Windows Intune Walkthrough: Windows Phone 8 Management

This document will review all the necessary steps to setup and manage Windows Phone 8 using the Windows Intune service.

Note: If you want to test the Windows Phone 8 management experience with a Windows Intune trial account you can use our sample Company Portal application and test Windows Phone 8 sample applications here: http://www.microsoft.com/en-us/download/details.aspx?id=39079. If you are using the sample Company Portal skip to the section Configuring your Windows Intune Account and signing/publishing the Company Portal. The sample Company Portal only works with Trial Accounts.

What exactly are we going to review?

- The requirements to setup Windows Phone 8 management
- Purchasing and importing a Symantec Enterprise Code Signing Certificate
- Configuring your Windows Intune account and signing/publishing the Company Portal
- Enrolling a Windows Phone 8 device into Windows Intune

In order to successfully setup and manage Windows Phone 8 devices a few things are needed:

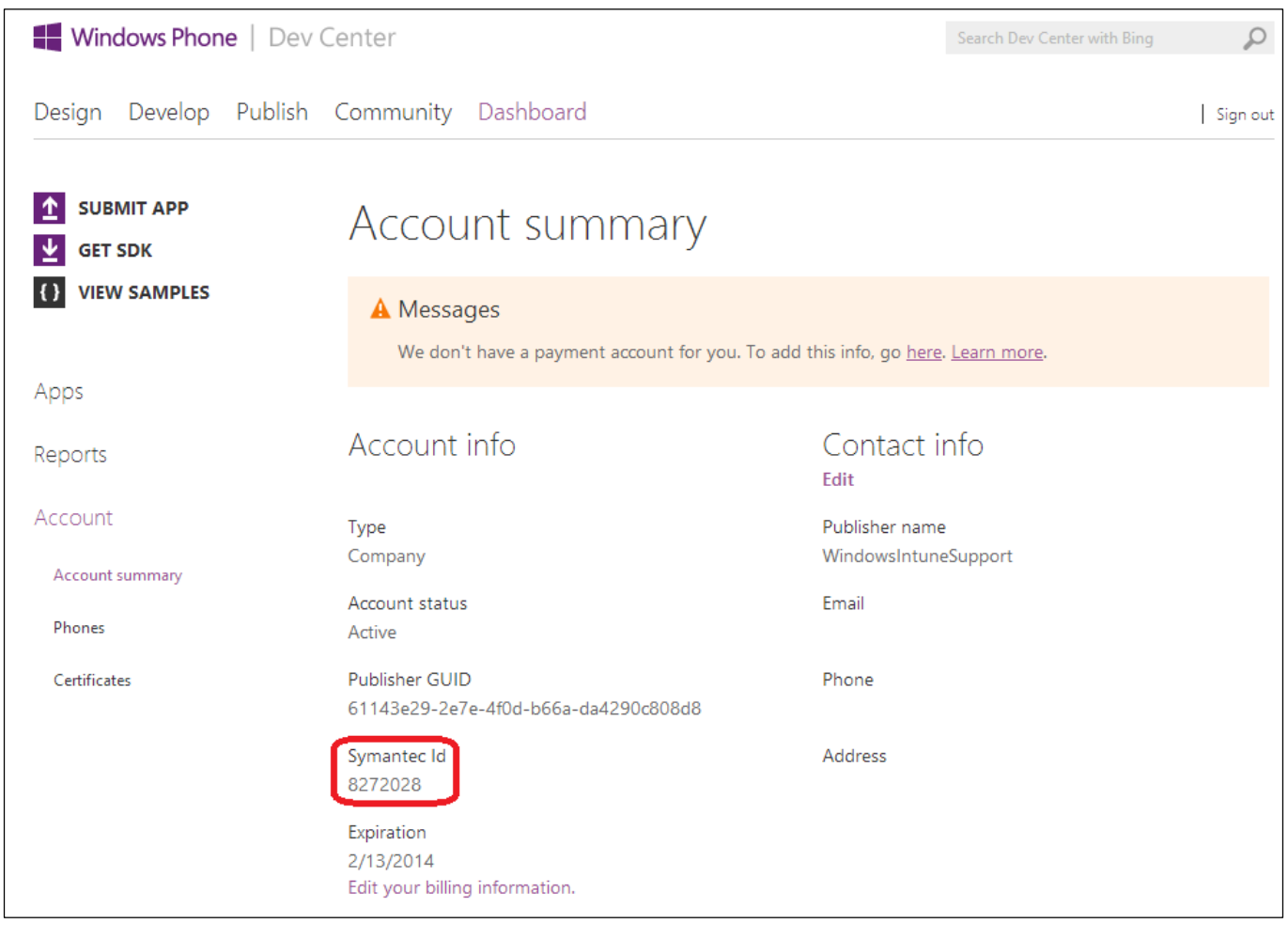
- A Windows Intune Paid account
- A Corporate Windows Phone Developer Account (personal accounts are not supported)
    - If you need a Corporate Windows Phone Developer Account you can get one here: https://dev.windowsphone.com/en-us/join
- A valid Credit Card to purchase a Symantec Code Signing Certificate ($299)
- A Windows 8 x64 machine
- Visual Studio 2012 Express or higher with the Windows Phone 8 SDK (we'll review installing the Visual Studio 2012 Express version)
- A Windows Phone 8 handset or virtual Windows Phone 8 device

Let's get started!

Purchasing and importing a Symantec Enterprise Code Signing Certificate

First, let's log into our Windows Phone Developer account. You can reach your Windows Phone Developer account by navigating to http://dev.windowsphone.com

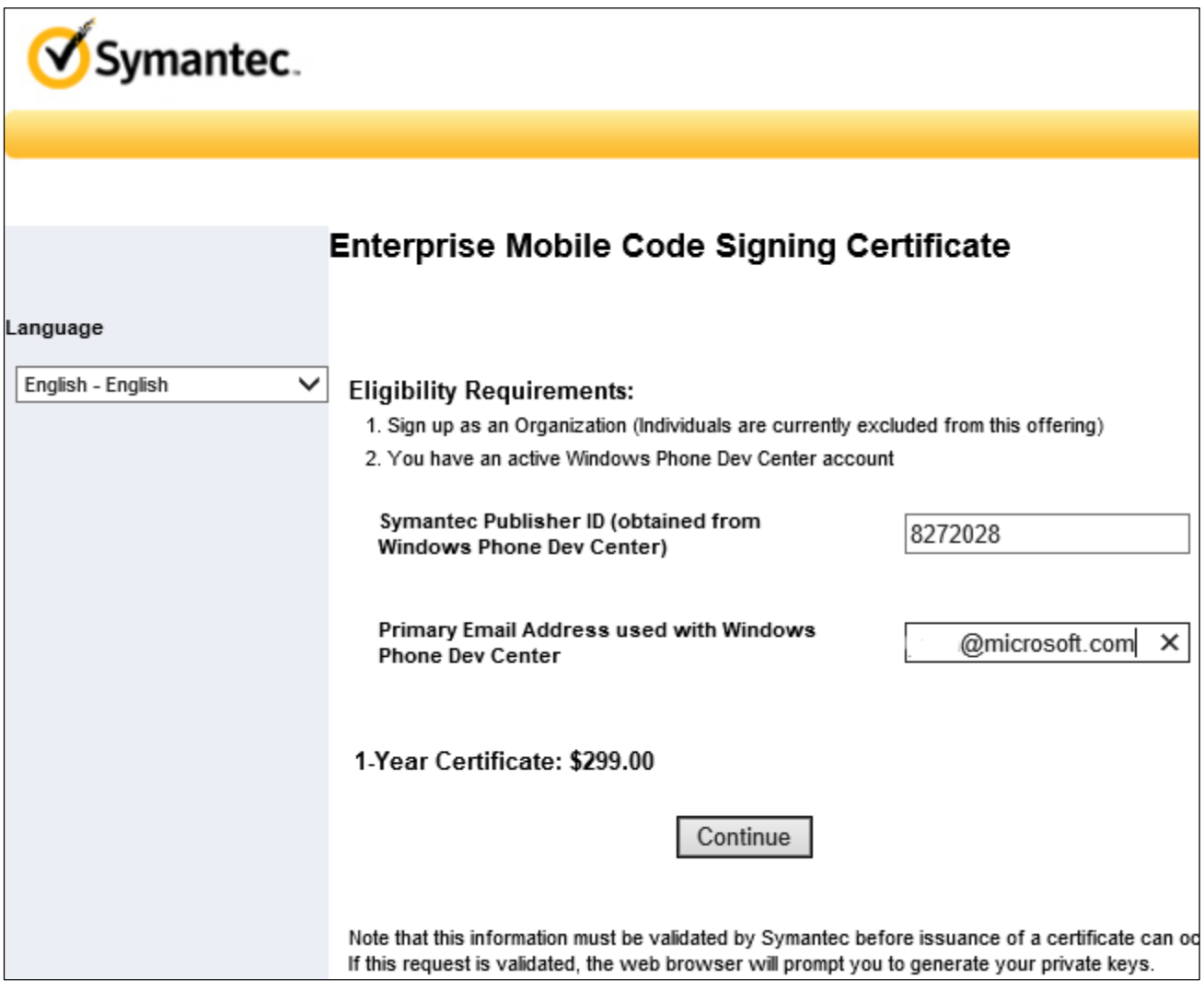
If you do not have a Windows Phone Developer account please use the same link above to create a company account. Once you have logged in to your Windows Phone Developer account please navigate to the dashboard and open account summary. If your account is fully setup you'll have a Symantec ID. Remember that ID as we'll need it in a moment.



Now that we have our Symantec ID, let's head over to the Symantec Enterprise Mobile Code signing certificate website so we can purchase our certificate

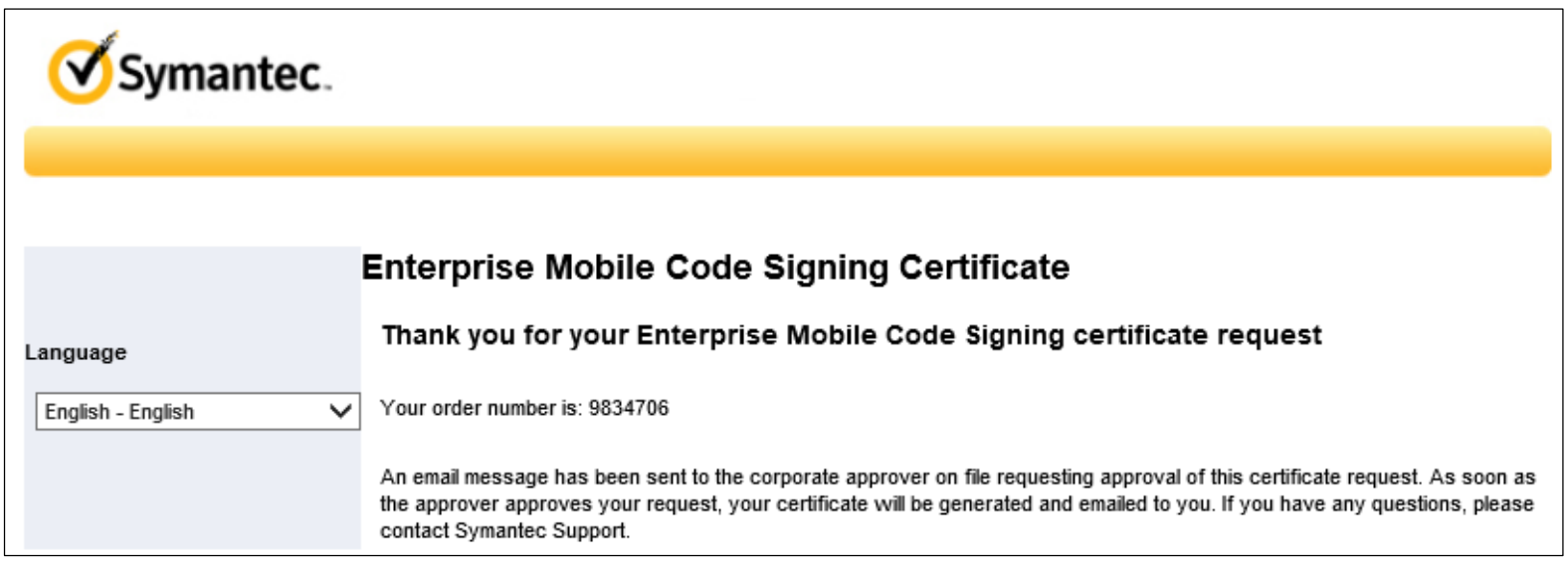
Open a web browser to https://products.websecurity.symantec.com/orders/enrollment/microsoftCert.do

On the Symantec Website enter your Symantec Publisher ID that we wrote down from our Windows Phone Developer account and the primary email associated with the Windows Phone Developer account

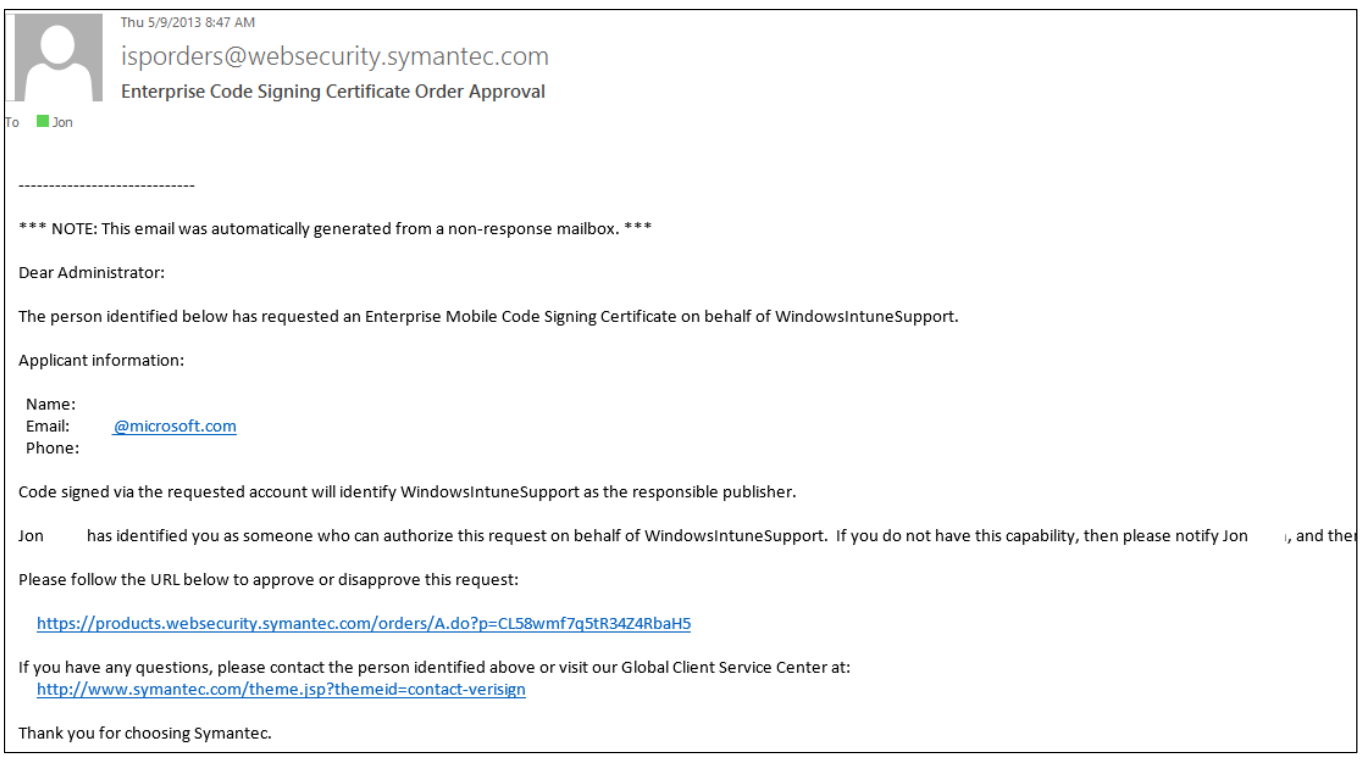


Once you hit continue, you'll navigate to a standard order page where you need to fill out all your information.

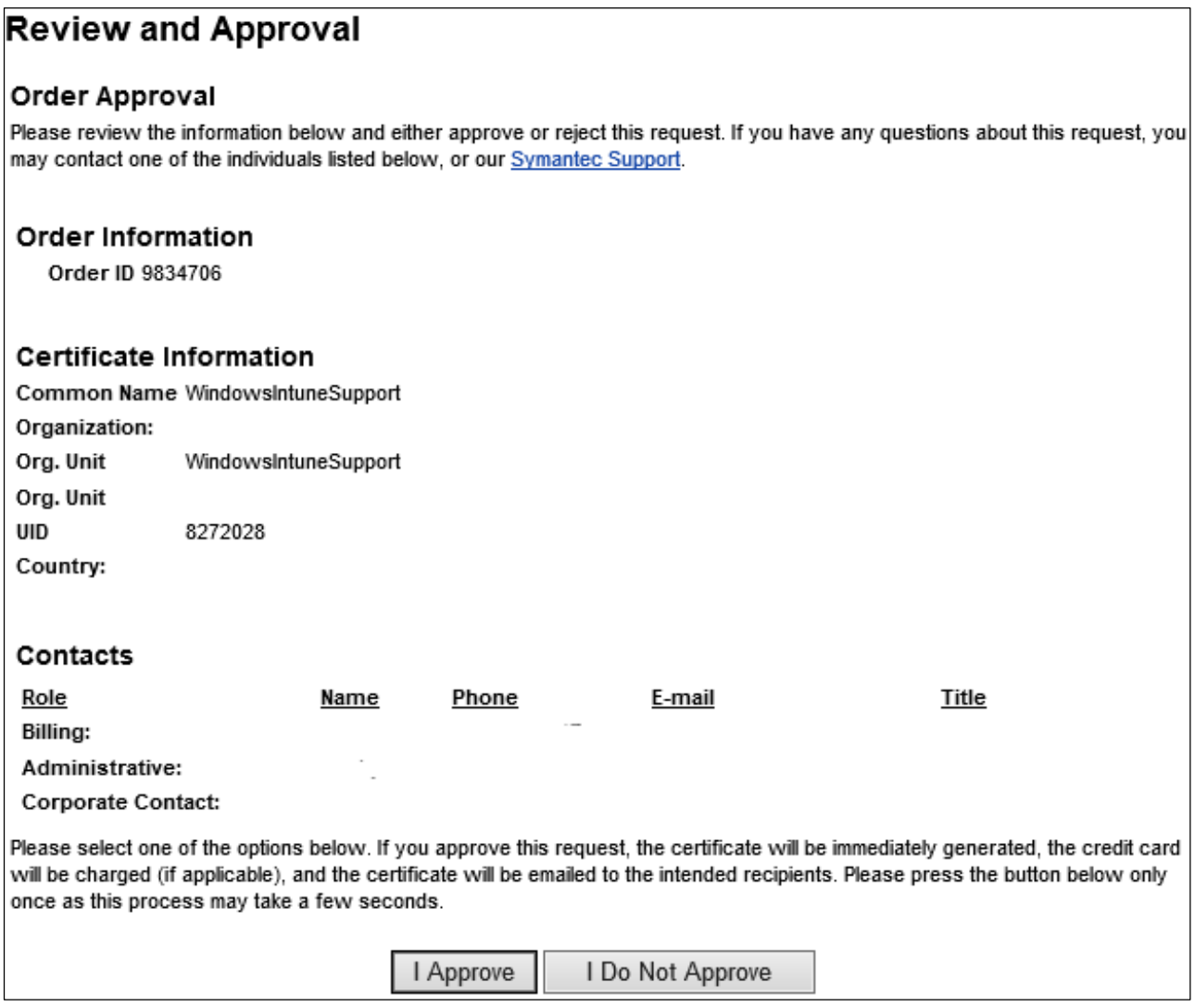
After you submit your information the order will be sent to Symantec. We're not quite done though.

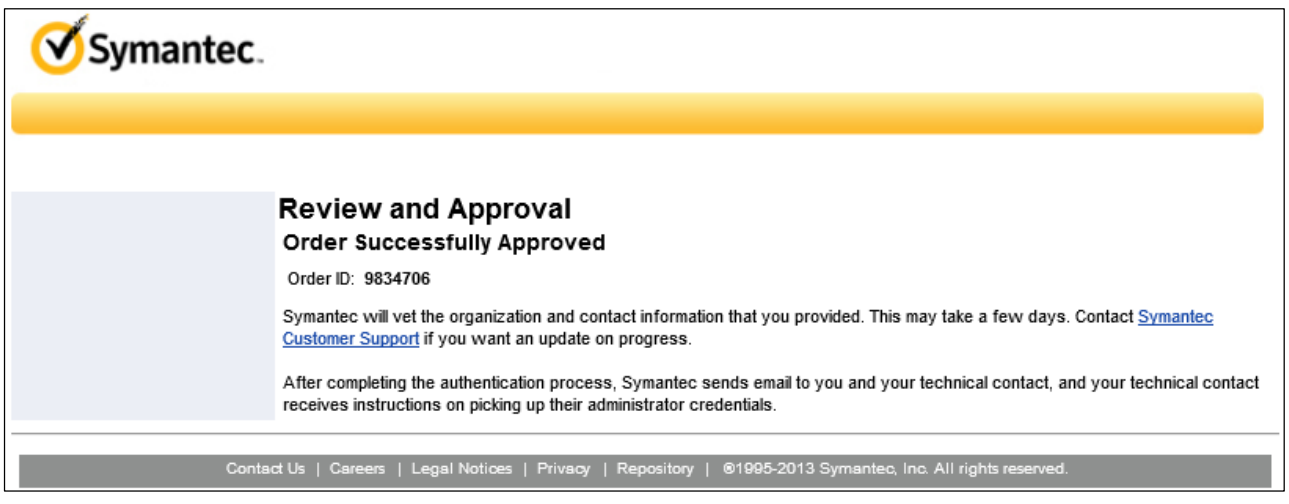


The order request must be approved by the Corporate Approver you designated in your Windows Phone Developer account. They will receive an email similar to the one below. They must approve the request before you can receive your certificate.



After clicking the link, the Corporate Approver will have the choice to approve or decline the request. It's advisable to communicate your incoming request to the approver prior to submission.





Once approved you'll receive an email with all the instructions on how to download your Code Signing certificate and the other Root and Intermediate Symantec certificates required to sign the Company Portal application. We need to follow these steps exactly or we'll run into issues.

First, download the Root and Intermediate Certificates located in the email. Save them to your desktop.

Congratulations! Symantec has approved your request for an Enterprise Code Signing Certificate.

ORDER NUMBER:

COMMON NAME: WindowsIntuneSupport

Note: Your Enterprise certificate is issued by a private Microsoft Root and CA, and is not inherently trusted by your computer. Please ensure that you install and trust the Root and CA certificates **before** installing your Enterprise certificate (newer Windows operating systems will not allow you to install your Enterprise certificate properly if the issuing chain is not already trusted).

STEP 1 – Install the Root certificate:

Click on the link below and install the Root certificate. When prompted for where to install the certificate, select the option to "**Place all certificates in the following store**" (DO NOT accept the automatic default) and select the "**Trusted Root Certification Authorities**" store.

https://knowledge.verisign.com/library/VERISIGN/ALL_OTHER/Symantec_Enterprise_Mobile_Root_for_Microsoft.cer

STEP 2 – Install the CA certificate:

Click on the link below and install the Intermediate certificate. When prompted for where to install the certificate, select the option to "**Place all certificates in the following store**" (DO NOT accept the automatic default) and select the "**Intermediate Certification Authorities**" store.

https://knowledge.verisign.com/library/VERISIGN/ALL_OTHER/Symantec_Enterprise_Mobile_CA_for_Microsoft_Cert.cer

STEP 3 – Install your Enterprise certificate:

Please use the pickup link below to install your certificate. If using **Windows 8 / IE 10** to pickup your certificate, please put your browser into "compatibility mode" first -- this is accomplished by clicking on the "ripped page" icon to the right of the URL. Clicking the icon toggles this mode.

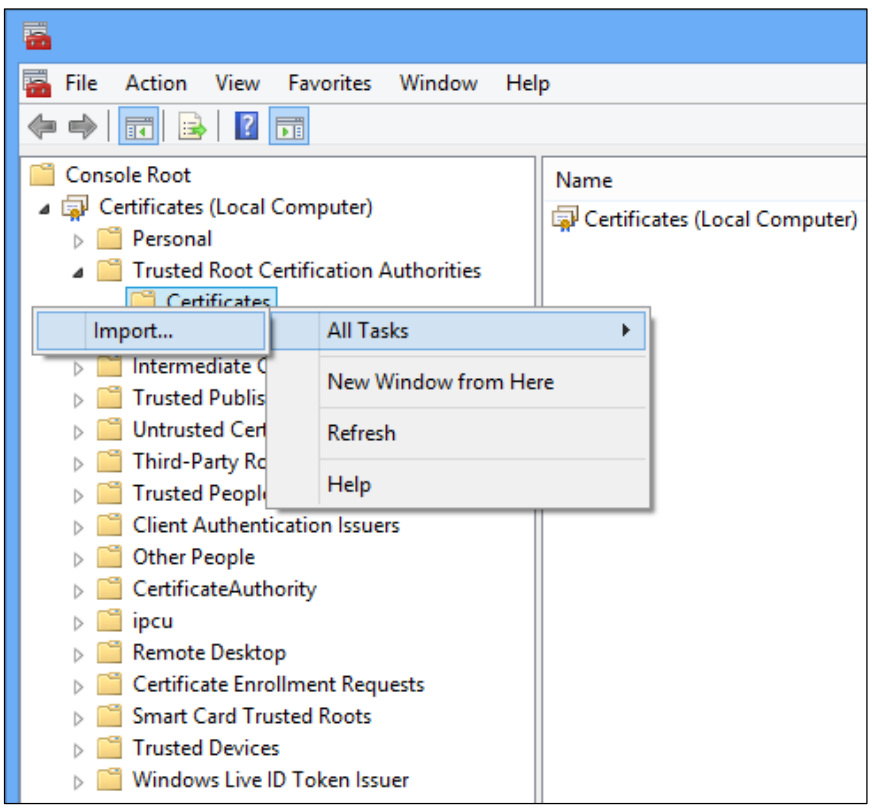
https://products.websecurity.symantec.com/orders/enrollment/CertPickup.do?pin

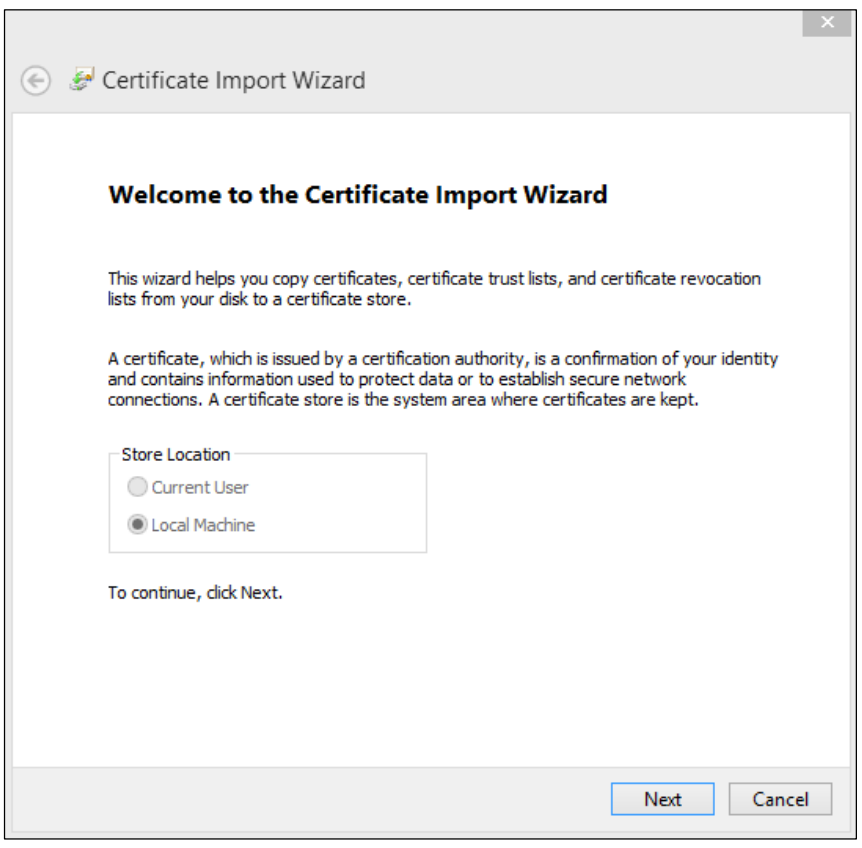
In order to import our certificates we must open a MMC Snap-in.

- Start, Run: MMC.exe
- Open the file menu, click "Add/Remove Snap-In"
- Select Certificates, then Computer Account and local computer.

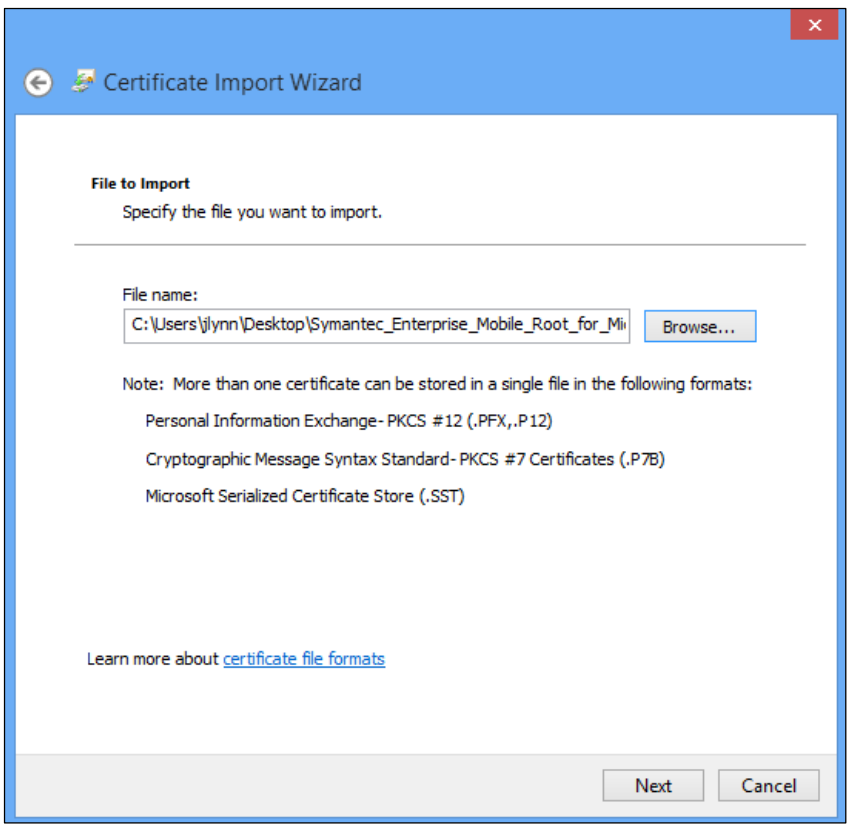
Now that we've opened the local machine certificate snap-in we'll need to import our two certificates from Symantec: Root and Intermediate Certificates

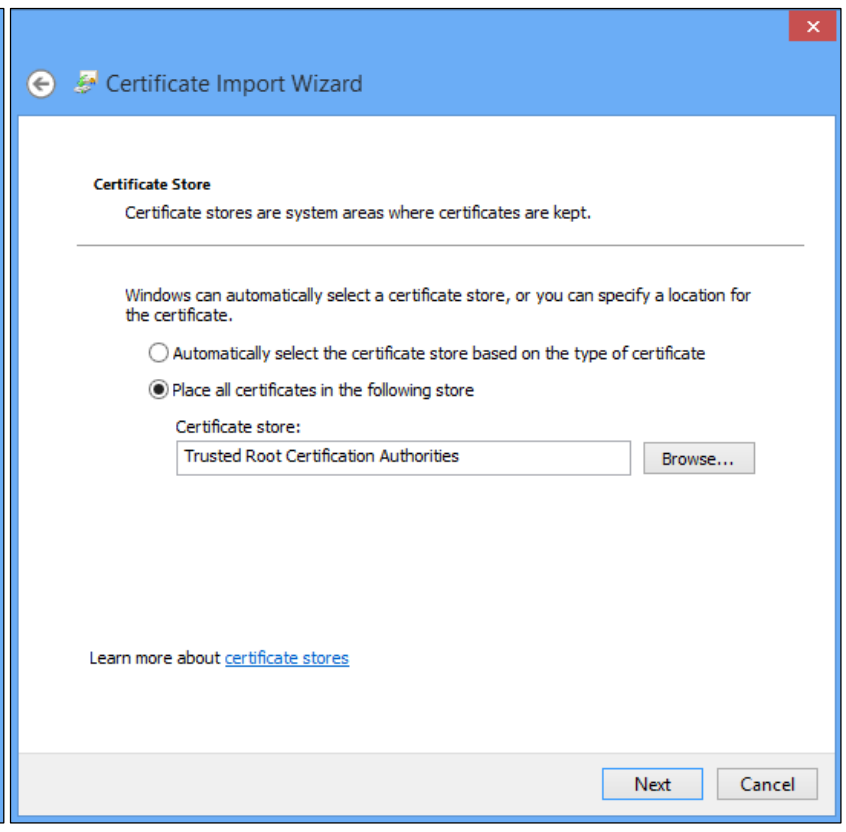
Right click on the Certificates folder under Trusted Root Certificate Authority and choose "All Tasks – Import".





Locate the certificate (Symantec_Enterprise_Mobile_Root_for_Microsoft.cer) and make sure to import the certificate into the Trusted Root Certification Authorities. Do not let Windows automatically place your certificate for you.





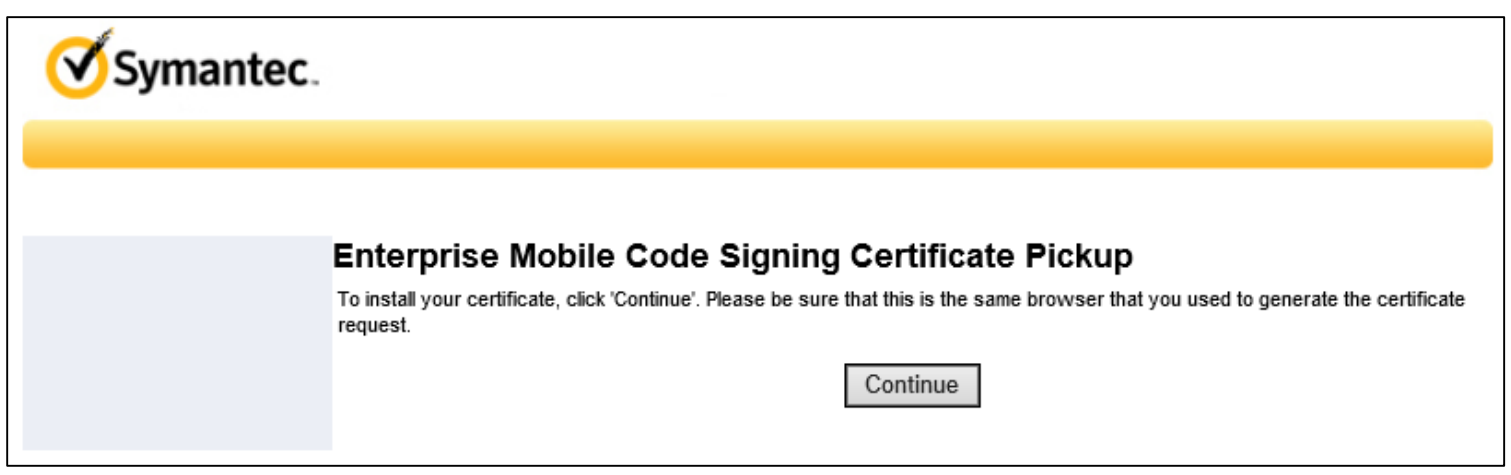
Repeat the previous process for the Intermediate Certificate (Symantec_Enterprise_Mobile_CA_for_Microsoft_Cert.cer), importing the certificate into the Intermediate Certification Authorities

Now that our certificates are imported, let's set up Internet Explorer to import the Enterprise Code Signing Certificate.

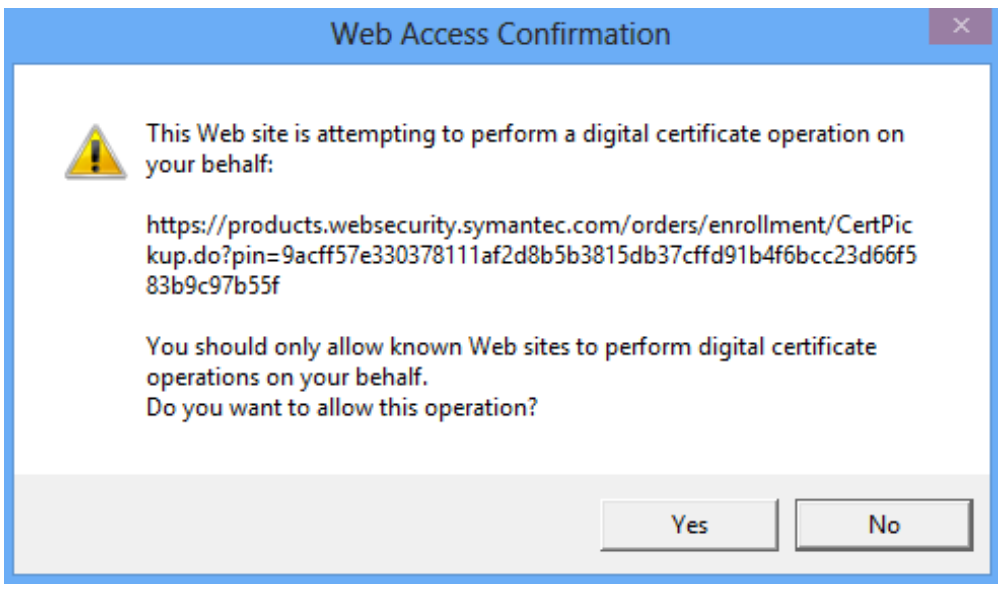
To ensure the certificate is imported correctly, open the compatibility view settings and add Symantec.com to the list of sites that run in compatibility view.

- Open Internet Explorer:
- Open tools menu
- Click on Compatibility View Mode Setting
- Add Symantec.com

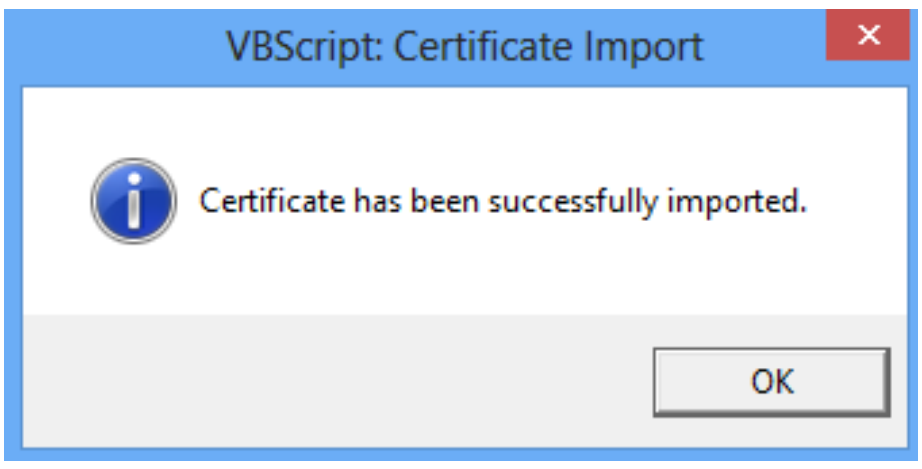
Now let's go back to the email we received from Symantec and click on the link in Step 3. This will take you to Symantec's website. Click the continue button to download your Code Signing certificate.



When prompted, select yes to import the certificate.



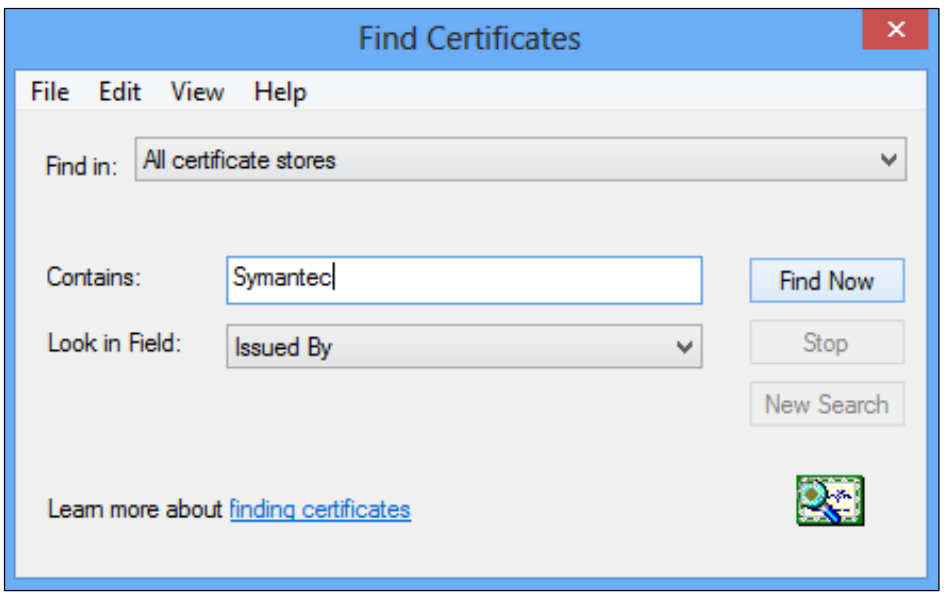
If the certificate successfully imports the website will report back like the screenshot below. If not, the website will return an error message. Please reference this error message when you contact support.



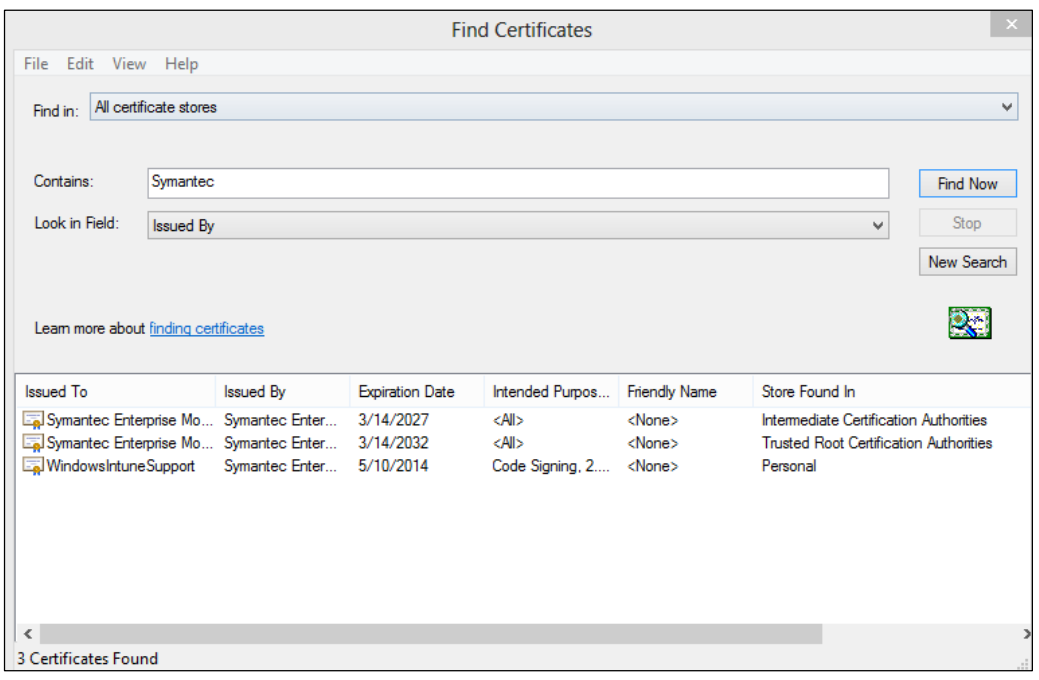
Now that the final certificate has been imported, let us do a quick search to confirm all of the certificates were imported correctly.

- Open MMC.exe and add the Certificates Snap In. (User or Computer is fine)
- Right click on the Certificates node at the top and choose "Find Certificates".

Search for "Symantec"

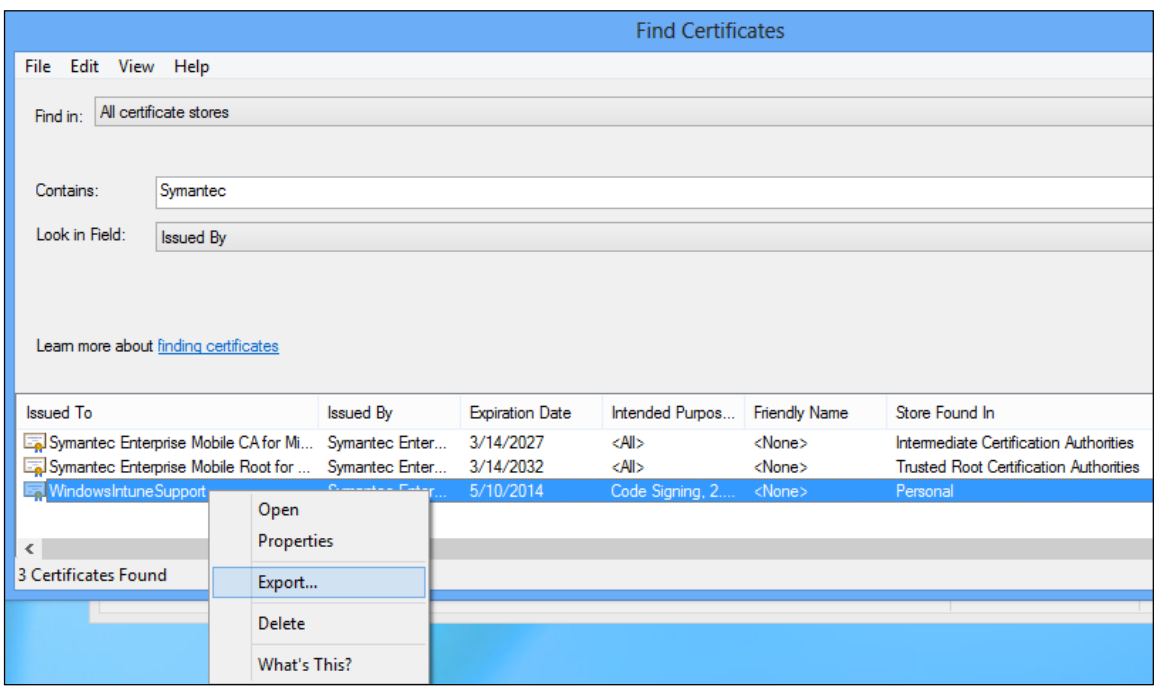


Results should show 3 certificates from Symantec, our root, intermediate and the code signing certificates.

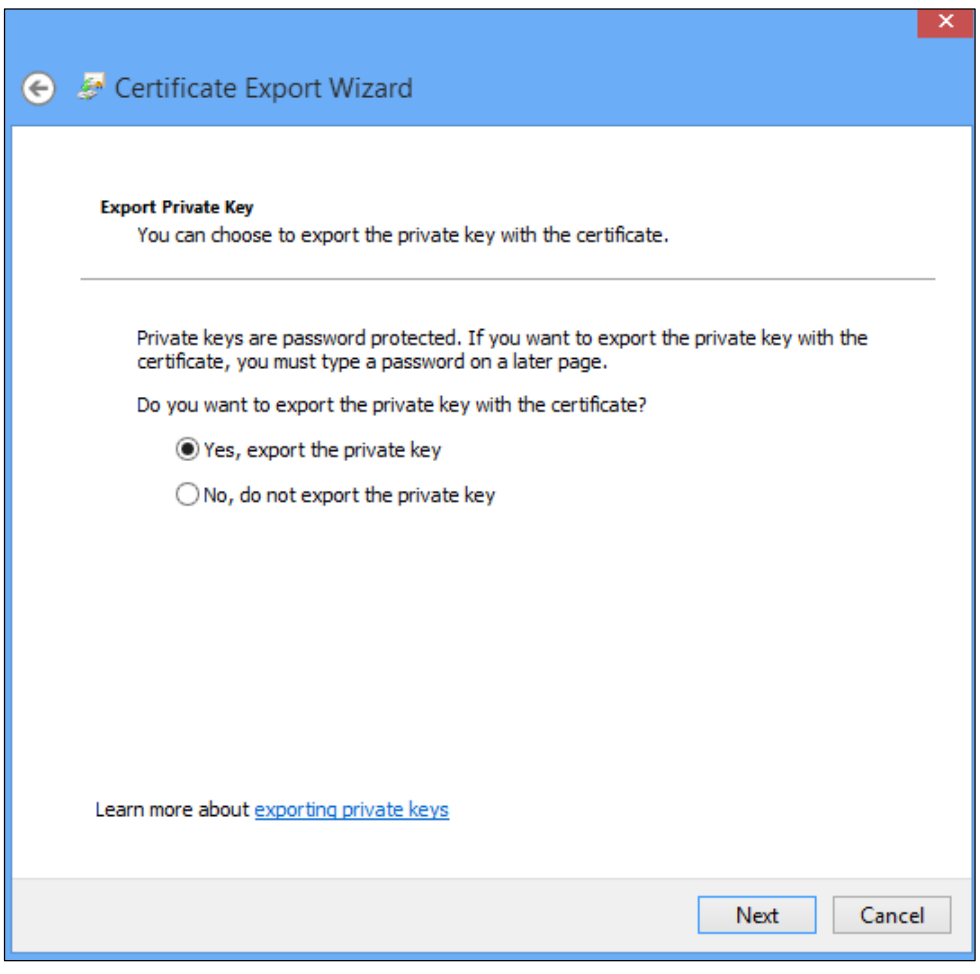


We've now imported the 3 certificates and you're ready to export the PFX file so you can sign the Company Portal.

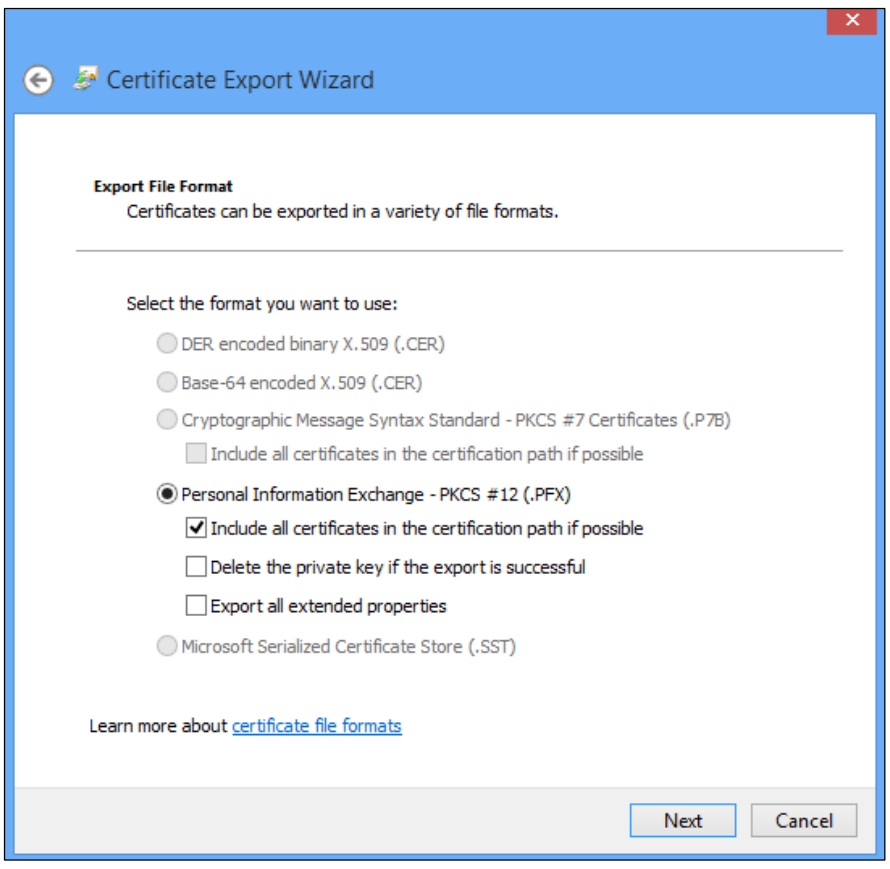
Right click on the Code Signing Certificate and choose "Export".



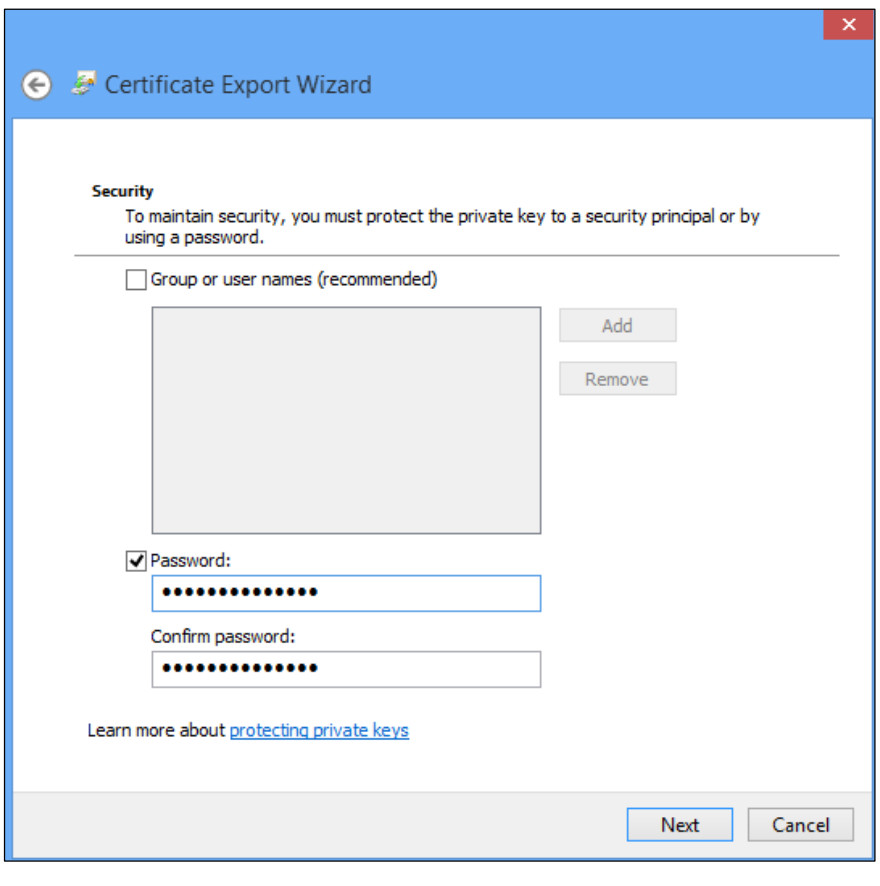
Once the wizard starts choose "Yes, export the private key"



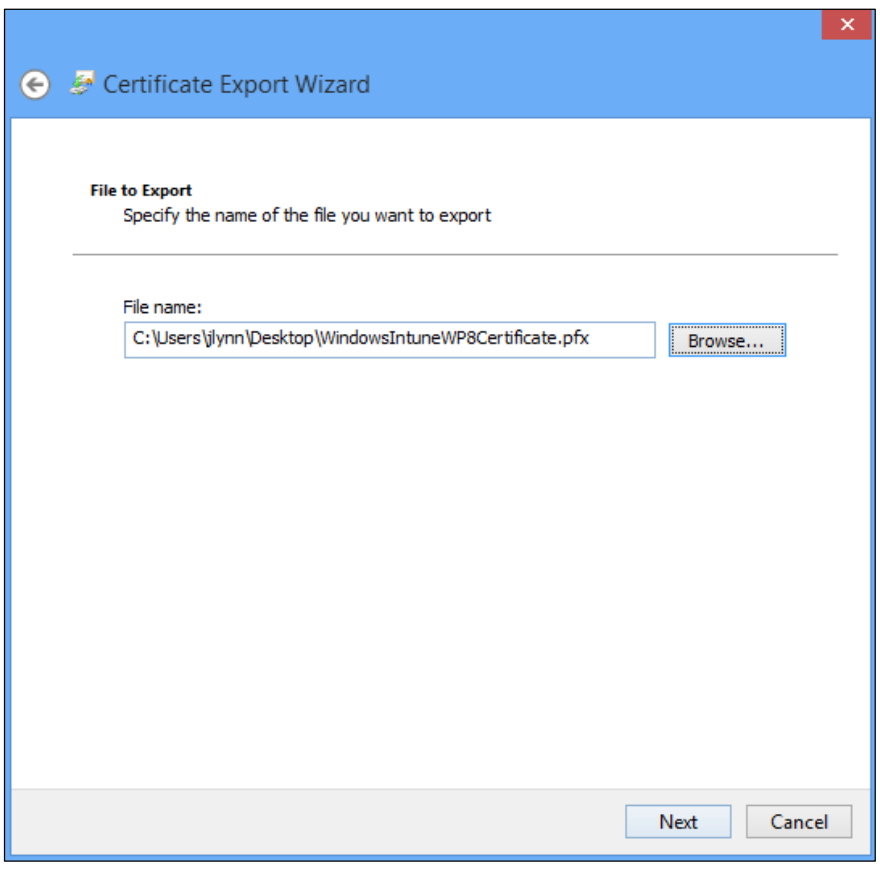
Next, make sure to check "include all certificates in the certification path if possible" option is checked. If this is not checked signing your Company Portal will fail.



Choose a strong password for your certificate.



Name the file and choose a path and complete the export wizard. Store the file in a safe location that is backed up.



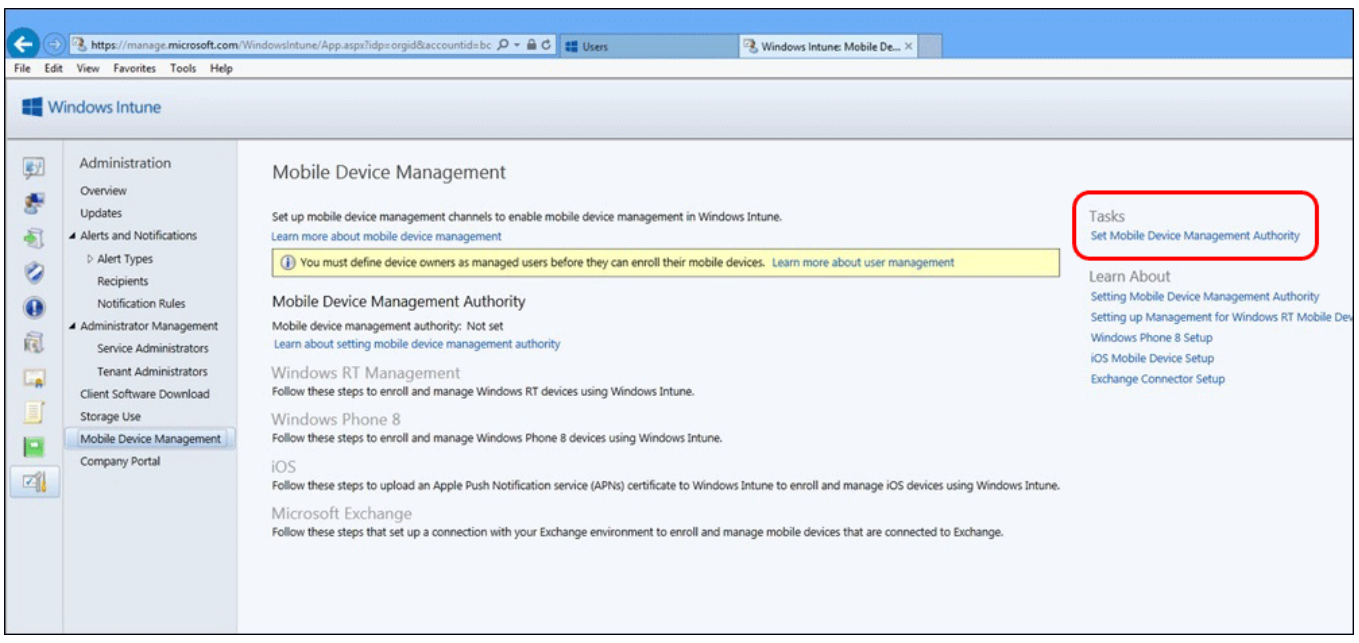
Congratulations! We've exported your Code Signing Certificate and now we're ready to setup your Windows Intune account.

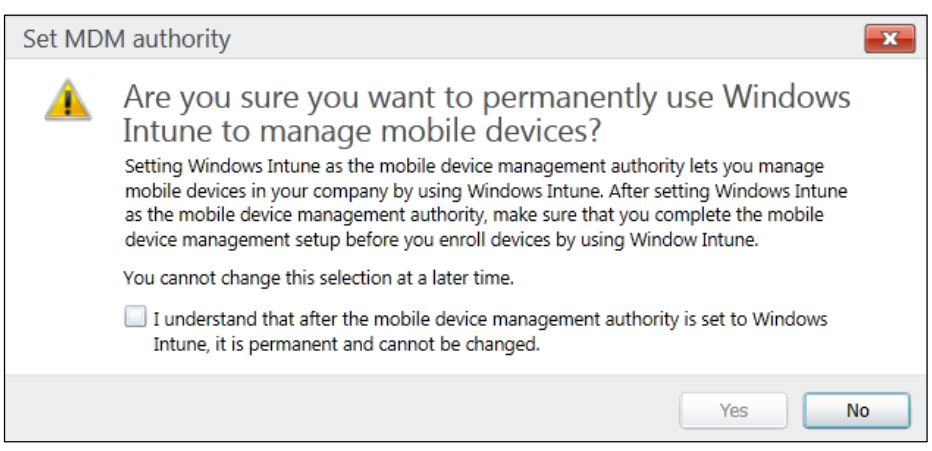
Configuring your Windows Intune account and signing/publishing the Company Portal

- Navigate to https://admin.manage.microsoft.com
- Open the Administration section in the Admin Console and click "Mobile Device Management".
- In order to manage devices we need to set the management authority to Windows Intune. The management authority gives Windows Intune permission to manage your Mobile Devices.

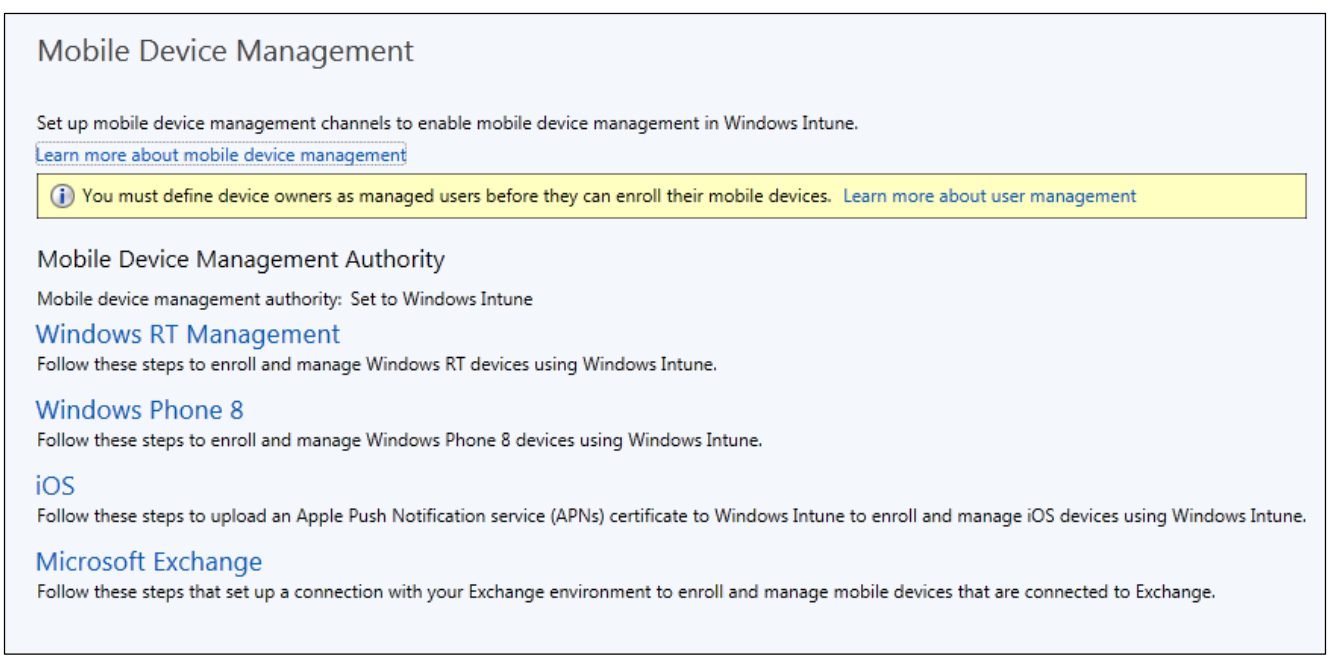
Note: If you plan on using Windows Intune with Configuration Manager 2012 SP1 do not set the management authority to Windows Intune as it cannot be changed.

On the right side of the page, click "Set Mobile Device Management Authority". After clicking that link you'll be prompted with a warning. Check the box and click "Yes".



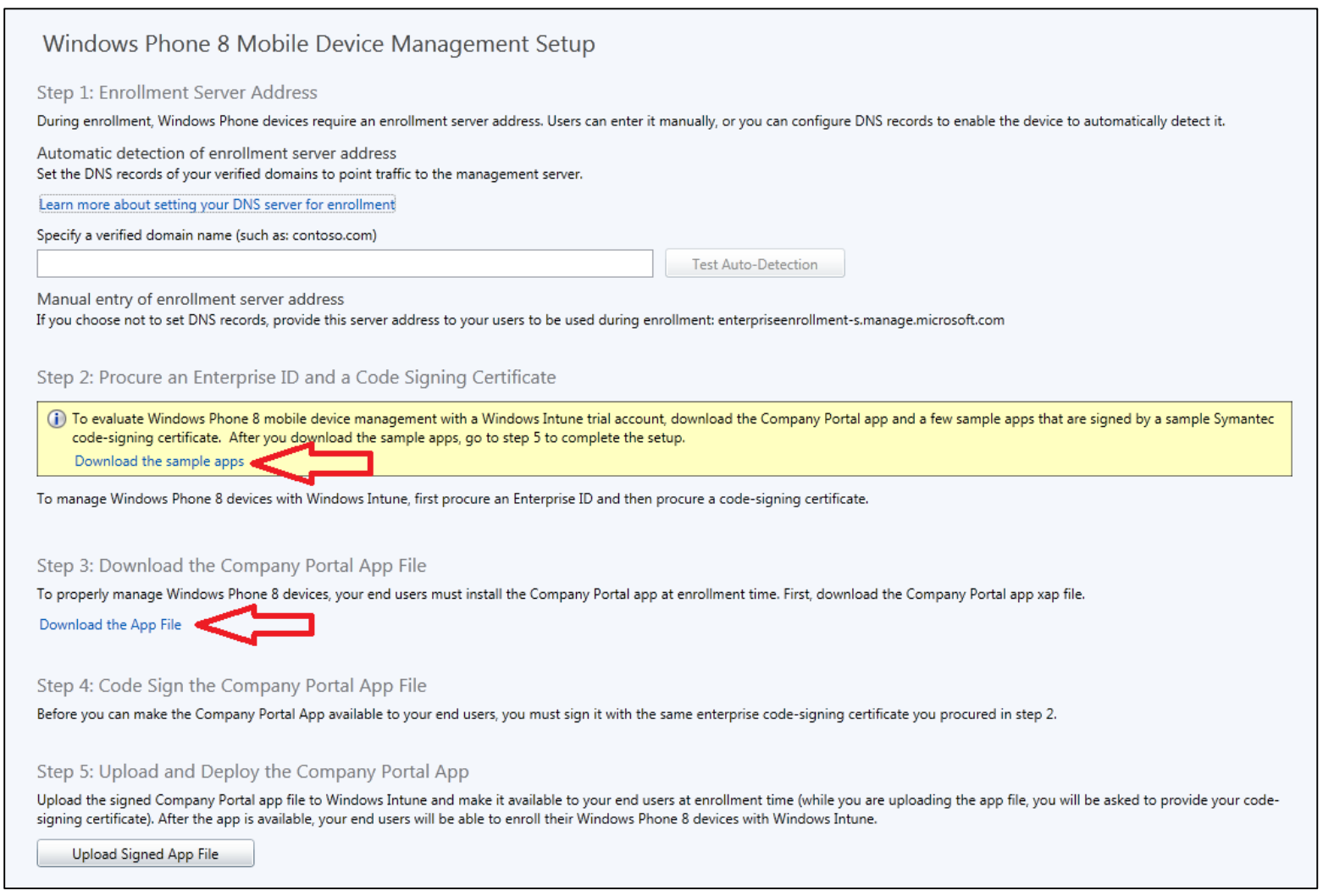


Now that our management authority is set to Windows Intune our Mobile Device Management options have been made available for configuration. Click on the **Windows Phone 8** Link.



In our Windows Phone 8 settings menu we have couple things to setup. An optional feature to enable is setting an Enrollment Server Address in your public domain's DNS. This is not a required step but it does simplify enrollment process for end users. By adding a DNS entry to your public domain users will not need enter a server name during enrollment. Click on the link "Learn more about setting your DNS server for enrollment" and open the Windows Phone 8 Enrollment link for assistance setting up your Enrollment Server Address.

Next we'll need to download the Company Portal. The Company Portal (or Self Service Portal) is the application that will install after enrolling our device into Windows Intune. The Company Portal provides your users access to software and deep links that you publish. Looking at the screenshot below if you are using a trial account download the Company Portal application sample in Step 2 or if you are deploying a corporate signed Company Portal for your paid Windows Intune account go to step 3. In either case, after installing make sure to remember the location the Company Portal files installed to as we'll need them in a moment.



After downloading the Company Portal we'll need to install the Windows Phone 8 SDK and Visual Studio 2012 Express on your Windows 8 machine. If you have a different version of Visual Studio 2012 already installed make sure to still install the Windows Phone 8 SDK. Customers using the sample Company Portal can skip ahead to uploading the Company Portal to Windows Intune as the sample Company Portal is already signed.

To download the Windows Phone 8 SDK and Visual Studio 2012 Express you can visit http://dev.windowsphone.com/en-us/downloadsdk

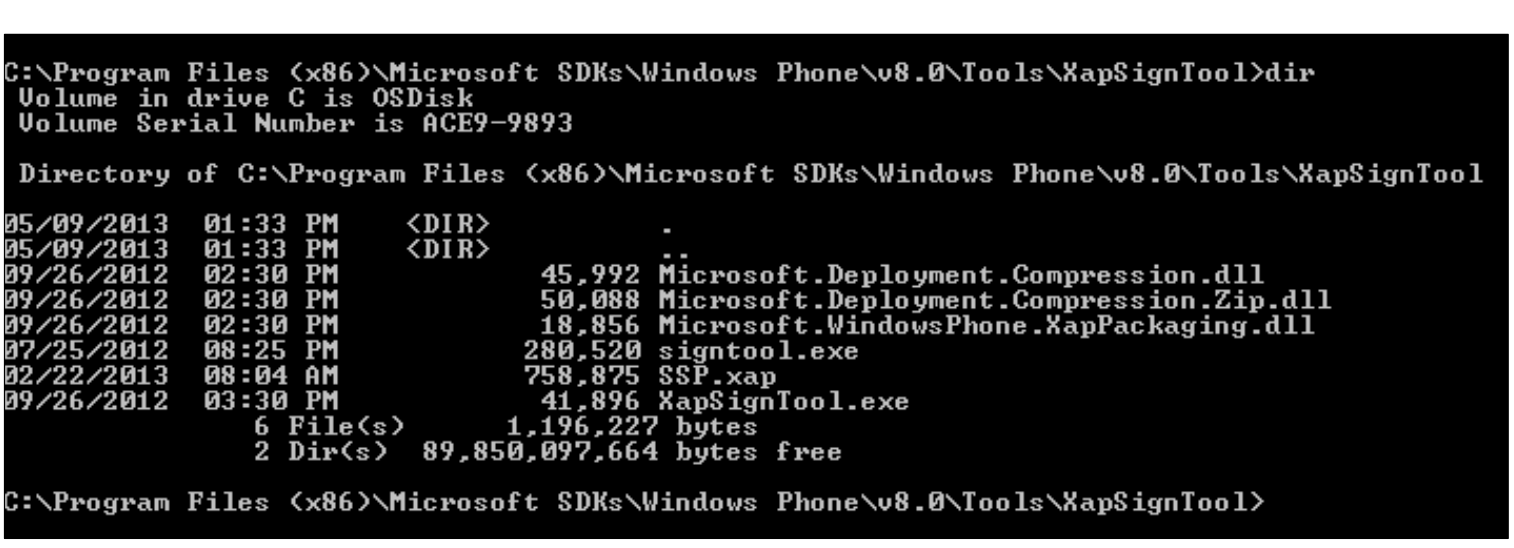
A reboot may be required during after the SDK install to enable Hyper-V.

Now that the SDK and Visual Studio are installed, we need copy some files to the XapSignTool folder. XapSignTool is the tool that signs our Company Portal.

To simplify the process copy signtool.exe from the Windows Kits folder in Program files (your path may differ) to the XapSignTool folder. At the same time please copy the Company Portal (SSP.XAP) and PFX file (Code Signing Certificate) we created earlier to the same folder.

After testing is complete make sure to remove your PFX to ensure it is secure.

Now open an Administrator Command Prompt and navigate to XapSignTool folder under your Microsoft SDK folder in Program Files (x86)



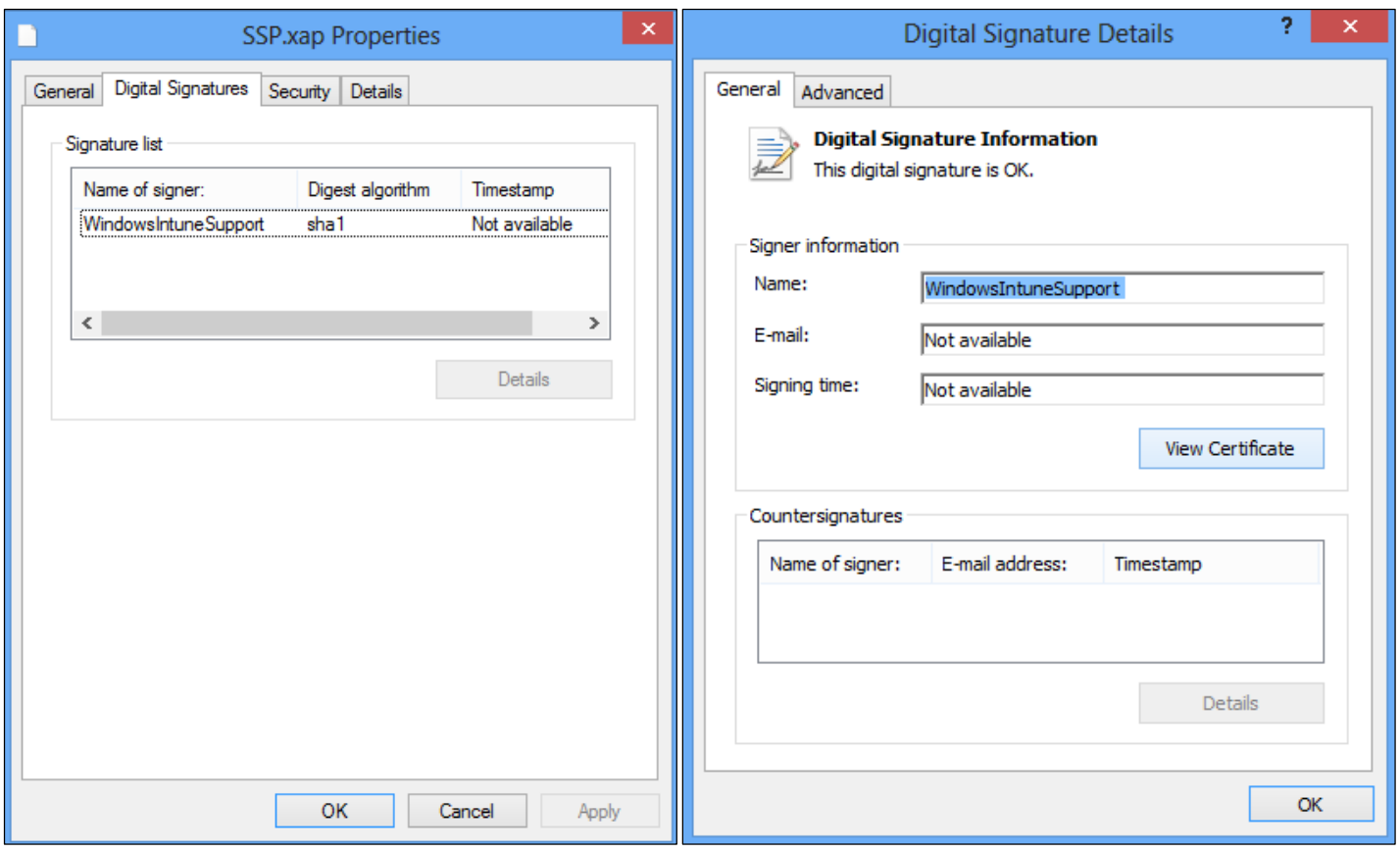
We're going to create a command line to sign our Company Portal.

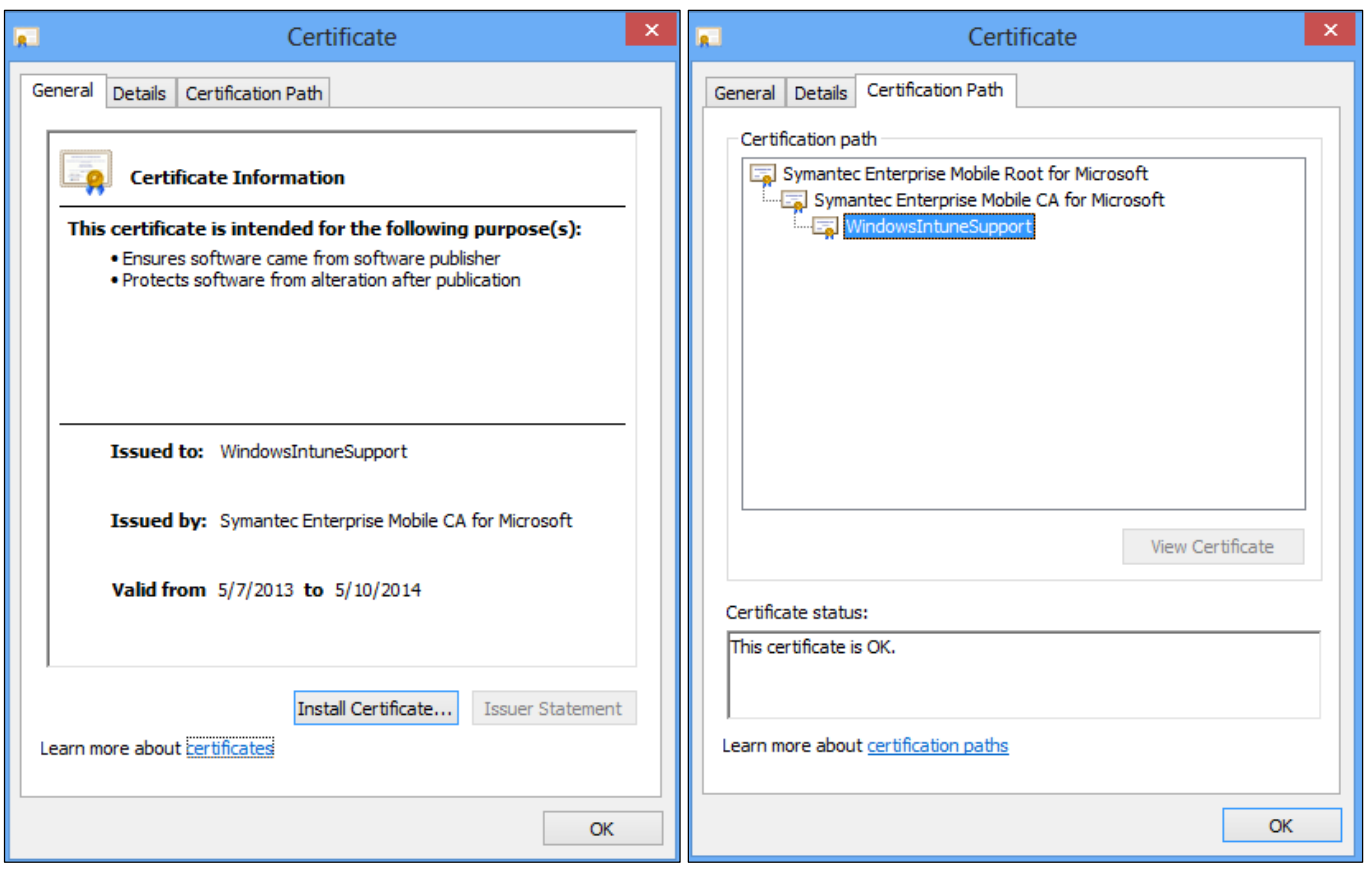
XapSignTool.exe Sign /f Nameofyourcertificate.pfx /p YourCertificatePassword SSP.XAP

If successful the tool will output a success message. If not, an error code will be returned and you can provide that to support.

To validate our file has been signed correctly open the folder where the SSP.XAP is stored, right click and choose properties.

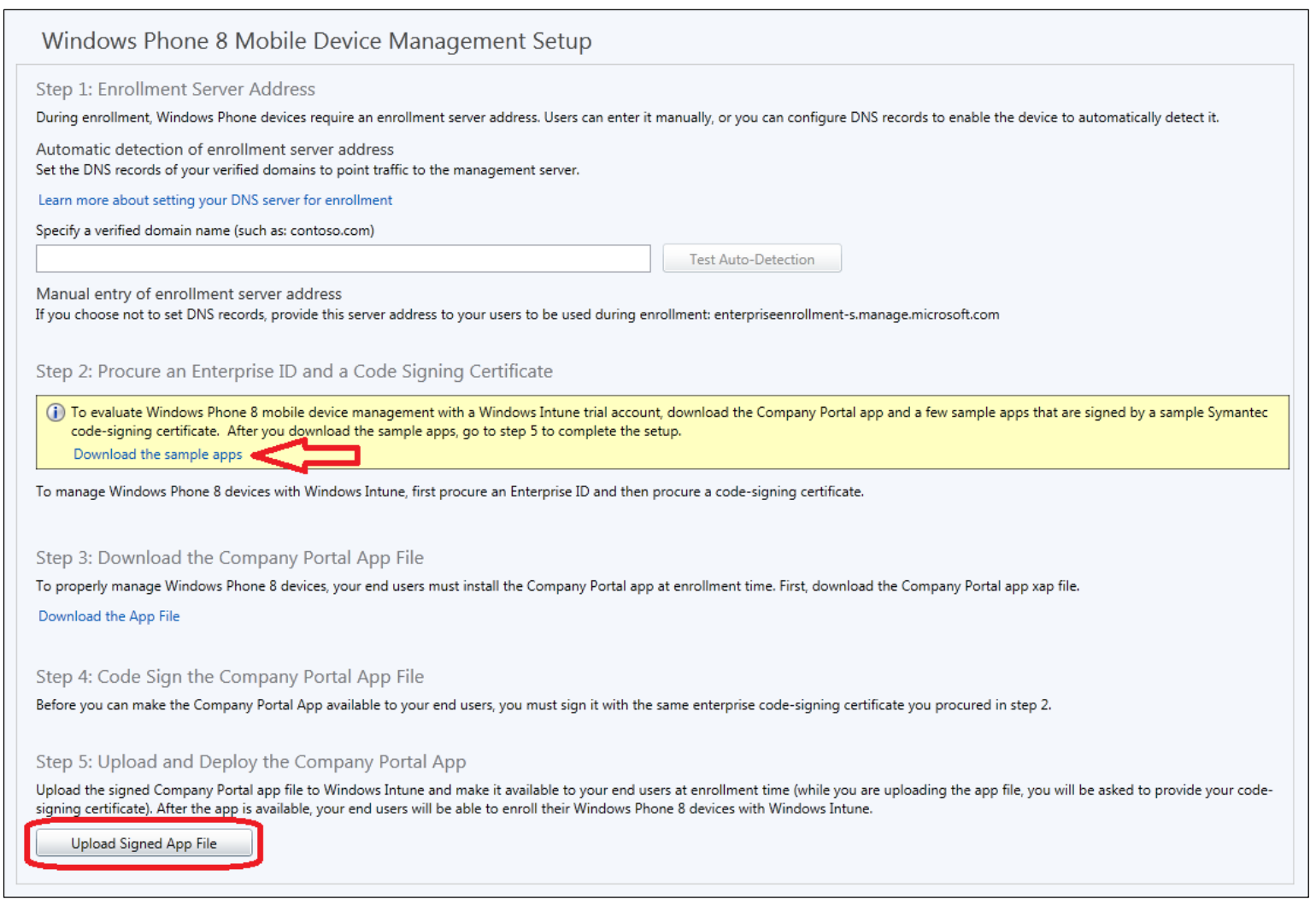
- Click the Digital Signatures Tab and make sure the Name of Signer is your company name.
- Click the Name of Signer and then the details button.
- On the Digital Signature page click "View Certificate".
- Click the Certification Path Tab. Make sure both Symantec Certificates as well as your enterprise code signing cert are present.



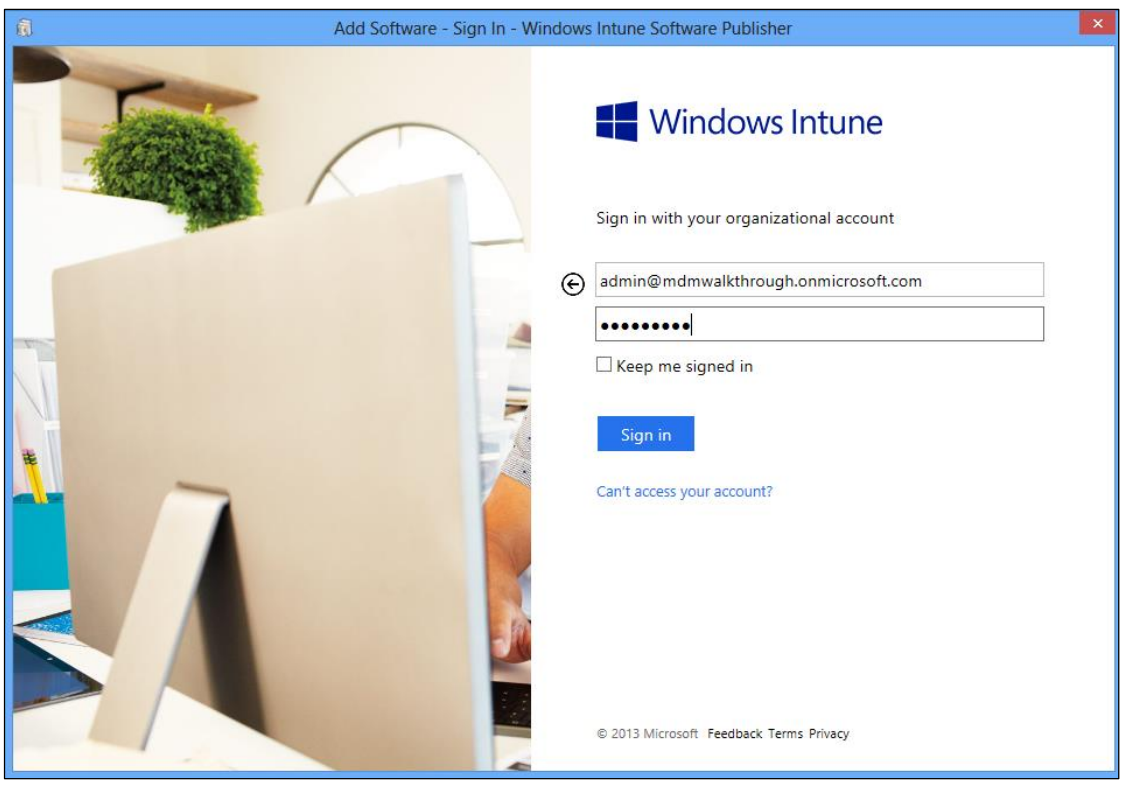


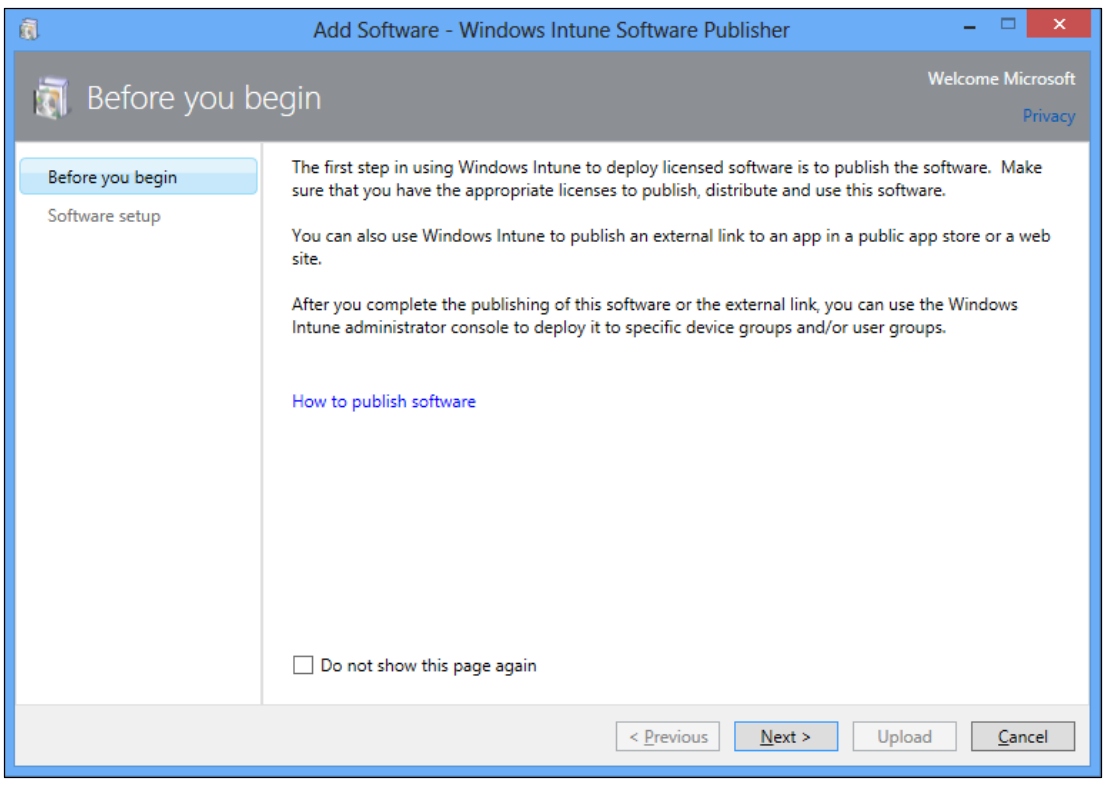
We've signed our Company Portal so it's ready to upload into Windows Intune so we can enroll our Windows Phone 8 devices.

Back in the Windows Intune Admin Console we're going to click "Upload Signed App File" in the Windows Phone 8 section under Mobile Device Management. If you are using the sample Company Portal application with your Windows Intune Trial make sure to set your management authority to Windows Intune as this page will not be accessible until completed.

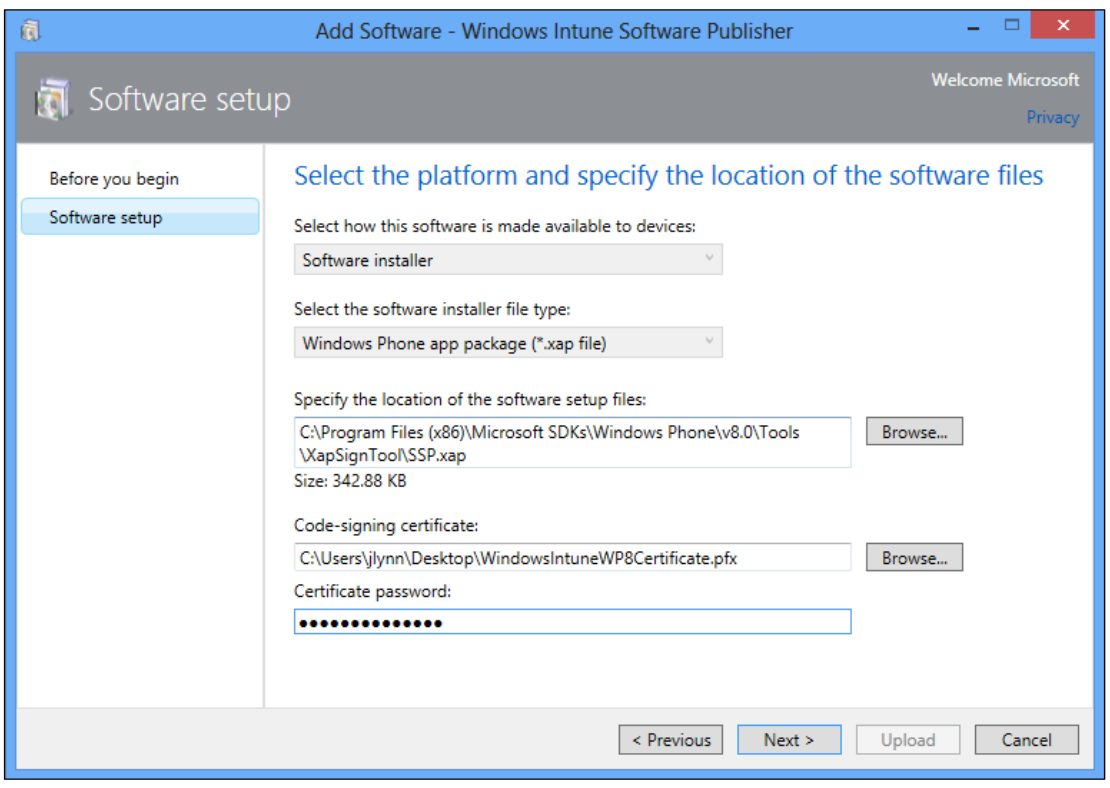


The Windows Intune Software Publisher Wizard will launch and you'll be prompted to sign into the service.

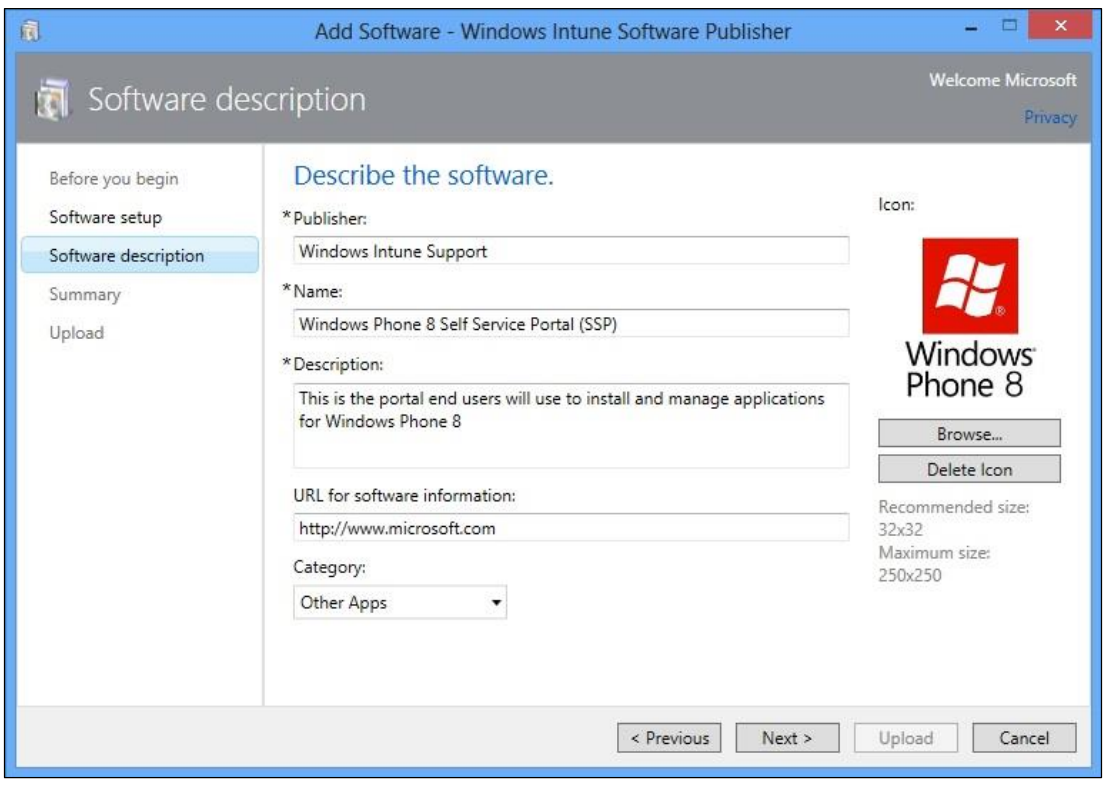




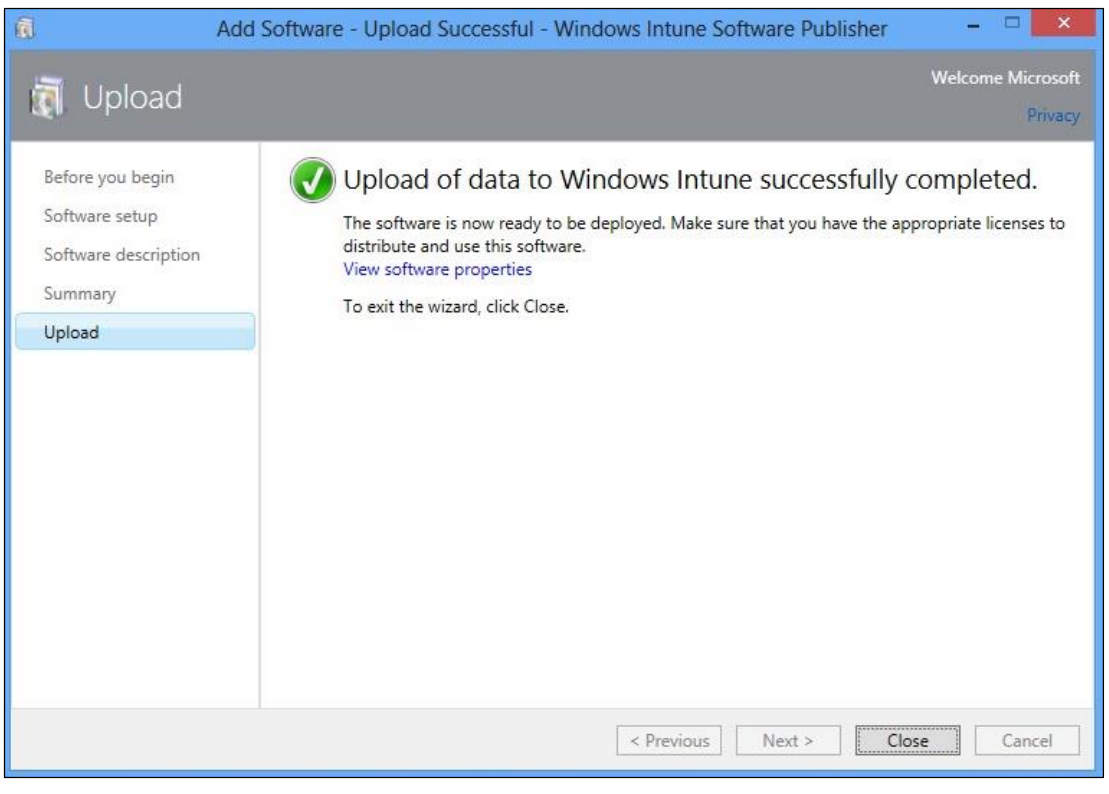
The first step is to provide the location to your Company Portal, then your PFX file. After both of those are complete, enter the password for your PFX file. If you are using the sample Company Portal application you will not need to enter a password and an option to use the sample Company Portal application will be shown when you launch the Software Publisher Wizard.



Fill out the next page how you wish. Your end users will see the Company Portal application when they launch the Company Portal as an available piece of software so keep the name friendly.

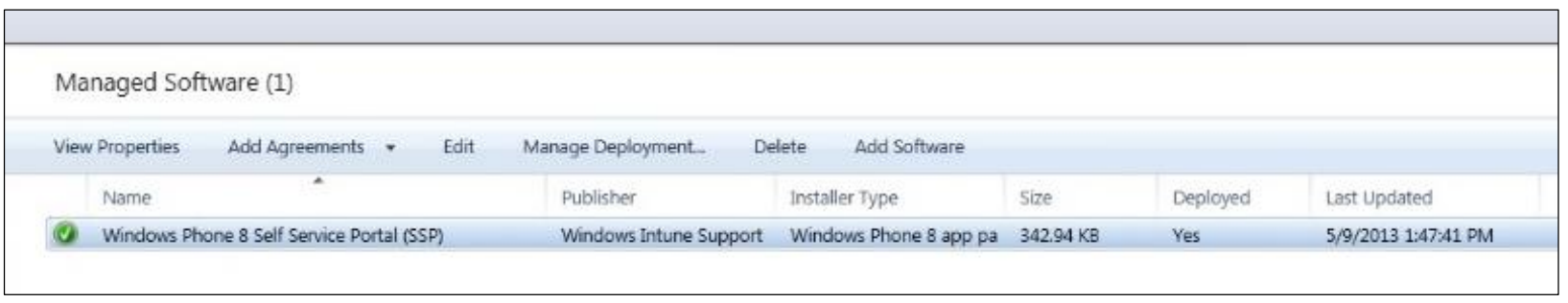


Review all the information you added and upload your Company Portal to the Cloud.



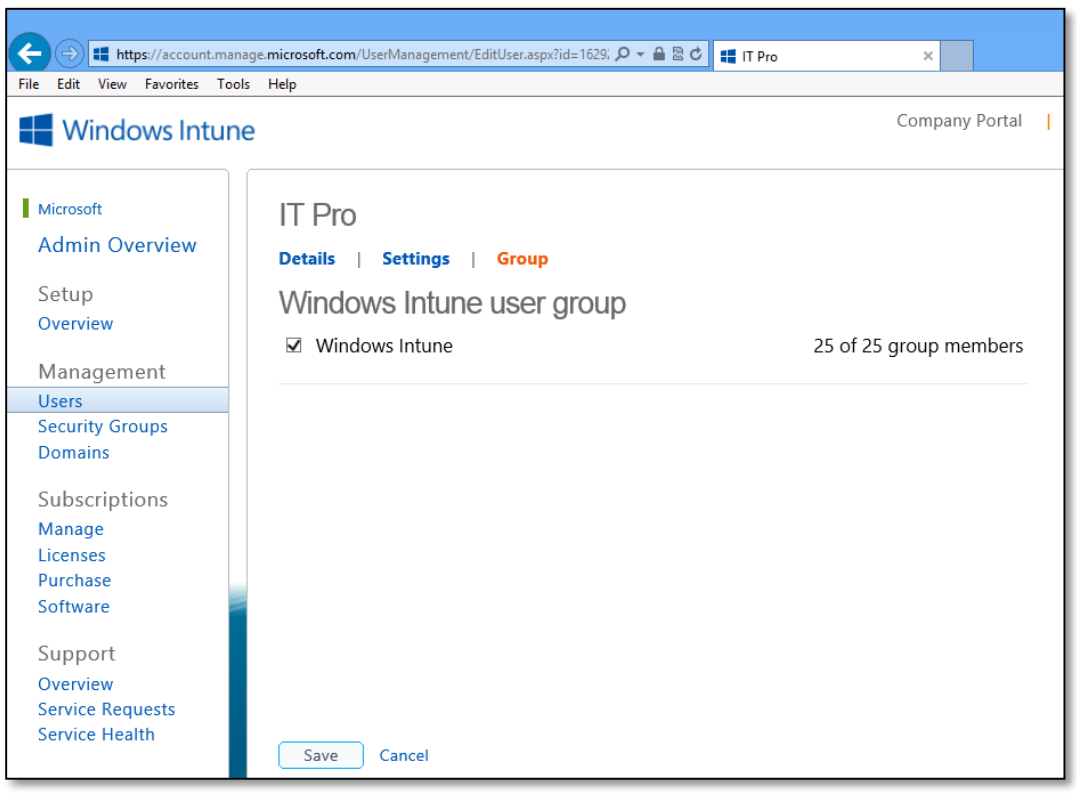
Once complete, validate your Company Portal is published and deployed correctly by navigating to your Software node and clicking Managed Software The Windows Phone 8 Company Portal is automatically deployed to all users.

Note: If you need to replace the Company Portal for any reason you must upload a new version prior to removing the previous version.



Finally, we need to license each of the users we want to have permission to enroll devices. Users get permission to enroll devices by being added into the Windows Intune User Group in the account portal (https://account.manage.microsoft.com)

Open the Users link and ensure each user that needs access to enroll devices is a member of the group.



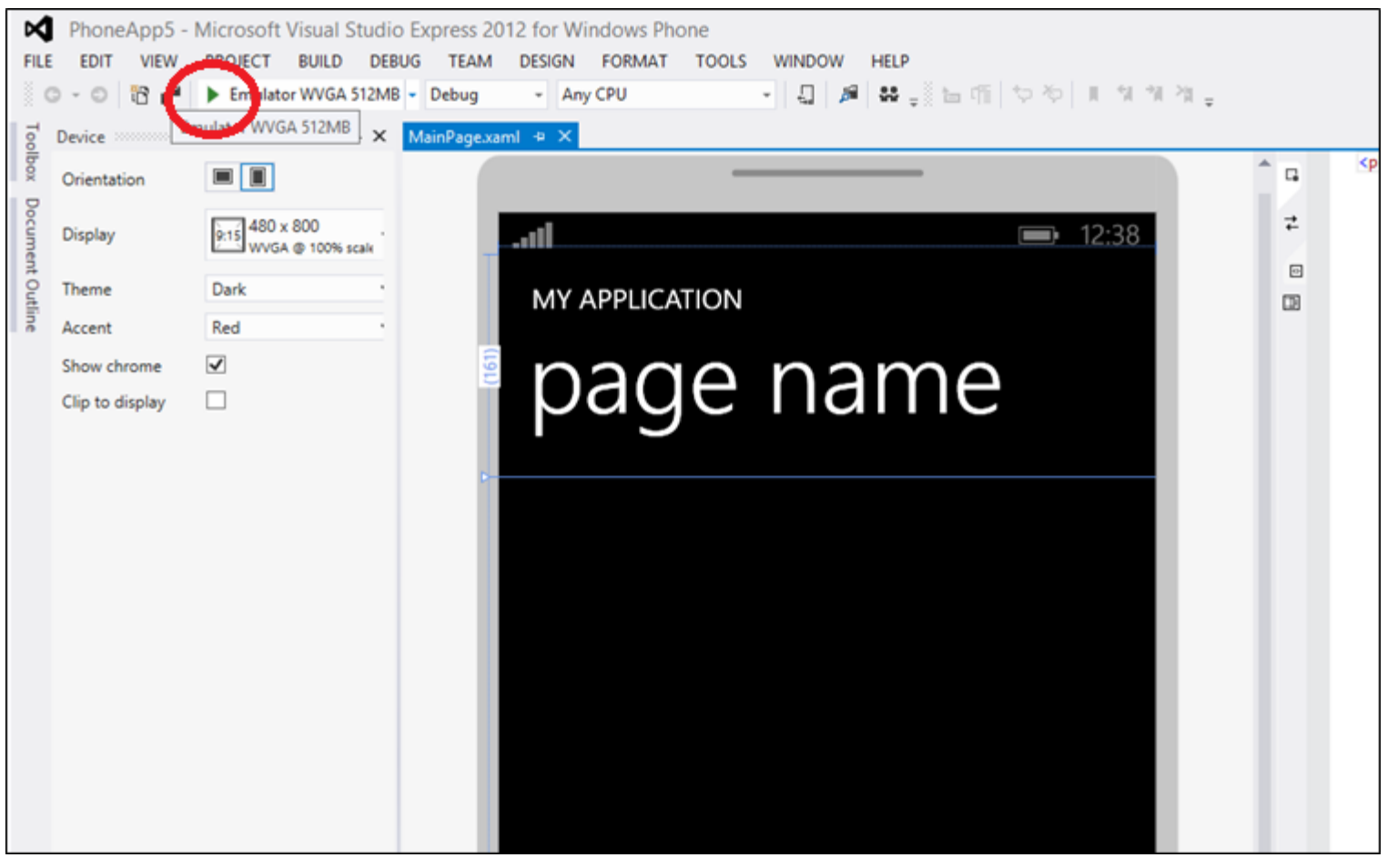
Our Windows Intune account is now completely setup and we're ready to enroll devices.

Enrolling a Windows Phone 8 device into Windows Intune

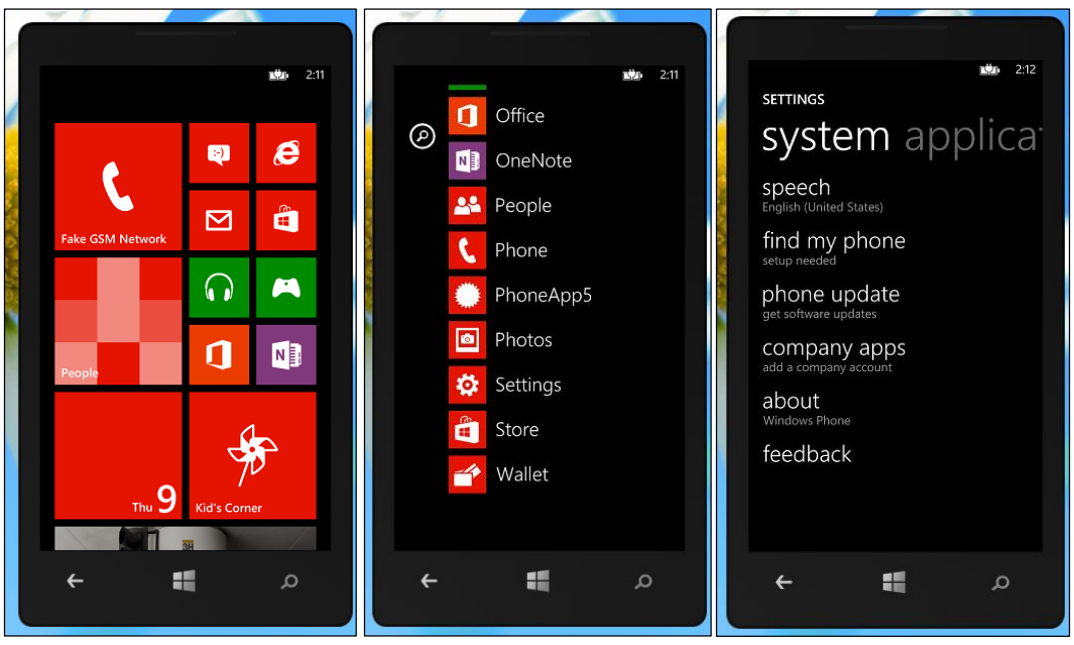
If you are going to test with a virtual Windows Phone 8 devices let's step through getting your virtual Windows Phone 8 running.

- Open Visual Studio 2012 Express
- Start a new project
- Choose Windows Phone, and when prompted choose Windows Phone OS 8.0

Once your project opens, you can start your virtual Windows Phone 8 client by clicking the start emulator button circled below:

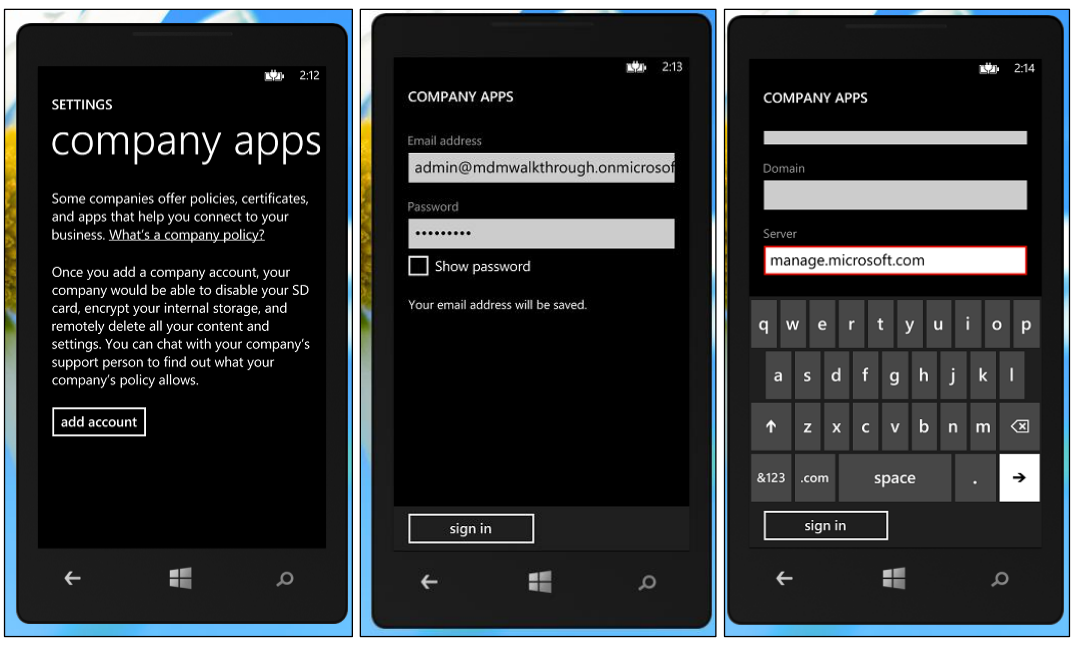


Either on your device or once your emulator starts swipe to the left and scroll down to settings. Open settings, scroll down and open “Company Apps”.

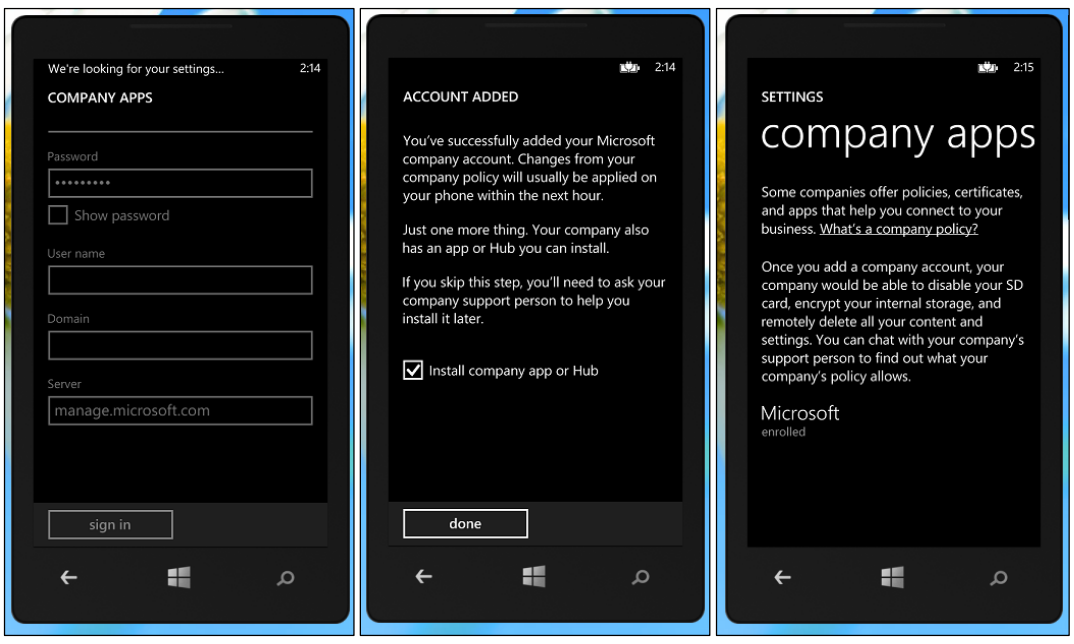


Once company apps opens up click “add accounts”. Earlier we added a user to the Windows Intune User group, enter that username and password in and click sign in. If you didn’t configure the DNS Server information we talked about earlier you will have to enter a server address.

Use manage.microsoft.com for your server address and click sign in.

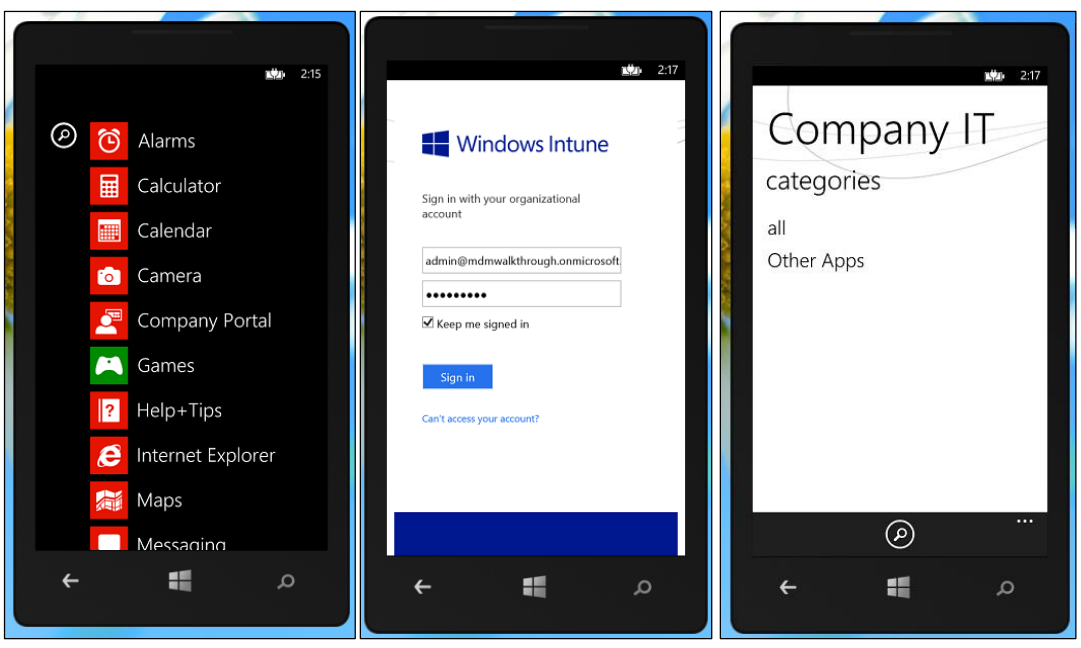


After a few moments, if everything was setup correctly your account will be added. Make sure to leave the “Install company app or Hub” box checked.



Press the Windows button on the phone and swipe over to the applications menu. Look for “Company Portal”. This is the Company Portal we signed earlier and it was pushed down from Windows Intune.

If you do not have the Company Portal application after 5-10 minutes please contact support. Open the application and sign in. You’ll see your company name and any applications you have published.



Congratulations, you have enabled Windows Phone 8 management with Windows Intune and deployed your first device. We hope this walkthrough was helpful. If you have any questions or need further assistance please visit our TechNet forums.

Thanks,

Jon Lynn

Service Engineer, Windows Intune

Copyright 2013. Microsoft Corporation.

This document is provided “as-is”. Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. This document does not provide you with any legal rights to any intellectual property in any Microsoft product.