

ZENworks 2020 Configuration Management

Evaluator's Guide



June 2020

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**.

How to Evaluate ZENworks

1. **Review the list of resources you'll need for this evaluation:**
 - ♦ [What You'll Need for the Evaluation \(page 1\)](#)
2. **Install and configure ZENworks:**
 - ♦ [Download ZENworks Software \(page 2\)](#)
 - ♦ [Install ZENworks \(page 3\)](#)
 - ♦ [Connect to a User Source \(page 5\)](#)
 - ♦ [Enable Communication with Mobile Devices \(page 6\)](#)
3. **Enroll devices with ZENworks:**
 - ♦ [Enroll Mobile Devices \(page 9\)](#)
 - ♦ [Enroll a Windows Device \(page 20\)](#)
4. **Use policies to secure your devices:**
 - ♦ [Secure Your Mobile Devices \(page 21\)](#)
 - ♦ [Secure Your Windows Device \(page 24\)](#)
5. **Distribute apps to your devices:**
 - ♦ [Distribute an App to Your Mobile Devices \(page 25\)](#)
 - ♦ [Distribute an Application to Your Windows Device \(page 31\)](#)
6. **Unenroll devices from ZENworks:**
 - ♦ [Unenroll Your iOS and Android Devices \(page 34\)](#)
 - ♦ [Unenroll Your Windows Devices \(page 35\)](#)

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.

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.

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.

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 the Firebase.

WINDOWS DEVICE MANAGEMENT

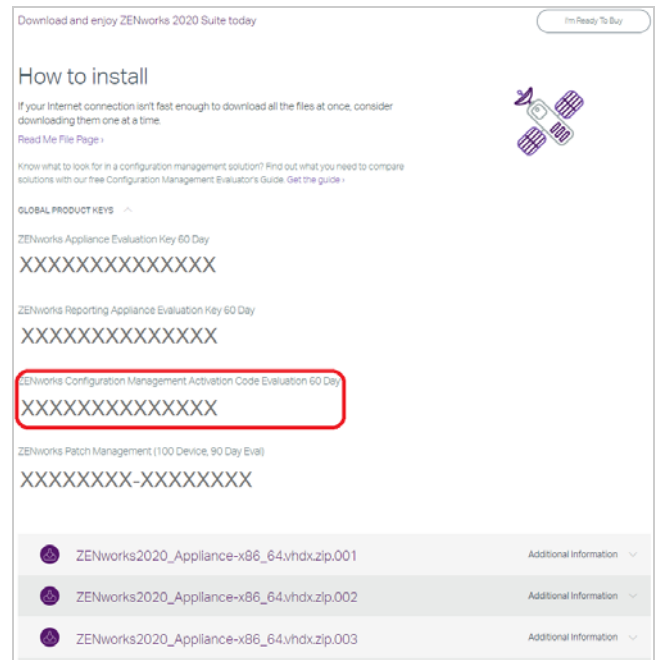
- ❑ **A Windows device.** This is a traditional Windows 7, 8.1, or 10 desktop or laptop. As with the mobile devices, you'll use it to test policies and apps.

Download ZENworks Software

If you don't already have the ZENworks software, you can get it through our evaluation site:

- 1 Go to the [ZENworks 2020 Suite Trial Registration page](https://www.microfocus.com/products/zenworks/trial/) (<https://www.microfocus.com/products/zenworks/trial/>).
- 2 Fill out the request form and submit it.
You'll be emailed a link to the software download page.

- 3 Use the emailed link to go to the download page.



- 4 Click **GLOBAL PRODUCT KEYS** to expand the section, then copy and save the ZENworks Configuration Management Activation Code (circled in the above screenshot).
- 5 Download the ZENworks software.

You'll quickly notice that there are a bunch of different download files. Which files you need depends 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.

Because the appliance is convenient and easy to use, we recommend using it if possible. The appliance is supported on the following hypervisors.

Hypervisor	File
VMware ESXi 6.x VMware Workstation 6.5 and newer (use in non-production environments only)	ZENworks2020_Appliance-x86_64.ova
Microsoft Hyper-V Server Windows 2012 2012 R2 2016 2019	ZENworks2020_Appliance-x86_64.vhd.zip ZENworks2020_Appliance-x86_64.vhdx.zip
XEN on SLES 12.x 15.x	ZENworks2020_Appliance-x86_64.xen.tar.gz
Citrix XenServer 7.x and Citrix Hypervisor 8.x	ZENworks2020_Appliance-x86_64.xva.tar.gz

Traditional Install: You can install the software on one of the servers in the following list.

Operating System	File
Windows 2012 Server x86_64	ZENworks_2020.iso
Windows 2012 Server R2 x86_64	
Windows 2016 Server x86_64	
Windows 2019 Server x86_64	
SLES 11 SP4 x86_64	ZENworks_2020.iso
SLES 12 SP3 and SP4 x86_64	
SLES 15 and SP1 x86_64	

Install ZENworks

Once you've downloaded the ZENworks software you want, refer to the appropriate section for installation instructions:

- [Deploying the ZENworks Virtual Appliance \(page 3\)](#)
- [Installing the ZENworks Software \(page 3\)](#)

DEPLOYING THE ZENWORKS VIRTUAL APPLIANCE

- 1 Make sure the host machine 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 Import the ZENworks Virtual Appliance into your hypervisor to create a new virtual machine.
- 3 Power on the new virtual machine.
- 4 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.
- Use the internal Certificate Authority.

If you need more details, refer to the [ZENworks Appliance Deployment and Administration Reference \(https://www.novell.com/documentation/zenworks-2020-update-1/zen_ca_appliance\)](https://www.novell.com/documentation/zenworks-2020-update-1/zen_ca_appliance).

INSTALLING THE ZENWORKS SOFTWARE

- 1 Make sure the target server meets the operating system requirements shown in the Download section, has at least 16 GB RAM and 40 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 Sybase Anywhere database.
- Use the internal Certificate Authority.

If you need more details, refer to the [ZENworks 2020 Server Installation Guide \(https://www.novell.com/documentation/zenworks-2020-update-1/zen_installation\)](https://www.novell.com/documentation/zenworks-2020-update-1/zen_installation).

Update Your ZENworks System

The software you installed is the **ZENworks 2020** software. The most recently released software is **ZENworks 2020 Update 1**. This evaluation is based on the functionality available in ZENworks 2020 Update 1, so you will want to apply the update to your system.

Updating your system is a simple process done through ZENworks System Update. This process is covered in the following sections:

- [Enabling Your ZENworks System to Receive Updates \(page 3\)](#)
- [Applying the System Update \(page 4\)](#)

ENABLING YOUR ZENWORKS SYSTEM TO RECEIVE UPDATES

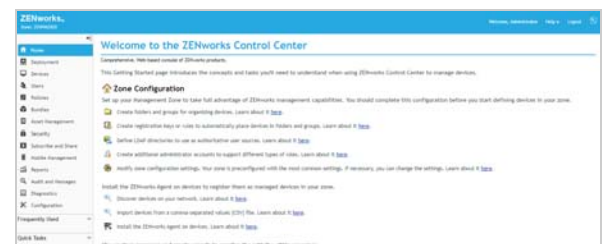
- 1 Log in to ZENworks Control Center:

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

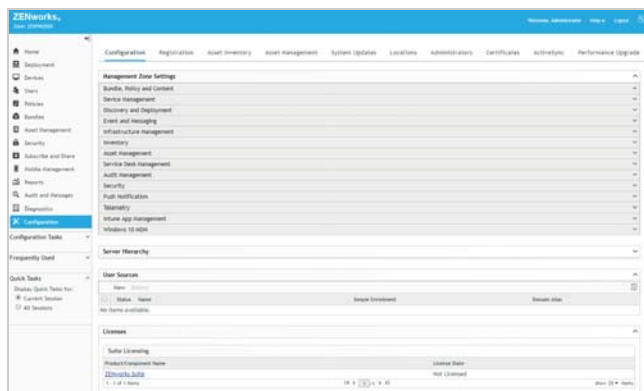
`https://ZENworks_Server_Address:port`

Replace `ZENworks_Server_Address` with the IP address or DNS name of the ZENworks Primary Server. You only need to specify the port if you are not using one of the default ports (80 or 443).

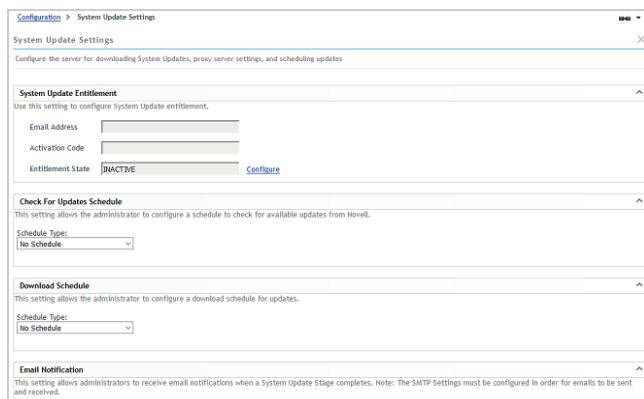
- 1b Specify *Administrator* as the username, specify the password you defined during installation, then click **Login** to display the Welcome page.



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



3 In the Management Zone Settings panel, click **Infrastructure Management** to expand the section, then click **System Update Settings** to display the System Update Settings page.

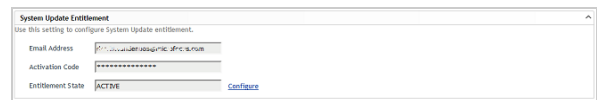


4 In the System Update Entitlement panel, click **Configure** to display the Configure System Update Entitlement dialog box.

5 Enter the email address used to request your evaluation, enter the activation code you copied from the Evaluation Download page, then click **Activate**.

If you don't have your activation code, go to the Evaluation Download page (using the link that was emailed to you) and copy the **ZENworks Configuration Management Activation Code Evaluation** key from the GLOBAL PRODUCT KEYS section.

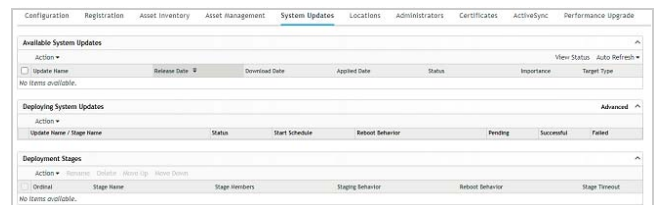
The entitlement is activated and the **Entitlement State** in the System Update Entitlement panel changes to **ACTIVE**.



6 Click **OK** to save the changes to the System Update settings.

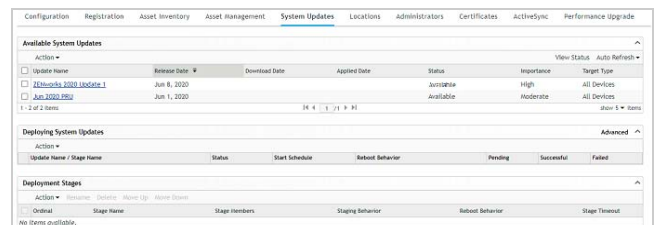
APPLYING THE SYSTEM UPDATE

1 In ZENworks Control Center, click **Configuration**, then click **System Updates** (one of the tabs at the top of the page) to display the System Updates page.



2 In the Available System Updates panel, click **Action > Check for Updates**.

Any updates that are available are displayed in the list. You should see *ZENworks 2020 Update 1* in the list as well as the most recent Product Recognition Update (PRU). *ZENworks 2020 Update 1* is what you apply to update your system. The PRU includes the latest hardware and software fingerprints used by ZENworks inventory to identify hardware and software on devices. We recommend that you apply these monthly as they come out.



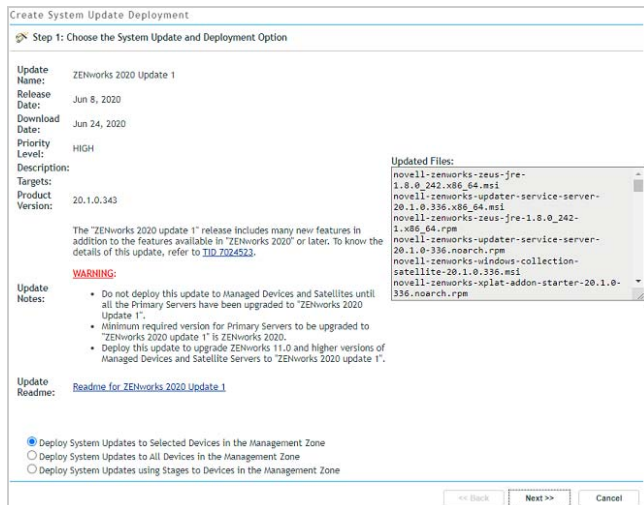
3 Select the check boxes next to *ZENworks 2020 Update 1* and the PRU, then click **Action > Download Update**.

The status for the two updates changes to *Downloading*. When the download is complete, the status changes to *Awaiting Authorization*.

4 Select the check box next to *ZENworks 2020 Update 1*, then click **Action > Authorize Update** to change the update status to *Ready to Deploy*.



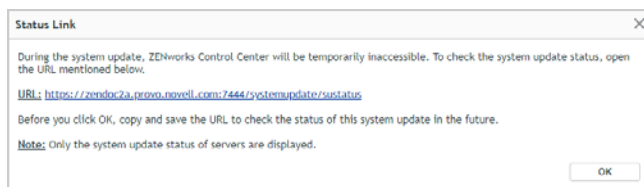
- 5 Select the check box next to **ZENworks 2020 Update 1**, then click **Action > Deploy Update to Devices** to launch the deployment wizard.



- 6 Select the **Deploy System Updates to All Devices in the Management Zone** option, then click **Next**.

Normally, you would want to deploy to selected devices rather than all, but since your zone only has the one Primary Server at this point you can use this option to avoid having to select your Primary Server as part of the wizard process.

- 7 Leave the **Prompt user for reboot when update finishes applying** option selected, then click **Next**.
- 8 In the Schedule Type list, select **Now**, then click **Next**.
- 9 Click **Finish** to start the update and display the following dialog box.



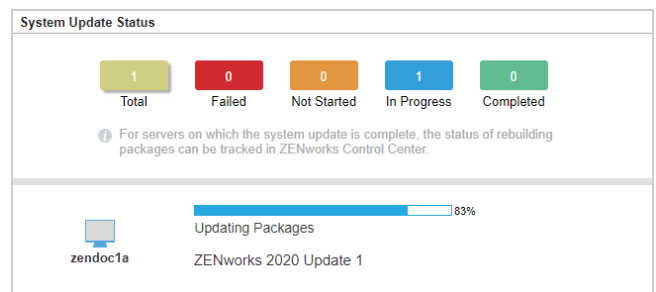
During update, the ZENworks Server is not accessible through ZENworks Control Center. Therefore, you need to use the System Update console to monitor system update progress.

- 10 Click the link to open the System Update console then click **OK** to start the update.

If the link cannot be clicked, copy the displayed URL to your web browser and replace **SERVER_NAME** with the IP address or DNS name of your ZENworks Primary Server. For example:

`https://zenserver.microfocus.com:7444/systemupdate/sustatus`


The System Update console is displayed, showing the current status of the update.



- 11 When the update has successfully completed, log in to ZENworks Control Center.

- 12 Go to the System Update page (**Configuration > System Updates**).

In the Deploying System Updates panel, notice that the update is still listed as *Pending*.



Update Name / Stage Name	Status	Start Schedule	Reboot Behavior	Pending	Successful	Failed
ZENworks 2020 Update 1	Pending	Per Device	Per Device	1	0	0

Although the ZENworks Server software was updated, there are still some update tasks, such as rebuilding the deployment packages used when distributing the ZENworks Agent to devices, that need to be completed.

When all update tasks are complete, the update status is changed to *Successful*.

- 13 (Optional) To apply the PRU at this time:

- 13a Select the check box next to the PRU, then select **Action > Authorize Update**.

- 13b Select the check box next to the PRU, then select **Action > Deploy PRU Now**.

Connect to a User Source

ZENworks ties into your LDAP user directory in order to provide user-based management of devices.

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

With 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.

- [Selecting an Evaluation User \(page 5\)](#)
- [Connecting to an LDAP Directory \(page 6\)](#)

SELECTING 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*.

CONNECTING TO AN LDAP DIRECTORY

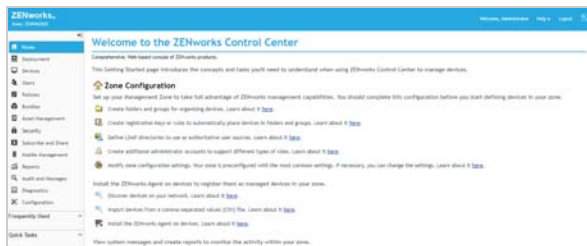
1 Log in to ZENworks Control Center:

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

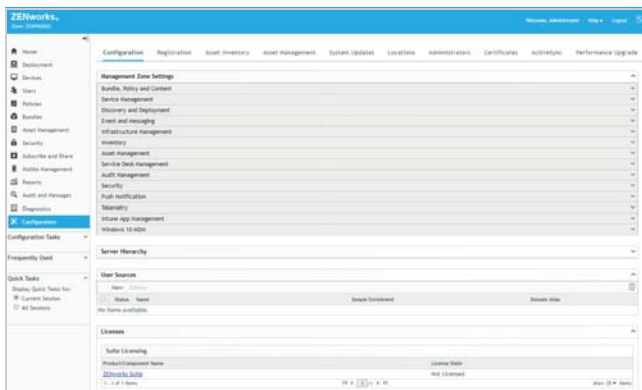
`https://ZENworks_Server_Address:port`

Replace *ZENworks_Server_Address* with the IP address or DNS name of the ZENworks Primary Server. You only need to specify the port if you are not using one of the default ports (80 or 443).

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



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



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

- 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 listening on a non-default port (636 or 389), select that 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.

Enable Communication with Mobile Devices

You need to complete several system configuration tasks to enable ZENworks to communicate with mobile devices. This includes defining your ZENworks Primary Server as the Mobile Device Management (MDM) Server that you want communicating with mobile devices, and then configuring ZENworks to communicate with the devices via the Apple and Google push notification services.

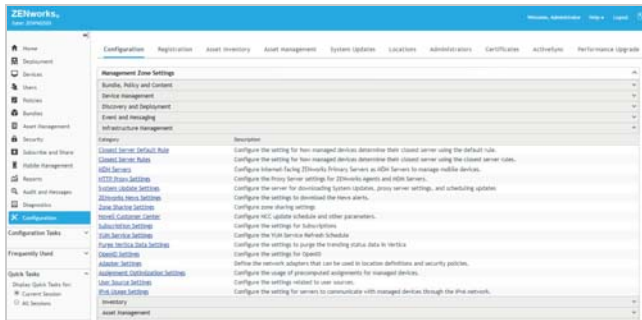
- ♦ [Designating an MDM Server \(page 7\)](#)
- ♦ [Enabling Push Notifications for iOS Devices \(page 7\)](#)
- ♦ [Enabling Push Notifications for Android Devices \(page 8\)](#)

DESIGNATING AN MDM SERVER

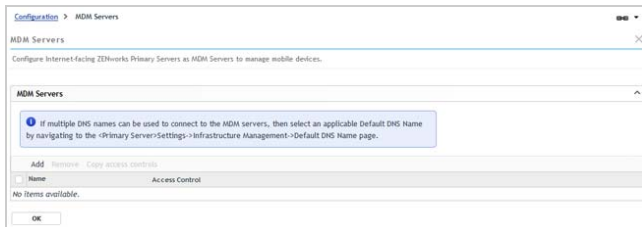
A ZENworks Management Zone must have at least one ZENworks Primary Server that is designated as a Mobile Device Management (MDM) Server. MDM Servers are the only servers in your zone that communicate with mobile devices.

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



- 2 In the Management Zone Settings panel, click **Infrastructure Management**, then click **MDM Servers** to display the MDM Servers page.



- 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.

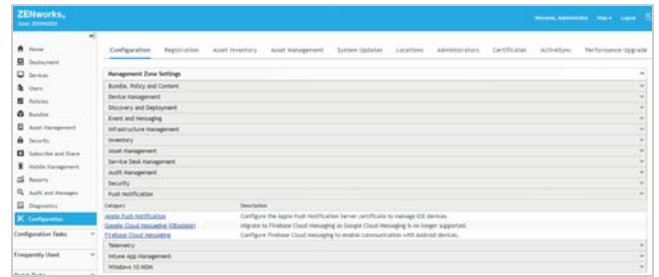
ENABLING PUSH NOTIFICATIONS FOR IOS DEVICES

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.

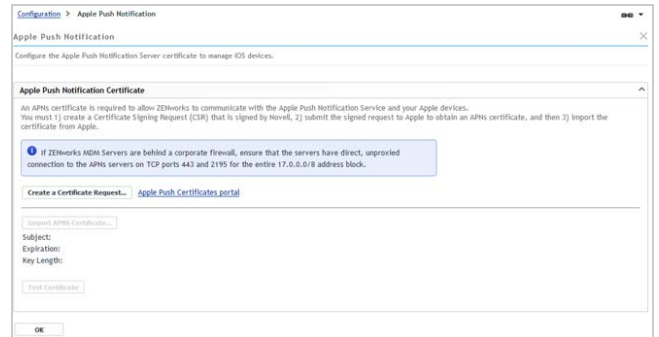
In order to use the Apple Push Notification service, an Apple Push Notification service certificate is required. The APNs certificate allows the ZENworks MDM Server and iOS devices to authenticate securely to the service.

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, click **Configuration** (in the left navigation pane).



- 2 In the Management Zone Settings panel, click **Push Notification**, then click **Apple Push Notification Service** to display the Apple Push Notification service settings.



- 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**.

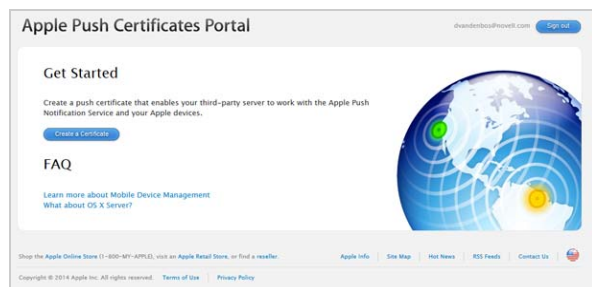
- 3e** After the Certificate Signing Request file is signed by Micro Focus, save the signed CSR file to a location of your choice.

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.



- 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 Now**.

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

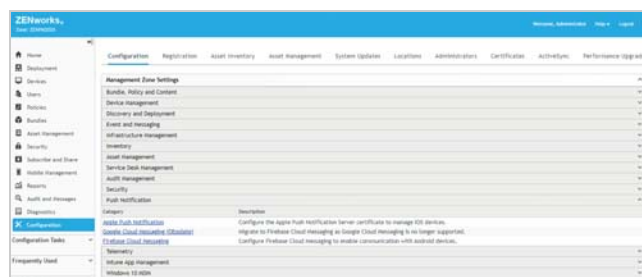
ENABLING PUSH NOTIFICATIONS FOR ANDROID DEVICES

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.

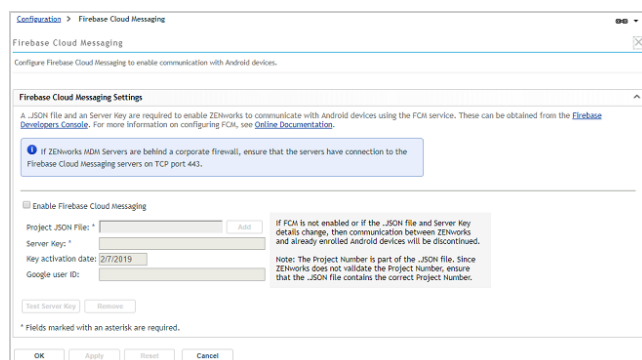
The MDM Server communicates with the Firebase Cloud Messaging service, which then pushes the notification to the device. After receiving the push notification, the device contacts the MDM Server directly to provide the requested information or receive the changes.

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, click **Configuration** (in the left navigation pane).



- 2** In the Management Zone Settings panel, click **Push Notification**, then click **Firebase Cloud Messaging** to display the Firebase Cloud Messaging settings.



- 3** Create a Firebase Project:

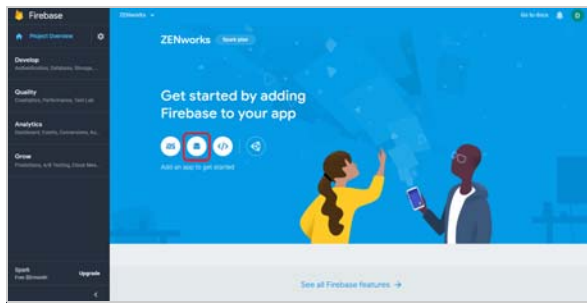
- 3a** Click **Firebase Developers Console**.

- 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 **Add Project**, supply a name for your project (such as ZENworks) and follow the remaining prompts to create the project.

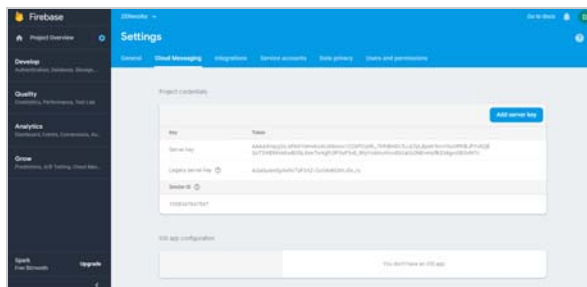
- 3d After the project is created, the Firebase Console is displayed.



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



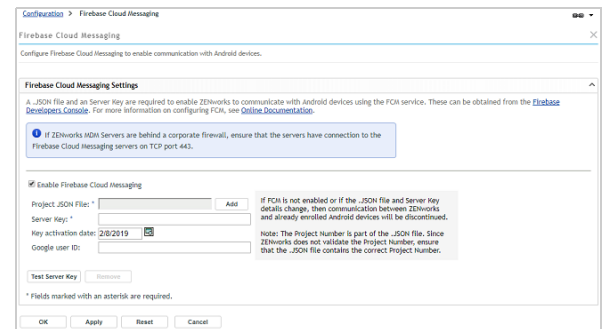
- 3f In the *Android package name* field, enter `com.novell.zapp`, then click **Register app**.
- 3g Click **Download google-services.json** to download the .JSON file.
- 3h Complete the wizard and return to the Firebase console.
- 3i In the console's upper-left corner, click the  icon, then click **Project Settings**.
- 3j Click **Cloud Messaging**.



- 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 Messaging settings), click the **Enable Firebase Cloud Messaging** check box to turn on the option.



- 4b Configure the following:

Project JSON File: Add the 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.

Enroll Mobile Devices

Whew! You've made it through the ZENworks installation and configuration tasks! Now it's time to enroll an iOS and Android device in your system so that you can get on with the fun stuff like distributing apps to the devices and securing them.

- ♦ [Creating a Mobile Enrollment Policy \(page 9\)](#)
- ♦ [Enrolling an iOS Device \(page 11\)](#)
- ♦ [Enrolling an Apple DEP iOS Device \(page 12\)](#)
- ♦ [Enrolling an Android Device \(page 16\)](#)

CREATING A MOBILE ENROLLMENT POLICY

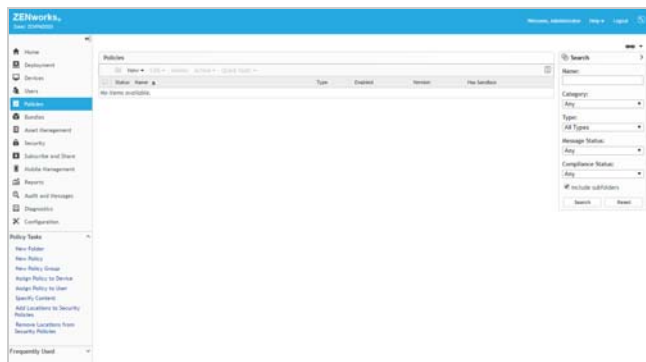
In order for mobile devices to be enrolled in your ZENworks Management Zone, you must create a Mobile Enrollment policy and assign it to any users who will enroll devices.

The 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

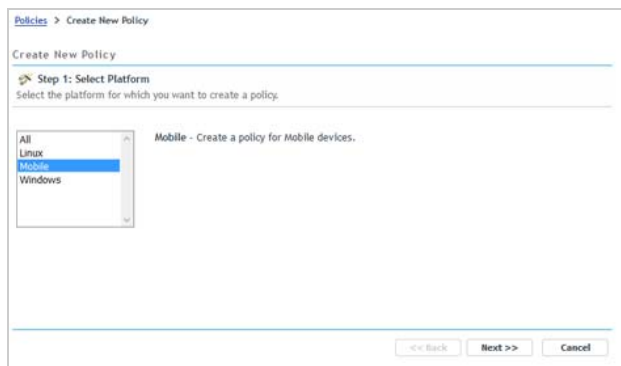
device, whether the device is designated as corporate owned or personal, and what happens to the device when it is unenrolled.

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, click **Policies** (in the left navigation pane).



- 2 In the Policies panel, 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 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.



- 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.

ENROLLING AN IOS DEVICE

You can enroll any device running iOS version 10 or newer. We used an iPhone running iOS version 13.1.2. Obviously, 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

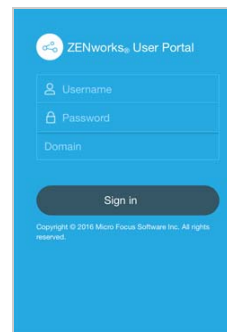
(available for Apple devices running iOS version 11 or newer), use the instructions in [“Enrolling an Apple DEP iOS Device” on page 12](#) instead.

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

`ZENworks_server_address/zenworks-eup`

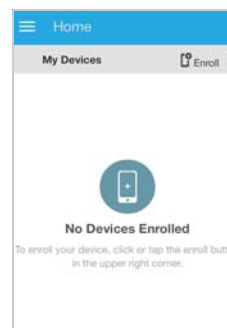
Replace `ZENworks_server_address` with the DNS name or IP address of your ZENworks Primary Server.

The login screen for the ZENworks User Portal is displayed.



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

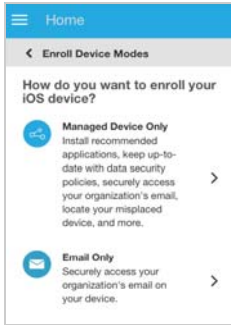
The Domain name field is not needed because the system is configured for simple enrollment, which allows users to log in with only their username rather than their full domain name.



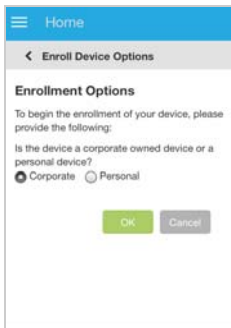
- 3 Tap **Enroll** in the upper-right corner to display the **Enroll Device Modes** screen.

The available enrollment options are determined by the Mobile Enrollment policy. If you configured the policy as recommended in [“Creating a Mobile](#)

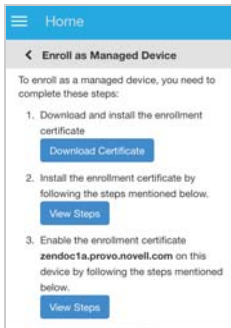
[Enrollment Policy](#)” on page 9, both options are available as shown below. Otherwise, only one of the two options is available.



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



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

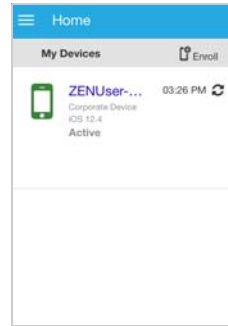


- 6 Complete the steps to enroll the device.

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.

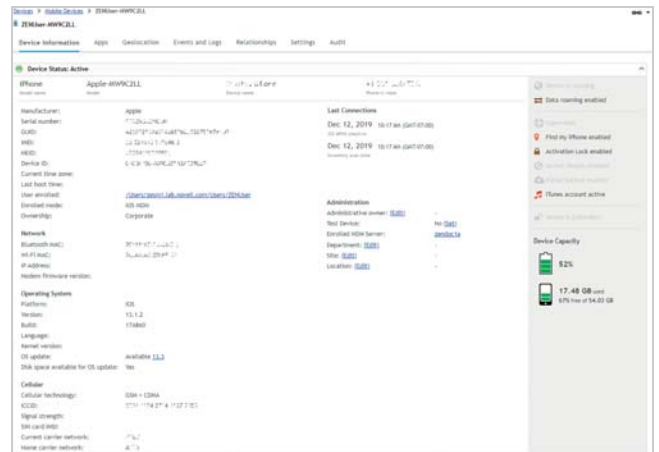


- 8 In ZENworks Control Center, go to the **Devices > Mobile Devices** list to confirm that the device is enrolled in the zone.



- 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.



ENROLLING 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.

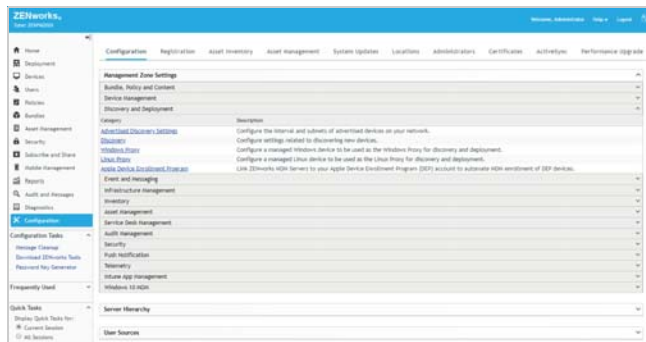
Using ZENworks Control Center, you configure setup options such as whether or not a device is supervised and what features (Location Services, Passcode, and so forth) are required to be configured at initial setup. Then, during

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.

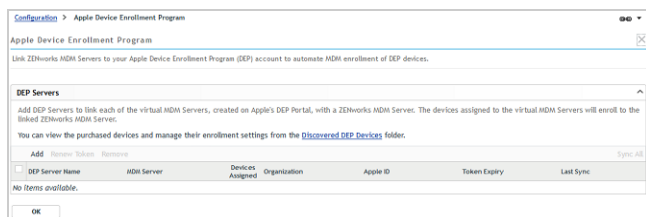
Linking Your MDM Server to the Apple Device Enrollment Program

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, click **Configuration** (in the left navigation pane).




- 2 In the Management Zone Settings panel, click **Discovery and Deployment**, then click **Apple Device Enrollment Program** to display the following page.



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.



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

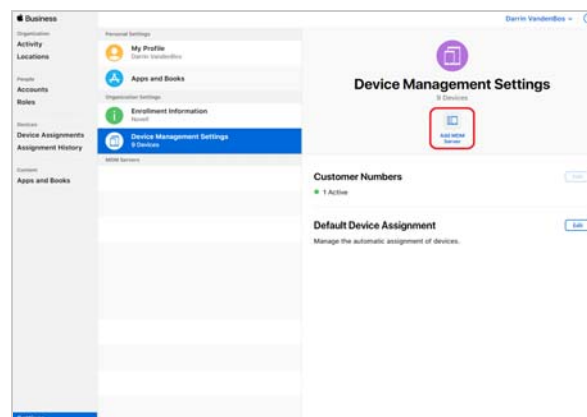


- 5 Click **Download**, then save the server's public key to your local drive.

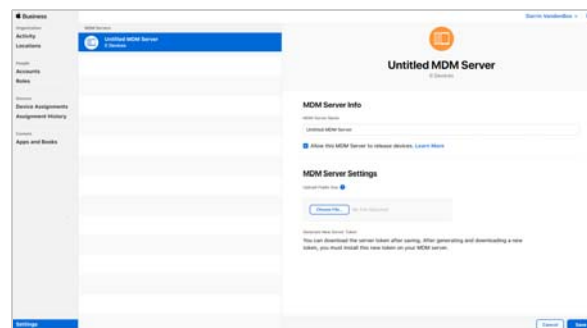
The key file is saved as `servername.der`. You'll need the file later when you add the MDM Server to your Apple Device Enrollment Program.

- 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**.



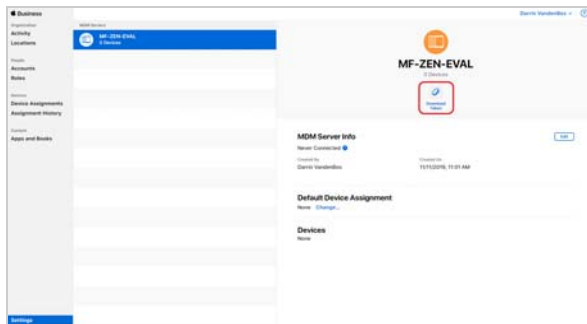
- 7b Click **Add MDM Server** to display the following settings.



- 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.

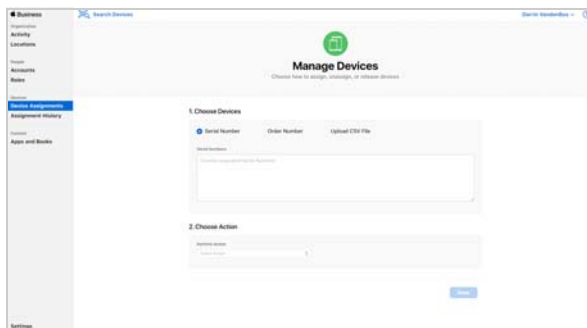


7f Click **Download Token** to download the MDM Server token to your local drive.

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.

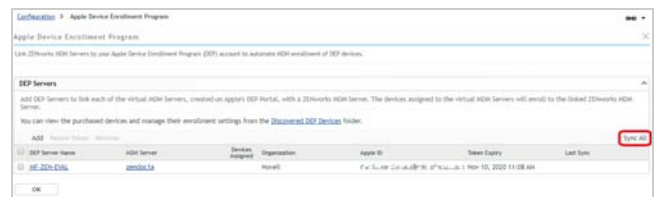


8 In ZENworks Control Center, you should still be in the Add DEP Server dialog box. Click **Upload** to upload the MDM Server token (the .p7m file generated from the Apple portal).

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



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



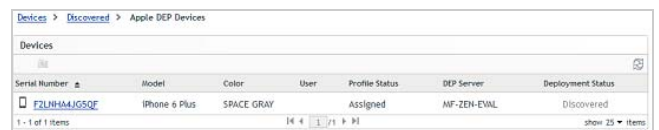
10 In the DEP Servers list, click **Sync All** (located on the right side of the list's menu) to sync the DEP devices into your ZENworks Management Zone.

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



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*.



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	Inventoried	Managed
Discovered		
Type		
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

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 (SGL):

Specify the support email address displayed during enrollment (SGL):

Specify the department name displayed during enrollment (SGL):

Specify the default language to be selected during enrollment (iOS only): en

Specify the default region to be selected during enrollment (iOS 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
☐ Screenreader (iOS only)
☐ Where is this Apple TV? (iOS only)

☐ Location Services
☐ Terms and Conditions
☐ Siri
☐ Keyboard
☐ Message and FaceTime
☐ Touch to setup (iOS only)

☐ Restore apps and data
☐ Touch ID
☐ Diagnostics
☐ Onboarding
☐ Screen Time
☐ Home Screen Sync (iOS only)

☐ Move from Android
☐ Apple Pay
☐ Display Time
☐ Watch Migration
☐ Software Update
☐ TV Provider sign in (iOS only)

OK Apply Reset Cancel

- 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.



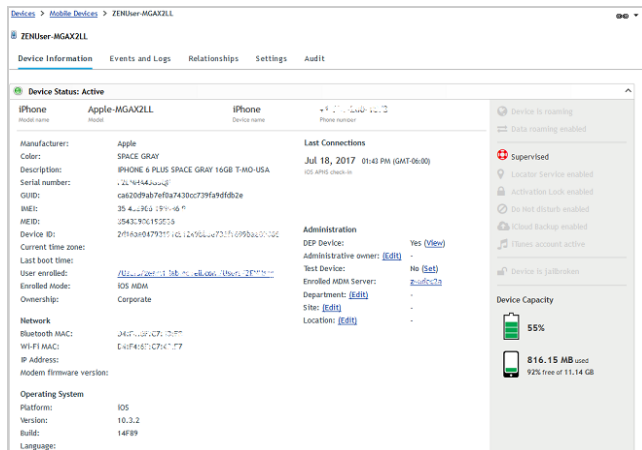
- 5 In ZENworks Control Center, go to the device in the Discovered devices list (**Devices > Discovered > Apple DEP Devices**).

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
F2LNH44JG5QE	iPhone6,1	SPACE GRAY	ZENUser	Assigned	MF-ZEN-EVAL	Managed
1 - 1 of 1 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.



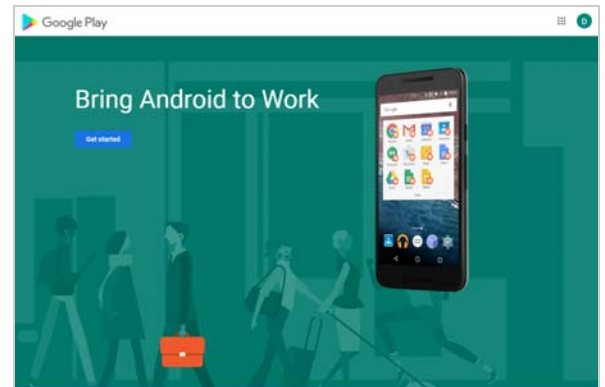
ENROLLING AN ANDROID DEVICE

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.

Registering 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 **Subscribe 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.



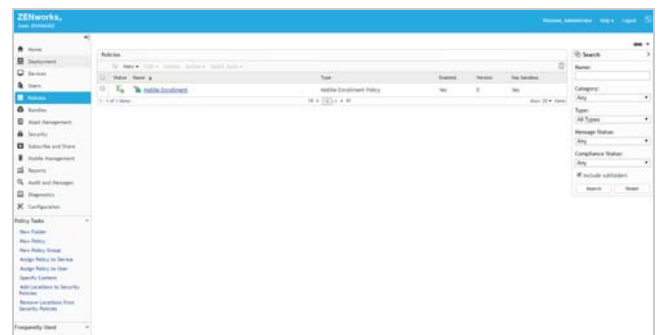
- 5d Click **Get started**, then follow the prompts to register your organization.
 - 5e After the account registration is complete, you are returned to ZENworks Control Center. Click **Next**.
- 6 On the Select User Context page, add the context in which your evaluation user resides, then click **Next**. 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.

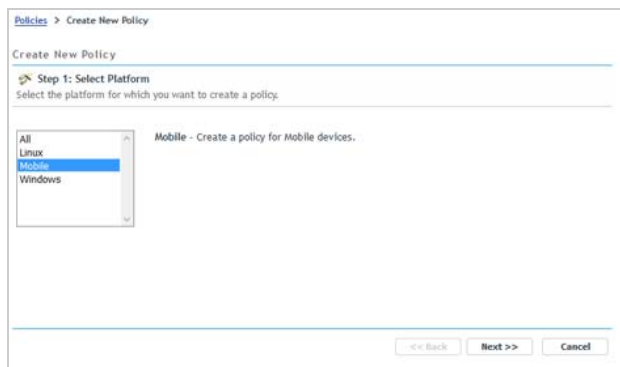
Creating an Android Enterprise Enrollment Policy

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).



- 2 In the Policies panel, 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 **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.



- 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.

Enrolling 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.



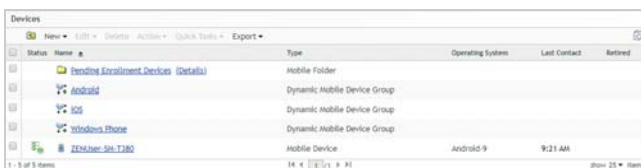
- 4 Select **Personal**, tap **OK**, then follow the prompts shown in the following screens to create the work profile and enroll the device.



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

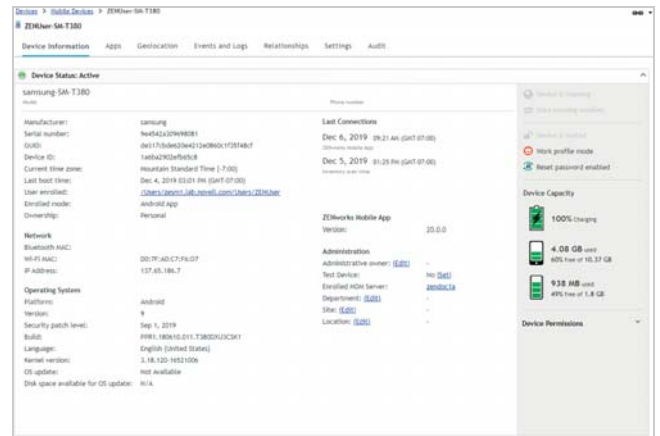


- 5 In ZENworks Control Center, go to the **Devices > Mobile Devices** list to confirm that the device is enrolled in the zone.



- 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.



Enrolling 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 [“Enrolling an Android Device in Work Profile Mode” on page 17.](#)

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.

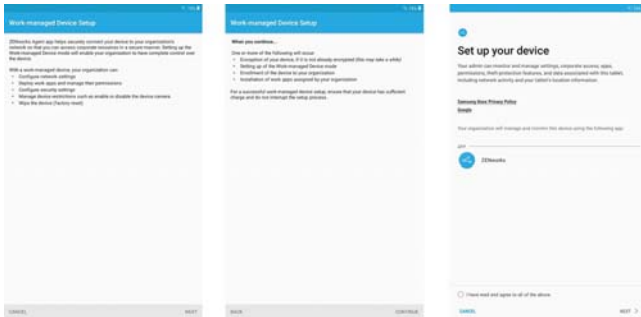
- 2 Start the device and complete the initial screens (language, Wi-Fi setup, Terms and Conditions) until you reach the following screen:



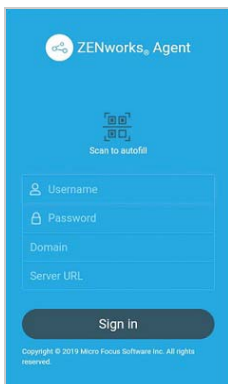
- 3 Enter `afw#zenworks`, then tap **Next**.



- 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.



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



- 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.



- 7 Tap **OK** to enroll the device as a corporate device.

When enrollment is complete, the Android device is listed in the mobile app.

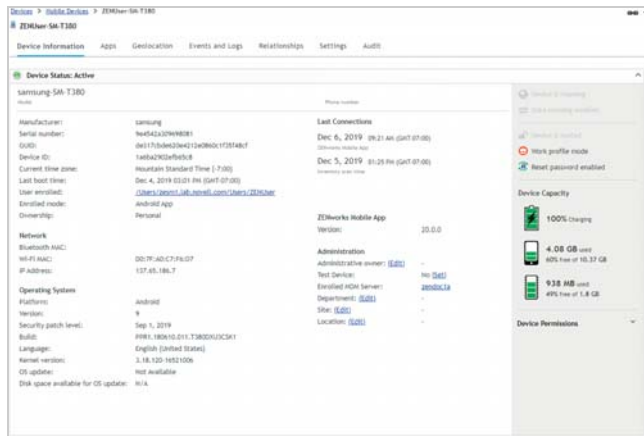


- 8 If you are notified that a password change is needed, tap the notification and enter a new password.
- 9 In ZENworks Control Center, go to the **Devices** > **Mobile Devices** list to confirm that the device is enrolled in the zone.

Status	Name	Type	Operating System	Last Contact	Enrolled
	Pending Enrollment Devices (Details)	Mobile Folder			
	Android	Dynamic Mobile Device Group			
	iOS	Dynamic Mobile Device Group			
	Windows Phone	Dynamic Mobile Device Group			
	ZENworks SH-T380	Mobile Device	Android 9	9/21 AM	

- 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.




- 2 In the list, click the package you want to download to the device, then follow the prompts to download it.

You want the Microsoft Windows package that is the Standalone install type, either 32 bit or 64 bit depending on your Windows device.


This will be either the *Default Agent (x86_Complete) Microsoft Windows x86 Architecture (32 bit) Standalone* package or the *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 install it on the device.

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

- 4 When installation is complete, reboot the device as prompted.
- 5 In ZENworks Control Center, go to the **Devices > Workstations** list to confirm that the device is enrolled in the zone.

The Windows device is listed after the predefined dynamic groups. In this example, we enrolled a Windows device named *DESKTOP-A7JSKD0*.

Devices				
	Status	Name	Type	Operating System
<input type="checkbox"/>		Apple macOS 10.12 (Sierra)	Dynamic Workstation Group	
<input type="checkbox"/>		Apple OS X 10.10 (Yosemite)	Dynamic Workstation Group	
<input type="checkbox"/>		Apple OS X 10.11 (El Capitan)	Dynamic Workstation Group	
<input type="checkbox"/>		Apple OS X 10.8 (Mountain Lion)	Dynamic Workstation Group	
<input type="checkbox"/>		Apple OS X 10.9 (Mavericks)	Dynamic Workstation Group	
<input type="checkbox"/>		Mac OS X 10.5 (Leopard)	Dynamic Workstation Group	
<input type="checkbox"/>		Mac OS X 10.6 (Snow Leopard)	Dynamic Workstation Group	
<input type="checkbox"/>		Mac OS X 10.7 (Lion)	Dynamic Workstation Group	
<input type="checkbox"/>		Red Hat Enterprise Linux Desktop 4	Dynamic Workstation Group	
<input type="checkbox"/>		Red Hat Enterprise Linux Desktop 5	Dynamic Workstation Group	
<input type="checkbox"/>		Red Hat Enterprise Linux Desktop 6	Dynamic Workstation Group	
<input type="checkbox"/>		Red Hat Enterprise Linux Desktop 7	Dynamic Workstation Group	
<input type="checkbox"/>		SUSE Linux Enterprise Desktop 10	Dynamic Workstation Group	
<input type="checkbox"/>		SUSE Linux Enterprise Desktop 11	Dynamic Workstation Group	
<input type="checkbox"/>		SUSE Linux Enterprise Desktop 12	Dynamic Workstation Group	
<input type="checkbox"/>		Windows 10 Workstations	Dynamic Workstation Group	
<input type="checkbox"/>		Windows 7 Workstations	Dynamic Workstation Group	
<input type="checkbox"/>		Windows 8 Workstations	Dynamic Workstation Group	
<input type="checkbox"/>		Windows 8.1 Workstations	Dynamic Workstation Group	
<input type="checkbox"/>		Windows Vista Workstations	Dynamic Workstation Group	
<input type="checkbox"/>		Windows XP Workstations	Dynamic Workstation Group	
<input checked="" type="checkbox"/>		DESKTOP-A7JSKD0	Workstation	windows10-ent-gen-x64 2:41 PM

Enroll a Windows Device

Windows devices don't require an enrollment policy. You can define a **registration rule** to determine some of the same stuff that a mobile enrollment policy does, such as the device's name, folder, and groups in ZENworks Control Center. However, since registration rules are not required, we'll have you skip rules for this evaluation and go straight to enrolling the device.

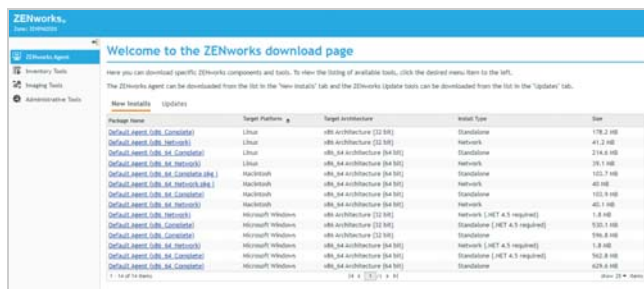
To enroll a Windows device in the zone, you install the ZENworks Agent on the device. The agent then contacts the ZENworks Primary Server and completes the enrollment.

There are several ways you can get the 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 device that you want to enroll, enter the following URL.

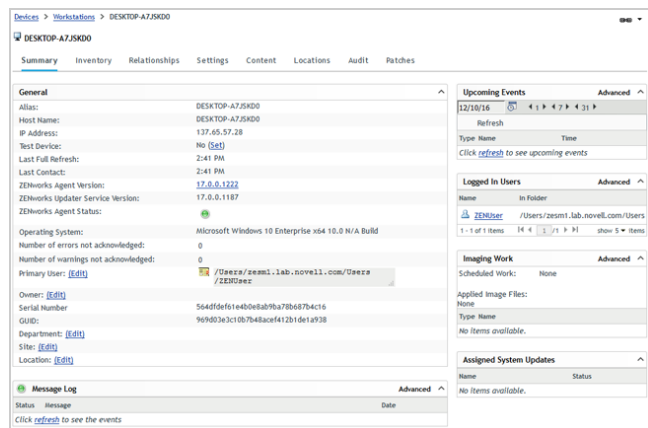
https://ZENworks_Server_Address/zenworks-setup

The ZENworks Agent download list is displayed.



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

The Summary page provides details about the device.



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.

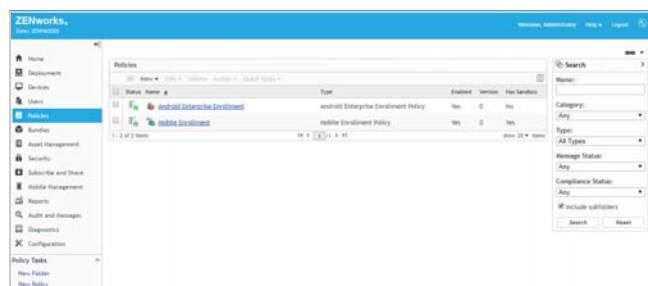
- Applying a Security Policy to Mobile Devices (page 21)
- Applying a Control Policy to Mobile Devices (page 22)

APPLYING A SECURITY POLICY TO MOBILE DEVICES

The Mobile Security policy controls password, encryption, and device inactivity settings on iOS and Android devices.

Creating a Mobile Security Policy

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



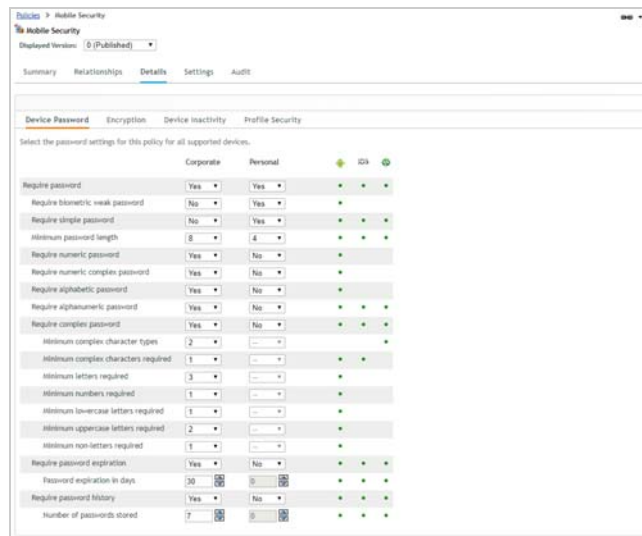
- Click **New > Policy** to display the Create New Policy wizard.
- On the Select Platform page, select **Mobile**, then click **Next**.
- On the Select Policy Category page, select **General Mobile Policies**, then click **Next**.

- On the Select Policy Type page, select **Mobile Security Policy**, then click **Next**.
- On the Define Details page, specify **Mobile Security** for the policy name, then click **Next**.
- 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.

- 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.



- 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.

- 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.

Assigning the Mobile Security Policy

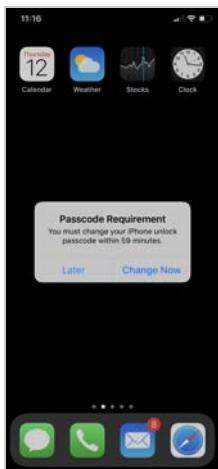
This policy can be assigned to either users or devices. We'll have you assign it to the evaluation user so that the policy will apply to all of the devices enrolled by the user. If you were to use a device assignment, you would need to assign it to each device.

- 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.

Testing the Mobile Security 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.



- 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.

Testing the Mobile Security 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.

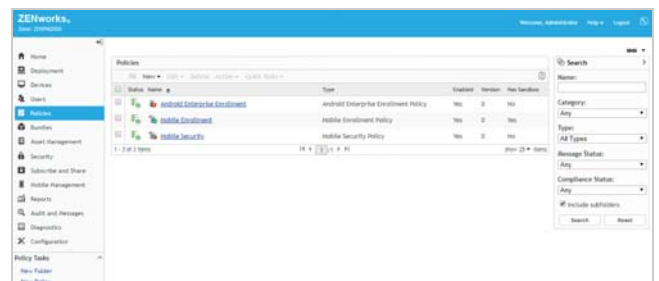
At this point, feel free to change the settings in the Mobile Security policy to see how they are enforced on the device. After you change settings, make sure you publish the policy again so that the changes are applied to the device. And remember, any changes you make to the policy are reflected on all of the evaluation user's devices.

APPLYING 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.

Creating the Mobile Device Control Policy

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



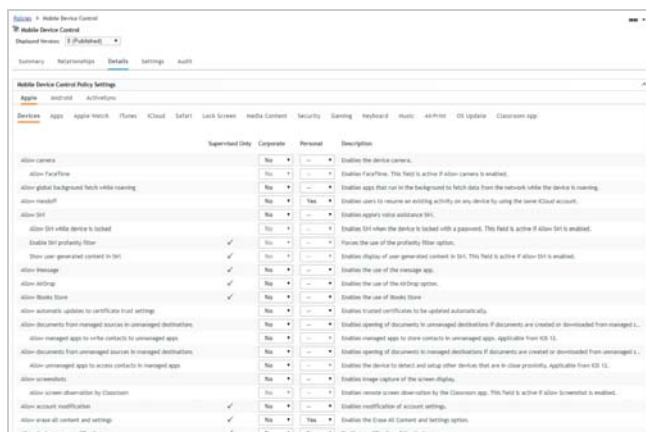
- 2 Click **New** > **Policy** to display the Create New Policy wizard.
- 3 On the Select Platform page, select **Mobile**, then click **Next**.
- 4 On the Select Policy Category page, select **General Mobile Policies**, then click **Next**.
- 5 On the Select Policy Type page, select **Mobile Device 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.

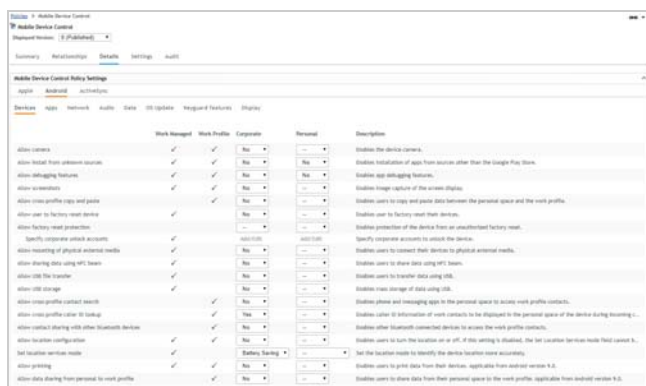


Setting	Work Managed	Work Profile	Corporate	Personal	Description
allow camera	✓	✓	No	Yes	Enables the device camera.
allow location	✓	✓	No	Yes	Enables location. This field is active if allow camera is enabled.
allow global background fetch while roaming	✓	✓	No	Yes	Enables apps that run in the background to fetch data from the network while the device is roaming.
allow hotspot	✓	✓	No	Yes	Enables users to secure an existing activity on any device by using the same iCloud account.
allow Siri	✓	✓	No	Yes	Enables users to use voice assistance (Siri).
allow Siri while device is locked	✓	✓	No	Yes	Enables Siri when the device is locked with a passcode. This field is active if allow Siri is enabled.
enable Siri profanity filter	✓	✓	No	Yes	Forces the use of the profanity filter option.
show user generated content in Siri	✓	✓	No	Yes	Enables display of user-generated content in Siri. This field is active if allow Siri is enabled.
allow streaming	✓	✓	No	Yes	Enables the use of the streaming option.
allow settings	✓	✓	No	Yes	Enables the use of the settings option.
allow mobile store	✓	✓	No	Yes	Enables the use of the mobile store.
allow automatic updates to certificate trust settings	✓	✓	No	Yes	Enables trust certificates to be updated automatically.
allow documents from managed sources to unmanaged destinations	✓	✓	No	Yes	Enables opening of documents in unmanaged destinations if documents are created or downloaded from managed sources.
allow managed apps to share contacts to unmanaged apps	✓	✓	No	Yes	Enables managed apps to share contacts to unmanaged apps, applicable from iOS 10.
allow documents from unmanaged sources to managed destinations	✓	✓	No	Yes	Enables opening of documents in managed destinations if documents are created or downloaded from unmanaged sources.
allow unmanaged apps to access contacts in managed apps	✓	✓	No	Yes	Enables the device to select and share other devices that are in close proximity, applicable from iOS 10.
allow screenshots	✓	✓	No	Yes	Enables image capture of the screen display.
allow screen observation by Classroom	✓	✓	No	Yes	Enables screen observation by the Classroom app. This field is active if allow screenshots is enabled.
allow account modification	✓	✓	No	Yes	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.



Setting	Work Managed	Work Profile	Corporate	Personal	Description
allow camera	✓	✓	No	Yes	Enables the device camera.
allow upload from unknown sources	✓	✓	No	Yes	Enables installation of apps from sources other than the Google Play Store.
allow debugging features	✓	✓	No	Yes	Enables app debugging features.
allow hotspot	✓	✓	No	Yes	Enables image capture of the screen display.
allow cross-profile copy and paste	✓	✓	No	Yes	Enables users to copy and paste data between the personal space and the work profile.
allow user to factory reset device	✓	✓	No	Yes	Enables user to factory reset their device.
allow factory reset protection	✓	✓	No	Yes	Enables protection of the device from an unauthorized factory reset.
Specify corporate-attached accounts	✓	✓	No	Yes	Specify corporate accounts to attach to the device.
allow mounting of physical external media	✓	✓	No	Yes	Enables users to connect their device to physical external media.
allow sharing data using NFC beam	✓	✓	No	Yes	Enables users to share data using NFC beam.
allow USB file transfer	✓	✓	No	Yes	Enables users to transfer data using USB.
allow USB storage	✓	✓	No	Yes	Enables mass storage of data using USB.
allow cross-profile contact search	✓	✓	No	Yes	Enables phone and messaging apps in the personal space to access work profile contacts.
allow cross-profile calendar lookup	✓	✓	No	Yes	Enables other (third-party) connected devices to be displayed in the personal space of the device during browsing.
allow contact sharing with other Bluetooth devices	✓	✓	No	Yes	Enables other Bluetooth-connected devices to access the work profile contacts.
allow location configuration	✓	✓	No	Yes	Enables users to view the location on a map. If the setting is disabled, the last location service mode field cannot be.
Set location service mode	✓	✓	No	Yes	See the location mode to identify the device location more accurately.
allow printing	✓	✓	No	Yes	Enables users to print data from their device. Applicable from Android version 4.0.
allow data sharing from personal to work profile	✓	✓	No	Yes	Enables users to share data from their personal space to the work profile, applicable from Android version 4.0.

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.

Assigning the Mobile Device Control 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.


Testing the Mobile Device Control 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.

Testing the Mobile Device Control 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.

Secure Your Windows Device

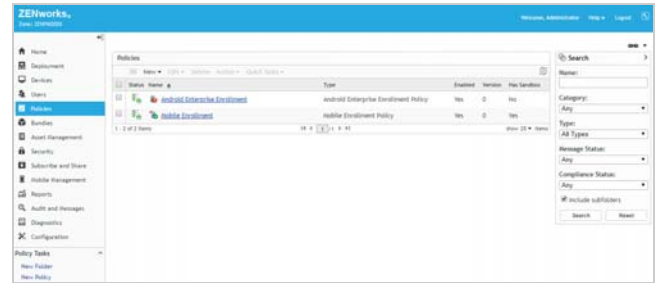
ZENworks lets you control the Windows Group policy to secure devices. In this evaluation, we'll use the Windows Group policy to enforce a complex password on your Windows device.

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 enrolled Windows device. For example, if you enrolled a Windows 10 64-bit device, you need to run ZENworks Control Center on a Windows 10 64-bit device. If you enrolled a Windows 7 32-bit device, run ZENworks Control Center on a Windows 7 32-bit device.

- ♦ [Creating the Windows Group Policy \(page 24\)](#)
- ♦ [Assigning the Windows Group Policy \(page 25\)](#)
- ♦ [Testing the Windows Group Policy \(page 25\)](#)

CREATING THE WINDOWS GROUP POLICY

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

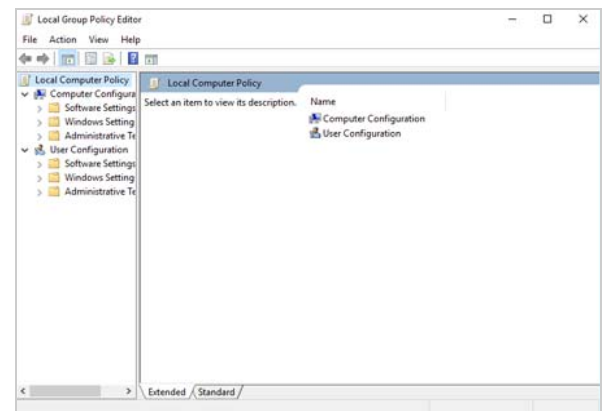


- 2 Click **New > Policy** to display the Create New Policy wizard.
- 3 On the Select Platform page, select **Windows**, then click **Next**.
- 4 On the Select Policy Category page, select **Windows Configuration Policies**, then click **Next**.
- 5 On the Select Policy Type page, select **Windows Group 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.

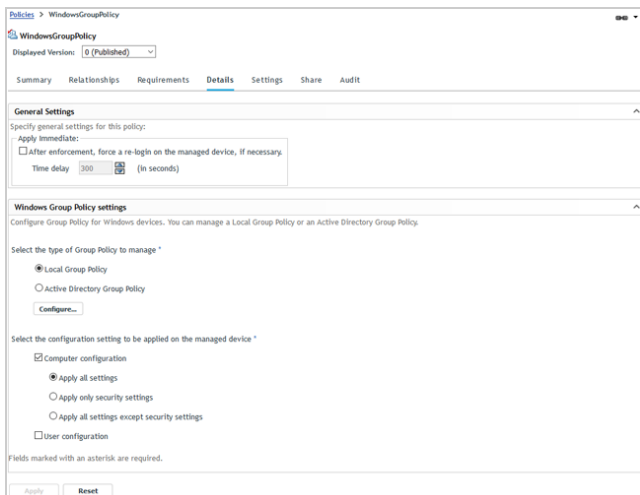
- 7c** In the Local Group Policy Editor, edit the Password Policy to enable the **Password must meet complexity requirements** option.

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.





ASSIGNING THE WINDOWS GROUP POLICY

The Windows Group policy can be assigned to either users or devices. We'll have you 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.

TESTING THE WINDOWS GROUP 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**.

- 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.

Distribute an App to Your Mobile Devices

ZENworks supports distributing of applications to iOS and Android devices.

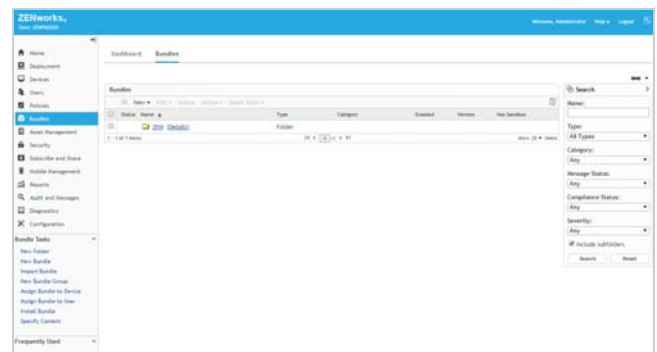
- ♦ [Distributing an Apple App Store App to an iOS Device \(page 25\)](#)
- ♦ [Distributing an Apple VPP App to an iOS Device \(page 27\)](#)
- ♦ [Distributing an Android Enterprise App to an Android Device \(page 29\)](#)
- ♦ [Viewing the Bundle Status \(page 30\)](#)

DISTRIBUTING AN APPLE APP STORE APP TO AN IOS DEVICE

ZENworks lets you distribute free apps from the Apple App Store.

Creating 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 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 Bundle

Create New iOS 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:

Region: Compatibility:

Name	Publisher	Cost	Size	Devices
Evernote - stay organized	Evernote	Free	166.59 MB	<input type="checkbox"/>
Evernote Scannable	Evernote	Free	81.29 MB	<input type="checkbox"/>
Instant Ever FREE for Evernote	Apps for Evernote Limited	Free	5.42 MB	<input type="checkbox"/>
FastEver - Quickly create Evernote text...	rakko entertainment	\$1.99	8.57 MB	<input type="checkbox"/>
Sketch - Snap, Mark Up, Send.	Evernote	Free	88.92 MB	<input type="checkbox"/>
Simple Ever Free for Evernote	Apps for Evernote Limited	Free	5.08 MB	<input type="checkbox"/>
*Note: Fastest Note Ever	Curt Grimes	Free	4.44 MB	<input type="checkbox"/>
vJournal For Evernote free	Apps for Evernote Limited	Free	8.47 MB	<input type="checkbox"/>
Microsoft OneNote	Microsoft Corporation	Free	335.67 MB	<input type="checkbox"/>
Notability	Ginger Labs, Inc.	\$9.99	94.14 MB	<input type="checkbox"/>

1 - 10 of 175 Items 10 | 25 | 50 | 100 | 400 << Back Next >> Cancel

- 6 Select the Evernote app, then click **Next** to display the Bundle Details page.

Bundles > Create New iOS Bundle

Create New iOS Bundle: Evernote - stay organized

Step 4: Bundle Details
Enter the details for the bundle.

Evernote - stay organized
By Evernote

Bundle Name:

Folder:

Description:

☐ Use App Description

App Details

Publisher: Evernote
Size: 158.58 MB
Categories: Productivity, Utilities
iTunes Store ID: 281796108
Cost: Free
App Region: United States
Device Compatibility: iPhone, iPad, iPod
OS Version Compatibility: iOS 9.3 and later
Supported Languages: German, Finnish, Russian, Swedish, Korean, Portuguese, Malay, English, Italian, French, Chinese, Spanish, Czech, Vietnamese, Norwegian Bokmål, Thai, Japanese, Indonesian, Polish, Danish, Dutch, Turkish

<< Back Next >> Cancel

- 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

<< Back Finish Cancel

- 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.

Bundles > Evernote - stay organized

Evernote - stay organized
Displayed Version: 0 (Published)

Summary Relationships Details Audit

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.

Assigning 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.

Bundles > Evernote > Assign Bundle

Assign Bundle

Step 2: App Installation Schedule
Select the schedule to determine when the app is installed on the mobile devices.

Schedule Type:

Select the event that this schedule should be triggered on:

☒ Next Refresh
☐ Allow users to install from the managed Google Play store
☐ Every Refresh

<< Back Next >> Cancel

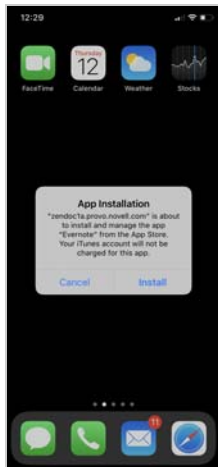
The App Installation Schedule page lets you determine if you want to push the bundle to the device now (upon completion of the assignment to the device) or let the device find out about the bundle the next time it refreshes information from the ZENworks zone.

- 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.

Testing the Bundle

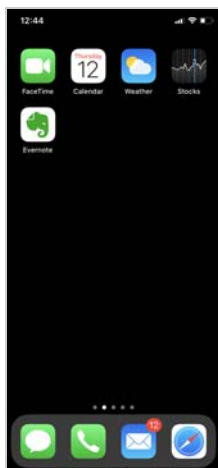
When the bundle is distributed to your iOS device, a notification is displayed on the device.



- 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.



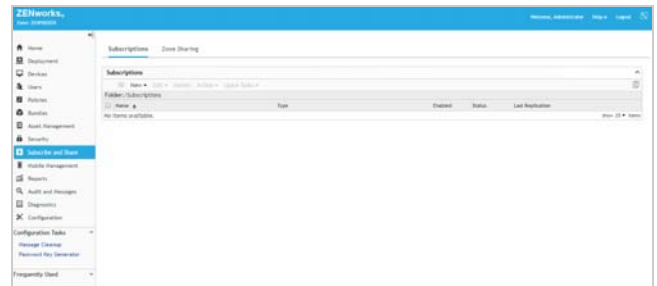
DISTRIBUTING AN APPLE VPP APP TO AN IOS DEVICE

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.

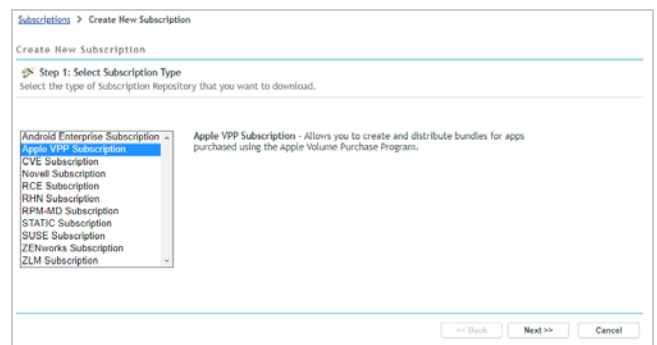
Connecting to Apple VPP

Before you can provision an app you've purchased through your Apple VPP, you need to connect ZENworks to your subscription.

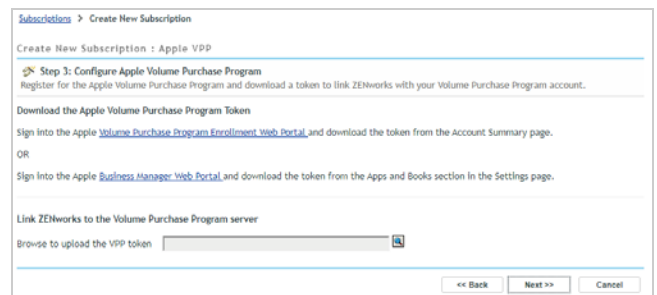
- 1 In ZENworks Control Center, click **Subscribe and Share** (in the left navigation pane).



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



- 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.



- 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.



- 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.

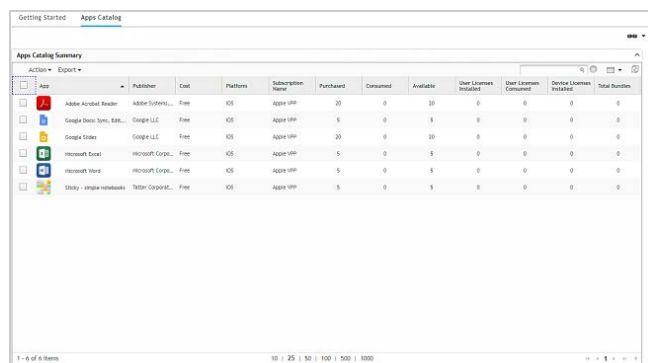
Creating an Apple VPP Bundle

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 **Mobile 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.

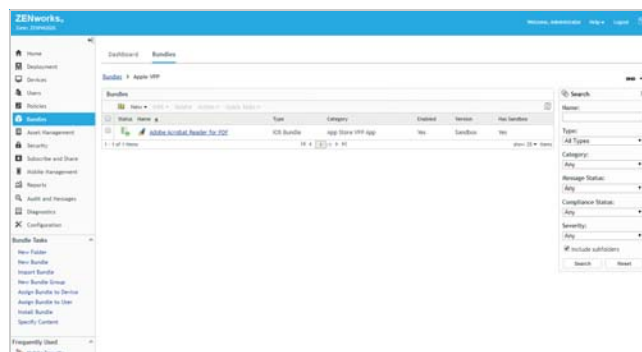
If for some reason your apps are not listed, click the refresh icon  to update the list.



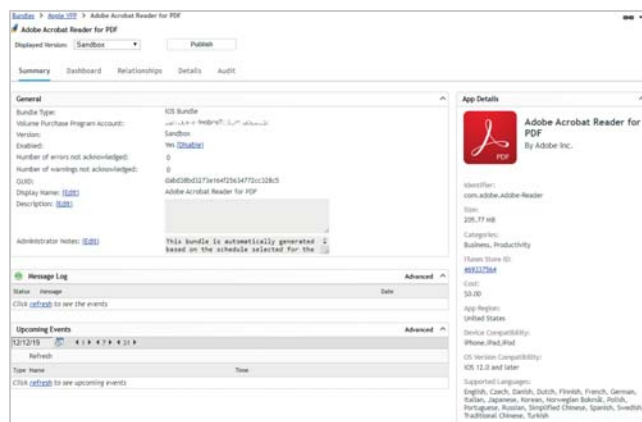
- 3 Select the check box in front of the app that you want to provision to your evaluation user, then click **Action > Create Bundles**, and then click **OK** to confirm creation of a bundle for the app.

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.



- 5 Click the bundle to display its details.



- 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.

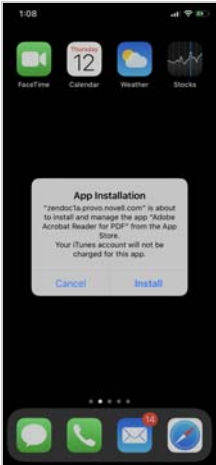
6f Click **Finish** to create the assignment.

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.

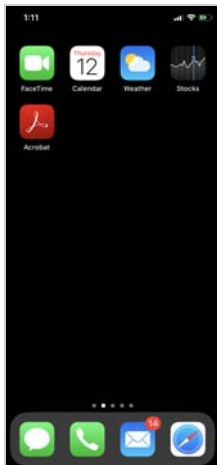
Testing the Apple VPP Bundle

When the bundle is distributed to your iOS device, a notification is displayed on the device.



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.



DISTRIBUTING 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.

Approving 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.

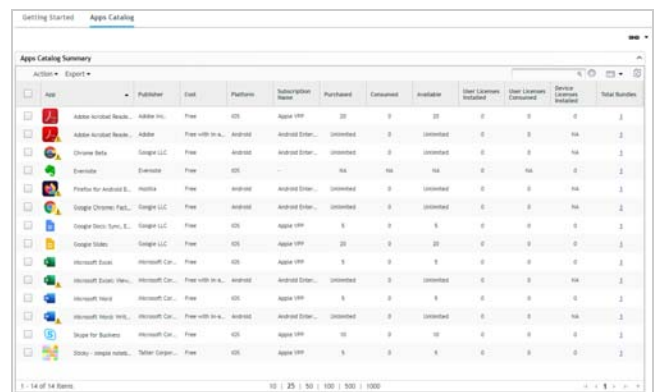
Creating an Android Bundle

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 **Mobile Management > Apps Catalog**.

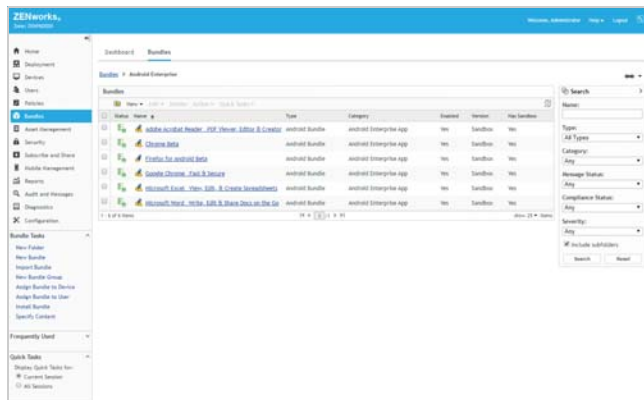
2 Click the Update View icon  to download the Android apps from your Play Store.

A bundle is created for each Android app and is added to the Android Enterprise folder in the Bundles list.

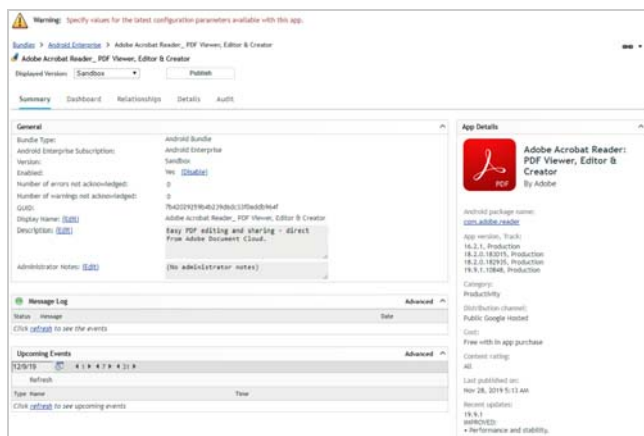


App	Publisher	Cost	Platform	Subscription Name	Purchased	Consumed	Available	User Licenses Installed	User Licenses Consumed	Device Licenses Installed	Total Bundles
Adobe Acrobat Reader...	Adobe Inc.	Free	iOS	Apple VPP	20	0	20	0	0	0	2
Adobe Acrobat Reader...	Adobe	Free with trial...	Android	Android Enter...	Unlimited	0	Unlimited	0	0	N/A	2
Chrome Beta	Google LLC	Free	Android	Android Enter...	Unlimited	0	Unlimited	0	0	N/A	2
Evernote	Evernote	Free	iOS		N/A	N/A	N/A	0	0	N/A	2
Pixel for Android B...	Pixel	Free	Android	Android Enter...	Unlimited	0	Unlimited	0	0	N/A	2
Google Chrome Pack...	Google LLC	Free	Android	Android Enter...	Unlimited	0	Unlimited	0	0	N/A	2
Google Drive, Scan, &...	Google LLC	Free	iOS	Apple VPP	0	0	0	0	0	0	2
Google Slides	Google LLC	Free	iOS	Apple VPP	20	0	20	0	0	0	2
Microsoft Excel	Microsoft Cor...	Free	iOS	Apple VPP	0	0	0	0	0	0	2
Microsoft Excel View...	Microsoft Cor...	Free with trial...	Android	Android Enter...	Unlimited	0	Unlimited	0	0	N/A	2
Microsoft Word	Microsoft Cor...	Free	iOS	Apple VPP	0	0	0	0	0	0	2
Microsoft Word Web...	Microsoft Cor...	Free with trial...	Android	Android Enter...	Unlimited	0	Unlimited	0	0	N/A	2
Sage for Business	Microsoft Cor...	Free	iOS	Apple VPP	10	0	10	0	0	0	2
Sony - Xperia mobile...	Sony Corpora...	Free	iOS	Apple VPP	0	0	0	0	0	0	2

- 3 Click **Bundles** (in the left navigation pane) to display the Bundles list, then click **Android Enterprise** to display the newly created Android bundles.



- 4 Click a bundle to display its details. Note the warning that you need to specify values for the latest configuration parameters. This means...



- 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 **Allow 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.

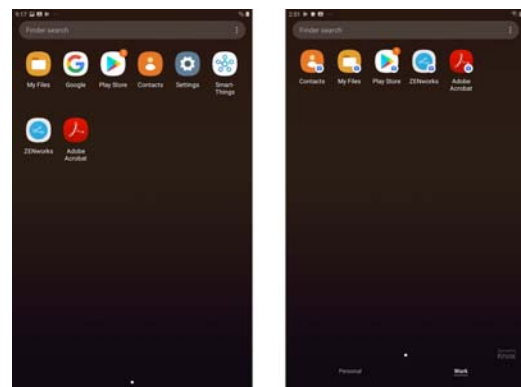
- 6 Click **Publish**, then follow the prompts to publish the bundle.

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

Testing the App

- 1 On the device, open the ZENworks Agent and tap the Refresh icon .

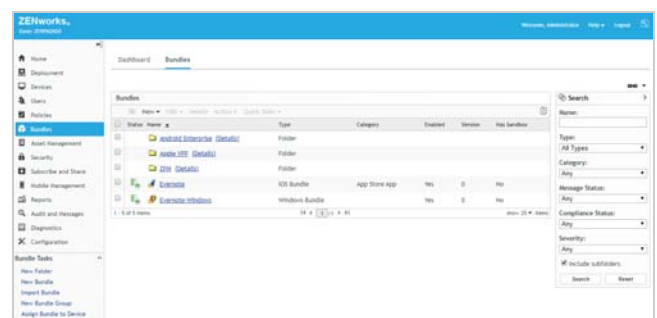
The app installation begins. When installation is complete, the app is displayed on the App screen on a work-managed device (left) and on the App Work screen on a work profile device (right).



VIEWING 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.

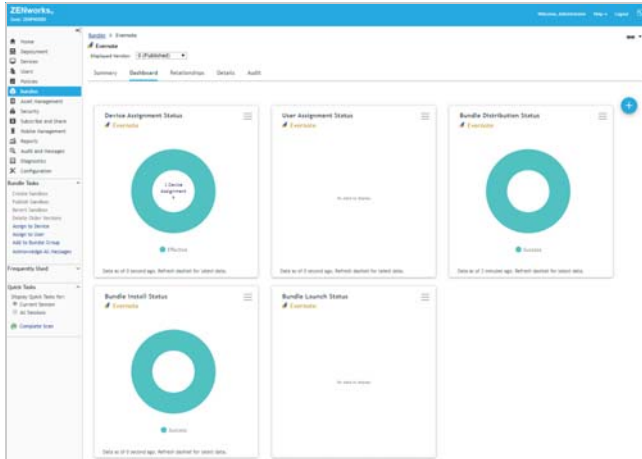
- 1 In ZENworks Control Center, click **Bundles** (in the left navigation pane).



- 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

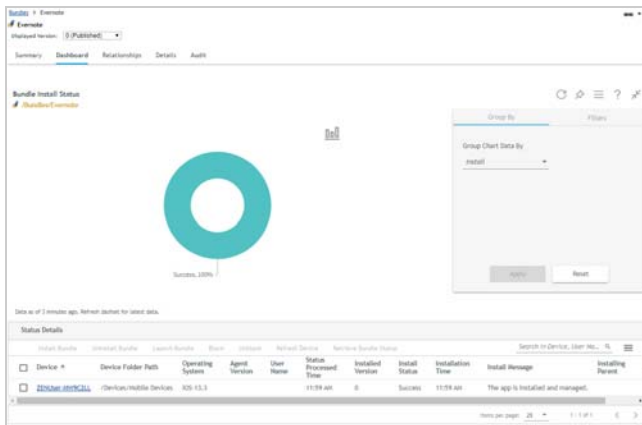
bundle is assigned. For this demo, we installed the bundle to one Windows device so the dashlets only reflect the bundle status for that one device.



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**.



5 Become familiar with the other dashlets as desired.

Distribute an Application to Your Windows Device

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

For this evaluation, you'll distribute the same Evernote application that you distributed to your iOS device. 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.

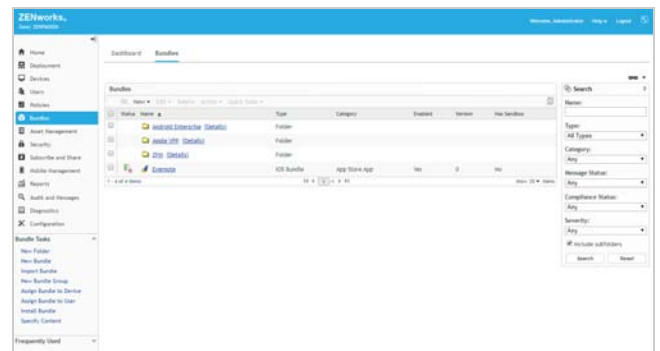
- ◆ “Creating the Windows Bundle” on page 31
- ◆ “Testing the Windows Bundle” on page 33
- ◆ “Viewing the Bundle Status” on page 33

CREATING 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_6.21.2.8716.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**.

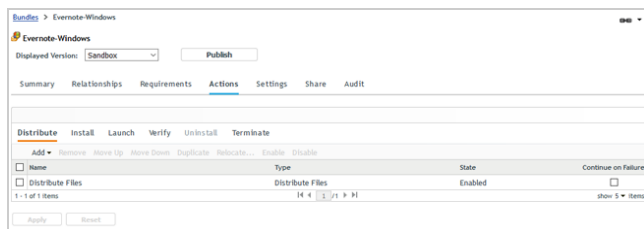
5 On the Select Bundle Category page, select **(Empty Bundle)**, then click **Next**.

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

The bundle's Actions page is displayed.

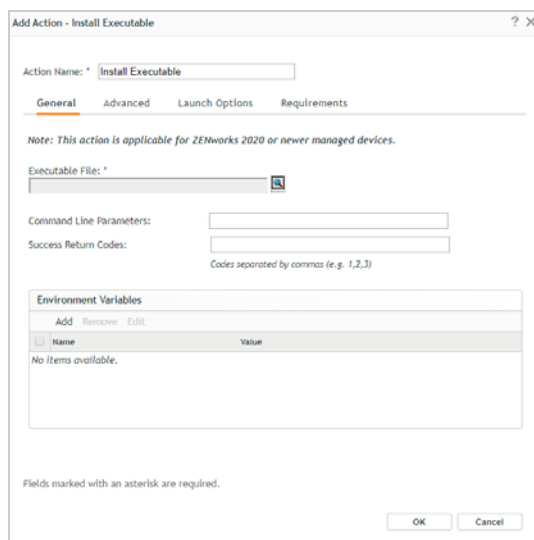


- 8 Configure the bundle to install the Evernote application:

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



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



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

- 8d For the Executable File, select the Evernote installation package.

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

- 8e In the File list, click **Add**, then upload the Evernote installation package.

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

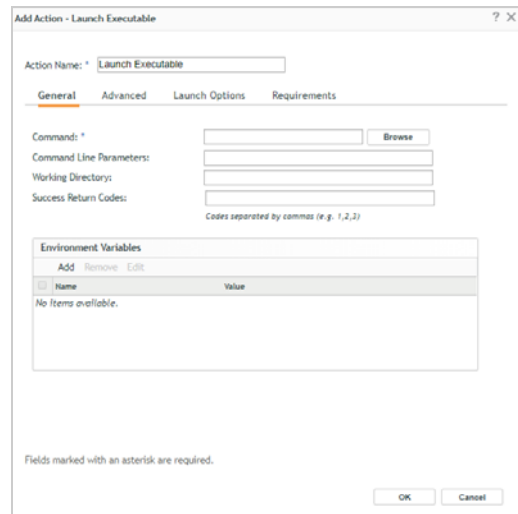
- 8f Click **OK** to add the action to the Install list.



- 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.



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

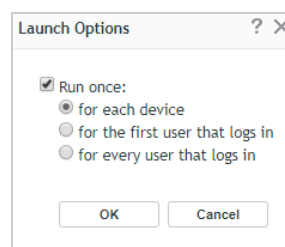
- 9d In the Command field, enter:

```
C:\Program Files  
(x86)\Evernote\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.



- 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.

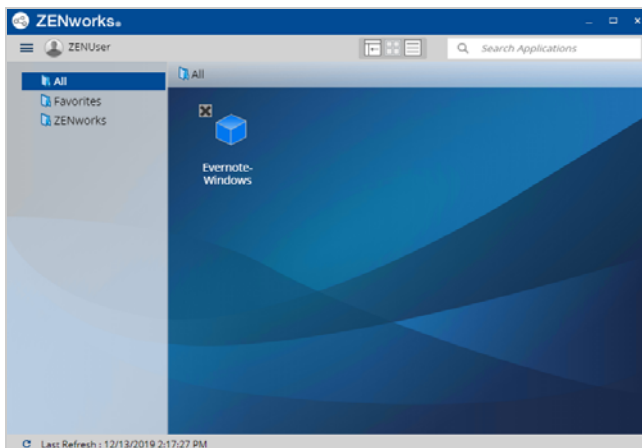
As you go through the assignment wizard, keep the default settings.

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.

TESTING THE WINDOWS BUNDLE

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



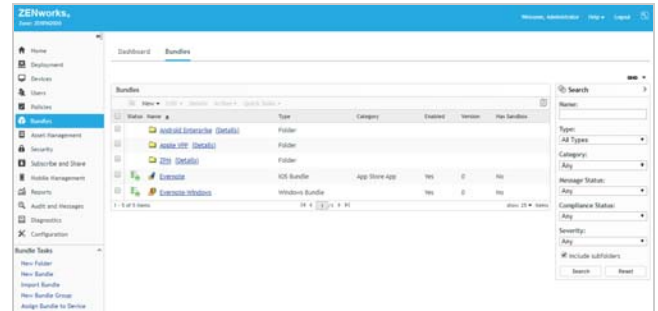
- 2 If the Evernote bundle is not displayed in the window, click the menu in the upper-left corner, then click **Refresh**.
- 3 Double-click the Evernote bundle to download the installation package and start the installation process.
- 4 Follow the prompts to install the application.

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.

VIEWING THE BUNDLE STATUS

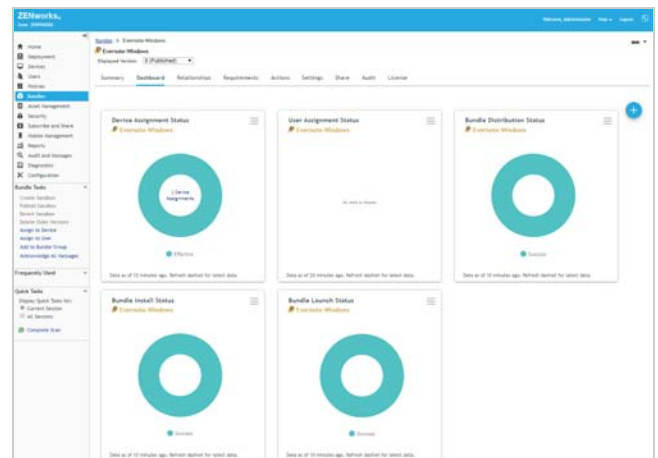
ZENworks Control Center makes it easy for you to know the status of the bundle on your Windows device, including whether it has been assigned, distributed, installed, and launched on the device.

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



- 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 demo, we installed the bundle to one Windows device so the dashlets only reflect the bundle status for that one device.

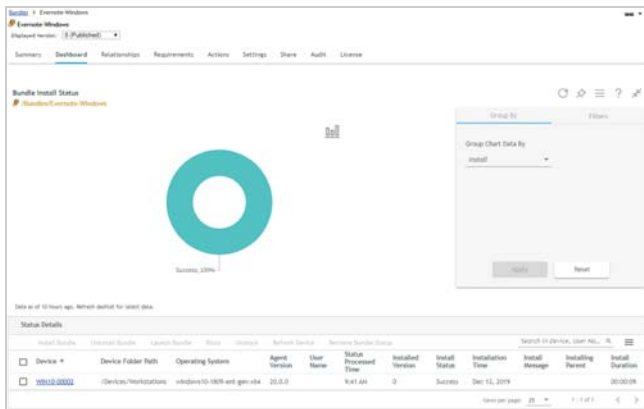


When you hover over the Device Assignment, Distribution, Install, and Launch Status charts, each dashlet shows success for the device. The User Assignment Status bundle has no data to display because the bundle is assigned to the device and not any users.

- 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**.



5 Become familiar with the other dashlets if desired.

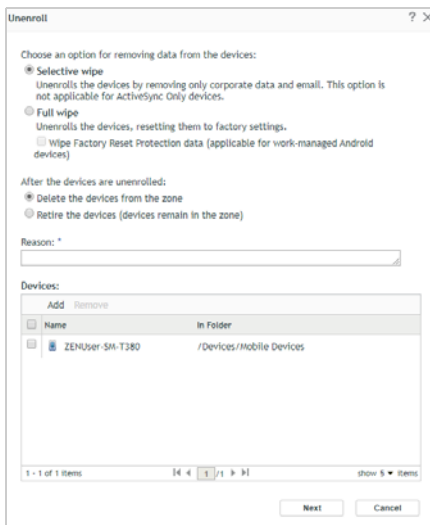
Unenroll Your iOS and Android Devices

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).

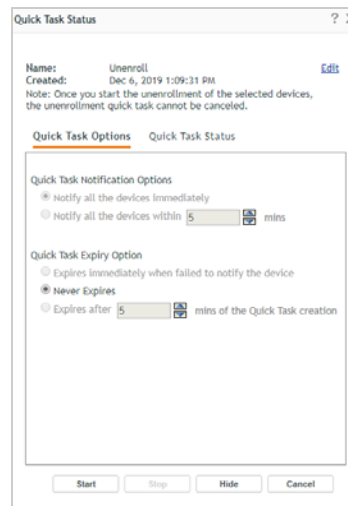
1 In ZENworks Control Center, click **Devices > Mobile Devices** to display your enrolled mobile devices.



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.




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.

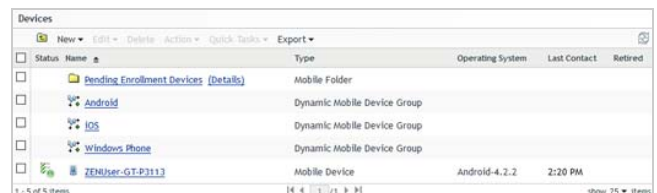


4 Leave the quick task options set to the defaults and click **Start** to send the task to the device.

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.



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.

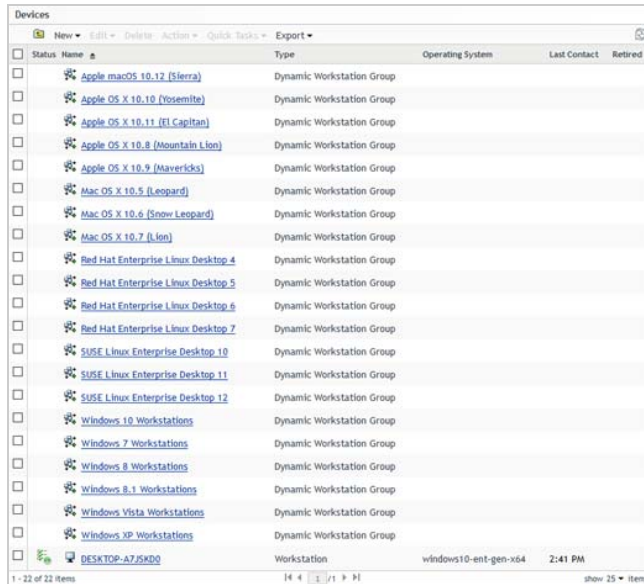
Selective Wipe: The policy restrictions have been removed.

Unenroll Your Windows Devices

During unenrollment, you choose whether the device is unregistered (removed) from the zone or retired (remains in zone but is inactive). In this evaluation, you can go ahead and unregister the device.

Unregistering a device uninstalls the ZENworks Agent from the device, which stops all ZENworks policy enforcement and software management.

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



The screenshot shows the 'Devices' window in ZENworks Control Center. It features a menu bar with 'New', 'Edit', 'Delete', 'Action', 'Quick Tasks', and 'Export'. Below the menu is a table with columns: Status, Name, Type, Operating System, Last Contact, and Retired. The table lists various workstations, including Apple macOS, Red Hat Enterprise Linux, SUSE Linux Enterprise Desktop, and Windows Workstations. The last item in the list is 'DESKTOP-A7J5KDQ', which is a Windows 10 workstation with the operating system 'windows10-ent-gen-x64' and a last contact time of '2:41 PM'. The status of this device is 'Retired'.

Status	Name	Type	Operating System	Last Contact	Retired
<input type="checkbox"/>	Apple macOS 10.12 (Sierra)	Dynamic Workstation Group			
<input type="checkbox"/>	Apple OS X 10.10 (Yosemite)	Dynamic Workstation Group			
<input type="checkbox"/>	Apple OS X 10.11 (El Capitan)	Dynamic Workstation Group			
<input type="checkbox"/>	Apple OS X 10.8 (Mountain Lion)	Dynamic Workstation Group			
<input type="checkbox"/>	Apple OS X 10.9 (Mavericks)	Dynamic Workstation Group			
<input type="checkbox"/>	Mac OS X 10.5 (Leopard)	Dynamic Workstation Group			
<input type="checkbox"/>	Mac OS X 10.6 (Snow Leopard)	Dynamic Workstation Group			
<input type="checkbox"/>	Mac OS X 10.7 (Lion)	Dynamic Workstation Group			
<input type="checkbox"/>	Red Hat Enterprise Linux Desktop 4	Dynamic Workstation Group			
<input type="checkbox"/>	Red Hat Enterprise Linux Desktop 5	Dynamic Workstation Group			
<input type="checkbox"/>	Red Hat Enterprise Linux Desktop 6	Dynamic Workstation Group			
<input type="checkbox"/>	Red Hat Enterprise Linux Desktop 7	Dynamic Workstation Group			
<input type="checkbox"/>	SUSE Linux Enterprise Desktop 10	Dynamic Workstation Group			
<input type="checkbox"/>	SUSE Linux Enterprise Desktop 11	Dynamic Workstation Group			
<input type="checkbox"/>	SUSE Linux Enterprise Desktop 12	Dynamic Workstation Group			
<input type="checkbox"/>	Windows 10 Workstations	Dynamic Workstation Group			
<input type="checkbox"/>	Windows 7 Workstations	Dynamic Workstation Group			
<input type="checkbox"/>	Windows 8 Workstations	Dynamic Workstation Group			
<input type="checkbox"/>	Windows 8.1 Workstations	Dynamic Workstation Group			
<input type="checkbox"/>	Windows Vista Workstations	Dynamic Workstation Group			
<input type="checkbox"/>	Windows XP Workstations	Dynamic Workstation Group			
<input type="checkbox"/>	DESKTOP-A7J5KDQ	Workstation	windows10-ent-gen-x64	2:41 PM	

- 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. On the device, the ZENworks Agent is uninstalled and the ZENworks icon is no longer available in the notification area.

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/>.

Copyright © 2017-2020 Micro Focus Software Inc. All Rights Reserved.

