Windows Phone

Windows Phone 8.1

Implementation Guide

1- Enrollment, Applications Access and Security Policies

Authors: B. Kiffer, JY Grasset (Microsoft)

Reviewers: B. Ourghanlian, P. Beraud, A. Jumelet (Microsoft)

This white paper is part of a series of technical papers designed for IT professionals.

This white paper describes the arrival of an employee in the company with his own Windows Phone and how he has to proceed to join the company's workplace.

Legal Disclaimer

Agenda

White Paper Overview

Figure 1.1: Windows Phone 8.1

Windows Phone 8.1 offers a lot of new capabilities designed for the enterprise such as simplified enrollment with MDM solutions, easy configuration management, client authentication certificates, network profiles for Wi-Fi and VPN, as well as enterprise certificates management, S/MIME support and a larger set of configuration and security policies.

This document is the first guide of a series of white papers addressing common usage scenarios focused on Windows Phone 8.1 enterprise and security features.

This first scenario demonstrates how the employee can join the Workplace with their Windows Phone and then get access to the enterprise's applications.

This scenario is illustrated from two different points of view: the first part of the document describes the user experience and, the second one, the IT administrator tasks necessary to put in place the scenario.

Considering the user experience, an employee comes with his/her own Windows Phone and wants to get access to business applications delivered by the company. He or she is given a description of the brief procedure by the mean, for example, of an email in their personal mailbox. The employee can then enroll the Windows Phone in the company's Workplace, download and install the Company Portal that will give access to the enterprise business applications. After the registration, security policies apply to the mobile phone that disable the capability for the user to take a screenshot.

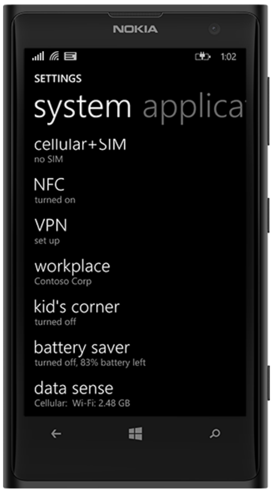
From the administrator perspective, some configuration tasks have to be realized in order to implement this scenario: a new user account must be created and the mobile device enrollment has to be enabled in the Windows Intune's portal. Then, the administrator configures an application pool so that applications can be automatically deployed on the Windows Phone device or made available on the portal.

In order to follow enterprise security policies and strengthen the Windows Phone security, the administrator will enforce compliance rules like disabling the screenshot capability.

Each functionality of this overview will be explained in more details in the rest of the white paper.

The lab infrastructure is made of two parts: the on-premises infrastructure is based on a virtual machine hosting Active Directory, System Center Configuration Manager and a Microsoft certification authority role. The Cloud infrastructure relies on a Windows Intune tenant linked to a Microsoft Azure Active Directory synchronized with the on-premises Active Directory.

User experience



SETTINGS

system applica

cellular+SIM
no SIM

NFC
turned on

VPN
set up

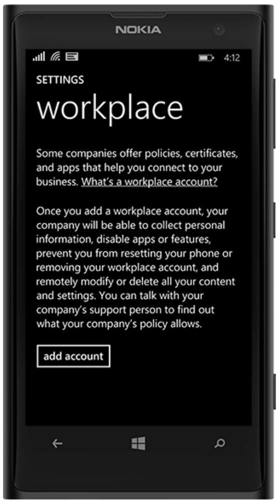
workplace
Contoso Corp

kid's corner
turned off

battery saver
turned off, 83% battery left

data sense
Cellular: Wi-Fi: 2.48 GB

Figure 2.1: Workplace



SETTINGS

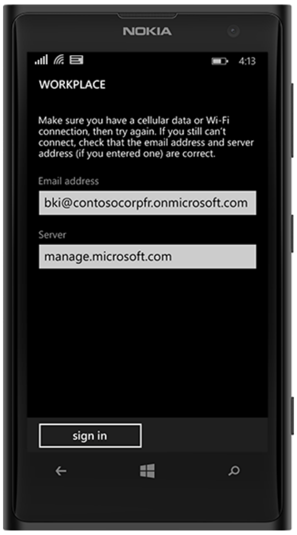
workplace

Some companies offer policies, certificates, and apps that help you connect to your business. What's a workplace account?

Once you add a workplace account, your company will be able to collect personal information, disable apps or features, prevent you from resetting your phone or removing your workplace account, and remotely modify or delete all your content and settings. You can talk with your company's support person to find out what your company's policy allows.

add account

Figure 2.2: Enrollment



WORKPLACE

Make sure you have a cellular data or Wi-Fi connection, then try again. If you still can't connect, check that the email address and server address (if you entered one) are correct.

Email address
bki@contosocorpfr.onmicrosoft.com

Server
manage.microsoft.com

sign in

Figure 2.3: Email address

Windows Phone Enrollment

In this first part, we will demonstrate the very straightforward steps that, as a new employee, you have to follow in order to enroll your Windows Phone 8.1 smartphone through the enterprise workplace. You will then be able to install the company portal application to get access the business applications delivered by the organization.

The enrollment process can made available by sending an email on your personal mailbox or by any other mean (IT enterprise web site, etc.).

The following steps demonstrate how to configure the Windows Phone to join the organization's workplace.

1. Go to the **main menu** and select **settings**.
2. In the settings panel, select "**workplace**" according to the figure 2.1.

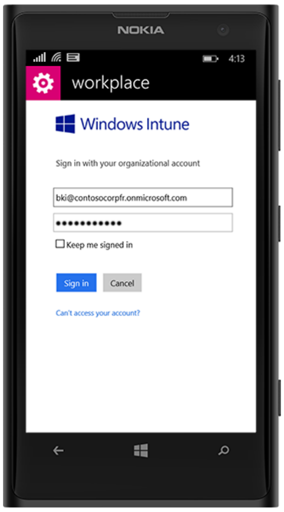
By joining the enterprise workplace, the Windows Phone will be configured to seamlessly download and install apps, but will also receive security policies defined by the enterprise's administrator: some features like, for example, the capability to take screenshots can be disabled to prevent data leak.

As Windows Phone 8.1 natively integrates the "**Workplace Join**" feature, you does not have to download any software.

3. Choose "**Add account**" (see figure 2.2)
4. Fill in the Email address field with your company **email account**, and the tap the **sign in** button.
5. (Optional) If the company domain name is in the form of mycompany.onmicrosoft.com, you have to specify **manage.microsoft.com** inside the Server field, otherwise you will not be able to access the company workplace.

As shown in figure 2.3, the demo domain name is "contosocorpfr.onmicrosoft.com" and the account name "bki".

Note: *To join the workplace, you must have a user account defined in the company's Active Directory, be enabled in Windows Intune and be allowed to enroll mobile devices for his account.*



Sign in with your organizational account

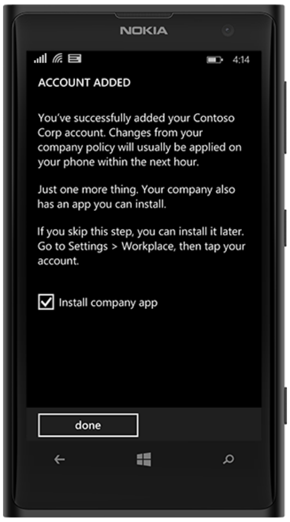
bki@contosocorpfr.onmicrosoft.com

••••••••••••

□ Keep me signed in

Figure 2.4: Windows Intune redirection

6. You will now be redirected to the **Windows Intune portal** to type your enterprise password as represented in figure 2.4.
7. After this step, the Windows Phone device is enrolled in the organization's workplace and, as a new employee, you are given the choice to **download and install the company portal to get access to enterprise applications** (see figure 2.5).



ACCOUNT ADDED

You've successfully added your Contoso Corp account. Changes from your company policy will usually be applied on your phone within the next hour.

Just one more thing. Your company also has an app you can install.

If you skip this step, you can install it later. Go to Settings > Workplace, then tap your account.

☑ Install company app

Figure 2.5: Company Portal installation

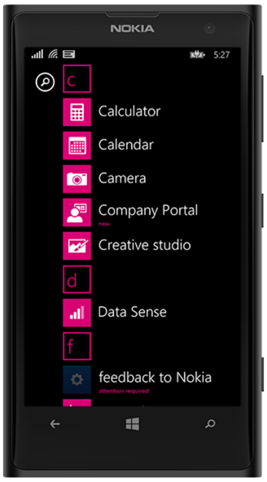


Figure 2.6: Accessing the Company Portal

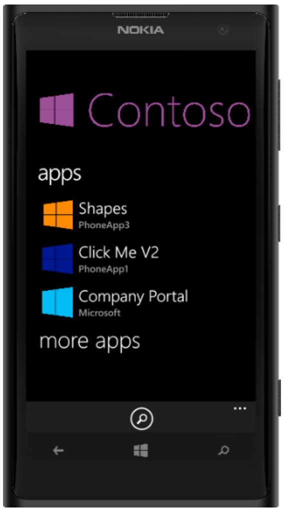


Figure 2.7: Applications on the Company Portal

Enterprise Applications

Usually, all required applications and updates will be installed automatically after the Windows Phone enrollment process. However, you have the option to manually install additional Enterprise applications of your choice from the Company Portal.

1. To access the Company Portal, go to the **main menu** and search **Company Portal** (figure 2.6)
2. On the Portal main page, enter your **professional email account** and associated **password** in the authentication window.
3. Once connected, all **available enterprise applications** will be presented that you can download and install (figure 2.7).

Security Policies

Windows Phone 8.1 implements a set of additional configuration policies that can be enforced by the enterprise IT administrator; these new policies can be used, for example, to control the hardware configuration (disable camera, Wi-Fi, location…), prevent usage of Microsoft Account, disable roaming between Windows devices with the same Microsoft Account, or remote device wipe or enterprise wipe in push mode.

To get the exhaustive list of new configuration policies, please refer to the **Windows Phone 8.1 Security Overview**.[1]

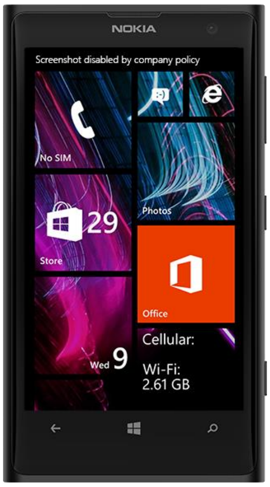
In this usage scenario, three configuration policies have been selected to demonstrate how enterprise security policies related to data leak prevention - screen capture, camera use and store access- can be enforced by the administrator.

The security policies are applied after enrollment; you will notice consequently that, if you try to make a screen capture by pressing simultaneously the **Volume UP and Power buttons** (see note), the error message **Screenshot disabled by company policy** will appear at the top of the screen as represented in figure 2.8.

Another policy forbids to take photos with your Windows Phone as shown in figure 2.9: you can access to the camera portal to record a video but you cannot take pictures.

Finally you can check that **public applications cannot be installed** on the Windows Phone because access to the public store has been disabled by the last security policy (see figure 2.10).

Note*: The hardware button combination was the Start and Power buttons for Windows Phone 8 but has been changed with Windows Phone 8.1.*



Screenshot disabled by company policy

Figure 2.8: Screenshot disabled

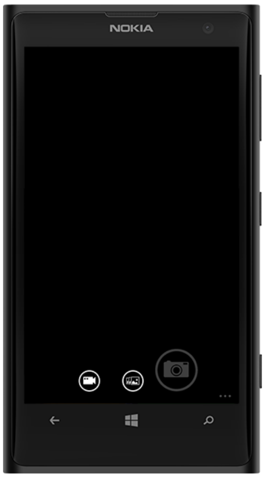


Figure 2.9: Camera disabled

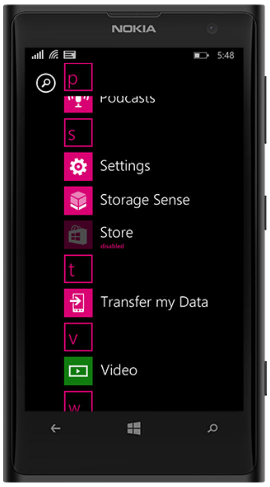


Figure 2.10: Public Store disabled

[1] **Windows Phone 8.1 Security Overview**: http://www.microsoft.com/en-us/download/details.aspx?id=42509

Administrator Experience

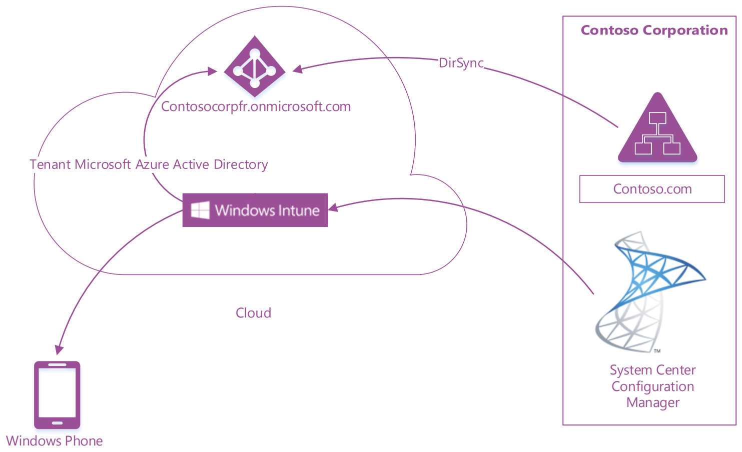
In this second part, we will show you how to easily deploy Windows Phone enrollment, first through System Center Configuration Manager 2012 R2 and then with Windows Intune.

At the time of this writing, all Windows Phone 8.1 features are not manageable through a Windows Intune Unified Architecture (based on System Center Configuration Manager 2012 R2 with Windows Intune), whereas some of them are available in the Cloud-Only Architecture (based on Windows Intune only). The management component which is necessary to access Windows Phone 8.1 additional functionalities will be included in the next update of System Center. However we can deploy a Unified Architecture for the demonstration to allow users' enrollment through System Center Configuration Manager and give employees access to enterprise applications.

In this section, we will cover how to configure System Center Configuration Manager 2012 R2, enable Windows Phone enrollment through the Company Portal, deploy enterprise applications to users, and finally set up security policies.

The domain name used for this demonstration is **contosocorpfr.onmicrosoft.com**.

The figure below depicts the high-level architecture of the Contoso Corporation infrastructure: an **on-premises Active Directory forest** contoso.com hosting a System Center Configuration Manager server, and, on the left side, a **Windows Intune tenant associated to the Azure Active Directory tenant** contosocorpfr.onmicrosoft.com.


Contoso Corporation
DirSync
Contosocorpfr.onmicrosoft.com
Tenant Microsoft Azure Active Directory
Windows Intune
Contoso.com
Cloud
System Center Configuration Manager
Windows Phone

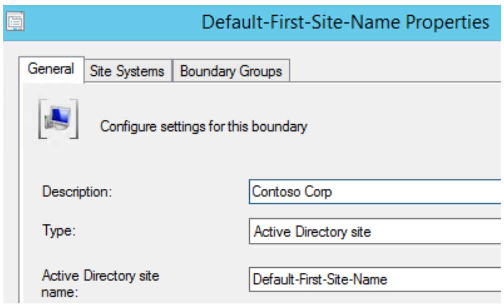
The on-premises Active Directory is synchronized with the Windows Azure Active Directory using **DirSync** to allow enterprise users accounts to be projected to the Cloud and appear as Windows Intune users in order for them to enroll their devices.

In order to manage Windows Phone mobiles, System Center Configuration Manager is linked to Windows Intune through a Windows Intune subscription and the Windows Intune Connector (see **Windows Intune Connector**).

SCCM Configuration

This part covers the SCCM configuration to authorize Windows Phone enrollment. First, on-premises Active Directory users must be imported in the System Center Configuration Manager database to be able to enroll their Windows Phone and to allow IT administrators to manage their devices.

1. In order to import all Active Directory users in the System Center database, you have to create a boundary for your Active Directory site: Open the **Administration** panel and expand **Overview**->**Hierarchy Configuration**->**Boundaries**. Right-click **Boundaries** and create a new boundary which will correspond to an Active Directory site which must include domain users (see figure 3.1).



Configure settings for this boundary

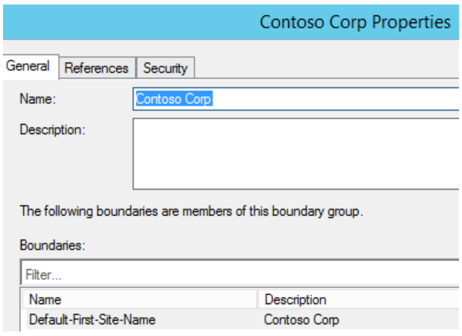
Description: Contoso Corp

Type: Active Directory site

Active Directory site name: Default-First-Site-Name

Figure 3.1: Boundary

2. Then, navigate to **Boundary Groups** and select the option **create Boundary Group**. Add the previously created boundary in this group (see figure 3.2).



Name: Contoso Corp

Description:

The following boundaries are members of this boundary group.

Boundaries:

Name	Description
Default-First-Site-Name	Contoso Corp

Figure 3.2: Boundary Group

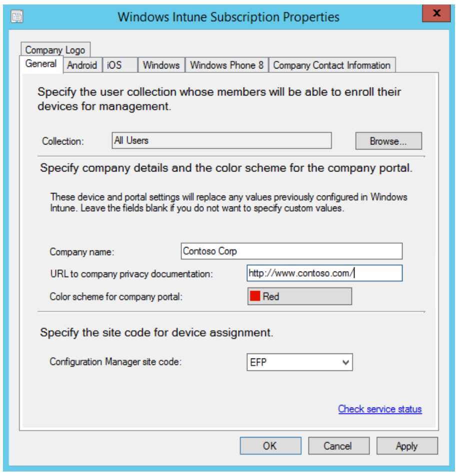
3. Go to the **Discovery Methods** linked to the Hierarchy Configuration, enable the **Active Directory User Discovery** and then select **Run Full Discovery Now**.
4. After a short period of time, all Active Directory users should be available in **Assets and Compliance**->**Overview**->**Users**.

Enabling Windows Phone Enrollment

Windows Intune Connector

The on-premises System Center Configuration Manager must be linked to Windows Intune to act as a mobile device management platform. You have first to declare (create) a Windows Intune subscription in SCCM and then install the Windows Intune Connector to act as a gateway.

1. In System Center, navigate to the **Administration** panel and expand **Overview**->**Cloud Services**. Right-click **Windows Intune Subscription** to create a new subscription. Follow the wizard, and fill in with your Windows Intune account and credentials when required. In the device enrollment selection, let everything unchecked. Select the **All Users** collection to allow all users to enroll their mobile devices (figure 3.3)



Specify the user collection whose members will be able to enroll their devices for management.

Collection: All Users

Specify company details and the color scheme for the company portal.

These device and portal settings will replace any values previously configured in Windows Intune. Leave the fields blank if you do not want to specify custom values.

Company name: Contoso Corp

URL to company privacy documentation: http://www.contoso.com/

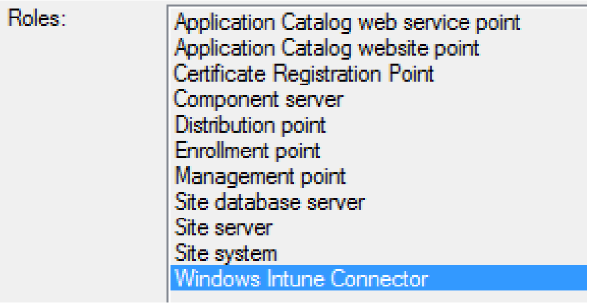
Color scheme for company portal: 🟥 Red

Specify the site code for device assignment.

Configuration Manager site code: EFP

Figure 3.3: Windows Intune Subscription

2. Once this step done, you have to add the **Windows Intune Connector System Role** to allow Windows Phone management. Go to the **Site system configuration** and select **Servers and Site System Roles**. Right-click the **System Center server** and **add a role**. In the role selection window, choose **Windows Intune Connector** as shown in the figure 3.4.



Roles:

Application Catalog web service point
Application Catalog website point
Certificate Registration Point
Component server
Distribution point
Enrollment point
Management point
Site database server
Site server
Site system
Windows Intune Connector

Figure 3.4: Windows Intune Connector

Company Portal

Windows Phone enrollment is available through a Company Portal application that needs to be signed with a certificate issued by Symantec. Two options are available:

- You can download the Company Portal application provided with Windows Intune and buy a Symantec Code Signing certificate in order to sign the portal application. You need in addition a Windows Phone Developer account that you can obtain by going to the **Windows Phone** website. This account is charged but can be obtained for free if you already have a MSDN subscription. For a complete description, please refer to **Windows_Intune_Windows_Phone_8_Walkthrough.pdf**[2]
- For demonstration purpose, you can use a trial pack which contains a signed certificate, a signed company portal and two basics apps. This is the **recommended option** for implementing this scenario.

Get the **Support Tool for Windows Intune Trial Management of Windows Phone**[3] and follow the installation steps.

1. **Download and Install the MSI** from this Microsoft Download Center page. It will extract the Support tool, signed Company Portal and other sample Windows Phone Apps included in the MSI. The default location for the files is *"C:\Program Files (x86)\Microsoft\Support Tool for Windows Intune Trial management of Windows Phone 8\"*
2. Within the Configuration Manager Console, select **Software Library** and navigate to **Overview** -> **Application Management** -> **Applications**. Right-click to create a new Windows Phone Application (**xap** file) which is the **Company Portal** for Windows Phone. Select SSP.xap that you will find

[2] **Windows Intune Windows Phone 8 Walkthrough :** http://download.microsoft.com/download/5/E/9/5E9F371B-65A3-4821-8A82-C4A68E81C120/Windows_Intune_Windows_Phone_8_Walkthrough.pdf

[3] **Support Tool for Windows Intune Trial Management of Windows Phone:** http://www.microsoft.com/en-us/download/details.aspx?id=39079

inside the "*Support Tool for Windows Intune Trial management of Windows Phone 8*" folder, and follow the wizard.

3. **Right-click** and **Deploy** this application to **Cloud Distribution Point** (manage.microsoft.com) targeting cloud managed users.
4. Now you can enable the management for Windows Phone 8.1 devices by opening a command prompt and running the script **ConfigureWP8Settings_Field.vbs** (included in the "*Support Tool for Windows Intune Trial management of Windows Phone 8*" folder) in query mode to get Company Portal name
   cscript ConfigureWP8Settings_Field.vbs EFP-Infra01.contoso.com QuerySSPModelName where EFP-Infra01.Contoso.com is server name for top level site (standalone site or CAS).
   The result looks like this "ScopeId_D863212F-F5D5-48EA-9C42-1CC6C0DDA03A/Application_95ac8248-d8fe-4686-9c16-e0a2fb0fe256". This will be used in the next step.
5. Run the script **ConfigureWP8Settings_Field.vbs** in save mode with SSP name. This will populate the necessary certificate information to enable Windows Phone 8 device management
   cscript ConfigureWP8Settings_Field.vbs EFP-Infra01.contoso.com SaveSettings ScopeId_D863212F-F5D5-48EA-9C42-1CC6C0DDA03A/Application_95ac8248-d8fe-4686-9c16-e0a2fb0fe256 where ScopeId_D863212F-F5D5-48EA-9C42-1CC6C0DDA03A/Application_95ac8248-d8fe-4686-9c16-e0a2fb0fe256 is the output from the earlier step.
6. After completion of the steps above, you can verify that Windows Phone 8.1 device management is enabled by going to the Intune subscription properties. Windows Phone 8.1 should be enabled, certificate should be present, and Company Portal App should be populated with whatever app you selected.
7. Deploy the sample apps provided in this package as appropriate
8. If you do not use a Microsoft domain name, users will now be able to enroll their Windows Phone 8.1 device and could browse the deployed sample apps in their Company Portal.

The next important step required to make Windows Phone enrollment operational is to synchronize identities between the on-premises Active Directory and the Windows Azure Active Directory.

Synchronization between on-premises Active Directory and Windows Azure Active Directory

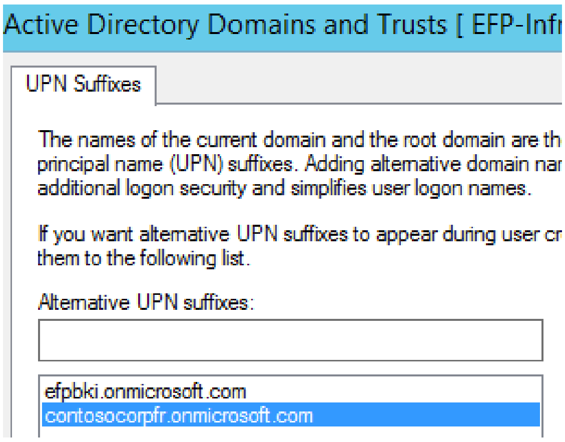
Before installing the directory synchronization tool, DirSync, you must check if, in your environment, the on-premises Active Directory forest name matches the Windows Azure Active Directory tenant domain name.

In the lab example, the Active Directory forest name **contoso.com** is different from the Windows Azure Active Directory tenant domain name **contosocoprfr.onmicrosoft.com**. To allow the Windows Phone enrollment feature, the User Principal Name (UPN) of user accounts that need to be synchronized must match the Windows Azure Active Directory domain name.

The UPN can be changed at the user level, but the best way to process is to create an additional UPN suffix at the forest level and affect the new UPN to targeted user accounts. For more information, please refer to **Add User Principal Name Suffixes**[4].

IMPORTANT: Note that this step is optional if the two domain names are identical.

1. **Log on as administrator** on your **Domain Controller** and open the **Active Directory Domain and Trusts** tool.
2. In the **Action** tab, select **Properties**. Add an **Alternative UPN suffix** (for ex. contosocorpfr.onmicrosoft.com) and **validate**. (See figure 3.5.)


Active Directory Domains and Trusts [EFP-Infr

The names of the current domain and the root domain are th
principal name (UPN) suffixes. Adding alternative domain nar
additional logon security and simplifies user logon names.

If you want alternative UPN suffixes to appear during user cr
them to the following list.

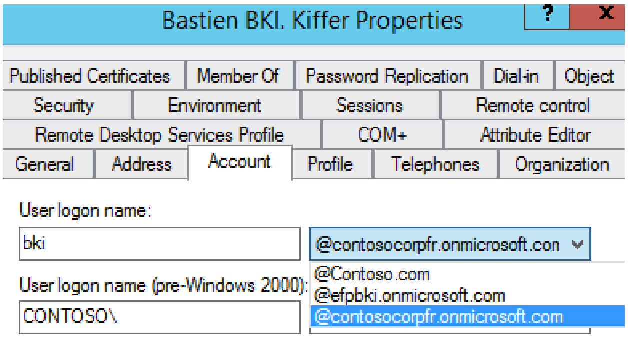
Alternative UPN suffixes:

efpbki.onmicrosoft.com
contosocorpfr.onmicrosoft.com

Figure 3.5: Active Directory Domains and Trusts

[4] **Add User Principal Name Suffixes** http://technet.microsoft.com/en-us/library/cc772007.aspx

3. In **Active Directory Users and Computers**, select one of the targeted users for whom you want to enable Windows Phone enrollment. Right-click the user account and select **Properties**. Go to the **Account** tab and change the user logon name with the additional UPN you previously set up (in this lab the UPN value which was initially contoso.com will be changed to contosocorpfr.onmicrosoft.com). See figure 3.6.



User logon name:
bki @contosocorpfr.onmicrosoft.con

@Contoso.com
@efpbki.onmicrosoft.com
@contosocorpfr.onmicrosoft.com

User logon name (pre-Windows 2000):
CONTOSO\

Figure 3.6: User logon name

On this next step, you will install the synchronization tool in order to project on-premises user accounts in the Azure Cloud directory and make them visible in the Windows Intune management portal.

First, go to the **Microsoft Azure portal**[5] and check, on the Active Directory tab, if **Active Directory Synchronization** is **enabled**. If not, **enable** it.

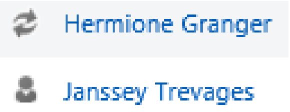
Then, go to the **Windows Intune management portal**[6] with an administrative account.

1. On the left panel, click **User** in the **Monitoring** group.
2. Click **Configuration** in the **Active Directory Synchronization**.
3. Check on Microsoft Azure, on the Active Directory tab, if **Active Directory Synchronization** is **enabled**. If not, **enable** it.
4. **Download** the synchronization **tool**. Once downloaded, **install** it by following the wizard. Installation can take several minutes.
5. First, the **Windows Azure Active Directory account** is required, then the **on-premises Active Directory account** has to be entered.
6. **Wait** a few minutes for the synchronization to occur and go back to the **Users** link in Windows Intune to see user accounts.

[5] **Microsoft Azure Portal** : https://manage.windowsazure.com/

[6] **Windows Intune Management Portal** : https://account.manage.microsoft.com/

7. On-premises users must have been synchronized and appear with the ⇄ icon. They need to be enabled by **clicking** on each one and selecting **Activate synchronized users**.



Hermione Granger

Janssey Trevages

Figure 3.7: On-premises and cloud hosted users

8. Select **Windows Intune Group** and specify the user country.

At this stage, users can enroll their device as described in the User Experience/ Windows Phone Enrollment section.

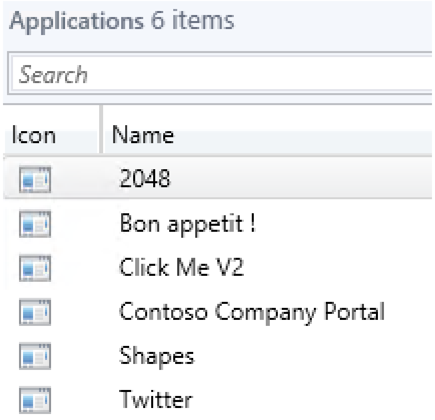
Deploying Enterprise Applications

After his/her Windows Phone enrollment, the employee will have to access the Company Portal in order to download business Company Apps.

This step describes how to deploy the sample application "Shapes" included in the the **Support Tool for Windows Intune Trial Management of Windows Phone**[7] package previously installed.

Note: *Push applications is not available on the current System Center version.*

1. Within the **System Center Configuration Manager** console, go to **Software Library**. Expand **Overview** and navigate to **Application Management**.



Applications 6 items

Search

Icon	Name
	2048
	Bon appetit !
	Click Me V2
	Contoso Company Portal
	Shapes
	Twitter

Figure 3.8: Enterprise Applications pool

2. Right-click **Applications** and choose **Create Application**.
3. Follow the wizard and select what kind of application you want to deploy (Windows Phone app package from a **xap file** or from the **Windows Phone Store**). In our case, we choose XAP file and fill in with the application's location *"C:\Program Files (x86)\Microsoft\Support Tool for Windows Intune Trial management of Windows Phone 8\Sample Apps\"*. Click **Next** two times.
4. In the **General Information** page, specify the **Application Name** (**Shapes** by default), click **Next** two times and then close the application wizard.
5. Now, right-click **Shapes** and click **Deploy**. Choose the **All users** collection then **Next**.

[7] **Support Tool for Windows Intune Trial Management of Windows Phone:** http://www.microsoft.com/en-us/download/details.aspx?id=39079

6. You need to select **specify Distribution Point**. Select the **Cloud Distribution Point** (Windows Intune) then click **Next**.
7. In **Deployment Settings**, select **Install** and **Available**. Click **Next** two times.

At this stage, users can go to the Company Portal to download Enterprise Apps as described in the User Experience/ Enterprise Applications section.

Security Policies

At the time of this writing, the current version of System Center Configuration Manager does not allow to manage the new Windows Phone 8.1 policies. However, Windows Intune can be used to specify and make them available to Windows Phone 8.1 devices.

Windows Intune

To deploy the new security policies with Windows Intune, follow these steps.

1. Go to the **Windows Intune admin console**[8] and navigate to the **policy** tab.
2. On the **Overview** page, choose **Add a policy** under the **Tasks** panel.
3. **Run the wizard** to select **security policy for mobile device**.
4. You can choose different security policies: cloud, mail account, apps, device features. For this demonstration, we want to disable the screen capture, camera and Windows Store. In the **System group**, enable **Allow screen capture** and select **No**. Do the same for **store apps** and **camera**.
5. **Save** the policy. Right-click on the policy and select **Deploy**.
6. After a short delay, the Windows Phone should receive the new policy settings. Please refer to the previous paragraph Error! Reference source not found. to see the corresponding user experience.

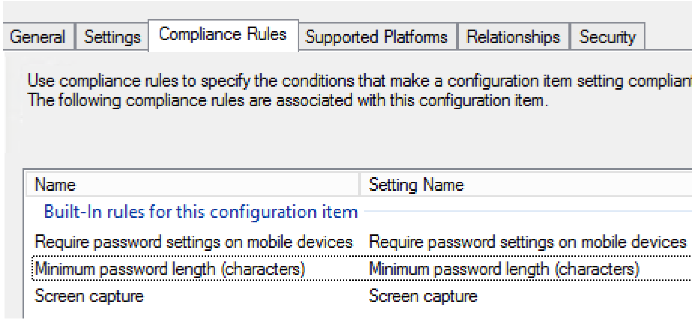
At this stage, security policies are deployed on users' Windows Phone; they will not be able to use the camera, store apps or make screen captures as described in the User Experience/Security Policies section.

[8] **Windows Intune Management Portal** : https://manage.microsoft.com/

System Center

As explained previously, deploying new policies for Windows 8.1 is not yet possible. However, the next section demonstrates how to use System Center Configuration Manager linked with Windows Intune (also called Windows Intune Unified Architecture) to deploy and enforce existing policies to increase enterprise security. A basic configuration including existing policies will be created to show how to proceed and could be enriched with new policies afterwards.

1. In **System Center Configuration Manager**, go to the **Assets and Compliance** tab. Expand **Overview** then **Compliance Settings** and **Configuration Items**.



Use compliance rules to specify the conditions that make a configuration item setting complian
The following compliance rules are associated with this configuration item.

Name	Setting Name
Built-In rules for this configuration item	
Require password settings on mobile devices	Require password settings on mobile devices
Minimum password length (characters)	Minimum password length (characters)
Screen capture	Screen capture

Figure 3.9: Compliance rules

2. Right-click **Configuration Items** then select **Create Configuration Item**.
3. To create a configuration item, a **name** (for example **Contoso Corp Policy**) is required and the **type of configuration item** (in our case, select **Mobile Device**). Then click **Next**.
4. Select **Device** then **Next**.
5. Locate the **Screen capture** section and click **Disabled** then **Next**.
6. Select **all the devices** then **Next three times** and close the wizard.
7. Go to the **Assets and Compliance** tab. Expand **Overview** then **Compliance Settings**. Finally right-click **Configuration Baselines** and then select **Create Configuration Baselines**.
8. Give a **name** to the baseline (for example **Windows Phone Configuration Baseline**).
9. In the **configuration table**, click **Add** and select **Configuration Items**. Choose **Contoso Corp Policy** and then **OK**.
10. Right-click on **Windows Phone Configuration Baseline** and deploy it to the **All user** collection. Schedule it to run every **15 minutes** to be sure that the baseline will be deployed on all the devices.

Resources

Windows Phone 8.1 Security Overview:

http://www.microsoft.com/en-us/download/details.aspx?id=42509

Support Tool for Windows Intune Trial Management of Windows Phone:

http://www.microsoft.com/en-us/download/details.aspx?id=39079

Windows Intune Portal:

https://manage.microsoft.com/

Windows Azure Portal:

https://manage.windowsazure.com/

Administrator Checklist: Configuring Configuration Manager to Manage Mobile Devices by Using Windows Intune:

http://technet.microsoft.com/en-us/library/jj943763.aspx

Windows_Intune_Windows_Phone_8_Walkthrough.pdf:

http://download.microsoft.com/download/5/E/9/5E9F371B-65A3-4821-8A82-C4A68E81C120/Windows_Intune_Windows_Phone_8_Walkthrough.pdf