

ZENworks Configuration Management 2017

Evaluator's Guide



July 2017

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 Configuration Management 2017 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 \(page 2\)](#)
 - ♦ [Update Your ZENworks System \(page 3\)](#)
 - ♦ [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 \(page 18\)](#)
4. **Use policies to secure your devices:**
 - ♦ [Secure Your Mobile Devices \(page 19\)](#)
 - ♦ [Secure Your Windows Device \(page 22\)](#)
5. **Distribute apps to your devices:**
 - ♦ [Distribute an App to Your Mobile Devices \(page 24\)](#)
 - ♦ [Distribute an Application to Your Windows Device \(page 28\)](#)
6. **Unenroll devices from ZENworks:**
 - ♦ [Unenroll Your iOS and Android Devices \(page 30\)](#)
 - ♦ [Unenroll Your Windows Devices \(page 31\)](#)

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.

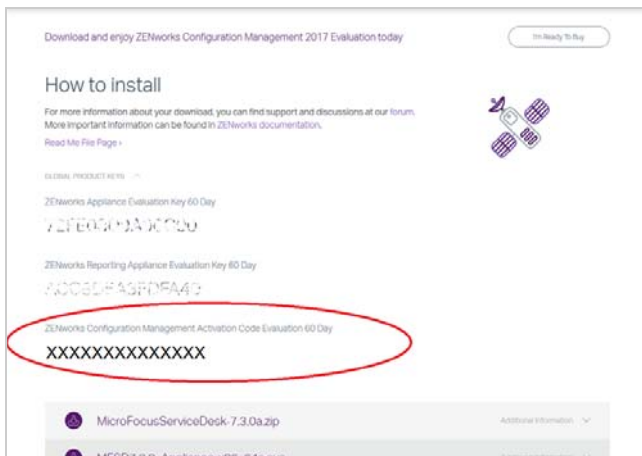
- ☐ **A ZENworks server.** This can be either a supported hypervisor where you can run the ZENworks Virtual Appliance or a server (physical or virtual) where you can install the ZENworks software.
- ☐ **An LDAP directory.** ZENworks user authentication and user-based management requires access to an LDAP user directory.
- ☐ **A Google account.** A ZENworks-dedicated account to link ZENworks to Google Cloud Messaging services.
- ☐ **Two Apple ID accounts.** One ZENworks-dedicated account to link ZENworks to Apple Push Notification services. A second individual account to receive apps distributed through ZENworks.
- ☐ **An Apple Volume Purchase Program account.** Not really required, but if you have one you can test how ZENworks supports distribution of apps purchased through the program.
- ☐ **An Apple Device Enrollment Program account.** Also not really required, but if you have one you can test how ZENworks manages enrollment of devices purchased through the program.

- ❑ **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 8. You're going to play with settings so we recommend it be a clean device that you can reset when finished.
- ❑ **An Android device.** Same purpose as the iOS device. It needs to be running a minimum of Android 4.1.
- ❑ **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 [site \(https://www.microfocus.com/products/zenworks/configuration-management/trial/\)](https://www.microfocus.com/products/zenworks/configuration-management/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 you use it if possible.

The appliance is supported on the following hypervisors. Download the files for the hypervisor you plan to use.

Hypervisor	File
VMware ESXi 5.x and 6.x VMware Workstation 6.5 and newer (use in non-production environments only)	ZENworks2017a_Appliance-x86_64.ova
Microsoft Hyper-V Server Windows 2008 R2 and 2012	ZENworks2017a_Appliance-x86_64.vhd.zip
XEN on SLES 12.x	.ZENworks2017a_Appliance-x86_64.xen.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 Windows 2012 Server R2 x86_64 Windows 2016 Server x86_64	ZENworks_2017a.iso
SLES 11 SP3 / SP4 x86_64 SLES 12 / SP1 / SP2 x86_64	ZENworks_2017a.iso

Install ZENworks

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

- ♦ [Deploying the ZENworks Virtual Appliance \(page 2\)](#)
- ♦ [Installing the ZENworks Software \(page 3\)](#)

DEPLOYING THE ZENWORKS VIRTUAL APPLIANCE

- 1 Import the ZENworks Virtual Appliance into your hypervisor to create a new virtual machine.
- 2 Power on the new virtual machine.
- 3 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 Sybase Anywhere database.
- ♦ Use the internal Certificate Authority.

If you need more details, refer to the [ZENworks Appliance Deployment and Administration Reference \(https://www.novell.com/documentation/zenworks2017/zen_ca_appliance\)](https://www.novell.com/documentation/zenworks2017/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 8 GB RAM and 20 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 2017 Server Installation Guide \(https://www.novell.com/documentation/zenworks2017/zen_installation\)](https://www.novell.com/documentation/zenworks2017/zen_installation).

Update Your ZENworks System

The software you installed is the **ZENworks 2017** software. The most recently released software is **ZENworks 2017 Update 1**. This evaluation is based on the functionality available in ZENworks 2017 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

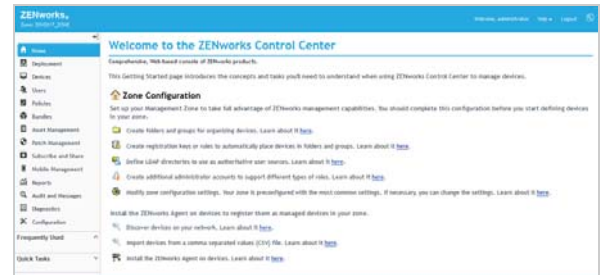
- 1 Log in to ZENworks Control Center:

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

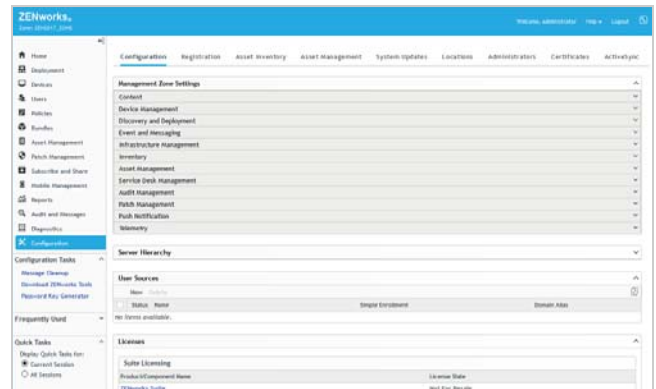
`https://ZENworks_Server_Address:port`

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).

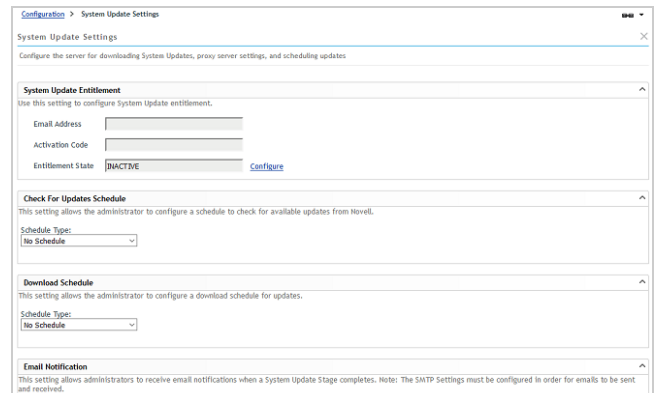
- 1b Specify **Administrator** as the username, specify the password you defined during installation, then click **Login** to display the Welcome page.



- 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 it from the GLOBAL PRODUCT KEYS section.

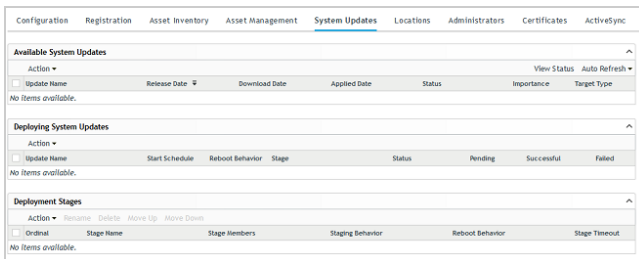
The entitlement is activated and the **Entitlement State** in the System Update Entitlement panel changes to **ACTIVE**.



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

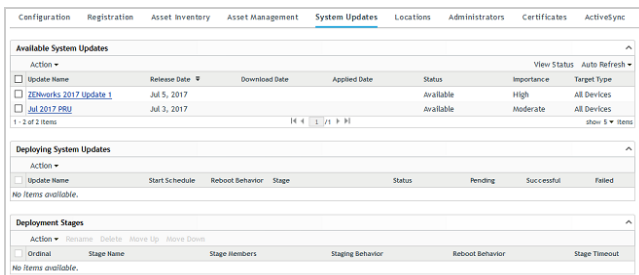
APPLYING THE SYSTEM UPDATE

- 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.



- 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 2017 Update 1** in the list as well as the most recent Product Recognition Update (PRU). **ZENworks 2017 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, but you don't have to do it right now if you don't want to.



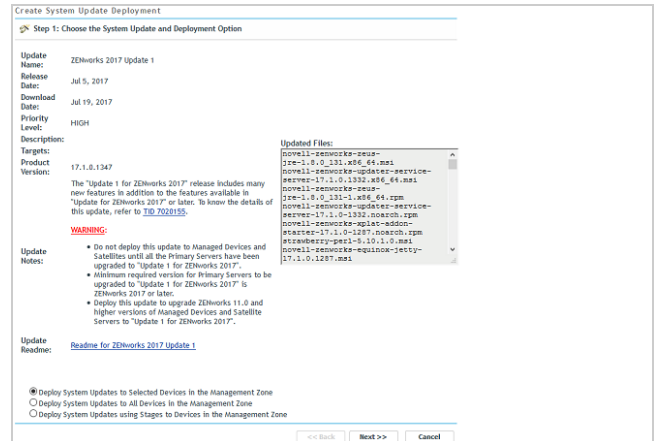
- Select the check boxes next to **ZENworks 2017 Update 1** and the PRU, then click **Action > Download Update**.

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

- Select the check box next to **ZENworks 2017 Update 1**, then click **Action > Authorize Update** to change the update status to **Ready to Deploy**.



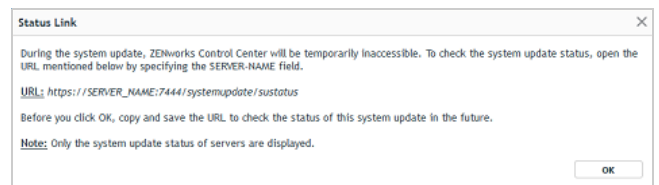
- Select the check box next to **ZENworks 2017 Update 1**, then click **Action > Deploy Update to Devices** to launch the deployment wizard.



- 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.

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



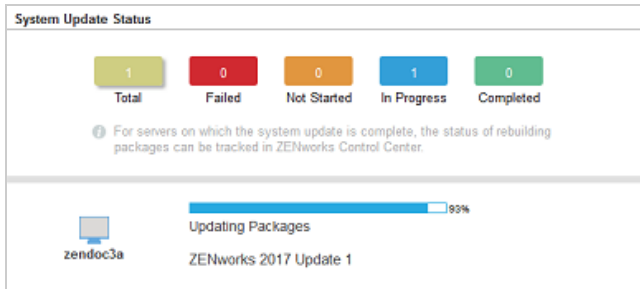
During update, the ZENworks Server is not accessible through ZENworks Control Center. Therefore, you need to use the System Update console to monitor system update progress.

- Copy the URL for the System Update console, then click **OK** to start the update.

- 11 Enter the System Update console URL in your web browser, replacing 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.



- 12 When the update has successfully completed, log in to ZENworks Control Center.
- 13 Go to the System Update page (**Configuration > System Updates**).

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

The screenshot shows the 'System Updates' page in ZENworks Control Center. It has three main sections: 'Available System Updates', 'Deploying System Updates', and 'Deployment Stages'. The 'Available System Updates' section shows a table with columns: Action, Update Name, Release Date, Download Date, Applied Date, Status, Importance, and Target Type. It lists 'ZENworks 2017 Update 1' and 'ZENworks 2017 PRU'. The 'Deploying System Updates' section shows a table with columns: Action, Update Name, Start Schedule, Reboot Behavior, Stage, Status, Pending, Successful, and Failed. It shows 'ZENworks 2017 Update 1' with a status of 'Pending'. The 'Deployment Stages' section shows a table with columns: Action, Ordinal, Stage Name, Stage Members, Staging Behavior, Reboot Behavior, and Stage Timeout. It shows 'Ordinal' with a status of 'No items available'.

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 is removed from the Deploying System Updates panel and its status is updated in the Available System Updates panel.

The screenshot shows the 'System Updates' page in ZENworks Control Center after the update is complete. The 'Available System Updates' section now shows 'ZENworks 2017 Update 1' with a status of 'Baselined' and 'ZENworks 2017 PRU' with a status of 'Awaiting Authorization'. The 'Deploying System Updates' section now shows 'No items available'. The 'Deployment Stages' section also shows 'No items available'.

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

- 14a Select the check box next to the PRU, then select **Action > Authorize Update**.
- 14b 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 device's user.

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

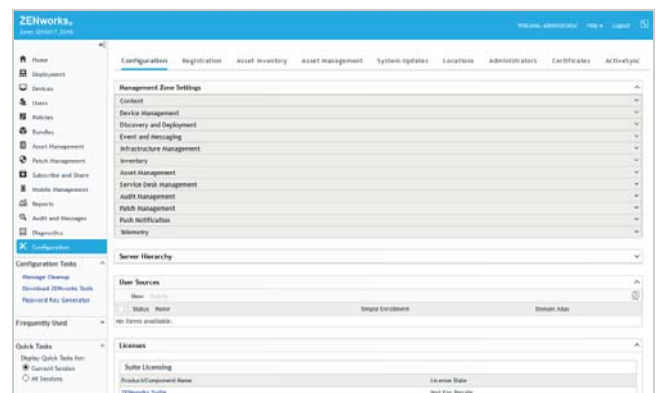
SELECTING AN EVALUATION USER

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



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

- 3 On the Connection Information page, define the following connection information, then click **Next**:
 - ♦ **Connection Name:** Specify a descriptive name for the connection to the LDAP directory.
 - ♦ **Address:** Specify the IP address or DNS hostname of the 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.
- 4 (Conditional) On the Certificate page (which is displayed only if the connection is using SSL), verify the certificate information, then click **Next**.
- 5 On the Credentials page, specify a Read-only username and password that ZENworks can use to access the directory, then click **Next**.
- 6 On the Authentication Mechanisms page, select **Username/Password**, then click **Next**.
- 7 On the User Containers page, add the container where your evaluation user resides, then click **Next**.
- 8 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.

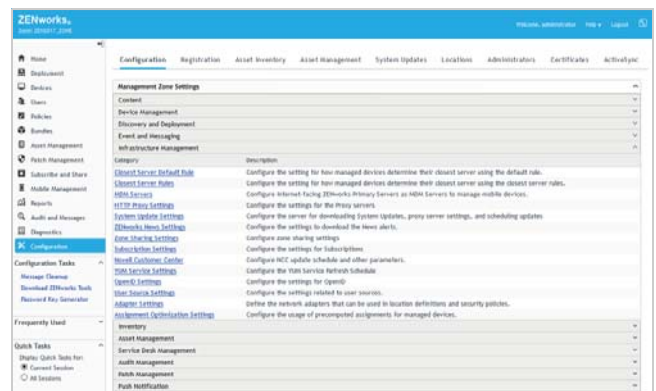
- ♦ Designating an MDM Server (page 6)
- ♦ Enabling Push Notifications for iOS Devices (page 6)
- ♦ Enabling Push Notifications for Android Devices (page 8)

DESIGNATING AN MDM SERVER

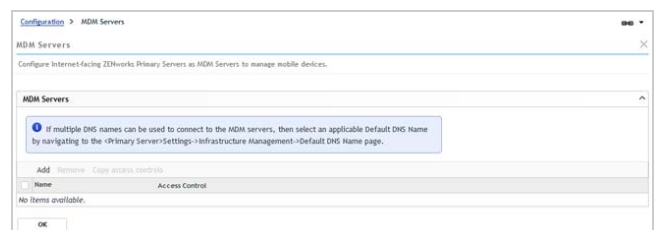
A ZENworks Management Zone must have at least one ZENworks Primary Server that is designated as a Mobile Device Management (MDM) Server. MDM Servers are the only servers in your zone that communicate with mobile devices.

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

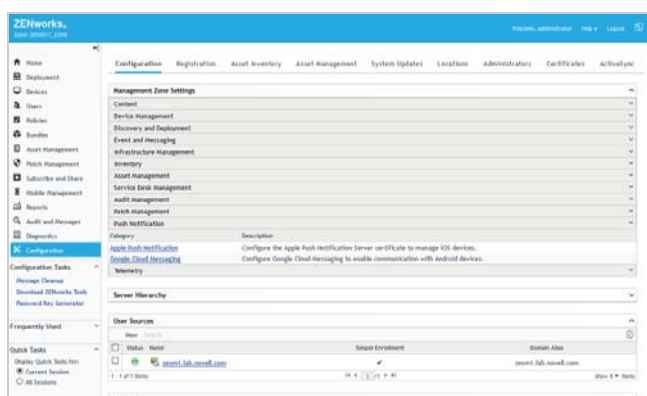
Apple Push Notification service (APNs) enables the ZENworks MDM Server to notify an iOS device when the server requires information from the device or has changes for the device. The ZENworks Primary Server

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.

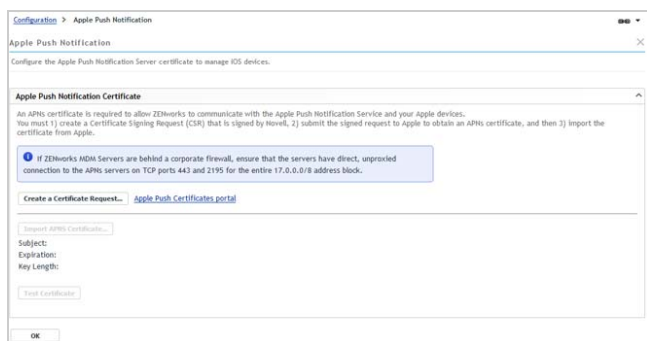
In order to use the Apple Push Notification service, an Apple Push Notification service certificate is required. The APNs certificate allows the ZENworks MDM Server and iOS devices to authenticate securely to the service.

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.

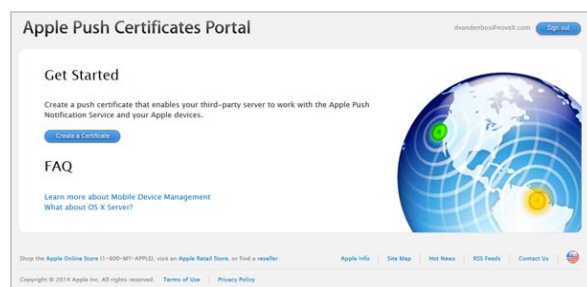
- 3d Click **Submit for Signing**.

- 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.

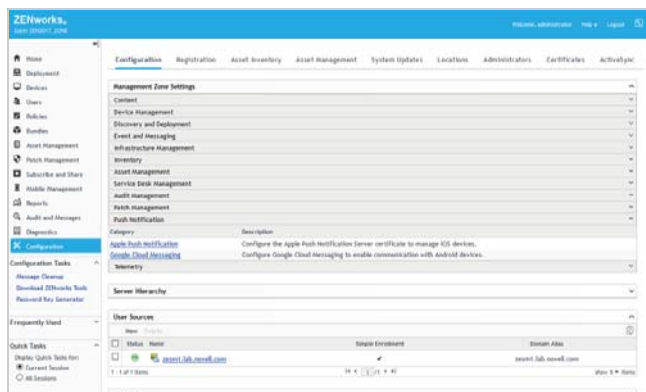
ENABLING PUSH NOTIFICATIONS FOR ANDROID DEVICES

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

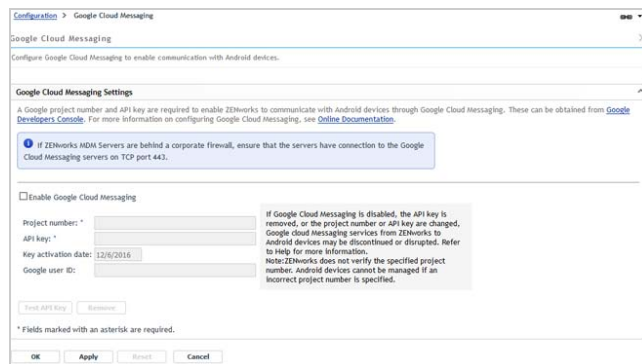
The MDM Server communicates with the Google Cloud Messaging service, which then pushes the notification to the device. After receiving the push notification, the device contacts the MDM Server directly to provide the requested information or receive the changes.

In order to use Google Cloud Messaging, you must have an existing GCM project or use the Firebase Console to create a Firebase project. The GCM or Firebase project provide 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 **Google Cloud Messaging** to display the Google Cloud Messaging settings.



3 Create a Firebase Project:

Follow these steps if you need to create a Firebase project. If you have an existing GCM project, skip to [Step 4](#).

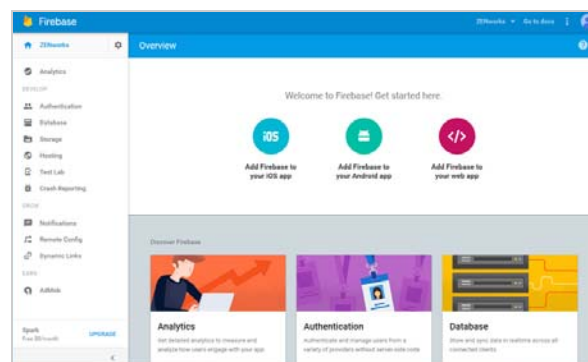
3a Click **Google Developers Console** to display the **Firebase console** (<https://console.firebase.google.com>).

3b Sign in using your Google account credentials.

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

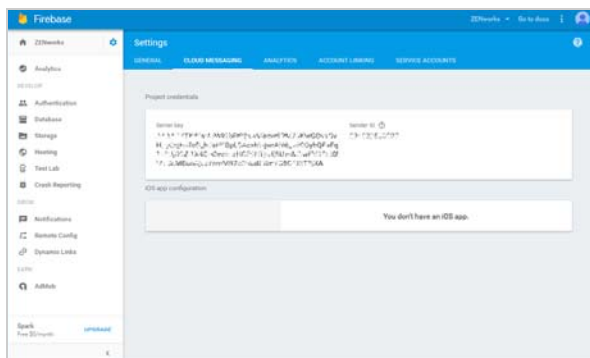
3c Click **Create New Project**, supply a name for your project (such as ZENworks), select the country/region in which your organization is located, then click **Create Project**.

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



3d In the upper-left corner, click the icon, then click **Project Settings**.

3e Click Cloud Messaging.



3f Copy the Server Key and the Sender ID to a file from which you can later paste it into ZENworks Control Center.

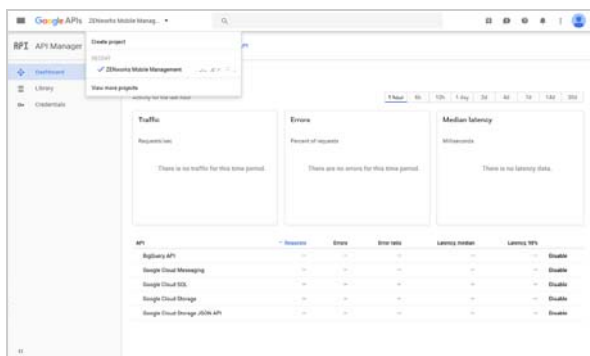
3g Skip to Step 5.

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

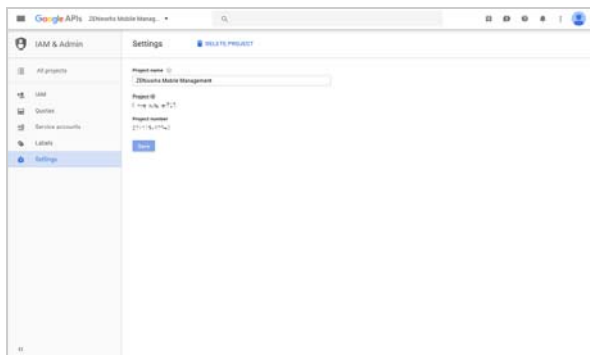
4a Go to the [Google API Console \(https://console.developers.google.com\)](https://console.developers.google.com).

4b Sign in using your Google account credentials.

4c Select your existing GCM project from the drop-down menu appearing on the top-left corner of the page.

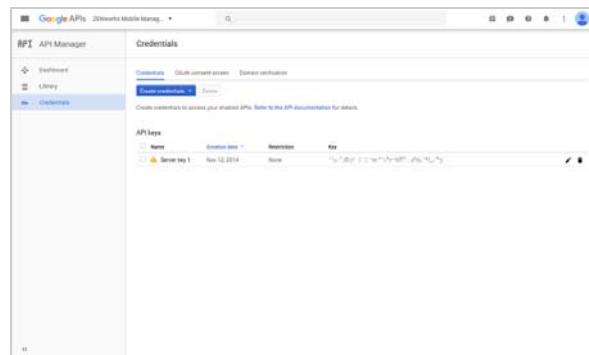


4d To retrieve the project number, click the Hamburger menu appearing in the top-left corner, click **IAM & Admin** to display the IAM & Admin page, then click **Settings**.



4e Record the project number (or copy it to a document) for use in ZENworks Control Center.

4f To retrieve the API key, click the Hamburger menu, click **API Manager** to display the API Manager page, then click **Credentials**.



4g Record the server key and creation date (or copy them to a document) for use in ZENworks Control Center.

4h Continue with Step 5.

5 Configure ZENworks with the Project Name and API Key:

5a Click the **Enable Google Cloud Messaging** check box to turn on the option.

5b Fill in the following fields with the information you gathered for your project:

Project number: Specify the Sender ID (Firebase project) or Project Number (GCM project).

API key: Specify the Server Key (Firebase project) or API Key (GCM project).

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

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

5c Click **Test API Key** to validate that the information is entered correctly and the key is active.

5d Click **OK** to save your Google 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 \(page 10\)](#)
- ♦ [Enrolling an iOS Device \(page 11\)](#)
- ♦ [Enrolling an Apple DEP iOS Device \(page 13\)](#)
- ♦ [Enrolling an Android Device \(page 16\)](#)

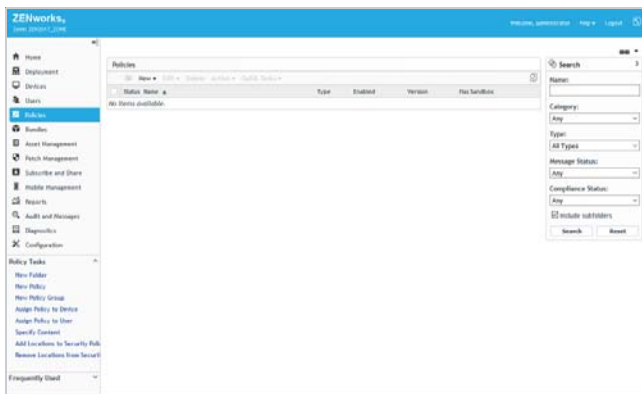
CREATING A MOBILE ENROLLMENT POLICY

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.

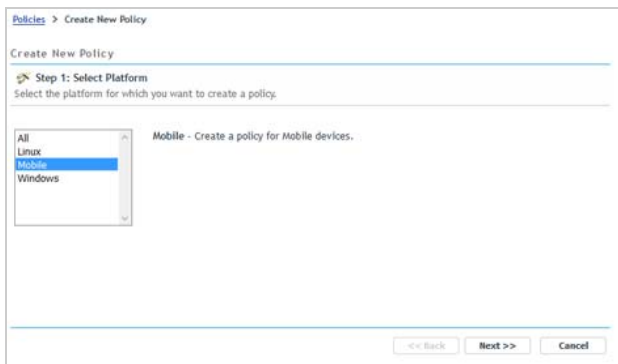
The Mobile Enrollment policy not only allows users to enroll devices but also assigns specific management settings to the device. For example, the policy determines the ZENworks name and group memberships assigned to the device, whether the device is designated as corporate owned or personal, and what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

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

- 7c Click **Next**

- 8 On the Configure Device Management Level page, keep the default settings, then click **Next**.

A device can be fully managed or ActiveSync only:

- ♦ **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 only 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

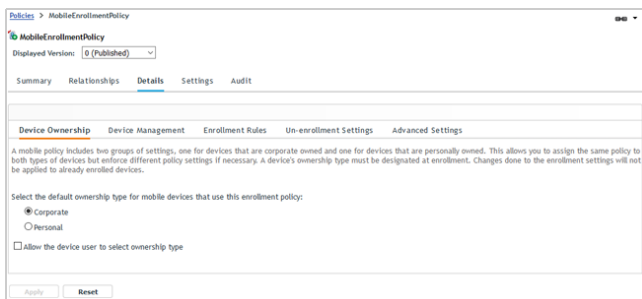
to these device. Android, iOS, Blackberry, and Windows devices can be enrolled as ActiveSync only devices.

The default settings allow the user to choose the management level during enrollment. 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.

- 9 On the Configure Device 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, 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.

ENROLLING AN IOS DEVICE

You can enroll any device running iOS version 8 or newer. We used an iPhone running iOS version 10.1.1. 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

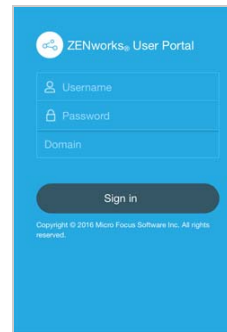
(available for Apple devices running iOS version 11 or newer), use the instructions in [“Enrolling an Apple DEP iOS Device”](#) on page 13 instead.

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

`ZENworks_server_address/zenworks-eup`

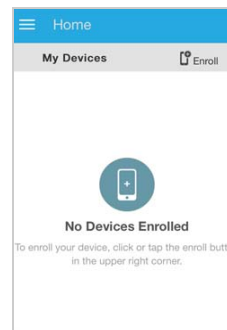
Replace `ZENworks_server_address` with the DNS name or IP address of your ZENworks Primary Server.

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.

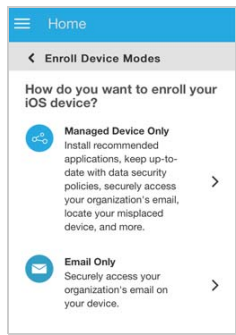
The Domain name field is not needed because the system is configured for simple enrollment, which allows users to log in with only their username rather than their full domain name.



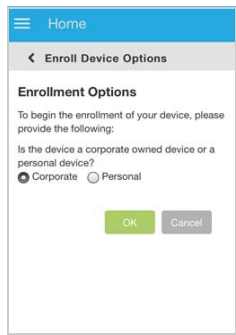
- 3 Tap **Enroll** in the upper-right corner to display the **Enroll Device Modes** screen.

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

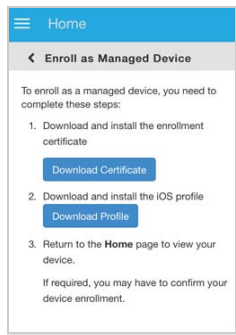
Enrollment Policy” on page 10, both options are available as shown below. Otherwise, only one of the two options is available.



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

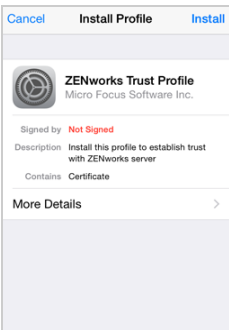


- 5 Click **OK** to enroll the device as a corporate device and display the **Enroll as Managed Device** screen.



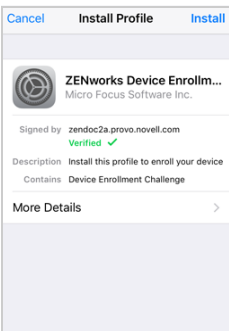
- 6 Tap **Download Certificate** to display the **Install Profile** screen, then tap **Install** and follow the prompts to install the certificate and return to the Enroll as Managed Device screen.

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

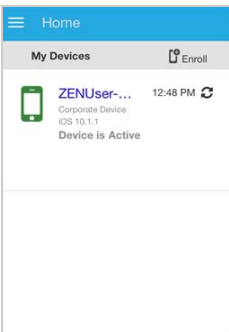


- 7 Tap **Download Profile** to display the following profile install screen, then tap **Install** and follow the prompts to install the profile and return to the Enroll as Managed Device screen.

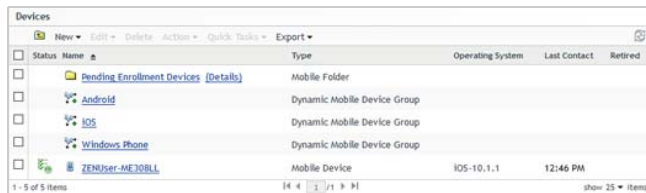
The ZENworks Device Enrollment Profile contains the MDM profile required for ZENworks to managed the device.



- 8 After the profile has finished installing, tap **Home** to return to the Home page.
- The enrolled device is displayed in the My Devices list.

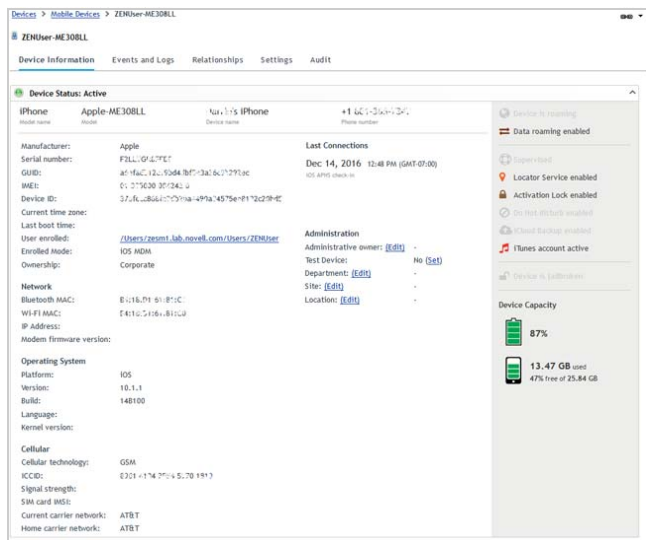


- In ZENworks Control Center, go to the **Devices > Mobile Devices** list to confirm that the device is enrolled in the zone.



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

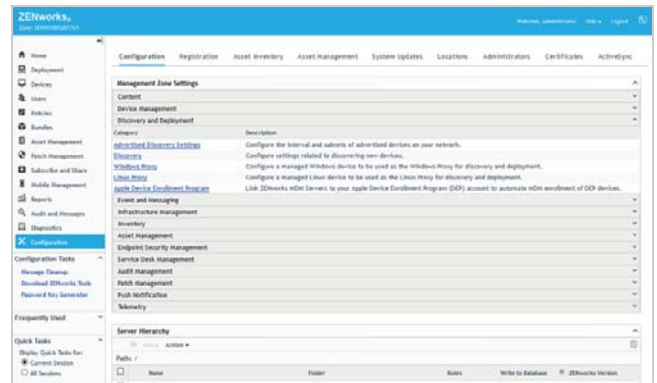
The Device Information page provides inventory details collected from the device.



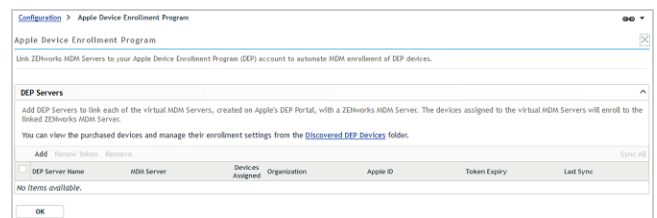
Linking Your MDM Server to the Apple Device Enrollment Program

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.

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



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



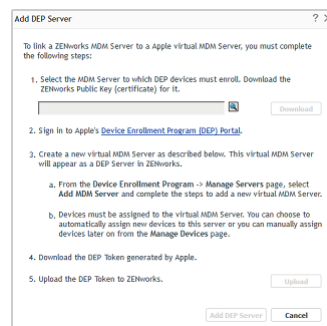
ENROLLING AN APPLE DEP IOS DEVICE


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.

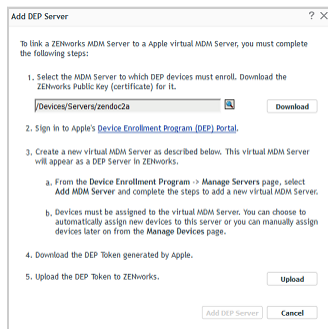
Using ZENworks Control Center, you configure setup options such as whether or not a device is supervised and what features (Location Services, Passcode, and so forth) are required to be configured at initial setup. Then, during the initial setup of a device, the device is configured according to your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

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.

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



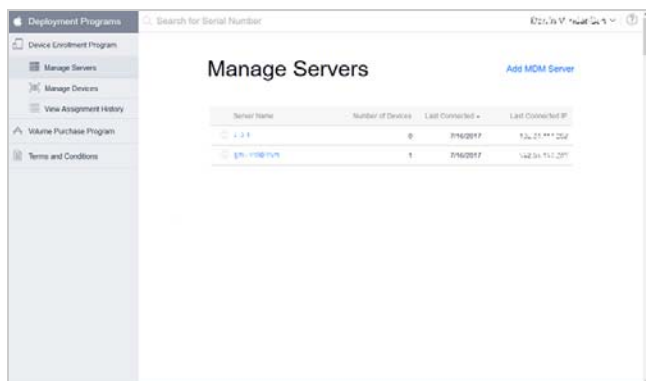
- 4 To select the MDM Server you want to designate as the DEP Server, click , then browse for and select the server.



- 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

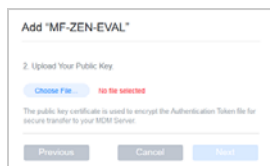
- 6 Click the **Device Enrollment Program (DEP) Portal** link, sign in to your Apple DEP account, then continue to the Manage Servers page.



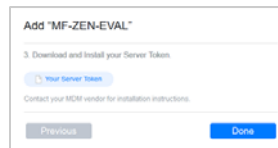
- 7 Click **Add MDM Server** to display the following dialog box.



- 8 Enter a name for your MDM Server. If you want any new devices that are added to your Apple Device Enrollment program to be assigned to the server, select **Automatically Assign New Devices**. Click **Next**.



- 9 Click **Choose File** to upload the key (`servername.der`) you generated in ZENworks Control Center for your MDM Server, then click **Next**.

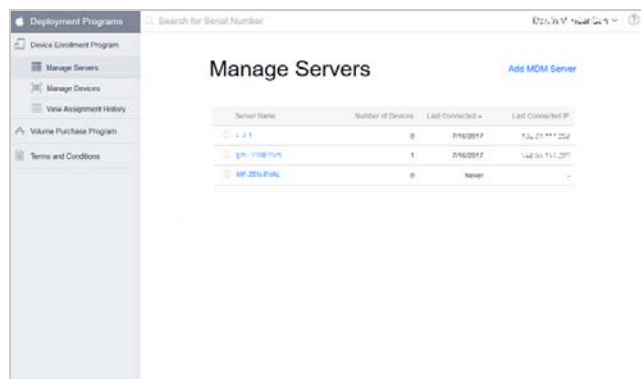


- 10 Click **Your Server Token** to download the Apple DEP token to your local drive.

The Apple DEP token file is saved with a name similar to the following:

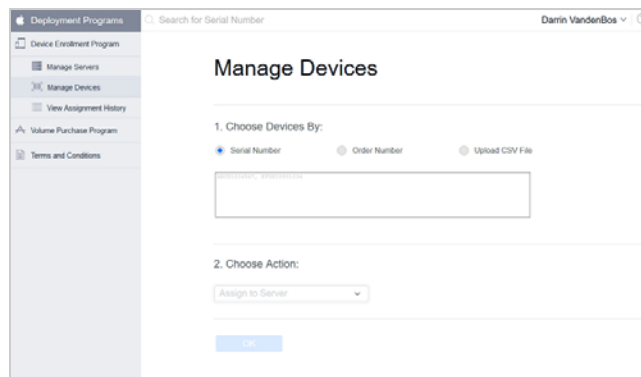
`MF-ZEN-EVAL_Token_2017-07-17T18-23-24Z_smime.p7m`

- 11 Click **Done** to add the server to the list of MDM Servers.




- 12 If you need to assign devices to the MDM Server, click **Managed Devices**, then assign the desired devices to the server.

For this evaluation, you need to have at least one unactivated device assigned to your MDM Server.

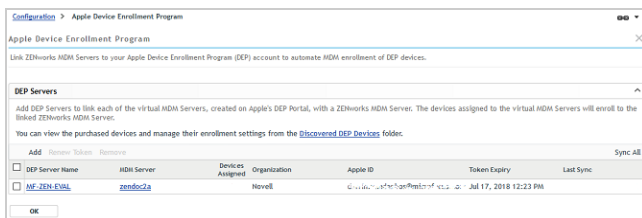


- 13 In ZENworks Control Center, you should still be in the Add DEP Server dialog box. Click **Upload** to upload the Apple DEP token (the .p7m file generated from the Apple Device Enrollment Program portal) for the MDM Server.

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

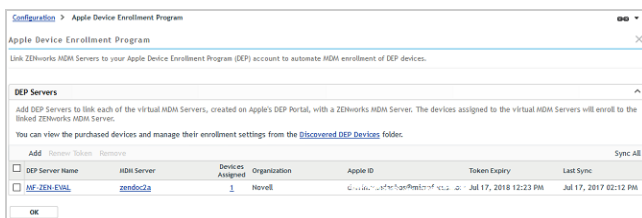


- 14 Click **Add DEP Server** to add it to the list.



- 15 In the DEP Servers list, click **Sync All** (located on the right side of the list's menu) to sync your 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.



- 16 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.

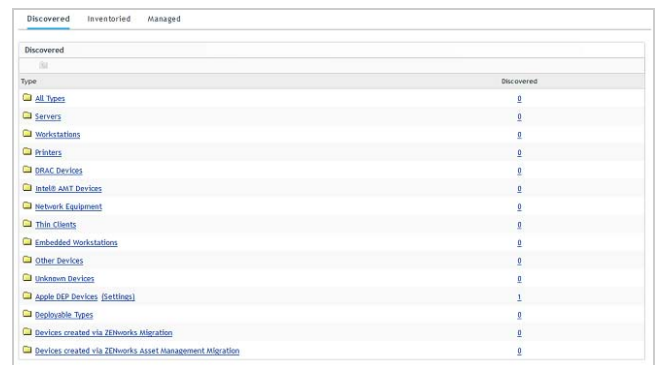
Configuring Apple Setup Options

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.

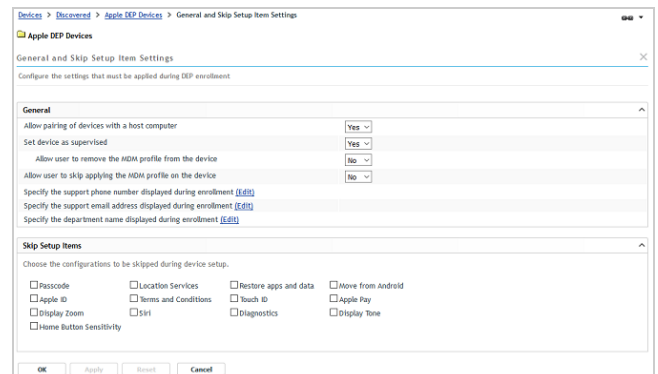
- 1 If the Apple DEP Devices list is still displayed, click **Discovered** (in the bread crumbs at the top) to display the Discovered devices list.

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.



- 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.



- 3 For this evaluation, change the following settings:

- 3a In the General section, add a support phone number, support email address, and department name.
- 3b In the Skip Setup Items, select **Location Services**, **Terms and Conditions**, **Touch ID**, and **Siri** so that those configurations are skipped during setup.
- 3c Leave all other options set to the defaults.

- 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 Now 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.

- Turn on the device and begin the setup process.
- When prompted for a login, specify the evaluation user's username and password.
- 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.

- On the device, tap  to display the Settings screen. Notice that the device is managed and supervised by your organization.



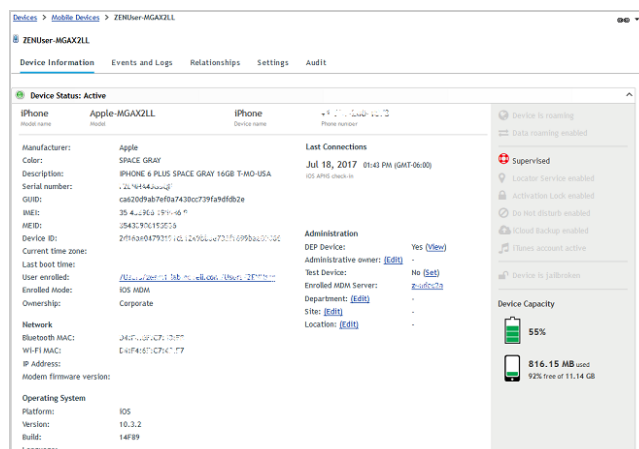
- In ZENworks Control Center, go to the device in the Discovered devices list (**Devices > Discovered > Apple DEP Devices**).

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
F2LNH44J050E	iPhone 6 Plus	SPACE GRAY	ZENuser	Assigned	MF-ZEN-EVAL	Managed

- (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

You can enroll any device running Android version 4.1 and newer. We used a Samsung Galaxy Tab 2 running Android version 4.2.2. Again, the screens and steps might vary slightly on other Android devices and versions.

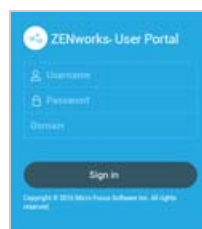
- In a Google Chrome browser on the Android device, enter the following URL:

`ZENworks_server_address/zenworks-eup`

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

Note: You must use Google Chrome. The native Internet browser is not supported. If you don't have Chrome on the device, download it from Google Play Store.

The login screen for the ZENworks User Portal is displayed.



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

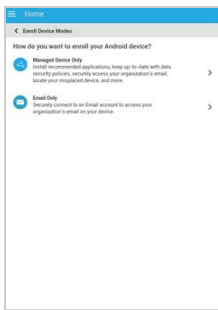
The Domain name field is not needed because the system is configured for simple enrollment, which allows users to log in with only their username rather than their full domain name.

The My Devices screen displays all devices that have been enrolled by the evaluation user. In this case, this includes the iOS device that you previously enrolled.



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

The enrollment options are determined by the Mobile Enrollment policy assigned to the user. If you configured the policy as recommended in [Creating a Mobile Enrollment Policy \(page 10\)](#), both options are available as shown below. Otherwise, only one of the two options is available.

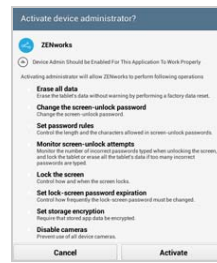


- 4 Tap **Managed Device Only**.



- 5 Tap **Download App**, then click Play Store (if prompted) to display the ZENworks Agent app in the Google Play Store.
- 6 Tap **Install**, then tap **Accept** to start the installation.

- 7 When the app is finished installing, tap **Open**.



ZENworks must be a device administrator in order to manage the device.

- 8 Tap **Activate** to allow the ZENworks Agent app to perform the listed operations.

The ZENworks Mobile login screen is displayed.



- 9 Fill in the evaluation user's username and password, fill in the URL of the ZENworks Primary Server, then tap **Sign In**.

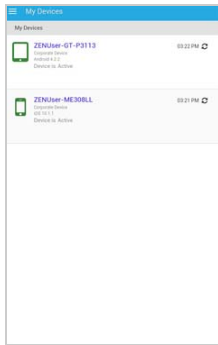
As with the ZENworks User Portal login, the Domain name field is not needed because the system is configured for simple enrollment, which allows users to log in with only their username rather than their full domain name.

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.

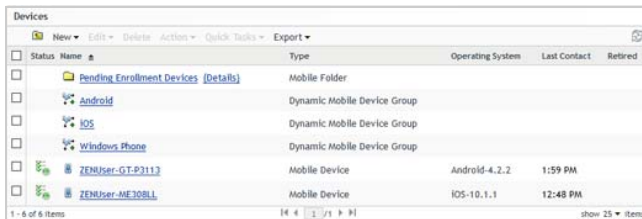


- 10 Click **OK** to enroll the device as a corporate device.

When enrollment is complete, the Android device is listed in the mobile app along with the iOS device (if you enrolled one previously).

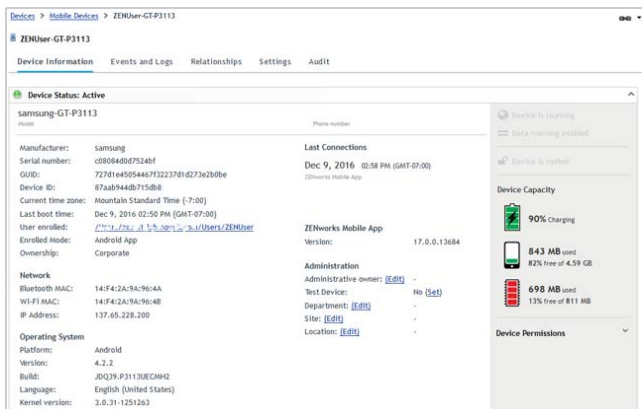


- 11 In ZENworks Control Center, go to the **Devices > Mobile Devices** list to confirm that the device is enrolled in the zone.



- 12 (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.



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.

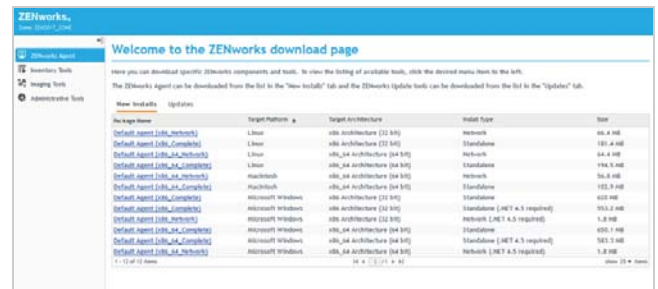
To enroll a Windows device in the zone, you install the ZENworks Agent on the device. The agent then contacts the ZENworks Primary Server and completes the enrollment.

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.




- 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.

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

- 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*.

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 checked="" type="checkbox"/>	DESKTOP-A7JSKD0	Workstation	windows10-ent-gen-x64	2:41 PM	

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

The Summary page provides details about the device.

General	
Alias:	DESKTOP-A7JSKD0
Host Name:	DESKTOP-A7JSKD0
IP Address:	137.65.57.28
Test Device:	No (Set)
Last Full Refresh:	2:41 PM
Last Contact:	2:41 PM
ZENworks Agent Version:	17.0.6.1222
ZENworks Updater Service Version:	17.0.6.1187
ZENworks Agent Status:	
Operating System:	Microsoft Windows 10 Enterprise x64 10.0 N/A Build
Number of errors not acknowledged:	0
Number of warnings not acknowledged:	0
Primary User:	/Users/zsaml.lab.novell.com/Users/ZENworks
Owner:	
Serial Number:	56aff6f1e4b0e8a7b786d784c19
GUID:	969d36c3c1b7948ac6412b1d6c1a738
Department:	
Site:	
Location:	

Upcoming Events	
12/18/16	
Refresh	
Type Name	Time
Click refresh to see upcoming events	

Logged In Users	
Name	In Folder
/Users/zsaml.lab.novell.com/Users	
1 - 1 of 1 items	

Imaging Work	
Scheduled Work:	None
Applied Image Files:	None
Type Name	No items available.

Assigned System Updates	
Name	Status
No items available.	

Message Log	
Status	Message
Click refresh to see the events	

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.

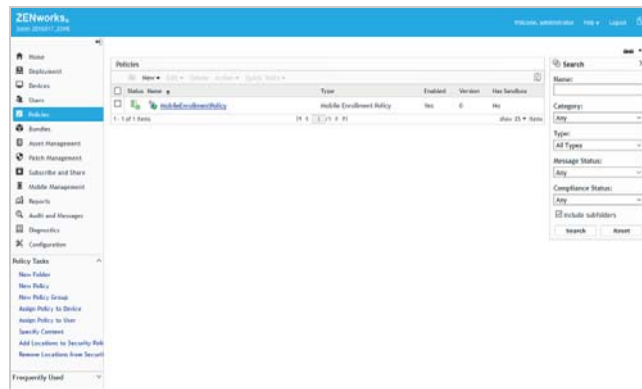
- ♦ Applying a Security Policy to Mobile Devices (page 19)
- ♦ Applying a Control Policy to Mobile Devices (page 21)

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

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



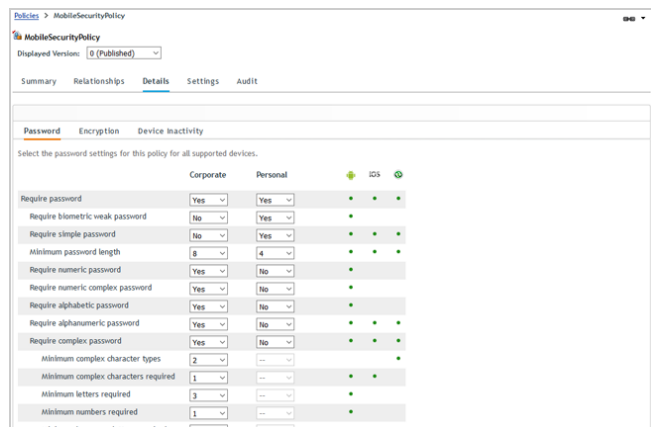
- 2 Click **New > Policy** to display the Create New Policy wizard.
- 3 On the Select Platform page, select **Mobile**, then click **Next**.
- 4 On the Select Policy Category page, select **General Mobile Policies**, then click **Next**.
- 5 On the Select Policy Type page, select **Mobile Security Policy**, then click **Next**.
- 6 On the Define Details page, specify *MobileSecurityPolicy* for the policy name, then click **Next**.

- 7 On the Select Security Level page, leave the default settings, then click **Next**.

The security policy includes dozens of settings. So that you don't have to deal with them individually, you select the security level you want and ZENworks populates the settings with the values appropriate to the level.

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

You can now see the individual settings and change them...except, don't change them for this 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

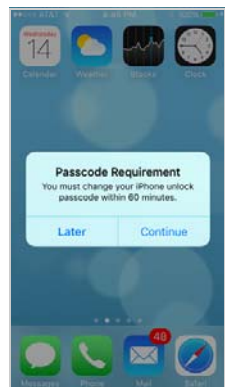
This policy can be assigned to either users or devices. We'll have you assign it to the evaluation user so that the policy will apply to both the user's iOS device and Android device. If you were to use a device assignment, you would need to assign it to both the iOS device and the Android device.

- 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.

Testing the Mobile Security Policy on an iOS Device

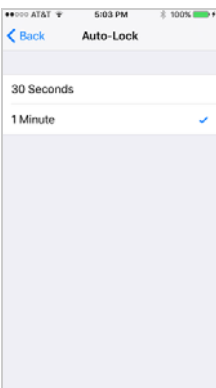
After the policy is assigned to the evaluation user, ZENworks refreshes the device so that the policy can be enforced. On iOS devices, if the policy requires the user to change something, such as the passcode, the user is prompted.

- 1 On the iOS device, wait for the following prompt to be displayed.

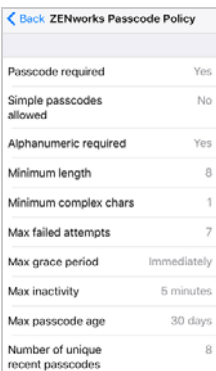


- 2 Tap **Continue**, then follow the prompts to change the passcode to meet the policy requirements.
- 3 Verify the inactivity timeout setting by tapping **Settings > Display & Brightness > Auto-Lock**.

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**.

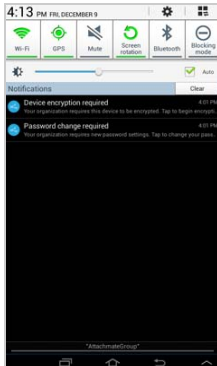


Testing the Mobile Security Policy on an Android Device

After the policy is assigned to the user, the user's Android device receives a ZENworks notification for each device setting that the user needs to change in order to meet the policy requirements. This notification should be almost immediate.

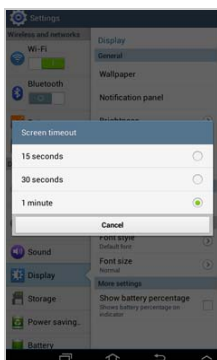
- 1 Go to the Notification area to display the ZENworks notifications.

On the device shown below, there are two individual security settings that need attention. Depending on the security settings for your device, the number and type might be different.



- 2 Tap the notifications to take care of the changes that need to be made.
- 3 Verify the inactivity timeout setting by tapping **Settings** > **Display** > **Screen timeout**.

The Mobile Security policy's *Strict* security level changes the setting to a maximum of 1 minute.



The policy also enforces the following requirements that you can verify if you'd like:

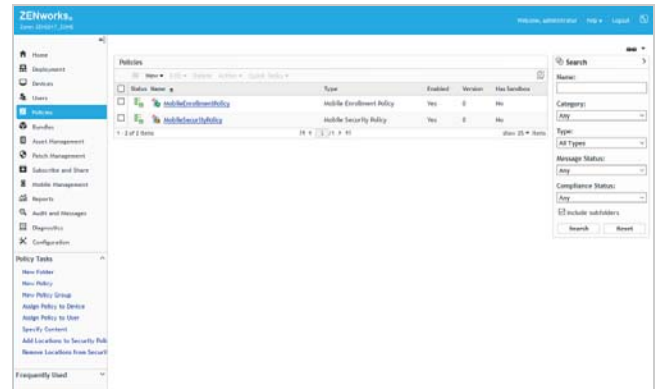
- ♦ Password expiration every 30 days
- ♦ Password history of last 7 passwords

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 *MobileDeviceControlPolicy* 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**.

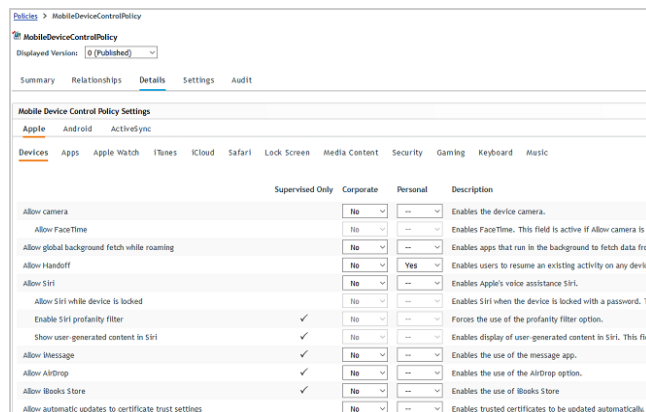
The device control policy includes over 50 settings. So that you don't have to deal with them individually, you select the control level you want and ZENworks populates the settings with the values appropriate to the level.

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

You can now see the individual settings and change them...except, don't change them for this evaluation. After you've finished the evaluation, go ahead and change whatever you want as you play and explore more.

As you explore the settings for Apple (iOS), Android, and ActiveSync, you'll notice that there are a lot more settings to control iOS devices at this time than there are for Android or ActiveSync-only devices. More Android and ActiveSync settings will come in future releases.

Also, notice that there are some Apple (iOS) settings that apply only to supervised devices.



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.

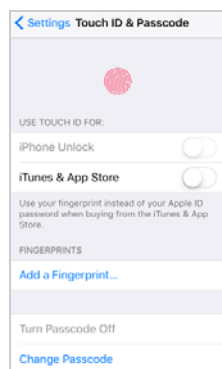
Testing the Mobile Device Control Policy on an iOS Device

- 1 Verify that the camera no longer works on the device.

The policy removes the Camera app from the device. It also disables the other standard ways to access the camera such as from the Lock Screen and the Control Center.

- 2 Verify that the Touch ID setting has been disabled by tapping **Settings**, tapping **Touch ID & Passcode**, and then entering the device's passcode.

The Mobile Device Control policy's *Strict* security level turns off the Touch ID for iPhone Unlock setting and then locks the setting so that it cannot be changed on the device.



- 3 To see a full list of the device control restrictions enforced by the policy, tap **Settings** > **General** > **Profiles & Device Management** > **ZENworks Management Profile** > **Restrictions**.



Testing the Mobile Device Control Policy on an Android Device

Currently, the Mobile Device Control policy on Android devices is limited to disabling the camera.

- 1 Tap the Camera app.

The policy blocks the camera and displays a message similar to the one in the following screenshot.



Secure Your Windows Device

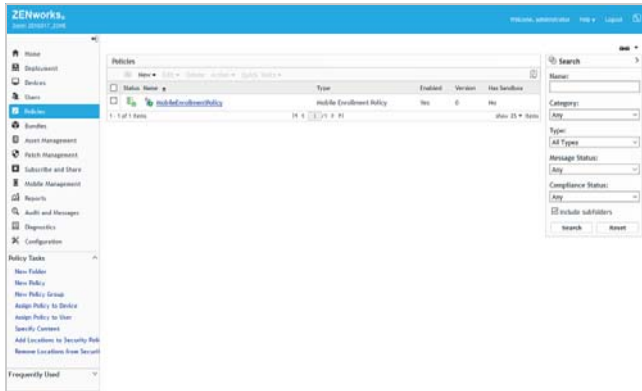
ZENworks lets you control the Windows Group policy to secure devices. In this evaluation, we'll use the Windows Group policy to enforce a complex password on your Windows device.

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 \(page 23\)](#)
- [Assigning the Windows Group Policy \(page 23\)](#)
- [Testing the Windows Group Policy \(page 23\)](#)

CREATING THE WINDOWS GROUP POLICY

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

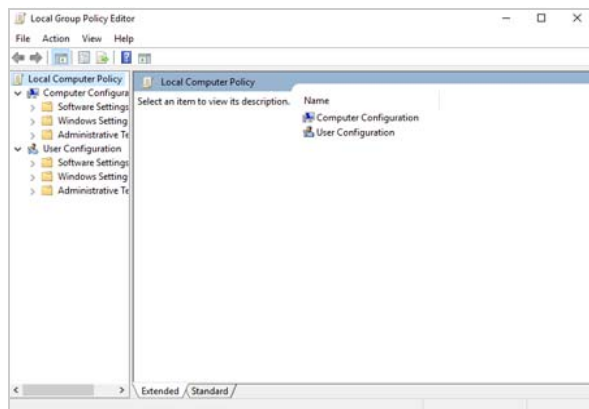


- 2 Click **New > Policy** to display the Create New Policy wizard.
- 3 On the Select Platform page, select **Windows**, then click **Next**.
- 4 On the Select Policy Category page, select **Windows Configuration Policies**, then click **Next**.
- 5 On the Select Policy Type page, select **Windows Group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

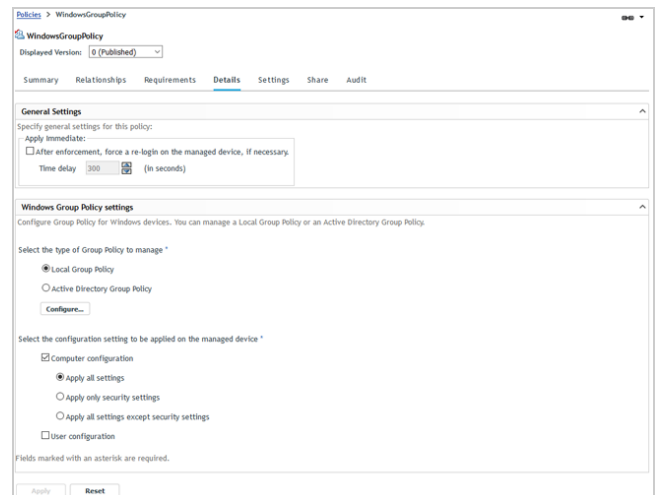
The path to the Password Policy is:

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

Currently, ZENworks supports distributing of applications to iOS devices. Don't worry, though, we are working on support for Android apps in our coming releases!

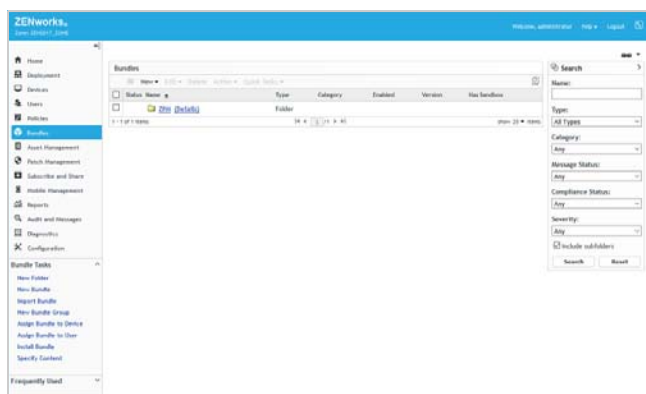
- Distributing an Apple App Store App to an iOS Device (page 24)
- Distributing an Apple VPP App to an iOS Device (page 25)

DISTRIBUTING AN APPLE APP STORE APP TO AN IOS DEVICE

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

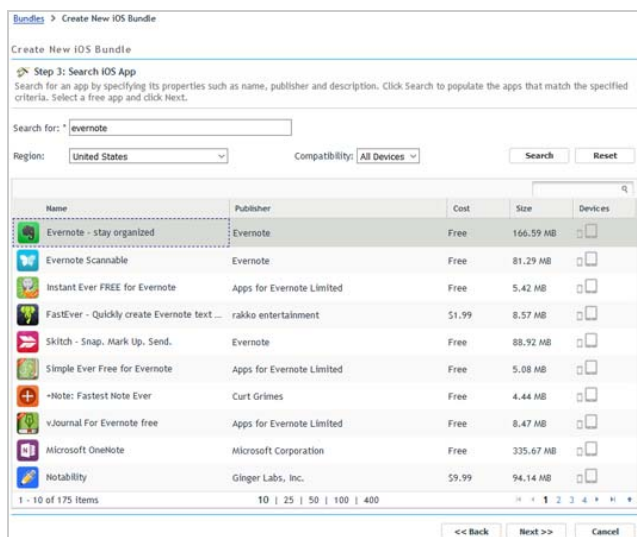
Creating a Bundle for the App Store App

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

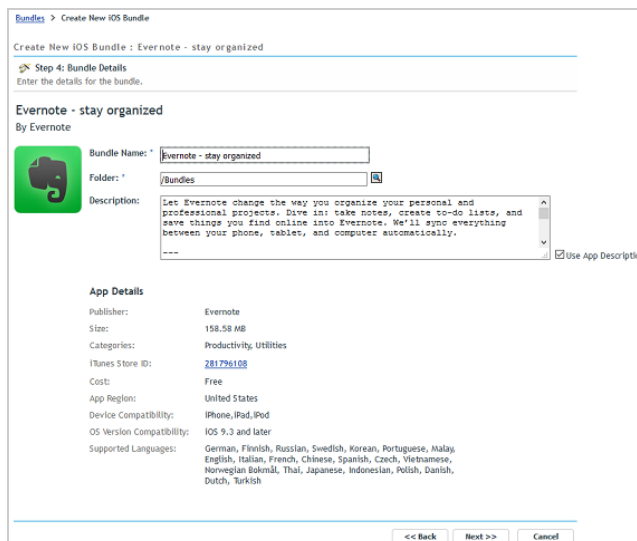


- 2 Click **New** > **Bundle** to display the Create New Bundle wizard.
- 3 On the Select Bundle Type page, select **iOS Bundle**, then click **Next**.
- 4 On the Select Bundle Category page, select **App Store** App, then click **Next**.

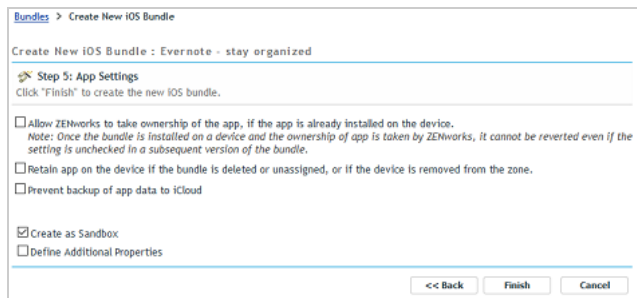
- 5 On the Search iOS App page, enter *Evernote* in the **Search for** box, select your region, then click **Search**.
ZENworks returns a list of App Store apps that match the search criteria.



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

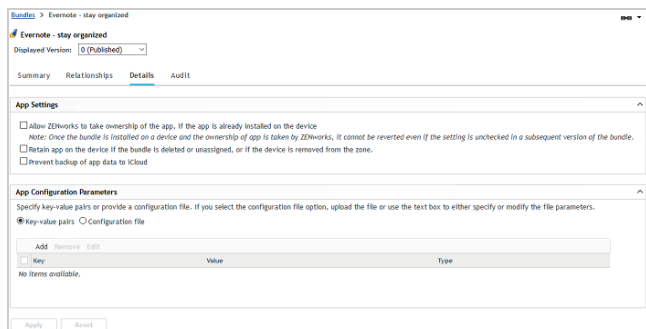


- 7 On the Bundle Details page, review the details, then click **Next** to display the App Settings page.



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.



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.



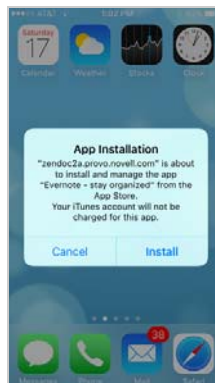
The App Installation Schedule page lets you determine if you want to push the bundle to the device now (upon completion of the assignment to the device) or let the device find out about the bundle the next time it refreshes information from the ZENworks zone.

- 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

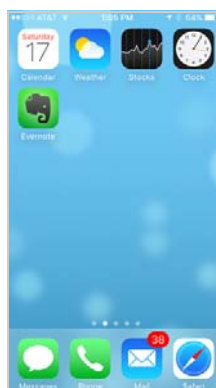
When the bundle is distributed to your iOS device, a notification is displayed on the device.



- 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.



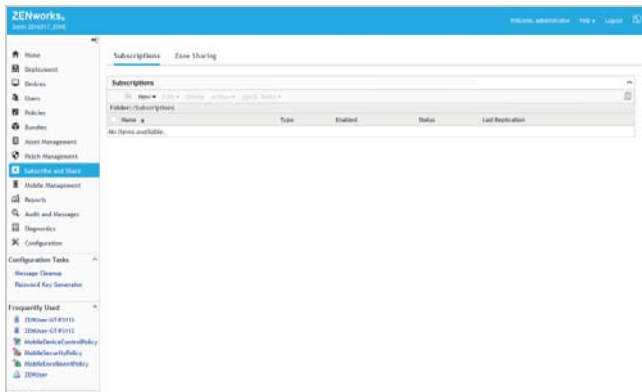
DISTRIBUTING AN APPLE VPP APP TO AN IOS DEVICE

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.

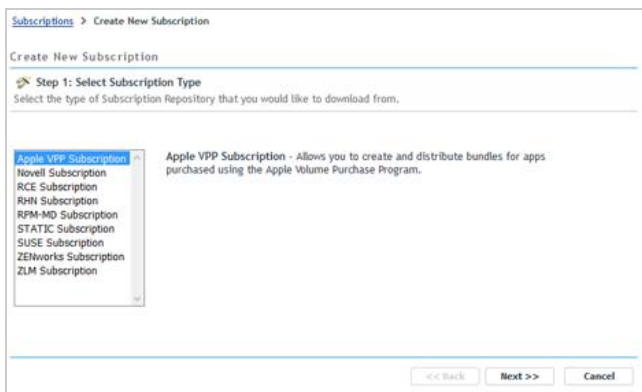
Connecting to Apple VPP

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).

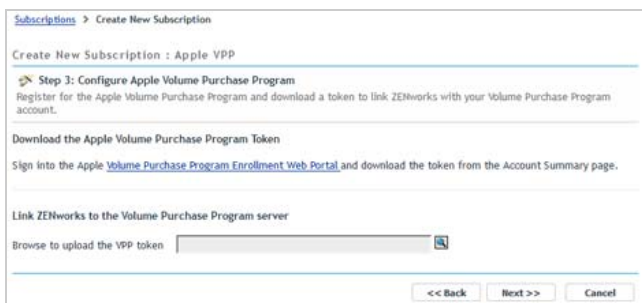


- 2 In the Subscriptions list, click **New > Subscription** to display the Create New Subscription wizard.



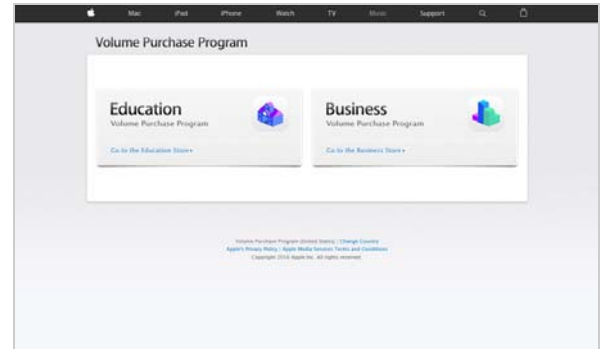
- 3 On the Select Subscription Type page, select **Apple VPP Subscription**, then click **Next**.

- 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.



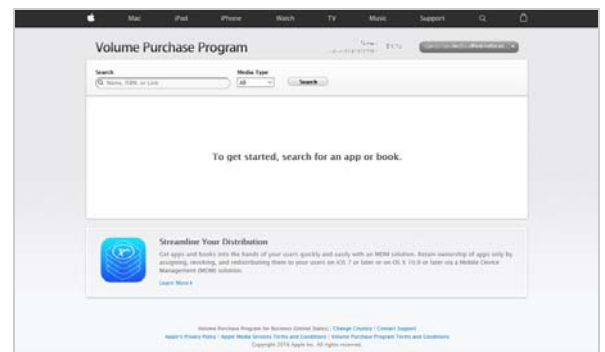
- 5 Download an Apple VPP token from your VPP account:

- 5a Click the **Volume Purchase Program Enrollment Web Portal** link to display the Apple volume Purchase Program web site.

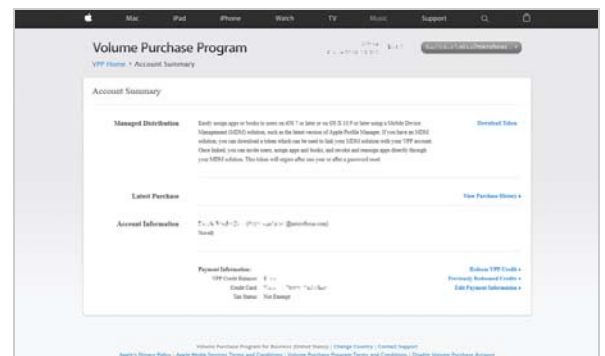


- 5b Click **Go to the Education Store** or **Go to the Business Store** depending on the type of account you have.

- 5c Sign in with your Apple ID and password.



- 5d Click your username in the list in the upper right, then click **Account Summary**.



- 5e Click **Download Token**, then follow the prompts to download the token file.

- 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 **Apple VPP** 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.

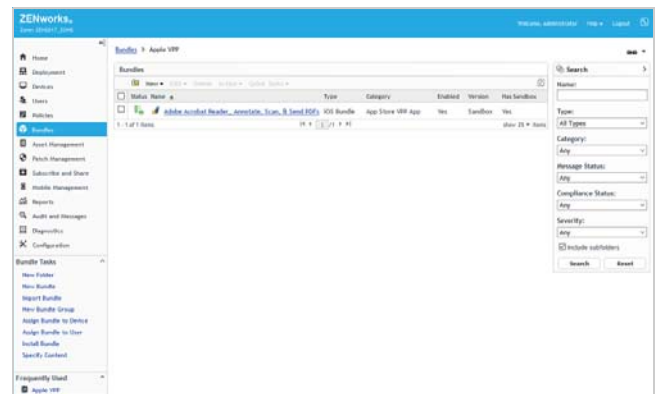
If for some reason your apps are not listed, click the refresh icon  to update the list.

Action	App	Publisher	Cost	Subscription Name	Purchased	Consumed	Available	User License Installed	User License Consumed	Device License Installed	Total Bundles
<input type="checkbox"/>	Sticky - Beautiful Not...	Thomas Greany	Free	Apple VPP	5	0	5	0	0	0	0
<input type="checkbox"/>	Microsoft Word	Microsoft Corp	Free	Apple VPP	5	0	5	0	0	0	0
<input type="checkbox"/>	Microsoft Excel	Microsoft Corp	Free	Apple VPP	5	0	5	0	0	0	0
<input type="checkbox"/>	Google Docs	Google, Inc.	Free	Apple VPP	5	0	5	0	0	0	0
<input type="checkbox"/>	Google Slides	Google, Inc.	Free	Apple VPP	20	0	20	0	0	0	0
<input type="checkbox"/>	GoToMeeting	Claris Online LLC	Free	Apple VPP	10	0	10	0	0	0	0
<input type="checkbox"/>	Adobe Acrobat Reader	Adobe Systems, Inc.	Free	Apple VPP	20	0	20	0	0	0	0

- 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.

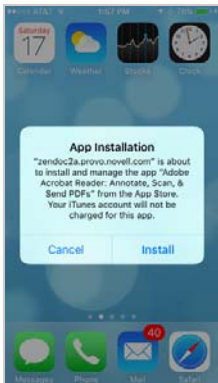


- 5 Click the bundle to display its details.
- 6 Assign the bundle to your managed iOS device:
 - 6a In the Device Assignments list, click **Add**.
 - 6b Use the Select Objects dialog to add the iOS device to the assignment list, then click **Next** to display the App Installation Schedule page.
The 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.
 - 6c 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.
 - 6d Select Device Precedence, then click **Next** to display the Summary page.
 - 6e 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.



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.

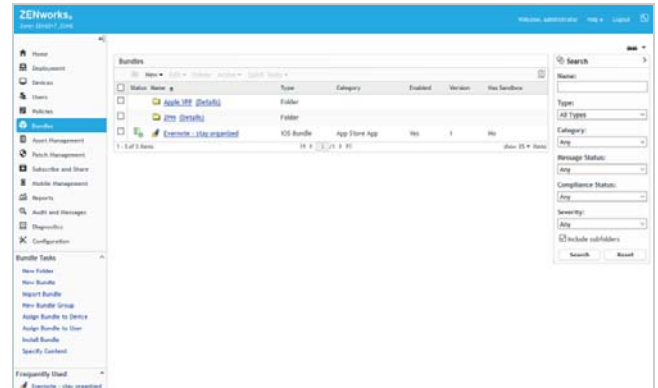
- ♦ "Creating the Windows Bundle" on page 28
- ♦ "Testing the Windows Bundle" on page 30

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_6.4.2.3788.exe.

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

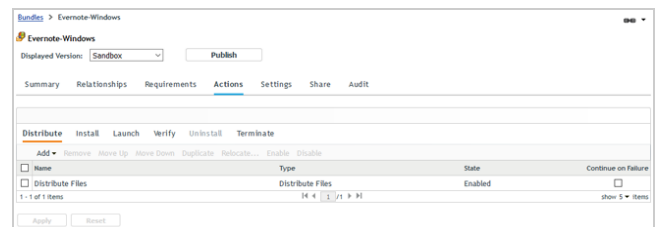


- 3 Click **New > Bundle** to display the Create New Bundle wizard.
- 4 On the Select Bundle Type page, select **Windows Bundle**, then click **Next**.
- 5 On the Select Bundle Category page, select **(Empty Bundle)**, then click **Next**.

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.

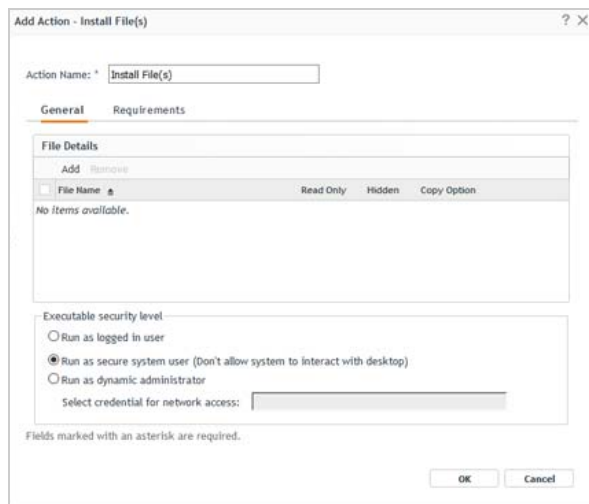


- 8 In the Actions list, click **Install**.



- 9 Create an action that copies the Evernote installation package to the Windows device:

- 9a Click **Add > Install File(s)** to display the Add Action - Install File(s) dialog.



- 9b In the File Details list, click **Add** to display the Select Files dialog.

- 9c In the File list, click **Add**, then upload the Evernote installation package.

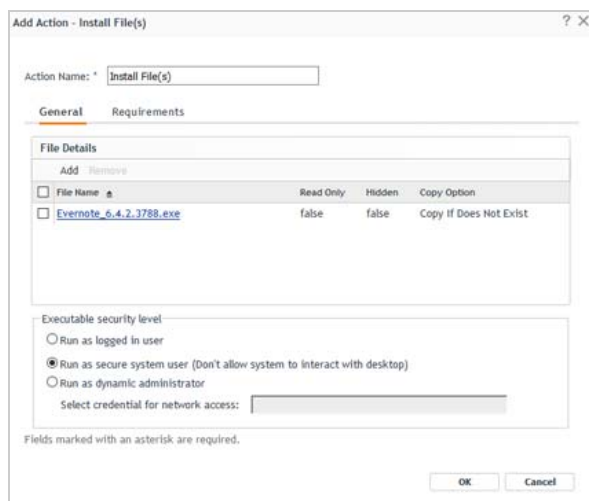
The file is uploaded to the ZENworks server's content repository. It can then be distributed from the repository to the Windows device.

- 9d In the Destination Directory, enter `c:\`.

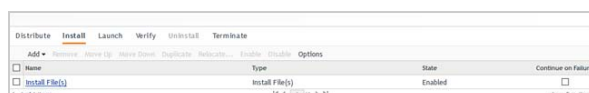
This is the location on the Windows device where the installation package will be copied.

- 9e In the Copy Option list, select **Copy if Does Not Exist**.

- 9f Click **OK** to add the file to the File Details list.



- 9g Click **OK** to add the action to the Install list.



- 10 Create an action that launches the Evernote installation on the Windows device:

- 10a Click **Add > Launch Executable** to display the Add Action - Launch Executable dialog.

- 10b In the Command field, enter:

`c:\evernote_installation_package`

For example:

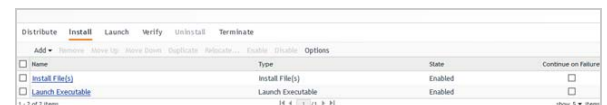
`c:\Evernote_6.4.2.3788.exe`

- 10c Click **Advanced**, then select **When action is complete** so that the next bundle action will not start until the installation has completed.

The next action (after the installation) will be to remove the installation package from the device. Using this option ensures that the file removal won't happen until after the installation is complete.



- 10d Click **OK** to add the action to the Install list.



- 11 Create an action that deletes the Evernote installation package from the Windows device after the installation is complete:

- 11a Click **Add > File Removal** to display the Add Action - File Removal dialog.

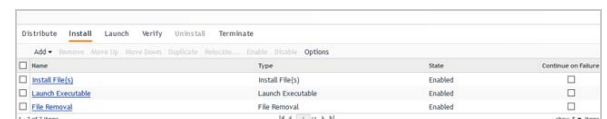
- 11b In the Full Path to Source Files/Directories field, enter the following, then click **Add** to add the file to the list.

`c:\evernote_installation_package`

For example:

`c:\Evernote_6.4.2.3788.exe`

- 11c Click **OK** to add the action to the Install list.



- 12 In the Actions list, click **Launch**.



- 13 In the Launch list, click **Options** to display the Launch Options dialog.

The bundle installs the Evernote application. After it is installed, you will use the application's shortcut to launch 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.




- 14 Click **Run once**, select the **for each device** option, then click **OK**.
- 15 Click **Apply** to save the changes you've made to the bundle's actions.
- 16 Assign the bundle to your managed Windows device:
 - 16a Click the **Relationships** tab.
 - 16b In the Device Assignments list, click **Add**, then follow the prompts to assign the bundle.

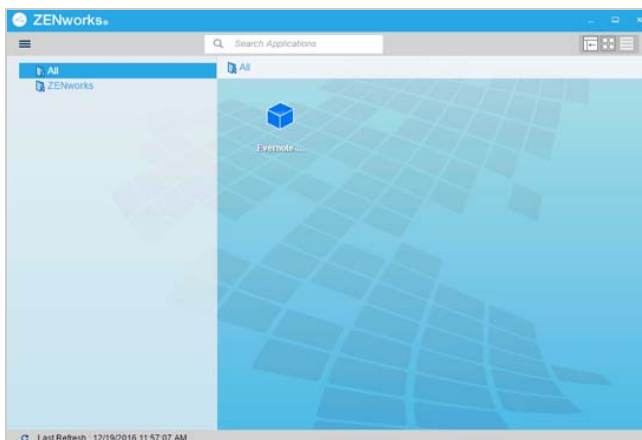
As you go through the assignment wizard, keep the default setting.

- 17 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 start the installation process.
- 4 Follow the prompts to install the application.

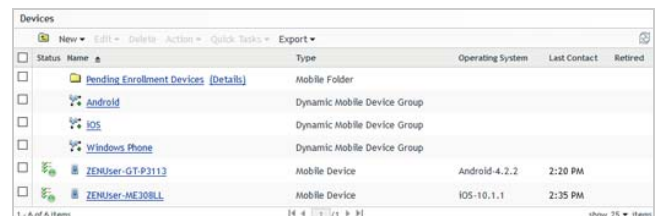
When the installation is complete, an Evernote shortcut is added to the desktop and the Evernote bundle is removed from the ZENworks application window.

You can also use Windows Explorer to verify that the Evernote installation package was removed from c:\ after the installation.

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.

Status	Name	Type	Operating System	Last Contact	Retired
<input type="checkbox"/>	Pending Enrollment Devices (Details)	Mobile Folder			
<input type="checkbox"/>	Android	Dynamic Mobile Device Group			
<input type="checkbox"/>	iOS	Dynamic Mobile Device Group			
<input type="checkbox"/>	Windows Phone	Dynamic Mobile Device Group			
<input checked="" type="checkbox"/>	ZENworks-GT-P3113	Mobile Device	Android-4.2.2	2:20 PM	

- 7 If you unenrolled an iOS device, verify that the unenrollment tasks have initiated or completed:

Full Wipe: The device has been reset using the *Erase all Content and Settings* option.

Selective Wipe: The ZENworks Management Profile and all policy restrictions have been removed (**Settings > General > Profiles**). All App Store apps have been uninstalled, unless you selected the *Retain App on Unenrollment* option when distributing them. All Apple VPP apps have been uninstalled.

- 8 If you unenrolled an Android device, verify that the unenrollment tasks have initiated or completed:

Full Wipe: The device has been reset using the *Erase all Content and Settings* option.

Selective Wipe: The policy restrictions have been removed. The device has received a notification stating that it has been unenrolled and that ZENworks needs to be uninstalled. Tap the notification to delete the ZENworks application.

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.

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 checked="" type="checkbox"/>	DESKTOP-A7JSDQ	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 Micro Focus Software Inc. All Rights Reserved.

