual MDM Server. You can choose to automatically assign new devices to this server or you can manually assign these devices using the Device Assignments setting displayed in left pane of the portal.

4. Download the DEP Token generated by Apple.

5. Upload the DEP Token to ZENworks.

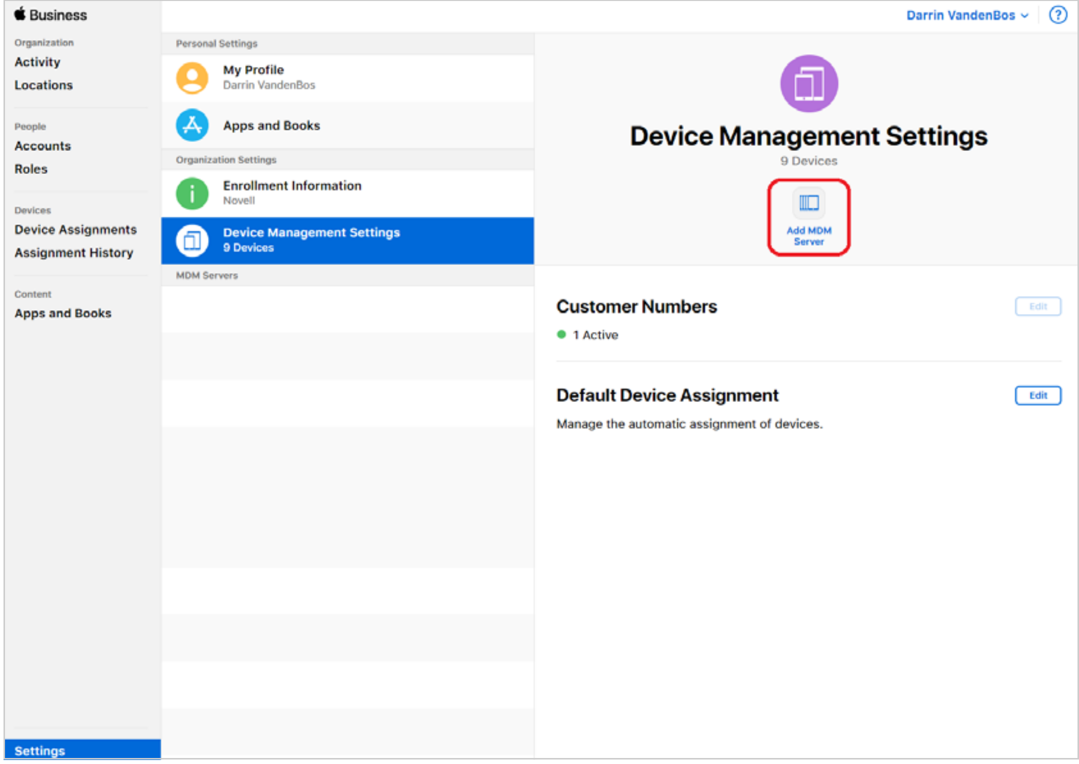
5 Click **Download**, then save the server's public key to your local drive.

The key file is saved as `*servername*.der`. You'll need the file later when you add the MDM Server to your Apple Device Enrollment Program.

6 Click the **Apple Business Manager** link or **Apple School Manager** link, sign in to your Apple account.

7 Add your MDM Server:

7a Click **Settings**, then click **Device Management Settings**.



Device Management Settings

9 Devices

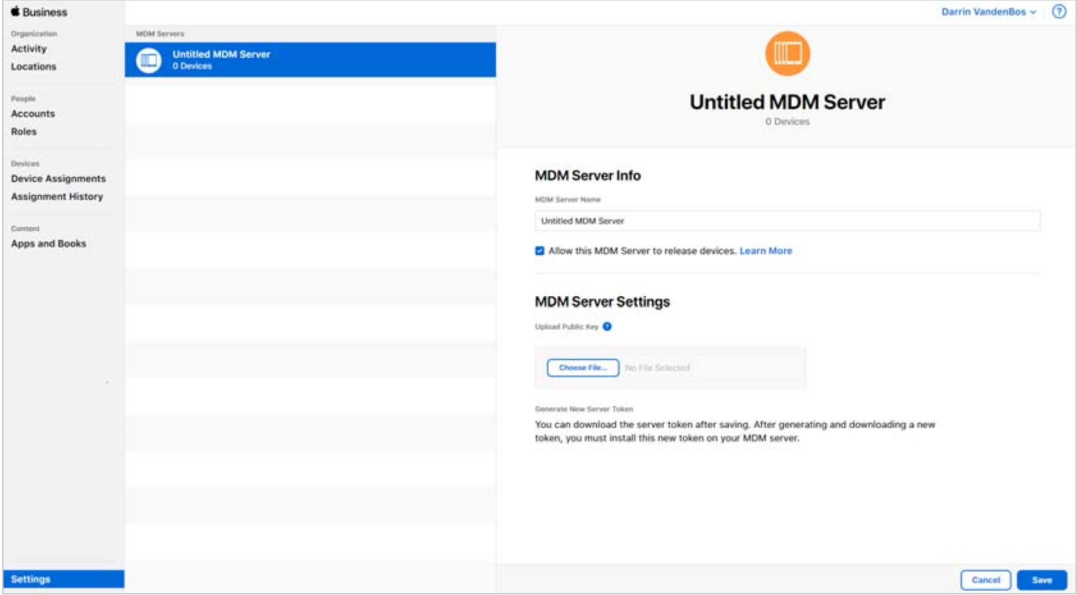
Customer Numbers

1 Active

Default Device Assignment

Manage the automatic assignment of devices.

7b Click Add MDM Server to display the following settings.



Untitled MDM Server

0 Devices

MDM Server Info

MDM Server Name: Untitled MDM Server

☑ Allow this MDM Server to release devices. Learn More

MDM Server Settings

Upload Public Key

No File Selected

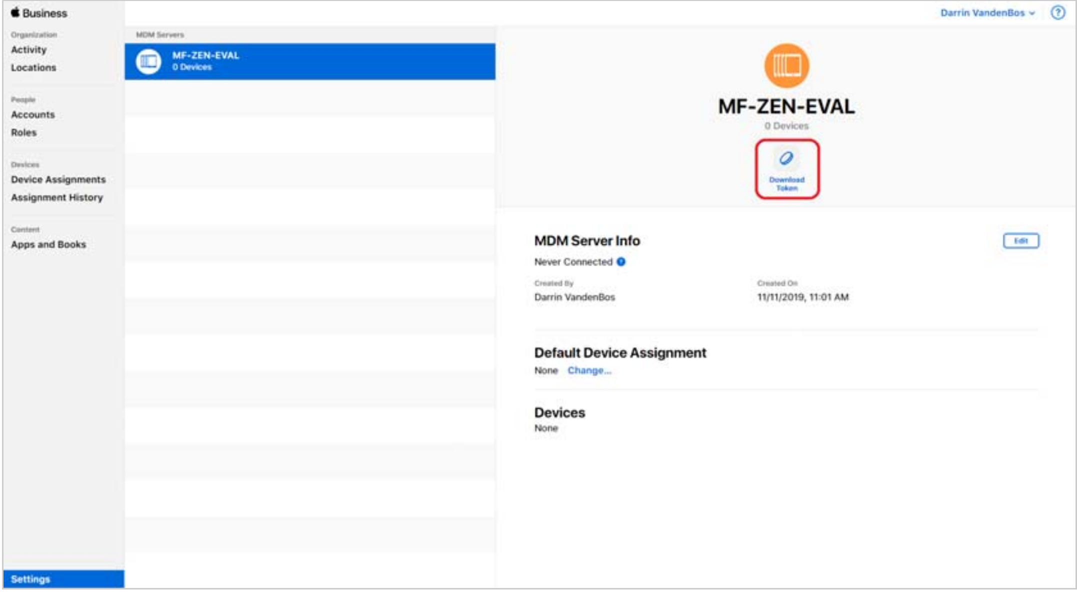
Generate New Server Token

You can download the server token after saving. After generating and downloading a new token, you must install this new token on your MDM server.

7c Enter a name for the MDM Server.

7d Click Choose File to upload the key (`*servername*.der`) you generated in ZENworks Control Center.

7e Click Save to add the MDM server.



MF-ZEN-EVAL
0 Devices

MF-ZEN-EVAL
0 Devices

MDM Server Info
Never Connected

Created By
Darrin VandenBos

Created On
11/11/2019, 11:01 AM

Default Device Assignment
None Change...

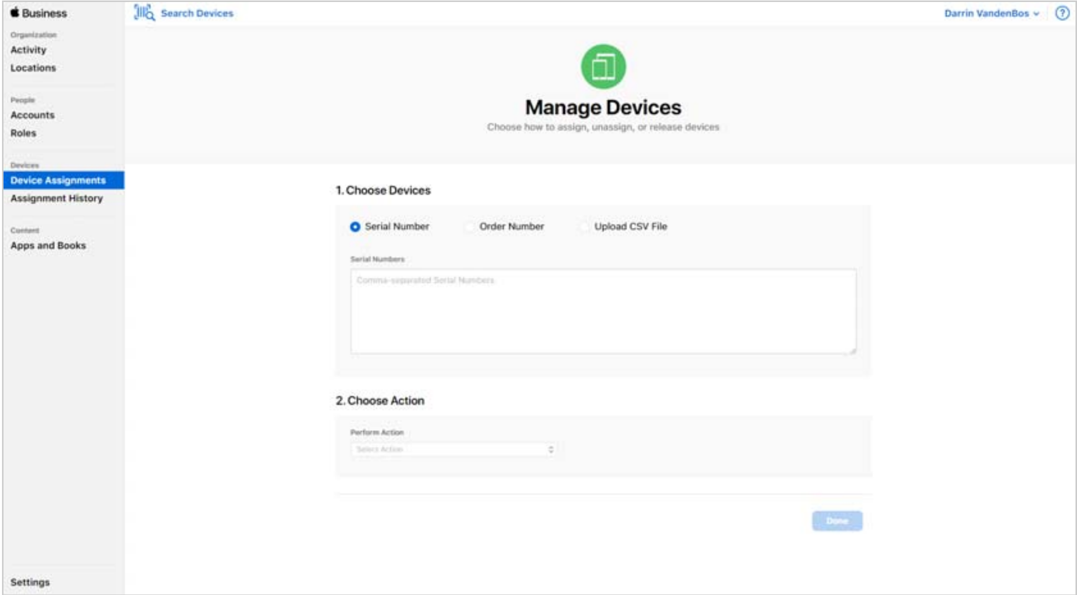
Devices
None

7f Click **Download Token** to download the MDM Server token to your local drive.

The MDM Server token file is saved with a name similar to the following:

```
MF-ZEN-EVAL_Token_2019-10-17T18-23-24Z_smime.p7m
```

7g For this evaluation, you need to have at least one unactivated device assigned to the MDM Server. Click **Device Assignments**, then assign the desired devices to the server.



Manage Devices
Choose how to assign, unassign, or release devices

1. Choose Devices

● Serial Number ○ Order Number ○ Upload CSV File

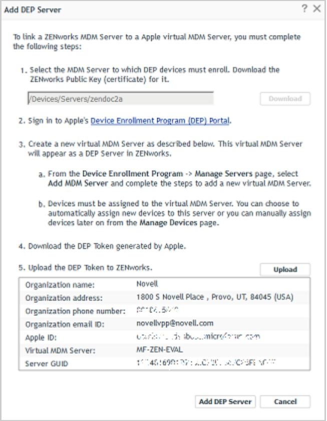
Serial Numbers
Comma-separated Serial Numbers

2. Choose Action

Perform Action
Select Action

8 In ZENworks Control Center, you should still be in the Add DEP Server dialog box. Click **Upload** to upload the MDM Server token (the `.p7m` file generated from the Apple portal).

After the token is uploaded, the organization information is displayed.



Add DEP Server

To link a ZENworks MDM Server to a Apple virtual MDM Server, you must complete the following steps:

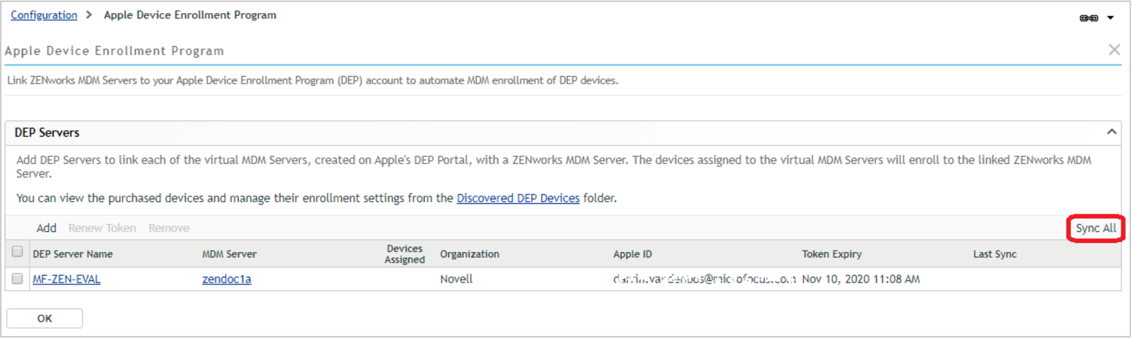
1. Select the MDM Server to which DEP devices must enroll. Download the ZENworks Public Key (certificate) for it.

   /Devices/Servers/zendoc2a

2. Sign in to Apple's Device Enrollment Program (DEP) Portal.
3. Create a new virtual MDM Server as described below. This virtual MDM Server will appear as a DEP Server in ZENworks.
   a. From the **Device Enrollment Program** -> **Manage Servers** page, select **Add MDM Server** and complete the steps to add a new virtual MDM Server.
   b. Devices must be assigned to the virtual MDM Server. You can choose to automatically assign new devices to this server or you can manually assign devices later on from the **Manage Devices** page.
4. Download the DEP Token generated by Apple.
5. Upload the DEP Token to ZENworks.

Organization name:	Novell
Organization address:	1800 S Novell Place , Provo, UT, 84045 (USA)
Organization phone number:	[illegible]
Organization email ID:	novellvpp@novell.com
Apple ID:	[illegible]
Virtual MDM Server:	MF-ZEN-EVAL
Server GUID	[illegible]

9 Click **Add DEP Server** to add it to the list.



Configuration > Apple Device Enrollment Program

Apple Device Enrollment Program

Link ZENworks MDM Servers to your Apple Device Enrollment Program (DEP) account to automate MDM enrollment of DEP devices.

DEP Servers

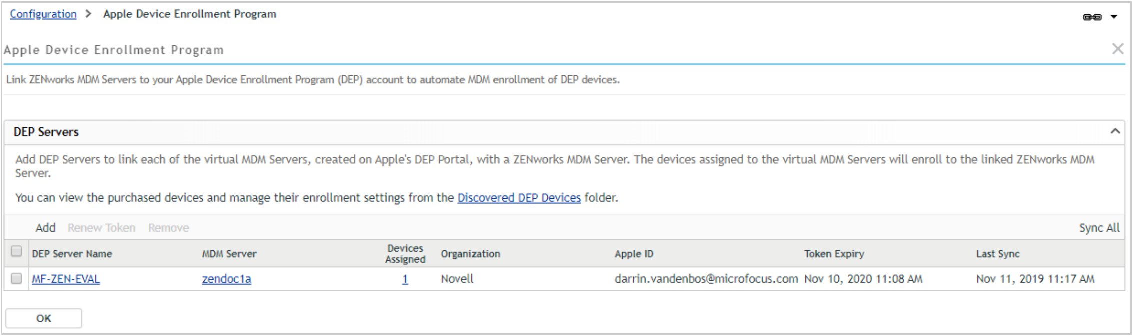
Add DEP Servers to link each of the virtual MDM Servers, created on Apple's DEP Portal, with a ZENworks MDM Server. The devices assigned to the virtual MDM Servers will enroll to the linked ZENworks MDM Server.

You can view the purchased devices and manage their enrollment settings from the Discovered DEP Devices folder.

☐	DEP Server Name	MDM Server	Devices Assigned	Organization	Apple ID	Token Expiry	Last Sync
☐	MF-ZEN-EVAL	zendoc1a		Novell	[illegible]	Nov 10, 2020 11:08 AM	

10 In the DEP Servers list, click **Sync All** (located on the right side of the list's menu) to sync the DEP devices into your ZENworks Management Zone.

Once the sync is complete, the number of DEP devices assigned to the server is displayed in the Devices Assigned column of the list.



Configuration > Apple Device Enrollment Program

Apple Device Enrollment Program

Link ZENworks MDM Servers to your Apple Device Enrollment Program (DEP) account to automate MDM enrollment of DEP devices.

DEP Servers

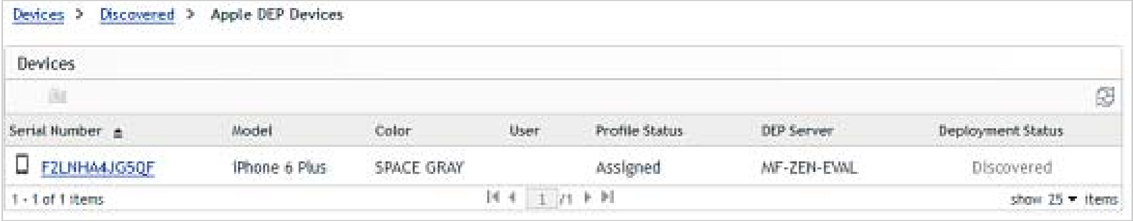
Add DEP Servers to link each of the virtual MDM Servers, created on Apple's DEP Portal, with a ZENworks MDM Server. The devices assigned to the virtual MDM Servers will enroll to the linked ZENworks MDM Server.

You can view the purchased devices and manage their enrollment settings from the Discovered DEP Devices folder.

☐	DEP Server Name	MDM Server	Devices Assigned	Organization	Apple ID	Token Expiry	Last Sync
☐	MF-ZEN-EVAL	zendoc1a	1	Novell	darrin.vandenbos@microfocus.com	Nov 10, 2020 11:08 AM	Nov 11, 2019 11:17 AM

11 Click the number in the Devices Assigned column to display the devices.

The DEP devices are added under Discovered devices in your ZENworks zone with a **Deployment Status** of *Discovered*.



Devices > Discovered > Apple DEP Devices

Devices

Serial Number	Model	Color	User	Profile Status	DEP Server	Deployment Status
F2LNHA4JG5QF	iPhone 6 Plus	SPACE GRAY		Assigned	MF-ZEN-EVAL	Discovered

1 - 1 of 1 items　　1 /1　　show 25 items

After a device is activated and enrolled, the deployment status will change to *Managed* and the device will be added to the Managed devices list.

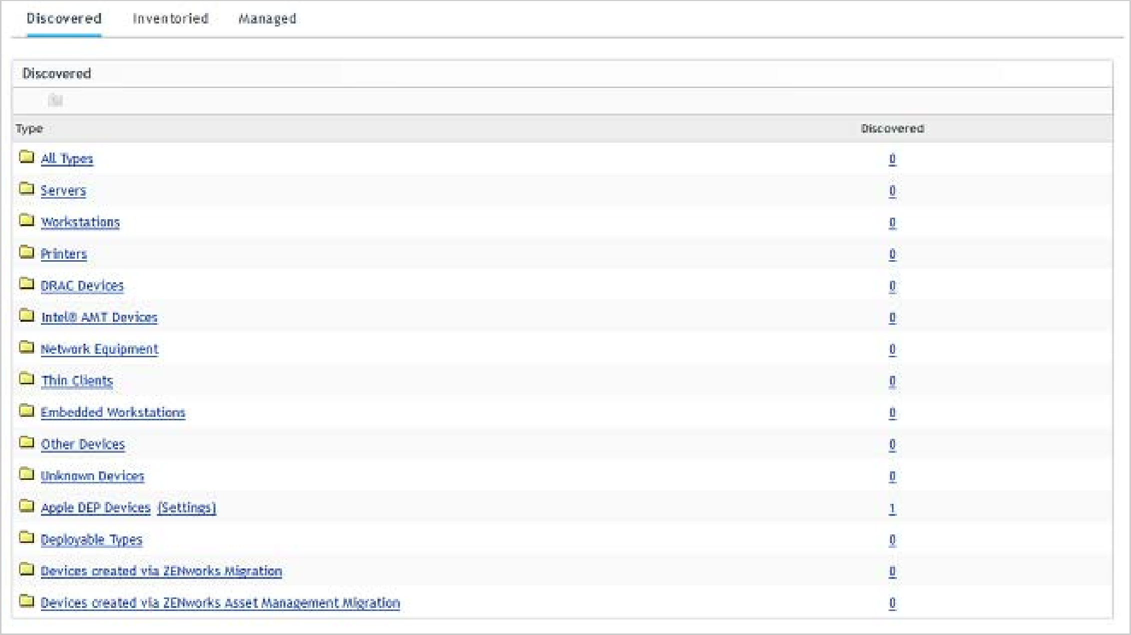
Configuring Apple Setup Options

During initial setup of a DEP device, the device is configured as a supervised device that is allowed to pair with host computers. These are the default settings, but you can change these and several other settings, and you can also select any iOS feature configurations (Location Services, Siri, and so forth) to skip during setup.

1 If the Apple DEP Devices list is still displayed, click **Discovered** (in the bread crumbs at the top) to display the Discovered devices list.

or

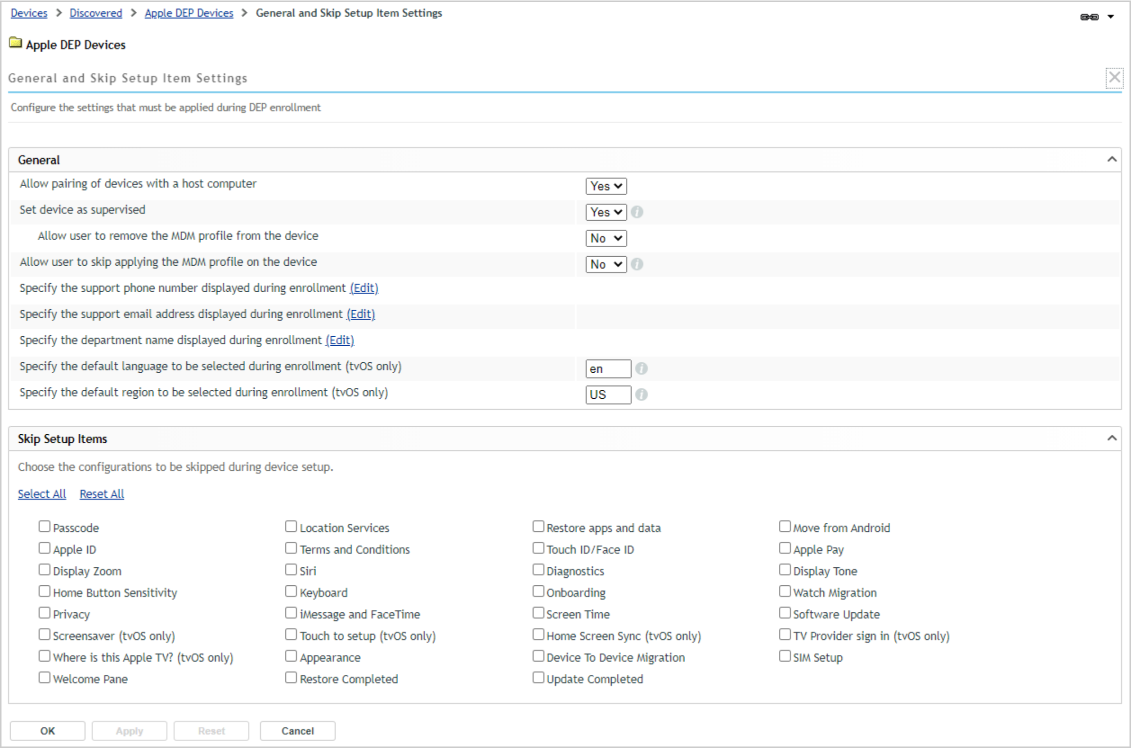
If you are not on that list, click **Devices** (in the left navigation pane), then click the **Discovered** tab to display the Discovered devices list.



Discovered

Type	Discovered
All Types	0
Servers	0
Workstations	0
Printers	0
DRAC Devices	0
Intel® AMT Devices	0
Network Equipment	0
Thin Clients	0
Embedded Workstations	0
Other Devices	0
Unknown Devices	0
Apple DEP Devices (Settings)	1
Deployable Types	0
Devices created via ZENworks Migration	0
Devices created via ZENworks Asset Management Migration	0

2 In the list, click the **Settings** link next to Apple DEP Devices, then click **General and Skip Setup Item Settings** to display the setup options.



Devices > Discovered > Apple DEP Devices > General and Skip Setup Item Settings

Apple DEP Devices

General and Skip Setup Item Settings

Configure the settings that must be applied during DEP enrollment

General

Allow pairing of devices with a host computer	Yes
Set device as supervised	Yes
Allow user to remove the MDM profile from the device	No
Allow user to skip applying the MDM profile on the device	No
Specify the support phone number displayed during enrollment (Edit)	
Specify the support email address displayed during enrollment (Edit)	
Specify the department name displayed during enrollment (Edit)	
Specify the default language to be selected during enrollment (tvOS only)	en
Specify the default region to be selected during enrollment (tvOS only)	US

Skip Setup Items

Choose the configurations to be skipped during device setup.

Select All Reset All

□ Passcode
□ Apple ID
□ Display Zoom
□ Home Button Sensitivity
□ Privacy
□ Screensaver (tvOS only)
□ Where is this Apple TV? (tvOS only)
□ Welcome Pane
□ Location Services
□ Terms and Conditions
□ Siri
□ Keyboard
□ iMessage and FaceTime
□ Touch to setup (tvOS only)
□ Appearance
□ Restore Completed
□ Restore apps and data
□ Touch ID/Face ID
□ Diagnostics
□ Onboarding
□ Screen Time
□ Home Screen Sync (tvOS only)
□ Device To Device Migration
□ Update Completed
□ Move from Android
□ Apple Pay
□ Display Tone
□ Watch Migration
□ Software Update
□ TV Provider sign in (tvOS only)
□ SIM Setup

3 For this evaluation, change the following settings:

3a In the General section, specify a support phone number, support email address, and department name. Also, change **Allow user to remove the MDM profile from the device** to **Yes**.

3b In the Skip Setup Items, select **Location Services**, **Terms and Conditions**, **Touch ID**, and **Siri** so that those configurations are skipped during setup. You can also select any others you'd like to skip.

3c Leave all other options set to the defaults.

4 Click **OK** to save the changes.

The setting changes must be synced to the Apple Device Enrollment Program service. After this occurs, any new devices will use the setup options. To initiate the sync immediately, you can use the Sync All option on the DEP Servers page (**Configuration** > **Management Zone Settings** > **Discovery and Deployment** > **Apple Device Enrollment Program**).

Enrolling a DEP Device

Now that your DEP Server is defined and the setup options configured, you can set up and enroll a DEP device.

1 Turn on the device and begin the setup process.

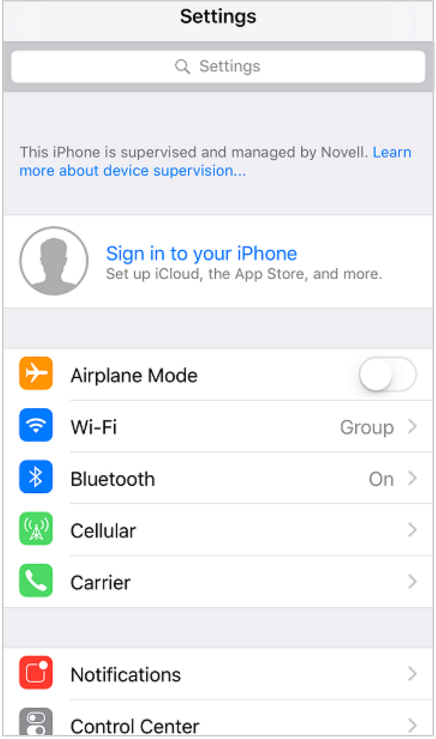
2 When prompted for a login, specify the evaluation user's username and password.

3 Complete the setup.

Based on the Apple setup options you configured in the previous section, the configuration will skip the setup for Location Services, Terms and Conditions, Touch ID, and Siri.

4 On the device, tap ⚙ to display the Settings screen.

Notice that the device is managed and supervised by your organization.



Settings

Settings

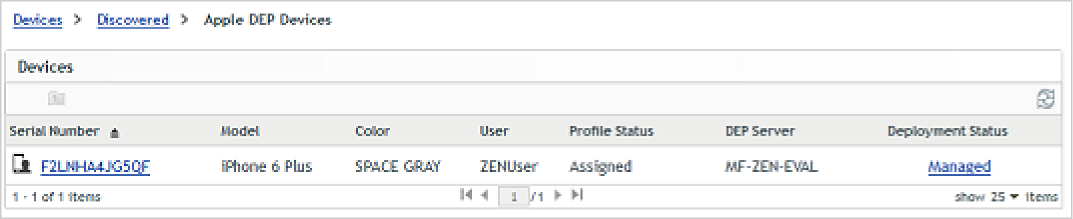
This iPhone is supervised and managed by Novell. Learn more about device supervision...

Sign in to your iPhone
Set up iCloud, the App Store, and more.

Airplane Mode	
Wi-Fi	Group
Bluetooth	On
Cellular	
Carrier	
Notifications	
Control Center	

5 In ZENworks Control Center, go to the device in the Discovered devices list (**Devices** > **Discovered** > **Apple DEP Devices**).

Notice that the device's Deployment Status is now listed as *Managed*.



Devices > Discovered > Apple DEP Devices

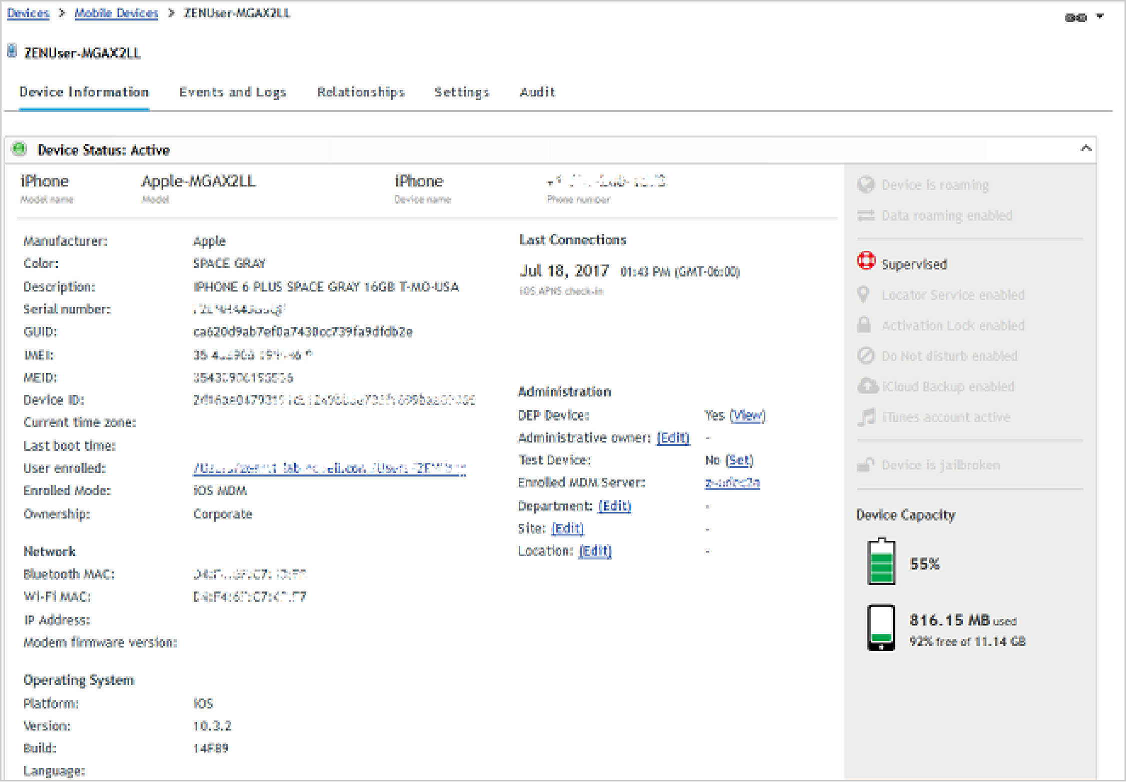
Devices

Serial Number	Model	Color	User	Profile Status	DEP Server	Deployment Status
F2LNHA4JG5QF	iPhone 6 Plus	SPACE GRAY	ZENUser	Assigned	MF-ZEN-EVAL	Managed

1 - 1 of 1 items   1 /1   show 25 items

6 (Optional) Click the **Managed** link to display the device's Information page.

The Device Information page provides inventory details collected from the device.



Devices > Mobile Devices > ZENUser-MGAX2LL

ZENUser-MGAX2LL

Device Information | Events and Logs | Relationships | Settings | Audit

Device Status: Active

iPhone	Apple-MGAX2LL	iPhone	[redacted]
Model name	Model	Device name	Phone number

Manufacturer: Apple
Color: SPACE GRAY
Description: IPHONE 6 PLUS SPACE GRAY 16GB T-MO-USA
Serial number: [redacted]
GUID: ca620d9ab7ef0a7430cc739fa9dfdb2e
IMEI: [redacted]
MEID: [redacted]
Device ID: [redacted]
Current time zone:
Last boot time:
User enrolled: [redacted]
Enrolled Mode: iOS MDM
Ownership: Corporate

Network
Bluetooth MAC: [redacted]
Wi-Fi MAC: [redacted]
IP Address:
Modem firmware version:

Operating System
Platform: iOS
Version: 10.3.2
Build: 14F89
Language:

Last Connections
Jul 18, 2017 01:43 PM (GMT-06:00)
iOS APNS check-in

Administration
DEP Device: Yes (View)
Administrative owner: (Edit) -
Test Device: No (Set)
Enrolled MDM Server: [redacted]
Department: (Edit) -
Site: (Edit) -
Location: (Edit) -

Device Capacity
55%
816.15 MB used
92% free of 11.14 GB

5.1.4 Enroll an Android Device

ZENworks manages Android devices using Android Enterprise. This requires your organization to register with the Android Enterprise program. Once you are registered and have created an Android Enterprise Enrollment policy in ZENworks, you can enroll devices in either of the two supported Android Enterprise modes: Work Profile mode and Work-Managed mode.

- "Register Your Organization in the Android Enterprise Program" on page 89
- "Create an Android Enterprise Enrollment Policy" on page 90
- "Enroll an Android Device in Work Profile Mode" on page 92
- "Enroll an Android Device in Work-Managed Mode" on page 95

Register Your Organization in the Android Enterprise Program

As a Google-approved Enterprise Mobility Manager (EMM), ZENworks facilitates the enrollment of your organization in the Android Enterprise program and the creation of the managed Google Play Store from which apps can be distributed to ZENworks-managed devices.

1 In ZENworks Control Center, click S**ubscribe and Share** (in the left-navigation pane).

2 In the Subscriptions list, click **New** > **Subscription** to launch the Create New Subscription wizard.

3 Select **Android Enterprise Subscription**, then click **Next**.

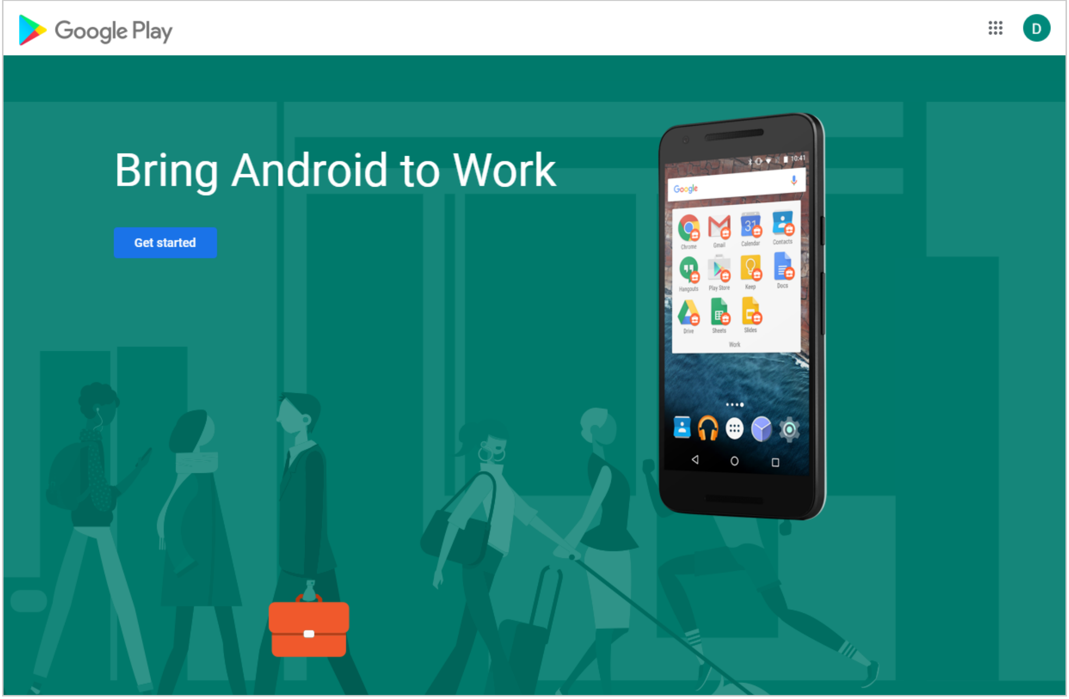
4 Enter a subscription name (for example, Android Enterprise), then click **Next**.

5 On the Configure Android Enterprise page:

5a For the Micro Focus (Novell) Customer Center credentials, use **ZENeval** as the username and **zeneval!** as the password.

5b Click Enroll to display the Google Play Bring Android to Work page.

5c If necessary, sign in with your Google account so that the Get started option is displayed.



5d Click Get started, then follow the prompts to register your organization.

5e After the account registration is complete, you are returned to ZENworks Control Center. Click Next.

6 On the Select User Context page, add the context in which your evaluation user resides, then click Next. If desired, you can also add other contexts that contain Android device users.

7 On the Select Languages page, select the language for displaying Google app details in ZENworks Control Center, then click Next.

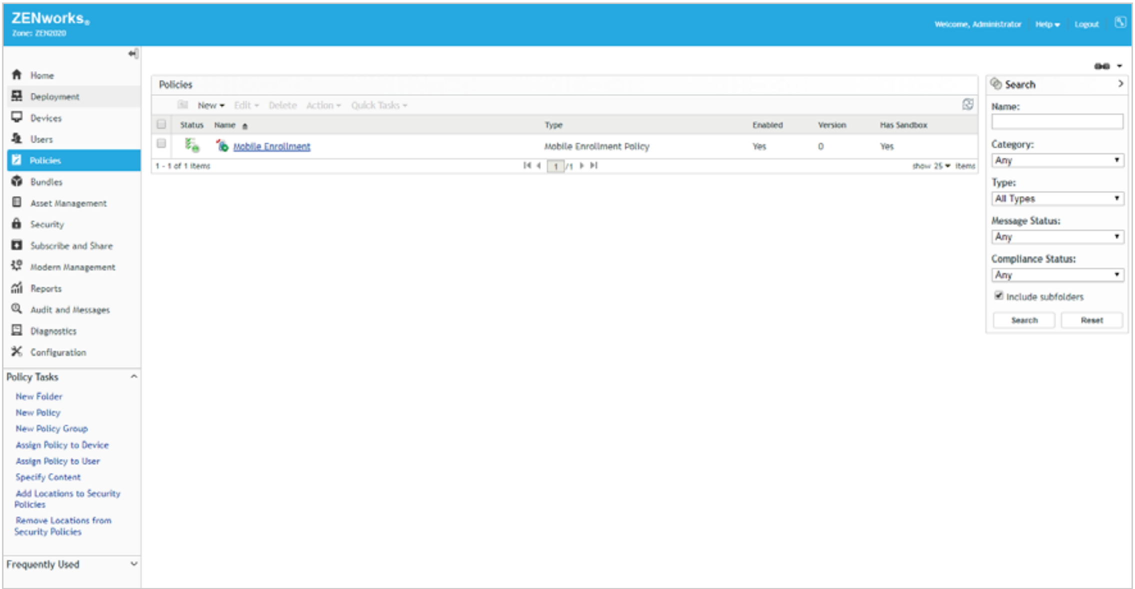
8 On the Select Bundles Folder page, keep the default settings, then click Next.

Right now, the Android Enterprise account you created doesn’t have any apps assigned to your account. We’ll come back and do that right before you distribute apps to an Android device.

Create an Android Enterprise Enrollment Policy

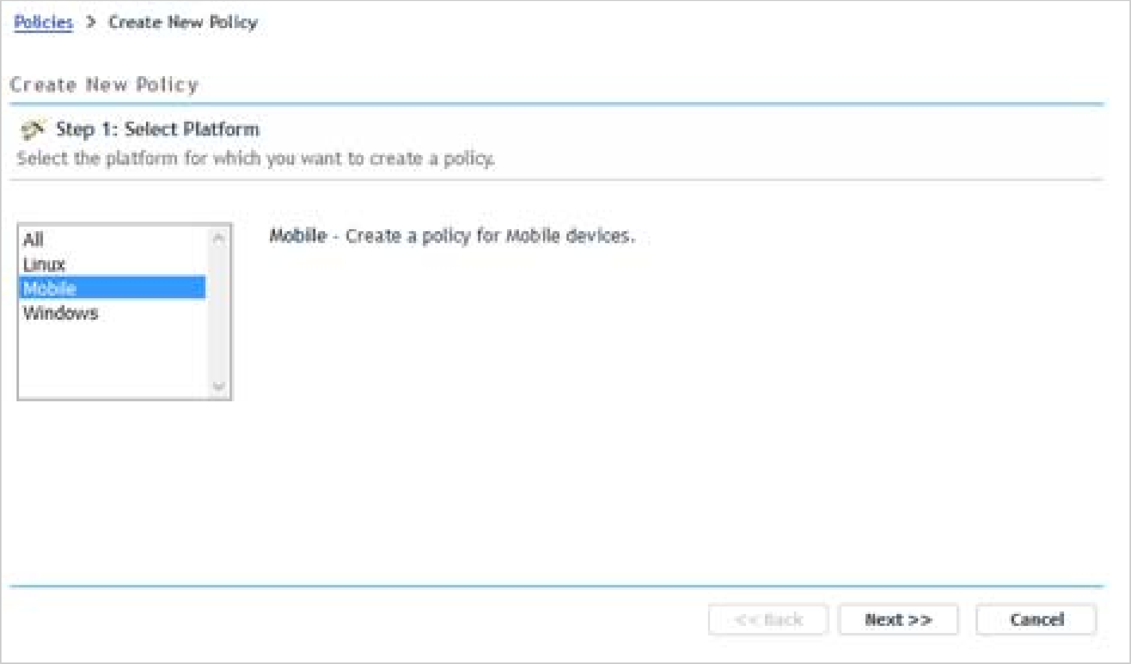
In addition to the Mobile Device Enrollment policy that you previously created, you must create an Android Enterprise Enrollment policy and assign it to Android device users.

1 In ZENworks Control Center, click Policies (in the left navigation pane).



Status	Name	Type	Enabled	Version	Has Sandbox
	Mobile Enrollment	Mobile Enrollment Policy	Yes	0	Yes

2 In the Policies panel, click **New** > **Policy** to display the Create New Policy wizard.



Policies > Create New Policy

Create New Policy

Step 1: Select Platform

Select the platform for which you want to create a policy.

Mobile - Create a policy for Mobile devices.

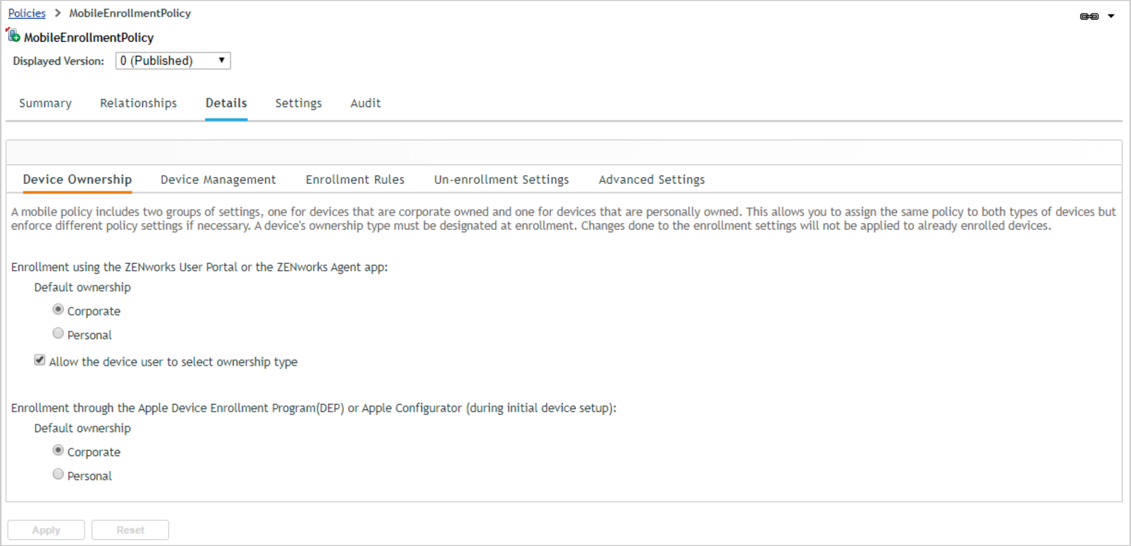
3 On the Select Platform page, select **Mobile**, then click **Next**.

4 On the Select Policy Category page, select **Android**, then click **Next**.

5 On the Select Policy Type page, select **Android Enterprise Enrollment Policy**, then click **Next**.

6 On the Define Details page, specify a name for the policy (for example, *Android Enterprise Enrollment*), then click **Next**.

7 On the Summary page, deselect **Create as Sandbox**, select **Define Additional Properties**, then click **Finish** to create the policy.



A mobile policy includes two groups of settings, one for devices that are corporate owned and one for devices that are personally owned. This allows you to assign the same policy to both types of devices but enforce different policy settings if necessary. A device's ownership type must be designated at enrollment. Changes done to the enrollment settings will not be applied to already enrolled devices.

Enrollment using the ZENworks User Portal or the ZENworks Agent app:

Default ownership

● Corporate

○ Personal

☑ Allow the device user to select ownership type

Enrollment through the Apple Device Enrollment Program(DEP) or Apple Configurator (during initial device setup):

Default ownership

● Corporate

○ Personal

8 Assign the policy to your evaluation user:

8a Click **Relationships**.

8b In the User Assignments list, click **Add**.

8c Select the evaluation user, then click **OK** to add the user to the assignment list.

8d Click **Next** > **Finish** to complete the assignment.

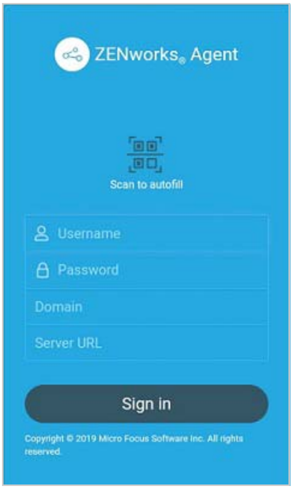
Enroll an Android Device in Work Profile Mode

Work Profile mode creates a dedicated container on the Android device for corporate apps and data. It provides support for personal devices (BYOD), enabling you to manage and secure corporate assets without touching personal data on the device.

You can enroll any device running Android version 5 and newer. We used a Samsung Galaxy Tab A running Android version 9. Again, the screens and steps might vary slightly on other Android devices and versions.

1 Install the ZENworks Agent from the Google Play Store.

2 Open the ZENworks Agent app, then follow the prompts to give the ZENworks Agent rights to the device and display the login screen.

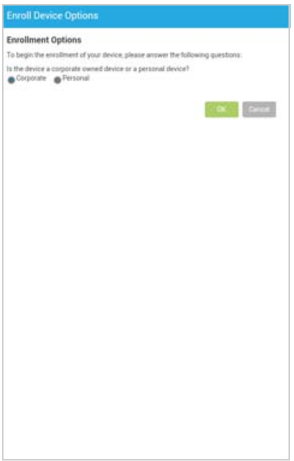


3 To log in and begin enrolling the device, fill in the evaluation user's username and password, fill in the URL of the ZENworks Primary Server, then tap **Sign In**.

The Domain name field is not needed because the system is configured for simple enrollment, which allows users to log in with only their username rather than their full domain name.

Notice the **Scan to autofill** option. This lets a user fill in the information by scanning a code included in an invitation email that you send. We didn't do the configuration required to use this, so ignore this option for now.

Because the Mobile Enrollment policy was configured to allow users to choose whether the device is a corporate or personal device, the Enrollment Options screen is displayed.



Enroll Device Options

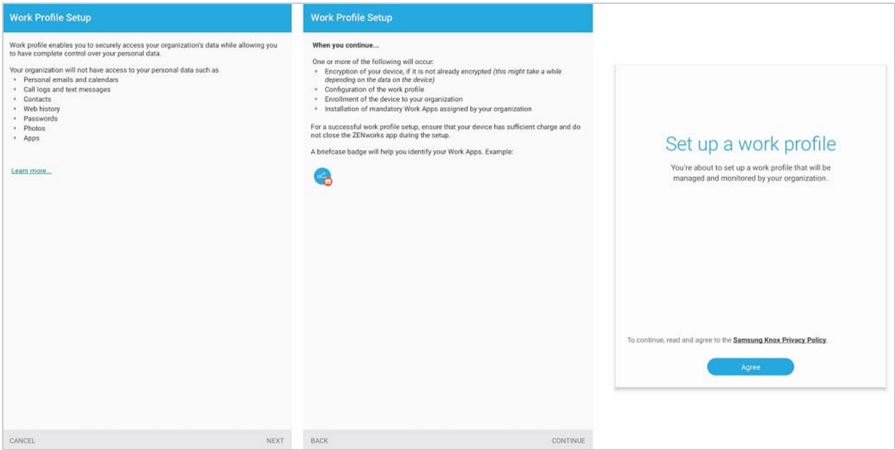
Enrollment Options

To begin the enrollment of your device, please answer the following questions:

Is the device a corporate owned device or a personal device?

● Corporate ● Personal

4 Select **Personal**, tap **OK**, then follow the prompts shown in the following screens to create the work profile and enroll the device.



Work Profile Setup

Work profile enables you to securely access your organization's data while allowing you to have complete control over your personal data.

Your organization will not have access to your personal data such as

- Personal emails and calendars
- Call logs and text messages
- Contacts
- Web history
- Passwords
- Photos
- Apps

Learn more...

Work Profile Setup

When you continue...

One or more of the following will occur:

- Encryption of your device, if it is not already encrypted *(this might take a while depending on the data on the device)*
- Configuration of the work profile
- Enrollment of the device to your organization
- Installation of mandatory Work Apps assigned by your organization

For a successful work profile setup, ensure that your device has sufficient charge and do not close the ZENworks app during the setup.

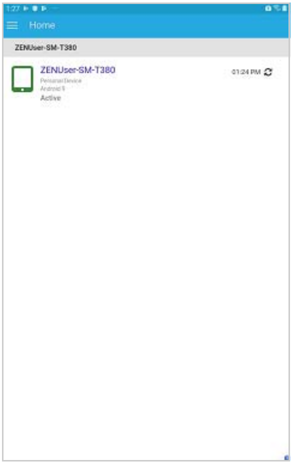
A briefcase badge will help you identify your Work Apps. Example:

Set up a work profile

You're about to set up a work profile that will be managed and monitored by your organization.

To continue, read and agree to the Samsung Knox Privacy Policy.

When enrollment is complete, the Android device is listed on the ZENworks Agent Home page.



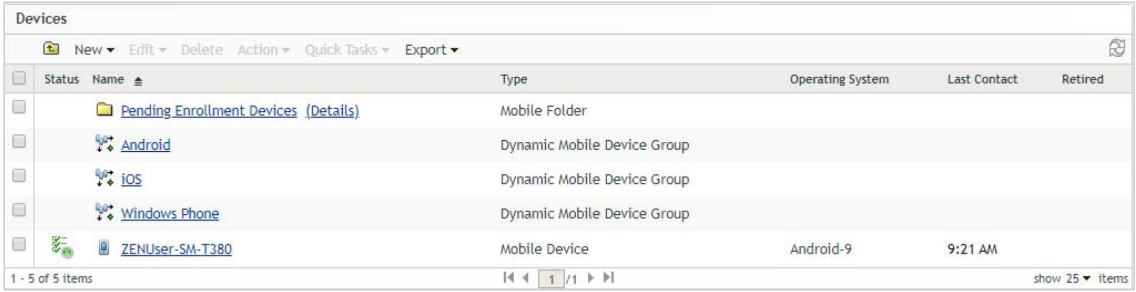
Home

ZENUser-SM-T380

ZENUser-SM-T380
Personal Device
Android 9
Active

01:24 PM

5 In ZENworks Control Center, go to the **Devices** > **Mobile Devices** list to confirm that the device is enrolled in the zone.



Devices

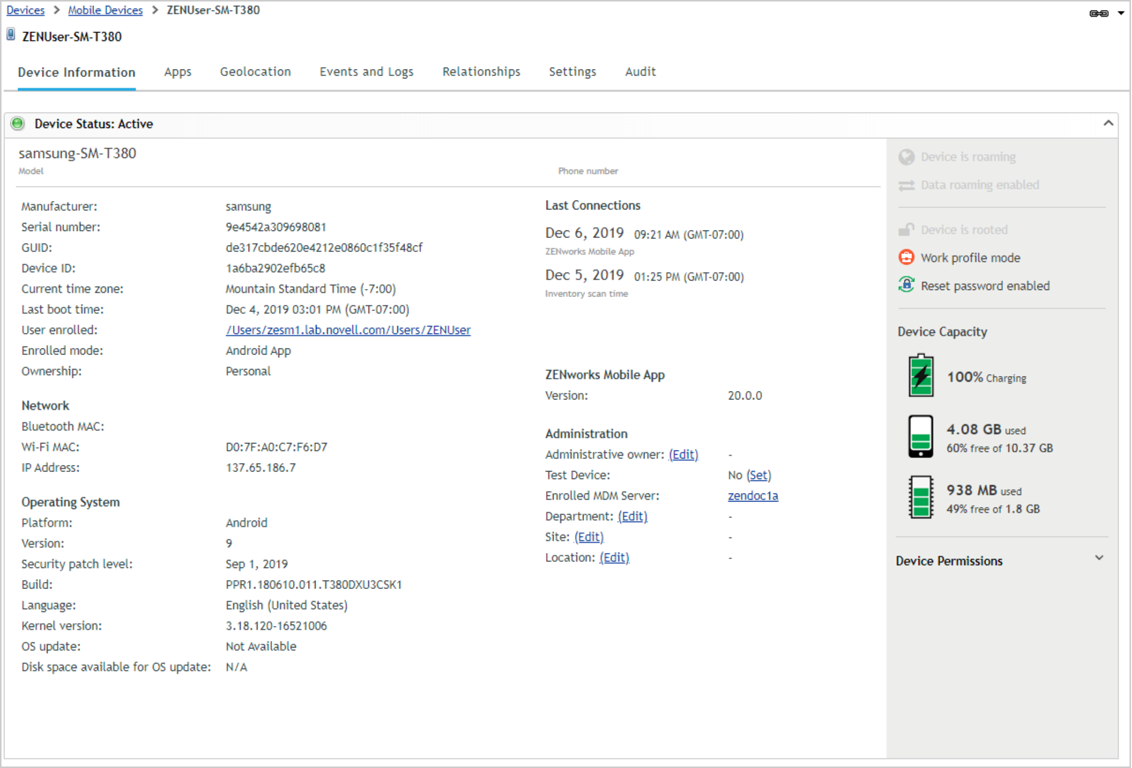
	Status	Name	Type	Operating System	Last Contact	Retired
☐		Pending Enrollment Devices (Details)	Mobile Folder			
☐		Android	Dynamic Mobile Device Group			
☐		iOS	Dynamic Mobile Device Group			
☐		Windows Phone	Dynamic Mobile Device Group			
☐		ZENUser-SM-T380	Mobile Device	Android-9	9:21 AM	

1 - 5 of 5 items

show 25 items

6 (Optional) In the list, click the Android device to display its Device Information page.

The Device Information page provides inventory details collected from the device.



Devices > Mobile Devices > ZENUser-SM-T380

ZENUser-SM-T380

Device Information | Apps | Geolocation | Events and Logs | Relationships | Settings | Audit

Device Status: Active

samsung-SM-T380
Model

Phone number

Manufacturer:	samsung
Serial number:	9e4542a309698081
GUID:	de317cbde620e4212e0860c1f35f48cf
Device ID:	1a6ba2902efb65c8
Current time zone:	Mountain Standard Time (-7:00)
Last boot time:	Dec 4, 2019 03:01 PM (GMT-07:00)
User enrolled:	/Users/zesm1.lab.novell.com/Users/ZENUser
Enrolled mode:	Android App
Ownership:	Personal

Network

Bluetooth MAC:	
Wi-Fi MAC:	D0:7F:A0:C7:F6:D7
IP Address:	137.65.186.7

Operating System

Platform:	Android
Version:	9
Security patch level:	Sep 1, 2019
Build:	PPR1.180610.011.T380DXU3CSK1
Language:	English (United States)
Kernel version:	3.18.120-16521006
OS update:	Not Available
Disk space available for OS update:	N/A

Last Connections

Dec 6, 2019 09:21 AM (GMT-07:00)
ZENworks Mobile App

Dec 5, 2019 01:25 PM (GMT-07:00)
Inventory scan time

ZENworks Mobile App

Version:	20.0.0

Administration

Administrative owner: (Edit)	-
Test Device:	No (Set)
Enrolled MDM Server:	zendoc1a
Department: (Edit)	-
Site: (Edit)	-
Location: (Edit)	-

Device is roaming

Data roaming enabled

Device is rooted

Work profile mode

Reset password enabled

Device Capacity

100% Charging

4.08 GB used
60% free of 10.37 GB

938 MB used
49% free of 1.8 GB

Device Permissions

Enroll an Android Device in Work-Managed Mode

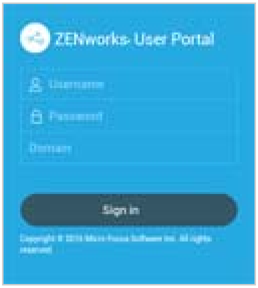
Work-managed mode enables you to manage and secure the entire Android device. This mode is mainly intended for corporate-owned devices. If you need to support personal devices (BYOD), see "Enroll an Android Device in Work Profile Mode" on page 92.

You can enroll any device running Android version 6 and newer. We used a Samsung Galaxy Tab A running Android version 9. Again, the screens and steps might vary slightly on other Android devices and versions.

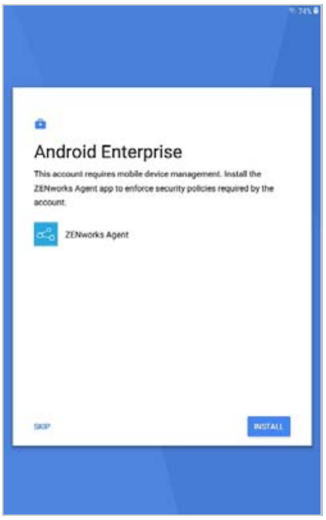
1 Make sure the device is factory fresh.

If the device has previously been started and configured, you must perform a factory reset before you can enroll it in work-managed mode.

2 Start the device and complete the initial screens (language, Wi-Fi setup, Terms and Conditions) until you reach the following screen:



3 Enter `afw#zenworks`, then tap **Next**.

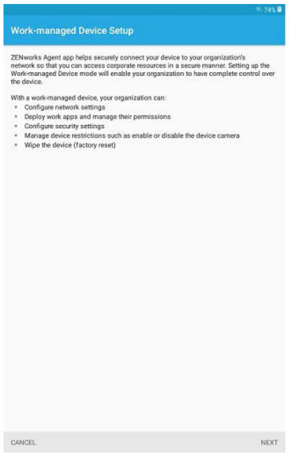


Android Enterprise

This account requires mobile device management. Install the ZENworks Agent app to enforce security policies required by the account.

4 Tap **Install** to download the ZENworks Agent. When prompted, tap **Install** again to confirm the installation of the ZENworks Agent on the device.

5 Follow the prompts shown in the following screens to set up the device.

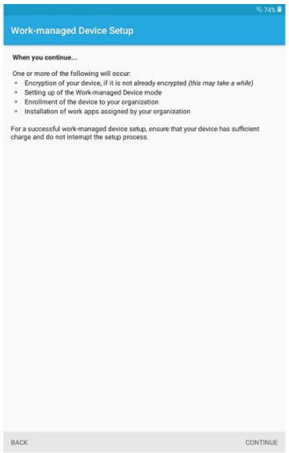


Work-managed Device Setup

ZENworks Agent app helps securely connect your device to your organization's network so that you can access corporate resources in a secure manner. Setting up the Work-managed Device mode will enable your organization to have complete control over the device.

With a work-managed device, your organization can:

- Configure network settings
- Deploy work apps and manage their permissions
- Configure security settings
- Manage device restrictions such as enable or disable the device camera
- Wipe the device (factory reset)



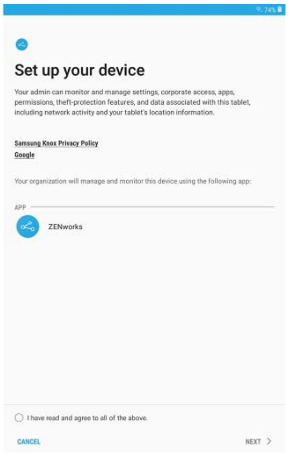
Work-managed Device Setup

When you continue...

One or more of the following will occur:

- Encryption of your device, if it is not already encrypted *(this may take a while)*
- Setting up of the Work-managed Device mode
- Enrollment of the device to your organization
- Installation of work apps assigned by your organization

For a successful work-managed device setup, ensure that your device has sufficient charge and do not interrupt the setup process.



Set up your device

Your admin can monitor and manage settings, corporate access, apps, permissions, theft-protection features, and data associated with this tablet, including network activity and your tablet's location information.

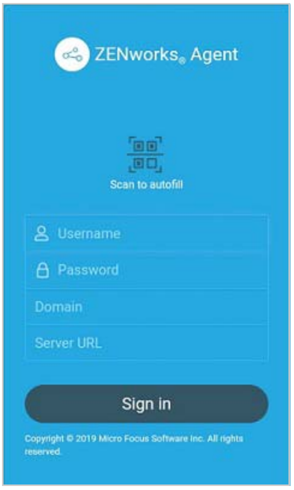
Samsung Knox Privacy Policy
Google

Your organization will manage and monitor this device using the following app:

APP
ZENworks

○ I have read and agree to all of the above.

When work profile setup is complete, the device is enrolled in ZENworks and the ZENworks Agent login screen is displayed:



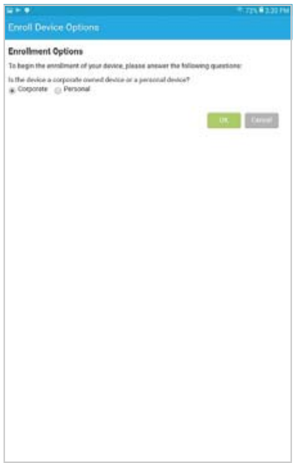
Copyright © 2019 Micro Focus Software Inc. All rights reserved.

6 To log in and complete the enrollment, fill in the evaluation user’s username and password, fill in the URL of the ZENworks Primary Server, then tap **Sign In**.

The Domain name field is not needed because the system is configured for simple enrollment, which allows users to log in with only their username rather than their full domain name.

Notice the **Scan to autofill** option. This lets a user fill in the information by scanning a code included in an invitation email that you send. We didn’t do the configuration required to use this, so ignore this option for now.

Because the Mobile Enrollment policy was configured to allow users to choose whether the device is a corporate or personal device, the Enrollment Options screen is displayed.



Enrollment Options

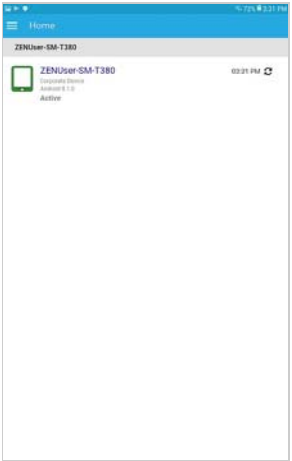
To begin the enrollment of your device, please answer the following questions:

Is the device a corporate owned device or a personal device?

● Corporate ○ Personal

7 Tap **OK** to enroll the device as a corporate device.

When enrollment is complete, the Android device is listed in the mobile app.

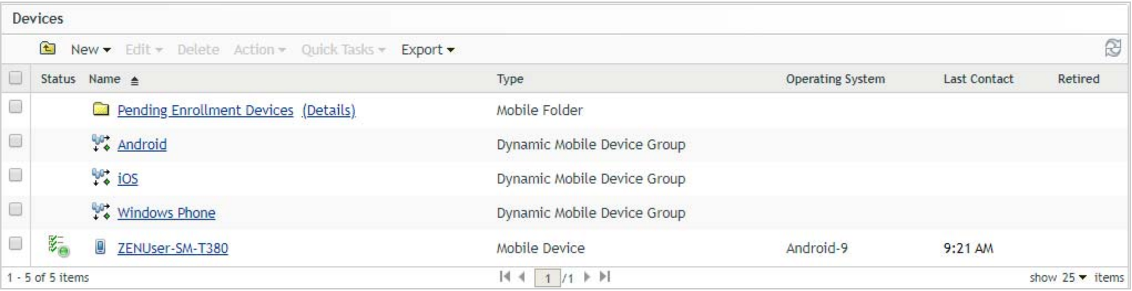


ZENUser-SM-T380

ZENUser-SM-T380 03:21 PM
Corporate Device
Android 8.1.0
Active

8 If you are notified that a password change is needed, tap the notification and enter a new password.

9 In ZENworks Control Center, go to the **Devices** > **Mobile Devices** list to confirm that the device is enrolled in the zone.

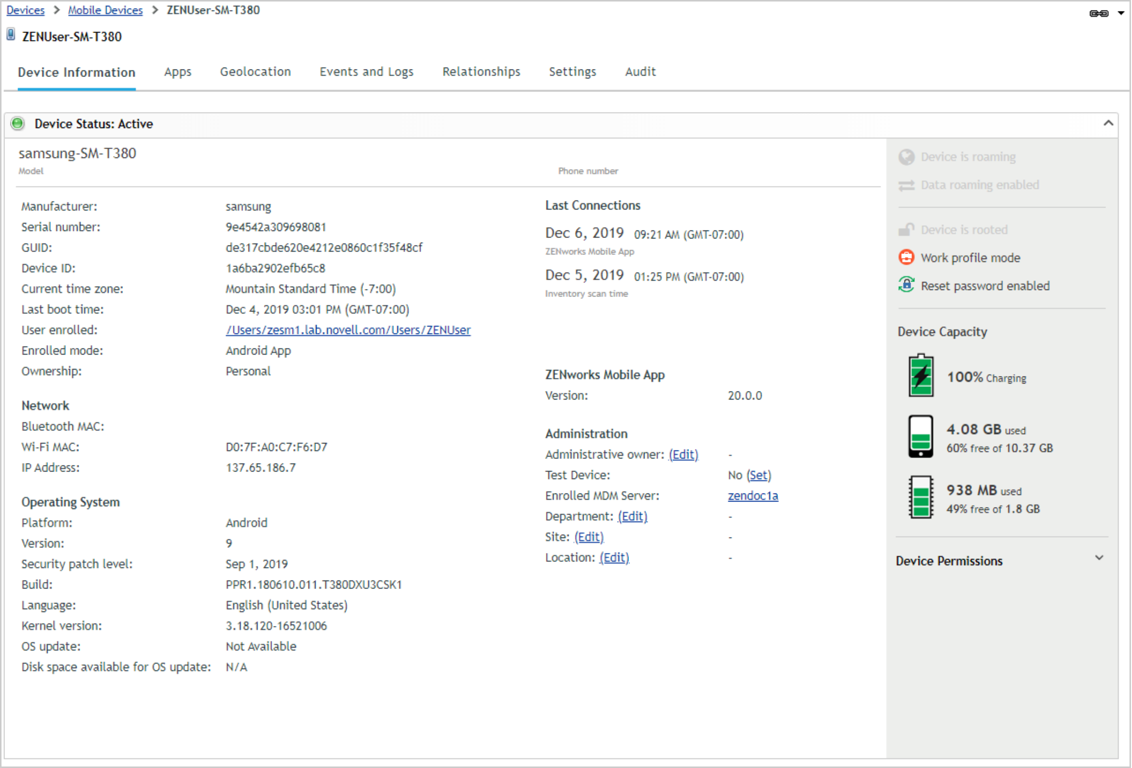


□	Status	Name	Type	Operating System	Last Contact	Retired
□		Pending Enrollment Devices (Details)	Mobile Folder			
□		Android	Dynamic Mobile Device Group			
□		iOS	Dynamic Mobile Device Group			
□		Windows Phone	Dynamic Mobile Device Group			
□		ZENUser-SM-T380	Mobile Device	Android-9	9:21 AM	

1 - 5 of 5 items 1 /1 show 25 items

10 (Optional) In the list, click the Android device to display its Device Information page.

The Device Information page provides inventory details collected from the device.



ZENUser-SM-T380

Device Status: Active

samsung-SM-T380
Model

Phone number

Manufacturer:	samsung
Serial number:	9e4542a309698081
GUID:	de317cbde620e4212e0860c1f35f48cf
Device ID:	1a6ba2902efb65c8
Current time zone:	Mountain Standard Time (-7:00)
Last boot time:	Dec 4, 2019 03:01 PM (GMT-07:00)
User enrolled:	/Users/zesm1.lab.novell.com/Users/ZENUser
Enrolled mode:	Android App
Ownership:	Personal

Network

Bluetooth MAC:	
Wi-Fi MAC:	D0:7F:A0:C7:F6:D7
IP Address:	137.65.186.7

Operating System

Platform:	Android
Version:	9
Security patch level:	Sep 1, 2019
Build:	PPR1.180610.011.T380DXU3CSK1
Language:	English (United States)
Kernel version:	3.18.120-16521006
OS update:	Not Available
Disk space available for OS update:	N/A

Last Connections

Dec 6, 2019 09:21 AM (GMT-07:00)
ZENworks Mobile App

Dec 5, 2019 01:25 PM (GMT-07:00)
Inventory scan time

ZENworks Mobile App

Version:	20.0.0

Administration

Administrative owner: (Edit)	-
Test Device:	No (Set)
Enrolled MDM Server:	zendoc1a
Department: (Edit)	-
Site: (Edit)	-
Location: (Edit)	-

Work profile mode

Reset password enabled

Device Capacity

100% Charging

4.08 GB used
60% free of 10.37 GB

938 MB used
49% free of 1.8 GB

5.2 Secure Your Mobile Devices

ZENworks secures devices through the use of policies. You configure a policy’s settings, assign the policy to the device’s user, and then sit back while the policy enforces your settings on the device.

- Apply a Security Policy to Mobile Devices (page 99)
- Apply a Control Policy to Mobile Devices (page 103)

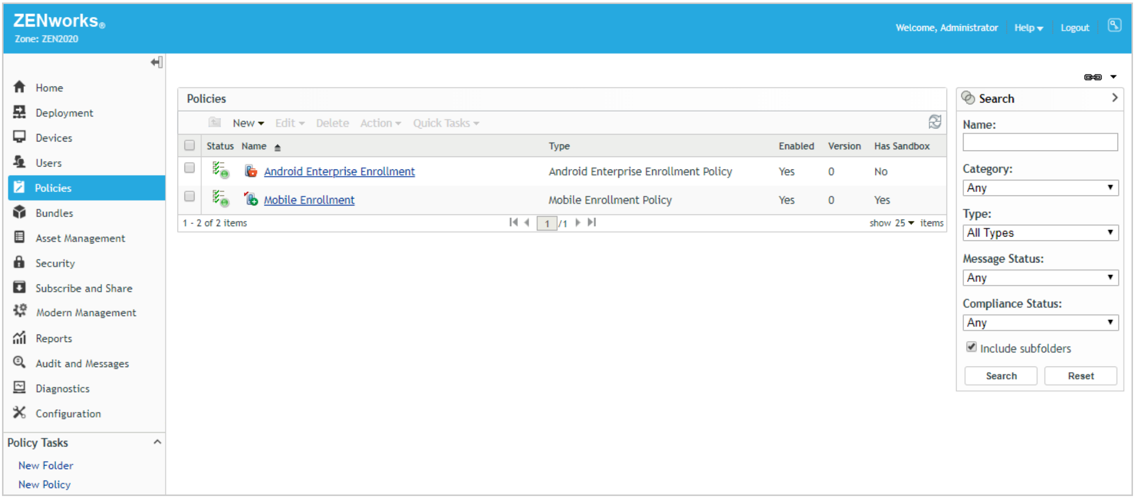
5.2.1 Apply a Security Policy to Mobile Devices

The Mobile Security policy controls password, encryption, and device inactivity settings on iOS and Android devices.

- “Create a Mobile Security Policy” on page 100
- “Assign the Policy” on page 101
- “Test the Policy on an iOS Device” on page 102
- “Test the Policy on an Android Device” on page 102

Create a Mobile Security Policy

1 In ZENworks Control Center, click **Policies** (in the left navigation pane).



Status	Name	Type	Enabled	Version	Has Sandbox
	Android Enterprise Enrollment	Android Enterprise Enrollment Policy	Yes	0	No
	Mobile Enrollment	Mobile Enrollment Policy	Yes	0	Yes

1 - 2 of 2 items 1/1 show 25 items

Name:
Category: Any
Type: All Types
Message Status: Any
Compliance Status: Any
☑ Include subfolders

2 Click **New** > **Policy** to display the Create New Policy wizard.

3 On the Select Platform page, select **Mobile**, then click **Next**.

4 On the Select Policy Category page, select **General Mobile Policies**, then click **Next**.

5 On the Select Policy Type page, select **Mobile Security Policy**, then click **Next**.

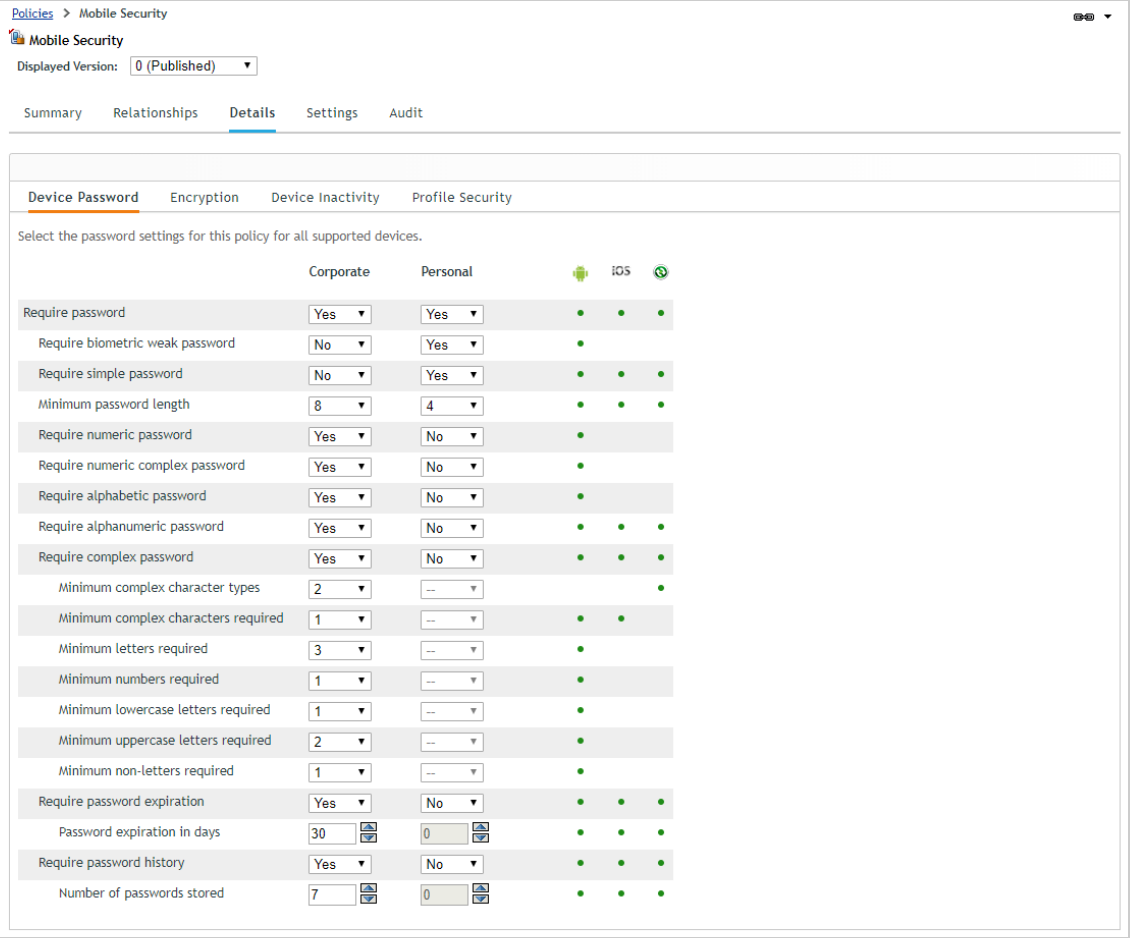
6 On the Define Details page, specify *Mobile Security* for the policy name, then click **Next**.

7 On the Select Security Level page, leave the default settings (*Strict* security for Corporate devices and *Low* security for Personal devices), then click **Next**.

The security policy includes dozens of settings. So that you don't have to deal with them individually, you select the security level you want and ZENworks populates the settings with the values appropriate to the level.

8 On the Summary page, deselect **Create as Sandbox**, select **Define Additional Properties**, then click **Finish** to create the policy and display it.

You'll notice that the security settings for Corporate devices have been configured to adhere to the Strict security level you selected when creating the policy and the Personal settings reflect the Low security level. This means that Corporate devices will enforce a complex password with a minimum of 8 characters including letters (both uppercase and lowercase), numbers, and special characters.



Select the password settings for this policy for all supported devices.

	Corporate	Personal		iOS	
Require password	Yes	Yes	●	●	●
Require biometric weak password	No	Yes	●		
Require simple password	No	Yes	●	●	●
Minimum password length	8	4	●	●	●
Require numeric password	Yes	No	●		
Require numeric complex password	Yes	No	●		
Require alphabetic password	Yes	No	●		
Require alphanumeric password	Yes	No	●	●	●
Require complex password	Yes	No	●	●	●
Minimum complex character types	2	--			●
Minimum complex characters required	1	--	●	●	
Minimum letters required	3	--	●		
Minimum numbers required	1	--	●		
Minimum lowercase letters required	1	--	●		
Minimum uppercase letters required	2	--	●		
Minimum non-letters required	1	--	●		
Require password expiration	Yes	No	●	●	●
Password expiration in days	30	0	●	●	●
Require password history	Yes	No	●	●	●
Number of passwords stored	7	0	●	●	●

9 Click the **Device Inactivity** tab.

Notice that an inactivity lock is enforced on Corporate devices, with the user being allowed to set the inactivity timeout to a maximum of 1 minute. Notice also that after 7 failed unlock attempts, the device is wiped.

10 You can change individual settings as needed...except, don’t change them at this point in the evaluation. After you’ve finished the evaluation, go ahead and change whatever you want as you play and explore more.

Assign the Policy

This policy can be assigned to either users or devices. We’ll have you assign it to the evaluation user so that the policy will apply to all of the devices enrolled by the user. If you were to use a device assignment, you would need to assign it to each device.

1 Click **Relationships**.

2 In the User Assignments list, click **Add**.

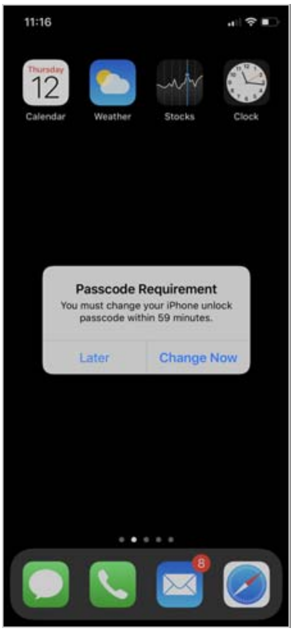
3 Select the evaluation user, then click **OK** to add the user to the assignment list.

4 Follow the prompts to complete the assignment wizard.

Test the Policy on an iOS Device

After the policy is assigned to the evaluation user, ZENworks refreshes the device so that the policy can be enforced. On iOS devices, if the policy requires the user to change something, such as the passcode, the user is prompted.

1 On the iOS device, wait for the following prompt to be displayed.



Passcode Requirement

You must change your iPhone unlock passcode within 59 minutes.

2 Tap **Continue**, then follow the prompts to change the passcode to meet the policy requirements.

3 Verify the inactivity timeout setting by tapping **Settings** > **Display & Brightness** > **Auto-Lock**.

The Mobile Security policy's *Strict* security level changes the Auto-Lock setting to a maximum of 1 minute.

4 (Optional) To see a list of the full passcode restrictions enforced by the policy, tap **Settings** > **General** > **Profiles & Device Management** > **ZENworks Management Profile** > **Restrictions** > **Passcode**.

At this point, feel free to change the settings in the Mobile Security policy to see how they are enforced on the device. After you change settings, make sure you publish the policy again so that the changes are applied to the device. And remember, any changes you make to the policy are reflected on all of the evaluation user's devices.

Test the Policy on an Android Device

After the policy is assigned to the user, the user's Android device receives a ZENworks notification that the password needs to be changed. If this doesn't happen within a minute, tap the ZENworks Agent app and then tap 🔄 to refresh the device.

1 Tap the notification to change the password on the device to conform to the policy password requirements.

2 Go to **Settings** > **Display** > **Screen timeout**. Notice that the timeout maximum setting is 1 minute as defined in the policy.

At this point, feel free to change the settings in the Mobile Security policy to see how they are enforced on the device. After you change settings, make sure you publish the policy again so that the changes are applied to the device. And remember, any changes you make to the policy are reflected on all of the evaluation user’s devices.

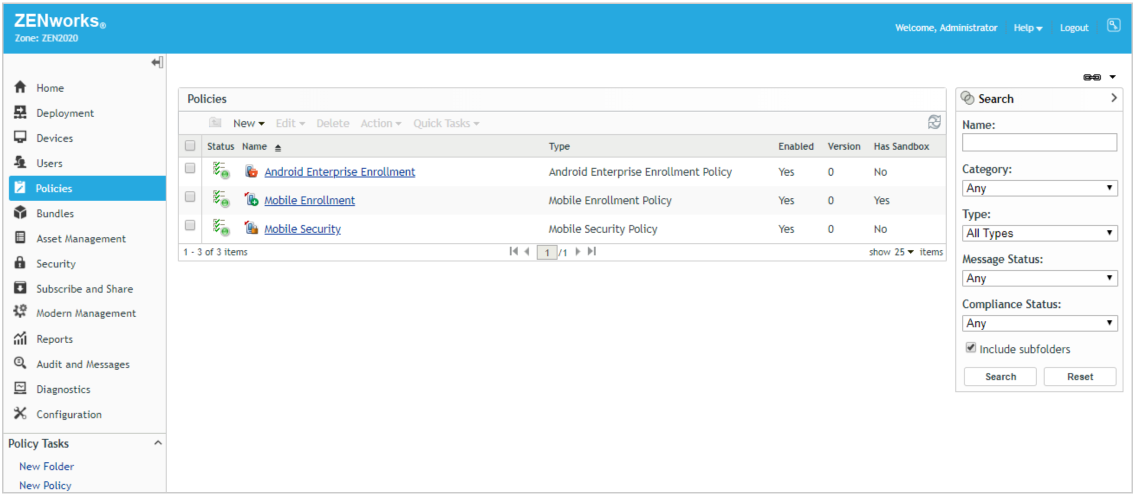
5.2.2 Apply a Control Policy to Mobile Devices

The Mobile Device Control policy lets you restrict access to the features of a mobile device such as the camera, the web browser, and voice assistance.

- “Create the Mobile Device Control Policy” on page 103
- “Assign the Policy” on page 105
- “Test the Policy on an iOS Device” on page 106
- “Test the Policy on an Android Device” on page 106

Create the Mobile Device Control Policy

1 In ZENworks Control Center, click **Policies** (in the left navigation pane).



Status	Name	Type	Enabled	Version	Has Sandbox
	Android Enterprise Enrollment	Android Enterprise Enrollment Policy	Yes	0	No
	Mobile Enrollment	Mobile Enrollment Policy	Yes	0	Yes
	Mobile Security	Mobile Security Policy	Yes	0	No

1 - 3 of 3 items   1 /1   show 25 items

Name:
Category: Any
Type: All Types
Message Status: Any
Compliance Status: Any
☑ Include subfolders

2 Click **New** > **Policy** to display the Create New Policy wizard.

3 On the Select Platform page, select **Mobile**, then click **Next**.

4 On the Select Policy Category page, select **General Mobile Policies**, then click **Next**.

5 On the Select Policy Type page, select **Mobile Device Control Policy**, then click **Next**.

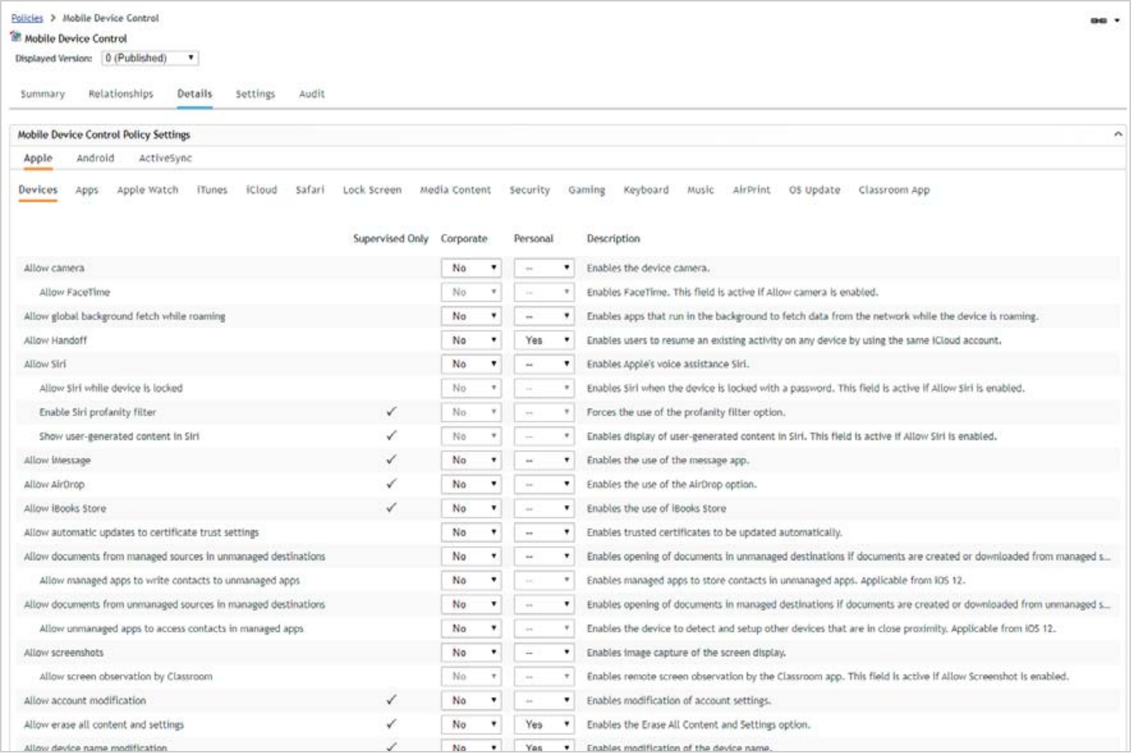
6 On the Define Details page, specify *Mobile Device Control* as the name of the policy, then click **Next**.

7 On the Configure Mobile Device Control Settings page, change the Corporate setting to **High**, then click **Next**.

The device control policy includes hundreds of settings. So that you don’t have to deal with them individually, you select the control level you want and ZENworks populates the settings with the values appropriate to the level.

8 On the Summary page, deselect **Create as Sandbox**, select **Define Additional Properties**, then click **Finish** to create the policy and display it.

The policy is opened with the Apple device settings displayed.



Policies > Mobile Device Control

Mobile Device Control

Displayed Version: 0 (Published)

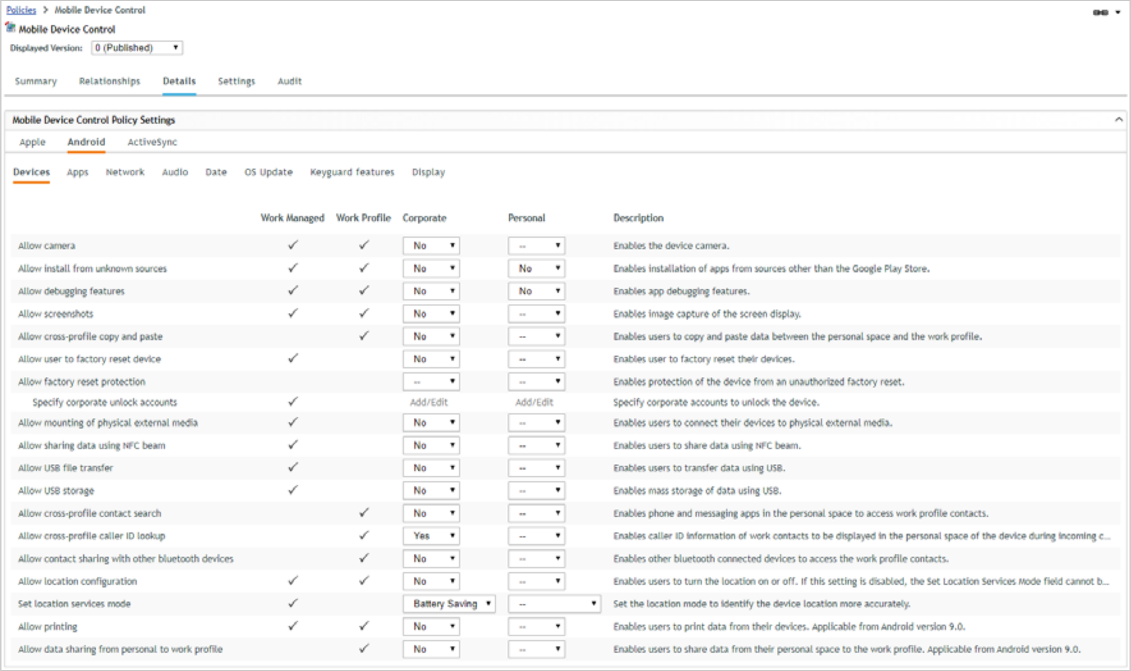
Mobile Device Control Policy Settings

	Supervised Only	Corporate	Personal	Description
Allow camera		No	--	Enables the device camera.
Allow FaceTime		No	--	Enables FaceTime. This field is active if Allow camera is enabled.
Allow global background fetch while roaming		No	--	Enables apps that run in the background to fetch data from the network while the device is roaming.
Allow Handoff		No	Yes	Enables users to resume an existing activity on any device by using the same iCloud account.
Allow Siri		No	--	Enables Apple's voice assistance Siri.
Allow Siri while device is locked		No	--	Enables Siri when the device is locked with a password. This field is active if Allow Siri is enabled.
Enable Siri profanity filter	✓	No	--	Forces the use of the profanity filter option.
Show user-generated content in Siri	✓	No	--	Enables display of user-generated content in Siri. This field is active if Allow Siri is enabled.
Allow iMessage	✓	No	--	Enables the use of the message app.
Allow AirDrop	✓	No	--	Enables the use of the AirDrop option.
Allow iBooks Store	✓	No	--	Enables the use of iBooks Store
Allow automatic updates to certificate trust settings		No	--	Enables trusted certificates to be updated automatically.
Allow documents from managed sources in unmanaged destinations		No	--	Enables opening of documents in unmanaged destinations if documents are created or downloaded from managed s...
Allow managed apps to write contacts to unmanaged apps		No	--	Enables managed apps to store contacts in unmanaged apps. Applicable from iOS 12.
Allow documents from unmanaged sources in managed destinations		No	--	Enables opening of documents in managed destinations if documents are created or downloaded from unmanaged s...
Allow unmanaged apps to access contacts in managed apps		No	--	Enables the device to detect and setup other devices that are in close proximity. Applicable from iOS 12.
Allow screenshots		No	--	Enables image capture of the screen display.
Allow screen observation by Classroom		No	--	Enables remote screen observation by the Classroom app. This field is active if Allow Screenshot is enabled.
Allow account modification	✓	No	--	Enables modification of account settings.
Allow erase all content and settings	✓	No	Yes	Enables the Erase All Content and Settings option.
Allow device name modification	✓	No	Yes	Enables modification of the device name.

The Corporate device control settings reflect the High control setting you selected when creating the policy, while the Personal settings reflect the Low control setting. Some of the settings apply only to devices that have Supervised mode enabled.

As you scan down the list of settings, notice that many Corporate device capabilities are not allowed, including use of the camera, capturing of screenshots, and installation of apps from the App Store (on the Apps tab). We'll verify these enforcements when we test the policy on an iOS device.

9 Click the **Android** link to see all of the Android device control settings.



Displayed Version: 0 (Published)

Mobile Device Control Policy Settings

	Work Managed	Work Profile	Corporate	Personal	Description
Allow camera	✓	✓	No	--	Enables the device camera.
Allow install from unknown sources	✓	✓	No	No	Enables installation of apps from sources other than the Google Play Store.
Allow debugging features	✓	✓	No	No	Enables app debugging features.
Allow screenshots	✓	✓	No	--	Enables image capture of the screen display.
Allow cross-profile copy and paste		✓	No	--	Enables users to copy and paste data between the personal space and the work profile.
Allow user to factory reset device	✓		No	--	Enables user to factory reset their devices.
Allow factory reset protection			--	--	Enables protection of the device from an unauthorized factory reset.
Specify corporate unlock accounts	✓		Add/Edit	Add/Edit	Specify corporate accounts to unlock the device.
Allow mounting of physical external media	✓		No	--	Enables users to connect their devices to physical external media.
Allow sharing data using NFC beam	✓		No	--	Enables users to share data using NFC beam.
Allow USB file transfer	✓		No	--	Enables users to transfer data using USB.
Allow USB storage	✓		No	--	Enables mass storage of data using USB.
Allow cross-profile contact search		✓	No	--	Enables phone and messaging apps in the personal space to access work profile contacts.
Allow cross-profile caller ID lookup		✓	Yes	--	Enables caller ID information of work contacts to be displayed in the personal space of the device during incoming c...
Allow contact sharing with other bluetooth devices		✓	No	--	Enables other bluetooth connected devices to access the work profile contacts.
Allow location configuration	✓	✓	No	--	Enables users to turn the location on or off. If this setting is disabled, the Set Location Services Mode field cannot b...
Set location services mode	✓		Battery Saving	--	Set the location mode to identify the device location more accurately.
Allow printing	✓	✓	No	--	Enables users to print data from their devices. Applicable from Android version 9.0.
Allow data sharing from personal to work profile		✓	No	--	Enables users to share data from their personal space to the work profile. Applicable from Android version 9.0.

ZENworks supports Android devices using either work managed or work profile modes. Notice that some settings apply to only one or the other of the modes.

As with the Apple settings, notice that many Corporate device capabilities are not allowed, including use of the camera and capturing of screenshots, which we'll test when the policy is applied to an Android device.

10 You can change individual settings as needed...except, don't change them at this point in the evaluation. After you've finished the evaluation, go ahead and change whatever you want as you play and explore more.

Assign the Policy

Like the Mobile Security policy, the Mobile Device Control policy can be assigned to either users or devices. Go ahead and assign it to the evaluation user.

1. Click **Relationships**.
2. In the User Assignments list, click **Add**.
3. Select the evaluation user, then click **OK** to add the user to the assignment list.
4. Follow the prompts to complete the assignment wizard.

Test the Policy on an iOS Device

The iOS device should receive the Mobile Device Control policy within a minute of it being assigned to the evaluation user. You can ensure that the policy has been received by tapping the ZENworks Agent app and then refreshing 🔄 the device.

1. Try to take a screenshot. You are informed that the security policy does not allow screenshots.
2. Try to use the camera. Again, no luck, because the Camera app has been removed.
3. (Optional) To see a list of the full restrictions enforced by the policy, tap **Settings** > **General** > **Profiles & Device Management** > **ZENworks Management Profile** > **Restrictions**.

At this point, feel free to change the settings in the Mobile Device Control policy to see how they are enforced on the device. After you change settings, make sure you publish the policy again so that the changes are applied to the device. And remember, any changes you make to the policy are reflected on all of the evaluation user’s devices.

Test the Policy on an Android Device

The Android device should receive the Mobile Device Control policy within a minute of it being assigned to the evaluation user. You can ensure that the policy has been received by tapping the ZENworks Agent app and then refreshing 🔄 the device.

1. Try to take a screenshot. You are informed that the security policy does not allow screenshots.
2. Try to use the camera. Again, no luck.
3. Go to **Settings** > **Display**. Notice that you can’t change the brightness or the screen timeout. Neither are allowed by the policy.
4. Go ahead and explore to see what else doesn’t work. Because the policy is set to High control, many things are disabled.

At this point, feel free to change the settings in the Mobile Device Control policy to see how they are enforced on the device. After you change settings, make sure you publish the policy again so that the changes are applied to the device. And remember, any changes you make to the policy are reflected on all of the evaluation user’s devices.

5.3 Distribute an App to Your Mobile Devices

ZENworks supports distributing of applications to iOS and Android devices.

- Distribute an Apple App Store App to an iOS Device (page 107)
- Distribute an Apple VPP App to an iOS Device (page 112)
- Distribute an Android Enterprise App to an Android Device (page 117)
- View the Bundle Status (page 120)

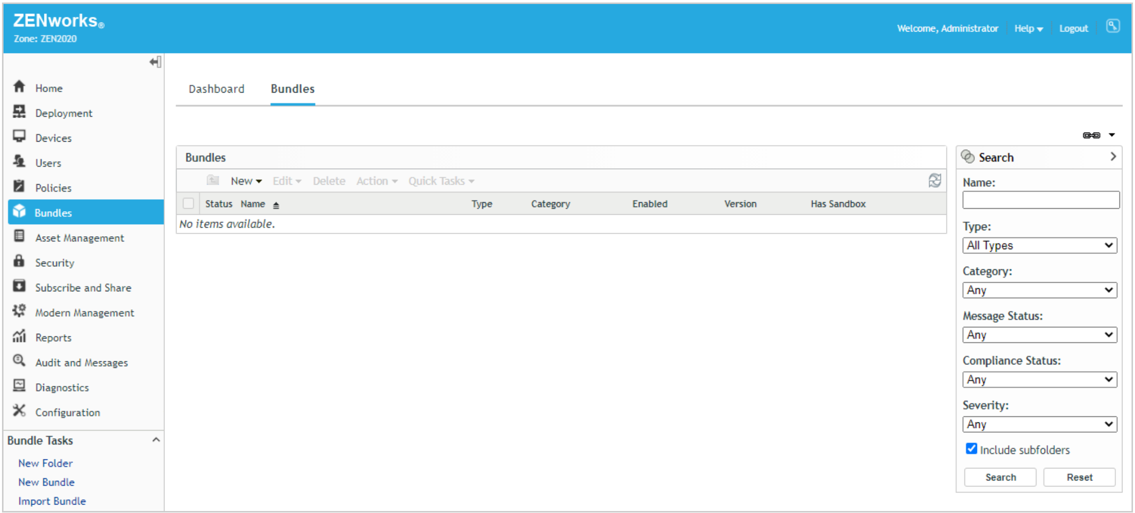
5.3.1 Distribute an Apple App Store App to an iOS Device

ZENworks lets you distribute free apps from the Apple App Store.

- "Create a Bundle for the App Store App" on page 107
- "Assign the Bundle" on page 110
- "Test the Bundle" on page 111

Create a Bundle for the App Store App

1 In ZENworks Control Center, click **Bundles** (in the left navigation pane).



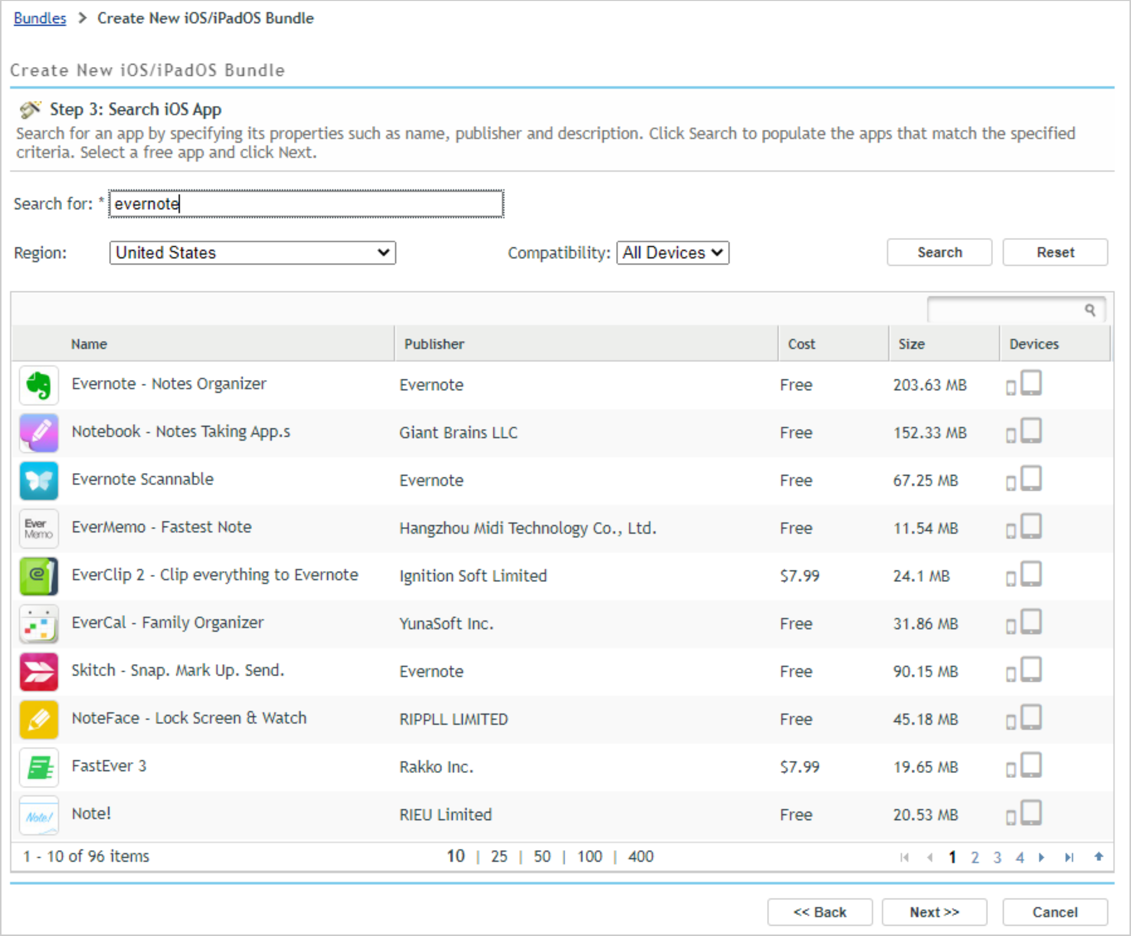
2 Click **New** > **Bundle** to display the Create New Bundle wizard.

3 On the Select Bundle Type page, select **iOS/iPadOS Bundle**, then click **Next**.

4 On the Select Bundle Category page, select **App Store App**, then click **Next**.

5 On the Search iOS App page, enter *Evernote* in the **Search for** box, select your region, then click **Search**.

ZENworks returns a list of App Store apps that match the search criteria.



Bundles > Create New iOS/iPadOS Bundle

Create New iOS/iPadOS Bundle

Step 3: Search iOS App

Search for an app by specifying its properties such as name, publisher and description. Click Search to populate the apps that match the specified criteria. Select a free app and click Next.

Search for: * evernote

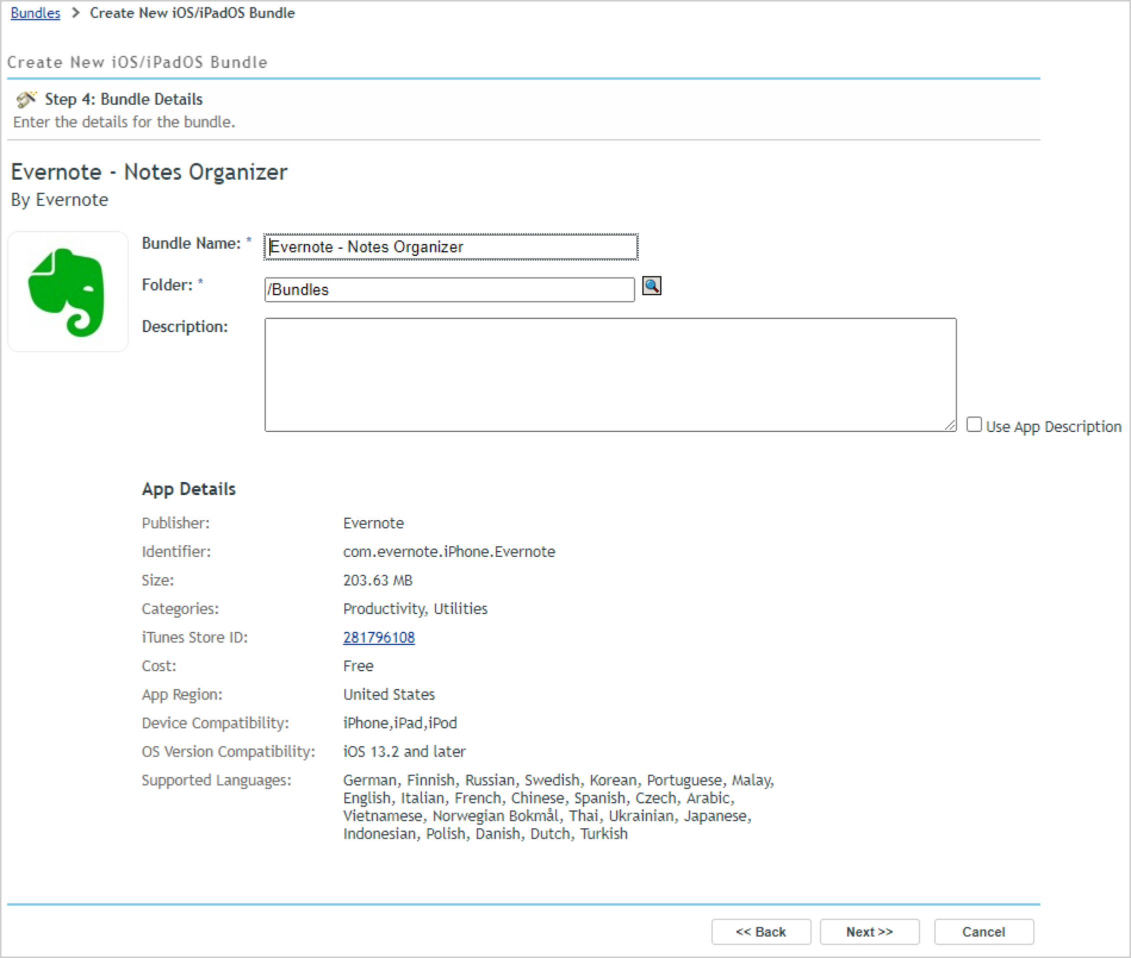
Region: United States

Compatibility: All Devices

Name	Publisher	Cost	Size	Devices
Evernote - Notes Organizer	Evernote	Free	203.63 MB	
Notebook - Notes Taking App.s	Giant Brains LLC	Free	152.33 MB	
Evernote Scannable	Evernote	Free	67.25 MB	
EverMemo - Fastest Note	Hangzhou Midi Technology Co., Ltd.	Free	11.54 MB	
EverClip 2 - Clip everything to Evernote	Ignition Soft Limited	$7.99	24.1 MB	
EverCal - Family Organizer	YunaSoft Inc.	Free	31.86 MB	
Skitch - Snap. Mark Up. Send.	Evernote	Free	90.15 MB	
NoteFace - Lock Screen & Watch	RIPPLL LIMITED	Free	45.18 MB	
FastEver 3	Rakko Inc.	$7.99	19.65 MB	
Note!	RIEU Limited	Free	20.53 MB	

1 - 10 of 96 items

6 Select the Evernote app, then click **Next** to display the Bundle Details page.



Bundles > Create New iOS/iPadOS Bundle

Create New iOS/iPadOS Bundle

Step 4: Bundle Details
Enter the details for the bundle.

Evernote - Notes Organizer
By Evernote

Bundle Name: * Evernote - Notes Organizer

Folder: * /Bundles

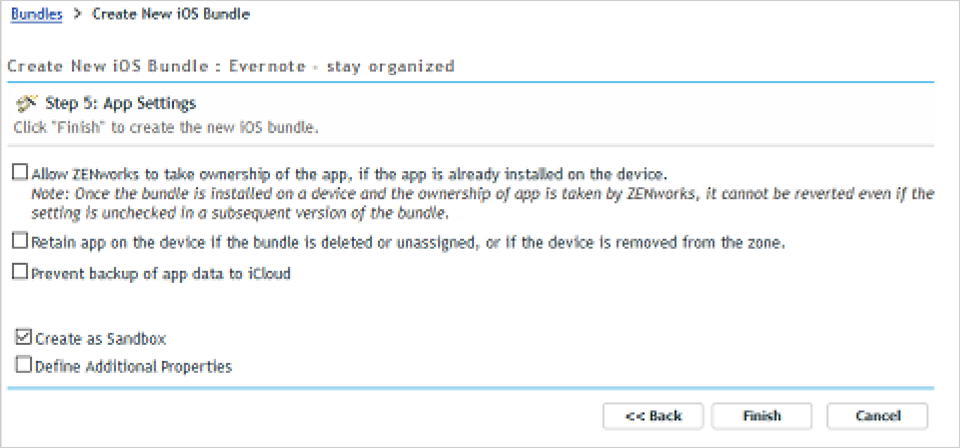
Description:

□ Use App Description

App Details

Publisher:	Evernote
Identifier:	com.evernote.iPhone.Evernote
Size:	203.63 MB
Categories:	Productivity, Utilities
iTunes Store ID:	281796108
Cost:	Free
App Region:	United States
Device Compatibility:	iPhone,iPad,iPod
OS Version Compatibility:	iOS 13.2 and later
Supported Languages:	German, Finnish, Russian, Swedish, Korean, Portuguese, Malay, English, Italian, French, Chinese, Spanish, Czech, Arabic, Vietnamese, Norwegian Bokmål, Thai, Ukrainian, Japanese, Indonesian, Polish, Danish, Dutch, Turkish

7 On the Bundle Details page, review the details, then click **Next** to display the App Settings page.



Bundles > Create New iOS Bundle

Create New iOS Bundle : Evernote - stay organized

Step 5: App Settings
Click "Finish" to create the new iOS bundle.

□ Allow ZENworks to take ownership of the app, if the app is already installed on the device.
Note: Once the bundle is installed on a device and the ownership of app is taken by ZENworks, it cannot be reverted even if the setting is unchecked in a subsequent version of the bundle.

□ Retain app on the device if the bundle is deleted or unassigned, or if the device is removed from the zone.

□ Prevent backup of app data to iCloud

☑ Create as Sandbox

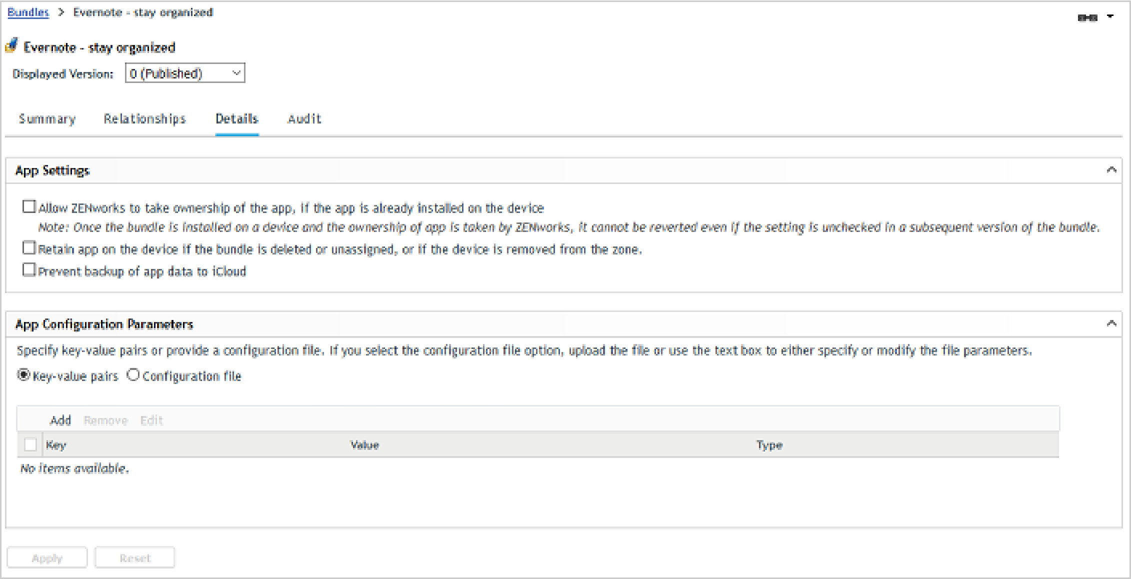
□ Define Additional Properties

8 On the App Settings page:

8a Leave the top three settings as configured (unselected).

8b Deselect the **Create as Sandbox** setting and select the **Define Additional Properties** setting.

8c Click **Finish** to create the bundle and display it.



Evernote - stay organized

Displayed Version: 0 (Published)

App Settings

□ Allow ZENworks to take ownership of the app, if the app is already installed on the device

Note: Once the bundle is installed on a device and the ownership of app is taken by ZENworks, it cannot be reverted even if the setting is unchecked in a subsequent version of the bundle.

□ Retain app on the device if the bundle is deleted or unassigned, or if the device is removed from the zone.

□ Prevent backup of app data to iCloud

App Configuration Parameters

Specify key-value pairs or provide a configuration file. If you select the configuration file option, upload the file or use the text box to either specify or modify the file parameters.

● Key-value pairs ○ Configuration file

□ Key	Value	Type

No items available.

Note the App Configuration Parameters settings. You don't need to change anything here for this evaluation, but just be aware that these settings can be used to preconfigure an app with data such as a user login name (via a variable) or a server address that the app needs to connect to.

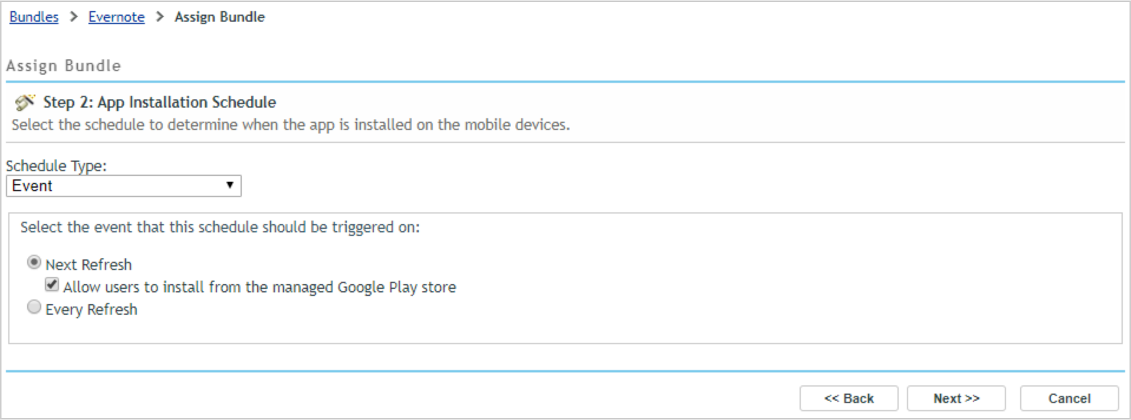
Assign the Bundle

Bundles can be assigned to users or devices. We'll have you assign the bundle to the iOS device this time.

1 Click **Relationships**.

2 In the Device Assignments list, click **Add**.

3 Use the Select Objects dialog to add the iOS device to the assignment list, then click **Next** to display the App Installation Schedule page.



Assign Bundle

Step 2: App Installation Schedule

Select the schedule to determine when the app is installed on the mobile devices.

Schedule Type: Event

Select the event that this schedule should be triggered on:

● Next Refresh

☑ Allow users to install from the managed Google Play store

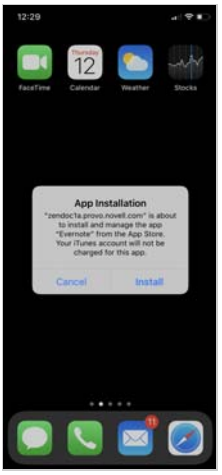
○ Every Refresh

The App Installation Schedule page lets you determine if you want to push the bundle to the device now (upon completion of the assignment to the device) or let the device find out about the bundle the next time it refreshes information from the ZENworks zone.

4. In the Schedule Type list, select **Now** so that the bundle is pushed to the device immediately, keep the Quick Task Notification Options default settings, then click **Next** to display the Bundle Conflict Resolution page.
5. Select Device Precedence, then click **Next** to display the Summary page.
6. Click **Finish** to create the assignment.

Test the Bundle

When the bundle is distributed to your iOS device, a notification is displayed on the device.



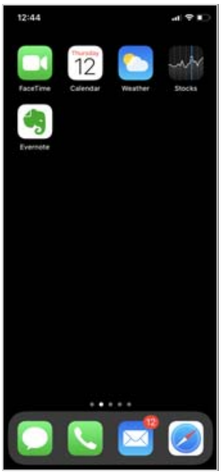
App Installation

"zendoc1a.provo.novell.com" is about to install and manage the app "Evernote" from the App Store. Your iTunes account will not be charged for this app.

1. Tap **Install** to initiate installation of the app from the App Store.
2. Enter your Apple ID (if prompted) and password.

   App Store app downloads always require an Apple ID account. This will be the case for any user/device to which you distribute App Store apps.

   When the download is complete, the app becomes available on the iOS screen.



5.3.2 Distribute an Apple VPP App to an iOS Device

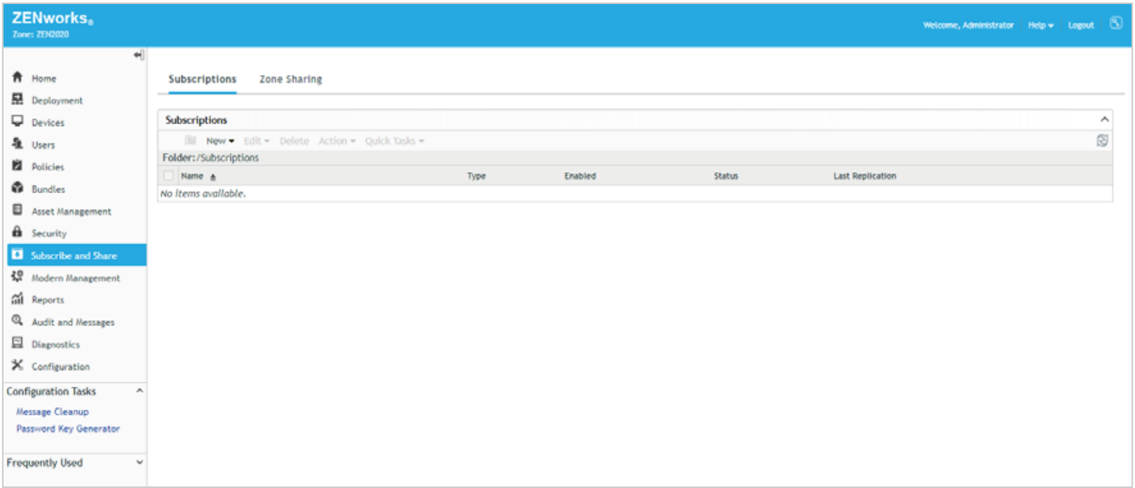
If you are enrolled in the Apple Volume Purchase Program (VPP), you can use ZENworks to distribute apps that you've purchased through that program. In addition, the Apple VPP dashboard in ZENworks Control Center lets you see the number of purchased licenses that have been consumed, the number that are still available, and the license consumption by user and device.

- "Connect to Apple VPP" on page 112
- "Create an Apple VPP Bundle" on page 114
- "Test the Bundle" on page 117

Connect to Apple VPP

Before you can provision an app you've purchased through your Apple VPP, you need to connect ZENworks to your subscription.

1 In ZENworks Control Center, click **Subscribe and Share** (in the left navigation pane).

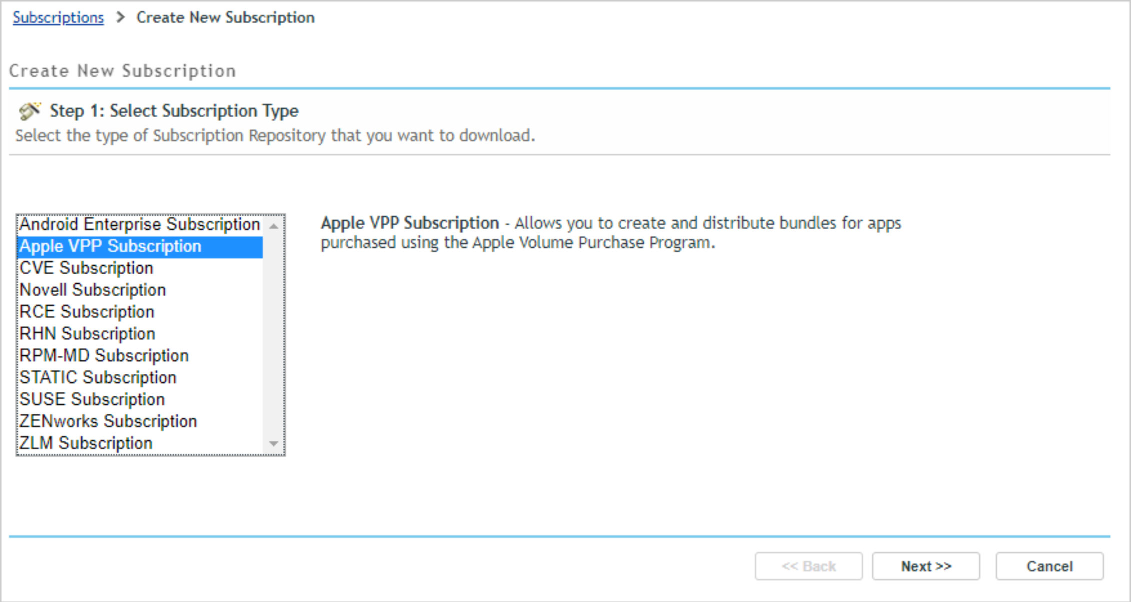


Folder: /Subscriptions

☐ Name	Type	Enabled	Status	Last Replication

No items available.

2 In the Subscriptions list, click **New** > **Subscription** to display the Create New Subscription wizard.



Subscriptions > Create New Subscription

Create New Subscription

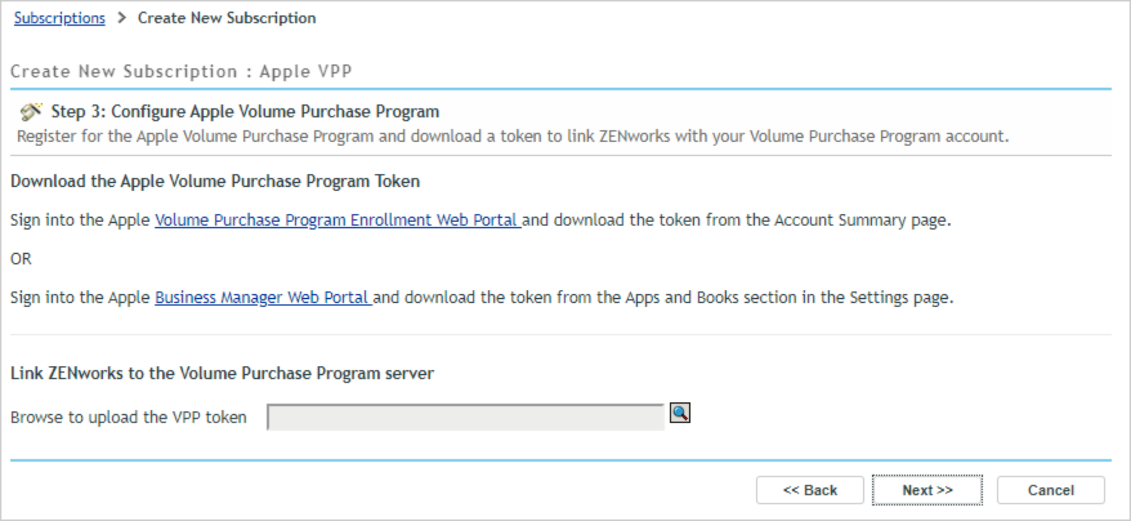
Step 1: Select Subscription Type

Select the type of Subscription Repository that you want to download.

Apple VPP Subscription - Allows you to create and distribute bundles for apps purchased using the Apple Volume Purchase Program.

3 On the Select Subscription Type page, select **Apple VPP Subscription**, then click **Next**.

4 On the Define Details page, enter *Apple VPP* for the subscription name, then click **Next** to display the Configure Apple Volume Purchase Program page.



Subscriptions > Create New Subscription

Create New Subscription : Apple VPP

Step 3: Configure Apple Volume Purchase Program

Register for the Apple Volume Purchase Program and download a token to link ZENworks with your Volume Purchase Program account.

Download the Apple Volume Purchase Program Token

Sign into the Apple Volume Purchase Program Enrollment Web Portal and download the token from the Account Summary page.

OR

Sign into the Apple Business Manager Web Portal and download the token from the Apps and Books section in the Settings page.

Link ZENworks to the Volume Purchase Program server

Browse to upload the VPP token

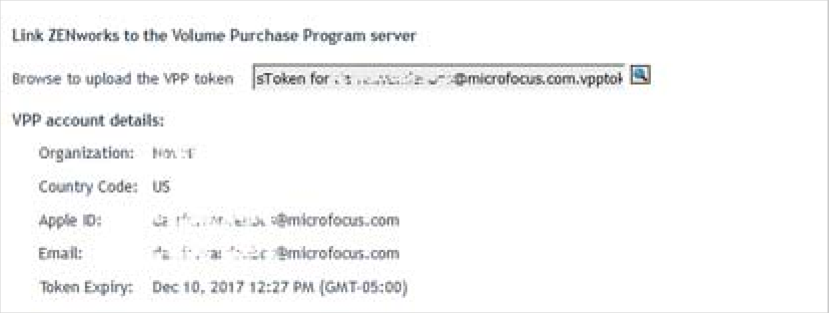
5 Download a VPP token from the Apple account you use:

5a Click the **Volume Purchase Program Enrollment Web Portal** link and sign in. Download the VPP token from the Account Summary page.

5b Click **Apple Business Manager Web Portal** and sign in. Download the specific location-based VPP token by navigating to the **Settings** > **Apps and Books** section.

6 In ZENworks Control Center subscription wizard, upload the VPP token to your zone.

After you upload the token, the VPP account details are displayed.



Link ZENworks to the Volume Purchase Program server

Browse to upload the VPP token: sToken for [redacted]@microfocus.com.vpptok

VPP account details:

Organization: [redacted]

Country Code: US

Apple ID: [redacted]@microfocus.com

Email: [redacted]@microfocus.com

Token Expiry: Dec 10, 2017 12:27 PM (GMT-05:00)

7 Click **Next** to display the Bundle Creation Settings page.

8 On the Bundle Creation Settings page, keep the default settings, then click **Next**.

9 On the Volume Purchase Program Subscription Schedule page, keep the default (No Schedule), then click **Finish**.

The Apple VPP subscription is created and added to the Subscriptions list. You can now use ZENworks to provision apps purchased through your Apple Volume Purchase Program.

Create an Apple VPP Bundle

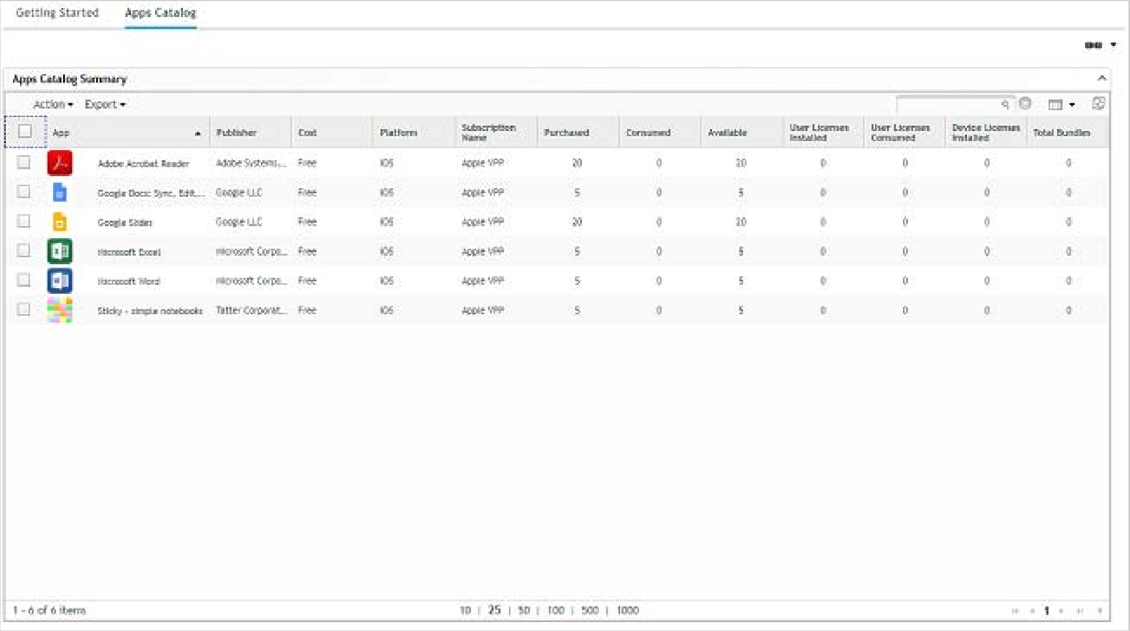
In ZENworks, apps are always distributed via bundles. This means you need to create a bundle for any Apple VPP app you want to provision to users. Fortunately, an Apple VPP bundle is the easiest bundle to create!

1 In ZENworks Control Center, click **Modern Management**.

2 Click **App Catalog** to display the list of your VPP apps.

The list displays all of the apps you’ve purchased through your Apple VPP subscription. For each app, you can see the number of purchased licenses as well as how many have been consumed and how many are still available.

If for some reason your apps are not listed, click the refresh icon 🔄 to update the list.



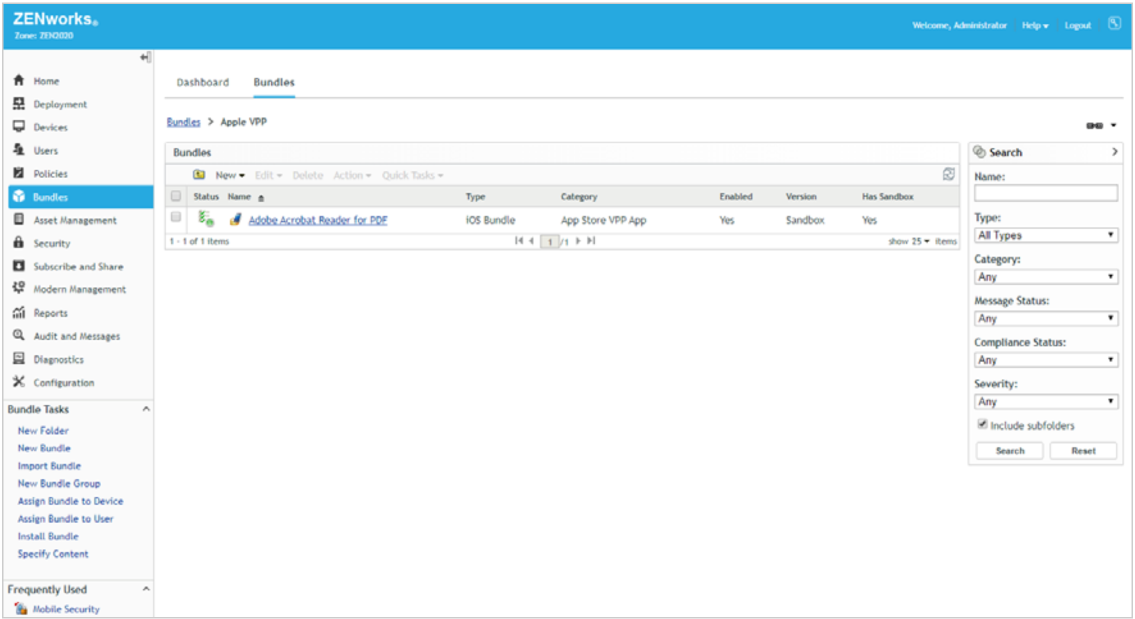
□	App	Publisher	Cost	Platform	Subscription Name	Purchased	Consumed	Available	User Licenses Installed	User Licenses Consumed	Device Licenses Installed	Total Bundles
□	Adobe Acrobat Reader	Adobe Systems,...	Free	iOS	Apple VPP	20	0	20	0	0	0	0
□	Google Docs: Sync, Edit,...	Google LLC	Free	iOS	Apple VPP	5	0	5	0	0	0	0
□	Google Slides	Google LLC	Free	iOS	Apple VPP	20	0	20	0	0	0	0
□	Microsoft Excel	Microsoft Corpo...	Free	iOS	Apple VPP	5	0	5	0	0	0	0
□	Microsoft Word	Microsoft Corpo...	Free	iOS	Apple VPP	5	0	5	0	0	0	0
□	Sticky - simple notebooks	Tatter Corporat...	Free	iOS	Apple VPP	5	0	5	0	0	0	0

1 - 6 of 6 items 10 | 25 | 50 | 100 | 500 | 1000

3 Select the check box in front of the app that you want to provision to your evaluation user, then click **Action** > **Create Bundles**, and then click **OK** to confirm creation of a bundle for the app.

The bundle is created and is added to the Apple VPP folder in the Bundles list.

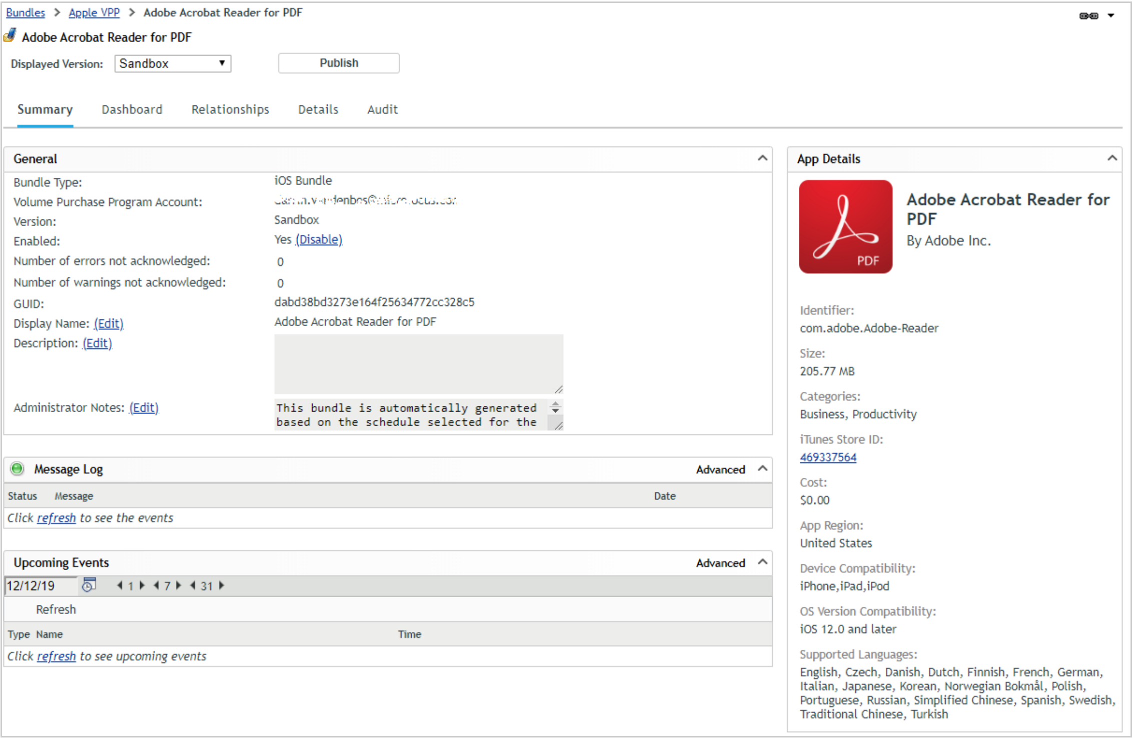
4 Click **Bundles** (in the left navigation pane) to display the Bundles list, then click **Apple VPP** to display the newly created Apple VPP bundle.



□	Status	Name	Type	Category	Enabled	Version	Has Sandbox
□		Adobe Acrobat Reader for PDF	iOS Bundle	App Store VPP App	Yes	Sandbox	Yes

1 - 1 of 1 items show 25 items

5 Click the bundle to display its details.



Bundles > Apple VPP > Adobe Acrobat Reader for PDF

Adobe Acrobat Reader for PDF

Displayed Version: Sandbox ▾ Publish

Summary Dashboard Relationships Details Audit

General

Bundle Type:	iOS Bundle
Volume Purchase Program Account:	[redacted]
Version:	Sandbox
Enabled:	Yes (Disable)
Number of errors not acknowledged:	0
Number of warnings not acknowledged:	0
GUID:	dabd38bd3273e164f25634772cc328c5
Display Name: (Edit)	Adobe Acrobat Reader for PDF
Description: (Edit)	
Administrator Notes: (Edit)	This bundle is automatically generated based on the schedule selected for the

Message Log Advanced

Status	Message	Date
Click refresh to see the events		

Upcoming Events Advanced

12/12/19 ◀ 1 ▶ ◀ 7 ▶ ◀ 31 ▶

Refresh

Type	Name	Time
Click refresh to see upcoming events		

App Details

Adobe Acrobat Reader for PDF
By Adobe Inc.

Identifier:
com.adobe.Adobe-Reader

Size:
205.77 MB

Categories:
Business, Productivity

iTunes Store ID:
469337564

Cost:
$0.00

App Region:
United States

Device Compatibility:
iPhone,iPad,iPod

OS Version Compatibility:
iOS 12.0 and later

Supported Languages:
English, Czech, Danish, Dutch, Finnish, French, German, Italian, Japanese, Korean, Norwegian Bokmål, Polish, Portuguese, Russian, Simplified Chinese, Spanish, Swedish, Traditional Chinese, Turkish

6 Assign the bundle to your managed iOS device:

- 6a Click **Relationships**.
- 6b In the Device Assignments list, click **Add**.
- 6c Use the Select Objects dialog to add the iOS device to the assignment list, then click **Next** to display the App Installation Schedule page.

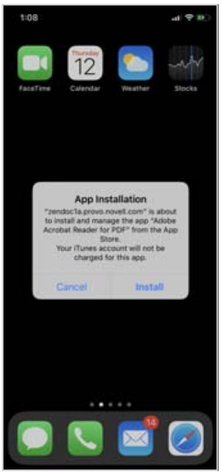
  The App Installation Schedule page lets you determine if you want to push the bundle to the device now (upon completion of the assignment to the device) or let the device find out about the bundle the next time it refreshes information from the ZENworks zone.
- 6d In the Schedule Type list, select **Now** so that the bundle is pushed to the device immediately, keep the Quick Task Notification Options default settings, then click **Next** to display the Bundle Conflict Resolution page.
- 6e Select Device Precedence, then click **Next** to display the Summary page.
- 6f Click **Finish** to create the assignment.

7 Click **Publish**, then follow the prompts to publish the bundle.

The bundle was created as a Sandbox version. A sandboxed app is not available to users or devices until it is published.

Test the Bundle

When the bundle is distributed to your iOS device, a notification is displayed on the device.

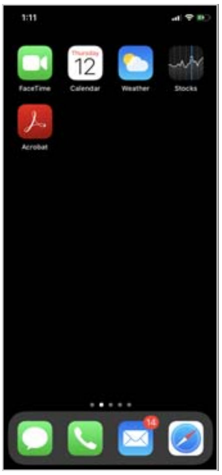


App Installation

"zendoc1a.provo.novell.com" is about to install and manage the app "Adobe Acrobat Reader for PDF" from the App Store.
Your iTunes account will not be charged for this app.

1 Tap **Install** to initiate installation of the app from the App Store.

When the download is complete, the app becomes available on the iOS screen.



5.3.3 Distribute an Android Enterprise App to an Android Device

To distribute apps from your managed Google Play Store account to your Android devices you need to approve the apps in Play Store and then create the Android bundle in ZENworks.

- "Approve Apps for Distribution" on page 118
- "Create an Android Bundle" on page 118
- "Test the App" on page 120

Approve Apps for Distribution

When you registered with Android Enterprise and created a managed Google Play Store, we didn’t have you approve any apps for distribution through ZENworks. We’ll have you do that now.

1. Log in to your managed Google Play Store account:

   `https://play.google.com/work`

2. Select an app, such as the Adobe Acrobat Reader app, and approve it. Repeat for as many apps as you’d like to distribute through ZENworks.

   After you approve an app, it is listed under **My Managed Apps** in your Play Store.

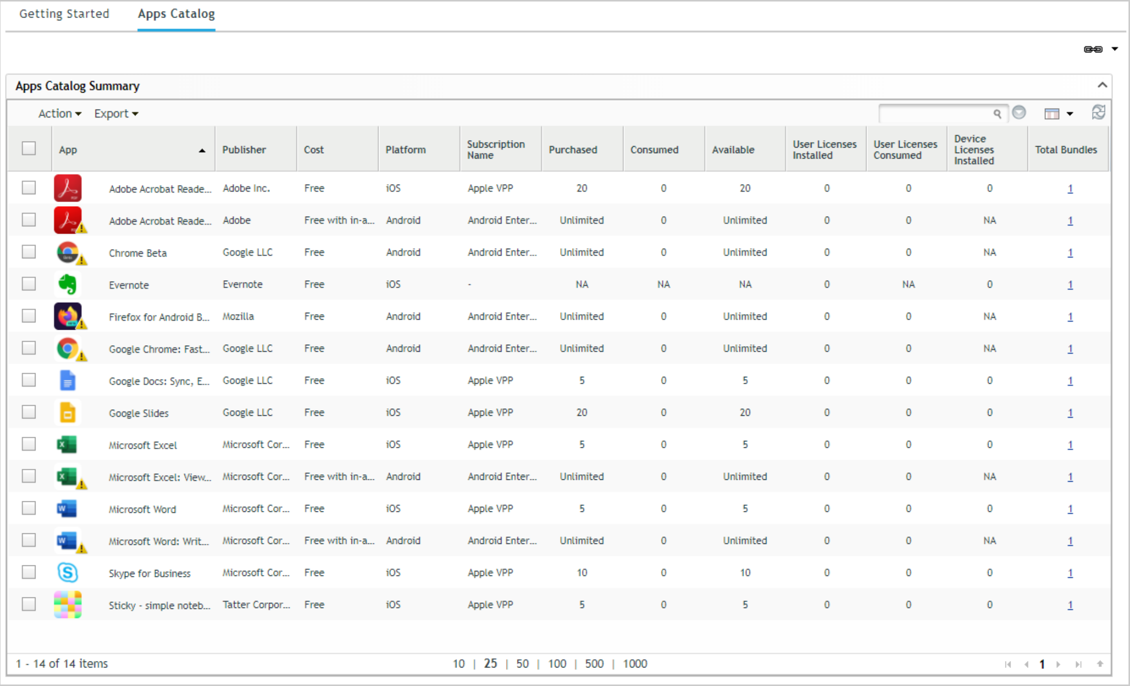
Create an Android Bundle

Bundles are created automatically for approved apps when the Android Enterprise subscription runs. We’ll have you run the subscription now to create bundles. After that, we’ll have you distribute a bundle to an Android device.

1. In ZENworks, click **Modern Management** > **Apps Catalog**.

2. Click the Update View icon to download the Android apps from your Play Store.

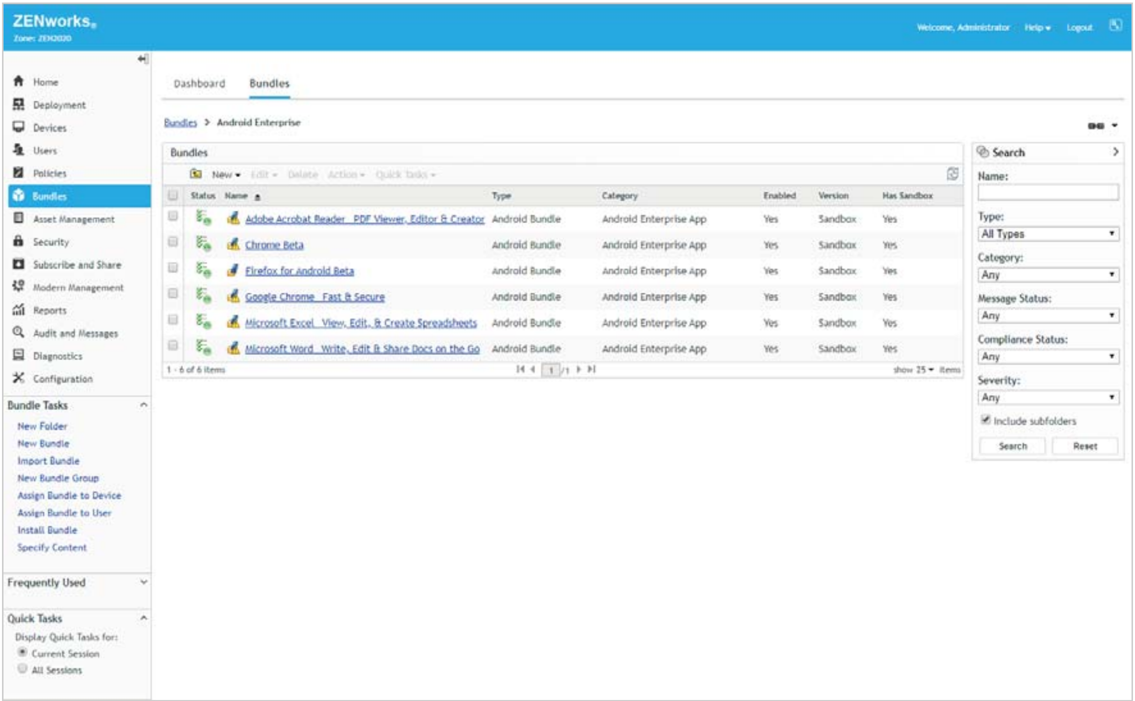
   A bundle is created for each Android app and is added to the Android Enterprise folder in the Bundles list.



□	App	Publisher	Cost	Platform	Subscription Name	Purchased	Consumed	Available	User Licenses Installed	User Licenses Consumed	Device Licenses Installed	Total Bundles
□	Adobe Acrobat Reade...	Adobe Inc.	Free	iOS	Apple VPP	20	0	20	0	0	0	1
□	Adobe Acrobat Reade...	Adobe	Free with in-a...	Android	Android Enter...	Unlimited	0	Unlimited	0	0	NA	1
□	Chrome Beta	Google LLC	Free	Android	Android Enter...	Unlimited	0	Unlimited	0	0	NA	1
□	Evernote	Evernote	Free	iOS	-	NA	NA	NA	0	NA	0	1
□	Firefox for Android B...	Mozilla	Free	Android	Android Enter...	Unlimited	0	Unlimited	0	0	NA	1
□	Google Chrome: Fast...	Google LLC	Free	Android	Android Enter...	Unlimited	0	Unlimited	0	0	NA	1
□	Google Docs: Sync, E...	Google LLC	Free	iOS	Apple VPP	5	0	5	0	0	0	1
□	Google Slides	Google LLC	Free	iOS	Apple VPP	20	0	20	0	0	0	1
□	Microsoft Excel	Microsoft Cor...	Free	iOS	Apple VPP	5	0	5	0	0	0	1
□	Microsoft Excel: View...	Microsoft Cor...	Free with in-a...	Android	Android Enter...	Unlimited	0	Unlimited	0	0	NA	1
□	Microsoft Word	Microsoft Cor...	Free	iOS	Apple VPP	5	0	5	0	0	0	1
□	Microsoft Word: Writ...	Microsoft Cor...	Free with in-a...	Android	Android Enter...	Unlimited	0	Unlimited	0	0	NA	1
□	Skype for Business	Microsoft Cor...	Free	iOS	Apple VPP	10	0	10	0	0	0	1
□	Sticky - simple noteb...	Tatter Corpor...	Free	iOS	Apple VPP	5	0	5	0	0	0	1

1 - 14 of 14 items

3 Click **Bundles** (in the left navigation pane) to display the Bundles list, then click **Android Enterprise** to display the newly created Android bundles.



Bundles > Android Enterprise

Bundles

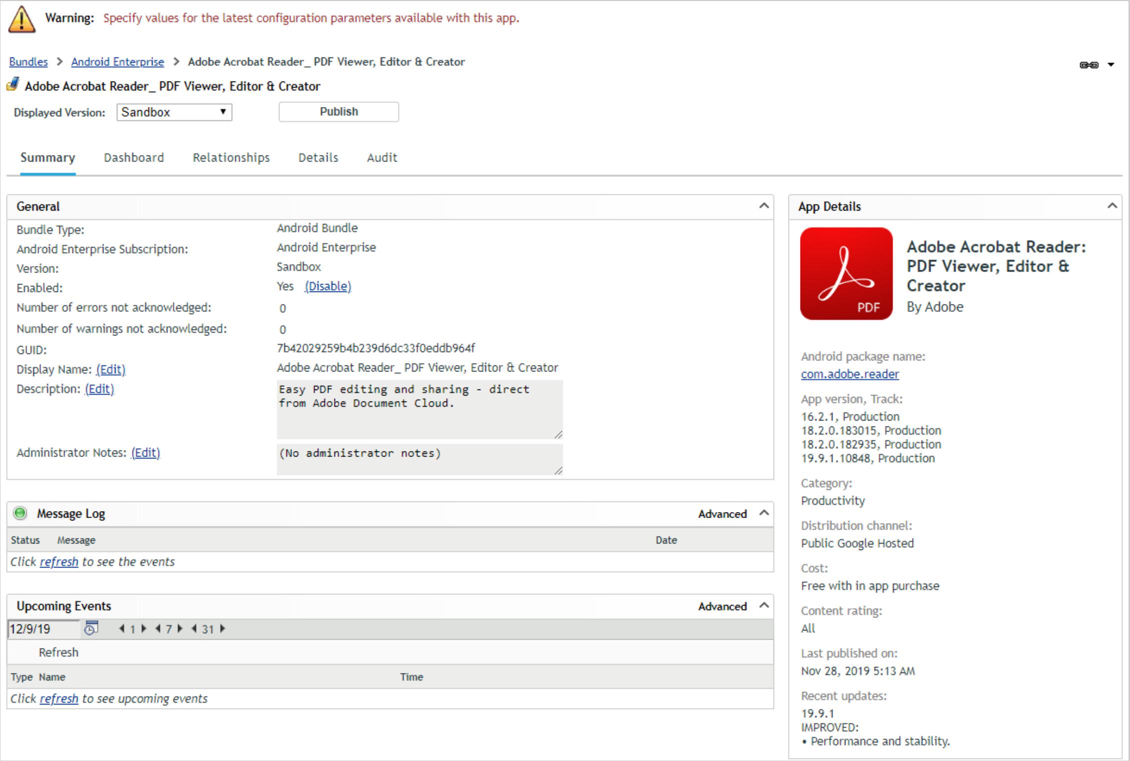
Status	Name	Type	Category	Enabled	Version	Has Sandbox
	Adobe Acrobat Reader_ PDF Viewer, Editor & Creator	Android Bundle	Android Enterprise App	Yes	Sandbox	Yes
	Chrome Beta	Android Bundle	Android Enterprise App	Yes	Sandbox	Yes
	Firefox for Android Beta	Android Bundle	Android Enterprise App	Yes	Sandbox	Yes
	Google Chrome_ Fast & Secure	Android Bundle	Android Enterprise App	Yes	Sandbox	Yes
	Microsoft Excel_ View, Edit, & Create Spreadsheets	Android Bundle	Android Enterprise App	Yes	Sandbox	Yes
	Microsoft Word_ Write, Edit & Share Docs on the Go	Android Bundle	Android Enterprise App	Yes	Sandbox	Yes

1 - 6 of 6 items 1 /1 show 25 items

Search
Name:
Type: All Types
Category: Any
Message Status: Any
Compliance Status: Any
Severity: Any
☑ Include subfolders

4 Click a bundle to display its details.

Note the warning that you need to specify values for the latest configuration parameters. This means...



Warning: Specify values for the latest configuration parameters available with this app.

Bundles > Android Enterprise > Adobe Acrobat Reader_ PDF Viewer, Editor & Creator

Adobe Acrobat Reader_ PDF Viewer, Editor & Creator

Displayed Version: Sandbox

General

Bundle Type:	Android Bundle
Android Enterprise Subscription:	Android Enterprise
Version:	Sandbox
Enabled:	Yes (Disable)
Number of errors not acknowledged:	0
Number of warnings not acknowledged:	0
GUID:	7b42029259b4b239d6dc33f0eddb964f
Display Name: (Edit)	Adobe Acrobat Reader_ PDF Viewer, Editor & Creator
Description: (Edit)	Easy PDF editing and sharing - direct from Adobe Document Cloud.
Administrator Notes: (Edit)	(No administrator notes)

Message Log

Status	Message	Date

Click refresh to see the events

Upcoming Events

12/9/19 1 7 31

Type	Name	Time

Click refresh to see upcoming events

App Details

Adobe Acrobat Reader: PDF Viewer, Editor & Creator
By Adobe

Android package name:
com.adobe.reader

App version, Track:
16.2.1, Production
18.2.0.183015, Production
18.2.0.182935, Production
19.9.1.10848, Production

Category:
Productivity

Distribution channel:
Public Google Hosted

Cost:
Free with in app purchase

Content rating:
All

Last published on:
Nov 28, 2019 5:13 AM

Recent updates:
19.9.1
IMPROVED:
• Performance and stability.

5 Assign the bundle to your managed Android device:

5a Click **Relationships**.

5b In the User Assignments list, click **Add**.

5c Use the Select Objects dialog to add the eval user (the one used to enroll the Android device into ZENworks), then click **Next** to display the App Installation Schedule page.

5d In the Schedule Type list, keep the **Next Refresh** option enabled but deselect the **Allow users to install from the managed Google Play Store** option, then click **Next**.

The A**llow users to install...** option adds the app to the user's managed Google Play Store so that the user can decide whether or not to install it. Deselecting the option causes the app to automatically be installed, which is what we want for this evaluation.

5e Click **Finish** to create the assignment.

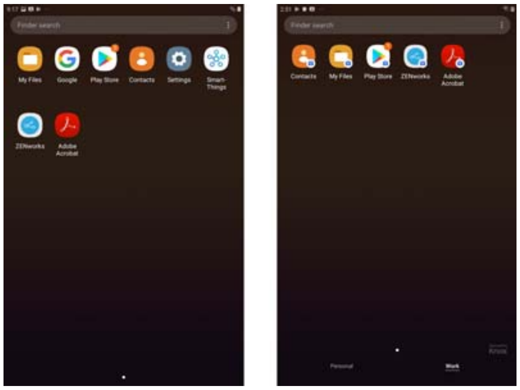
6 Click **Publish**, then follow the prompts to publish the bundle.

The bundle was originally created as a Sandbox version. A sandboxed app is not available to users or devices until it is published.

Test the App

1 On the device, open the ZENworks Agent and tap the Refresh icon 🔄.

The app installation begins. When installation is complete, the app is displayed on the App screen on a work-managed device (left) and on the App Work screen on a work profile device (right).



5.3.4 View the Bundle Status

ZENworks Control Center makes it easy for you to know the status of the bundle on your iOS and Android devices, including whether it has been assigned, distributed, and installed on a device.

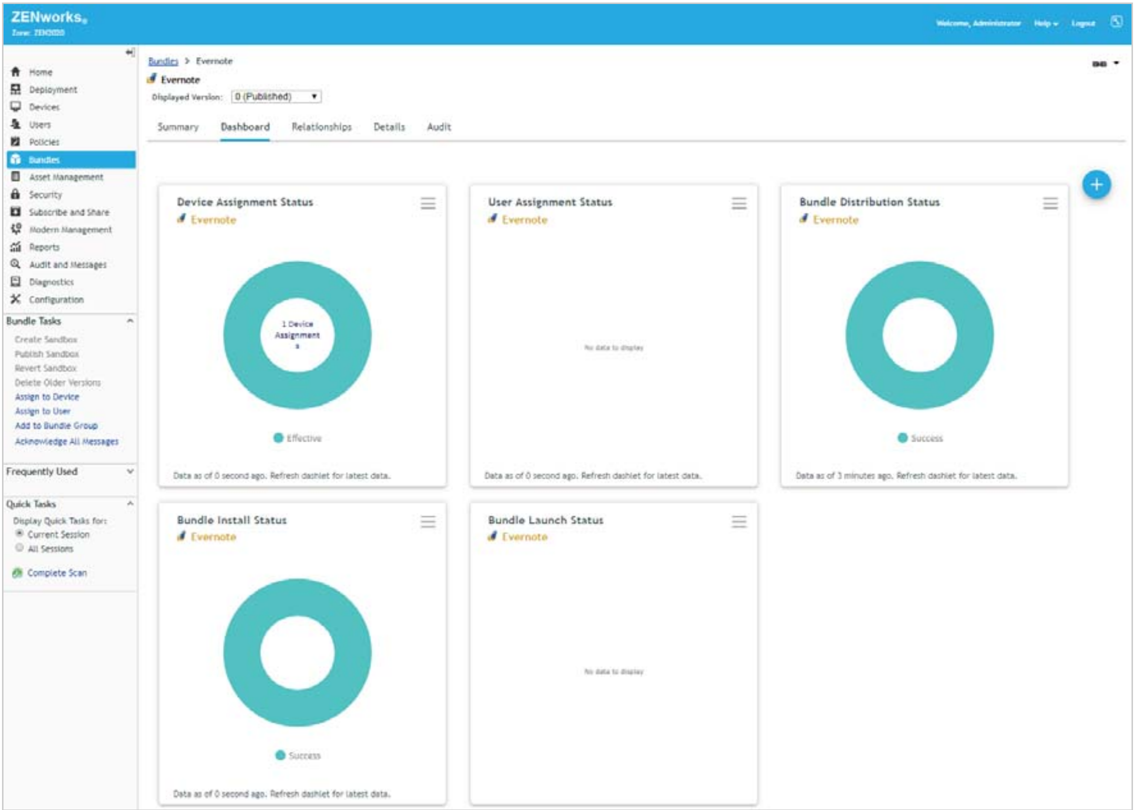
1 In ZENworks Control Center, click **Bundles** (in the left navigation pane).

2 In the Bundles list, click one of the iOS or Android bundles you distributed to display its properties.

We'll use the iOS Evernote bundle, but you can use any of the bundles you created.

3 Click the Dashboard tab.

The Dashboard displays a set of dashlets that shows the assignment, distribution, installation, and launch status of the bundle for every device to which the bundle is assigned. For this demo, we installed the bundle to one Windows device so the dashlets only reflect the bundle status for that one device.



Data as of 0 second ago. Refresh dashlet for latest data.

Data as of 0 second ago. Refresh dashlet for latest data.

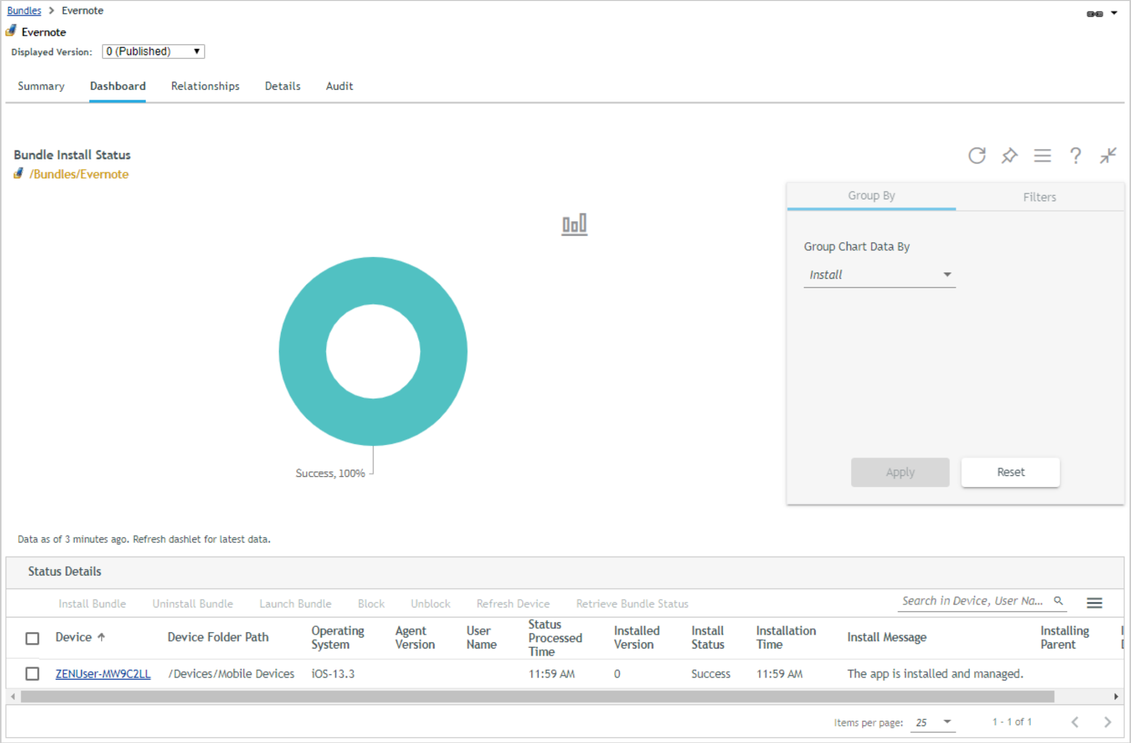
Data as of 3 minutes ago. Refresh dashlet for latest data.

Data as of 0 second ago. Refresh dashlet for latest data.

When you hover over the Device Assignment, Distribution, and Install status charts, each dashlet shows success for the device. The User Assignment Status dashlet has no data to display because the bundle is assigned to the device and not any users. And the Launch Status dashlet also has no data because there are no launch actions associated with the bundle.

4 Click the Bundle Installation Status dashlet.

The expanded dashlet gives installation information for each device on which the bundle is installed. Go ahead and play around with the filters and columns to see how you can customize the dashlet. You can save any changes by clicking the menu icon ≡ above the Filters box and then selecting **Save As**.



Data as of 3 minutes ago. Refresh dashlet for latest data.

Status Details

□	Device ↑	Device Folder Path	Operating System	Agent Version	User Name	Status Processed Time	Installed Version	Install Status	Installation Time	Install Message	Installing Parent
□	ZENUser-MW9C2LL	/Devices/Mobile Devices	iOS-13.3			11:59 AM	0	Success	11:59 AM	The app is installed and managed.	

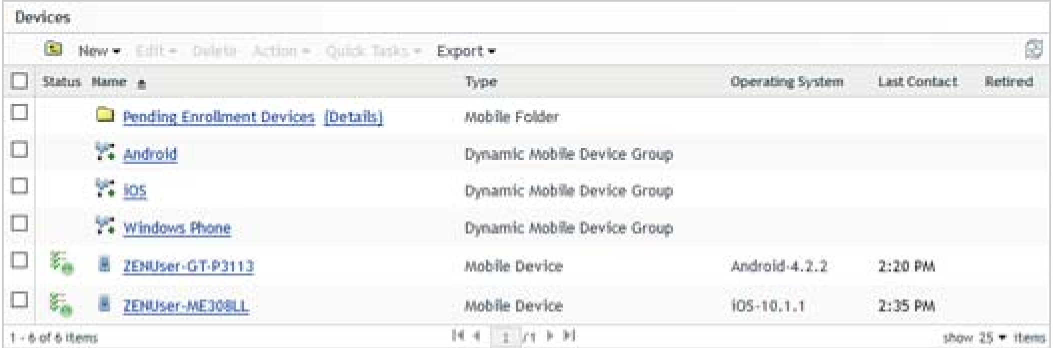
Items per page: 25 1 - 1 of 1

5 Become familiar with the other dashlets as desired.

5.4 Unenroll Your iOS and Android Devices

During unenrollment, you choose whether the device is deleted from the zone or retired (remains in zone but is inactive). You also choose whether to fully wipe the device or selectively wipe the device (corporate data only).

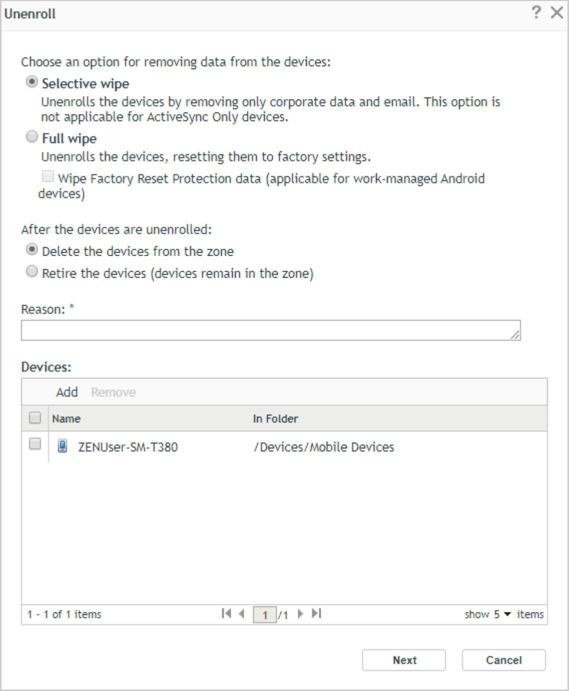
1 In ZENworks Control Center, click **Devices** > **Mobile Devices** to display your enrolled mobile devices.



□	Status	Name	Type	Operating System	Last Contact	Retired
□		Pending Enrollment Devices (Details)	Mobile Folder			
□		Android	Dynamic Mobile Device Group			
□		iOS	Dynamic Mobile Device Group			
□		Windows Phone	Dynamic Mobile Device Group			
□		ZENUser-GT-P3113	Mobile Device	Android-4.2.2	2:20 PM	
□		ZENUser-ME308LL	Mobile Device	iOS-10.1.1	2:35 PM	

1 - 6 of 6 items 1 /1 show 25 items

2 Select the check box in front of the mobile device you want to unenroll, click **Quick Tasks** > **Unenroll Device** to display the Unenroll dialog.



Unenroll

Choose an option for removing data from the devices:

● Selective wipe
Unenrolls the devices by removing only corporate data and email. This option is not applicable for ActiveSync Only devices.

○ Full wipe
Unenrolls the devices, resetting them to factory settings.
□ Wipe Factory Reset Protection data (applicable for work-managed Android devices)

After the devices are unenrolled:

● Delete the devices from the zone
○ Retire the devices (devices remain in the zone)

Reason: *

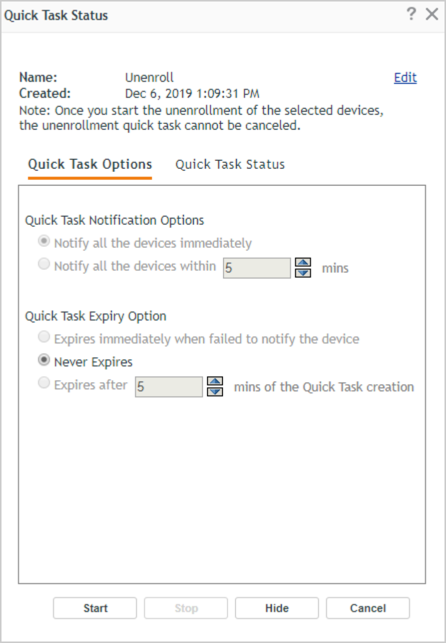
Devices:

Add Remove

□	Name	In Folder
□	ZENUser-SM-T380	/Devices/Mobile Devices

1 - 1 of 1 items 1 /1 show 5 items

3 Select the data removal option for the device (full wipe or selective wipe), select **Delete the devices from the zone**, enter a reason for unenrolling the device, then click **Next** to display the quick task options.



Quick Task Status

Name: Unenroll
Created: Dec 6, 2019 1:09:31 PM
Note: Once you start the unenrollment of the selected devices, the unenrollment quick task cannot be canceled.

Quick Task Notification Options
● Notify all the devices immediately
○ Notify all the devices within 5 mins

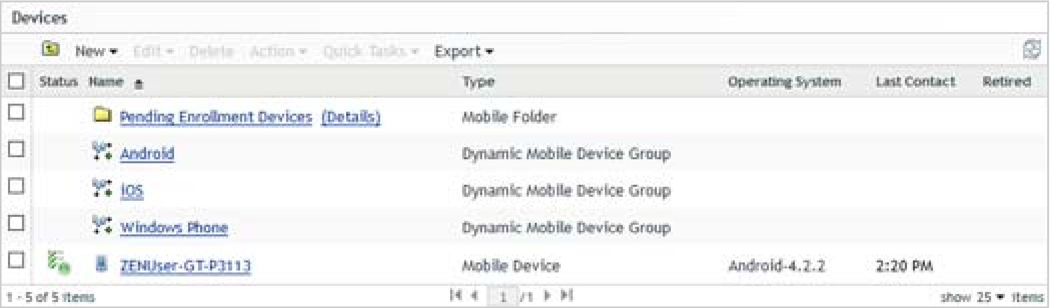
Quick Task Expiry Option
○ Expires immediately when failed to notify the device
● Never Expires
○ Expires after 5 mins of the Quick Task creation

4 Leave the quick task options set to the defaults and click **Start** to send the task to the device.

5 When the quick task status shows that the device has received the unenrollment task, click **Hide** to close the quick task.

6 Click 🔄 in the upper-right corner of the **Devices** list to refresh the list.

The unenrolled device is no longer listed.



□	Status	Name ▲	Type	Operating System	Last Contact	Retired
□		Pending Enrollment Devices (Details)	Mobile Folder			
□		Android	Dynamic Mobile Device Group			
□		iOS	Dynamic Mobile Device Group			
□		Windows Phone	Dynamic Mobile Device Group			
□		ZENUser-GT-P3113	Mobile Device	Android-4.2.2	2:20 PM	

7 If you unenrolled an iOS device, verify that the unenrollment tasks have initiated or completed:

Full Wipe: The device has been reset using the *Erase all Content and Settings* option.

Selective Wipe: The ZENworks Management Profile and all policy restrictions have been removed (**Settings** > **General** > **Profiles**). All App Store apps have been uninstalled, unless you selected the *Retain App on Unenrollment* option when distributing them. All Apple VPP apps have been uninstalled.

8 If you unenrolled an Android device, verify that the unenrollment tasks have initiated or completed:

Full Wipe: The device has been reset using the Erase all Content and Settings option.

Selective Wipe: The policy restrictions have been removed.

6 Explore Other Areas

ZENworks 2020 Configuration Management includes many additional features and capabilities you might want to explore.

6.1 Imaging

ZENworks Imaging lets you capture and deploy images to your devices regardless of the number, location, or types of devices. You can watch this YouTube video to learn more about the capabilities and use the Imaging documentation to set up and use it.

6.2 Remote Management

Using ZENworks Control Center, you can remotely manage devices. This includes being able to control a device, run executables on a device, transfer files to and from a device, diagnose problems with the device, and wake up powered-off devices. For more information and instructions, see the Remote Management documentation.

6.3 Configuration Policies

ZENworks lets you apply policies to manage the configuration settings of devices. This includes configuring local file/folder rights, printers, roaming profiles, dynamic users, power management schemes, and group policies. For more information and instructions, see the Configuration Policies documentation.

6.4 Asset Inventory

ZENworks Asset Inventory allows you to take an inventory of all the devices in your Management Zone, including data on hardware, software, and demographics. For more information and instructions, see the Asset Inventory documentation.

6.5 Locations

ZENworks lets you define locations (based on network environment attributes) and determine which ZENworks Primary Servers and Satellites a device uses when in a location as well as what bundles and policies are available while in the location. For more information and instructions, see the Location documentation.

6.6 Auditing

ZENworks Audit lets you track events that happen on devices as well as activities performed by ZENworks administrators in ZENworks Control Center. For more information and instructions, see the ZENworks Audit documentation.

6.7 Reports

ZENworks Reporting provides predefined reports for common use cases as well as the ability to create custom reports and charts for analyzing your device management processes and device status. For more information and instructions, see the ZENworks Reporting documentation.