Microsoft

Windows Tech Series

Security Module

10/7/2016

Version 1.1 Final

Prepared by

Sebastian Meiforth

Partner Technical Consultant]

[semeif@microsoft.com]

Contributors

[Type Contributors Here]

Versions

Version	Author	Changes
1.0	Semeif	
1.1	Semeif	Basic modules finished

Index

Prerequisites

Classroom:

PCs with IE 11 Browser
Internet Connection
Pre-checked access to Learn on demand LAB system

LAB System:

1 DC/DNS/DHCP (Server 2016 (Current Branch?))
1 Config Manager (Current Branch)/ADK full installation
1 Client saved to OOBE (possibility to apply ppkg)
1 Client Managed through Config Manager
1 BYOD Client
1 Windows 10 for Mobile emulator

Students:

Microsoft Account **with no Azure Trial attached** (if using trial)
Valid Credit Card for identification only
Mobile Phone (for receiving MFA Codes)

or

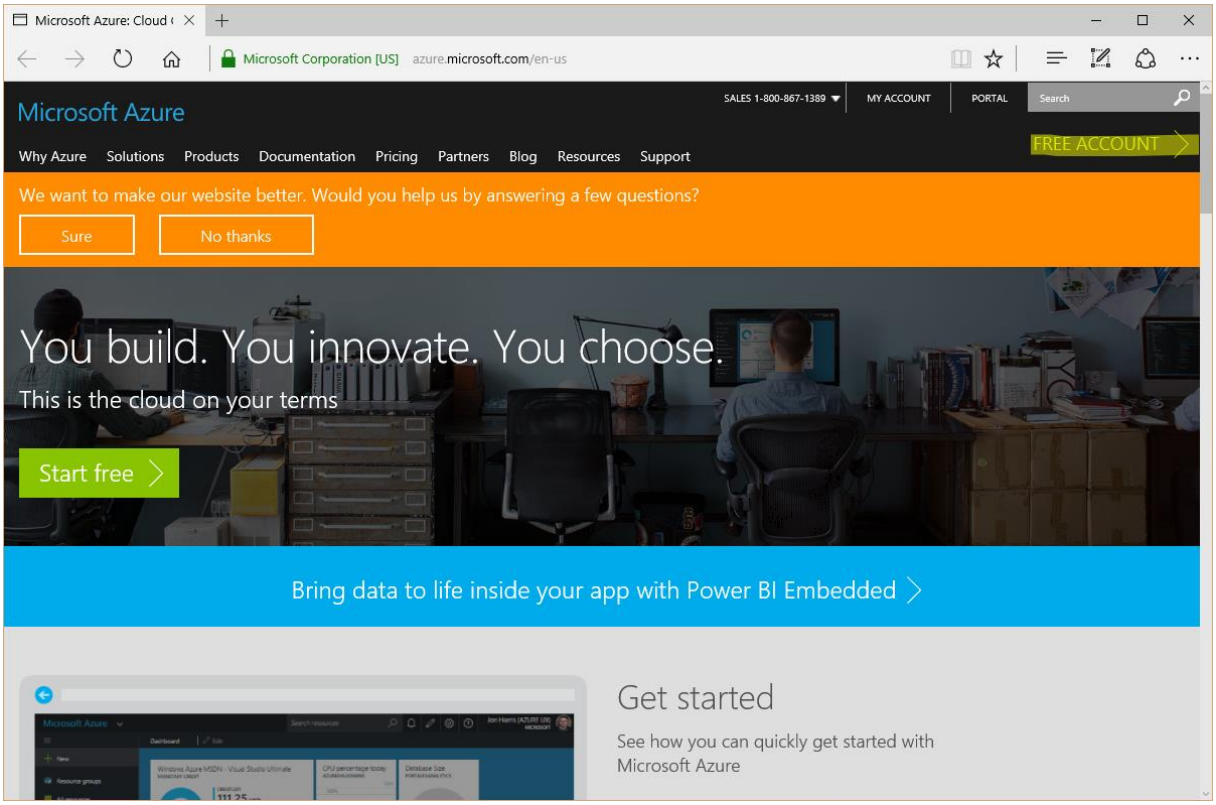
Azure trial subscription or Azure MSDN Subscription (with less than 18 Azure ADs)
EMS Trial or Partner Licenses for demonstration purpose.
Mobile Phone (for receiving MFA Codes)

1. Lab guide part 1 – Security with EMS

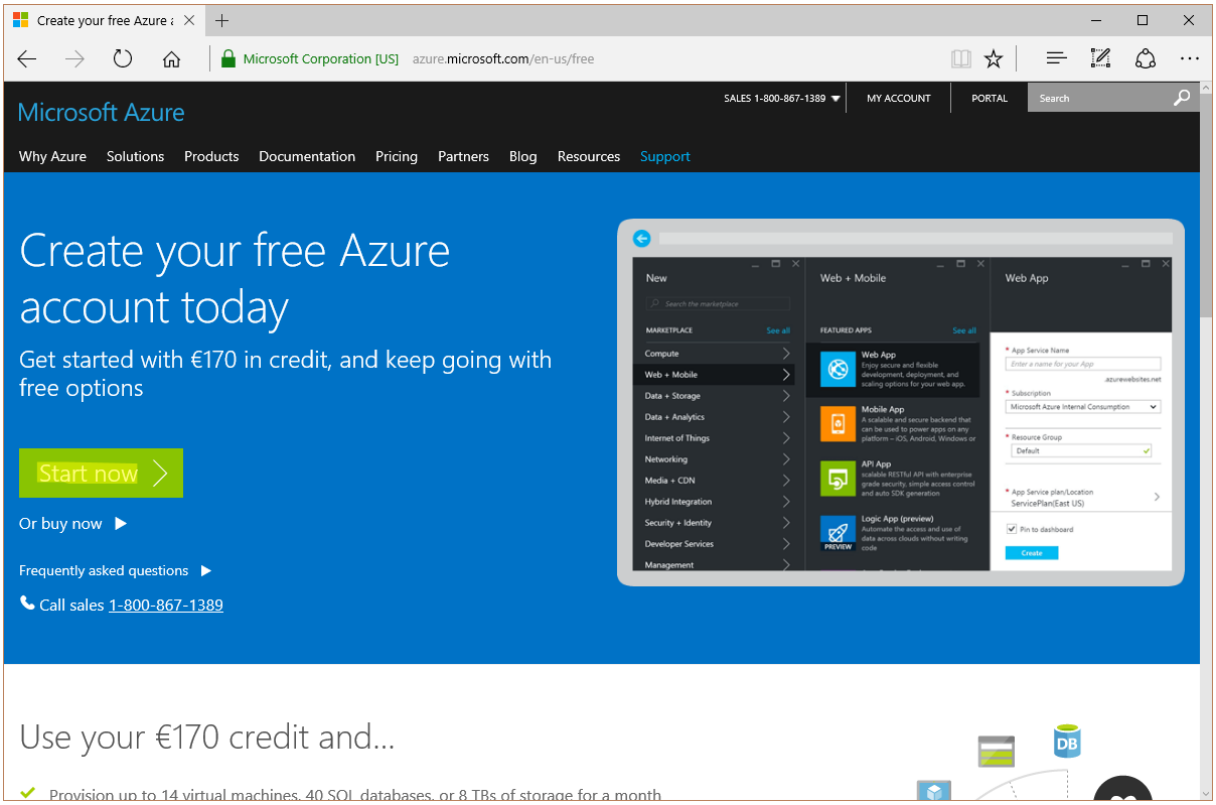
1.1. Azure AD & EMS setup and configuration

1.1.1. Create Microsoft Azure Trial account (Time: 5:00)

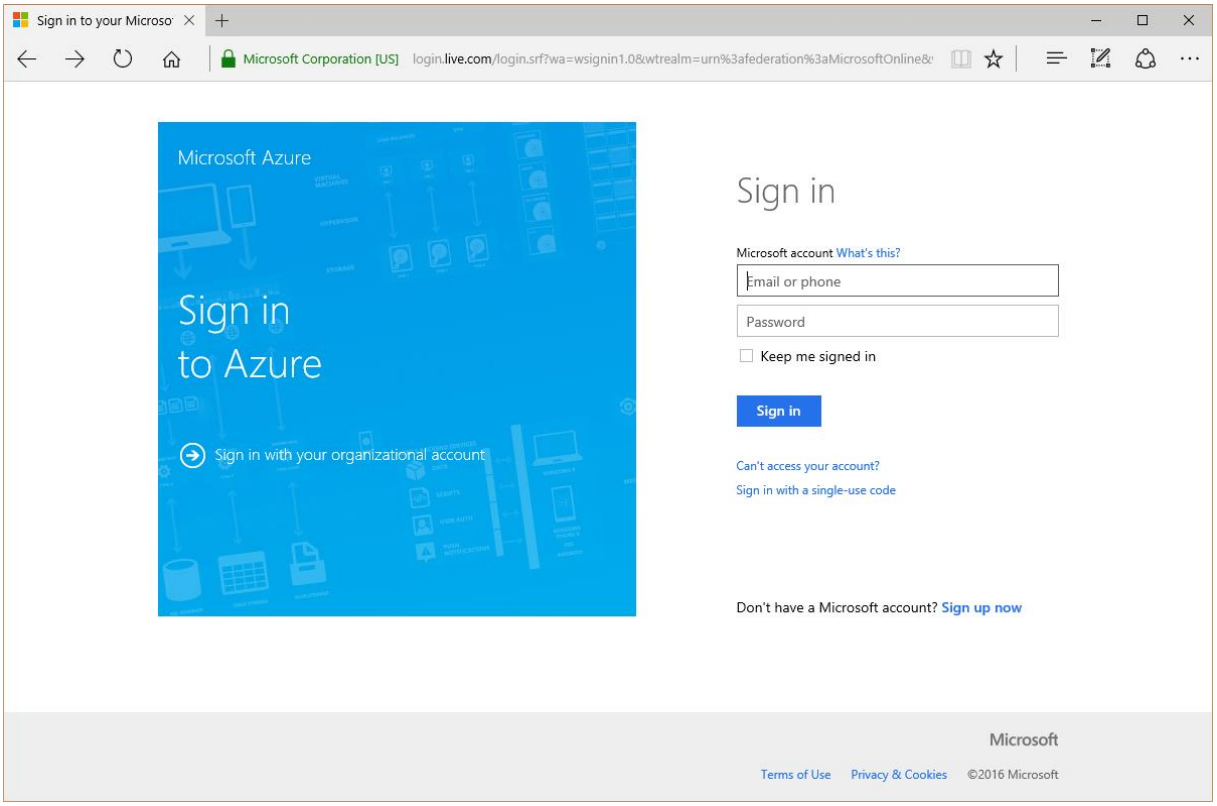
2. Navigate to https://azure.microsoft.com/en-us/ and click "Free Account".



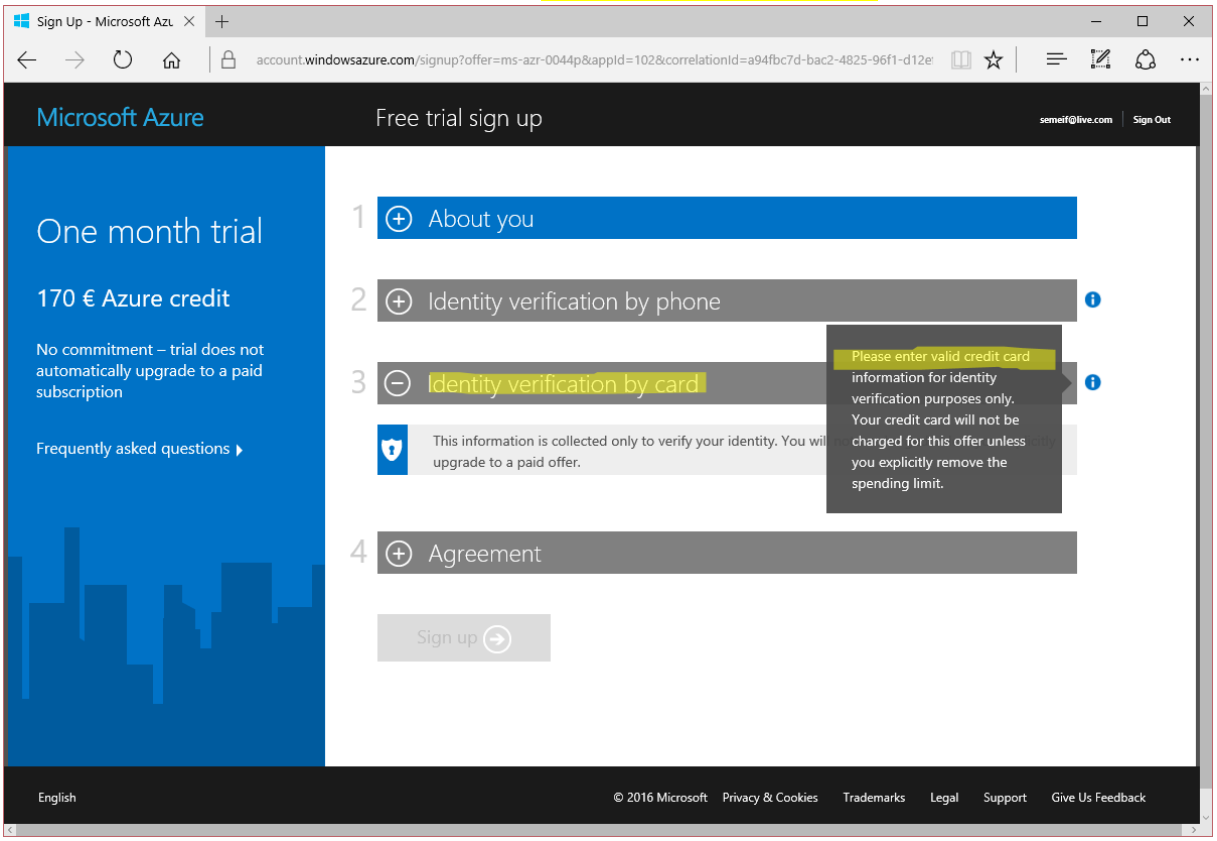
3. On the next page click "Start now".



4. Sign-in with a Microsoft Account.



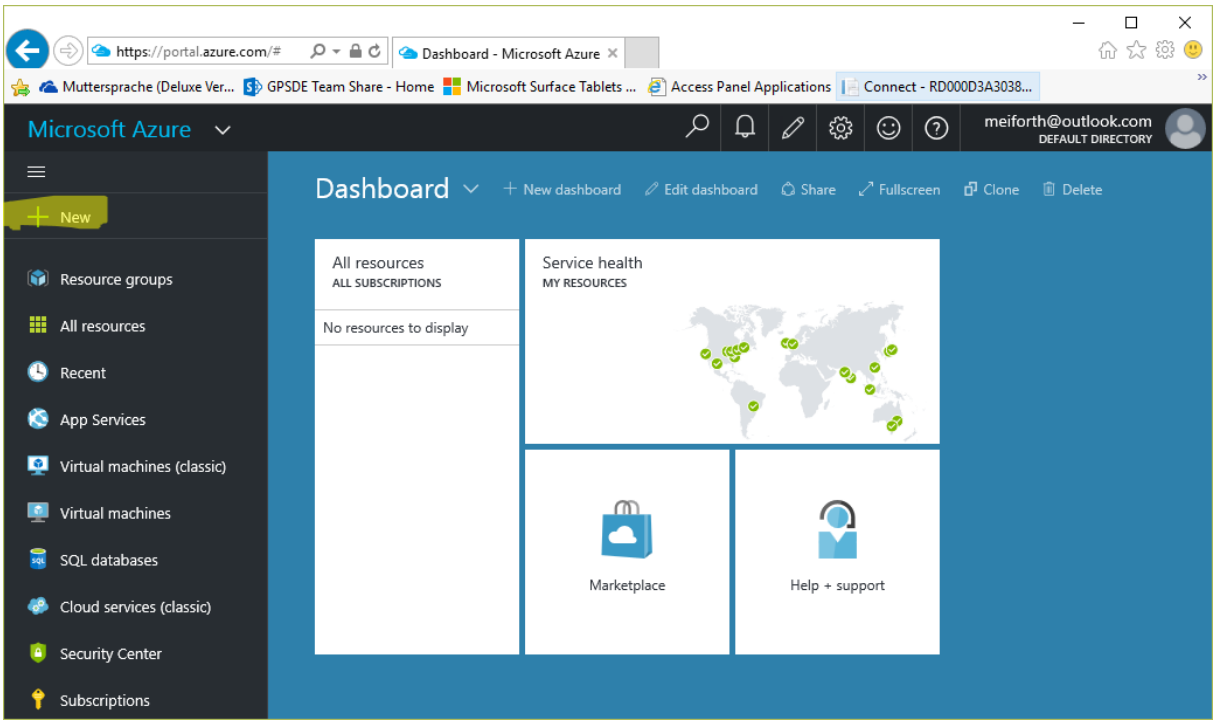
5. Enter additional verification information. (Valid Credit Card required!!!)



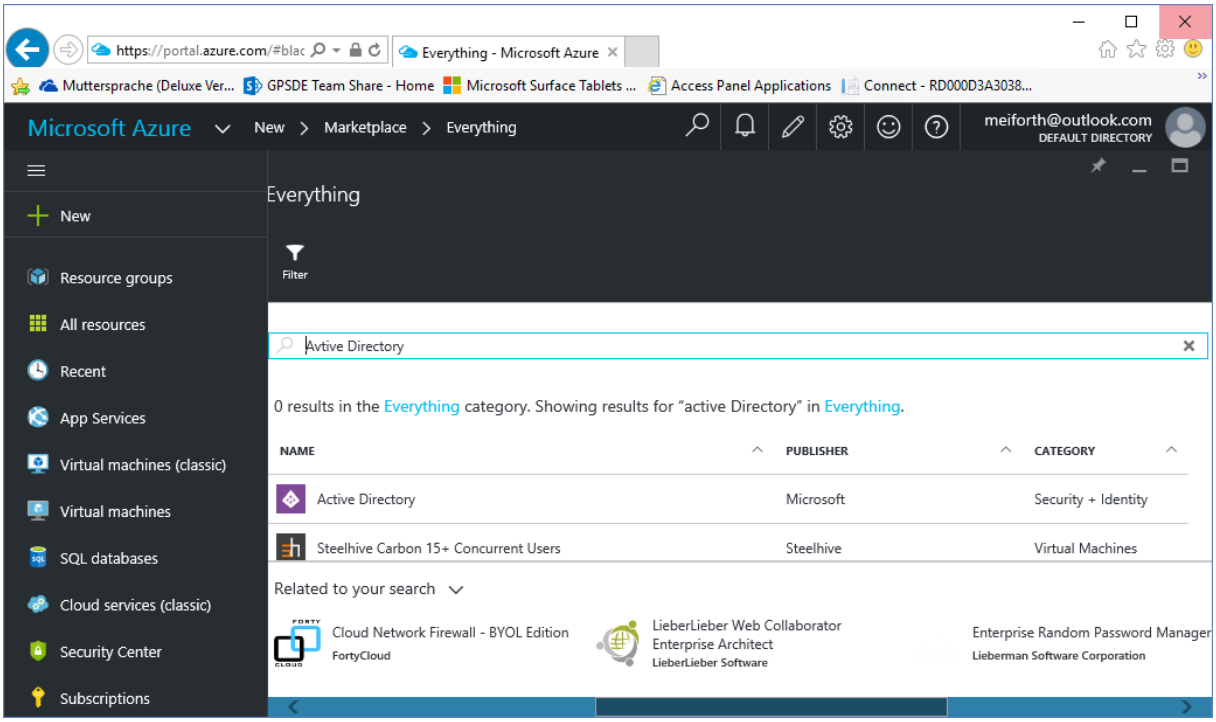
6. The Trial should be ready in a few minutes.

1.1.2. Create Azure AD (Time: 6:30)

1. When the setup has completed click on “Start managing my service”.
2. In the Microsoft Azure portal click “+ New”.



3. Search for “Active Directory”.



4. Click on 

.

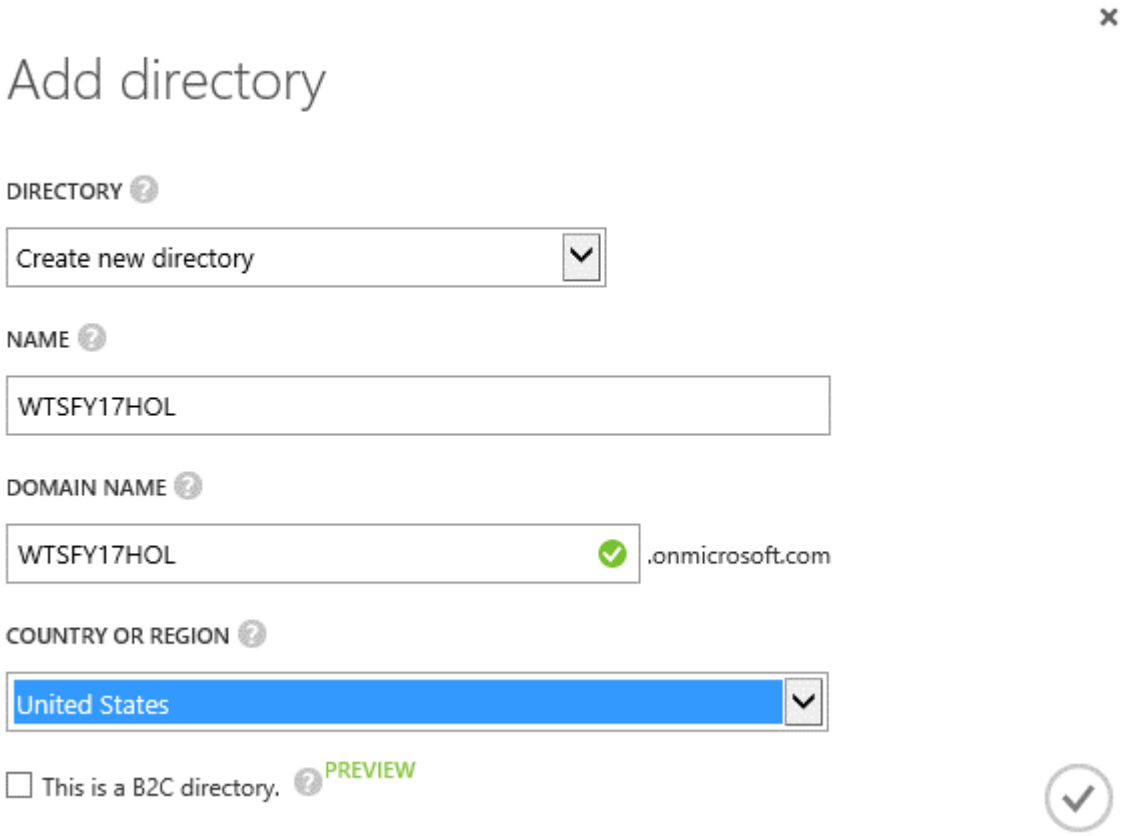
5. Click on 

.

1.1.3. Azure AD in the “old” Portal

1. You will be forwarded to the “old” Azure Portal right into the “active directory” workspace. Click on 

.
2. Create a new directory give it a Name, choose a free Domain Name and enter the appropriate Country or Region. Then click on 
.



3. Now your Active Directory will be created and shows up with the status 

in the console.
4. Click on the name of your just created Active Directory to start the configuration.
5. On the Get Started page scroll down to 

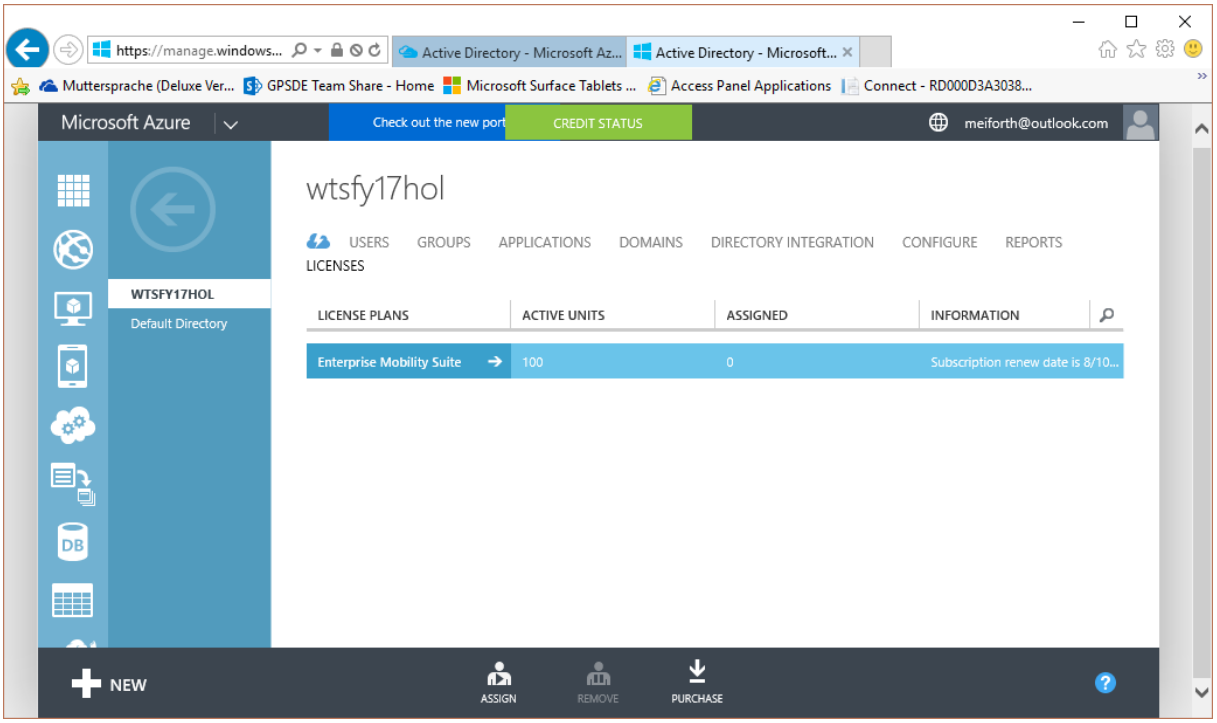
and click on 

.
6. On the next screen click on 

.
7. To Activate Enterprise Mobility Suite trial, click on 
.
8. Now the EMS will be attached to your AD.
9. Click on 

to check the status.

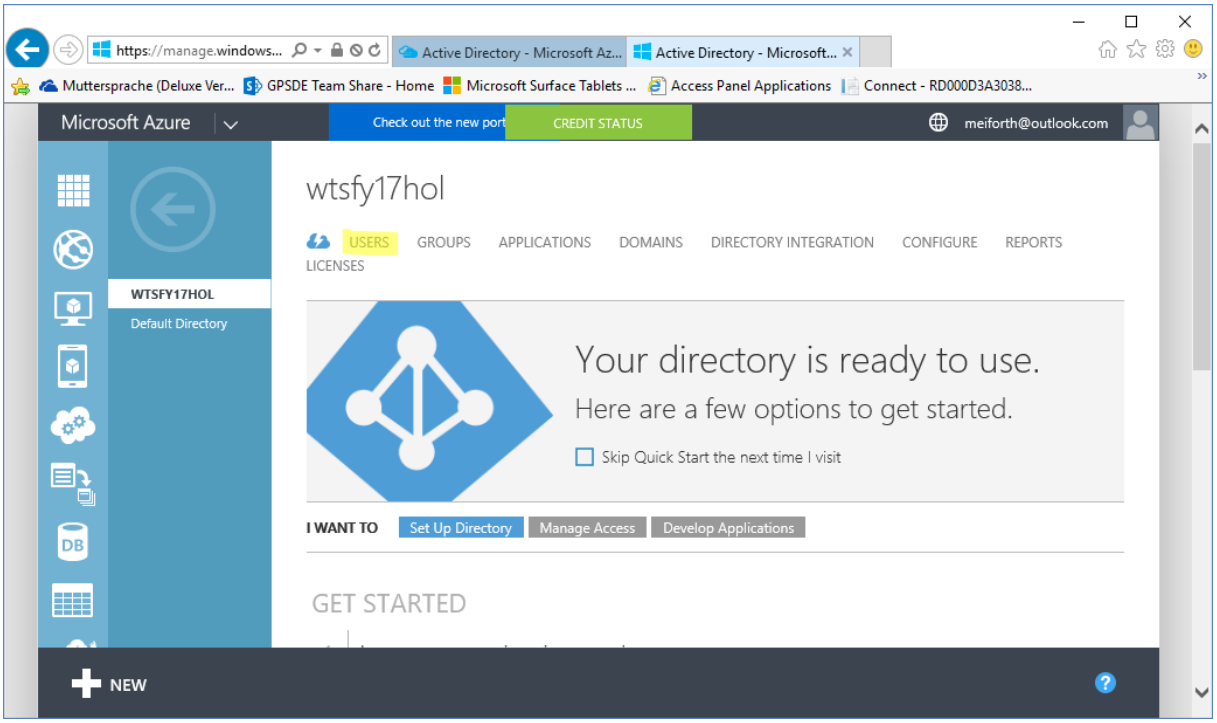
10. After a short time, the License should show up in the “Licenses” section of your Active Directory.



1.1.4. Configure Azure Active Directory

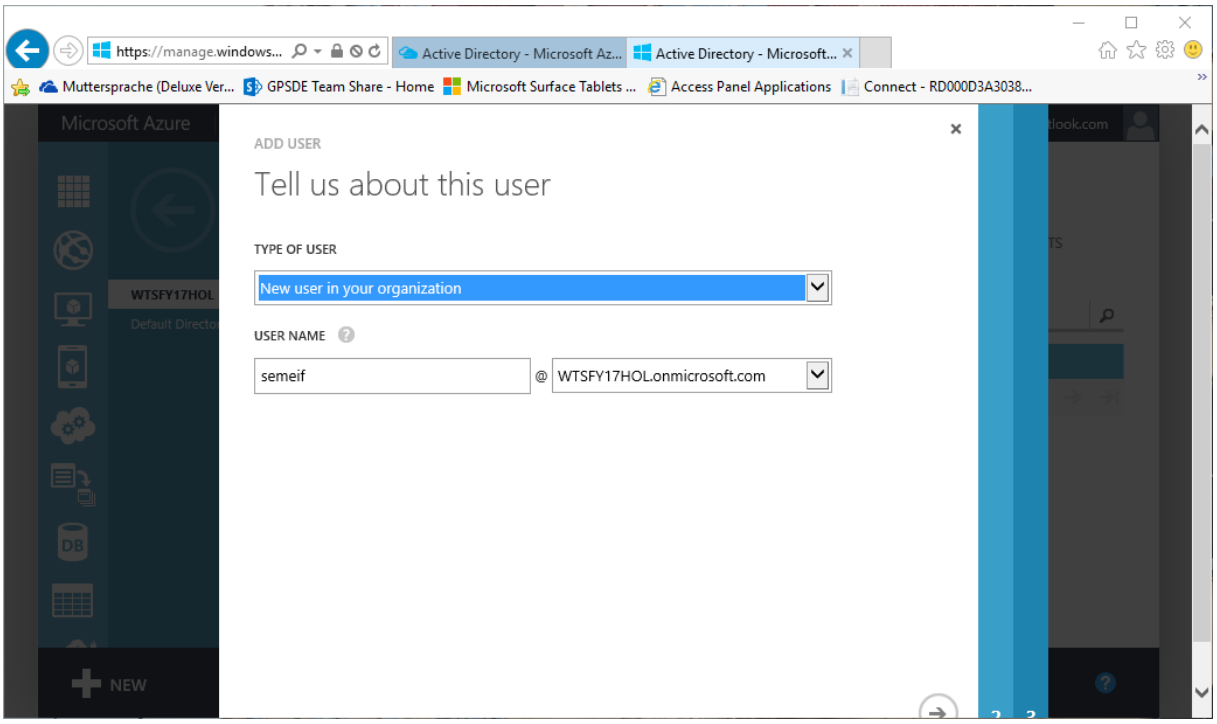
Create Global Administrator

1. In the administration workspace of your Active Directory click on the “Users” section.

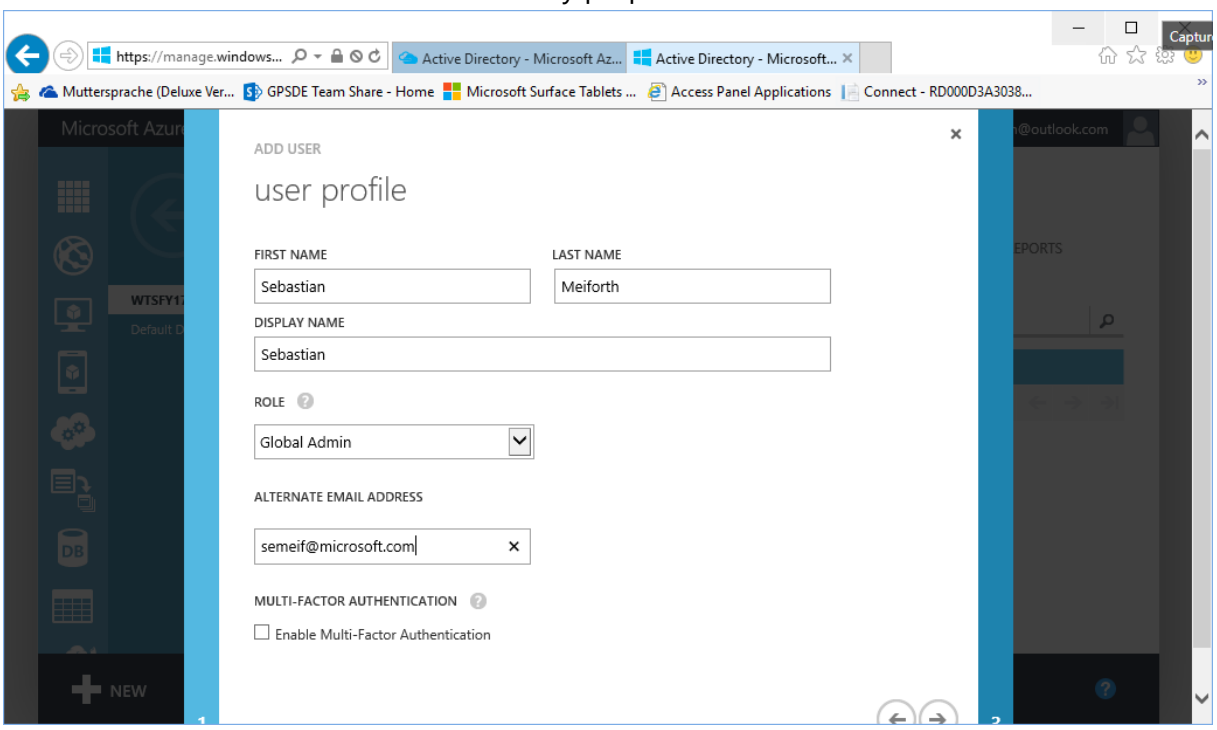


2. Click on 

.
3. Select “New user in your organization” and give it a “User Name”.



4. Enter the user profile information and choose „Global Admin” as a Role. Enter an alternate email address for account recovery purposes. Then click 
.



5. Click on 

to get a temporary password.
6. Open a “In-Private” browsing session and navigate to http://myapps.microsoft.com.
7. Enter the just created global admin credentials and click next.
8. On the next page enter the temporary password and click “Sign-in”.

9. Now the temporary password can be replaced with a new password.
10. Close the "In-Private" browser window.
11. In the window where we just created the user click on  .

Assign EMS License to the Global Administrator

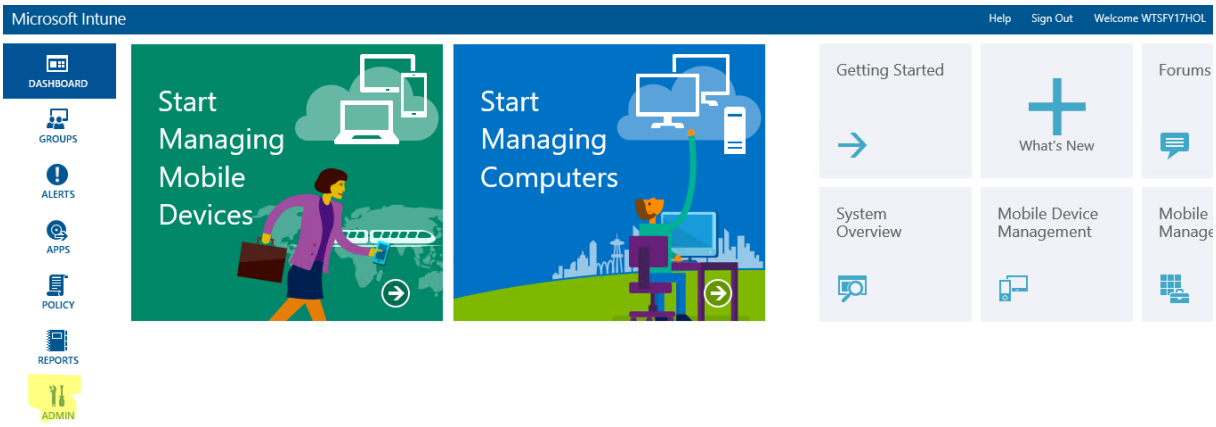
1. In the administration workspace of your Active Directory click on the "Licenses" section.
2. Click 

.
3. Select the just created Global Administrator user and click on  .

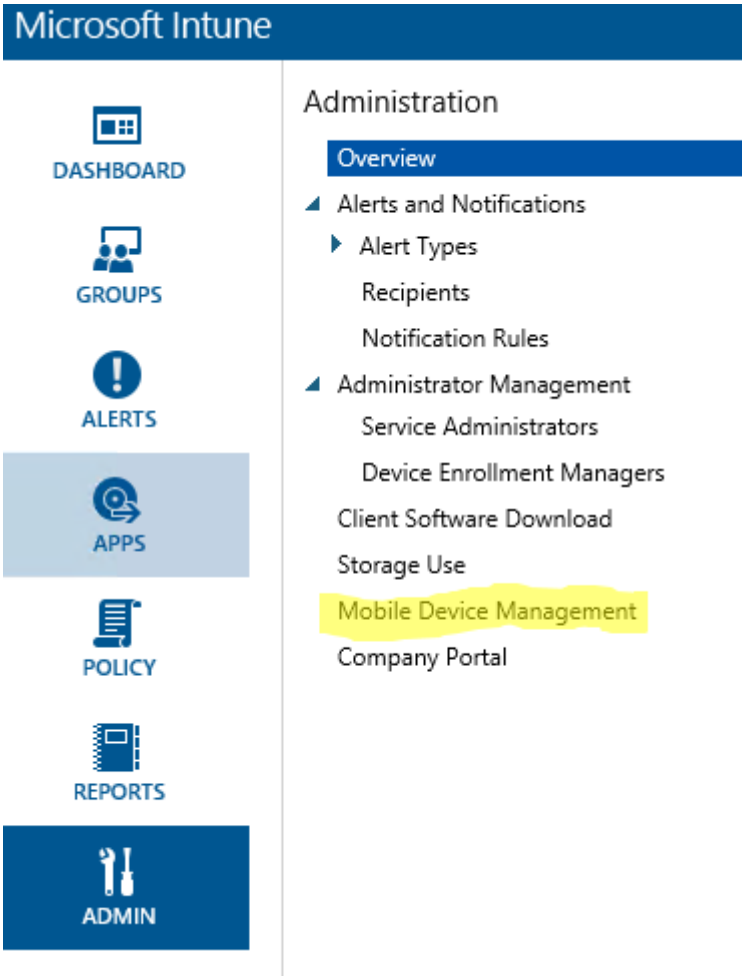
1.1.5. Intune setup and initial configuration (Time: 5:00)

Activate Intune as Mobile Device Management Authority

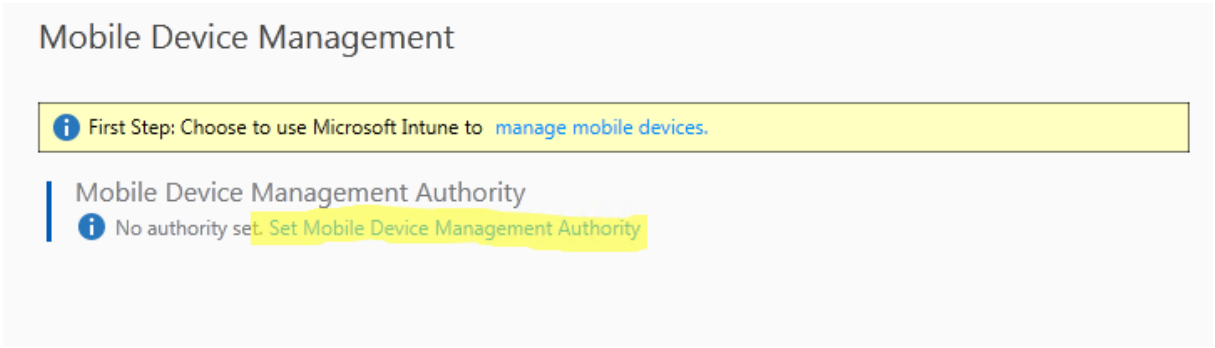
1. On your PC open http://manage.microsoft.com. (Use Internet Explorer or any other SilverLight capable browser.)
2. Log on with the Global Administrator created in the Azure Active Directory section.
3. In the Microsoft Intune Management Console open the Admin workspace.



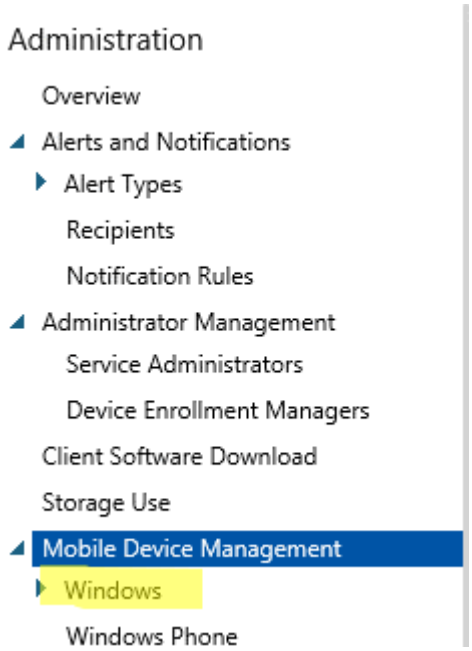
4. Navigate to the Mobile Device Management section.



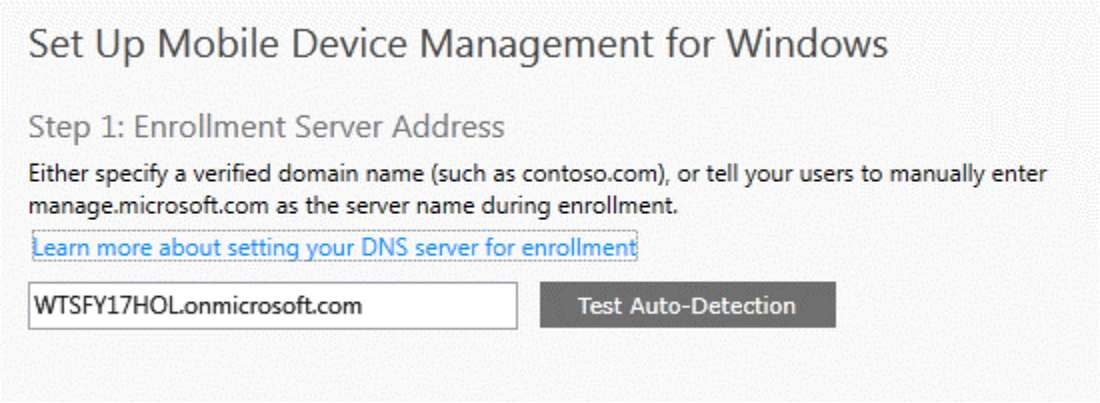
5. Click on „Set Mobile Device Management Authority“.



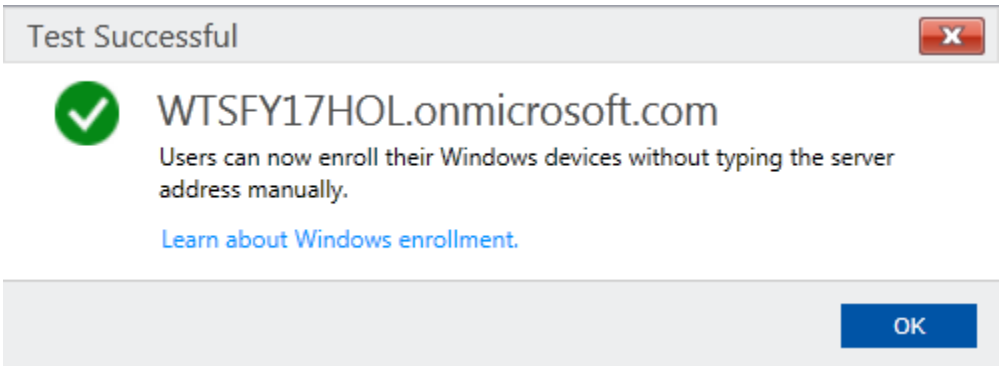
6. Open the „Windows“ section.



7. Enter your Azure Active Directory domain name in the “Enrollment Server Address” field and click on “Test Auto-Detection”.

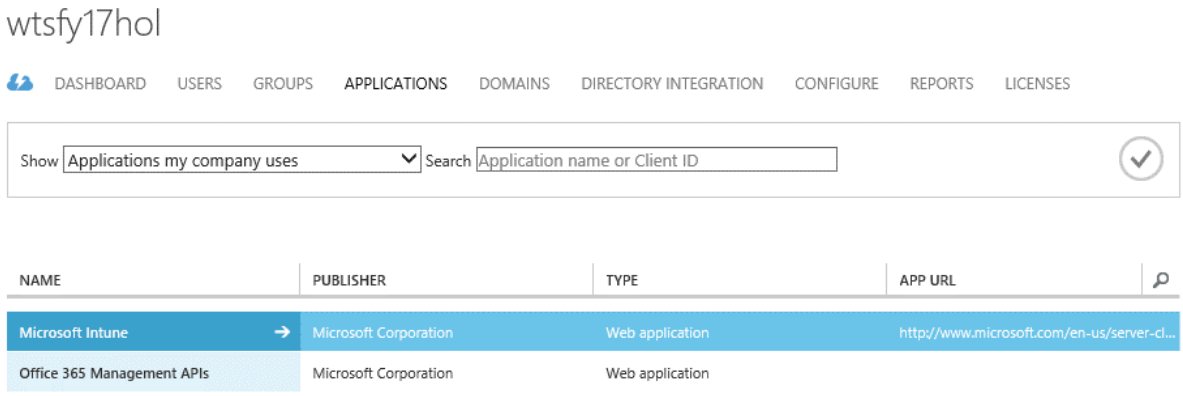


8. Wait for the test to finish and review the result and click OK.

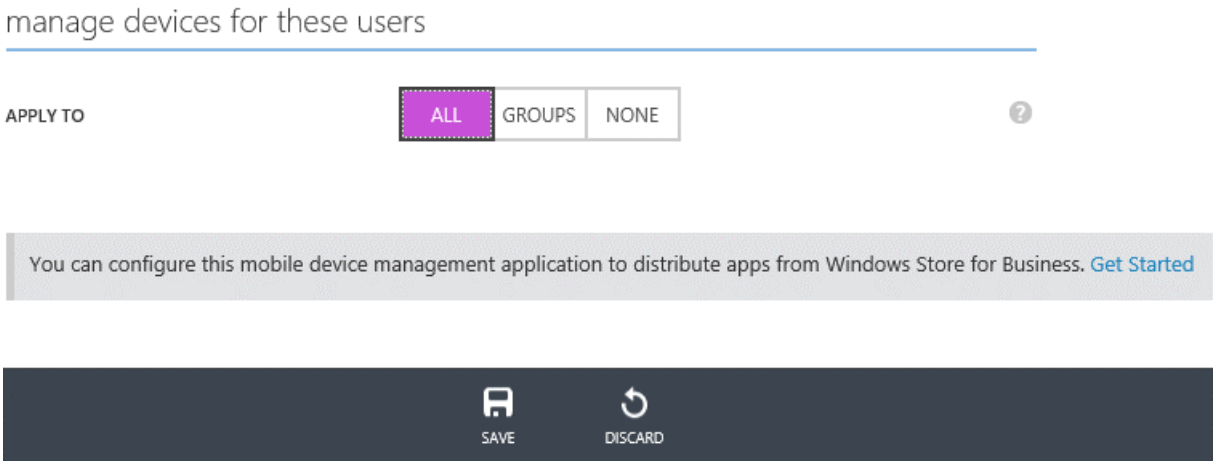


Activate Mobile Device Management in Azure Active Directory

1. Navigate to the "Applications" section in the Azure Active Directory Workspace and click on "Microsoft Intune".



2. Within the Microsoft Intune App click on Configure.
3. In the "manage devices for these users" select "All" and click "SAVE".

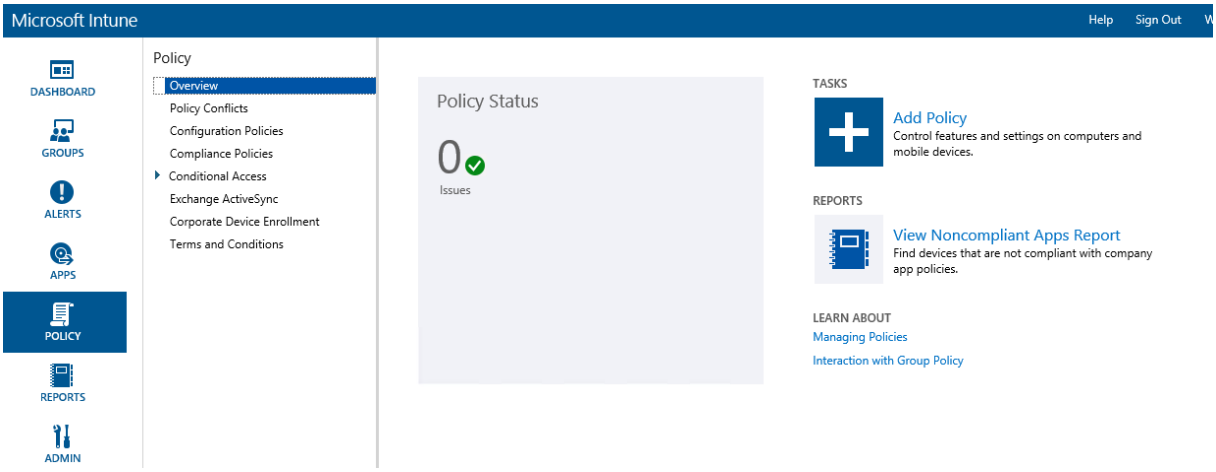


1.2. Set MDM Policies in Intune (EDP, Whitelist Apps..) (Time: 20:00)

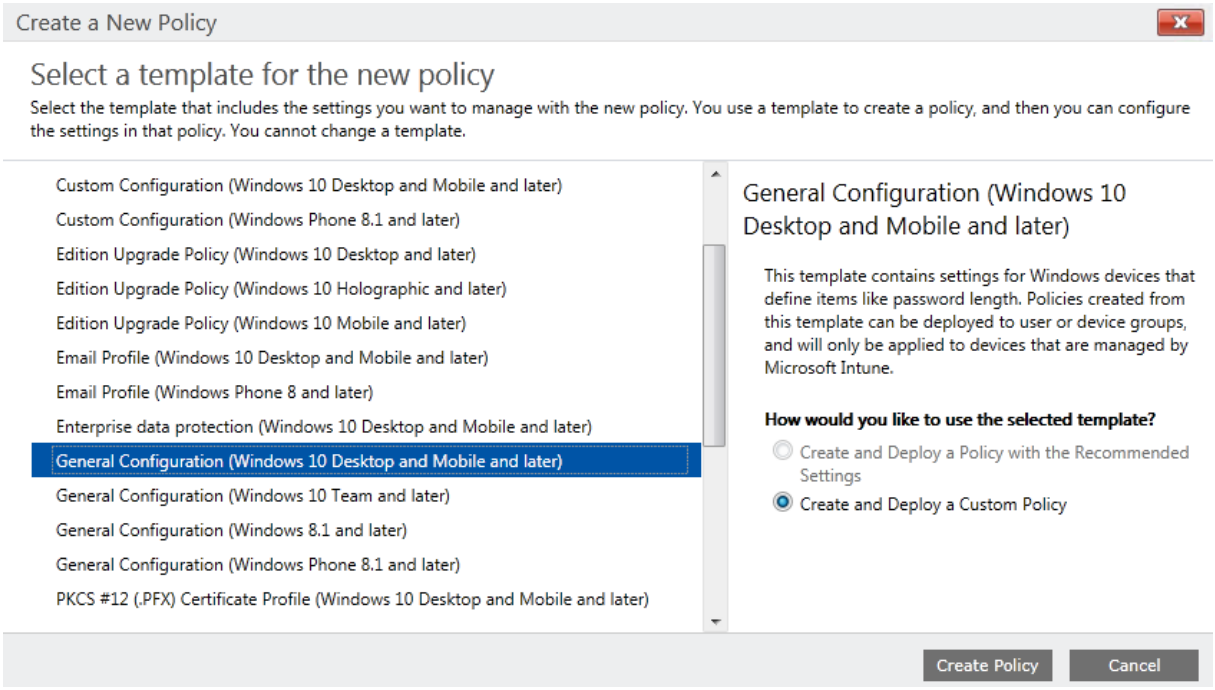
Create PIN Policy

1. On WTS-12-CLI.
2. Open http://manage.microsoft.com in Internet Explorer
3. Log on with the Global Administrator created in the Azure Active Directory section

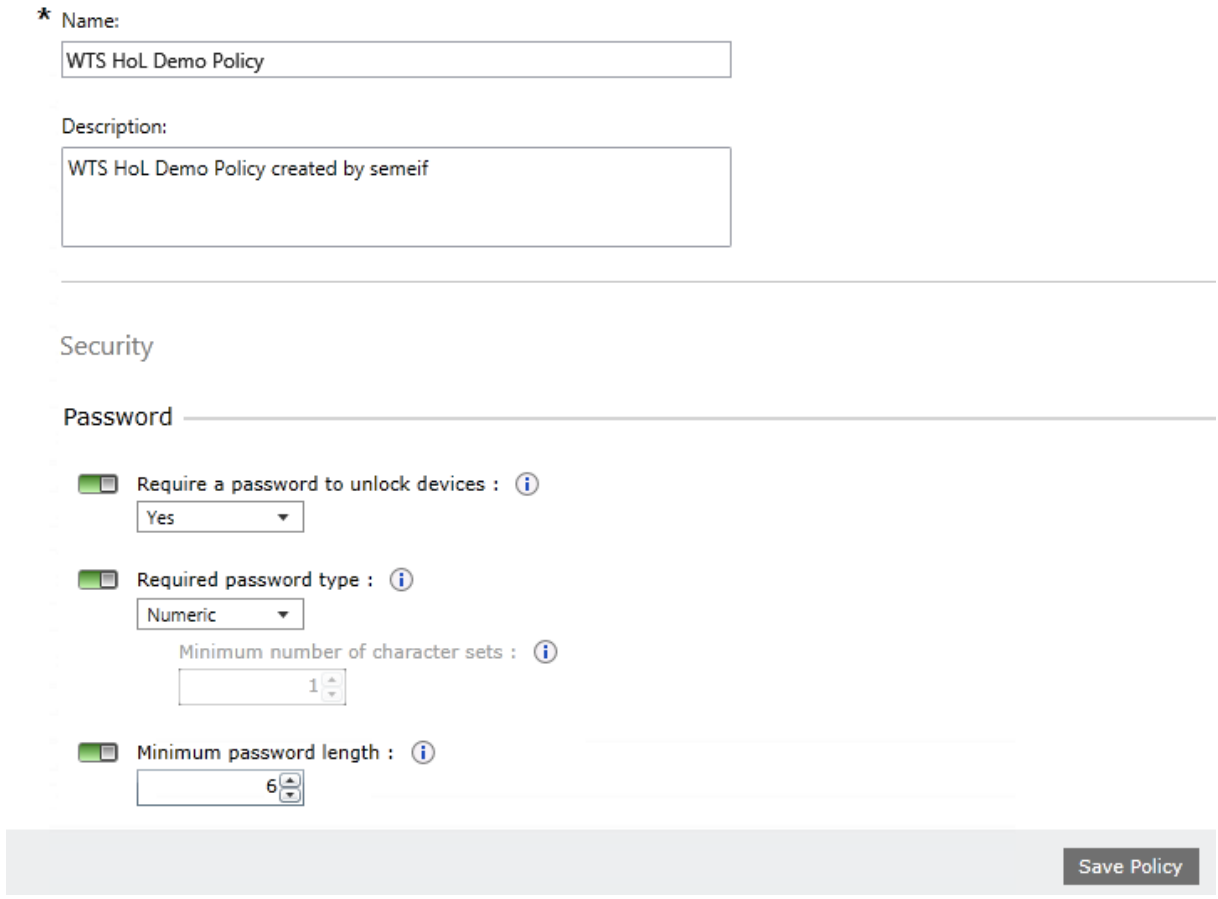
4. Browse to “Polcy” Workspace in Microsoft Intune and click on “Add Policy”



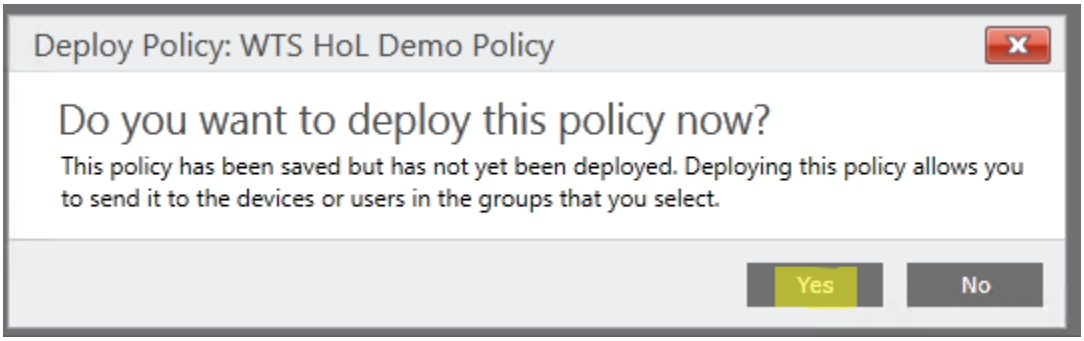
5. Choose “General Configuration (Windows 10 Desktop and Mobile and later) Template and click “Create Policy”



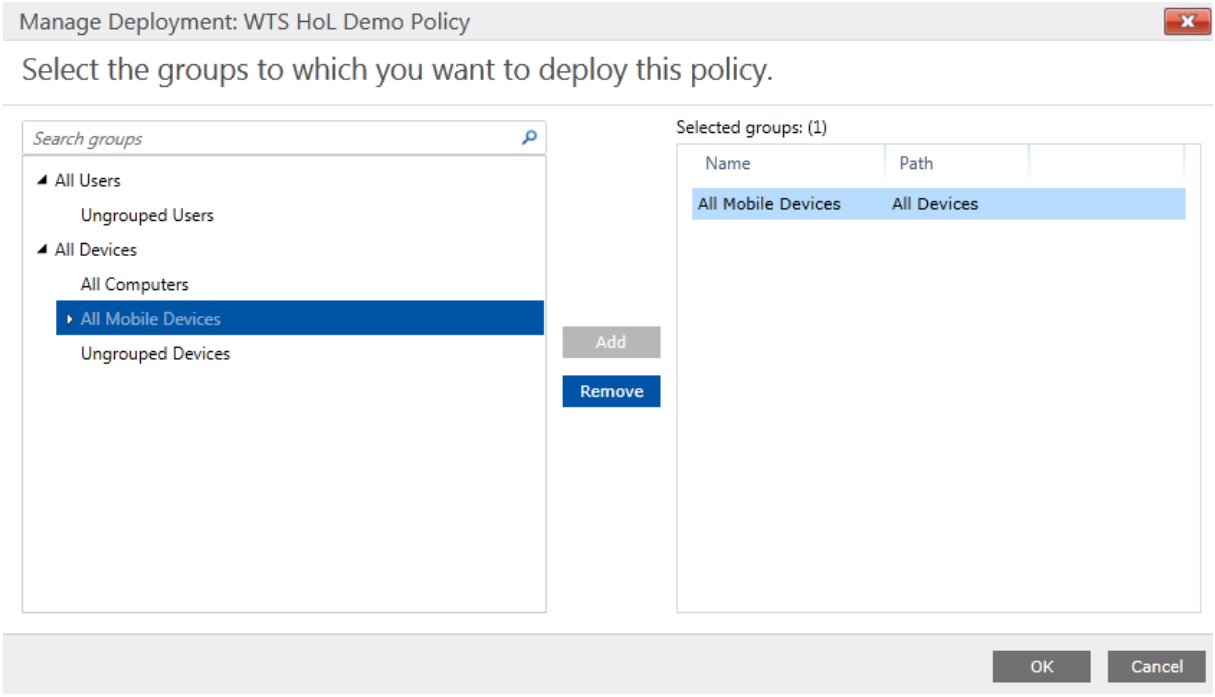
6. Enter a Password policy like shown in the screenshot and click on “Save Policy”.



7. On the “Deploy Policy” window click “Yes”



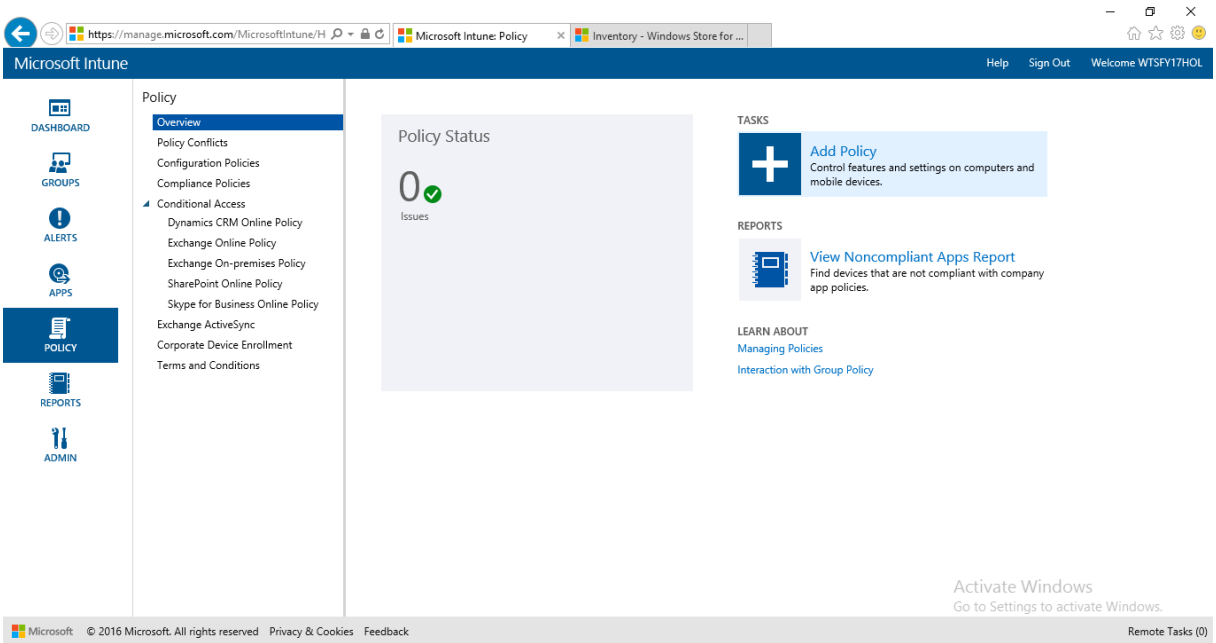
8. On the Manage Deployment for your just created policy select „All Mobile Devices" and click "Add" then click "OK".



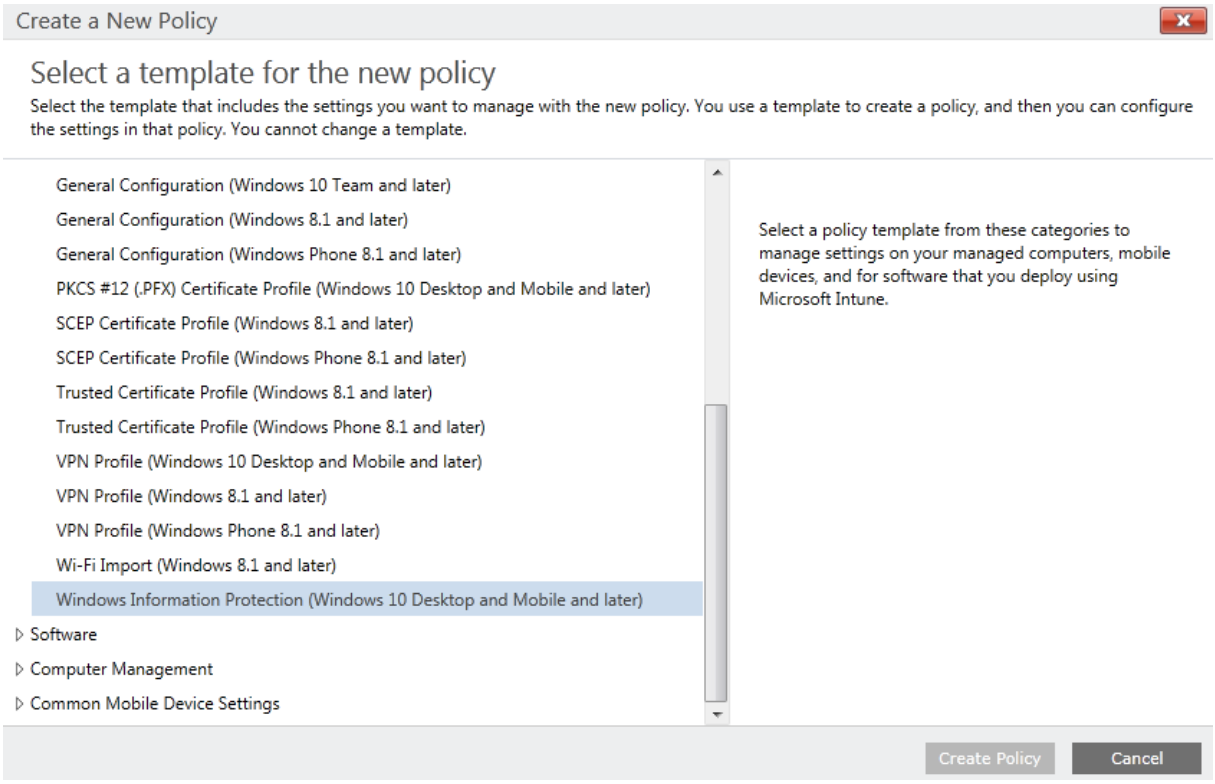
9. Your Policy will now be applied to all systems which are managed through MDM.

Create Windows Information Protection Policy

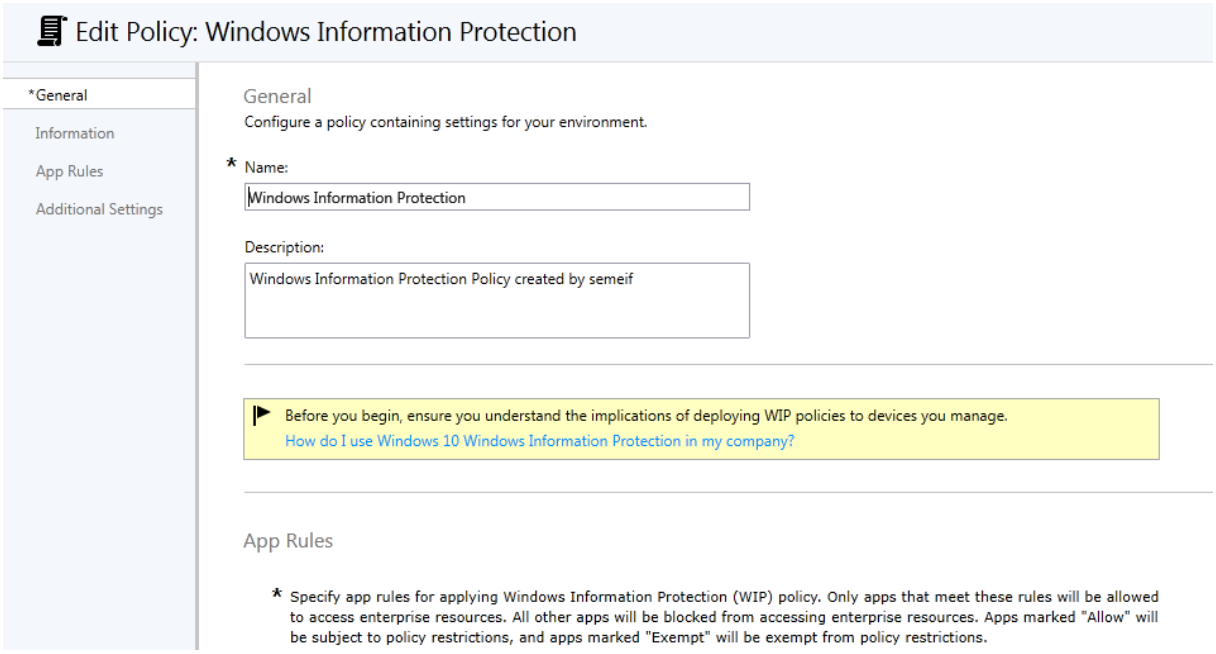
1. On WTS-12-CLI.
2. Open http://manage.microsoft.com
3. Log on with the Global Administrator created in the Azure Active Directory section.
4. Navigate to the "Policy" workspace and click on "Add Policy"



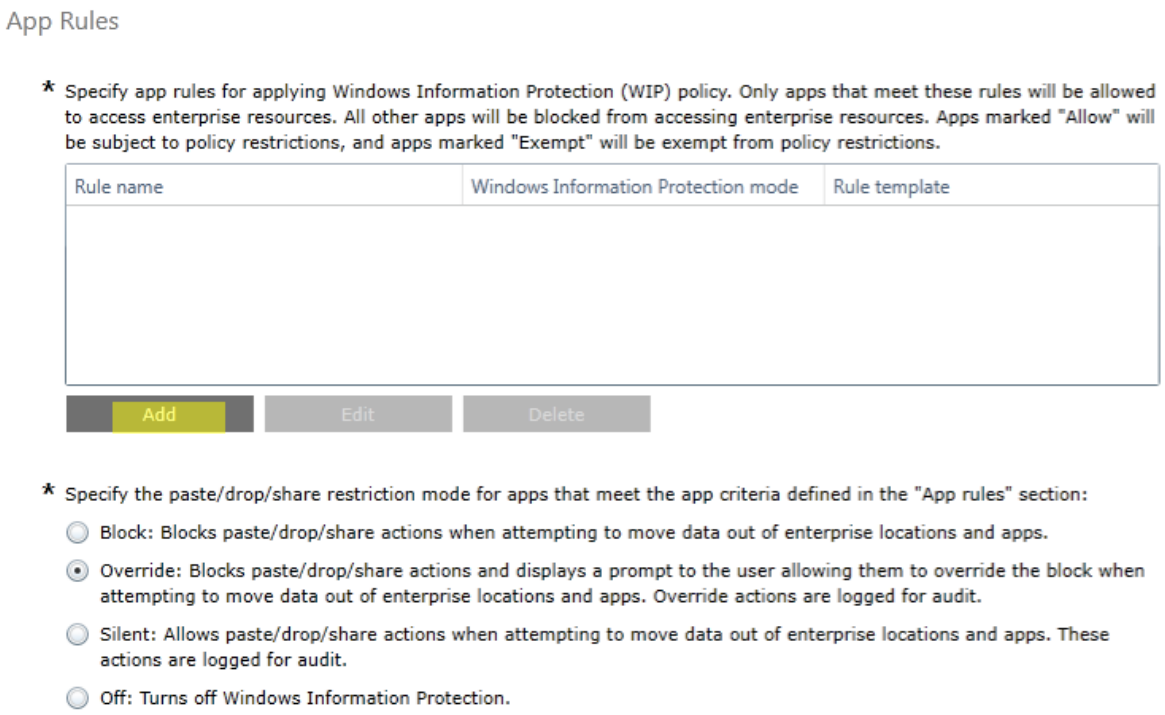
5. Expand Windows and select “Windows Information Protection” and click on “Create Policy”.



6. Enter a policy name and description.

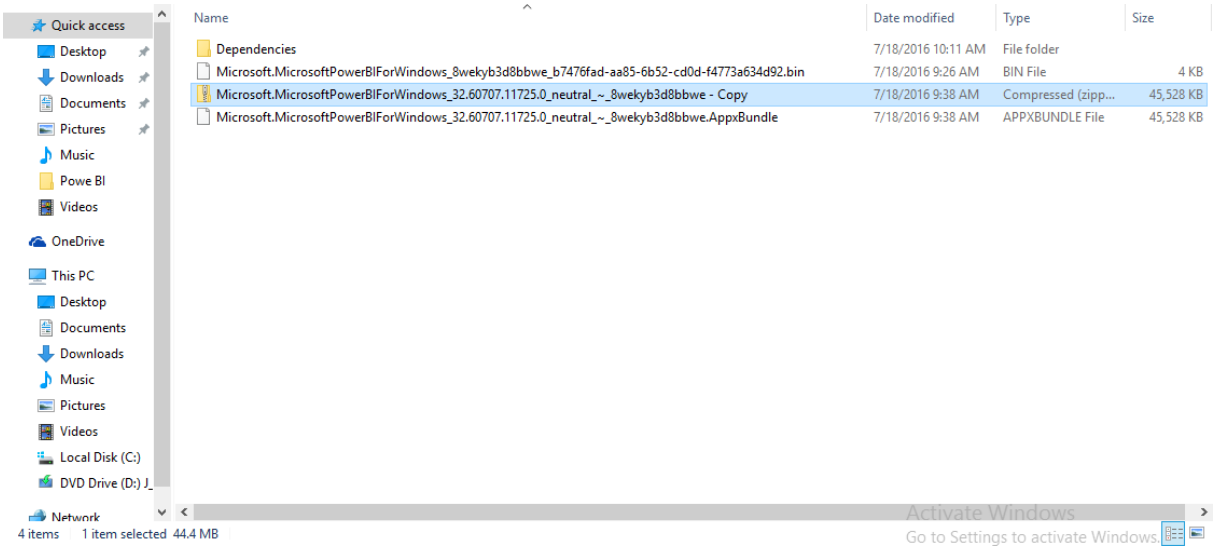


7. In the “App Rules” section click on “Add”.

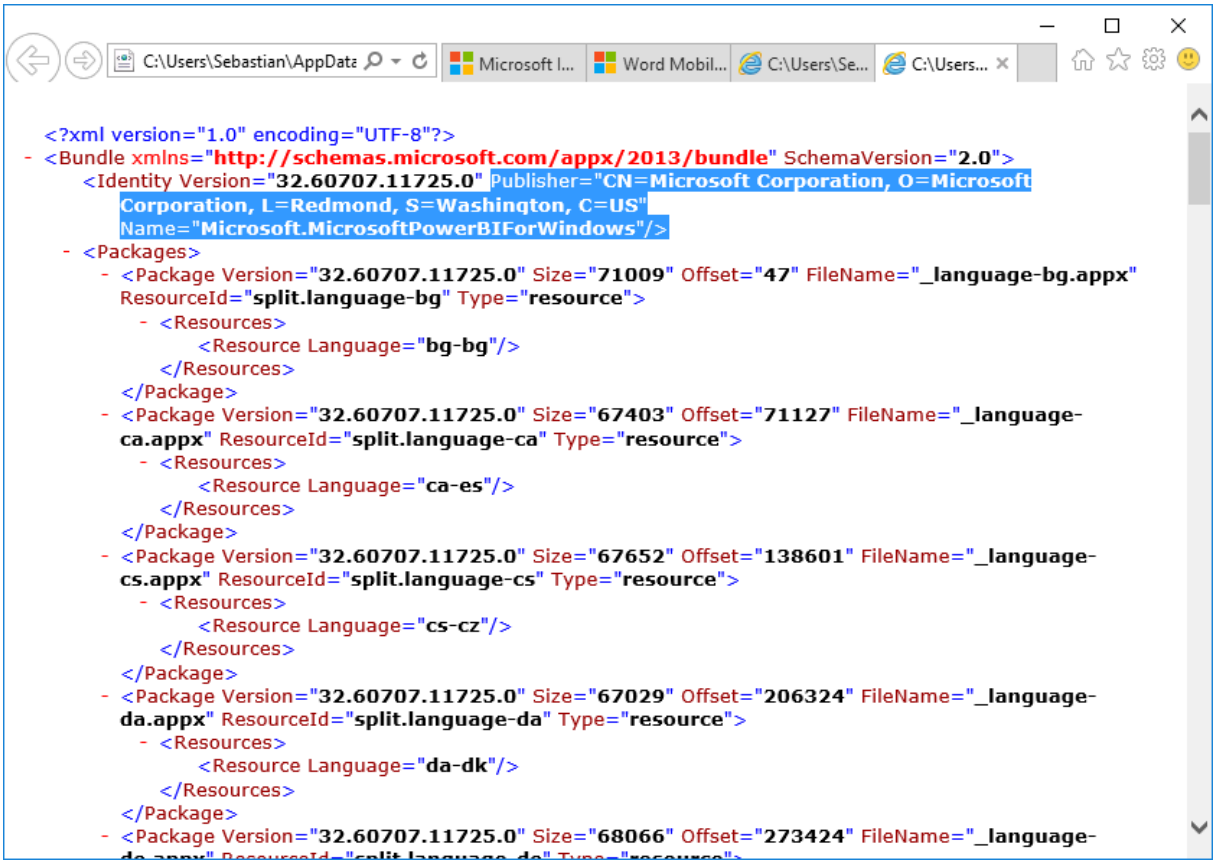


8. In the “Add App Rule” page enter the following information and click “OK”:
   Title: Power BI
   Enterprise data protection mode: Allow
   Rule template: Store App
   Publisher: CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
   Product name: Microsoft.MicrosoftPowerBIForWindows
9. Repeat the step for “Word Mobile”
   Title: Word Mobile
   Enterprise data protection mode: Allow
   Rule template: Store App
   Publisher: CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
   Product name: Microsoft.Office.Word
10. Repeat the step for “Mail and Calendar”
    Title: Communications Apps
    Enterprise data protection mode: Allow
    Rule template: Store App
    Publisher: CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
    Product name: microsoft.windowscommunicationsapps

11. **FYI only:** You can get the **above information** from the appxbundle file. If exchange the .appxbundle file extention with .zip you can open the File within the file explorer.

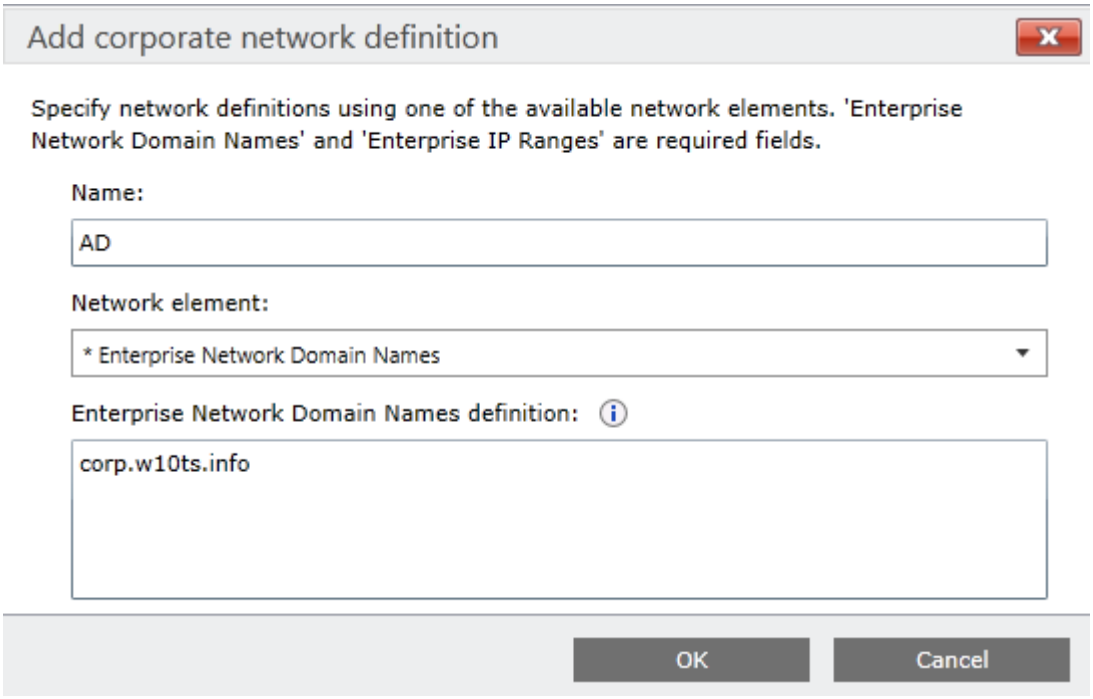


12. Within the Zip browse to the Folder AppxMetadata and open the AppxBundleManifest.xml. there you find the needed Information. Publisher and Name.

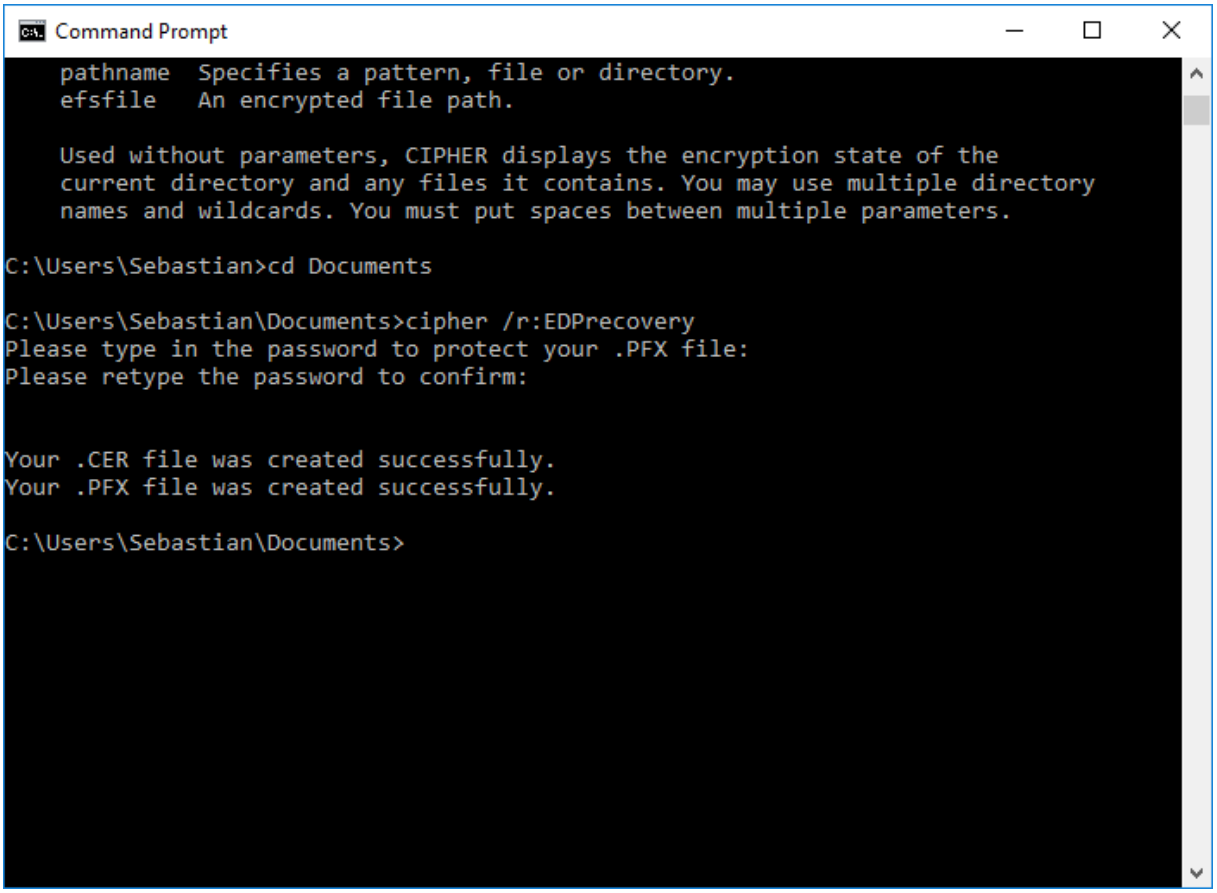


13. For "Corporate identity enter: corp.w10ts.info.

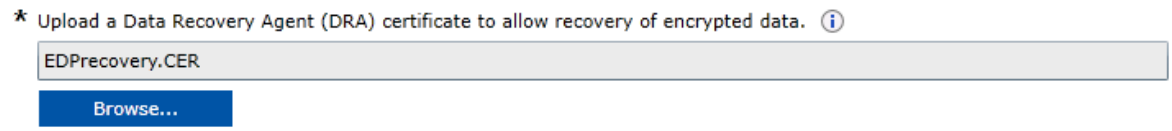
14. For network boundary click add and enter the following information.



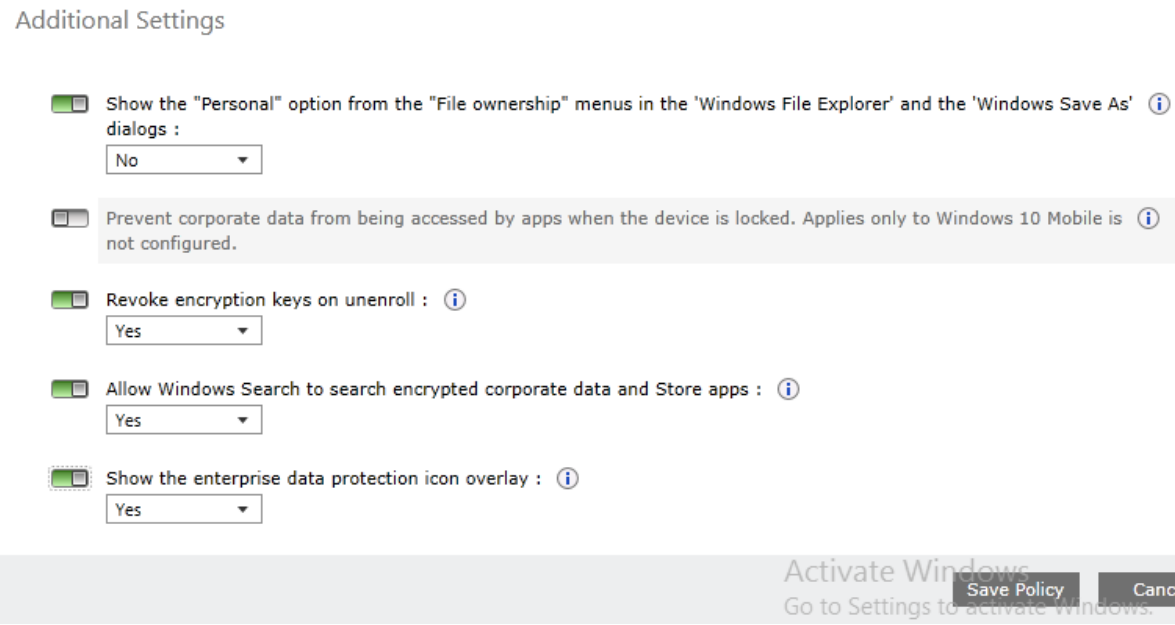
15. To create a Data Recovery Certificate open a command prompt and type: cipher /r:EDPrecovery and enter an Password when prompted.



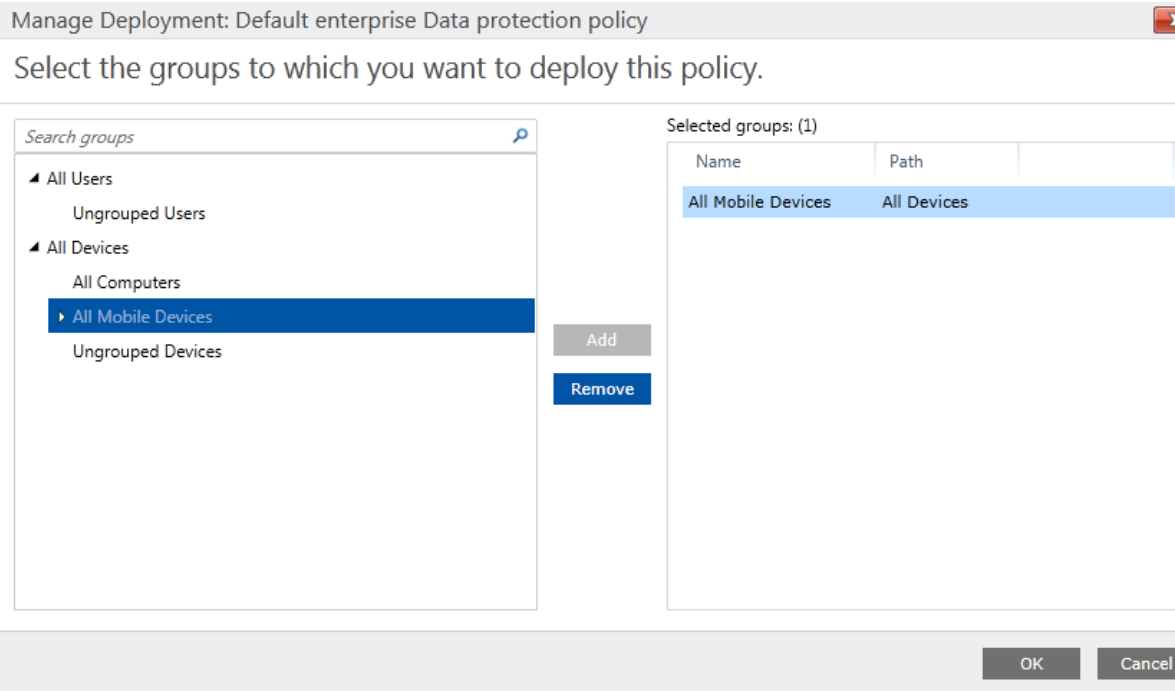
16. Within the “Upload a Data Recovery Agent certificate…” click browse and upload the just created certificate.



17. Configure the “Additional Settings” like this and click on “Save Policy”:

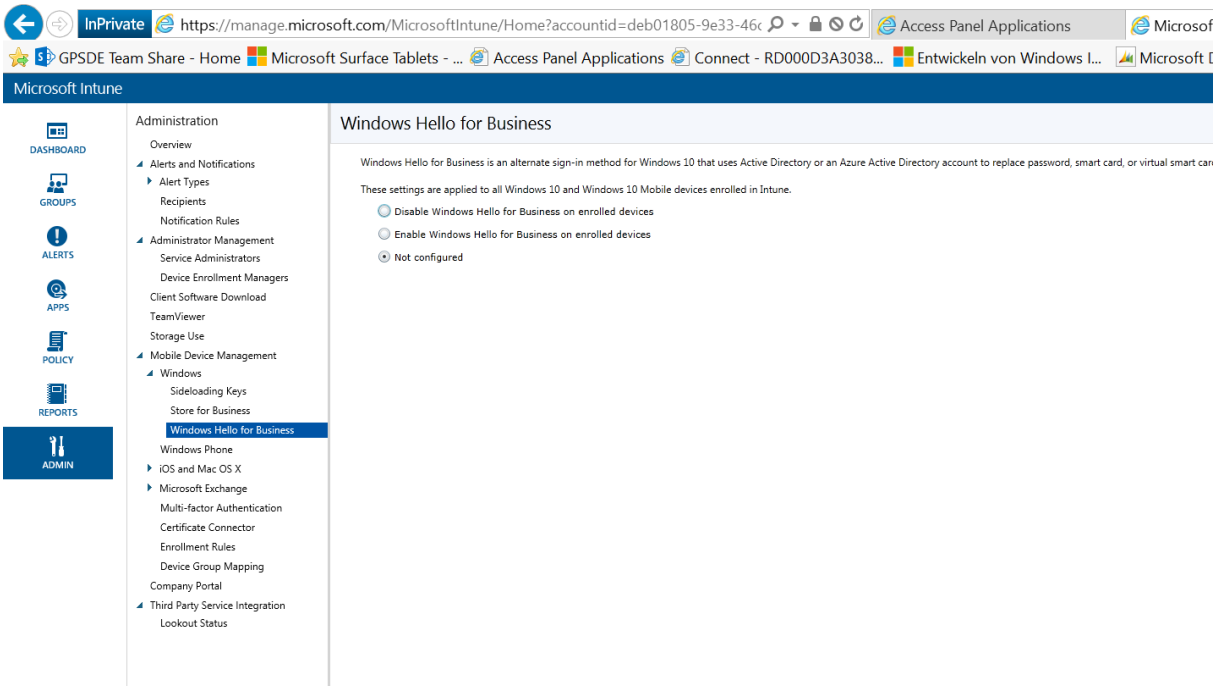


18. When you are asked if you want to deploy the Policy, click “Yes”.
19. Deploy the policy to the “All Mobile Devices” group and click “OK”:

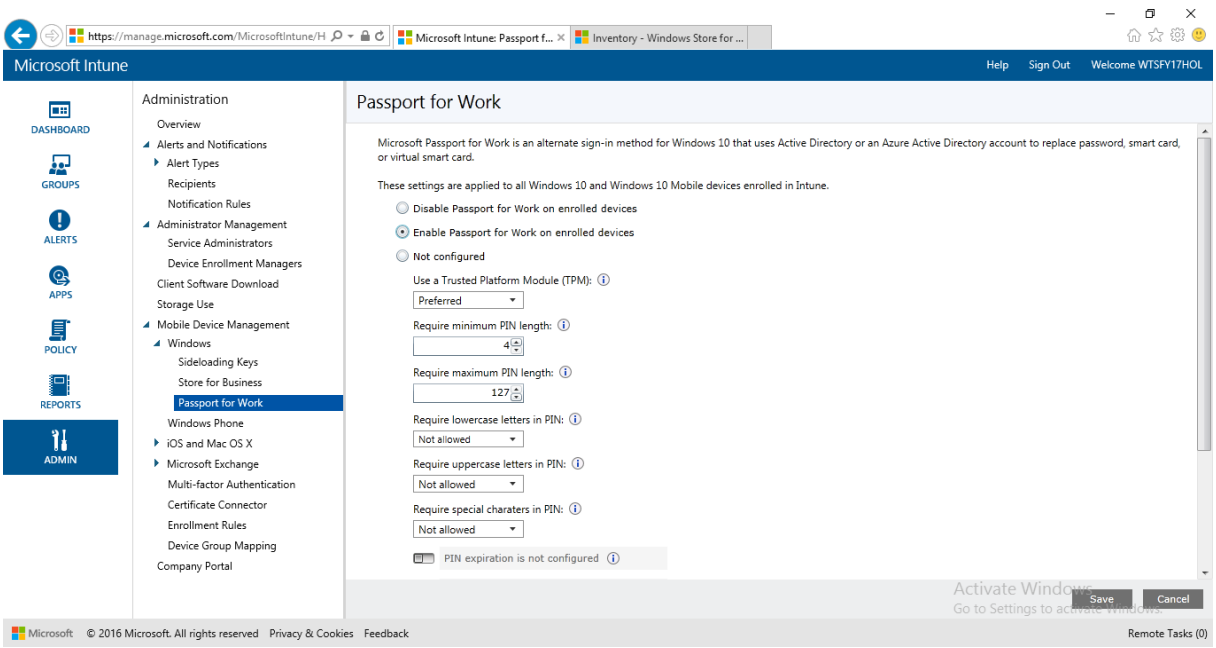


Enable Hello for Business

1. On WTS-12-CLI.
2. Open http://manage.microsoft.com
3. Log on with the Global Administrator created in the Azure Active Directory section.
4. Navigate to “Admin” Workspace and expand “Mobile Device Management” → “Windows” and click on “Hello for business”.



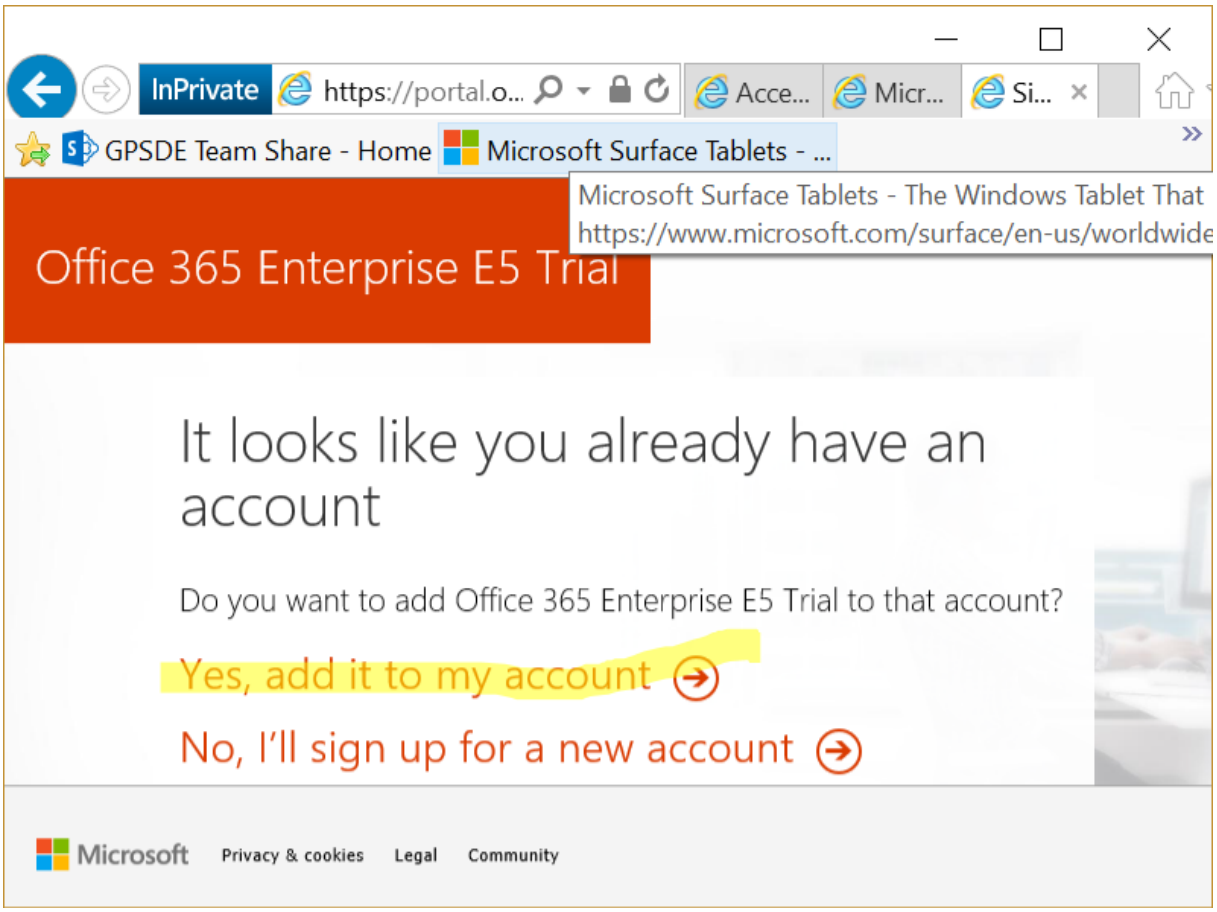
5. Set the Radio Button to “Enable Passport for Work on enrolled devices” leave the default settings and click on “Save”.



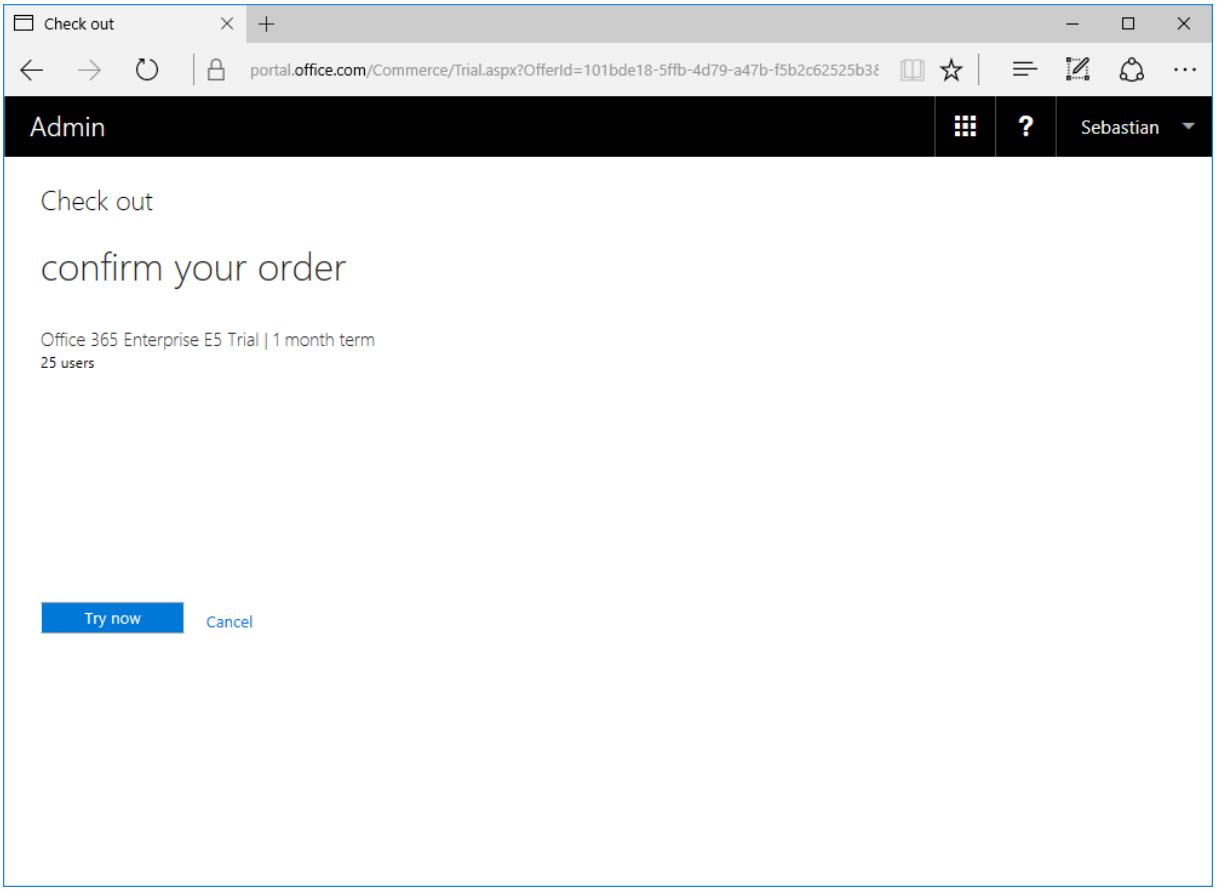
1.3. Conditional access

Attach O365 to Azure AD

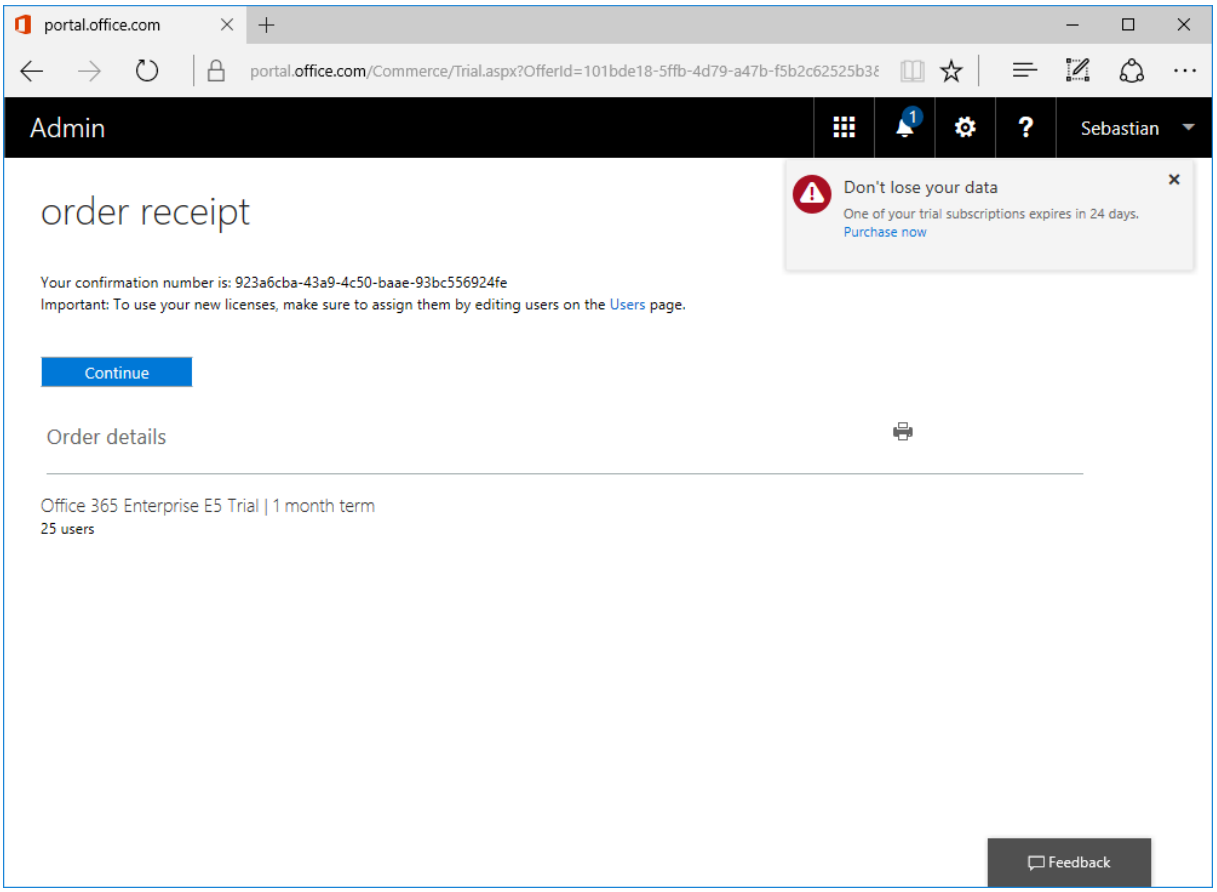
1. On the WTS-12-CLI machine navigate to https://go.microsoft.com/fwlink/p/?LinkID=698279&culture=en-US&country=US (**already as o365 in the Favorites**) and click on "Yes, add it to my account".



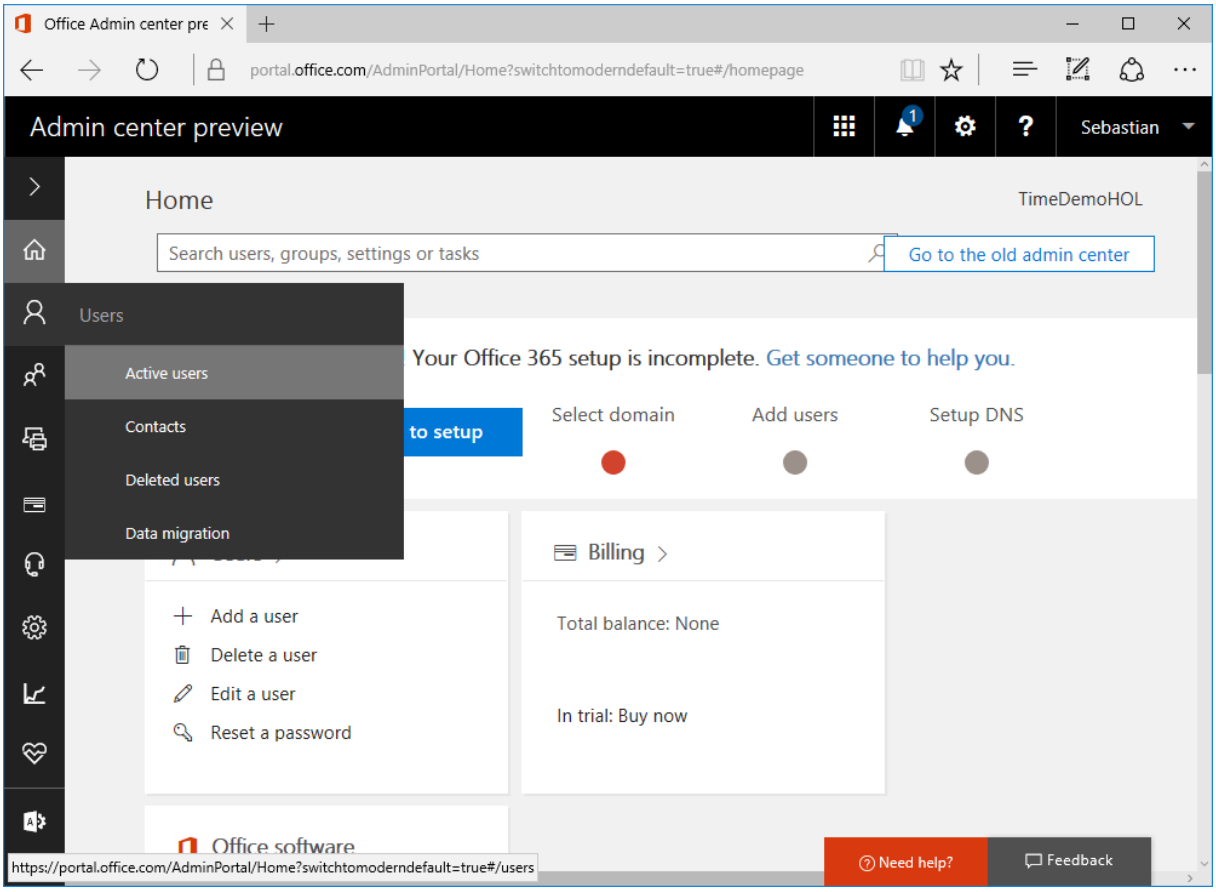
2. Click on “Try now”.



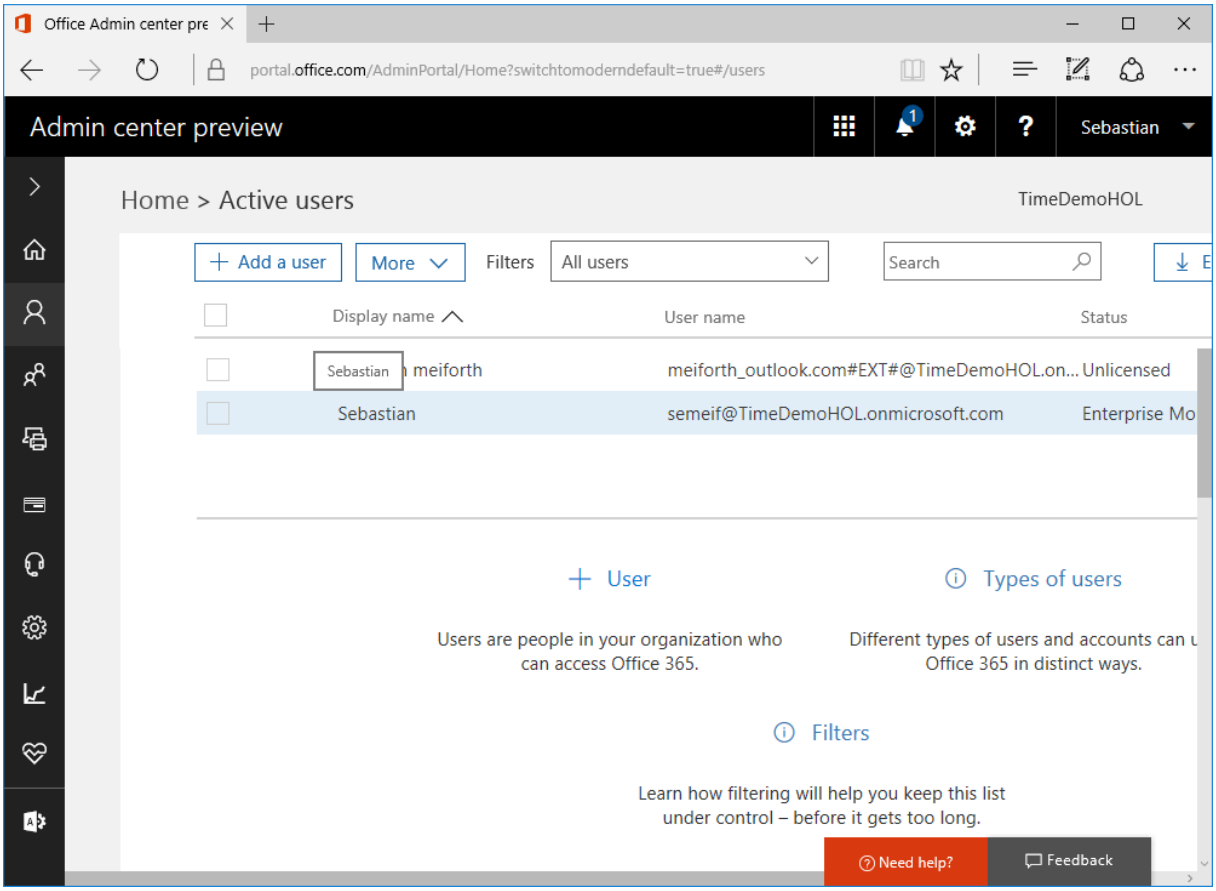
3. Click on “Continue”.



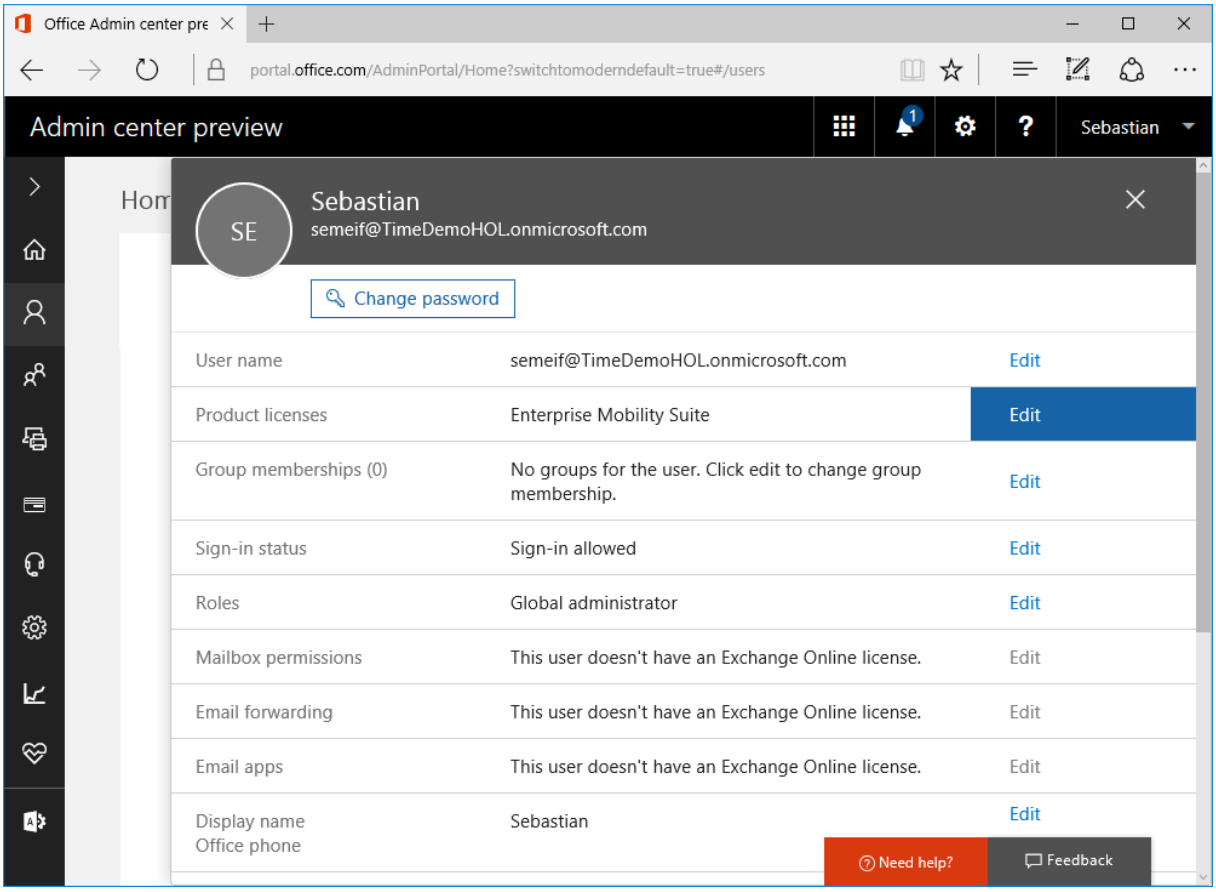
4. In the O365 Admin Center Preview navigate to “Users” → “Activce Users”.



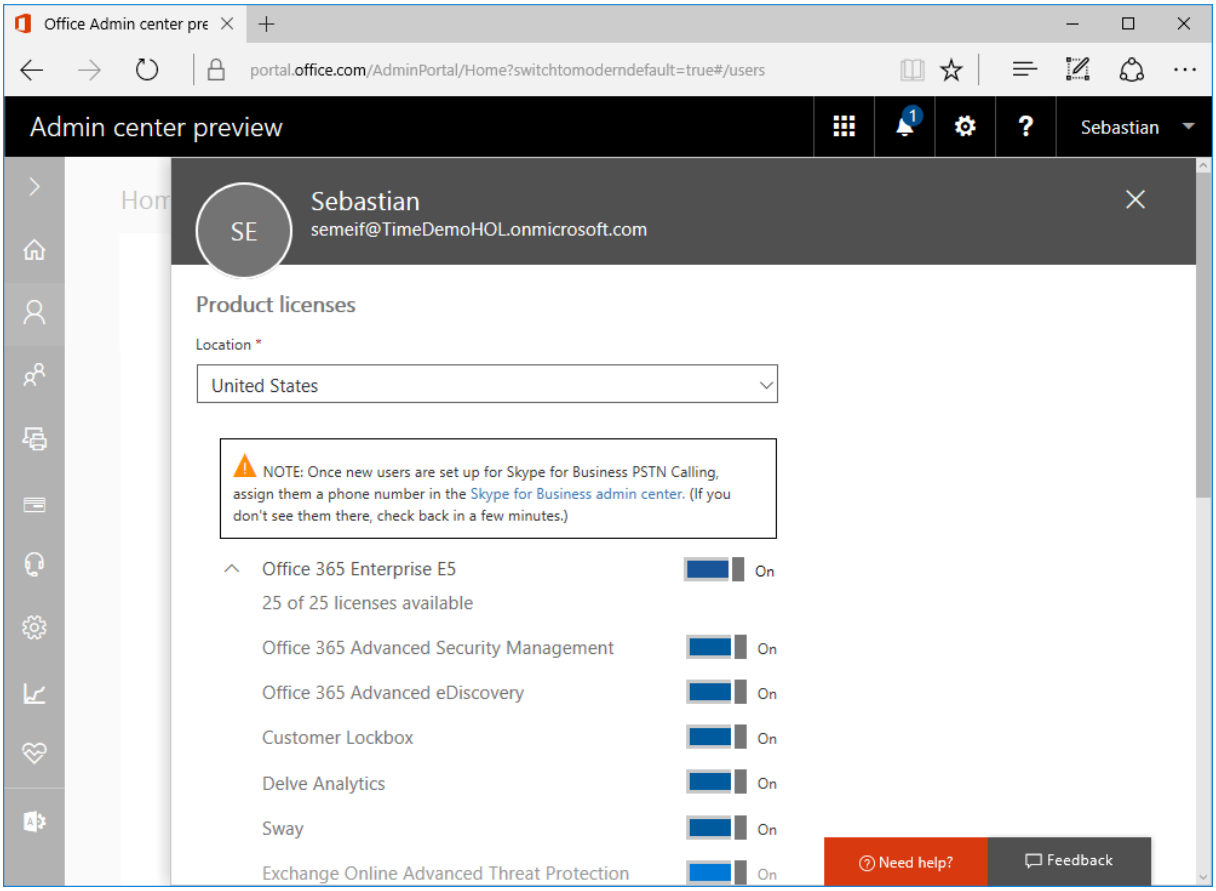
5. Click on the global administrator from your Auzure AD.



6. In the “Product licenses” section click on “Edit”.

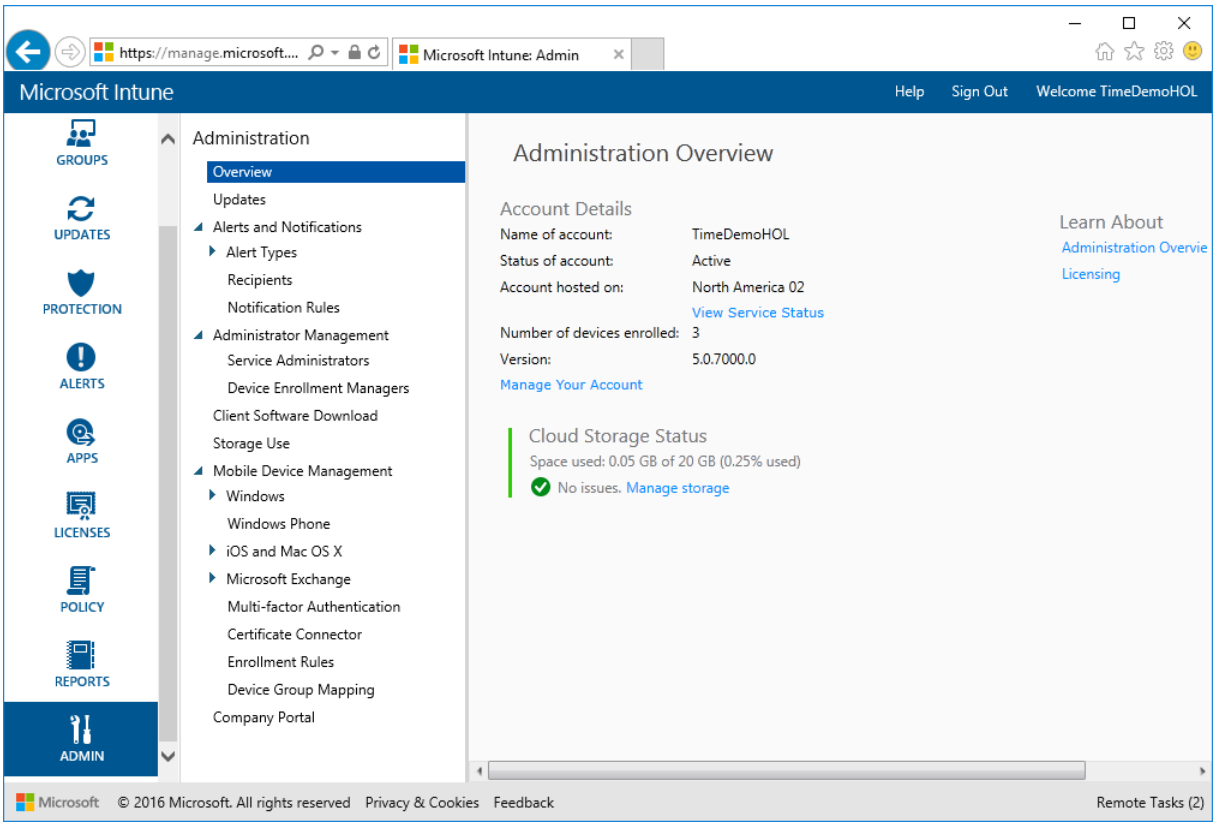


7. On the “Product Licenses” page set the location and activate “Office 365 Enterprise E5” and click on “Save”.

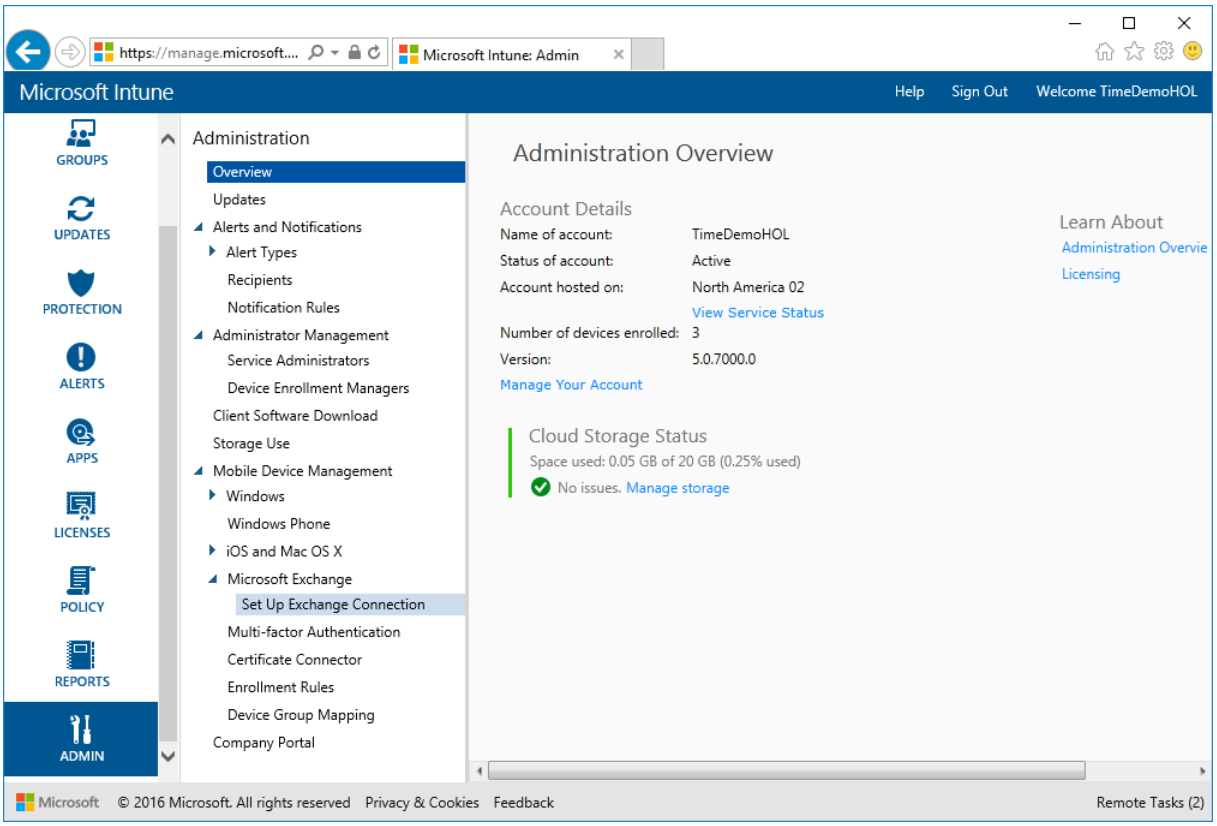


Set up “Service to Service” connector.

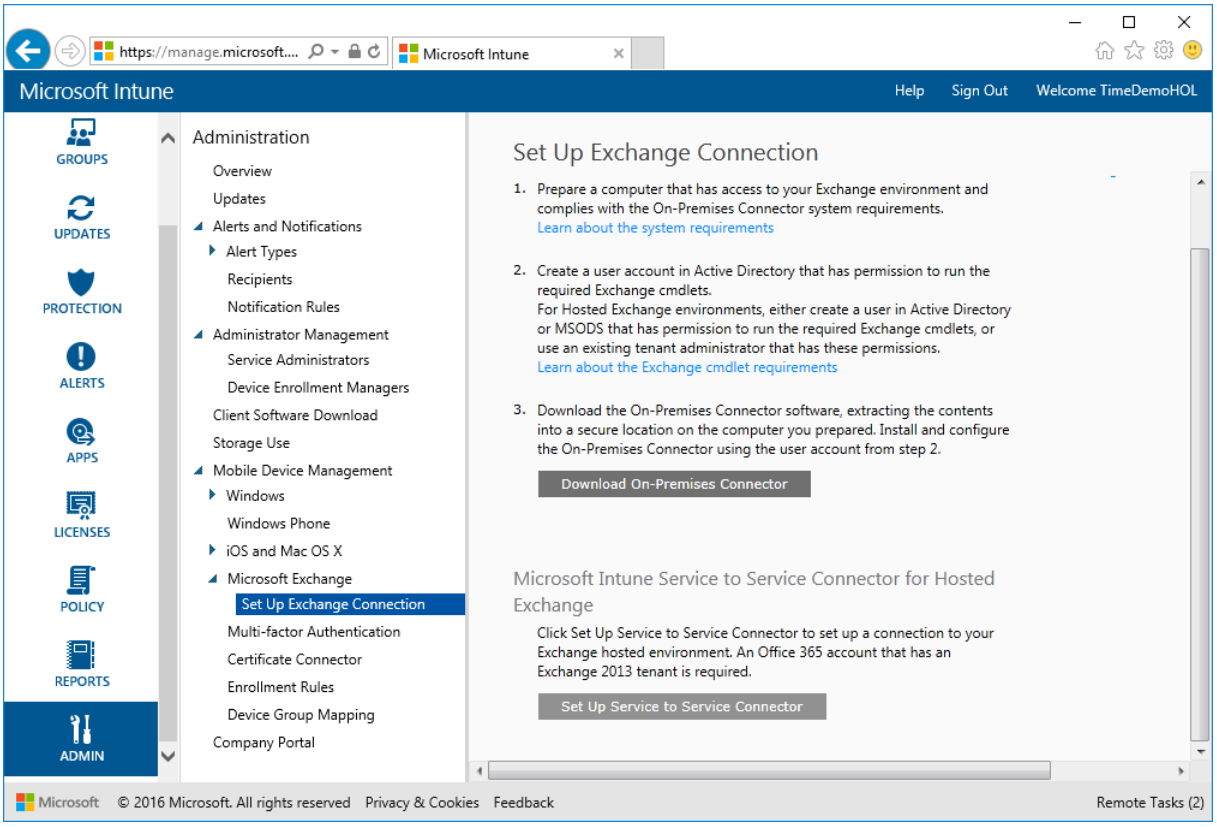
1. On the WTS-12-CLI machine navigate to http://manage.microsoft.com in Internet Explorer and open the “ADMIN” workspace.



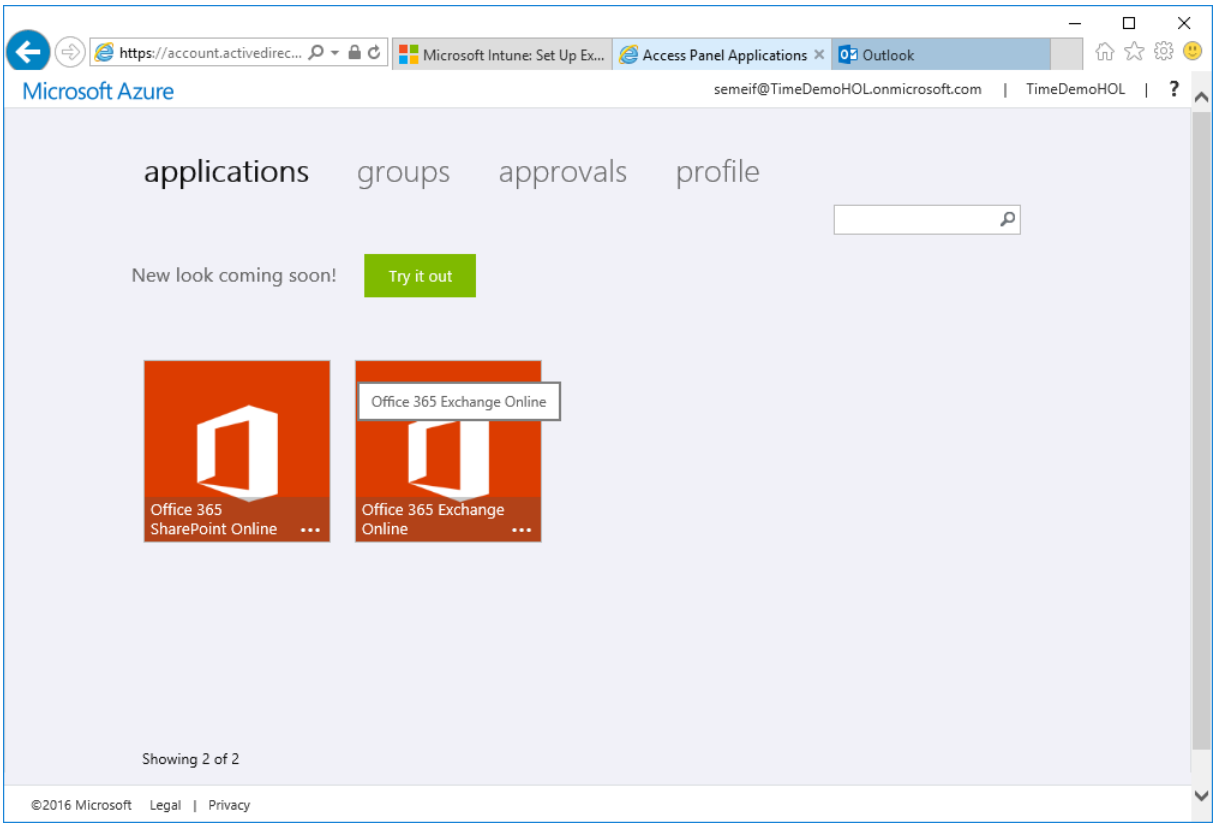
2. Expand “Microsoft Exchange” and click on Set up Exchange connection”.



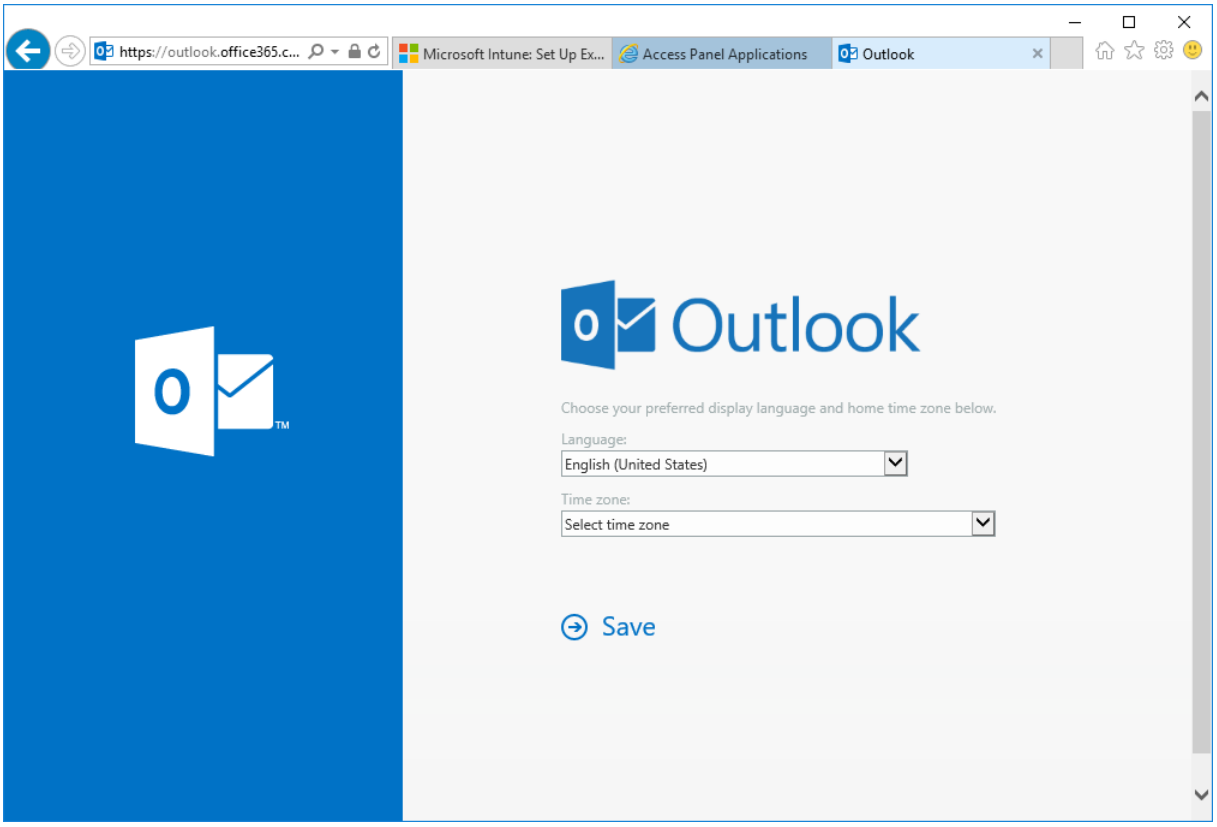
3. Click on “Set Up Service to Service Connector”.



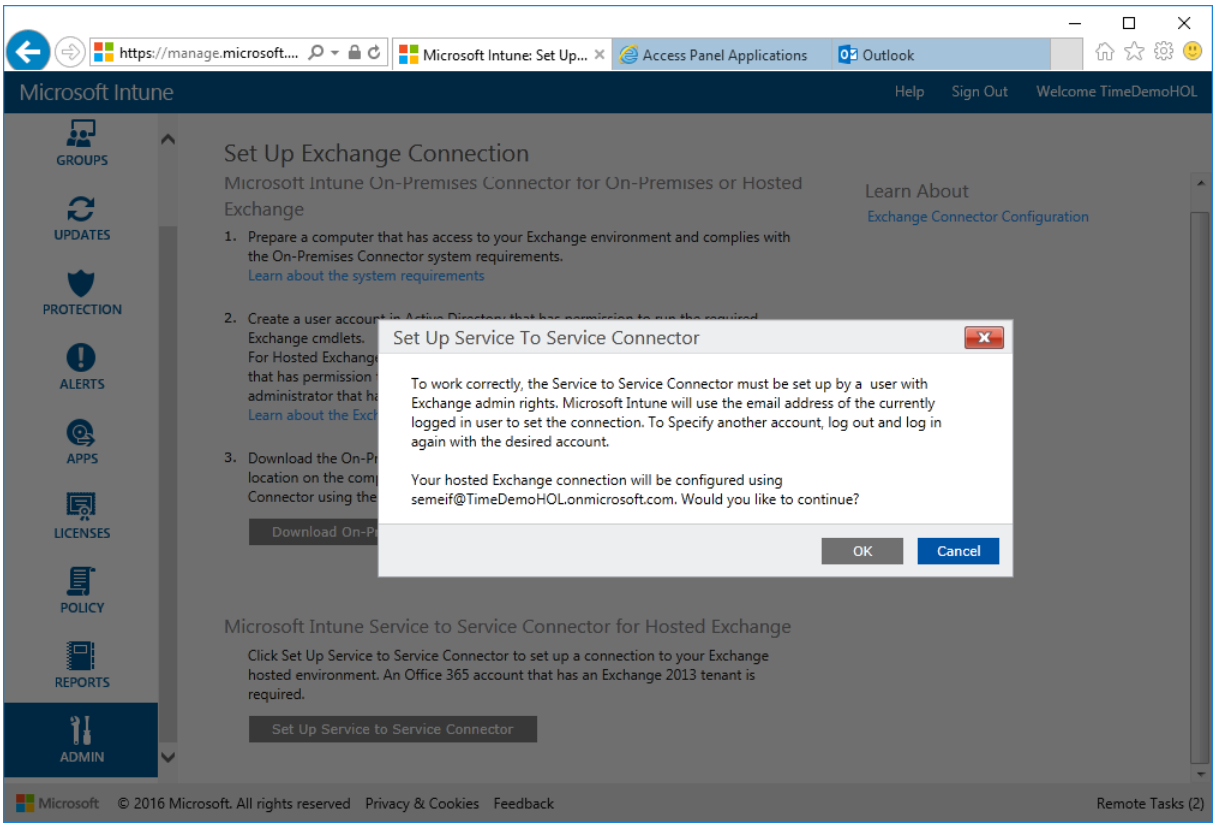
4. If you get a error message that the user has no email account, log open http://myapps.microsoft.com and click on “Office 365 Exchange online”.



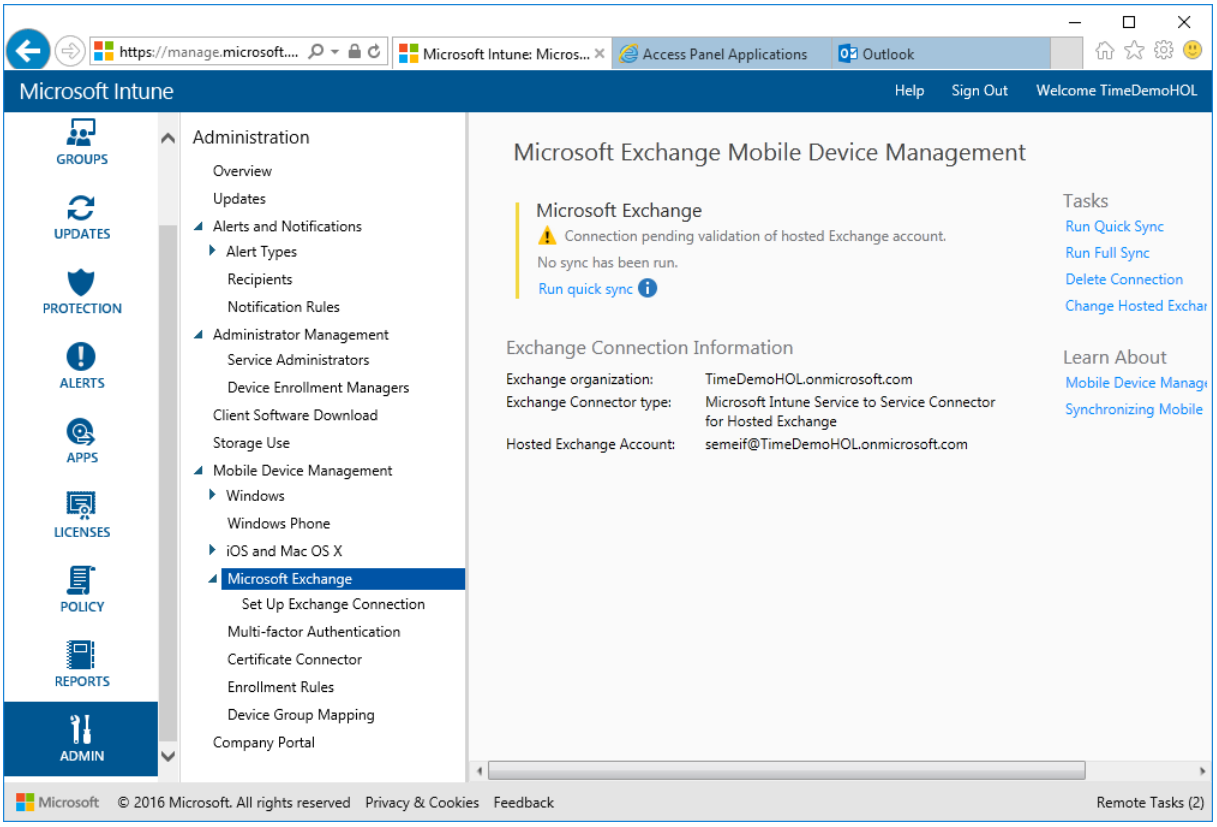
5. Fill out the form on the next page and click “Save”.



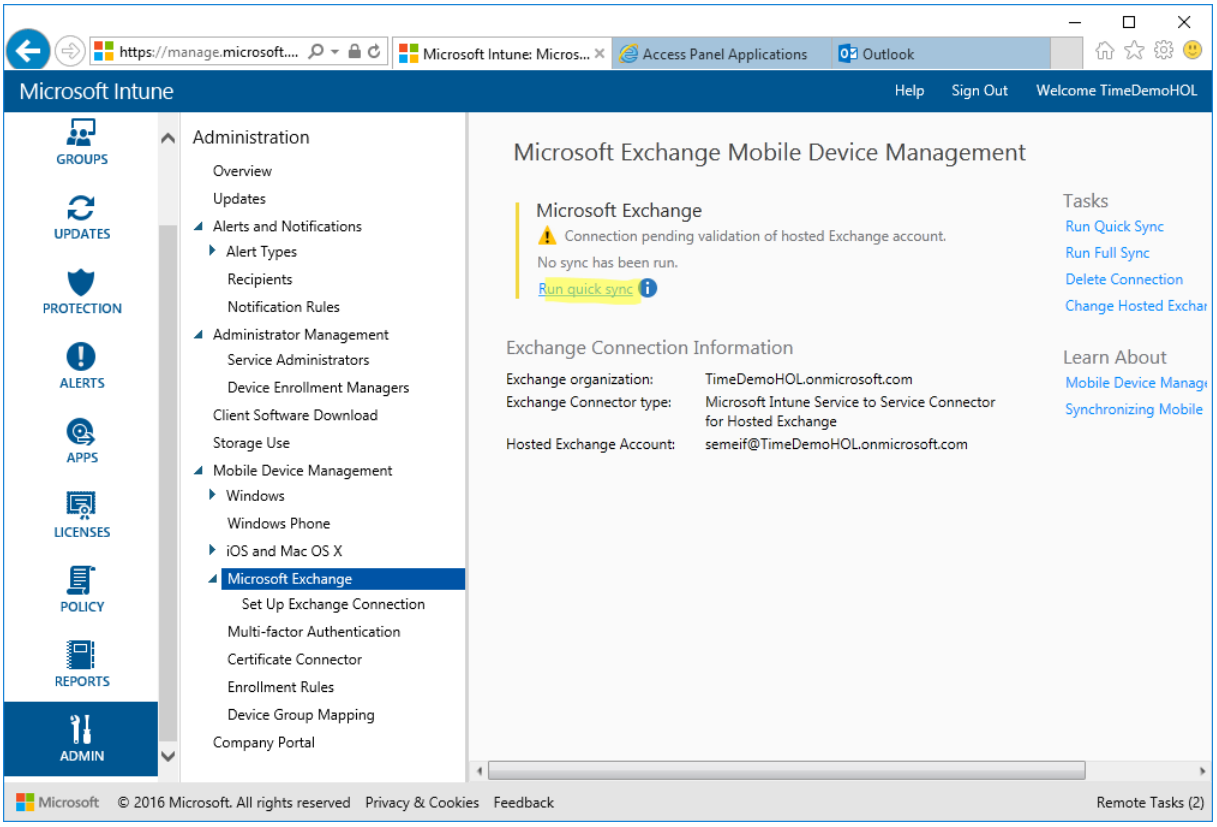
6. Go back to Microsoft intune, sign out and back in, then try it again.
7. On the “Set Up Service To Service Connector” pop-up click on “OK”.



8. Now the connector gets validated against Exchange Online.

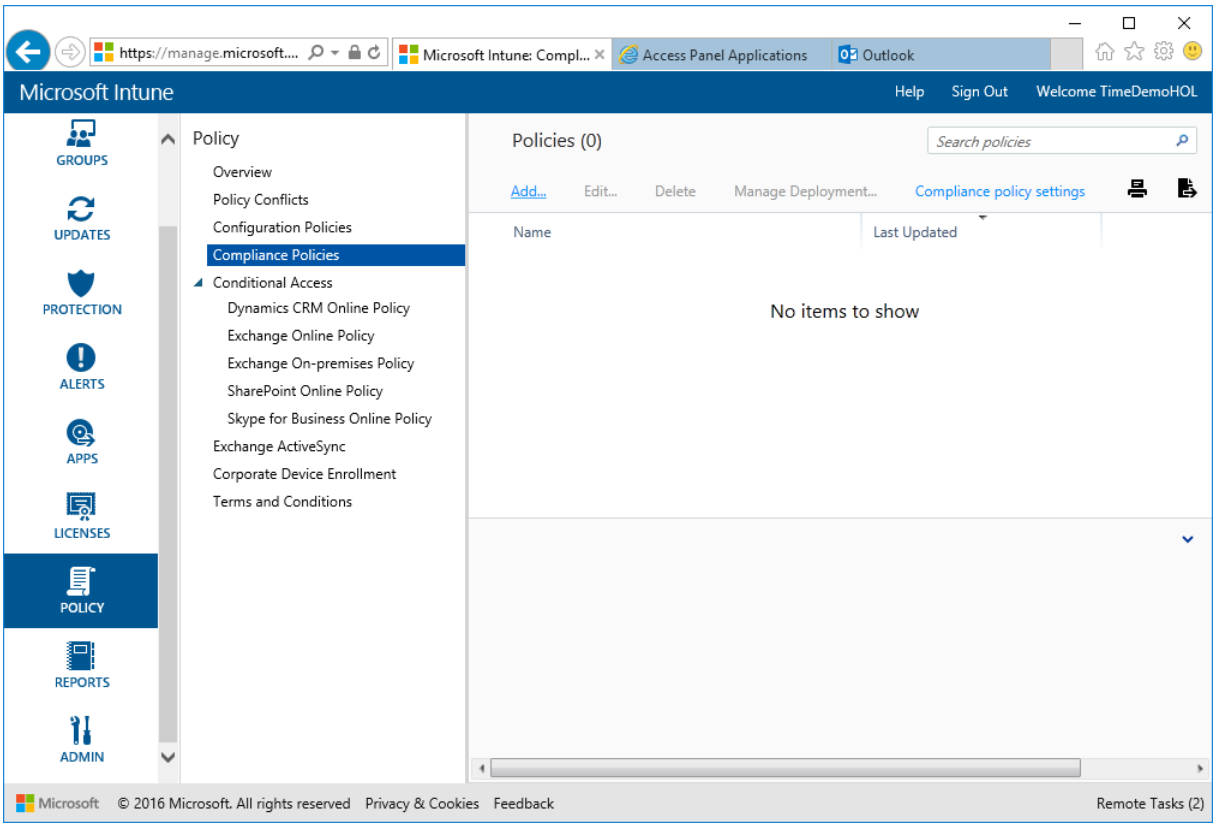


9. Click on “Run quick sync”.

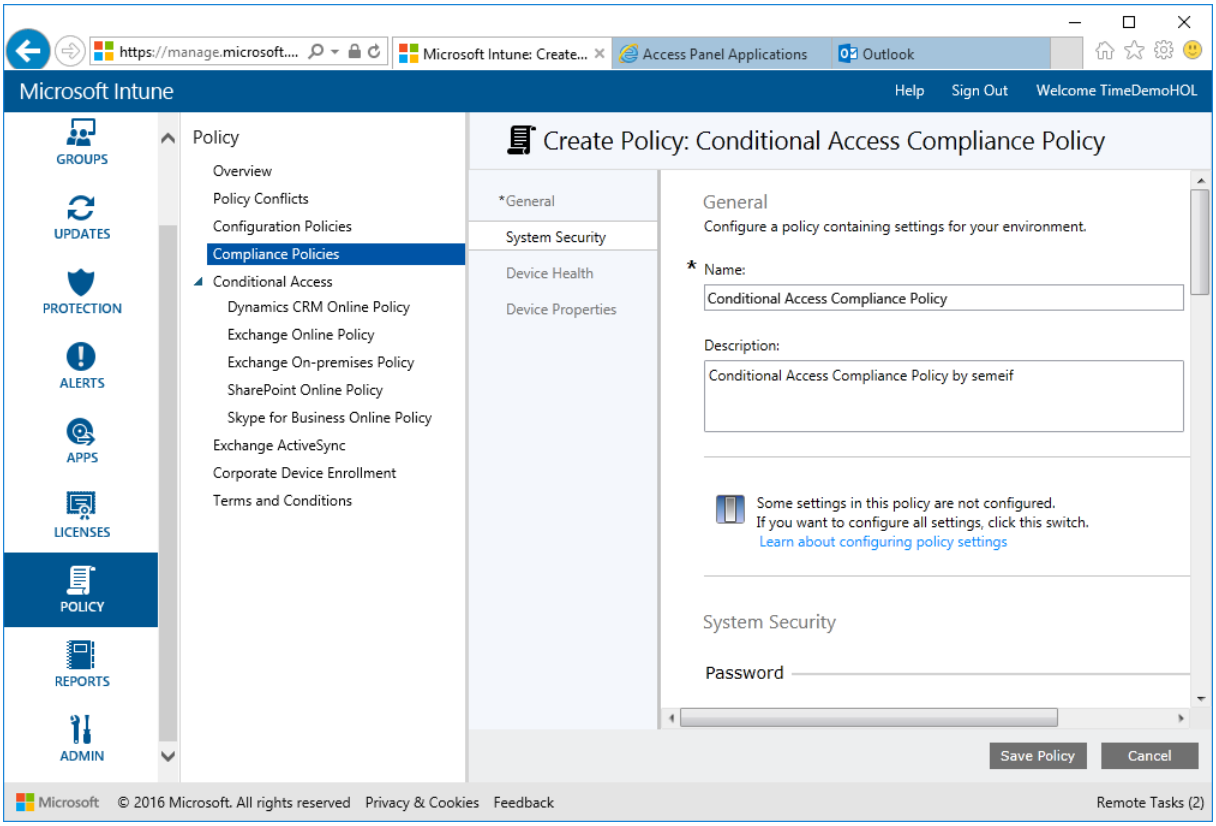


Create a device compliance policy

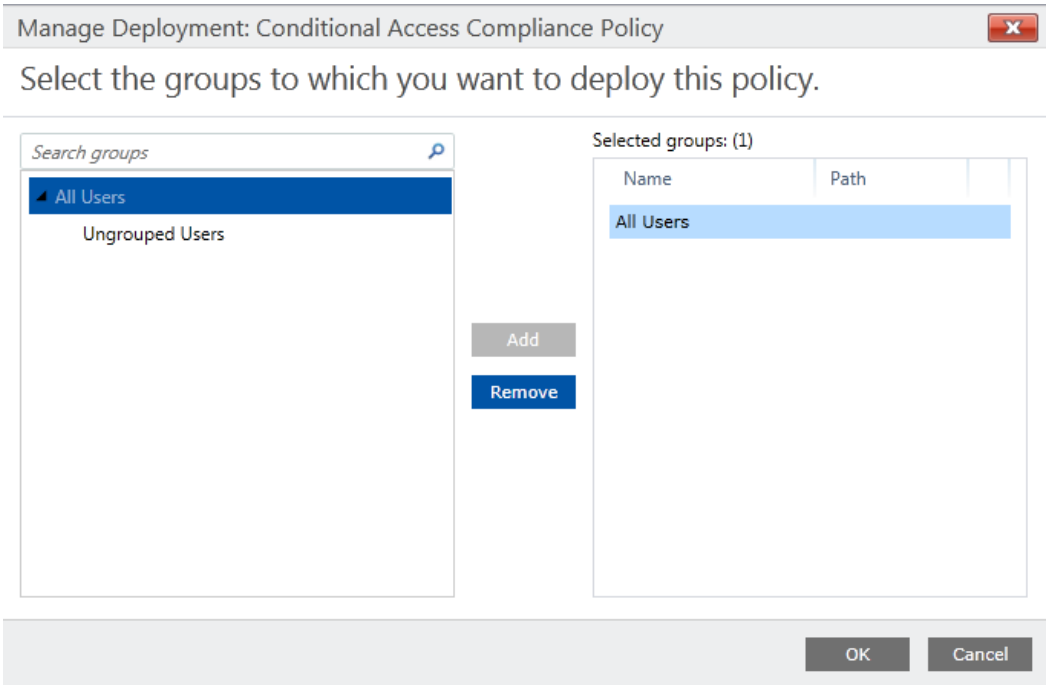
1. Go to the “Policy” workspace → “Compliance Policies” and click on “Add…”.



2. Enter a name for the policy and enable some password settings (Numeric 4-digit PIN) and click “Save Policy”, then you can deploy the policy to all users right away.

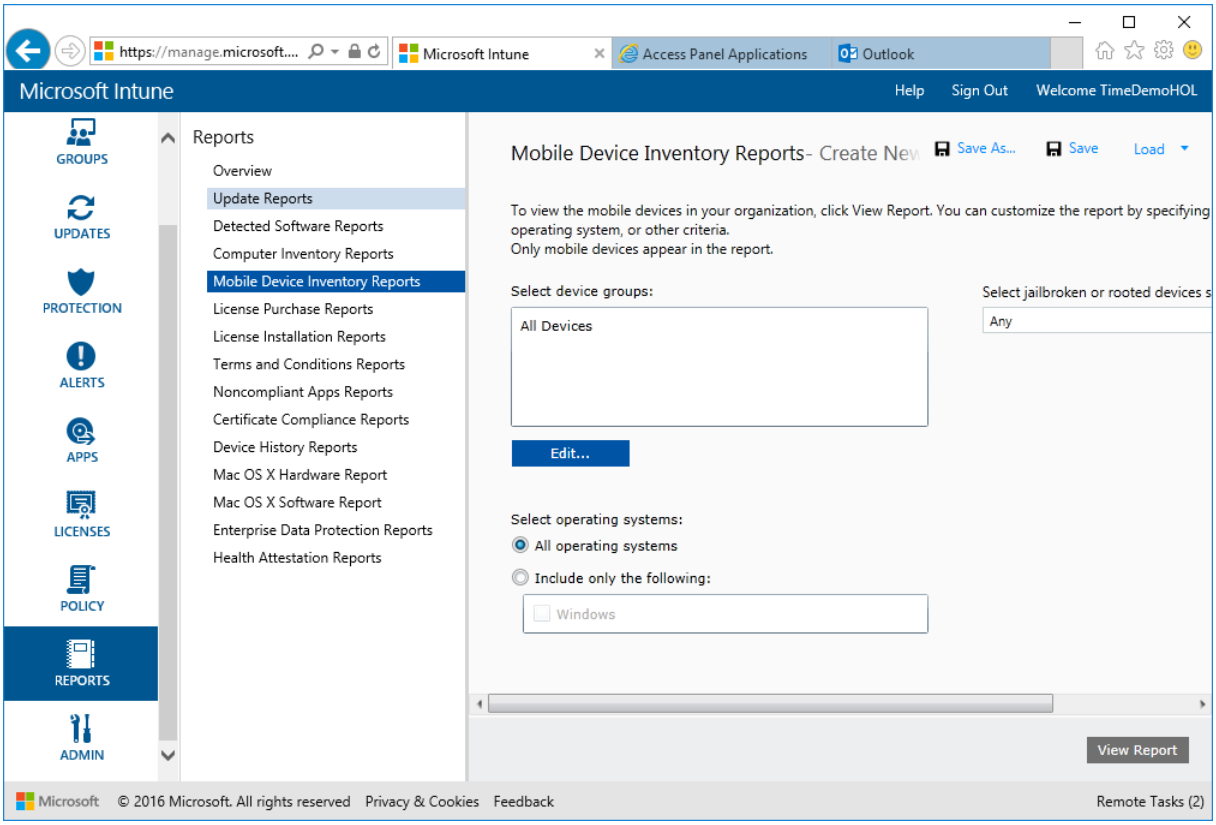


3. Deploy to all users and click “OK.

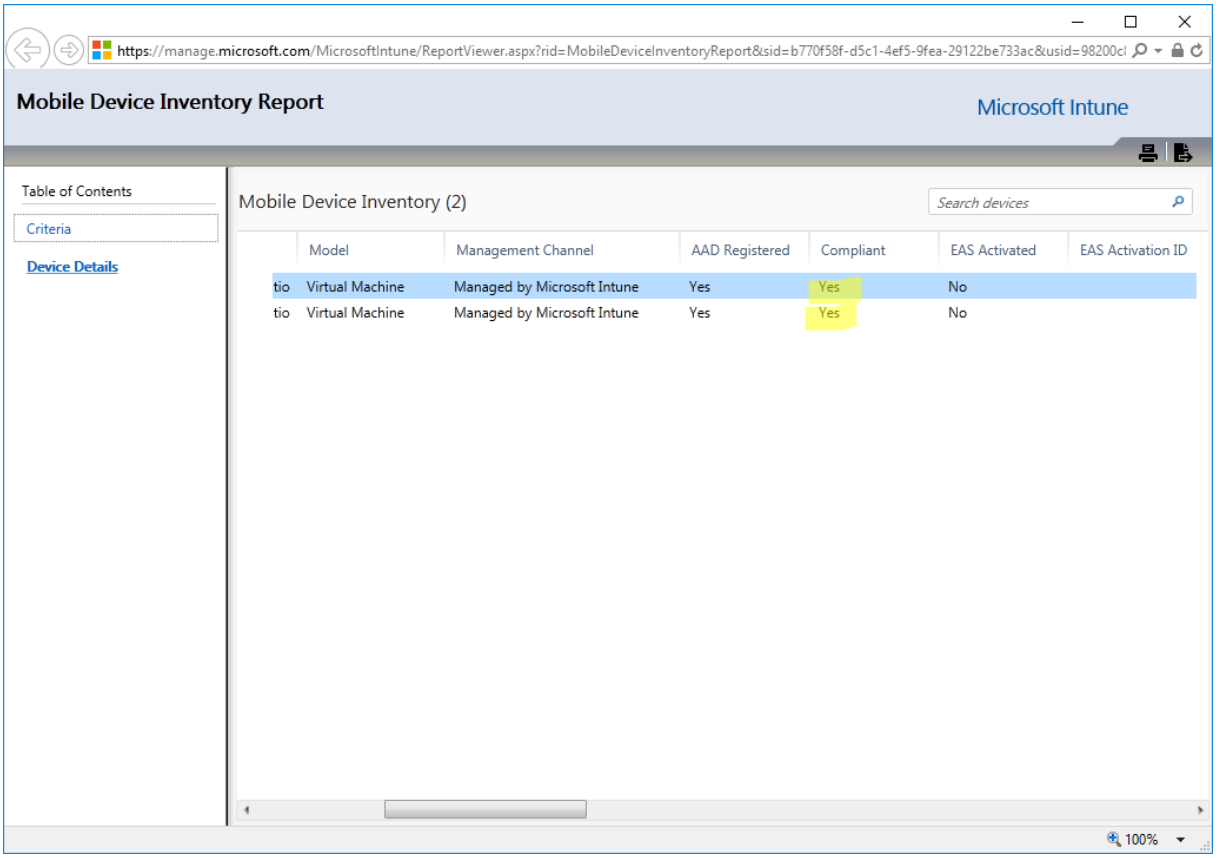


Evaluate the effect of the conditional access policy

1. Navigate to the “REPORTS” workspace, select the “Mobile Device Inventory Reports” and click on “View Report”.

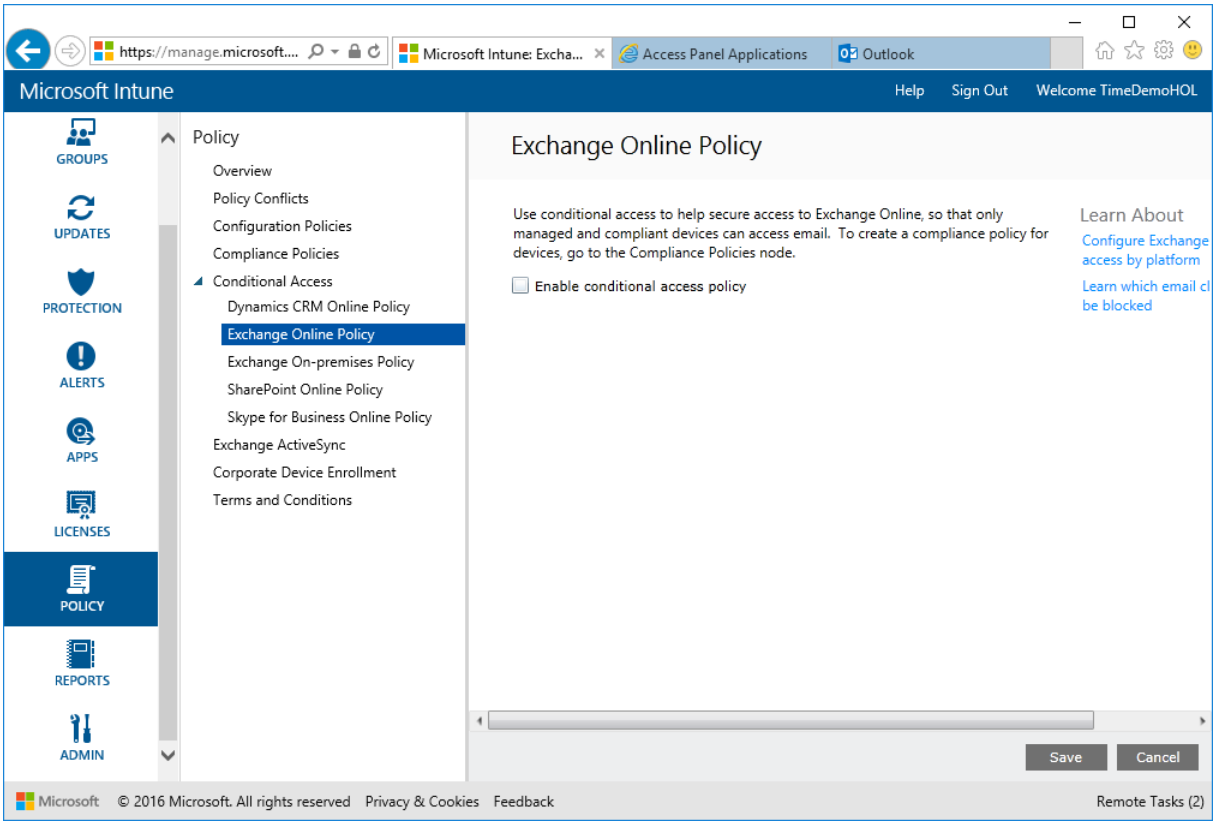


2. Review the report to verify if the devices are compliant and close the report.

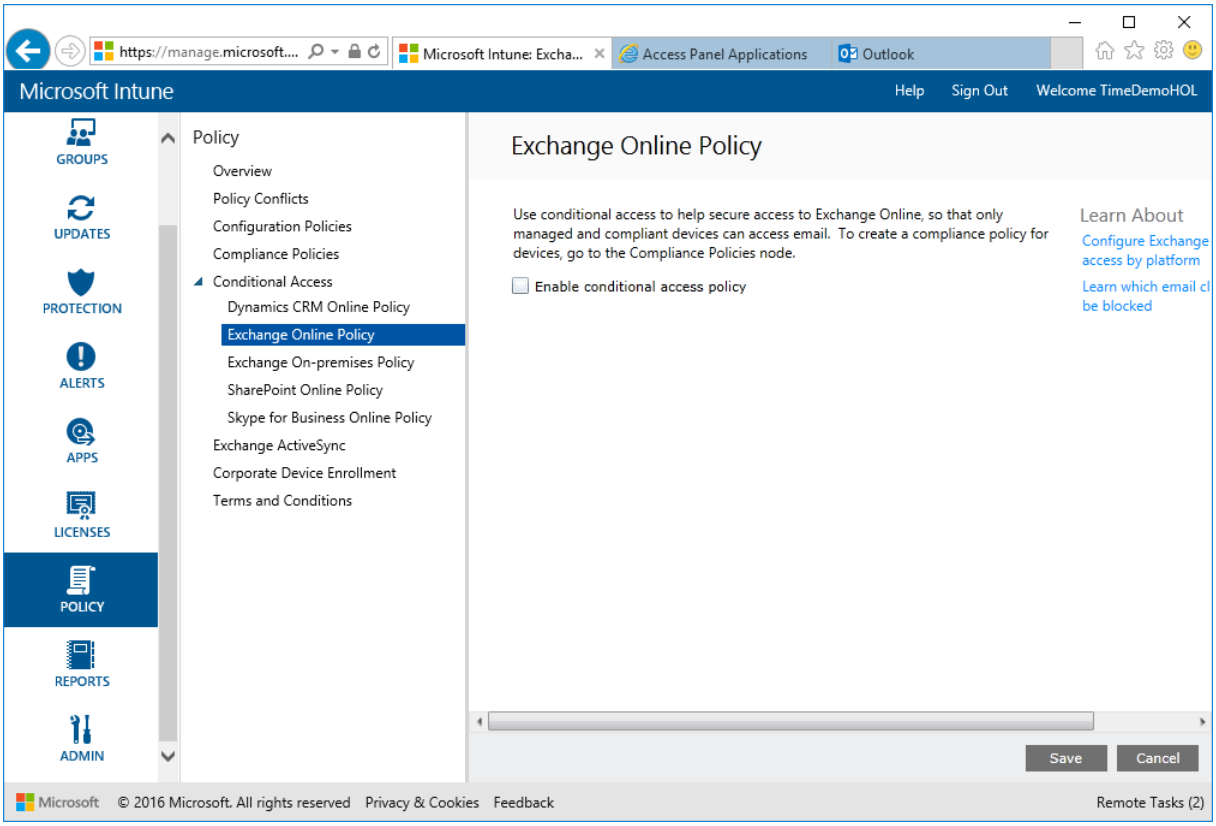


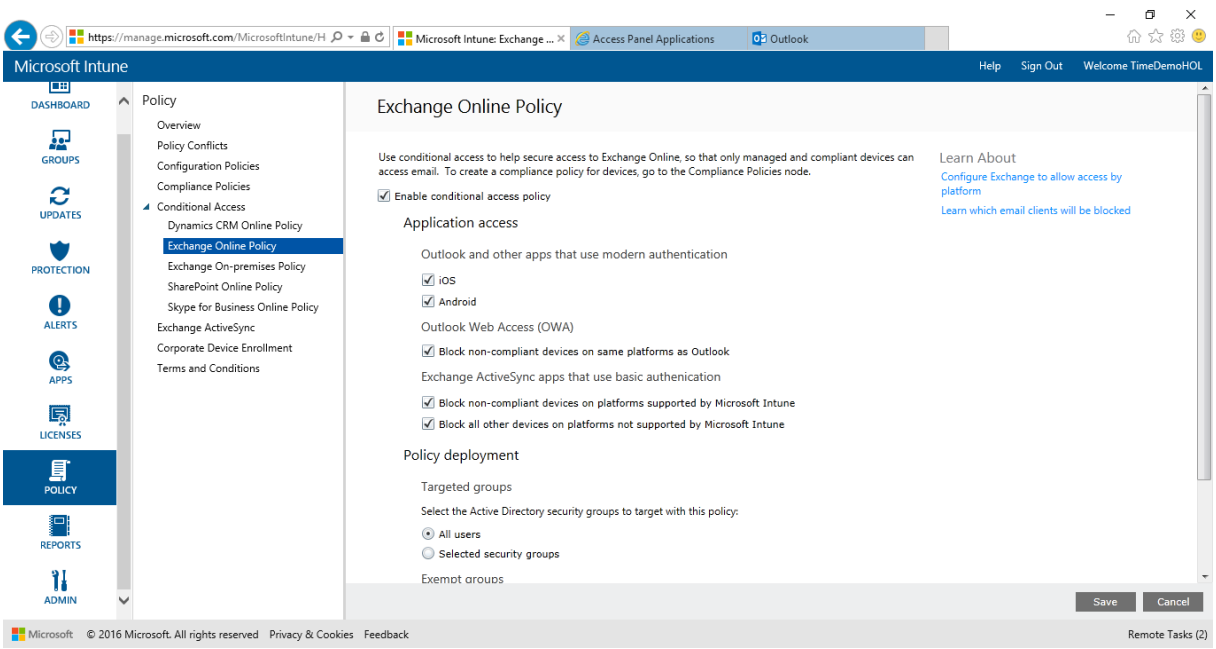
Set Conditional Access Policy

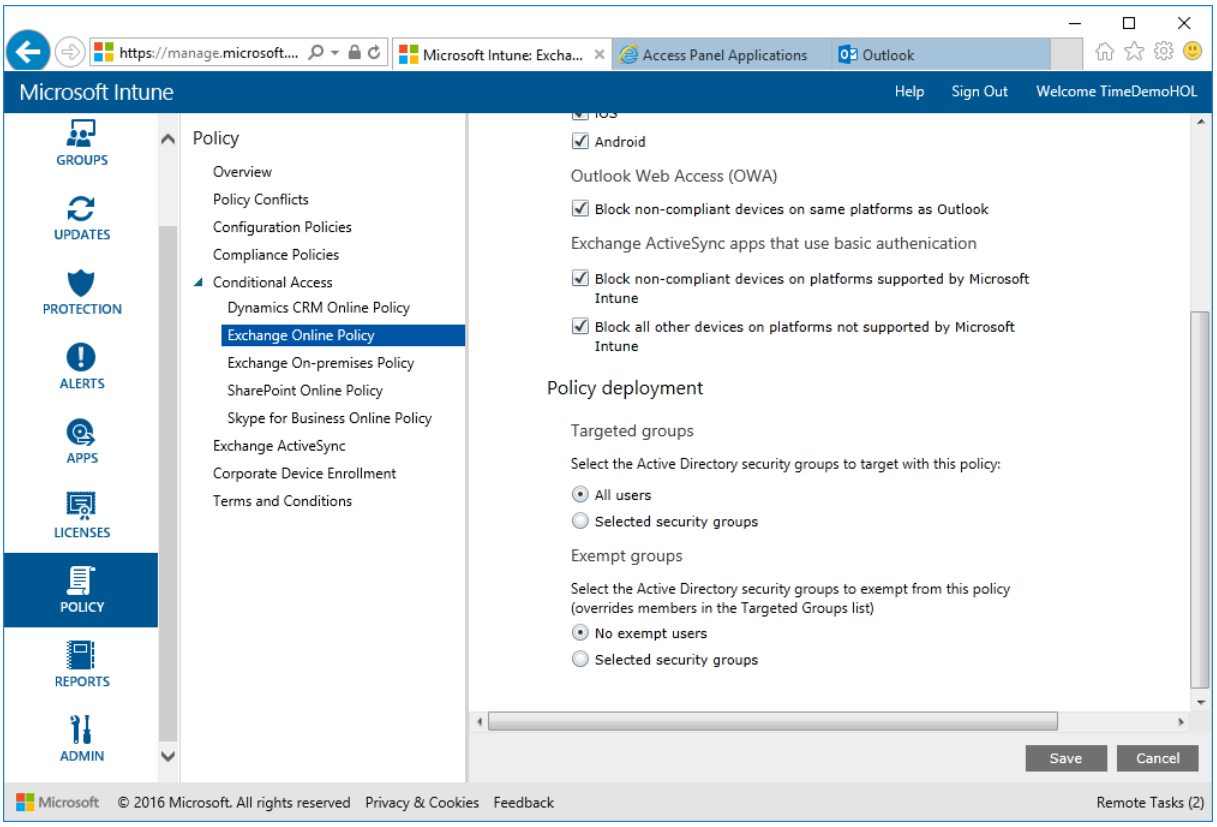
3. Go to the "Policy" workspace → expand "Conditional Access" → select "Exchange Online Policy".



4. Activate “Enable conditional access policy”, configure as the following and click “Save".

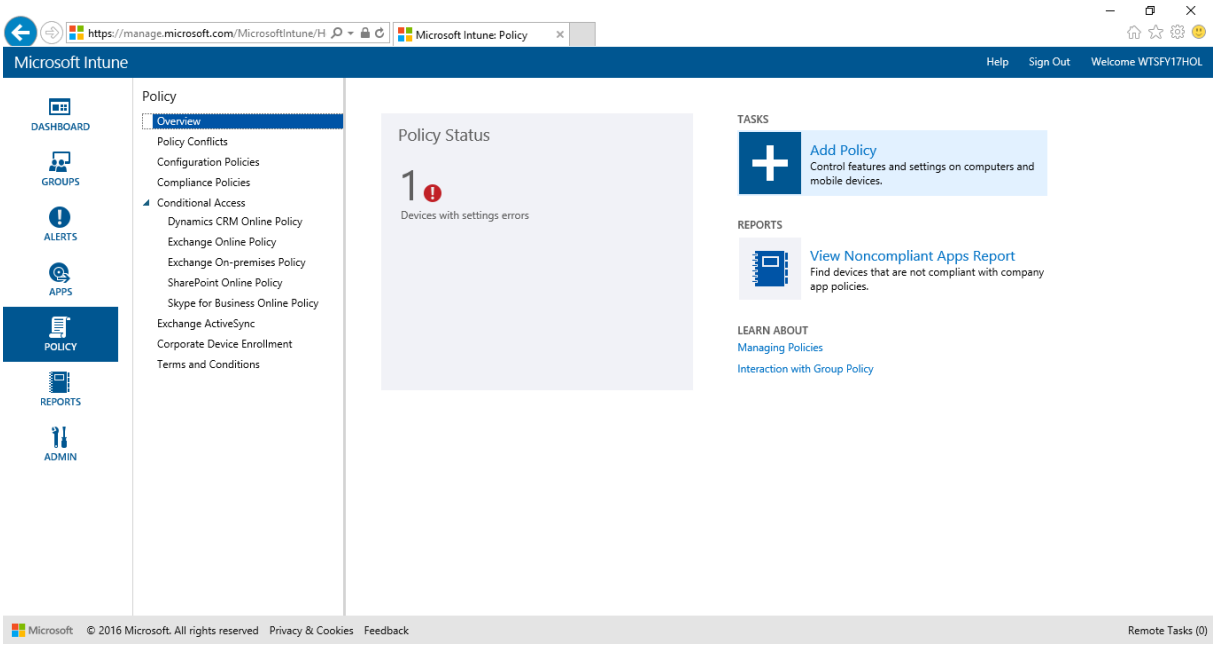




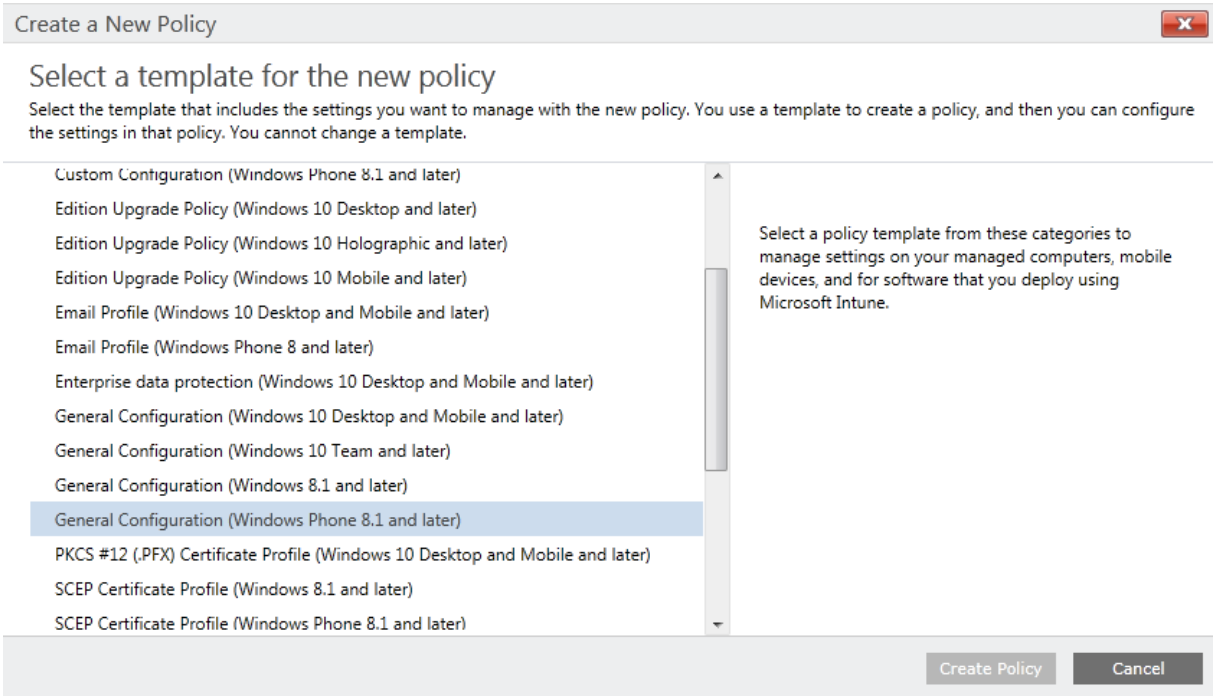
5. 
https://manage.microsoft....
Microsoft Intune: Excha...
Access Panel Applications
Outlook
Microsoft Intune
Help
Sign Out
Welcome TimeDemoHOL
GROUPS
UPDATES
PROTECTION
ALERTS
APPS
LICENSES
POLICY
REPORTS
ADMIN
Policy
Overview
Policy Conflicts
Configuration Policies
Compliance Policies
Conditional Access
Dynamics CRM Online Policy
Exchange Online Policy
Exchange On-premises Policy
SharePoint Online Policy
Skype for Business Online Policy
Exchange ActiveSync
Corporate Device Enrollment
Terms and Conditions
Android
Outlook Web Access (OWA)
Block non-compliant devices on same platforms as Outlook
Exchange ActiveSync apps that use basic authenication
Block non-compliant devices on platforms supported by Microsoft Intune
Block all other devices on platforms not supported by Microsoft Intune
Policy deployment
Targeted groups
Select the Active Directory security groups to target with this policy:
All users
Selected security groups
Exempt groups
Select the Active Directory security groups to exempt from this policy (overrides members in the Targeted Groups list)
No exempt users
Selected security groups
Save
Cancel
Microsoft
© 2016 Microsoft. All rights reserved
Privacy & Cookies
Feedback
Remote Tasks (2)

App White-/Blacklisting (Optional)

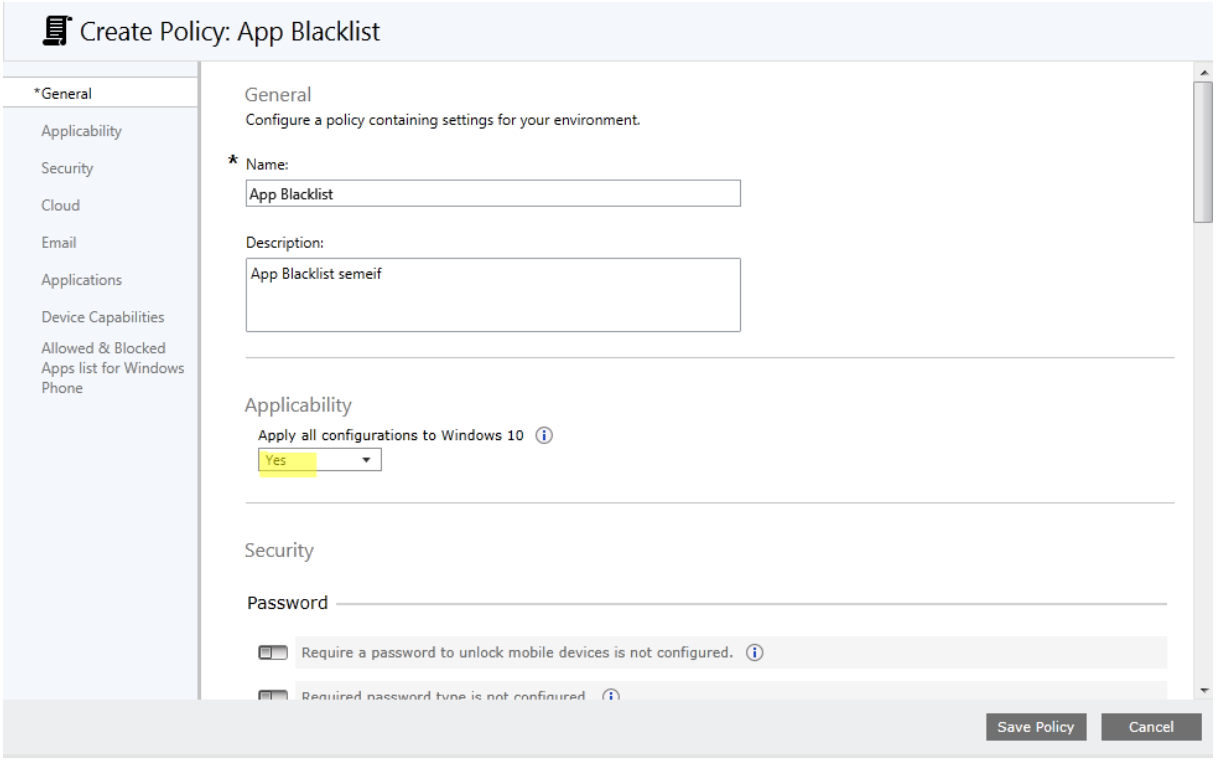
1. On WTS-12-CLI.
2. Open http://manage.microsoft.com
3. Log on with the Global Administrator created in the Azure Active Directory section. Navigate to the "Policy" workspace and click on "Add Policy".



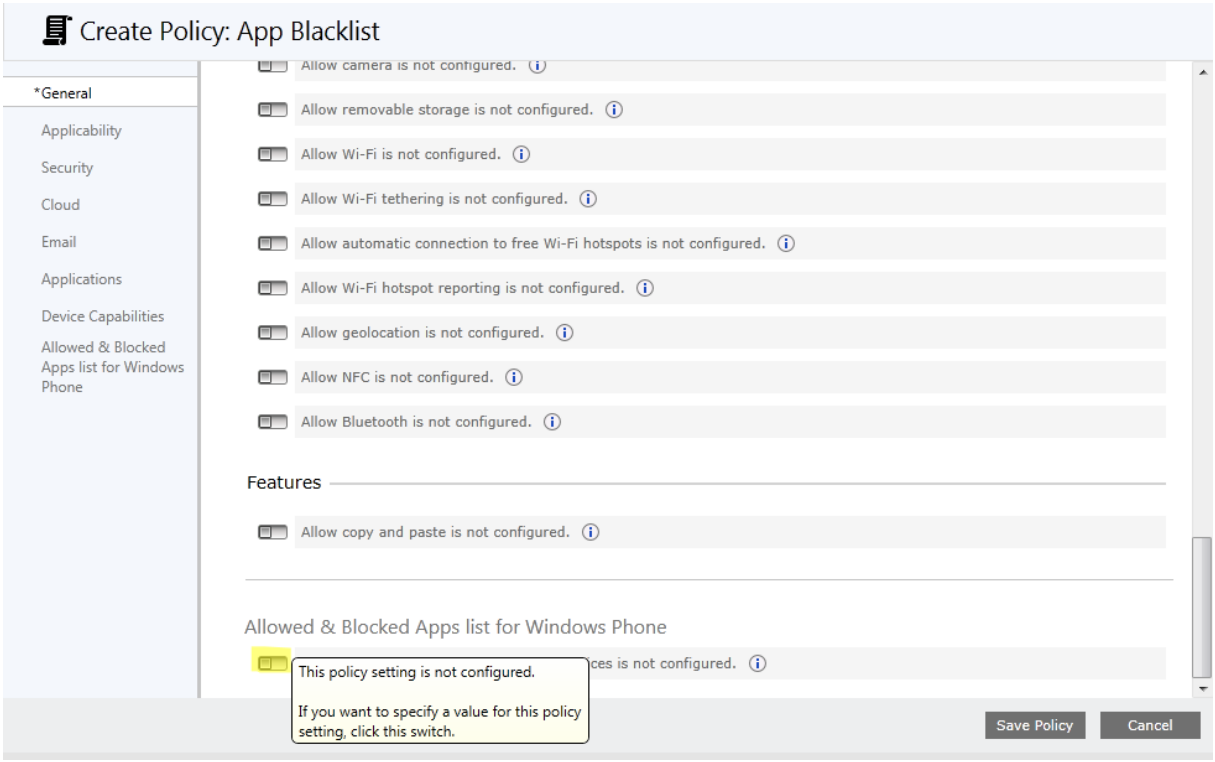
4. Expand Windows and select "General Configuration (Windows Phone 8.1 and later)" and click on "Create Policy".



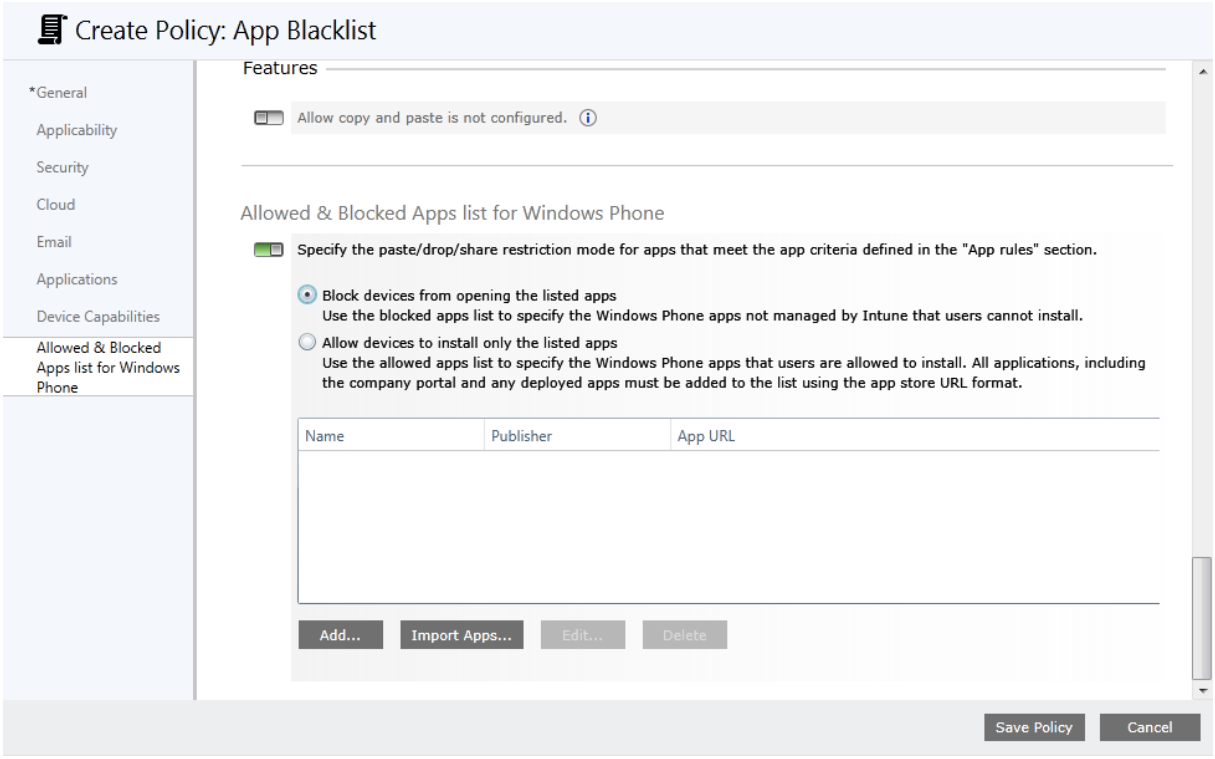
5. Enter a name and discription for the policy and make shure that under “Applicability” “Apply all configurations to windows 10” is set to “Yes”.



6. Scroll down to the bottom of the page and activate the switch “Managed settings for Windows Phone …”.



7. Select “Block devices from opening the listed apps” and click “Add…”.

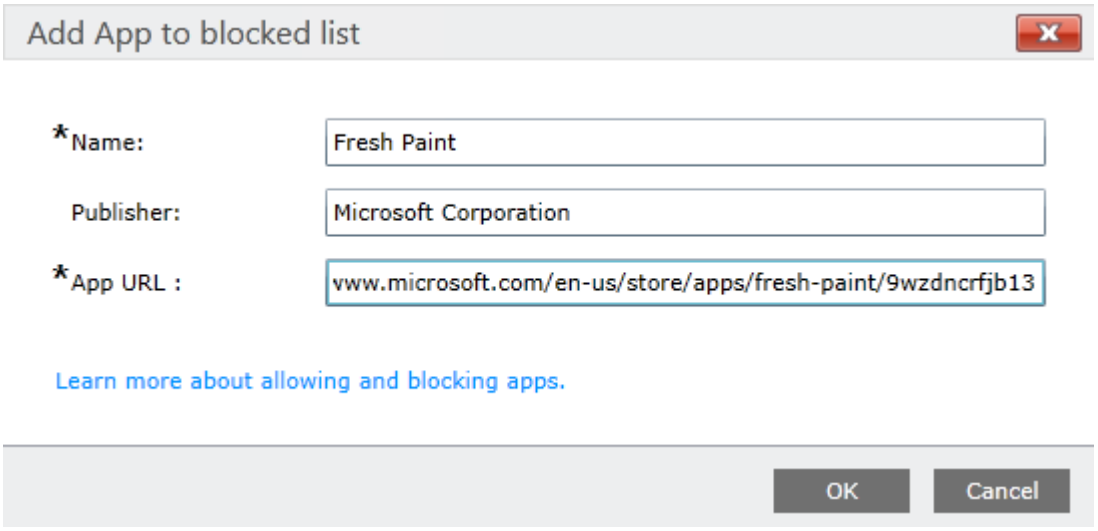


8. Enter the following information and click “OK”:

   Name: Fresh Paint

   Publisher: Microsoft Corporation

   App URL: https://www.microsoft.com/en-us/store/apps/fresh-paint/9wzdncrfjb13



9. Repeat this for the following Apps and click “Save Policy”:

   Name: WhatsApp

   Publisher: WhatsApp Inc.

   App URL: https://www.microsoft.com/en-us/store/apps/whatsapp/9wzdncrdfwbs

   Name: Twitter

   Publisher: Twitter Inc.

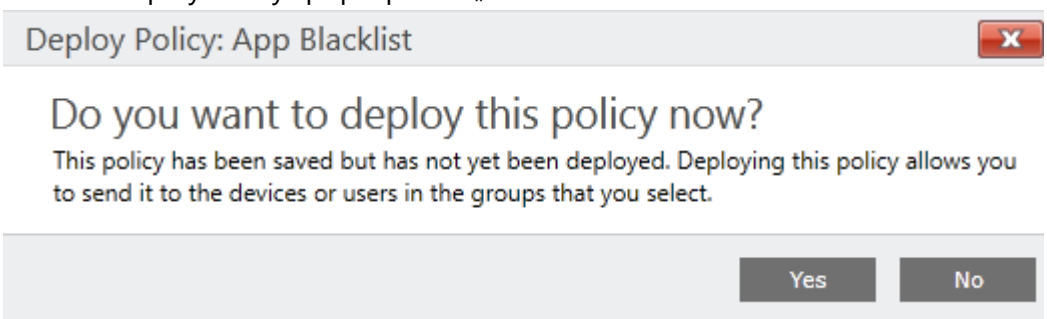
   App URL: https://www.microsoft.com/en-us/store/apps/twitter/9wzdncrfj140

   Name: Candy Crush Saga

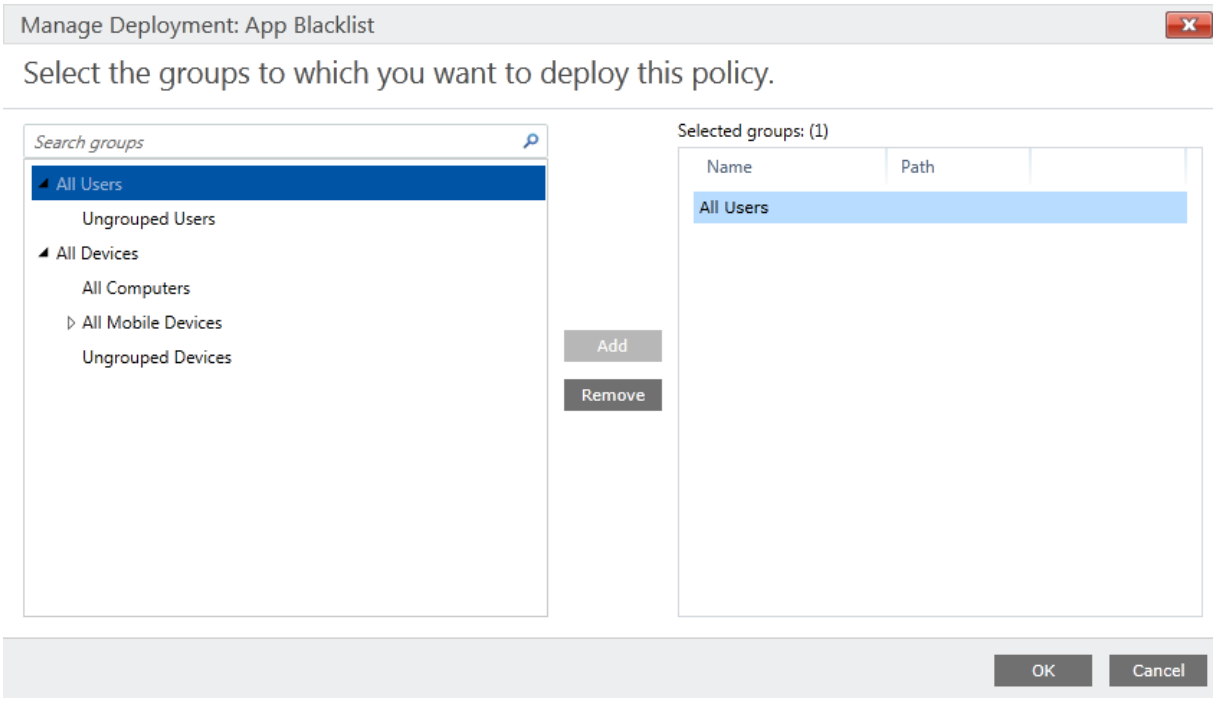
   Publisher: king.com

   App URL: https://www.microsoft.com/en-us/store/apps/candy-crush-saga/9nblggh18846

10. On the “Deploy Policy” pop-up click „Yes”.

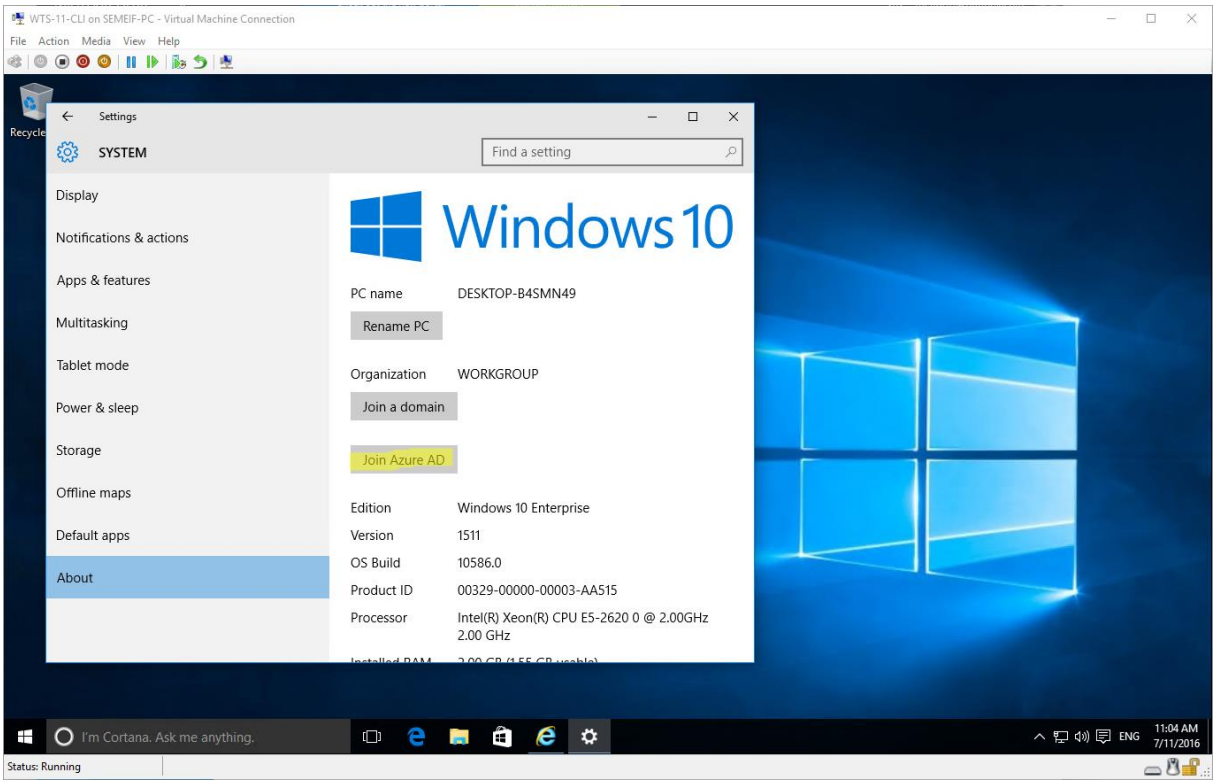


11. Add the “All Users” group and click “OK”.

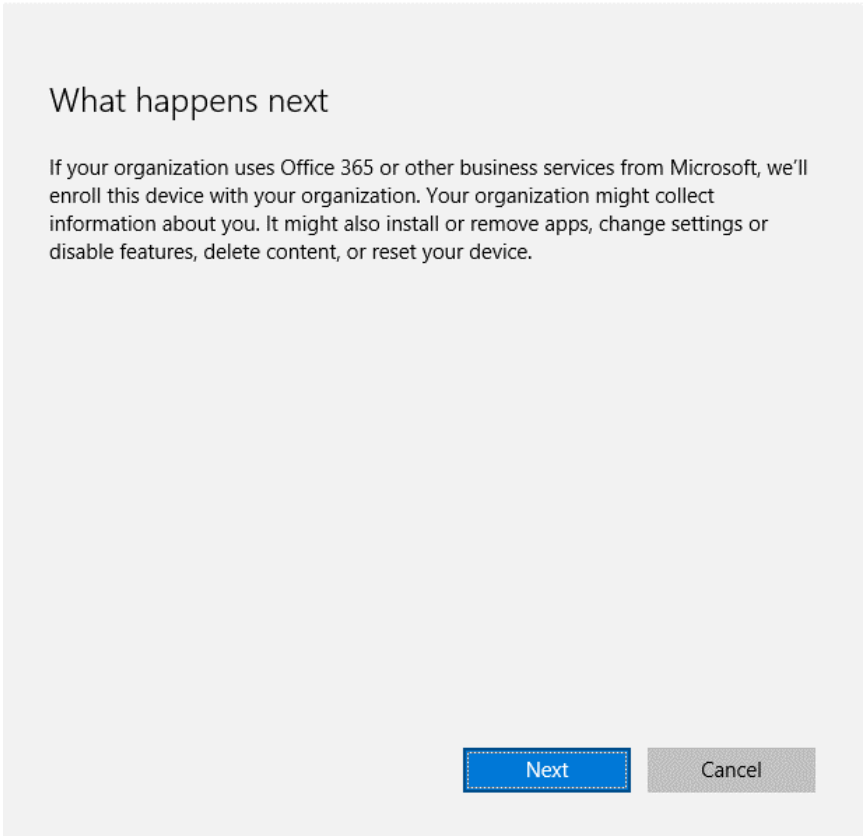


Azrue Active Directory Domain join

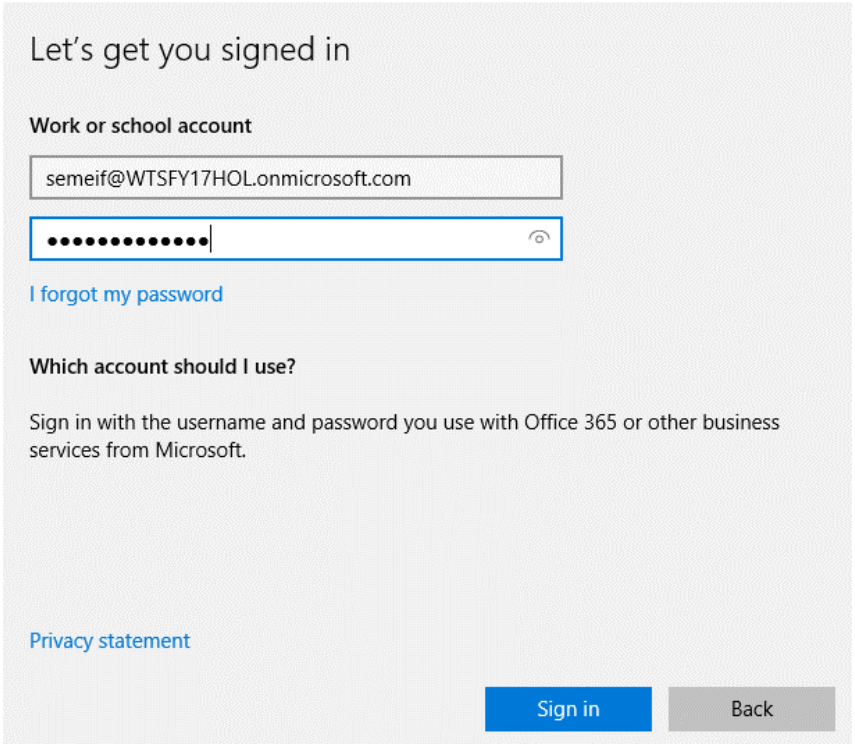
1. On the Client Lab machine WTS-12-CLI click on Start → Settings → System → About → Join Azure AD. (This sometimes takes **multiple attempts**!!! Cause of NAT→NAT→NAT)



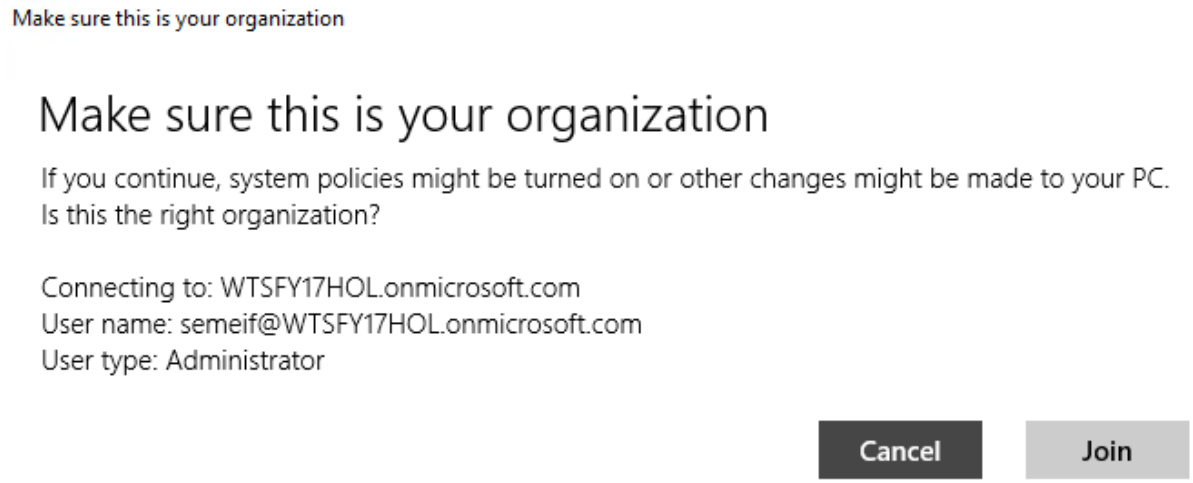
2. On the “What happens next” screen click “Next”.



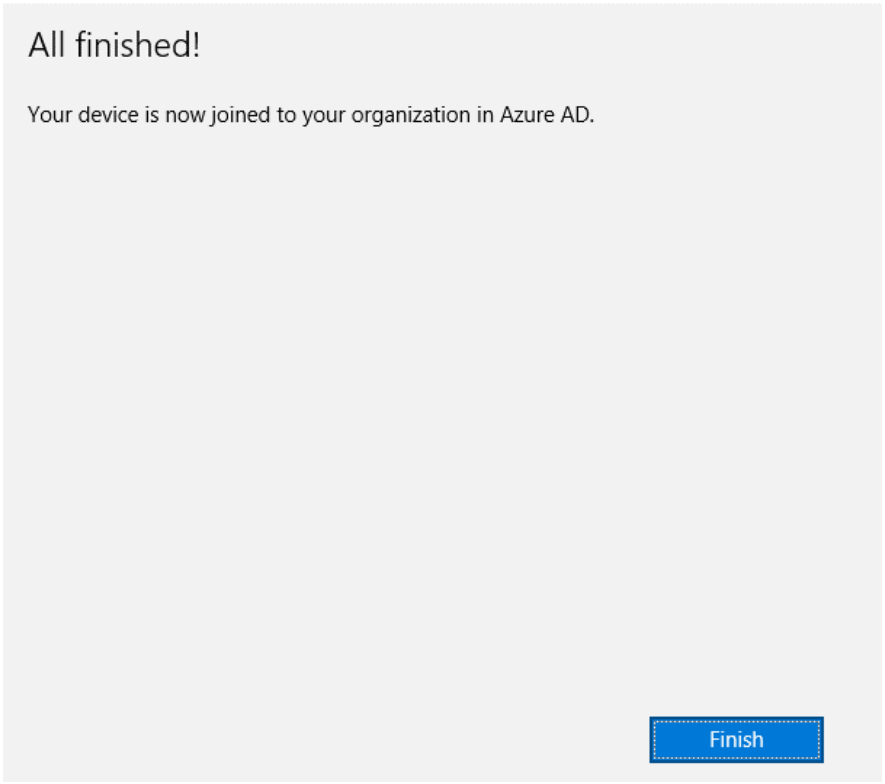
3. On the “Let’s get you signed in” screen enter the credentials of your Global administrator and click “Sign in”.



4. On the “Make sure this is your organization” scrren review the information and click “Join”.

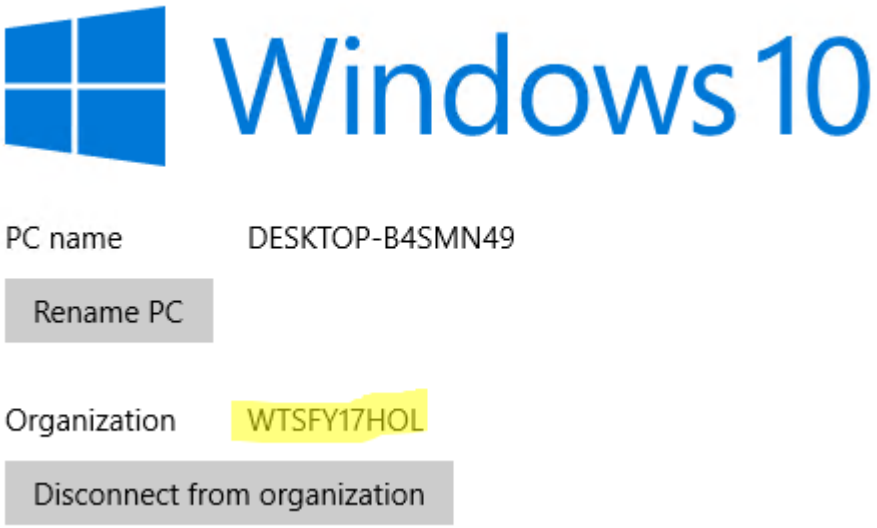


5. On the “All finished!” screen click “Finish”.

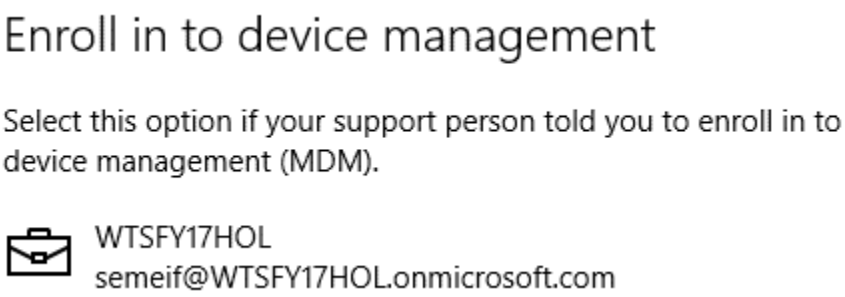


Verify Azure AD Connection

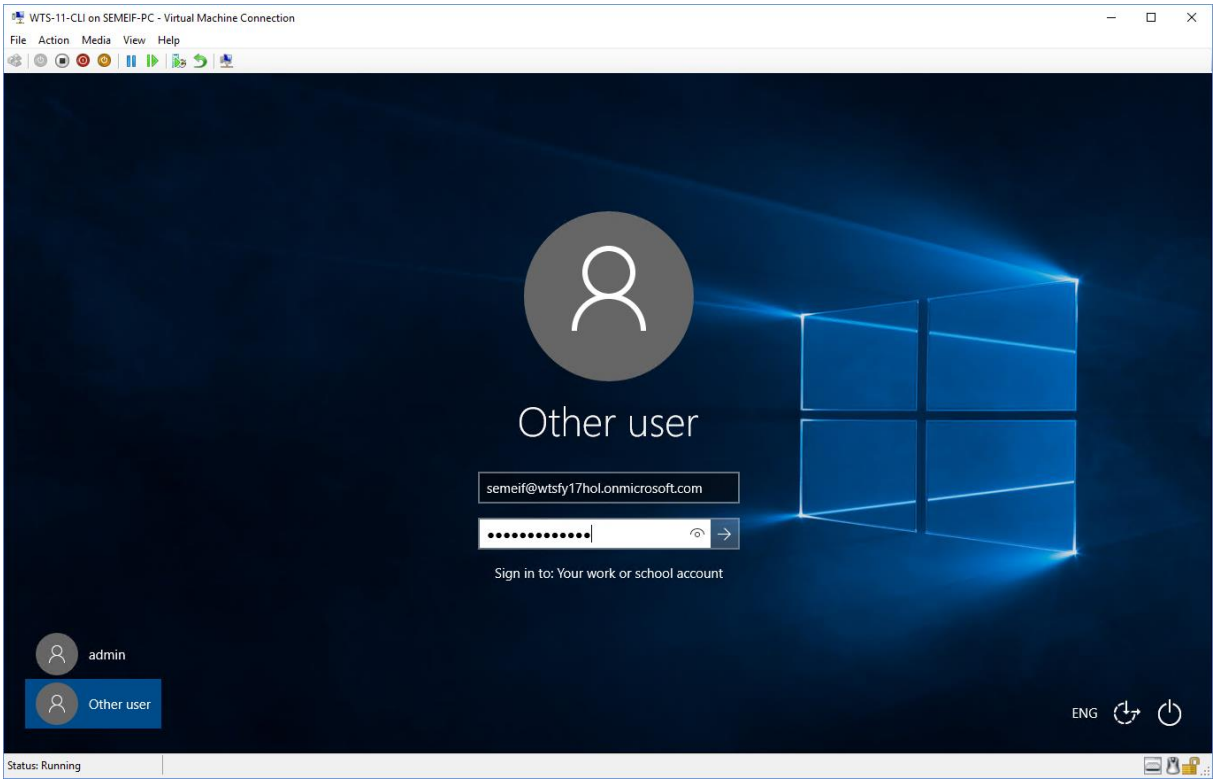
1. Verify that you are conncted to the organization in the settings menu:



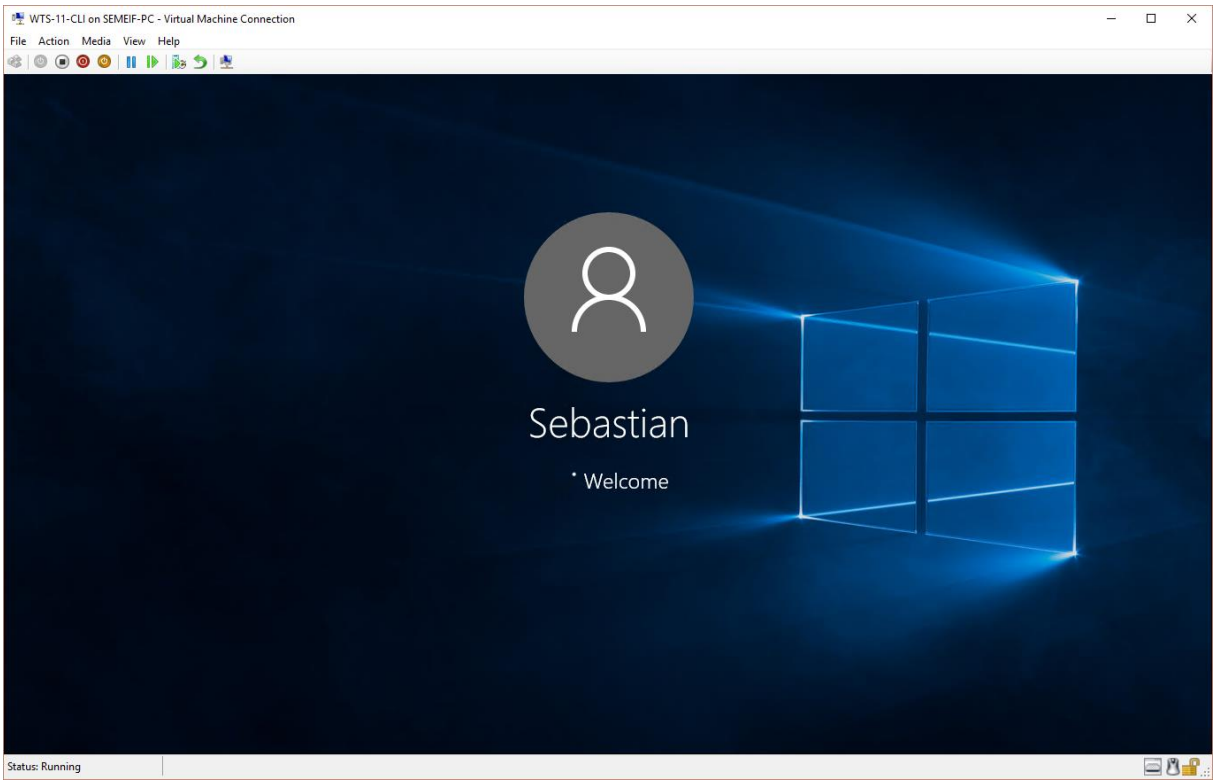
2. Verify that the system is managed through MDM. Go to Settings → Accounts → Work Access.



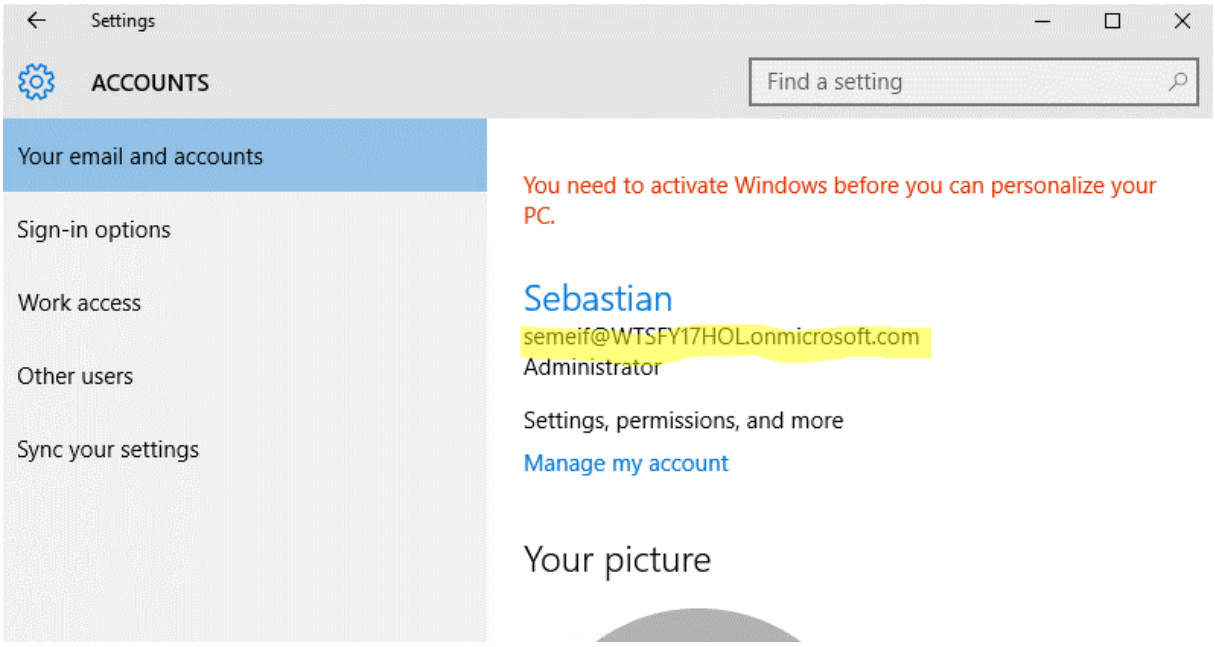
3. Reboot the machine and log in with the Global Admin account.



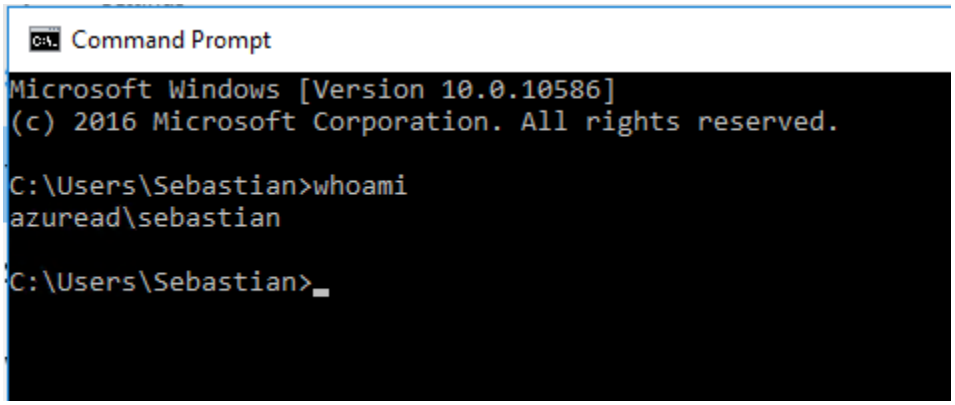
4.



5. Go to Start → Settings → Accounts and verify your user account.

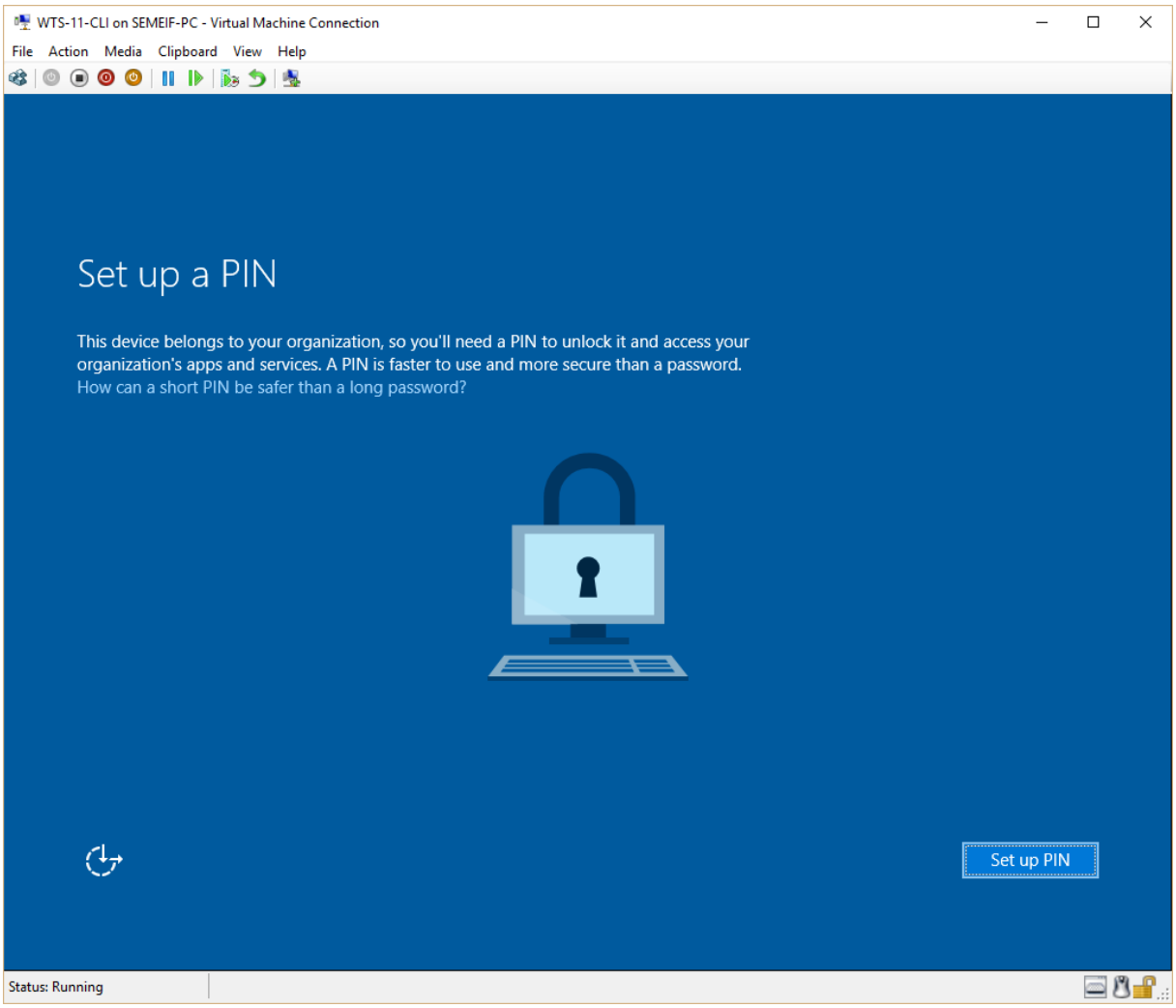


6. You also can verify through a command propt with the command “whoami”.

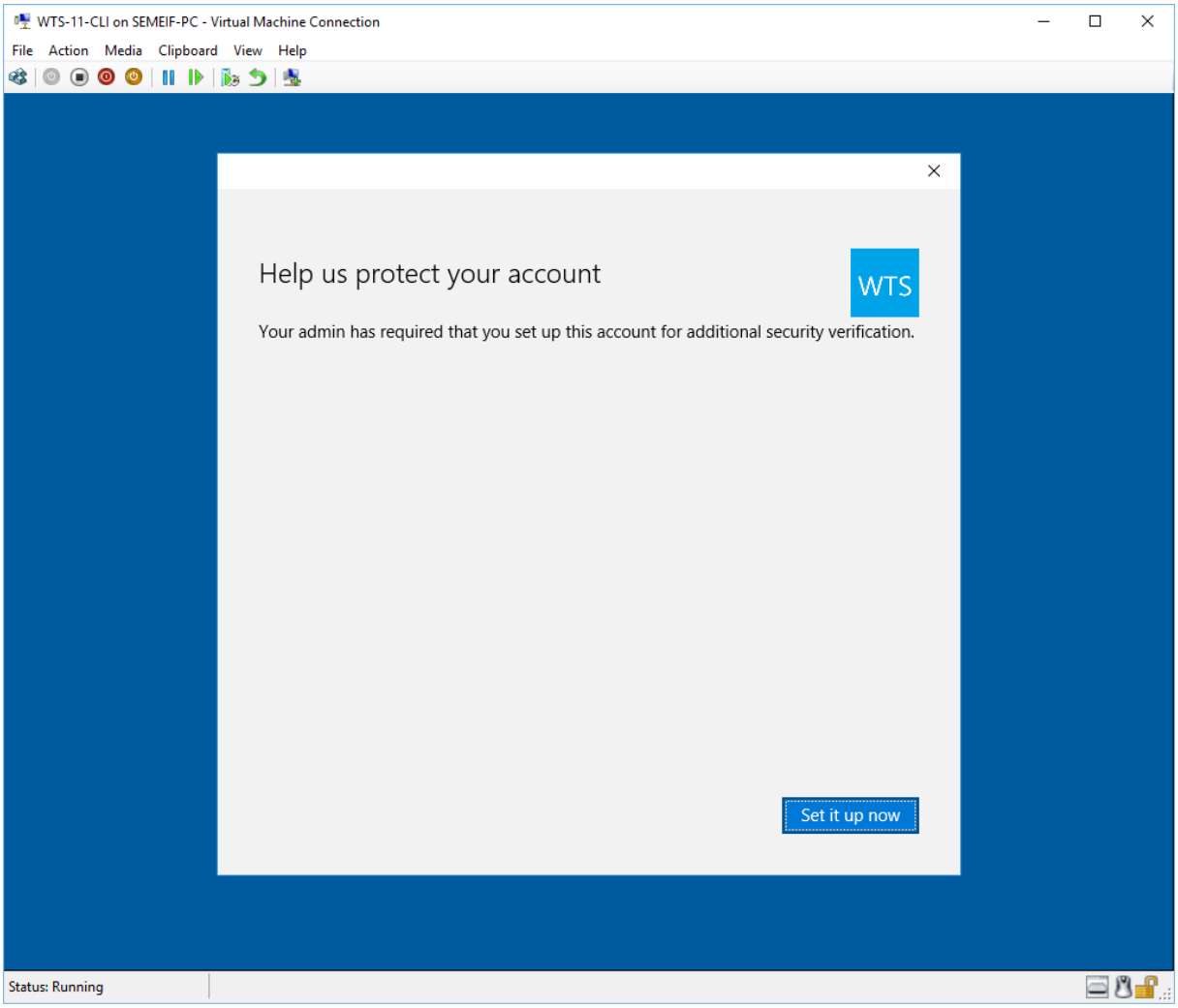


After some time the client will receive the policy (Check if it works in LoD System. In Hyper-V the screen just pops up in a "Basic" Session)

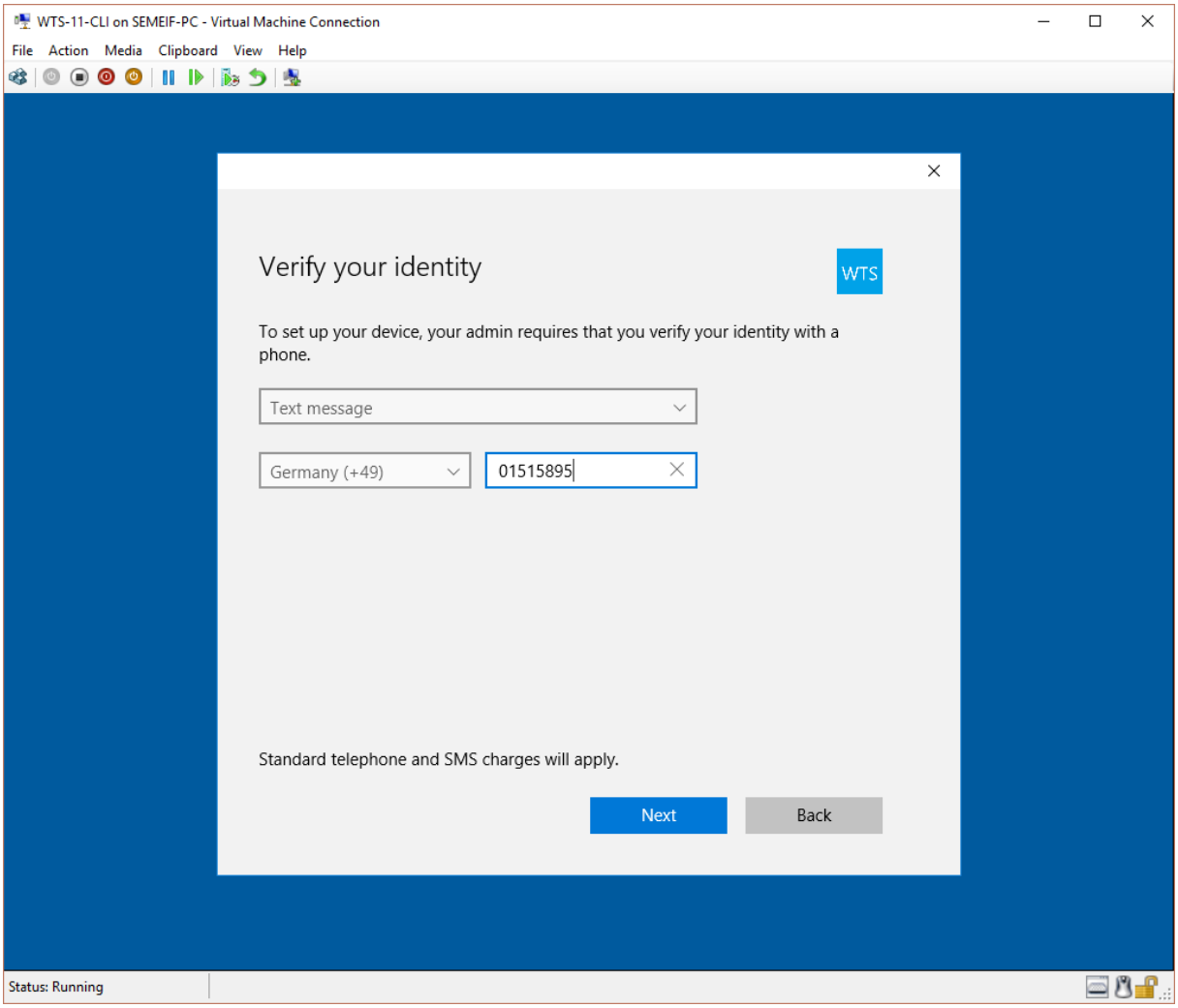
1. When you log on the machine you will get the "Set up a pin" dialogue. Click on "Set-up PIN".



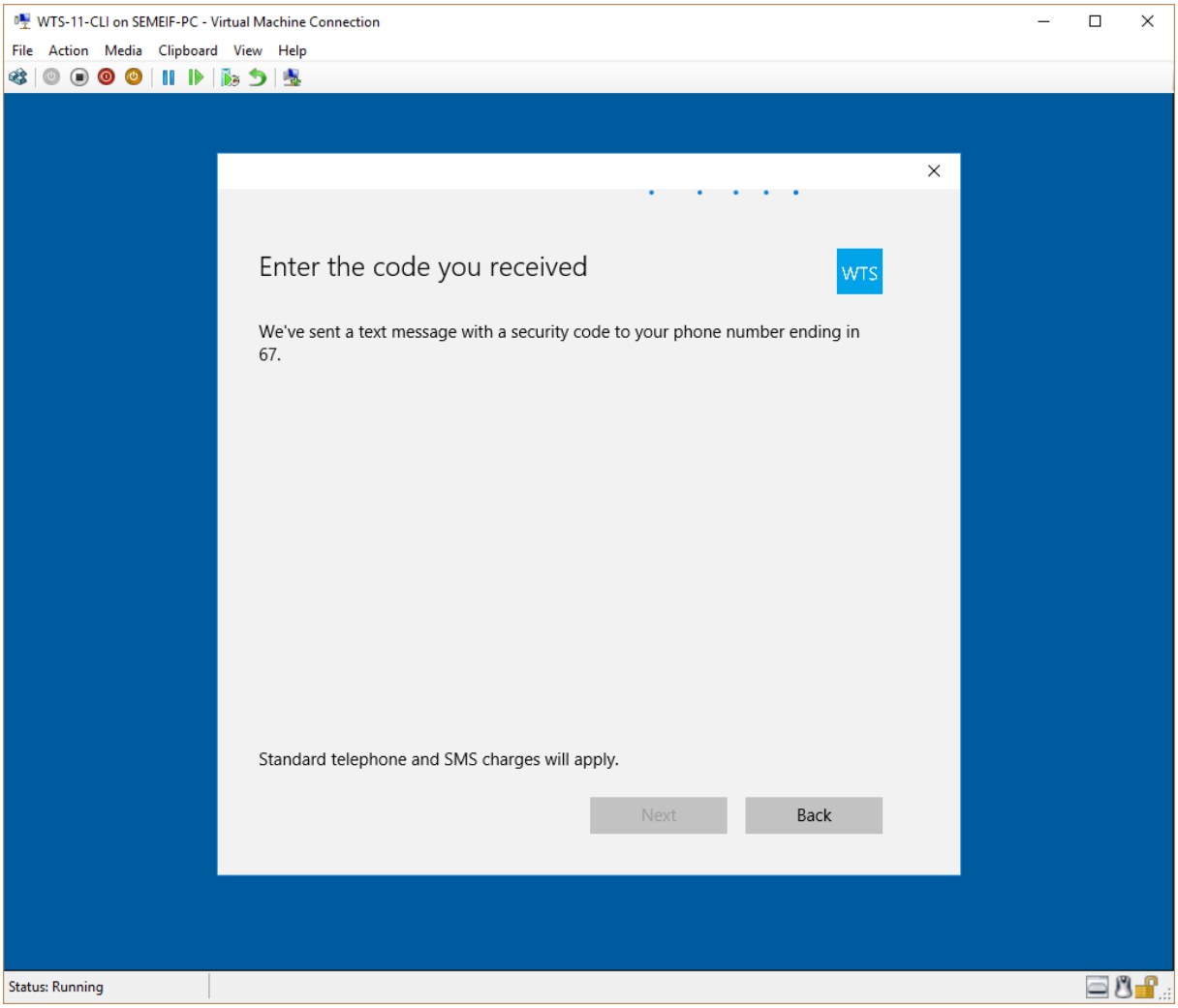
2. On the „Help us protect your account“ screen click „Set it up now”.



3. On the „Verify your identity“ screen choose “Text message” and enter your country code and mobile phone number and click “Next”.



4. Enter the code you received and click “Next”

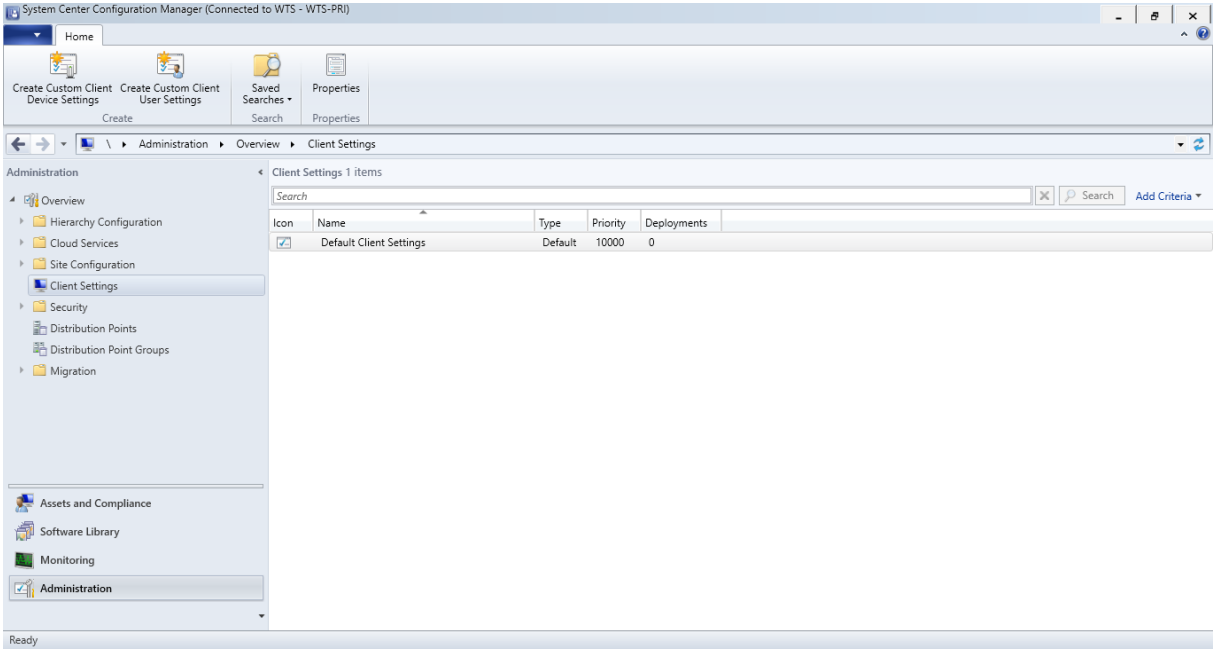


5. Now you can set-up your PIN.

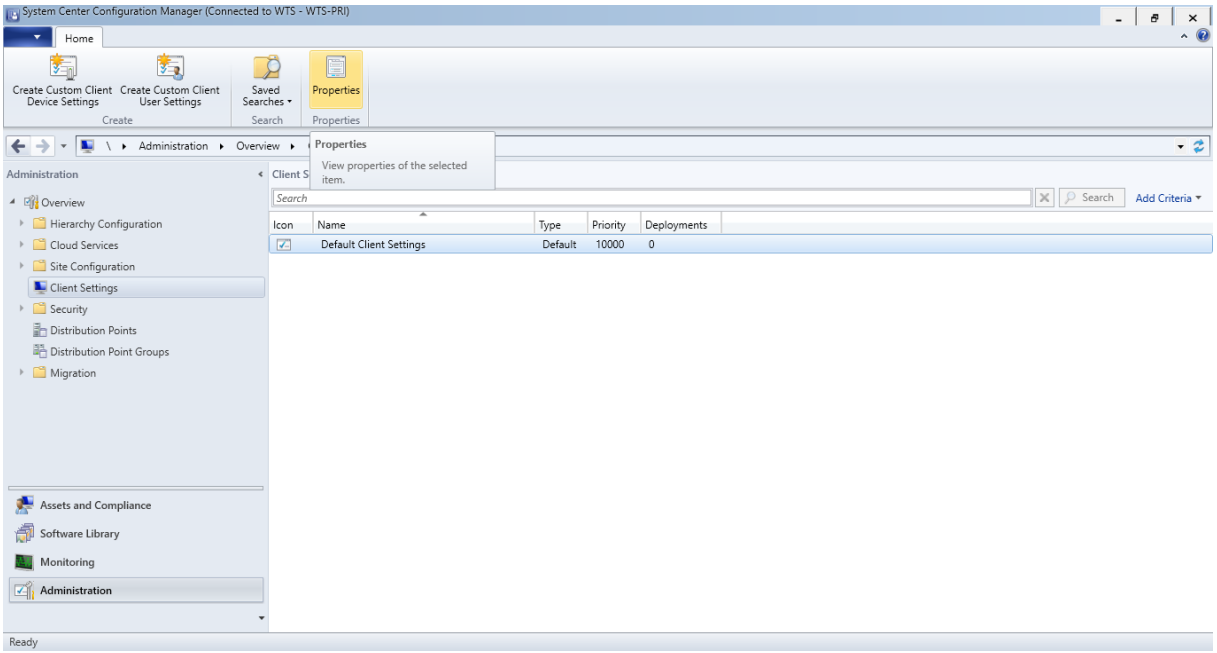
2. Lab guide part 2 – Security with Configuration Manager

2.1. Client Settings in Configuration Manager (Time: 5:00)

1. On the Configuration Manager Server WTS-04-CAS log-on as admin.
2. In the Configuration Manager console navigate to the Administration workspace and click on “Client Settings”.

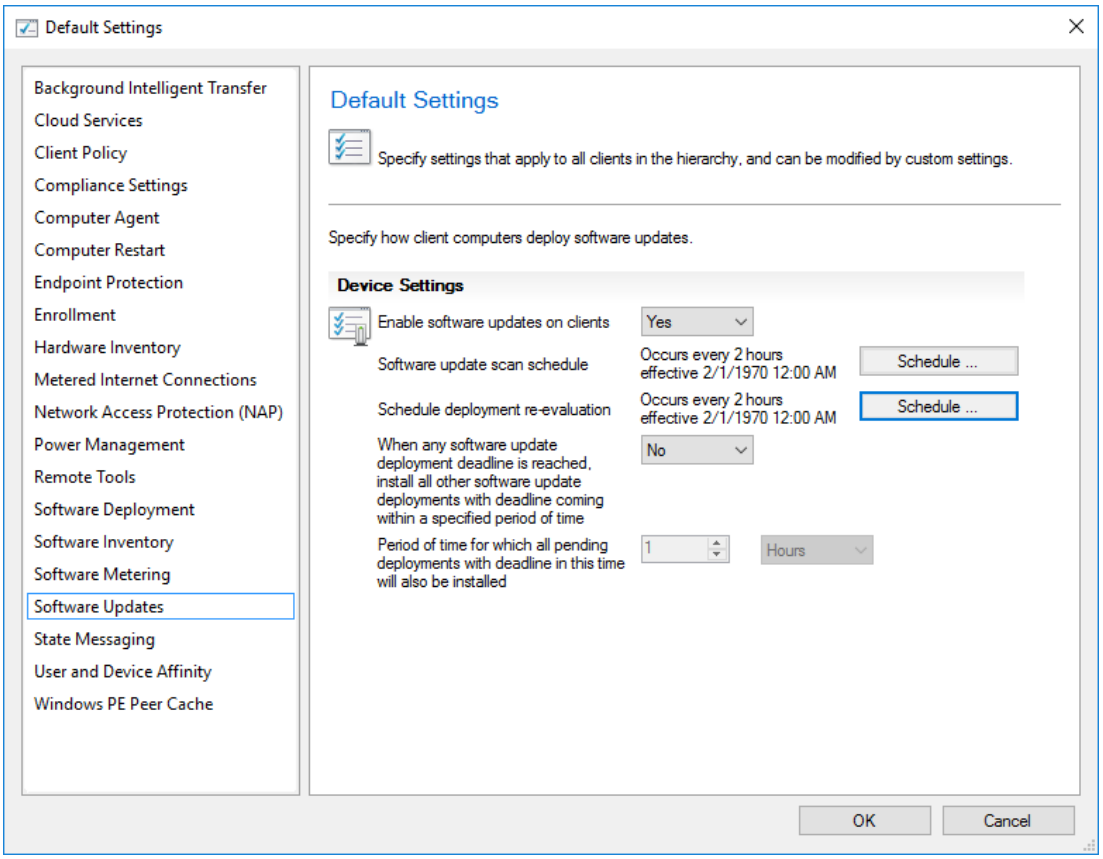


3. Highlight the “Default client Settings” and click on “Properties”.

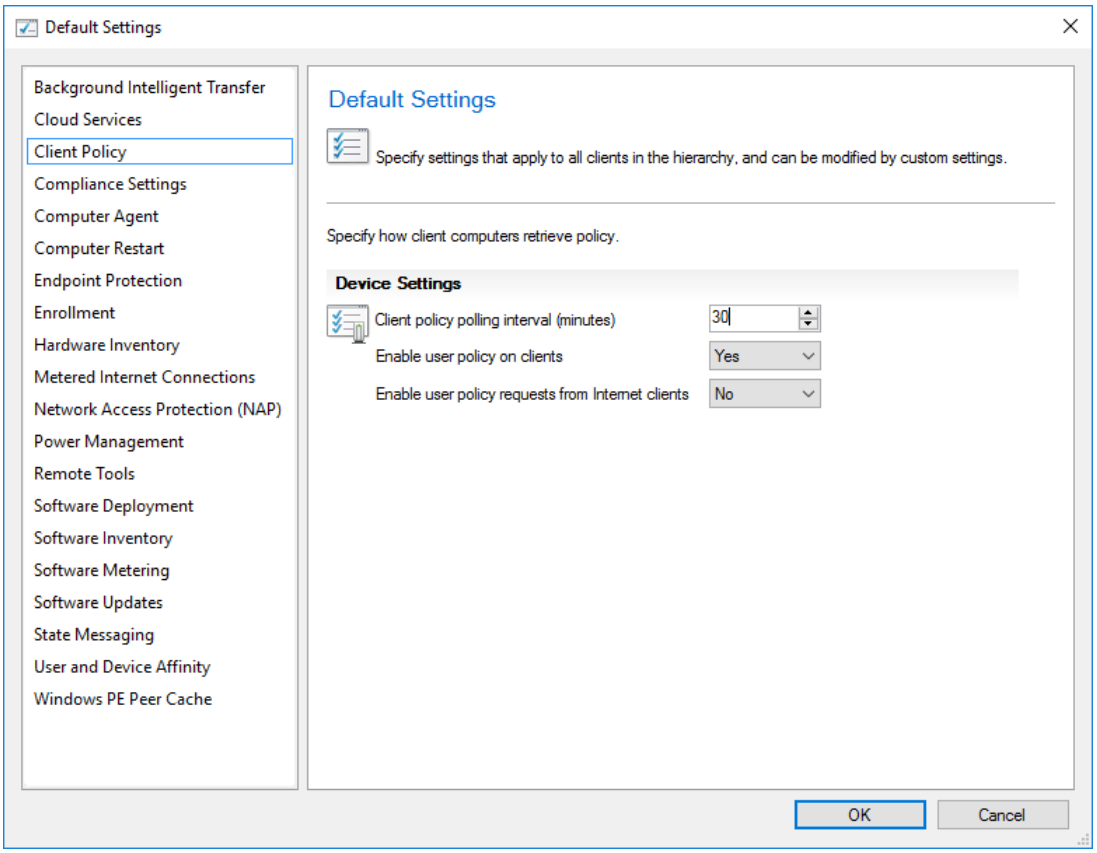


4. Edit the Client Settings as the following:

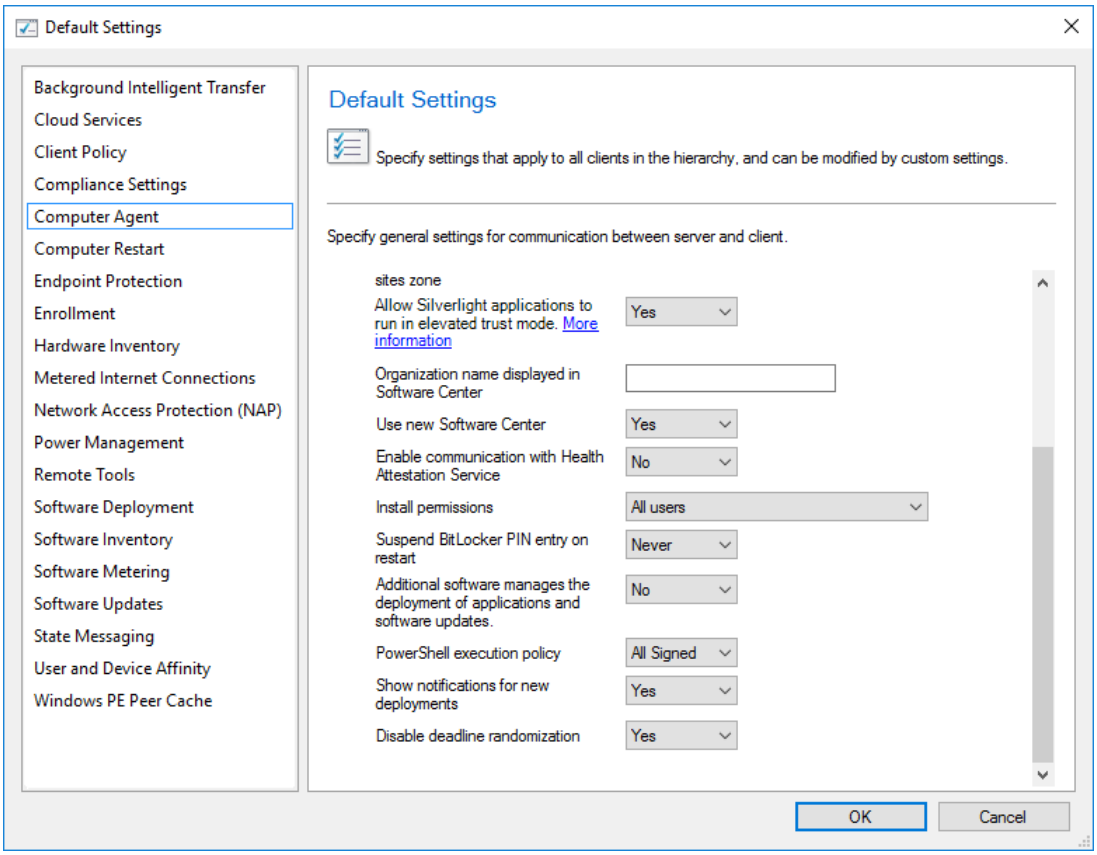
Software updates schedule



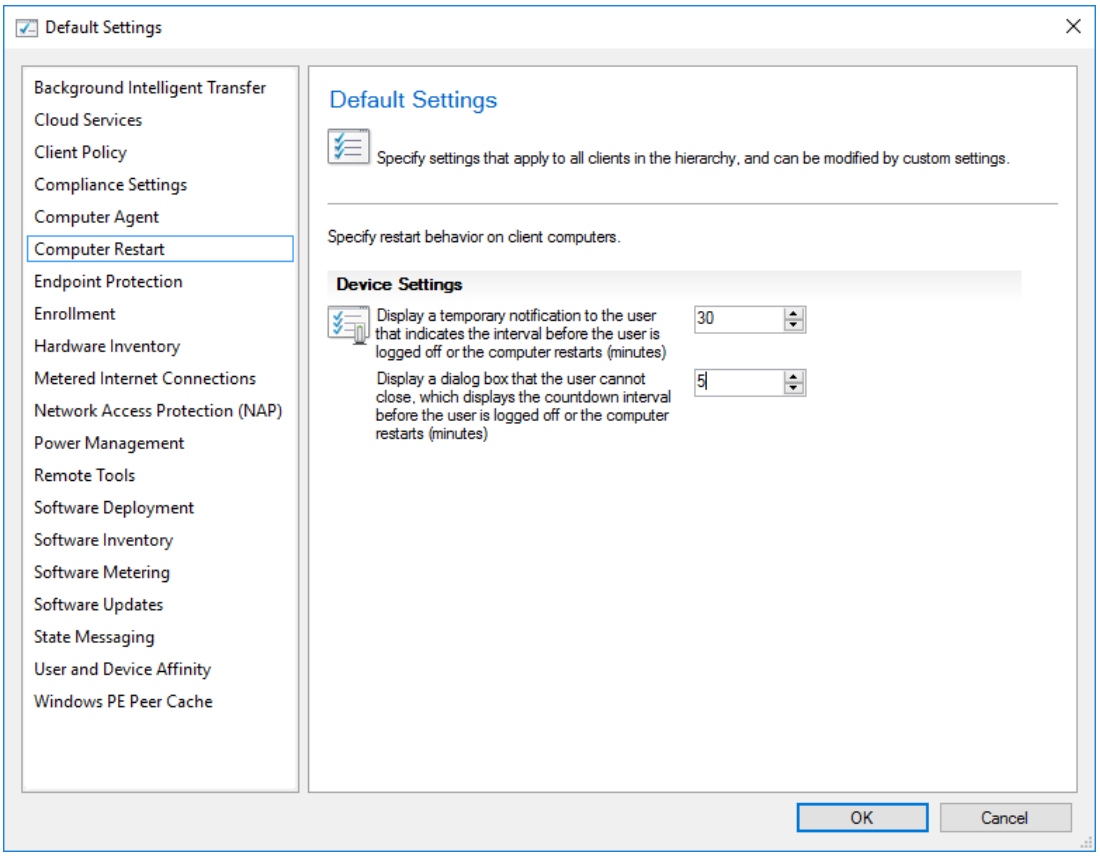
Client Policy



Default settings



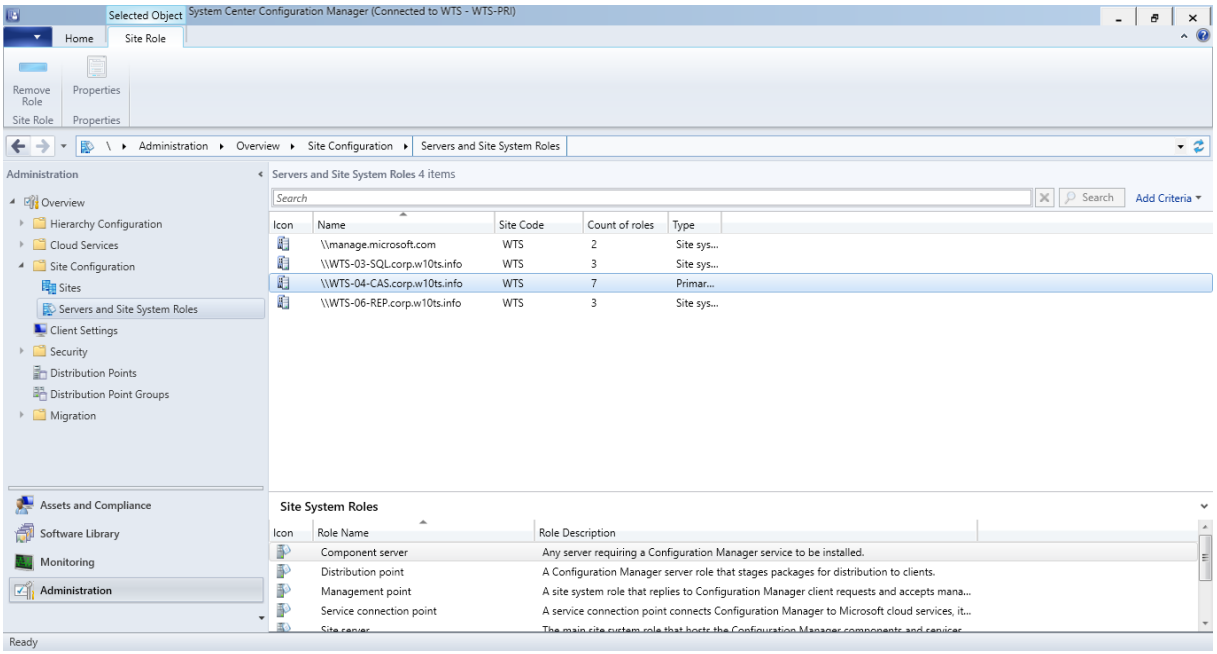
Computer restart



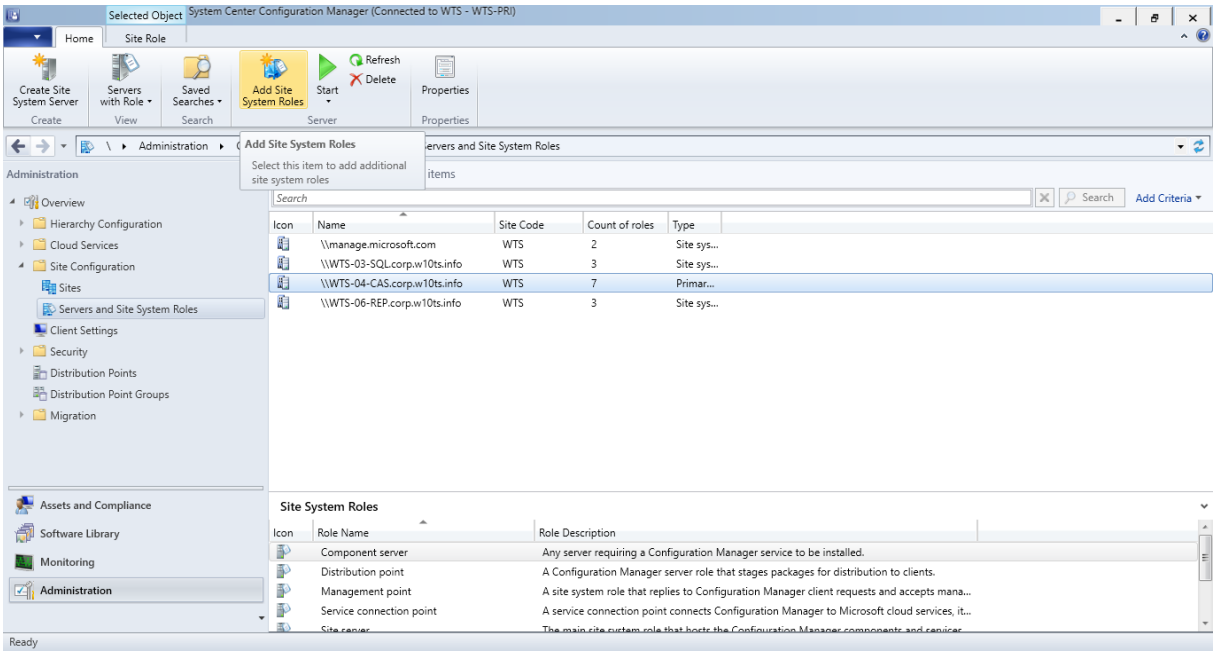
2.2 Managing Endpoint Protection/Defender with Config Manager

2.1.1. Install Endpoint Protection Site System Role

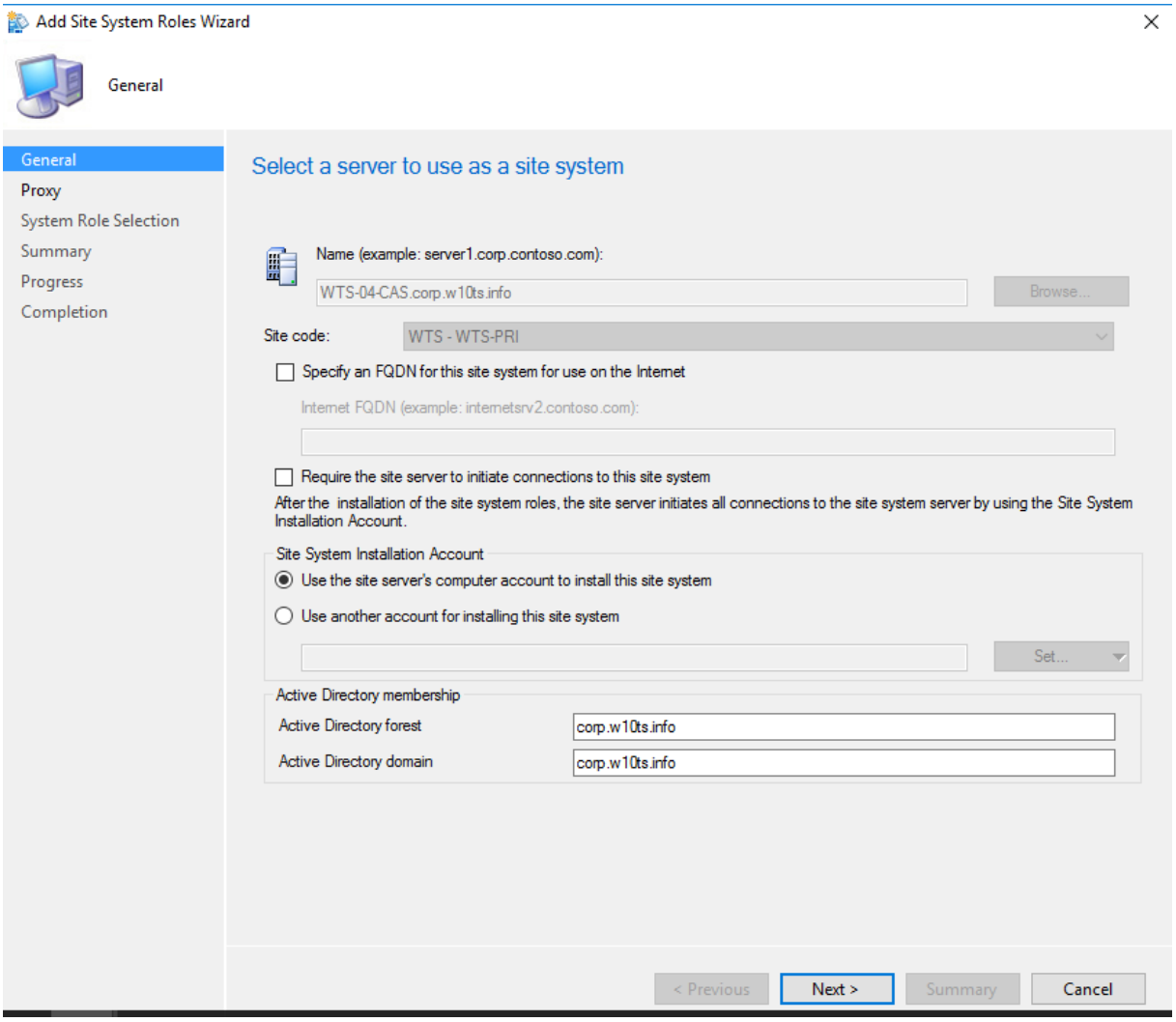
1. In the Configuration Manager console, click Administration.
2. In the Administration workspace, expand Site Configuration, click Servers and Site System Roles, and then select the server that you want to use for Endpoint Protection.



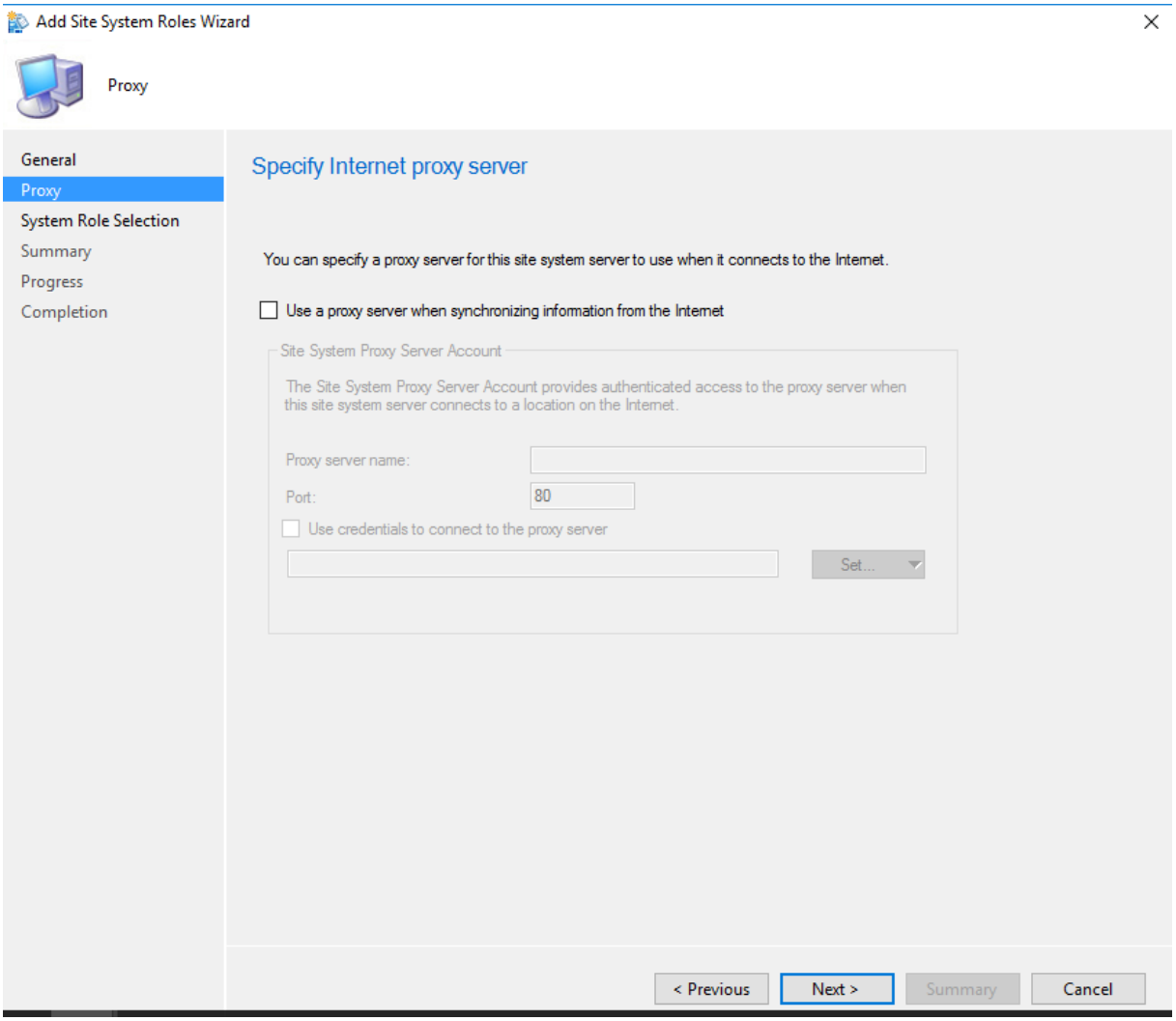
3. On the Home tab, in the Server group, click Add Site System Roles.



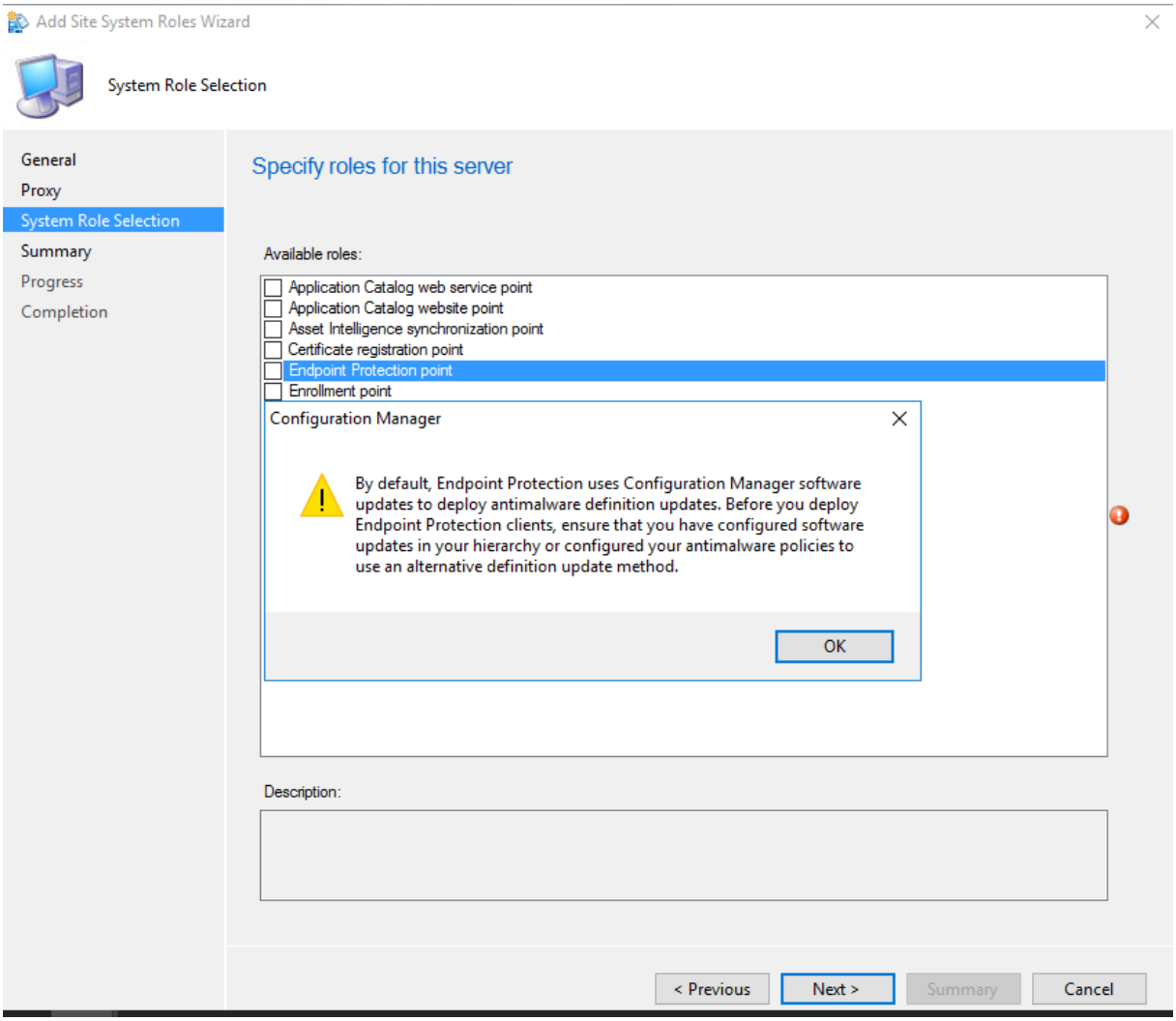
4. On the General page, leave the defaults and then click “Next”.



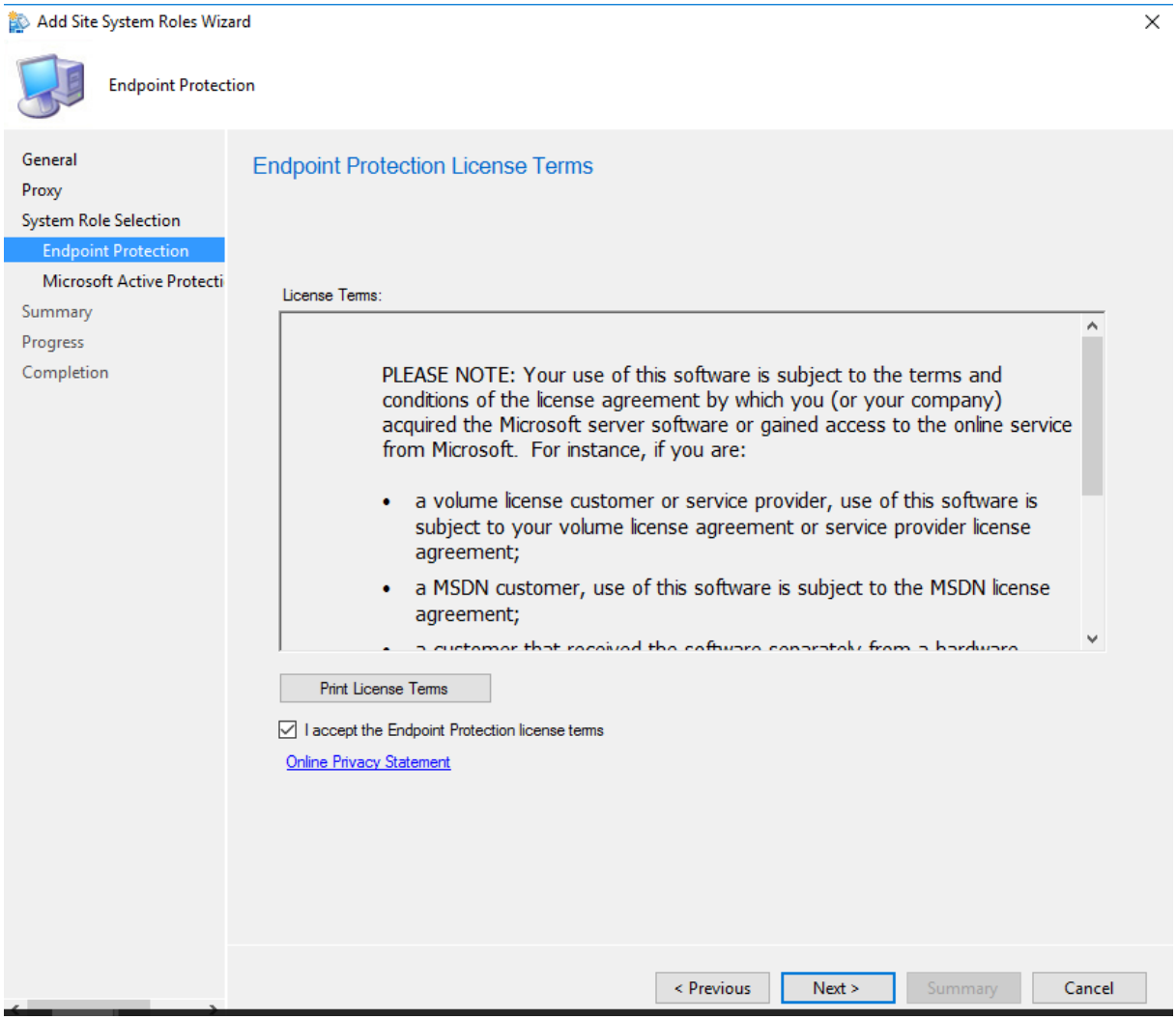
5. On the Proxy page, leave the defaults and then click “Next”.



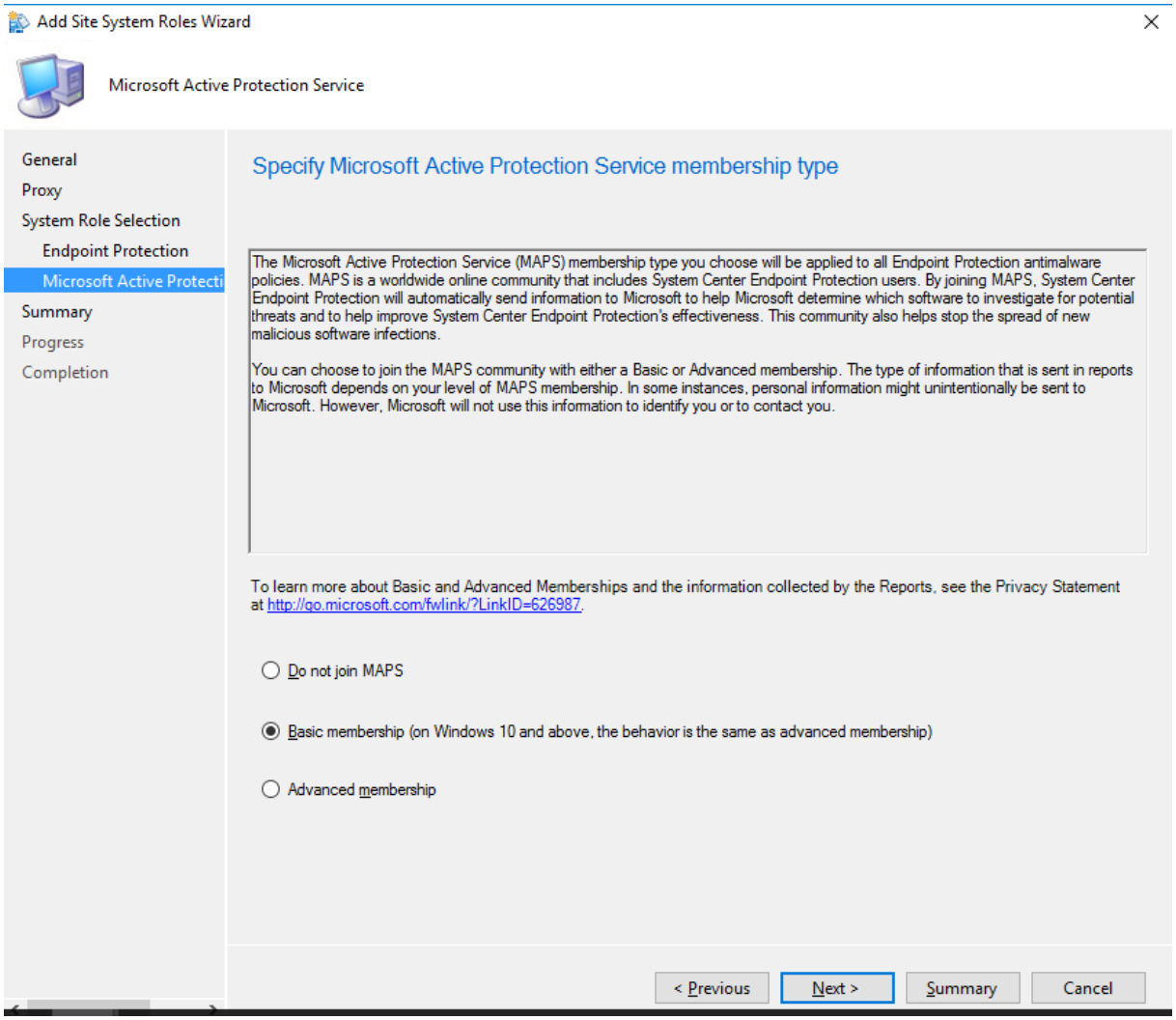
6. On the System Role Selection page, select Endpoint Protection point in the list of available roles, confirm the warning dialog and then click “Next”.



7. On the Endpoint Protection page, select the I accept the Endpoint Protection license terms check box, and then click “Next”.



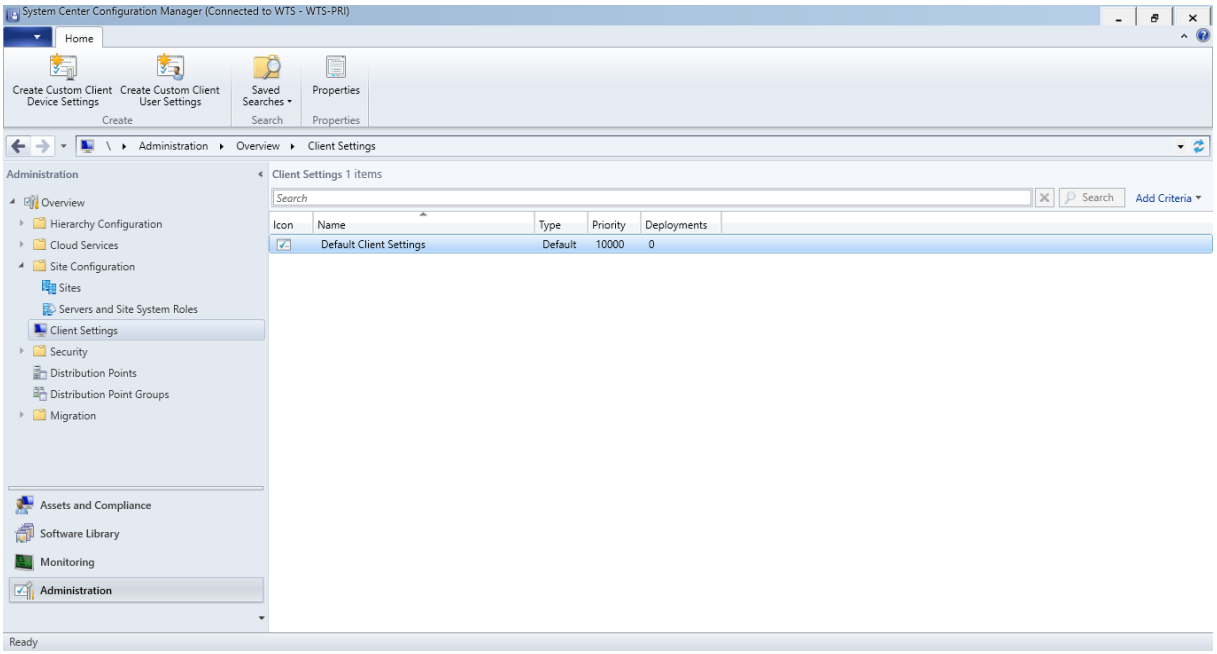
8. On the Microsoft Active Protection Service page, select the level of information that you want to send to Microsoft to help develop new definitions, and then click “Next”.



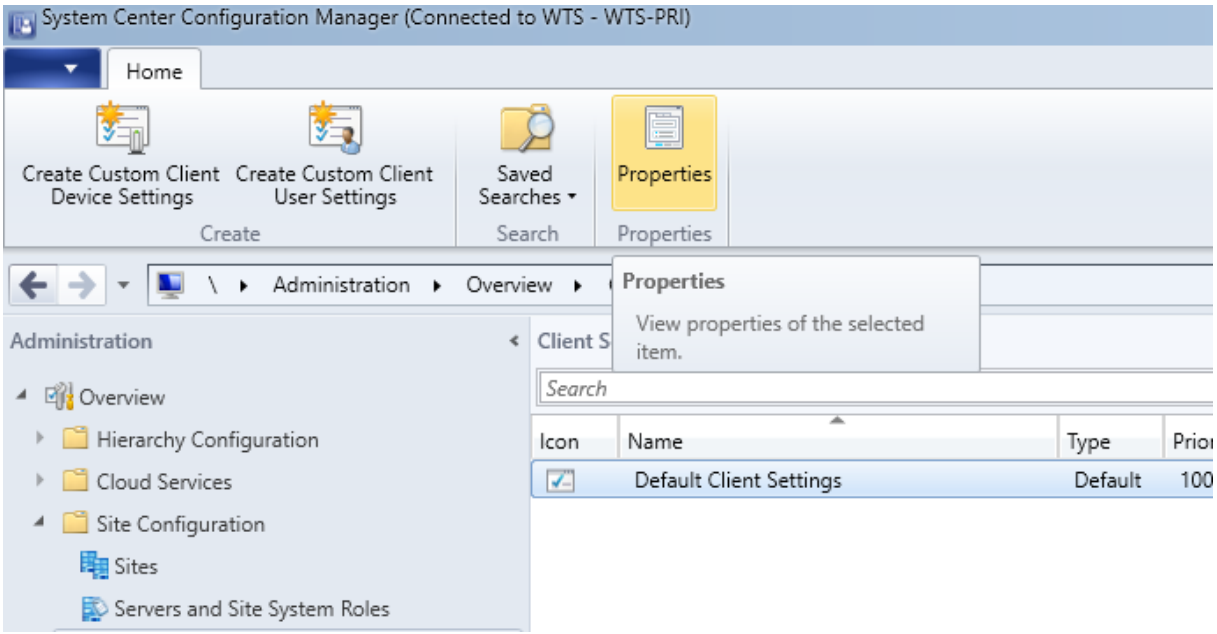
9. Complete the wizard and click on “Close”.

2.1.2. Enable Endpoint Protection in client settings

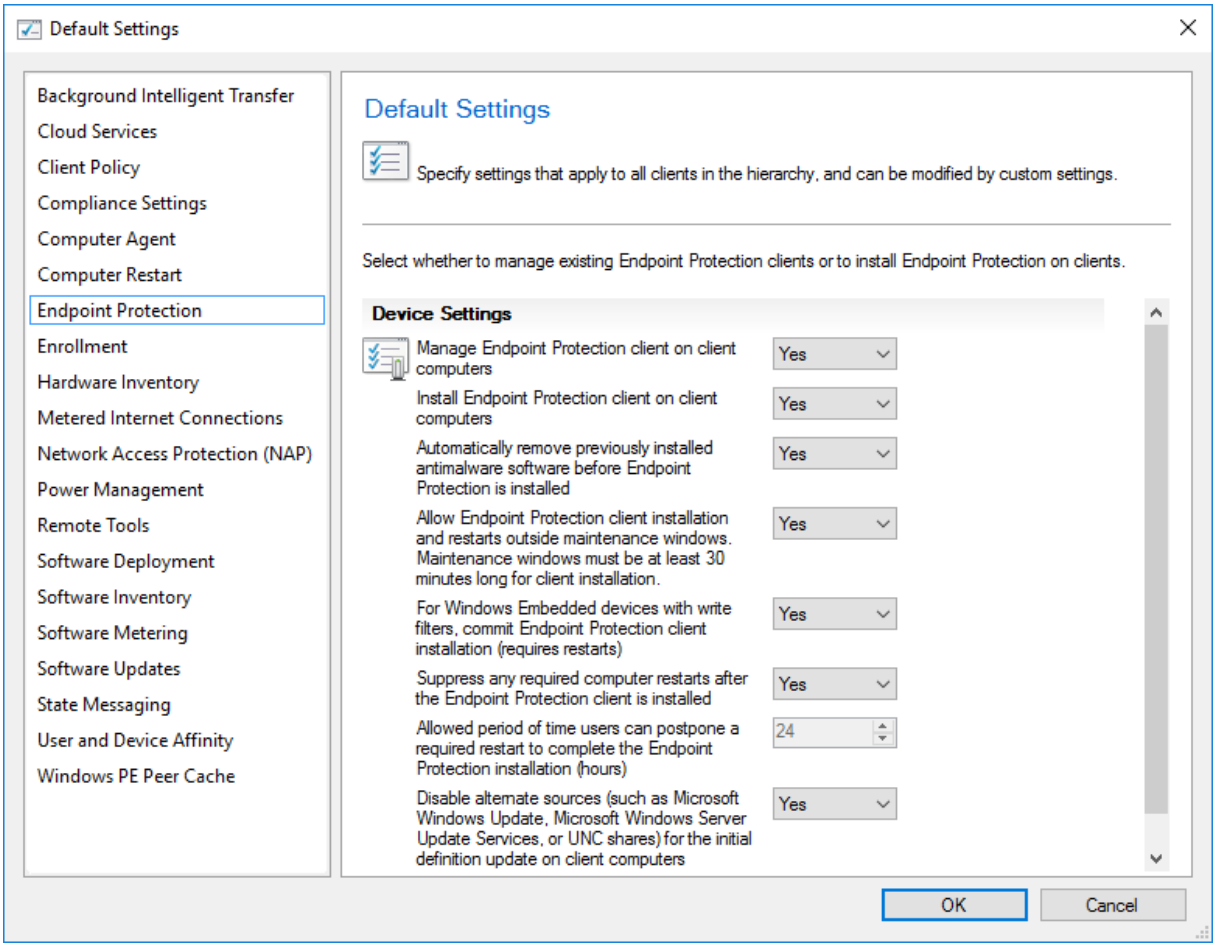
1. In the Administration workspace, expand ”Site Configuration”, select “Client Settings” and highlight the “Default Client Settings”.



2. Click on Properties.



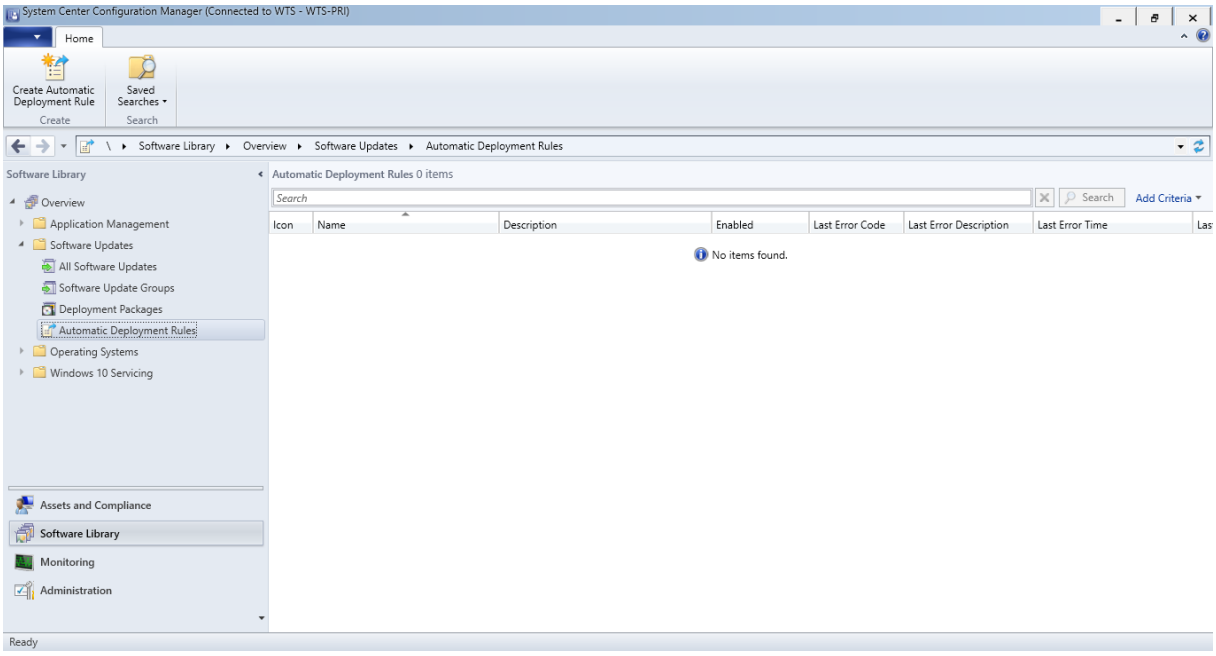
3. Select “Yes” at “Manage Endpoint Protection client on client computers” in the Endpoint Protection “Device Settings”.



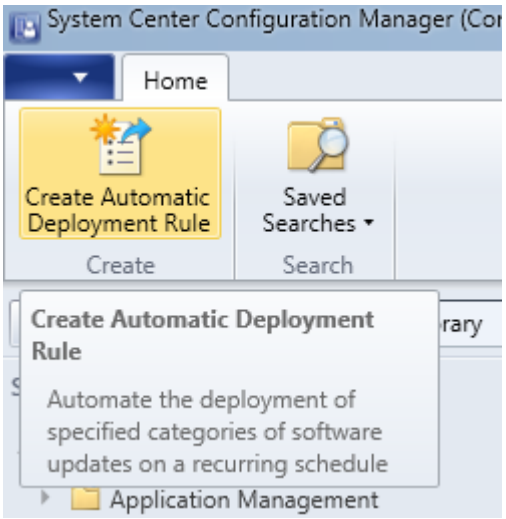
4. Click “OK”.

2.1.3. Configure Configuration Manager Software Updates to Deliver Definition Updates

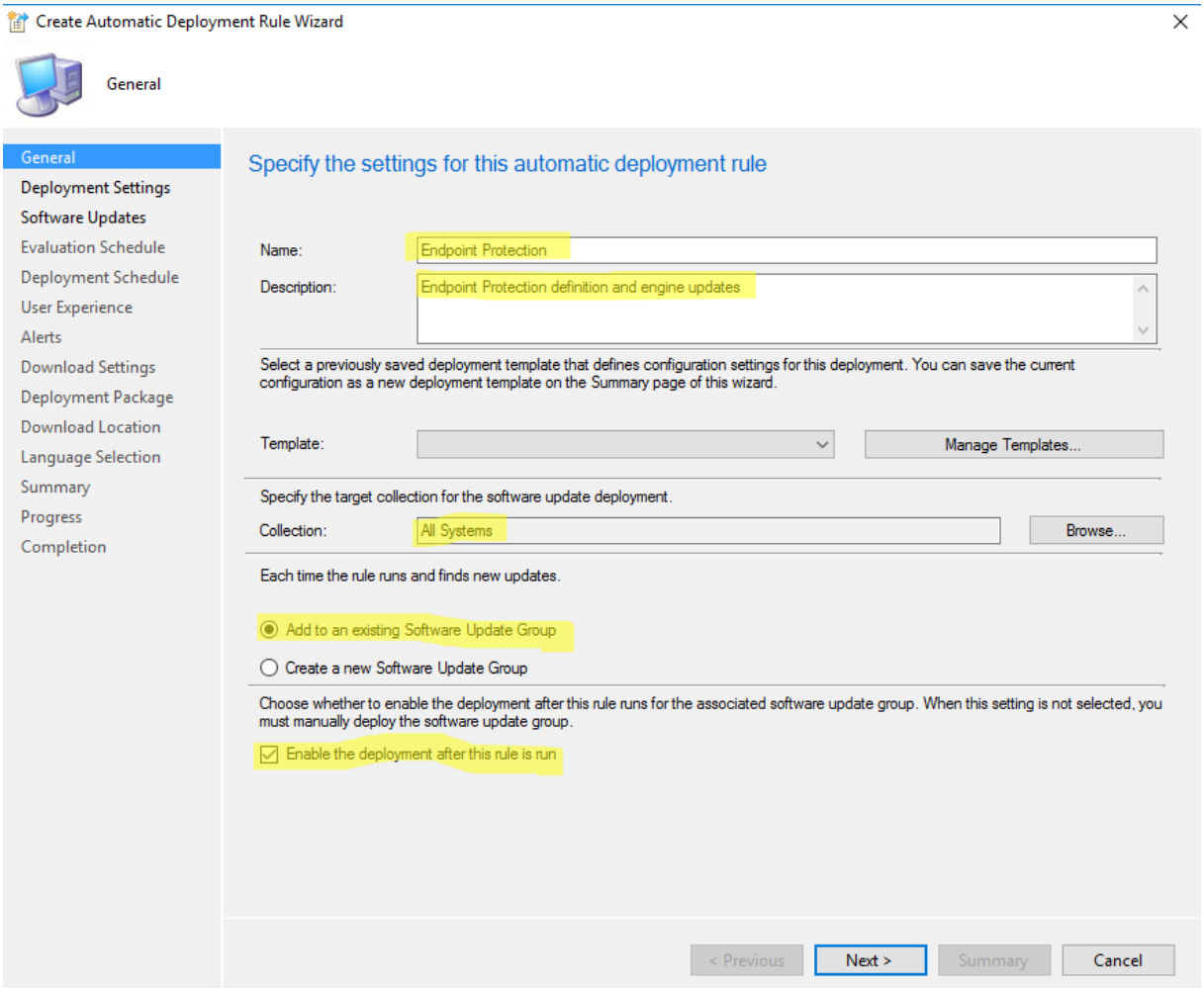
1. In the Configuration Manager console, click Software Library.
2. In the Software Library workspace, expand Software Updates, and then click Automatic Deployment Rules.



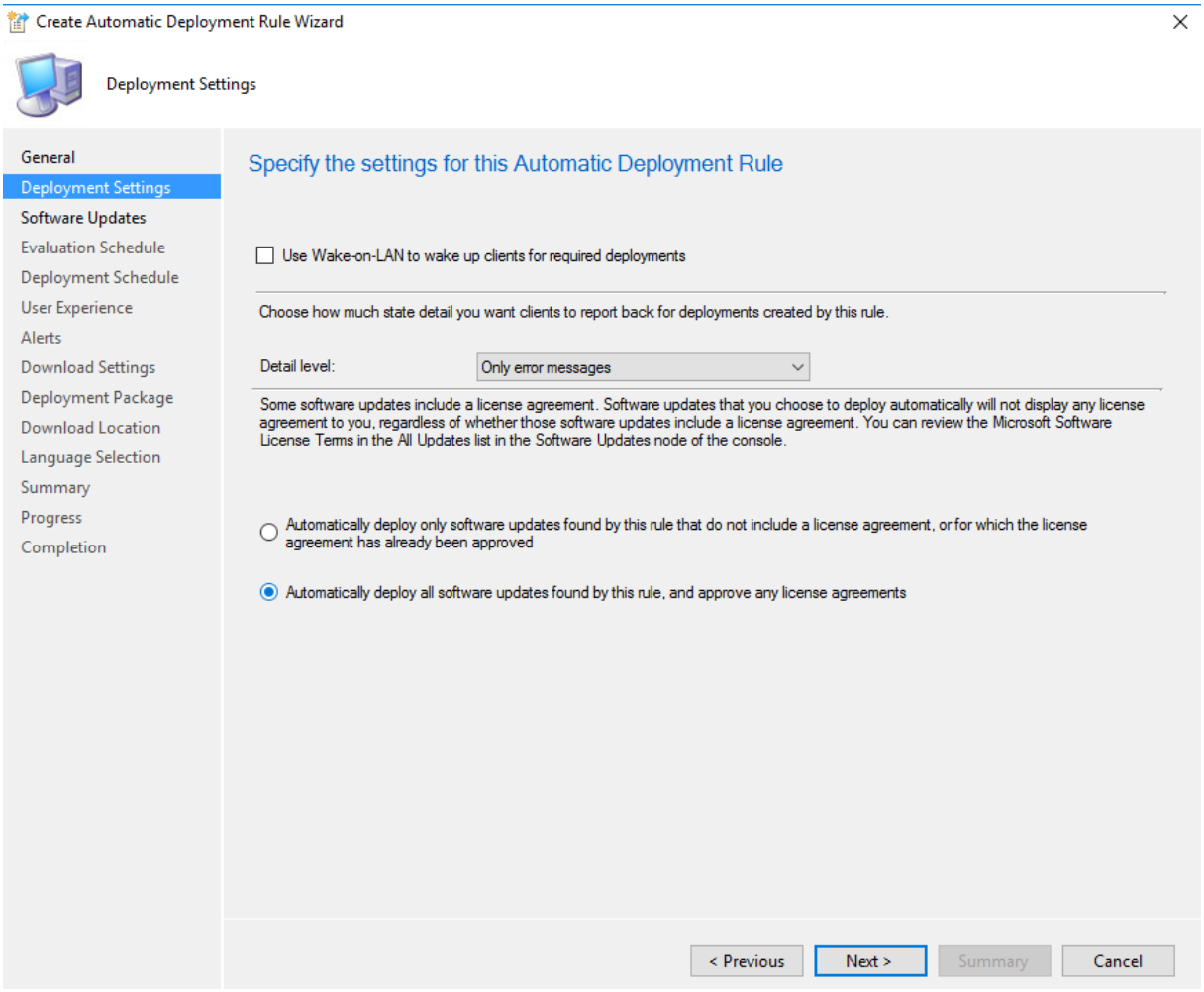
3. On the Home tab, in the Create group, click Create Automatic Deployment Rule.



4. On the General page of the Create Automatic Deployment Rule Wizard, specify the following information: Name, Description and Collection.
   - Click Add to an existing Software Update Group.
   - Make sure that the Enable the deployment after this rule is run check box is selected, and then click “Next”.

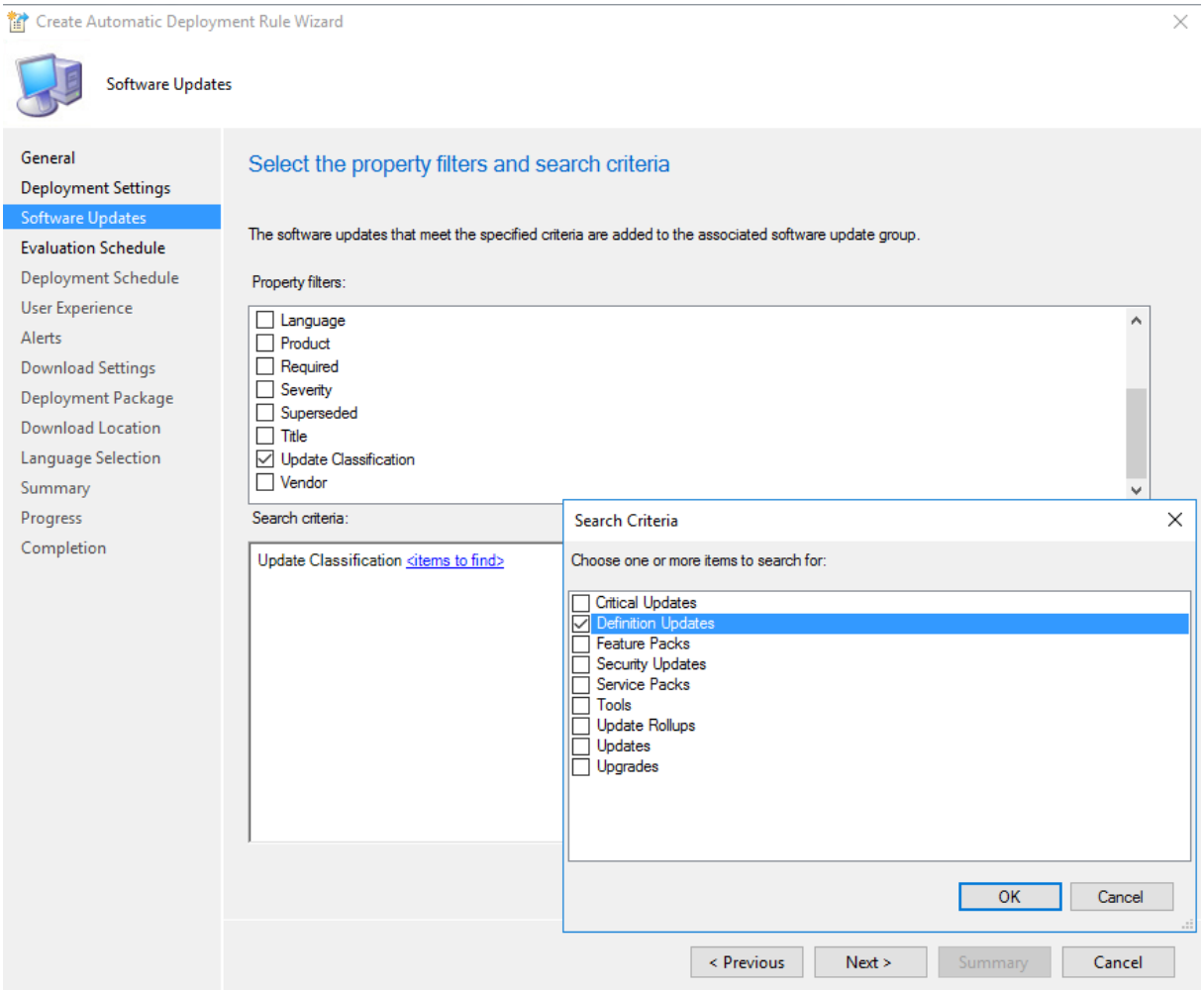

Create Automatic Deployment Rule Wizard
General
General
Deployment Settings
Software Updates
Evaluation Schedule
Deployment Schedule
User Experience
Alerts
Download Settings
Deployment Package
Download Location
Language Selection
Summary
Progress
Completion
Specify the settings for this automatic deployment rule
Name:
Endpoint Protection
Description:
Endpoint Protection definition and engine updates
Select a previously saved deployment template that defines configuration settings for this deployment. You can save the current configuration as a new deployment template on the Summary page of this wizard.
Template:
Manage Templates...
Specify the target collection for the software update deployment.
Collection:
All Systems
Browse...
Each time the rule runs and finds new updates.
Add to an existing Software Update Group
Create a new Software Update Group
Choose whether to enable the deployment after this rule runs for the associated software update group. When this setting is not selected, you must manually deploy the software update group.
Enable the deployment after this rule is run
< Previous
Next >
Summary
Cancel

5. On the Deployment Settings page of the wizard, in the Detail level list, select “Only Error Messages”, and then click “Next”.



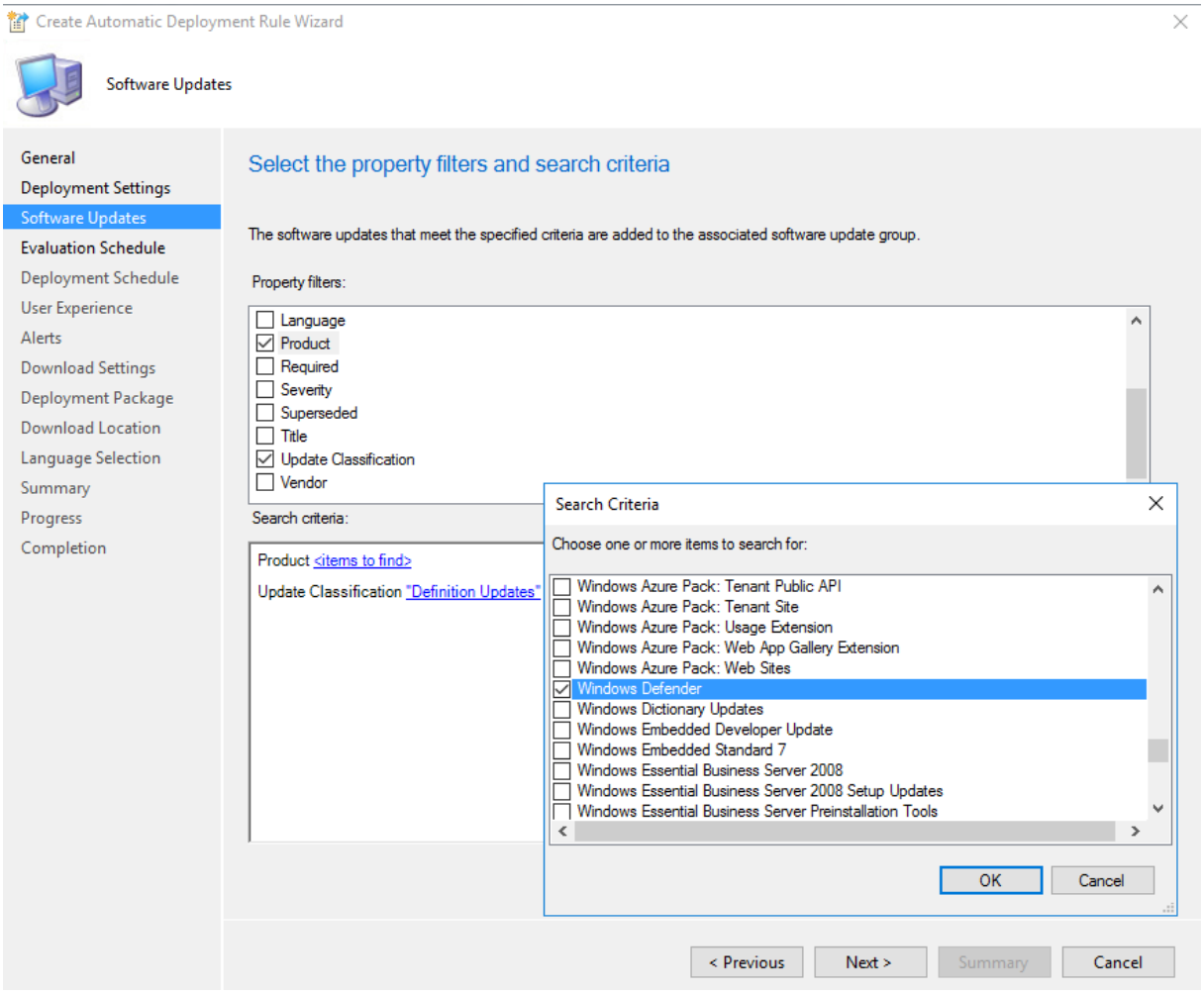
6. In the Property filters list, select the Update Classification check box and in the Search criteria list, click <items to find>. Then, in the Search Criteria dialog box, in the Specify the value to search for list, select Definition Updates. Click OK to close the Search

Criteria dialog box.



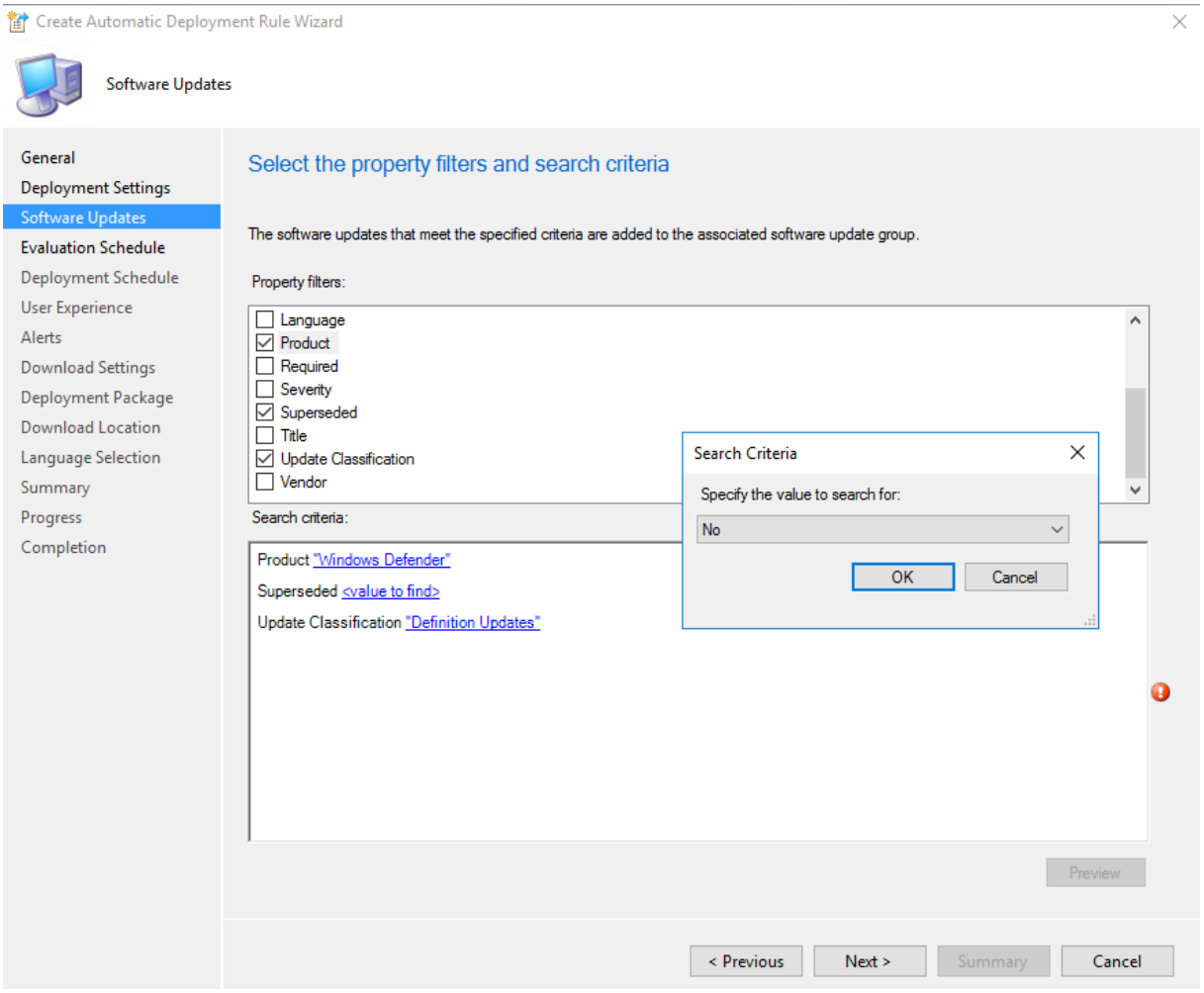
7. In the Property filters list, select the Product check box and in the Search criteria list, click <items to find>. Then, in the Search Criteria dialog box, in the Specify the value to search for list, select “Windows Defender” for Windows 10 and later. Click OK to

close the Search Criteria dialog box, and then click “Next”.



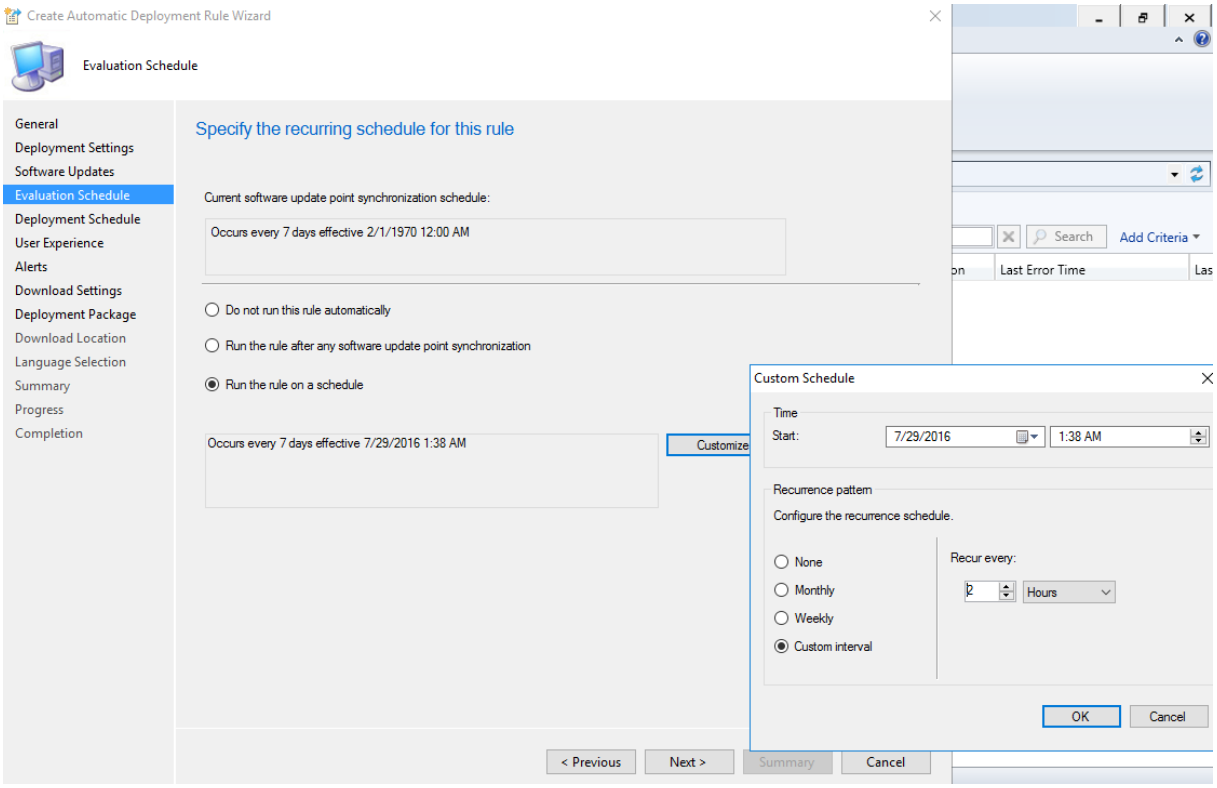
8. In the Property filters list, select the Superseded check box and in the Search criteria list, click <items to find>. Then, in the Search Criteria dialog box, in the Specify the value to search for list, select No. Click OK to close the Search Criteria dialog box, and

then click “Next”.



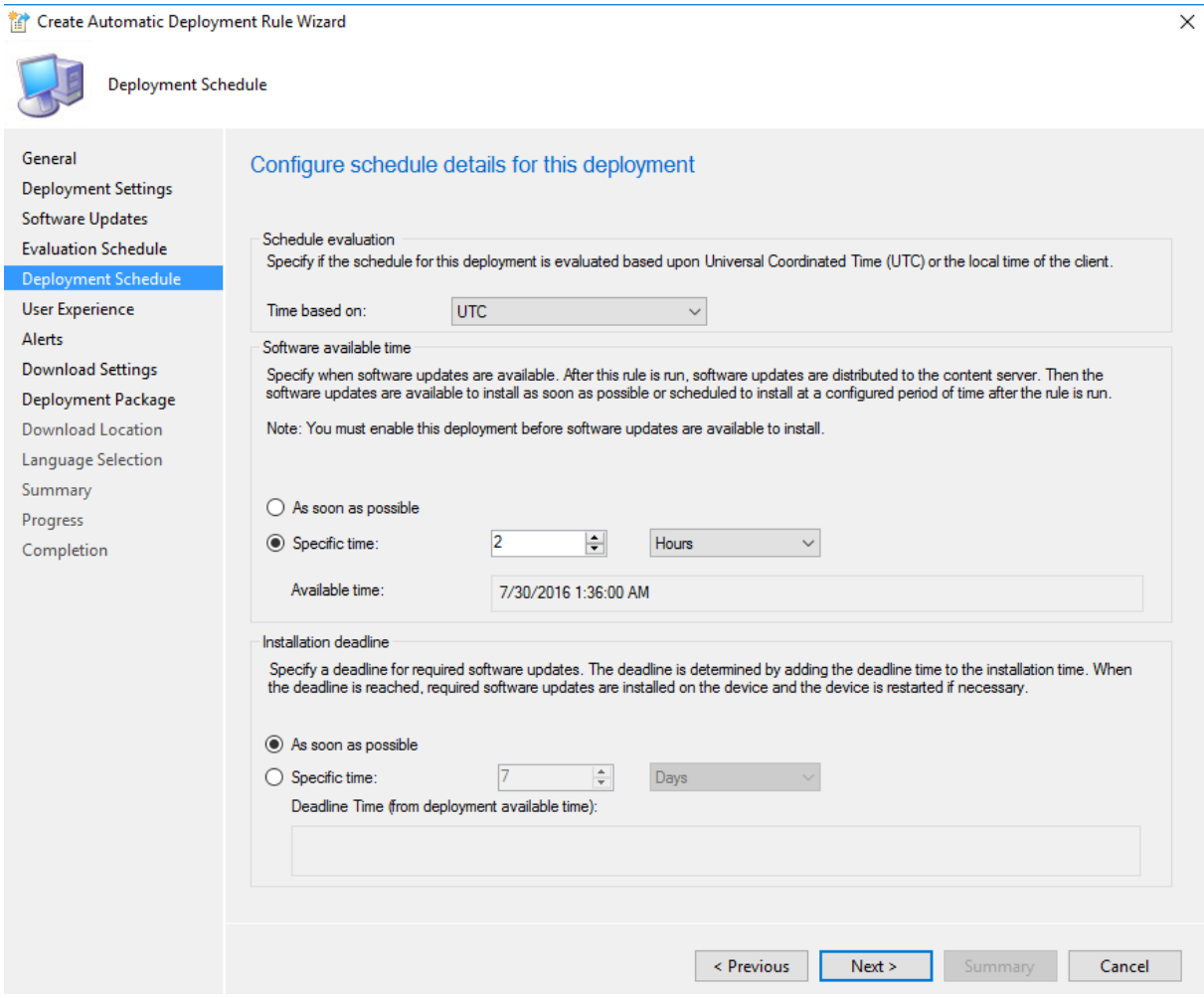
9. On the Evaluation Schedule page of the wizard, select Enable rule to run on a schedule, and then configure the schedule by which to download definition updates. At a minimum, set the rule to run two hours after each software update point

synchronization. Click “Next”.



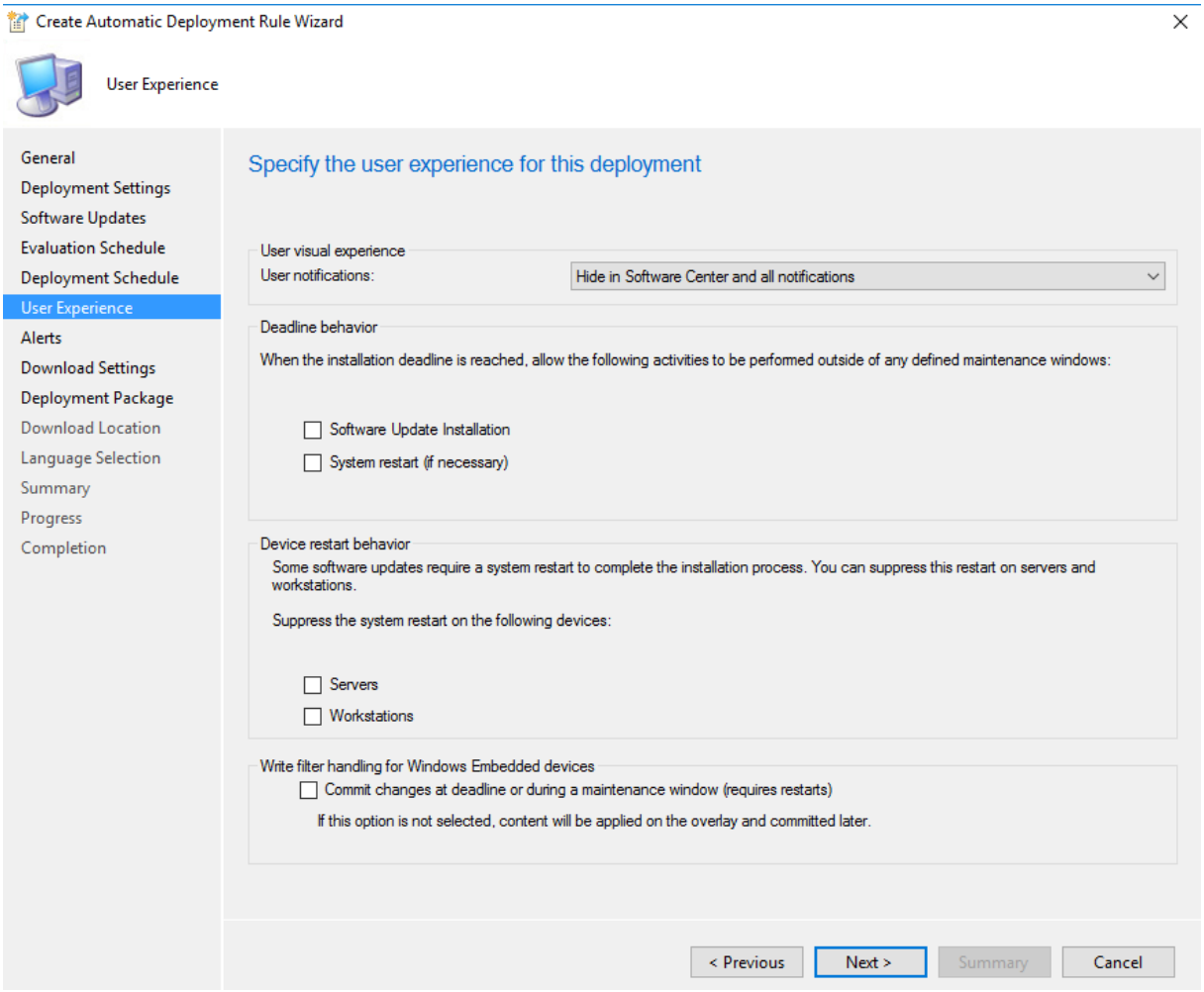
10. On the Deployment Schedule page of the wizard, configure the following settings and then click “Next”:
    a. Time based on: Select UTC if you want all clients in the hierarchy to install the latest definitions at the same time. The actual installation time will vary within a two-hour window. This setting is a recommended best practice.
    b. Software available time: Specify the available time for the deployment that is created by this rule. The specified time must be at least one hour after the automatic deployment rule runs. This helps to ensure that the content has sufficient time to replicate to the distribution points in your hierarchy. Some definition updates might also include antimalware engine updates, which might take longer to reach distribution points.

c. Installation deadline: Select As soon as possible.



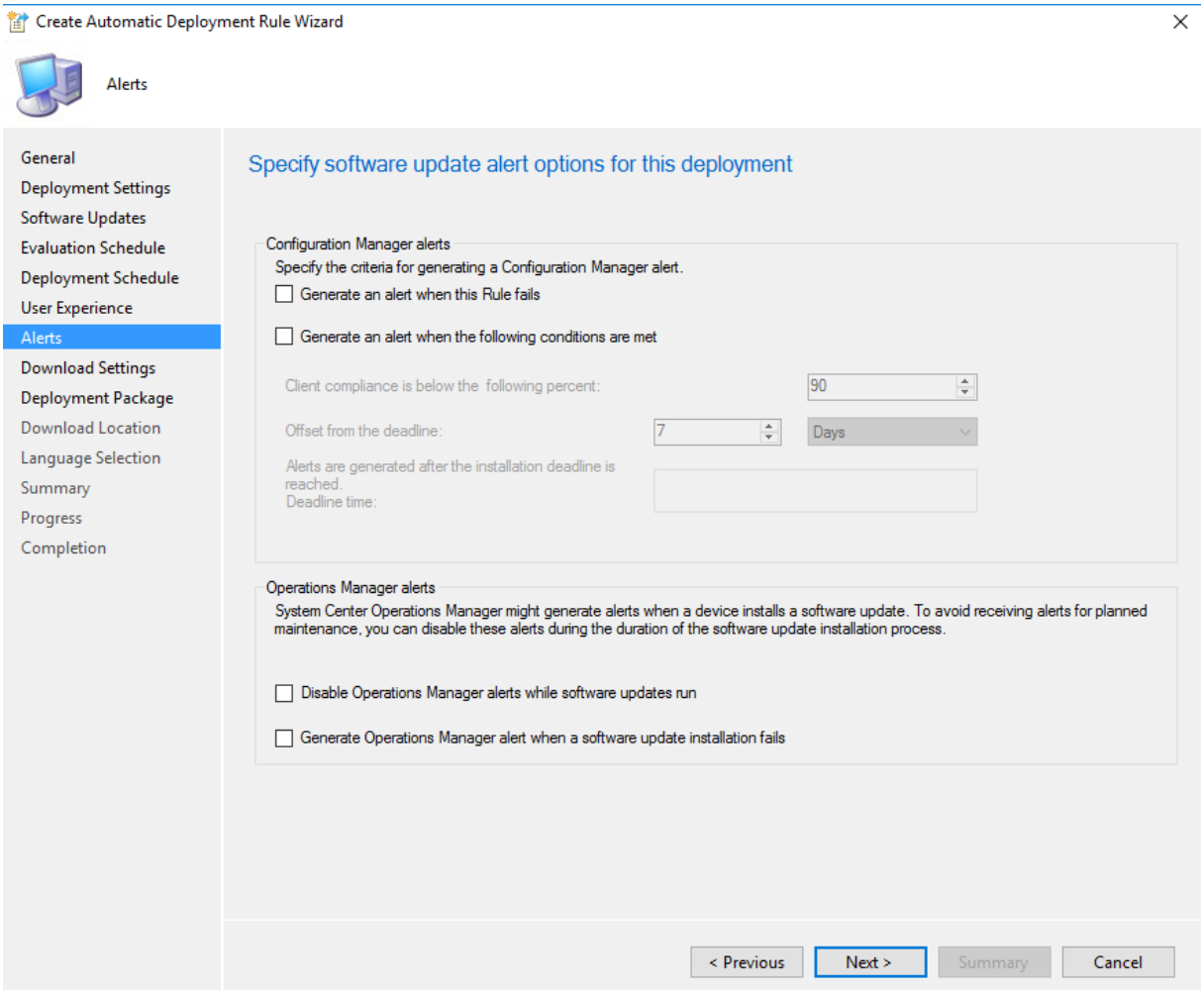
11. On the User Experience page of the wizard, in the User notifications list, select Hide in Software Center and all notifications. This ensures that the definition updates install

silently. Click “Next”.

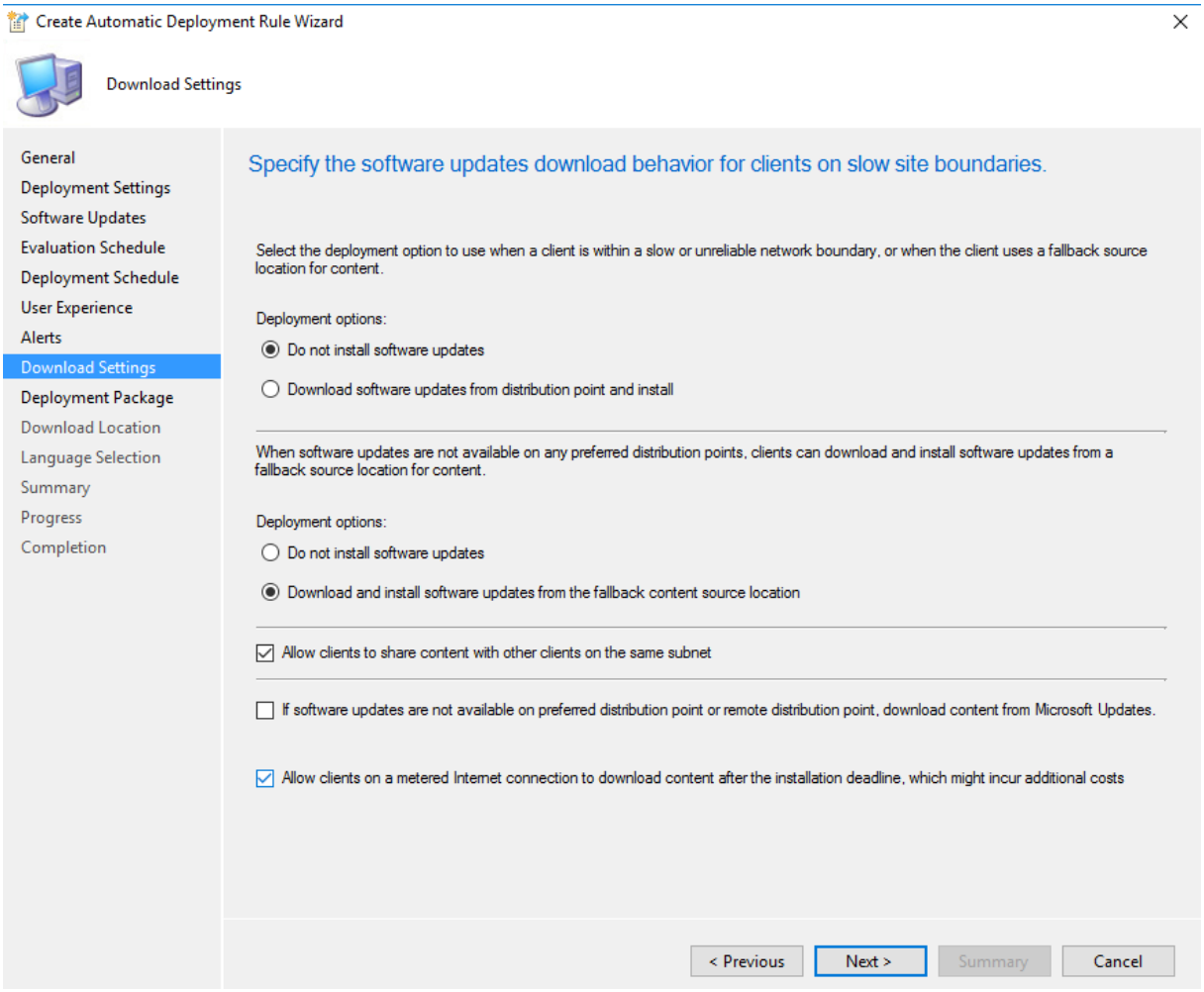


12. On the Alerts page of the wizard, you do not have to configure any alerts. Endpoint Protection in Configuration Manager generates any alerts that might be required.

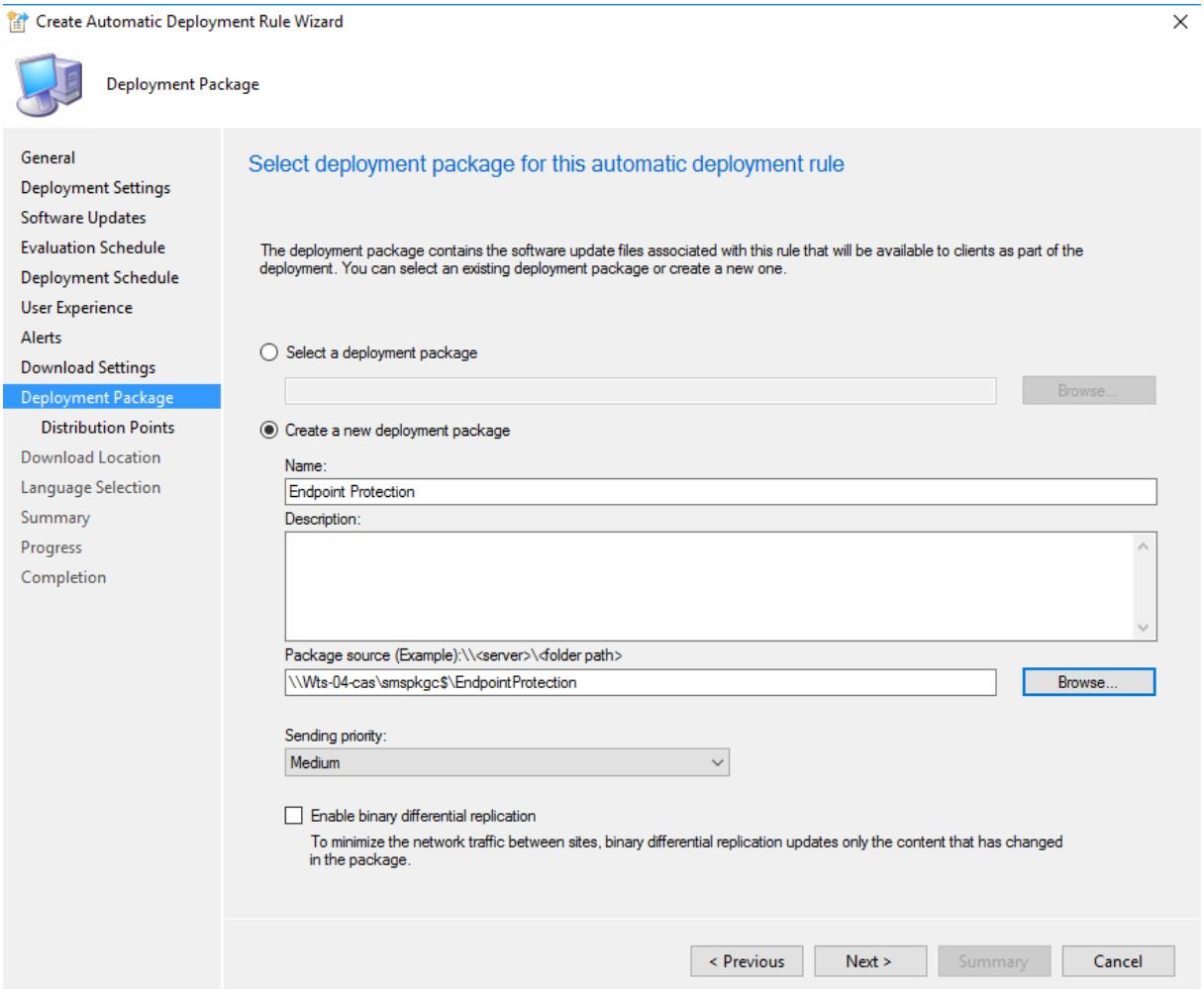
Click “Next”.


Create Automatic Deployment Rule Wizard
Alerts
General
Deployment Settings
Software Updates
Evaluation Schedule
Deployment Schedule
User Experience
Alerts
Download Settings
Deployment Package
Download Location
Language Selection
Summary
Progress
Completion
Specify software update alert options for this deployment
Configuration Manager alerts
Specify the criteria for generating a Configuration Manager alert.
Generate an alert when this Rule fails
Generate an alert when the following conditions are met
Client compliance is below the following percent:
90
Offset from the deadline:
7
Days
Alerts are generated after the installation deadline is reached.
Deadline time:
Operations Manager alerts
System Center Operations Manager might generate alerts when a device installs a software update. To avoid receiving alerts for planned maintenance, you can disable these alerts during the duration of the software update installation process.
Disable Operations Manager alerts while software updates run
Generate Operations Manager alert when a software update installation fails
< Previous
Next >
Summary
Cancel

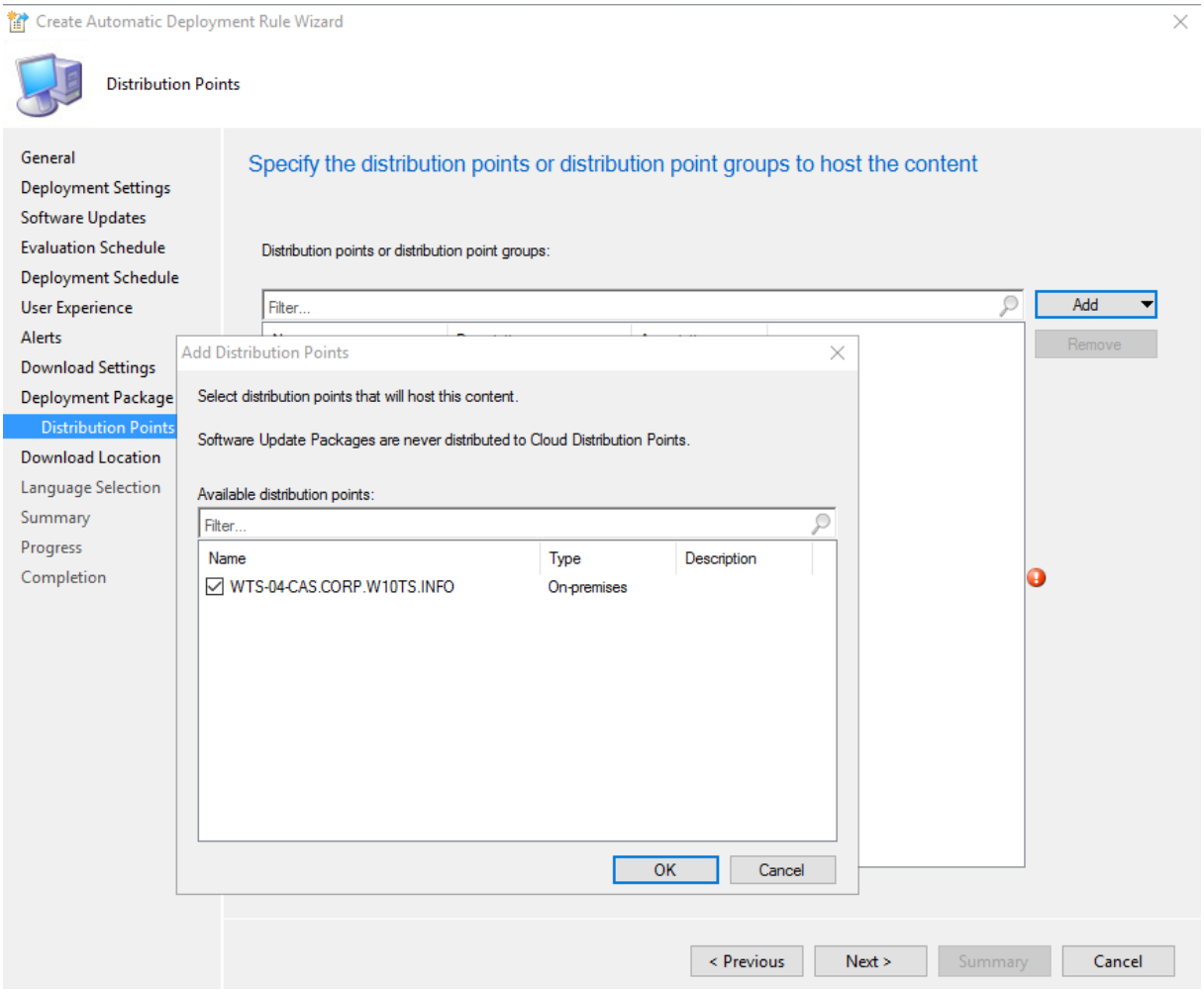
13. On the Download Settings page of the wizard, select the necessary software updates download behavior, and then click “Next”.



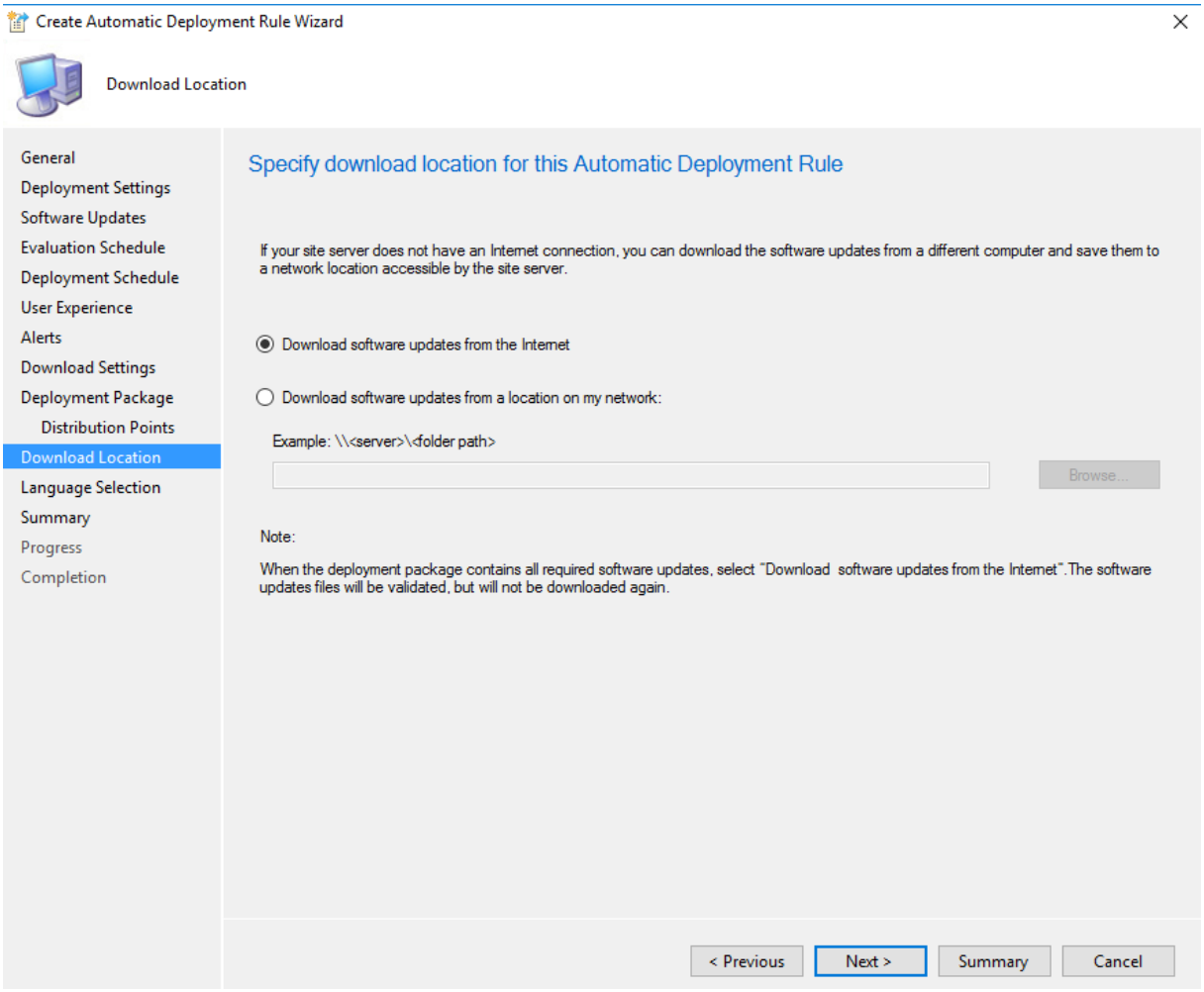
14. On the Deployment Package page of the wizard, create a new deployment package to contain the software update files associated with the rule and click “Next”.



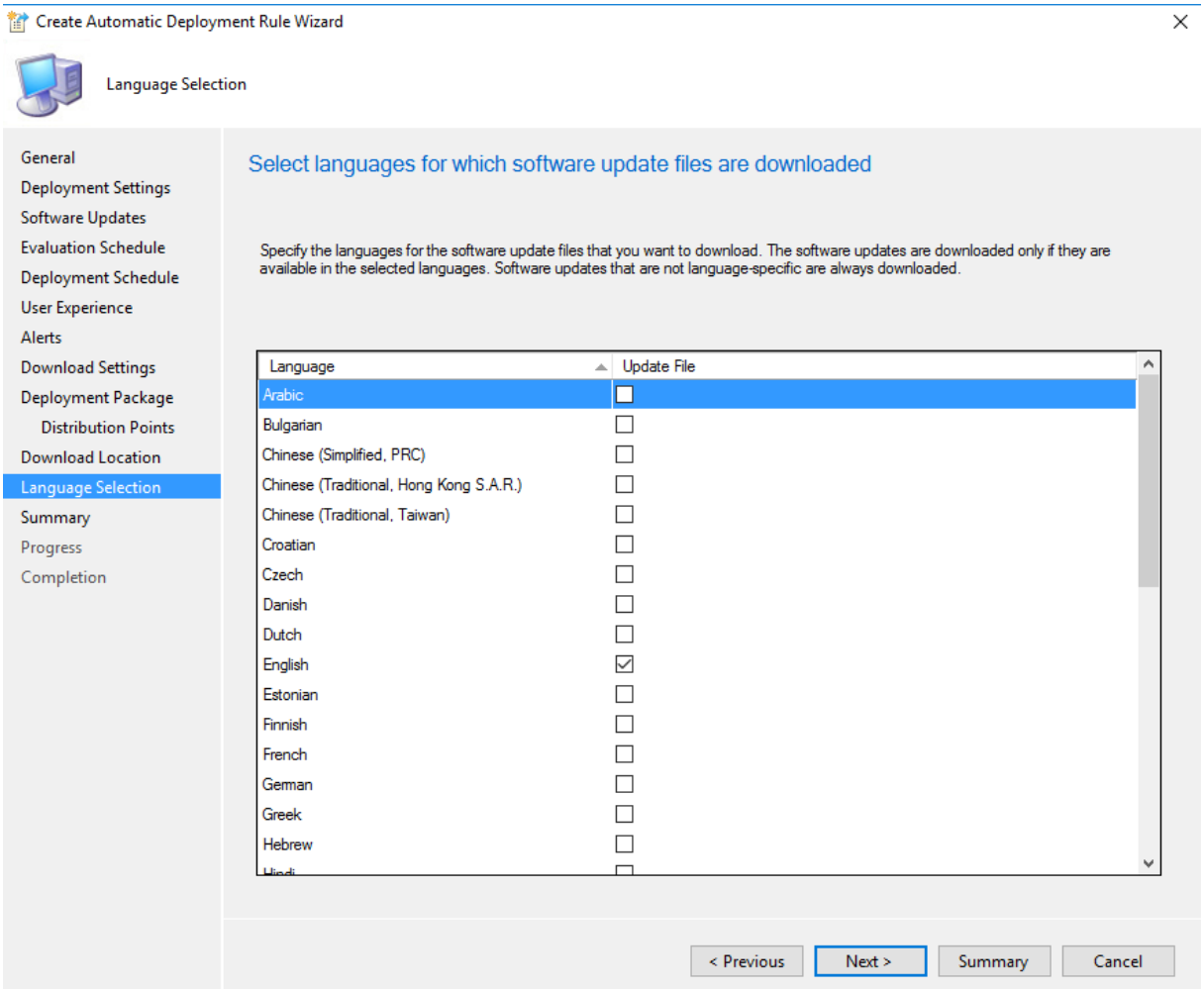
15. On the Distribution Points page of the wizard, select one or more distribution points to which the content for this package will be copied, and then click “Next”.



16. On the Download Location page of the wizard, select Download software updates from the Internet, and then click “Next”.



17. On the Language Selection page of the wizard, select each language version of the updates to be downloaded, and then click “Next”.

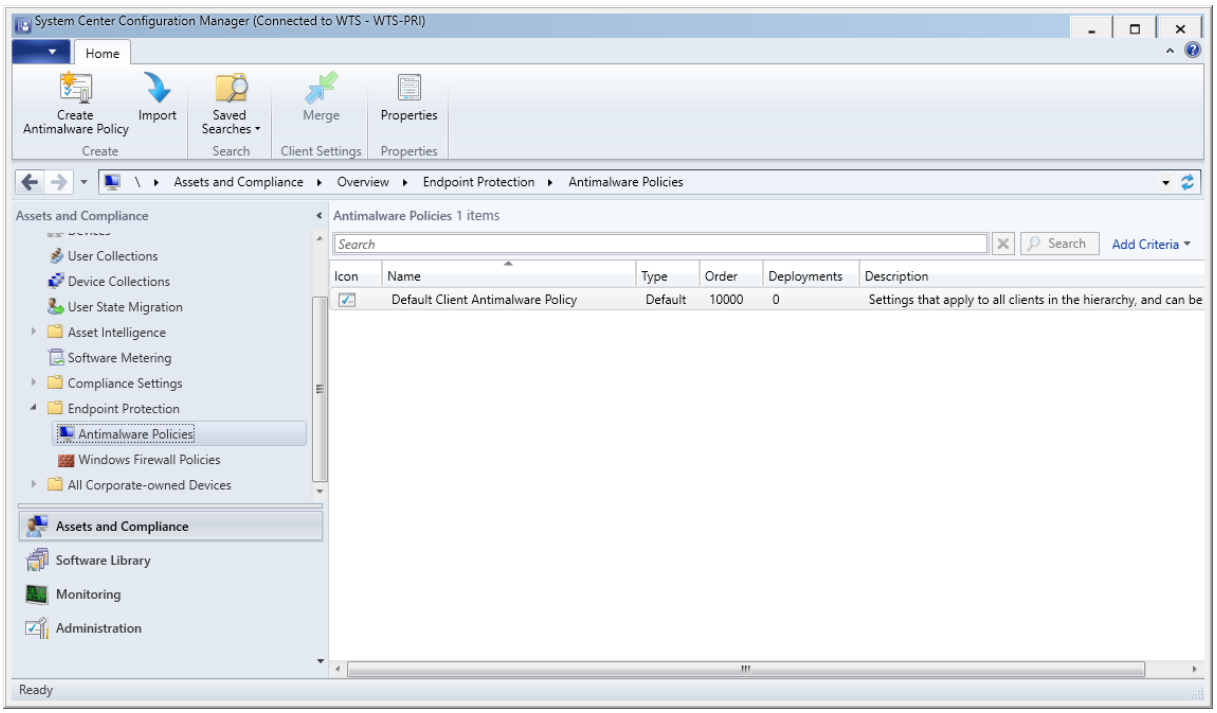


18. Complete the Create Automatic Deployment Rule Wizard.

2.1.4. Create and deploy antimalware policies for Endpoint Protection

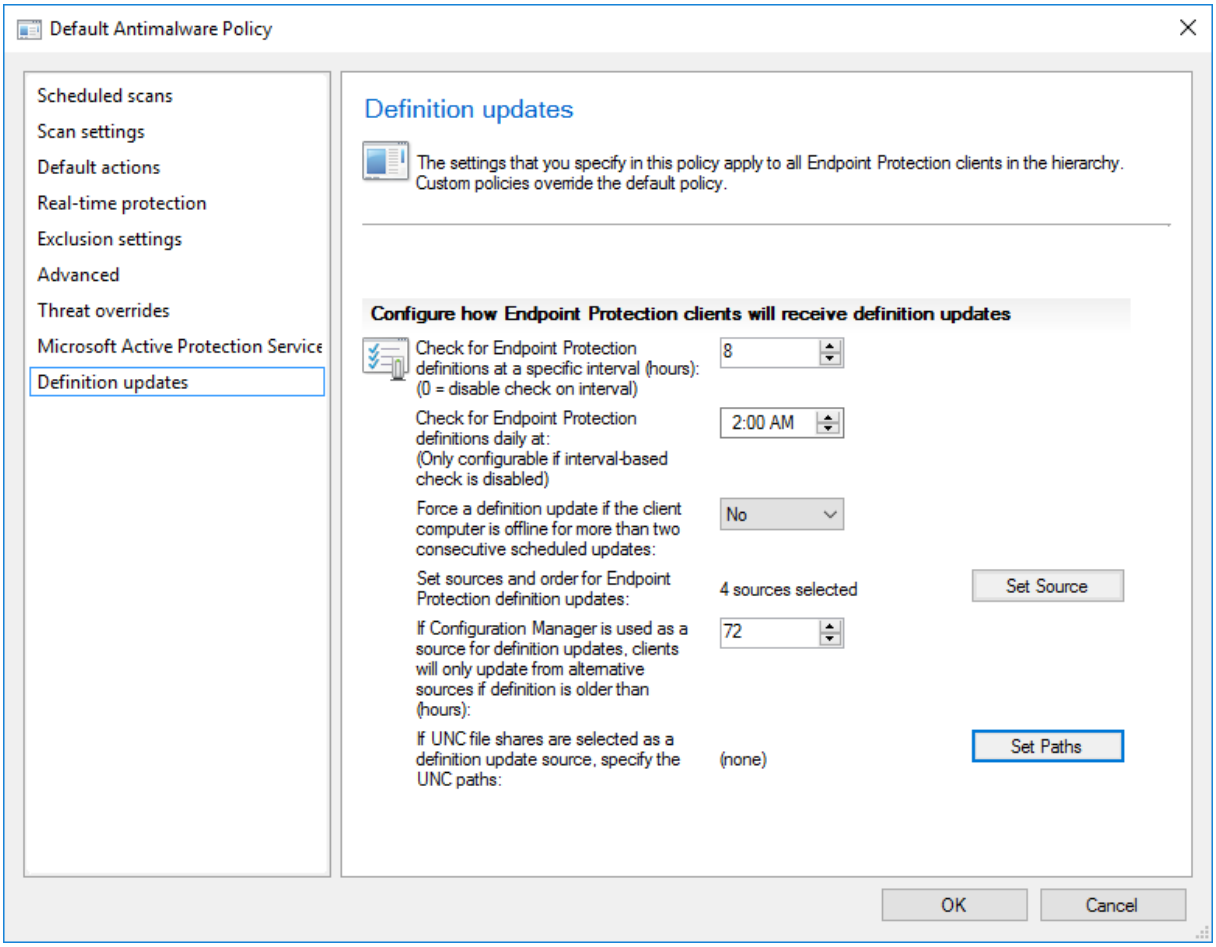
Modify the default antimalware policy

1. Open the "Assets and Compliance" workspace, expand Endpoint Protection, and then click Antimalware Policies.



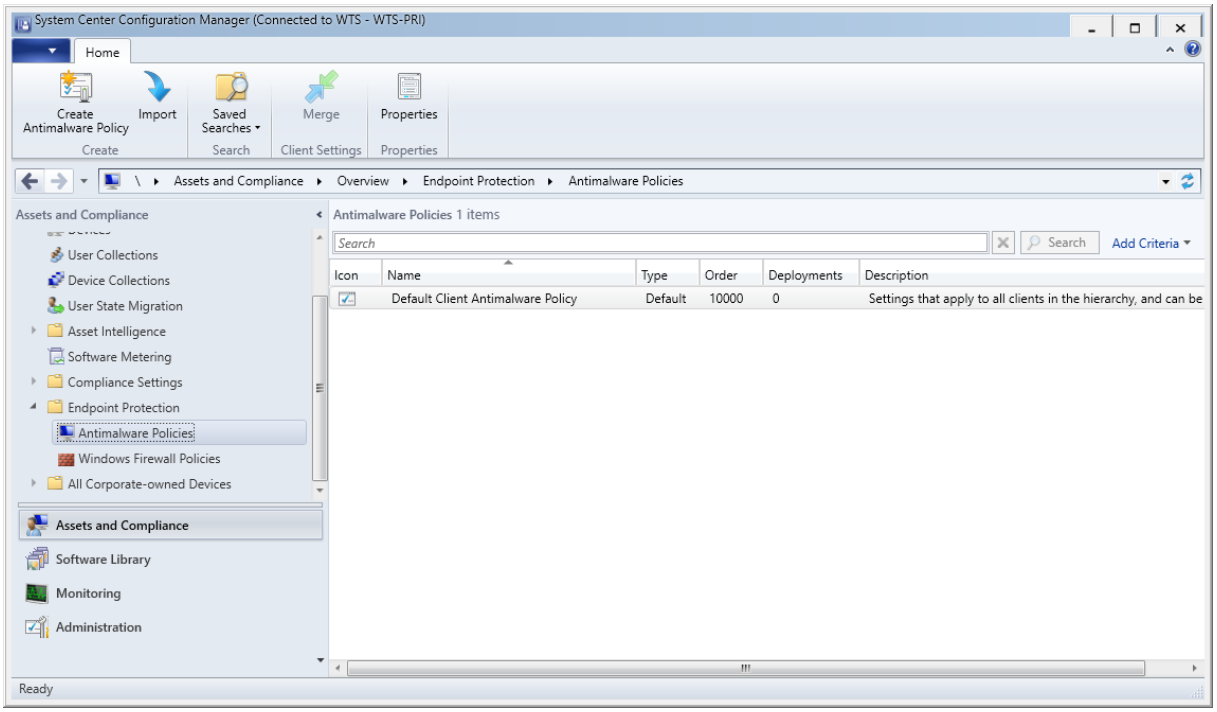
2. Select the antimalware policy Default Client Antimalware Policy and then, on the Home tab, in the Properties group, click Properties.

3. In the Default Antimalware Policy dialog box, configure the settings that you require for this antimalware policy, and then click OK.

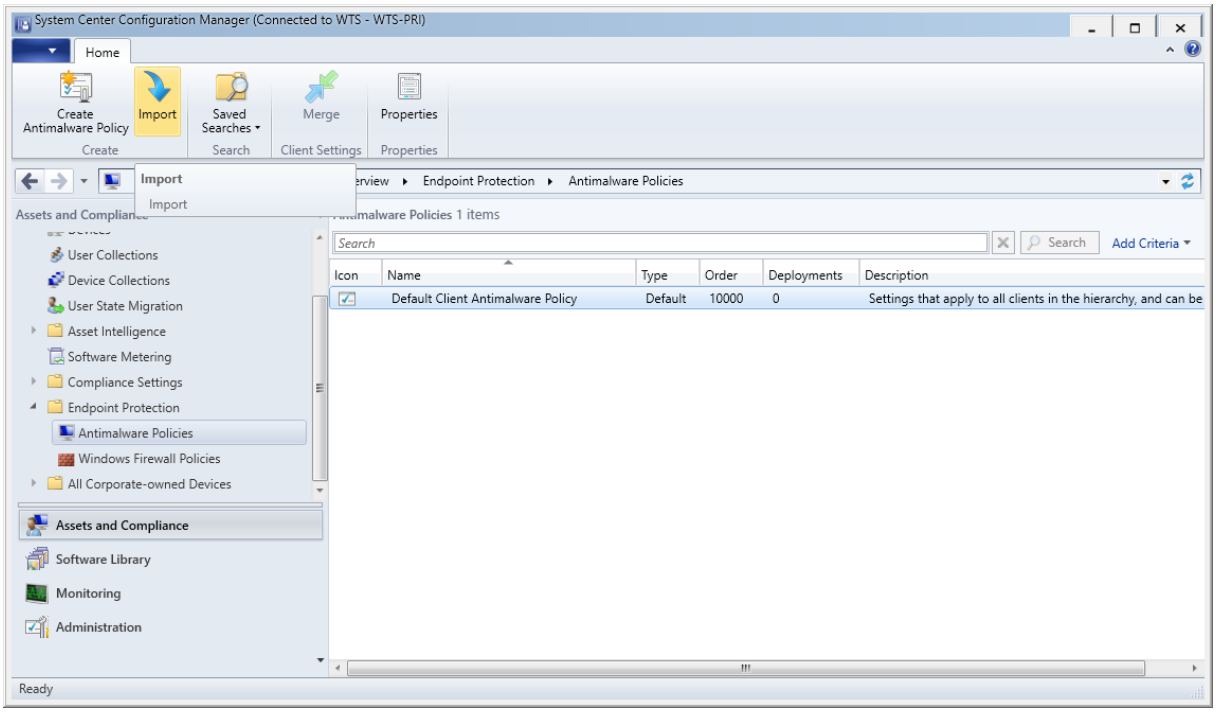


Import an antimalware policy

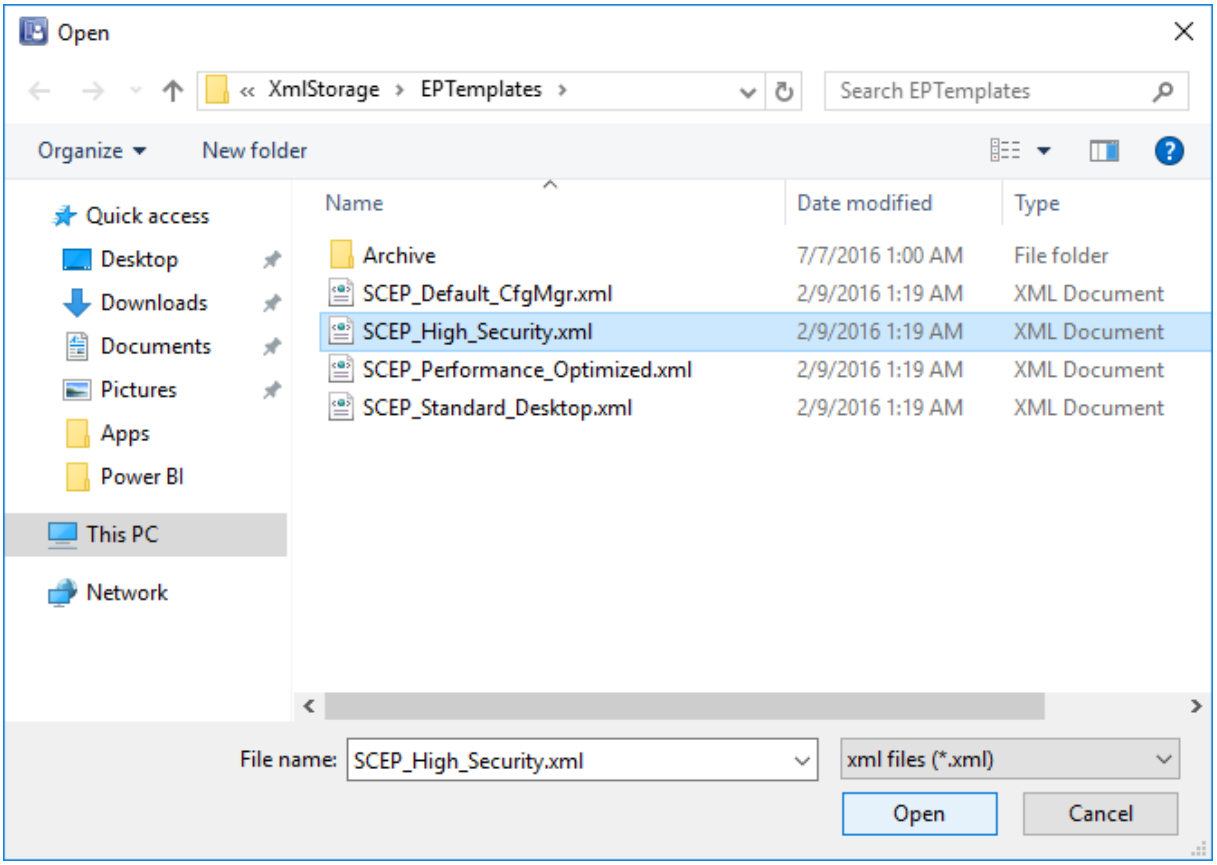
1. In the Configuration Manager console, click Assets and Compliance.



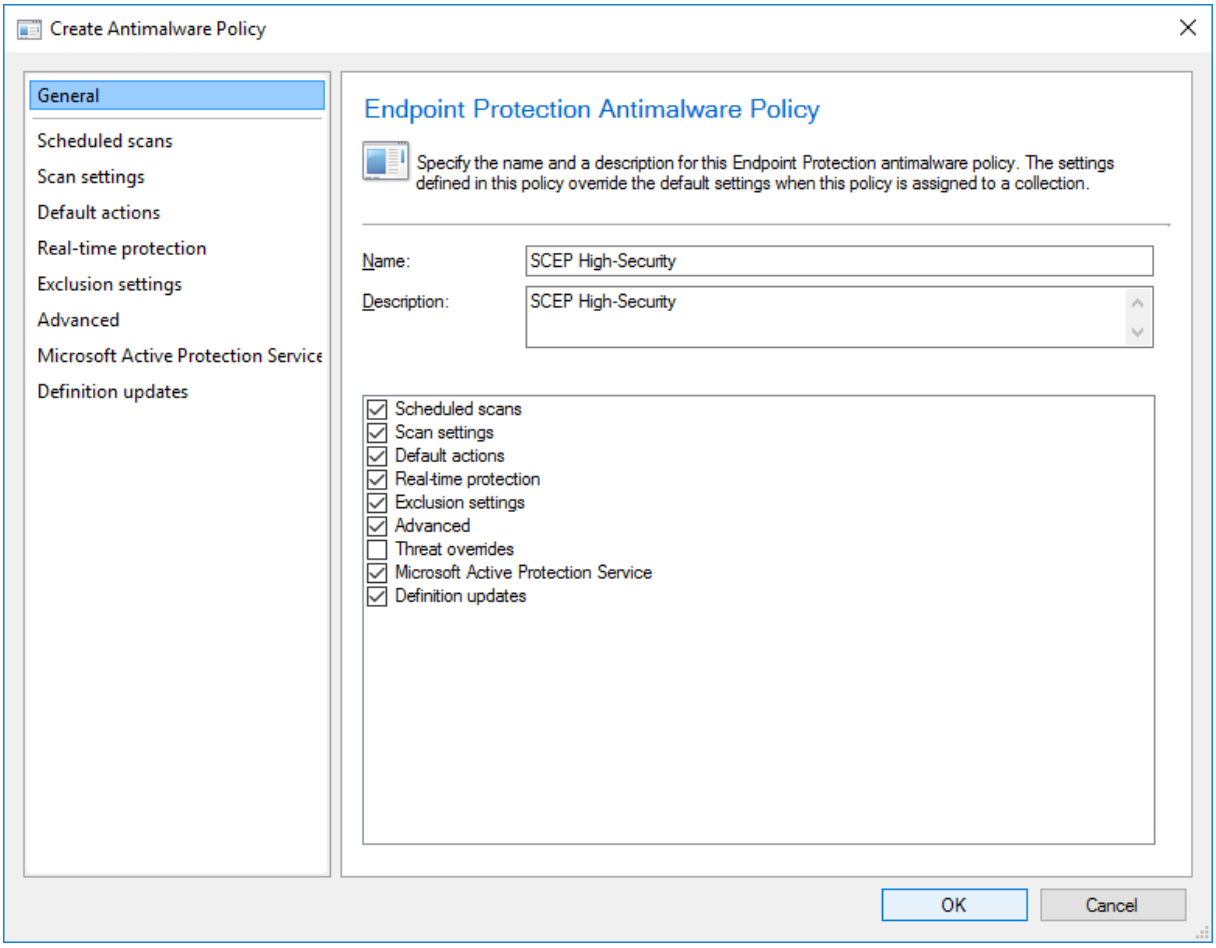
2. In the Assets and Compliance workspace, expand Endpoint Protection, and then click Antimalware Policies.
3. In the Home tab, in the Create group, click Import.



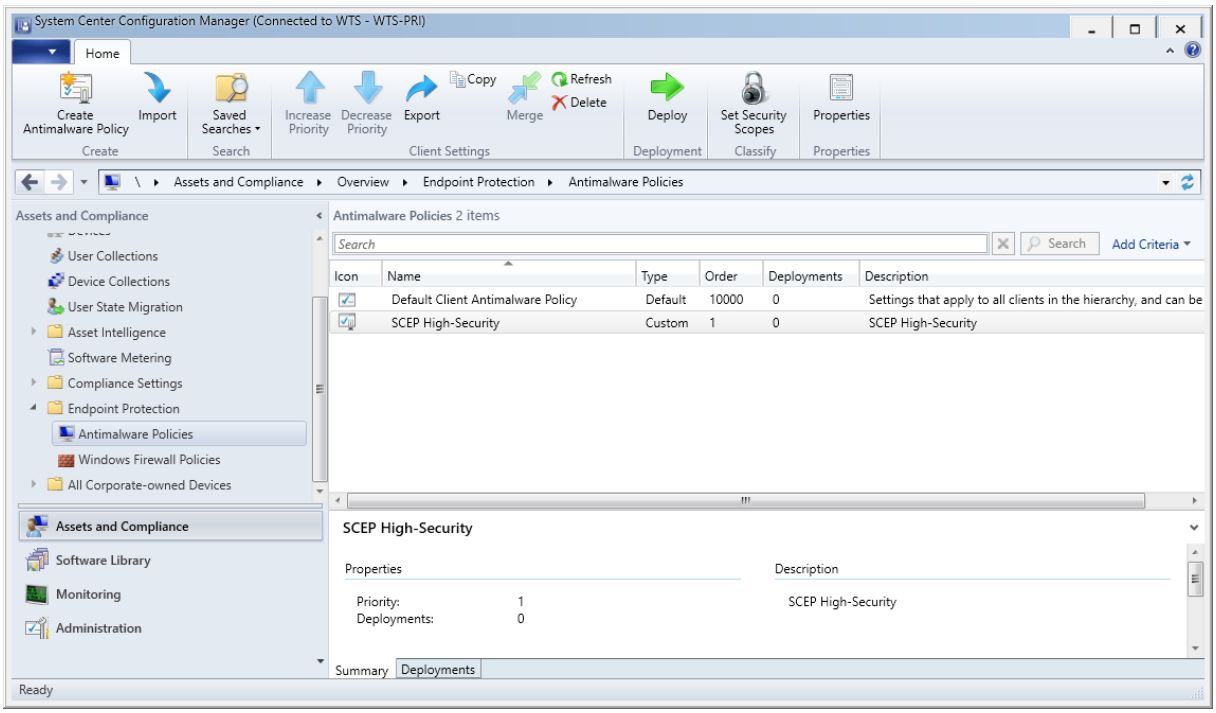
4. In the Open dialog box, browse to the "SCEP_High_Security.xml" policy file to import, and then click Open.



5. In the Create Antimalware Policy dialog box, review the settings to use, and then click OK.

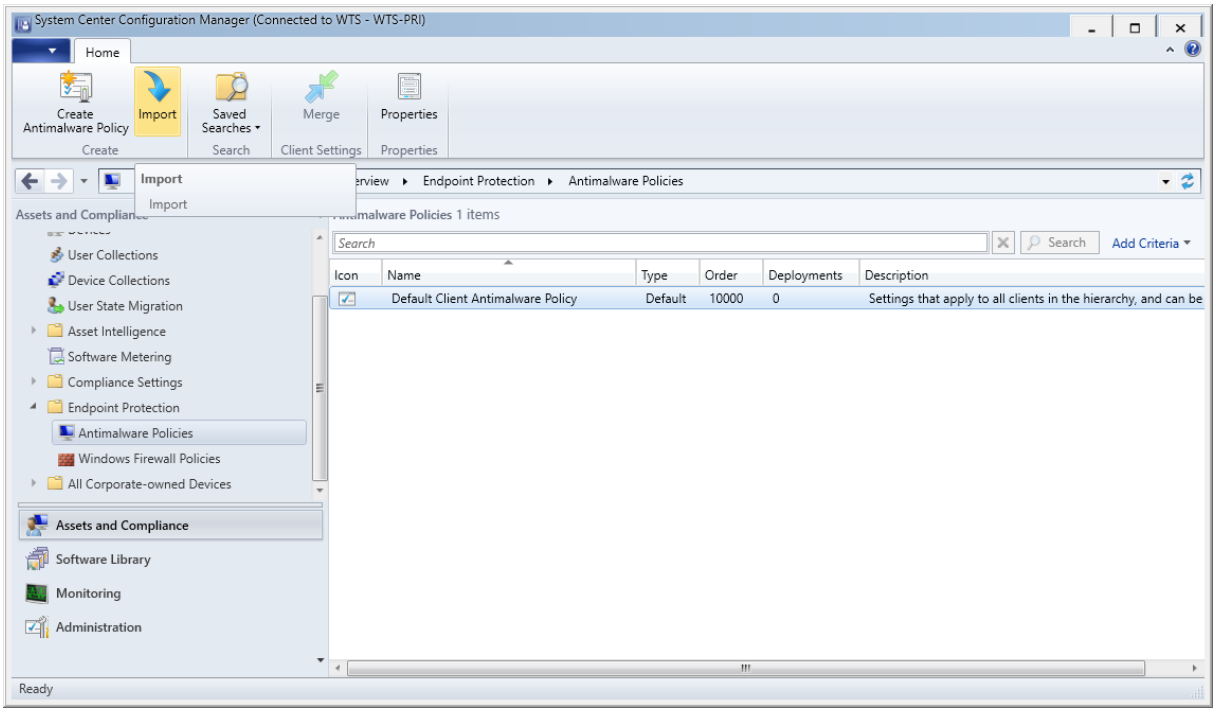


6. Verify that the new antimalware policy is displayed in the Antimalware Policies list.

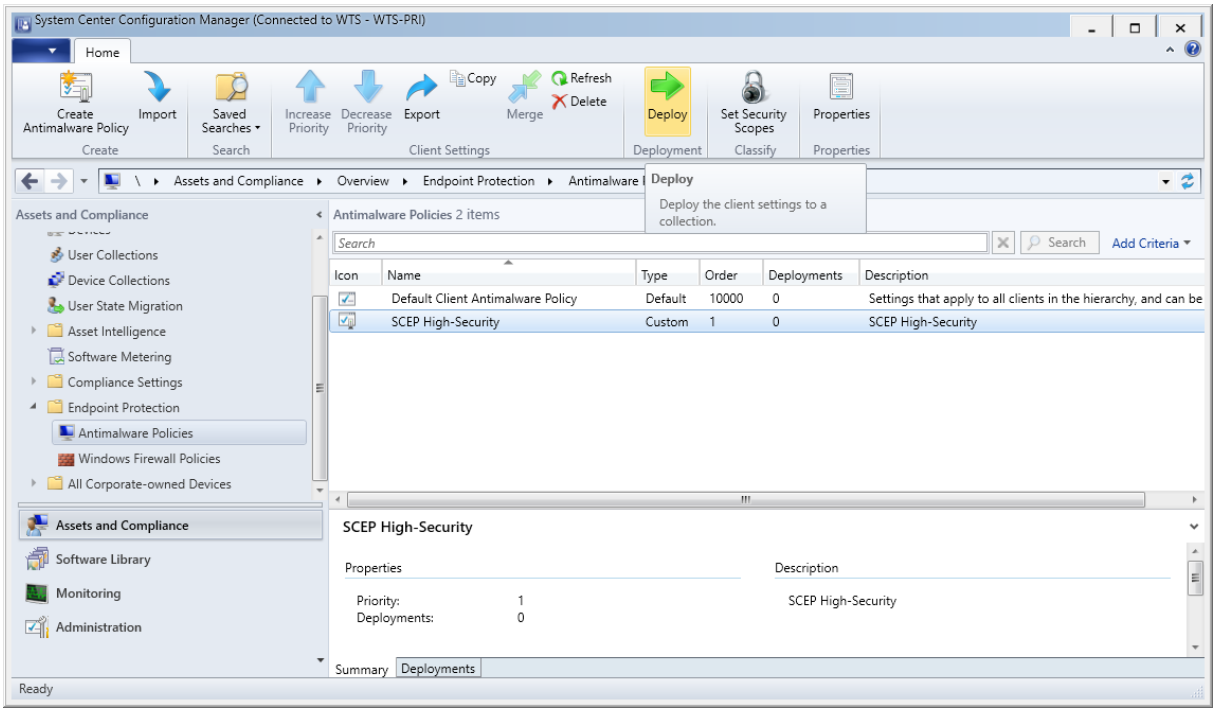


Deploy an antimalware policy to client computers

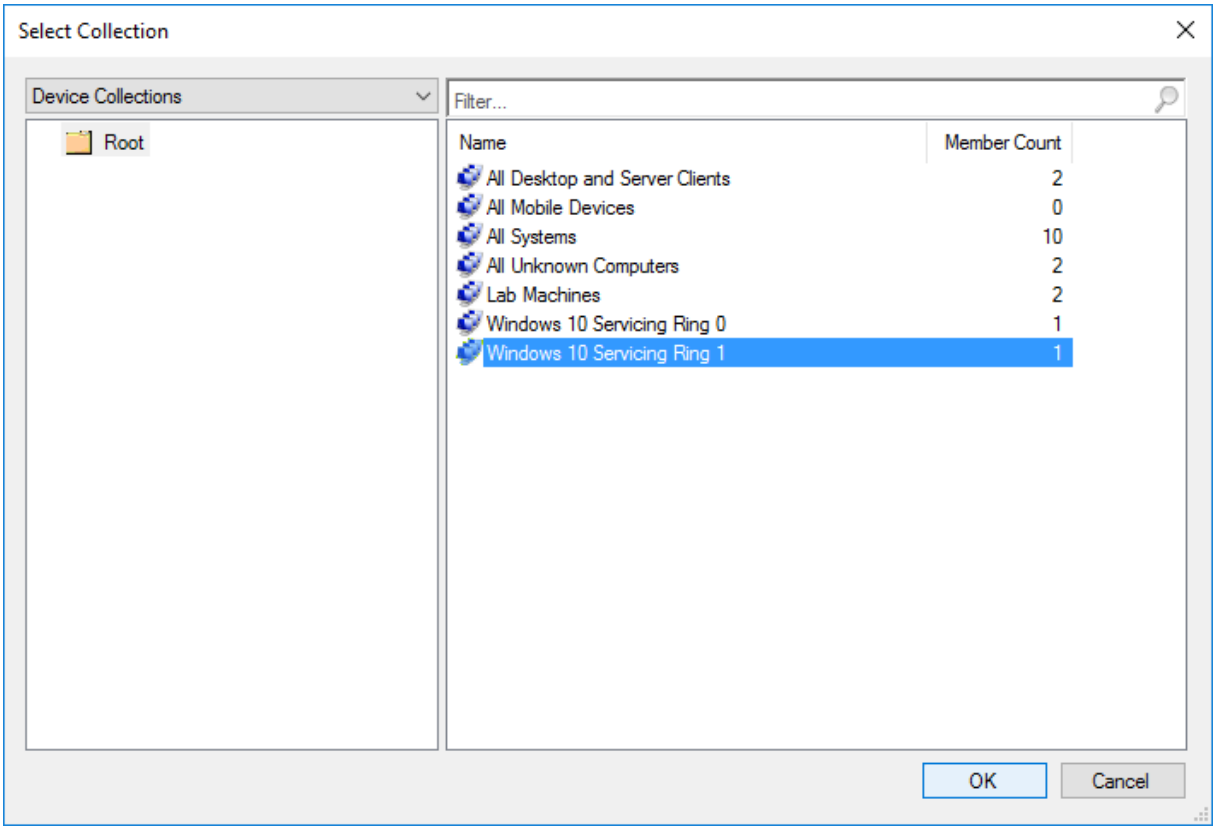
1. In the Configuration Manager console, click Assets and Compliance.
2. In the Assets and Compliance workspace, expand Endpoint Protection, and then click Antimalware Policies.



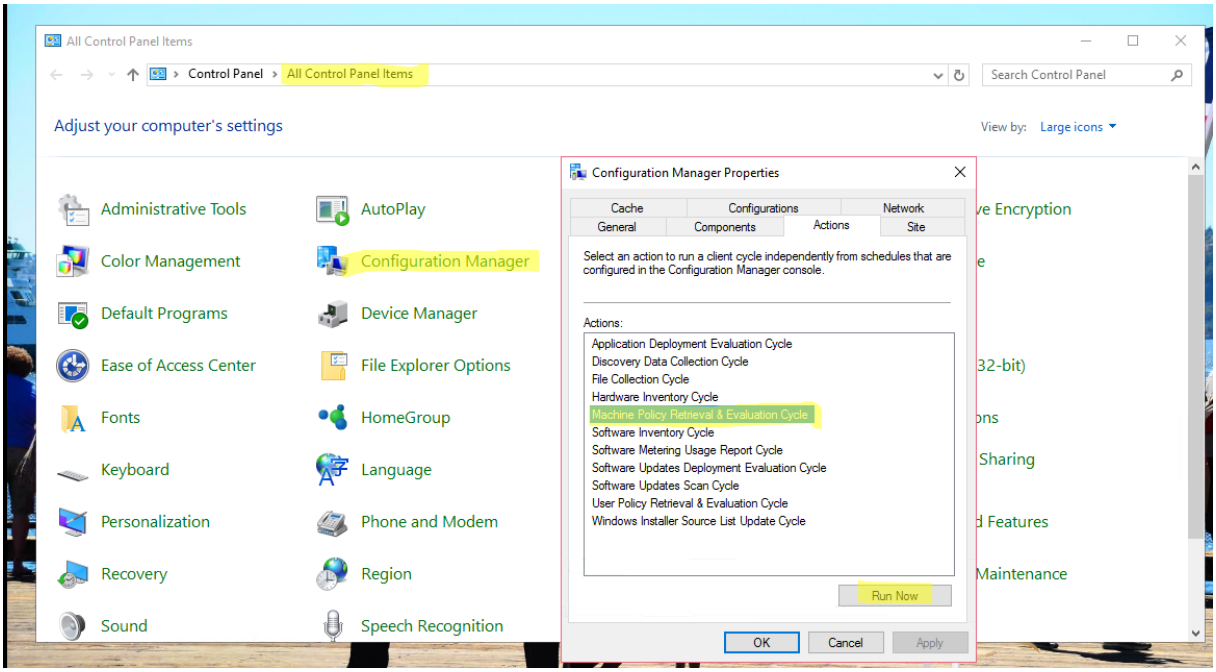
3. In the Antimalware Policies list, select the *"SCEP High-Security"* antimalware policy to deploy. Then, on the Home tab, in the Deployment group, click Deploy.



4. In the Select Collection dialog box, select the “Windows 10 Servicing Ring 1” device collection to deploy the antimalware policy, and then click OK.

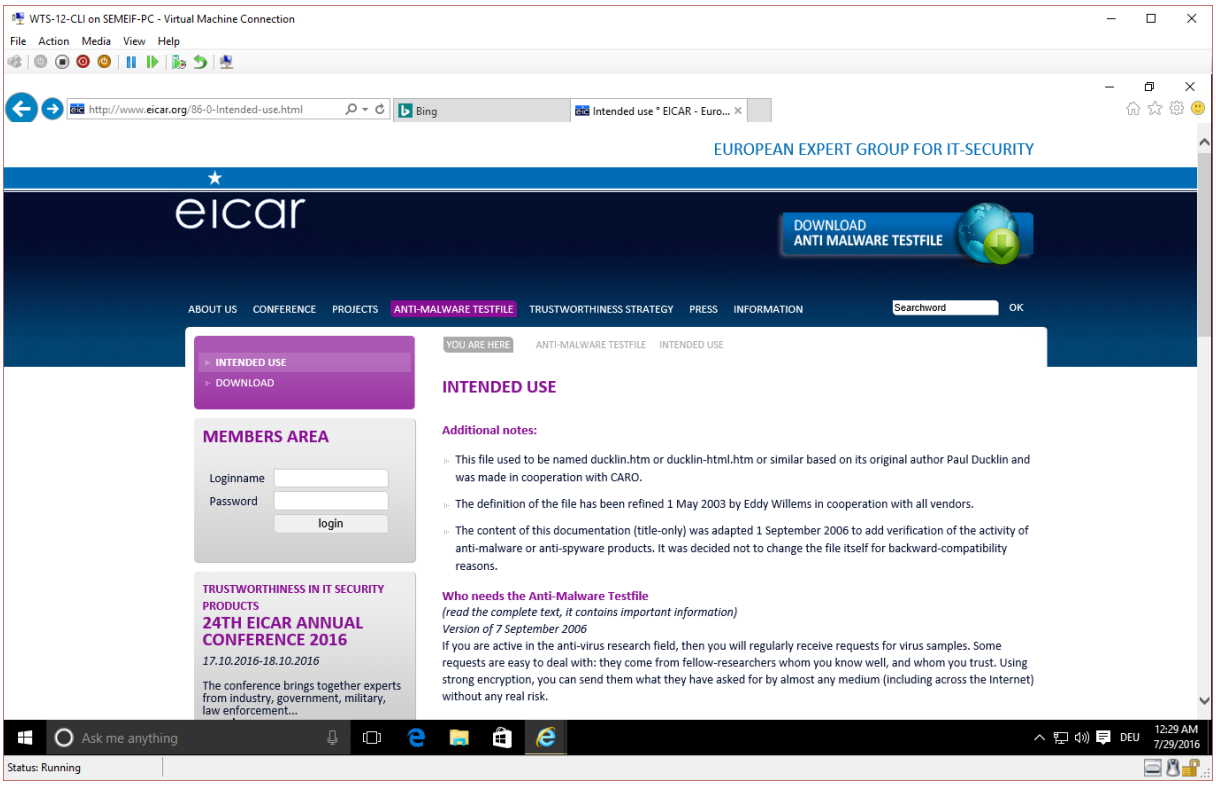


5. Log on as corp\admin to the WTS-10-CLI and run the Machine Policy Retrieval & Evaluation Cycle in the Configuration Manager Properties on the Actions tab.

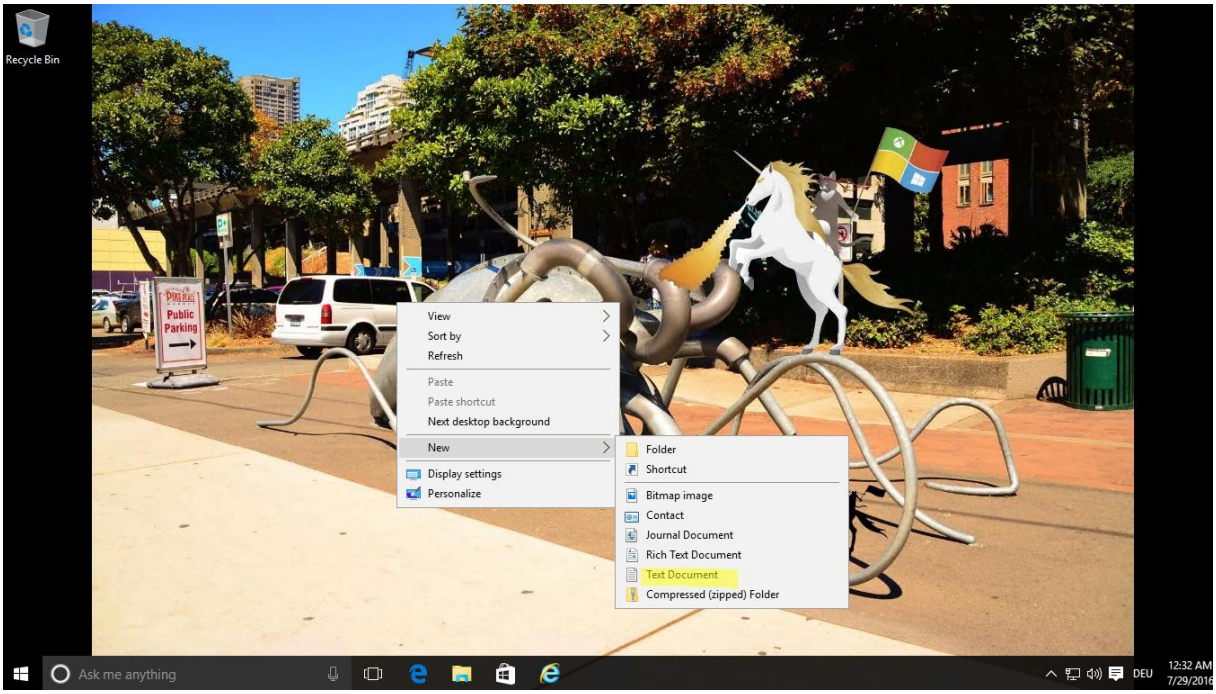


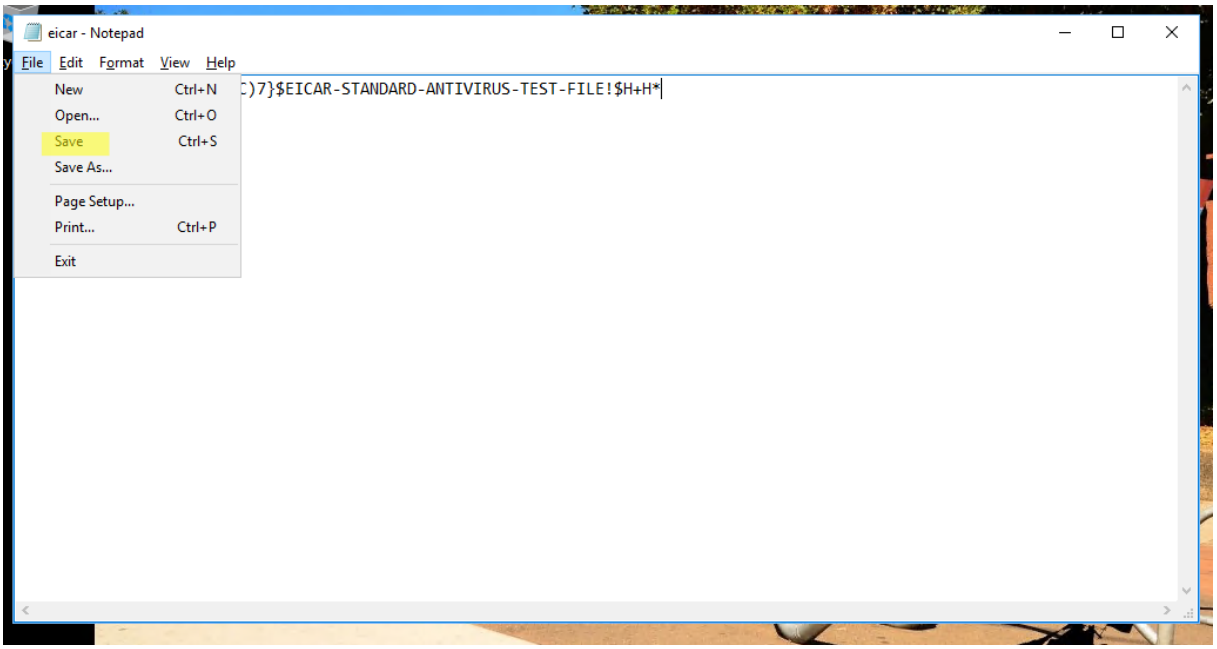
Let's have some fun and bring some Malware on a client machine.

1. Log on as corp\admin to the WTS-10-CLI and open http://www.eicar.org in Internet Explorer.

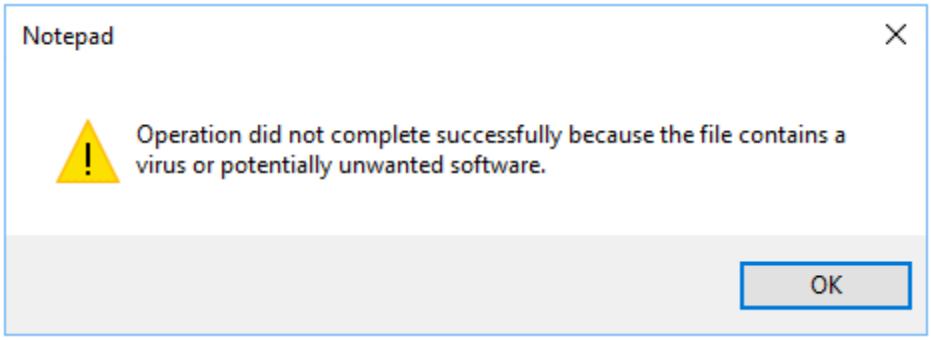


2. Scroll down to until you see the eicar Test String which starts with "X5O!P%@AP[4\".
3. Copy the string into your clipboard, create a text document on the desktop, paste the string into the file and try to save it.

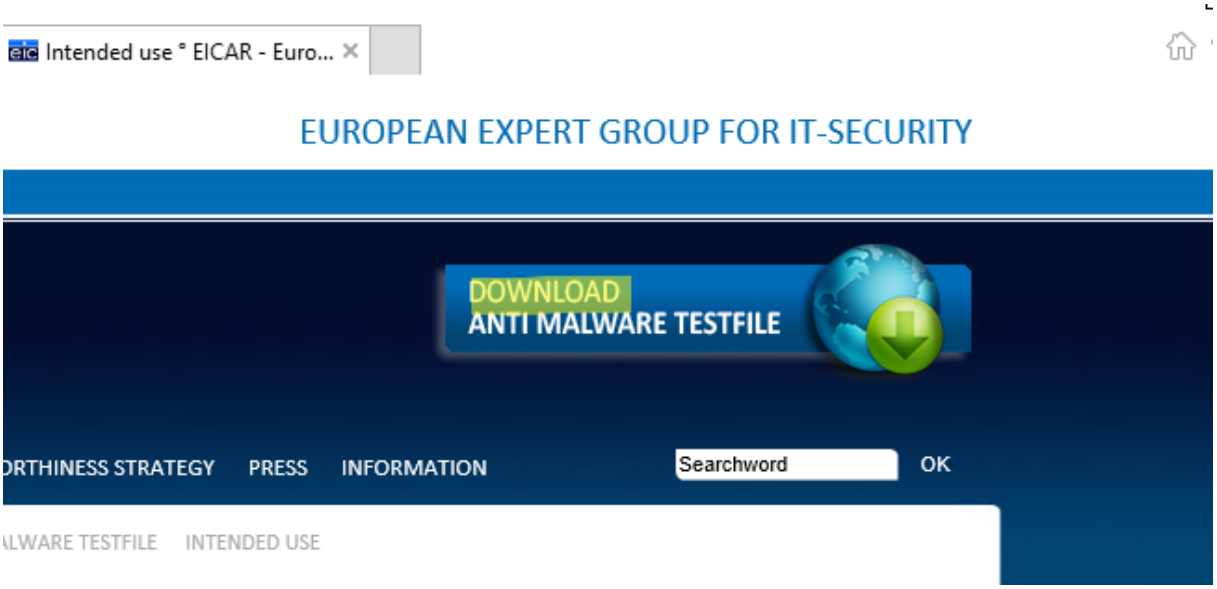


4. 

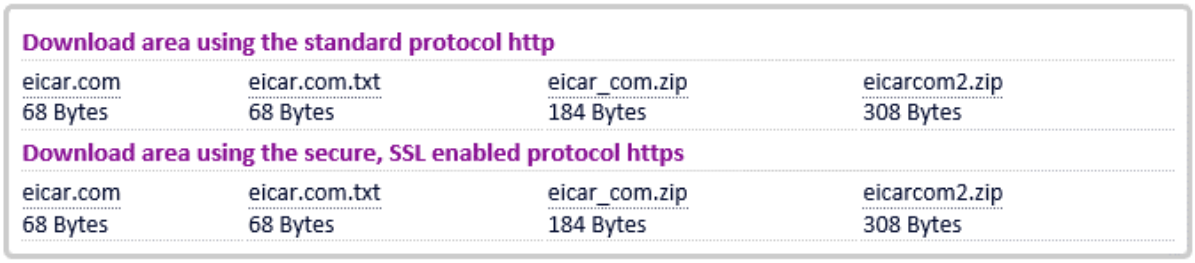
5. In the warning dialog click “OK” and then “cancel” in the Save dialog.



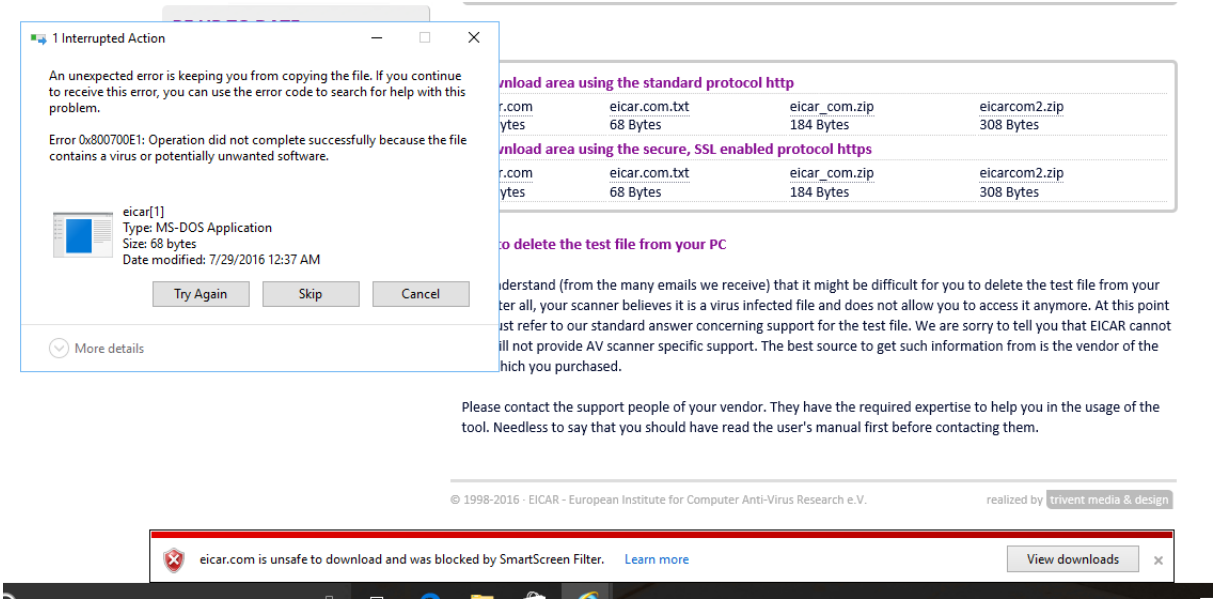
6. Go back to the eicar.org webpage and click on “Download anti Malware Testfile”.



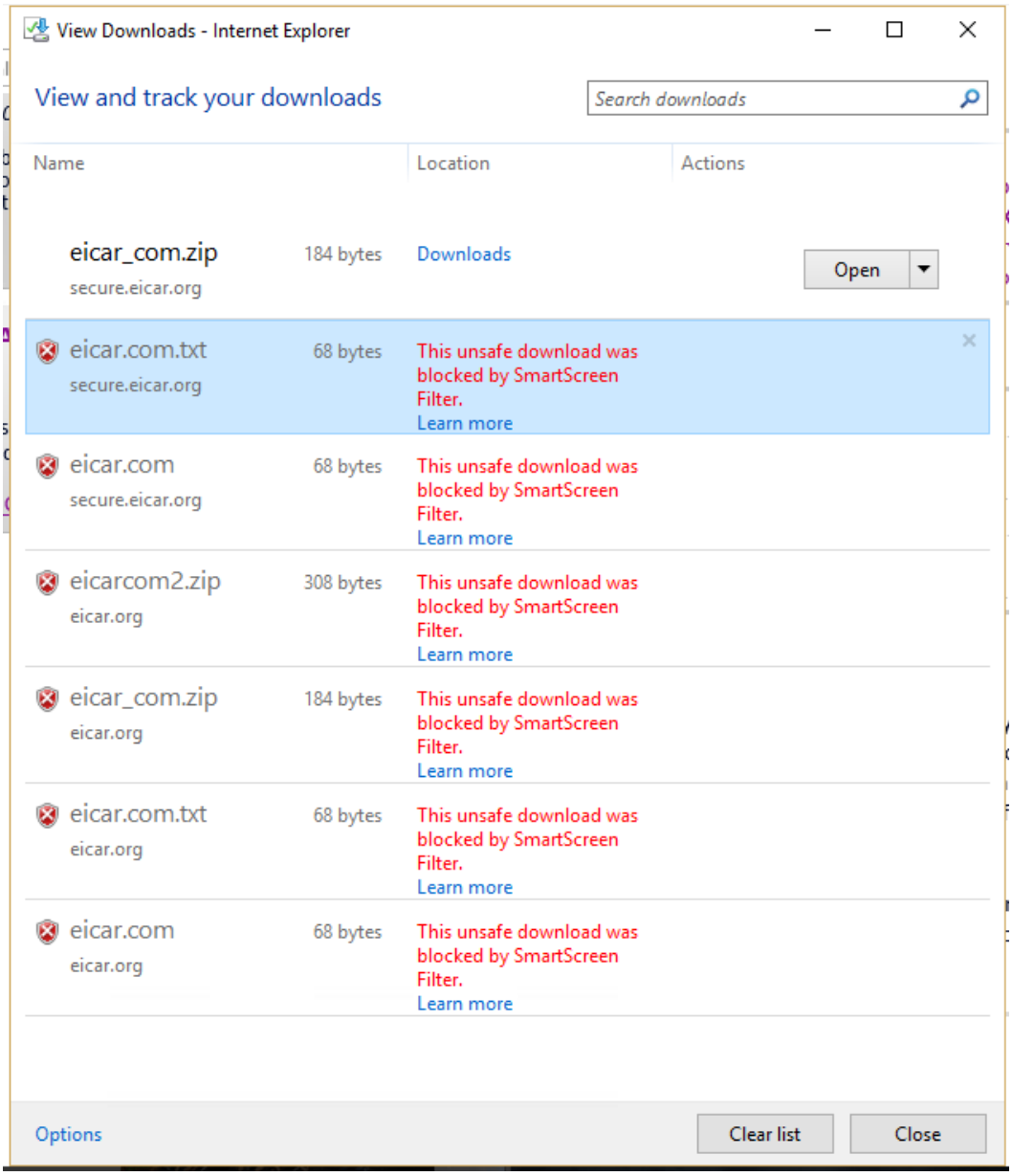
7. In the download area try to download all testfiles.



8. There will be several warnings like this.



9. At the and all downloads will fail.

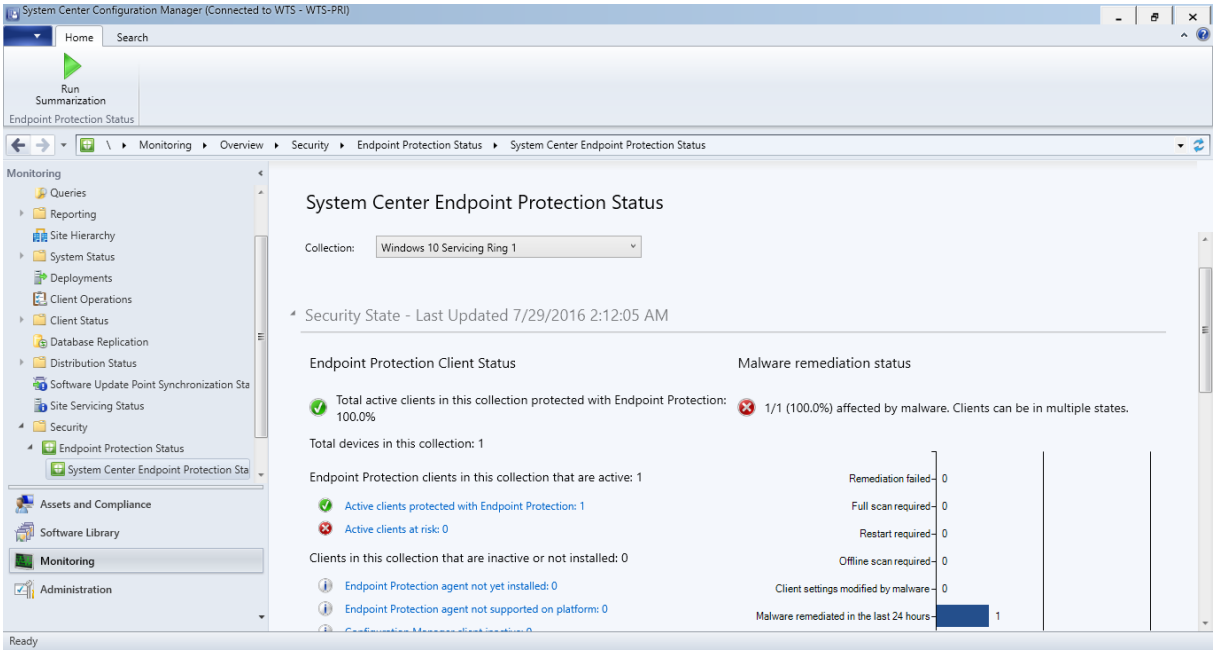


2.1.5. Monitor Endpoint Protection

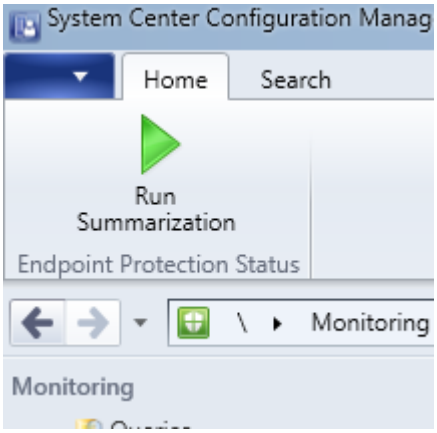
Monitor Endpoint Protection by Using the Endpoint Protection Status Node

1. In the Configuration Manager console, click Monitoring.
2. In the Monitoring workspace, expand “Security” and click Endpoint Protection Status.

3. In the Collection list, select the collection for which you want to view status information.



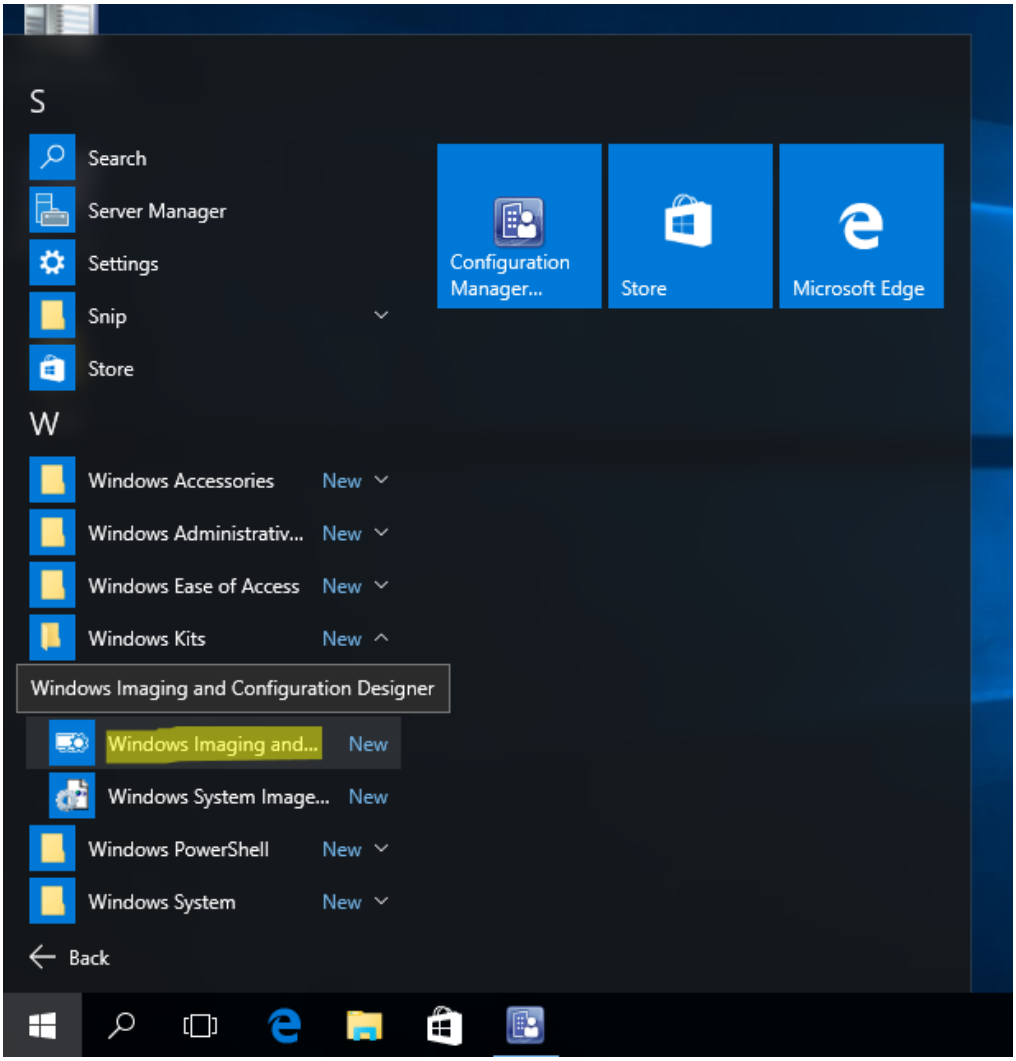
4. Review Status. If the status is empty, click on “Run Summarization”.



3. Lab guide part 3 – Security through Provisioning

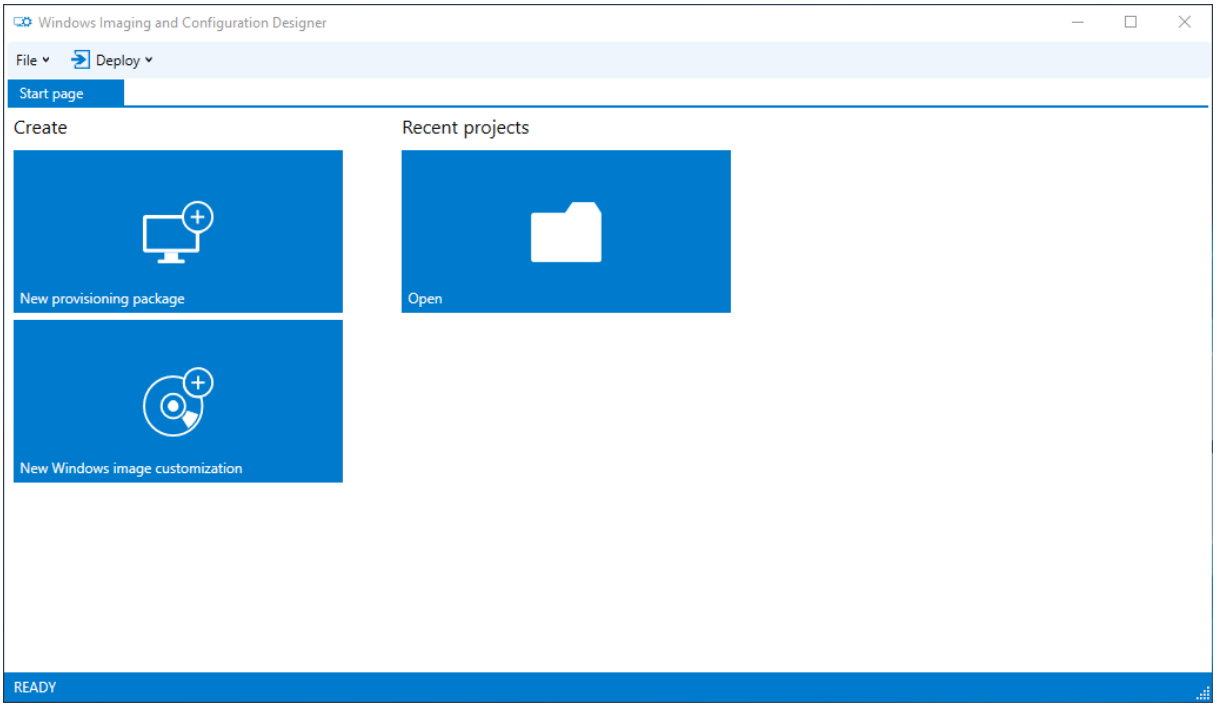
3.1. Create Provisioning Package with ICD (Time: 10:00)

1. On the WTS-04-CAS machine open the "Windows Imaging and Configuration Designer" (ICD). This is located in the "Windows Kits" section of the start menu.

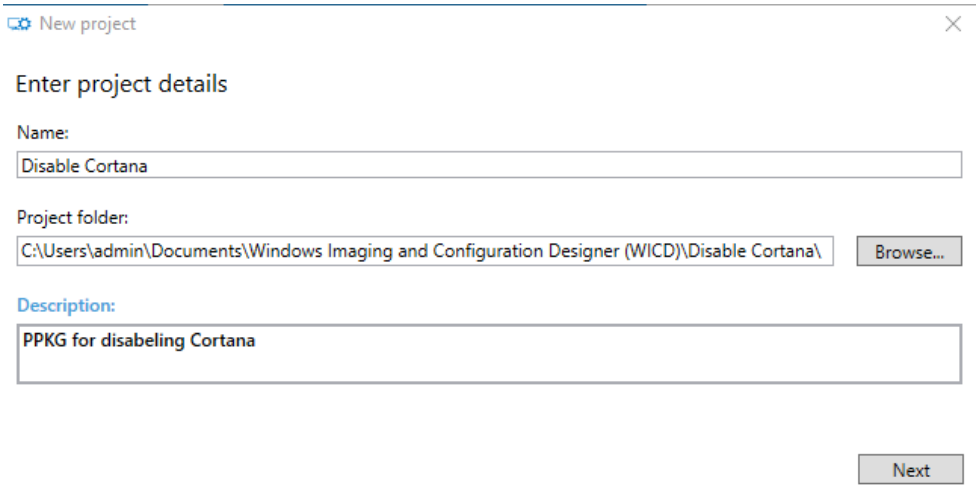


2. Click "Yes" on the UAC prompt.

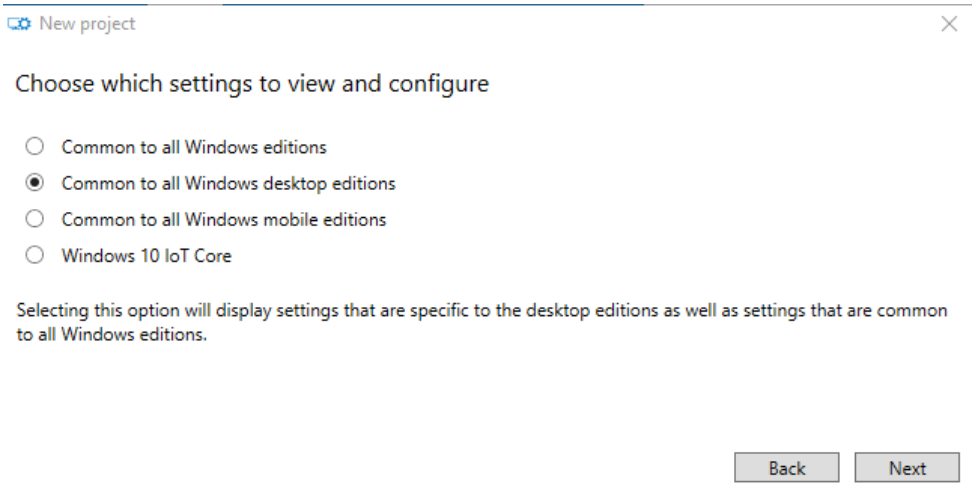
3. In the ICD click on “New provisioning package”.



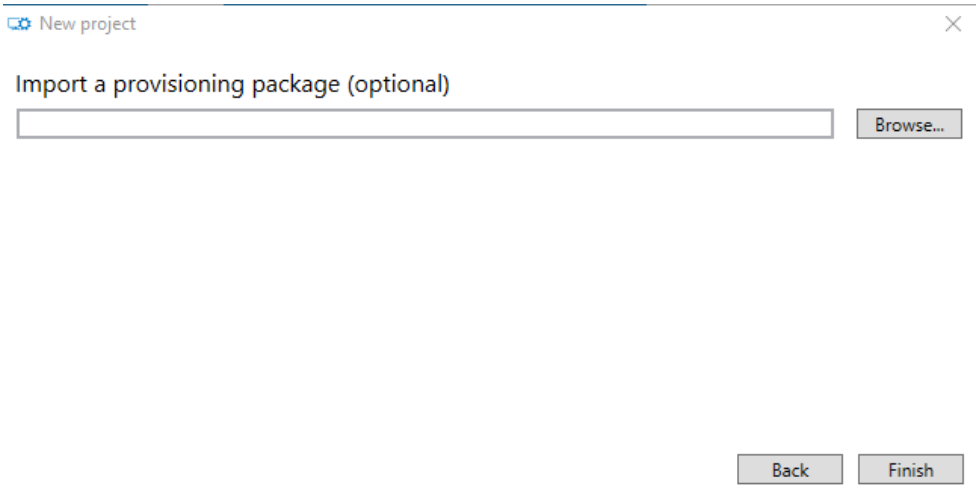
4. Enter the project details and click “Next”.



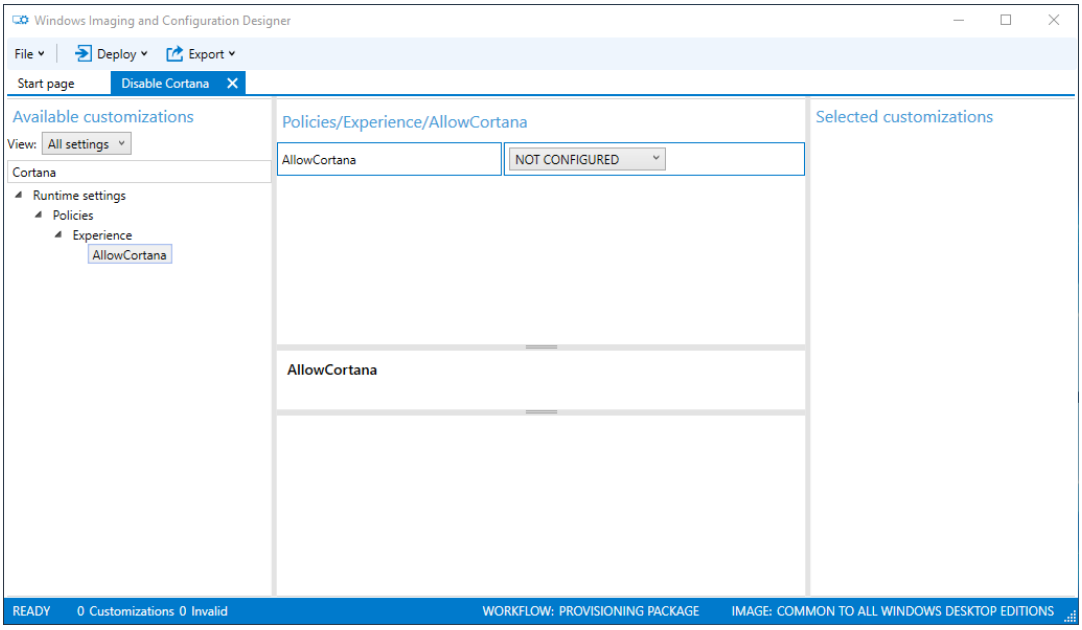
5. On the Edition selection screen select “Common to all Windows desktop editions” and click “Next”.



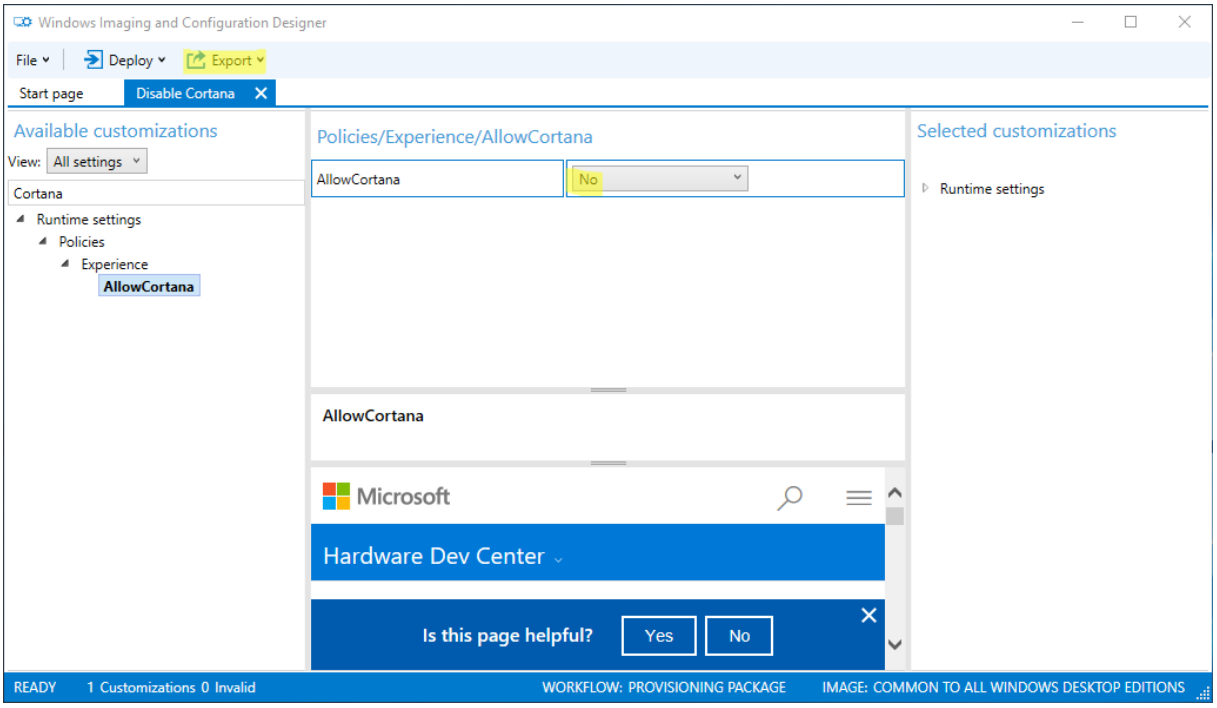
6. On the “Import a provisioning package” screen click “Finish”.



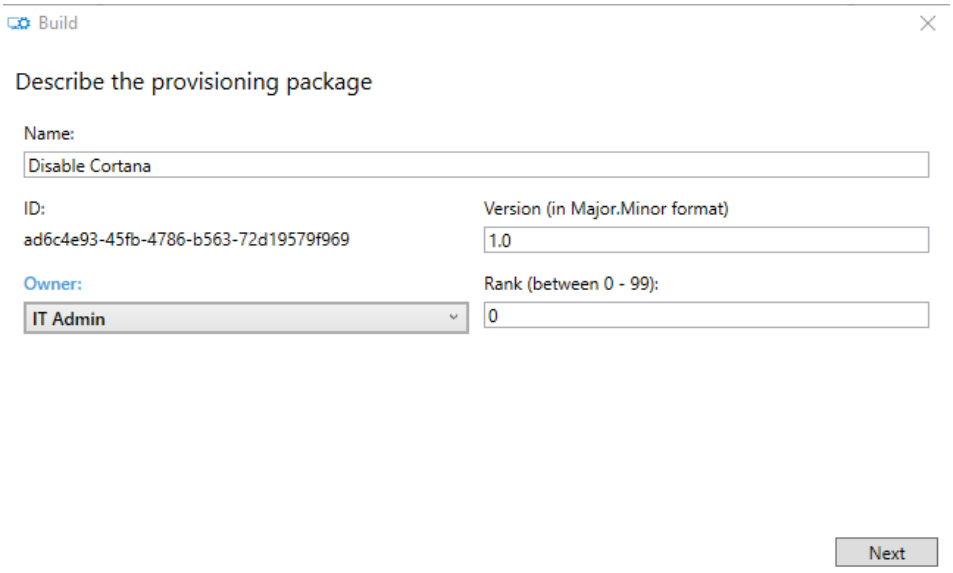
7. Scroll through the available policies and in the “Available customizations” and then search for “Cortana” and select the “AllowCortana” policy.



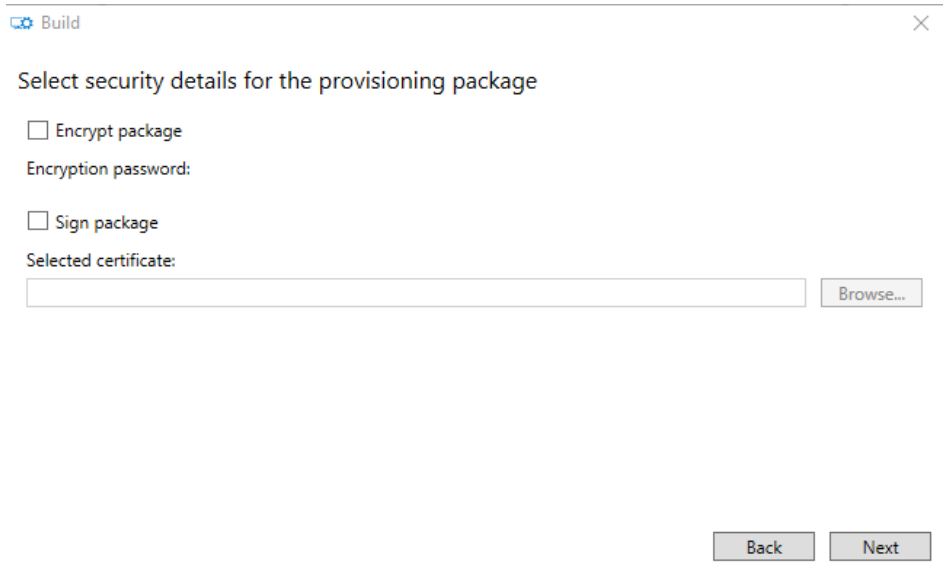
8. Set the policy to “No” and click on “Export” → “Provisioning Package”.



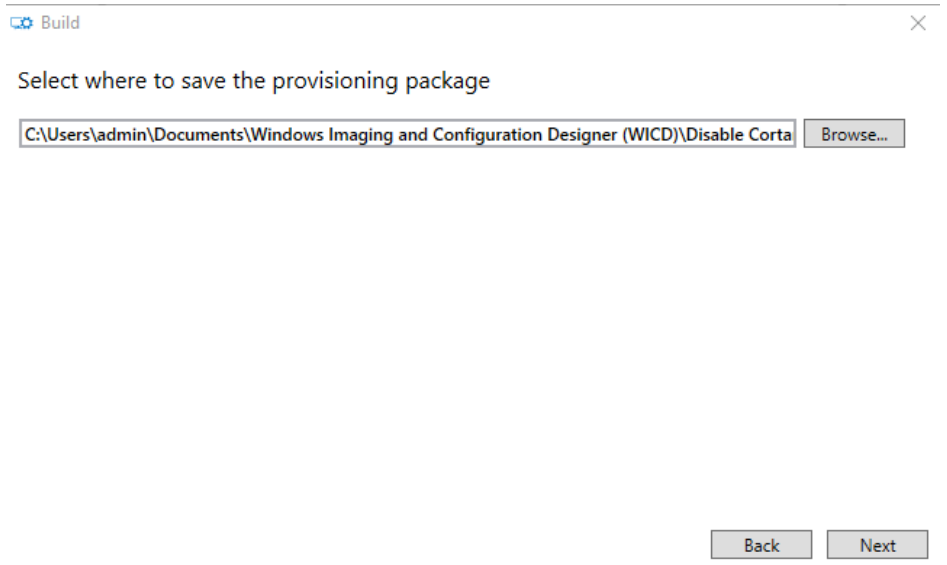
9. Select “IT Admin” as owner and click “Next”.



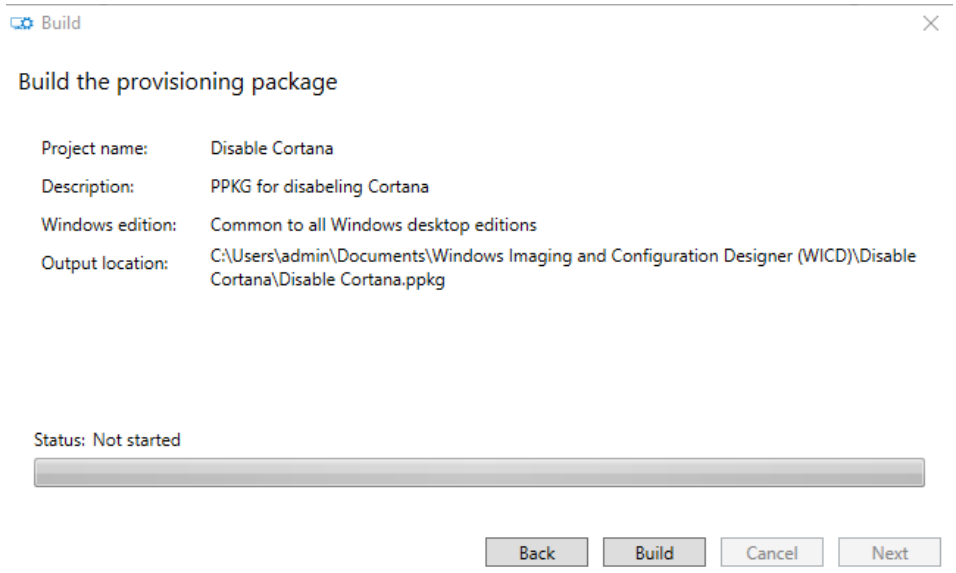
10. On the “Select security details” screen leave the defaults and click “Next”.



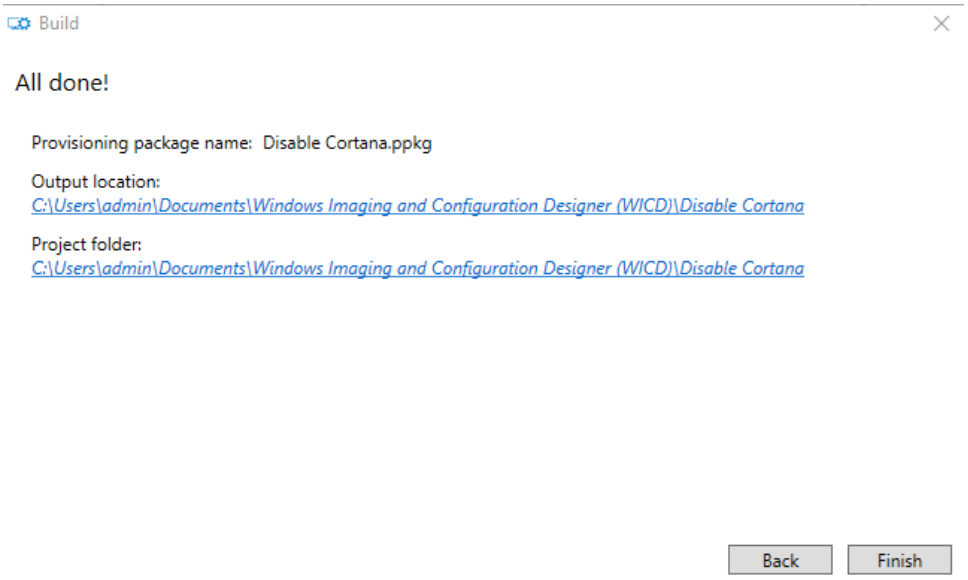
11. Remember the path where the package is stored and click “Next”.



12. On the “Build the provisioning package” click “Build”.



13. Open the output location.

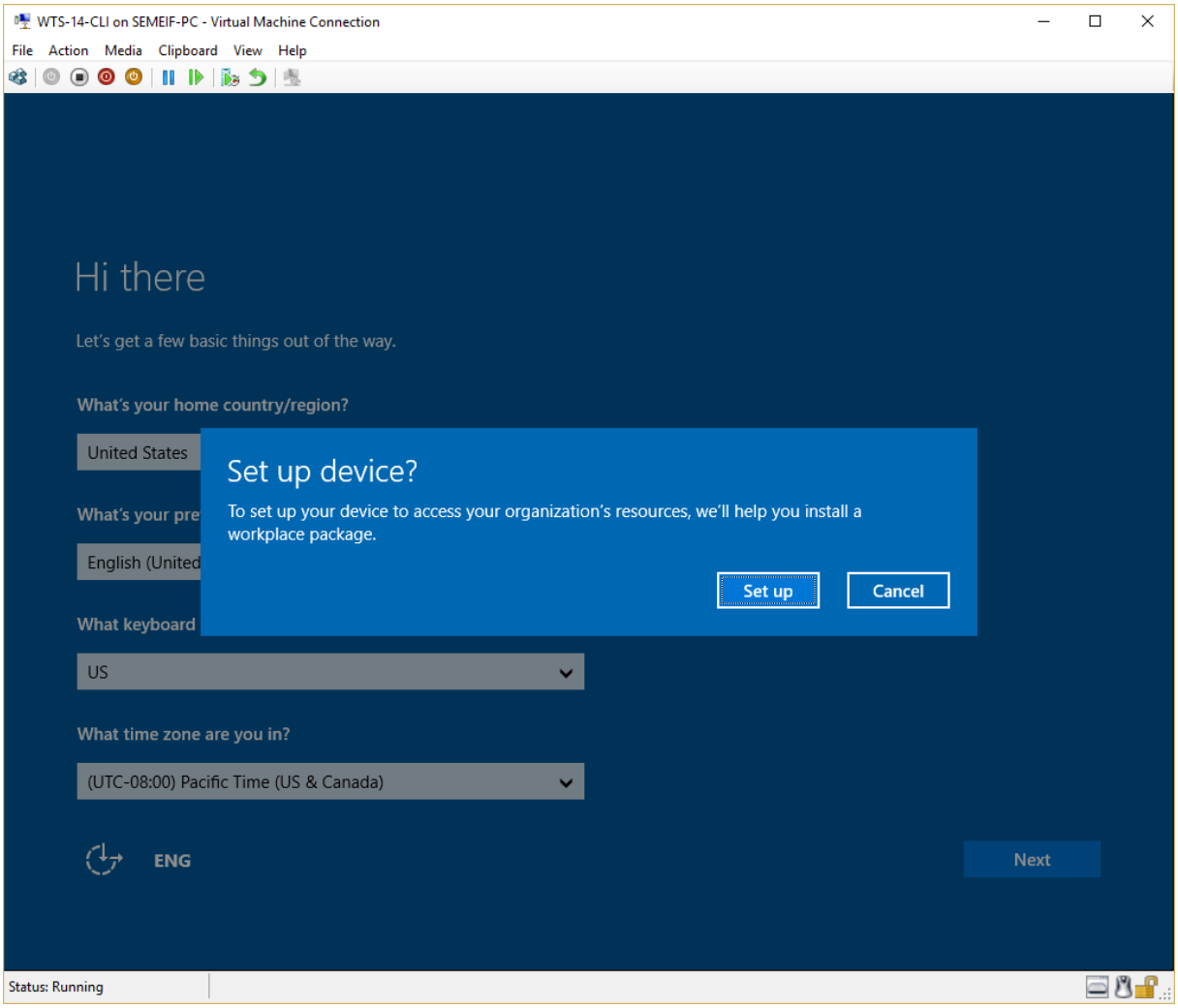


14. And copy the file <Disable Cortana.ppkg> to the App folder on the desktop of the WTS-04-CAS machine.

3.2. Apply PPKG in OOBE (optional)

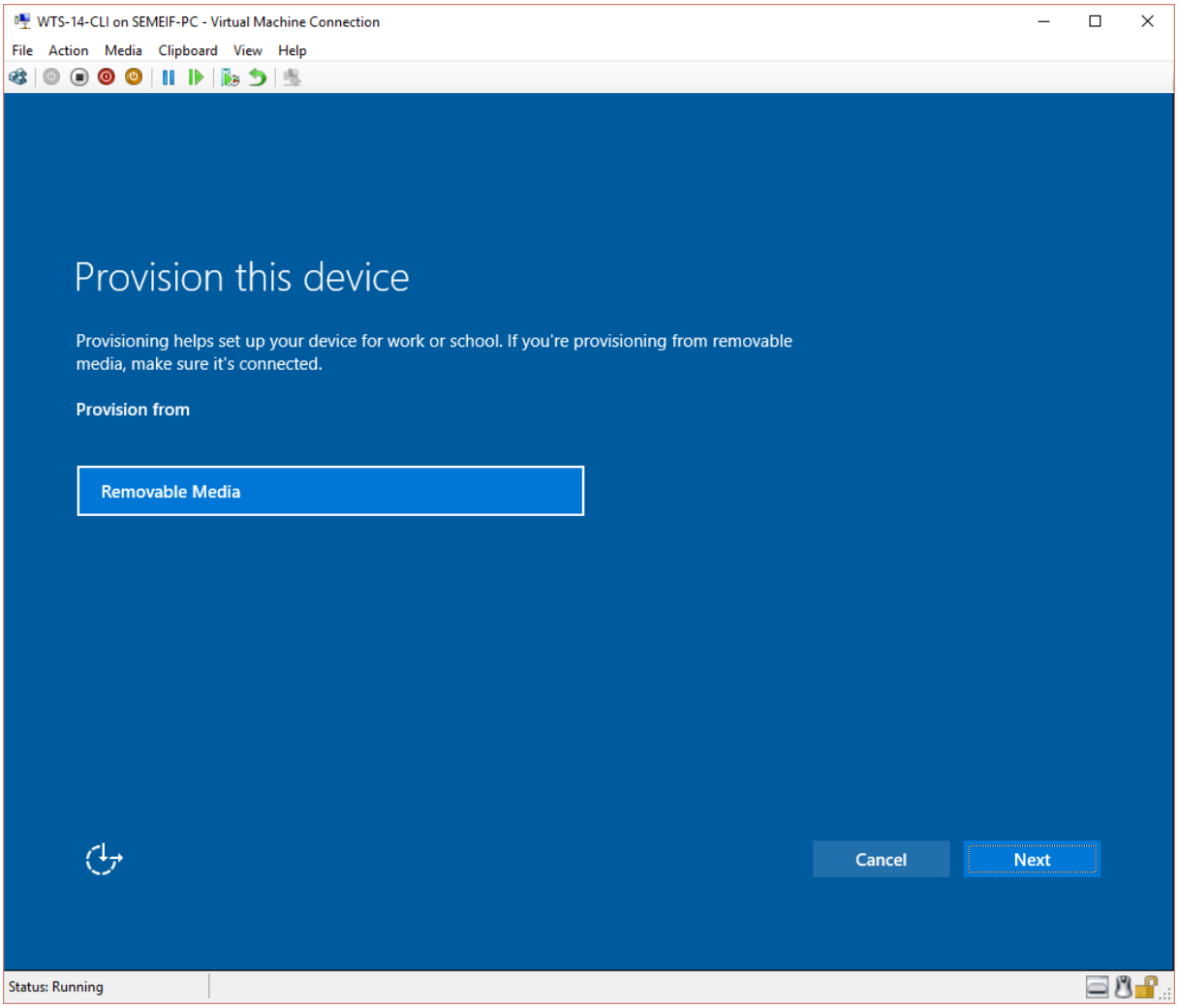
1. Due to the restrictions that you can't insert a USB stick to VM during the OOBE this part of the Module will only describe the theory.

2. On the first screen of the OOBE hit the button five times to open provisioning menu and click “Set up”.

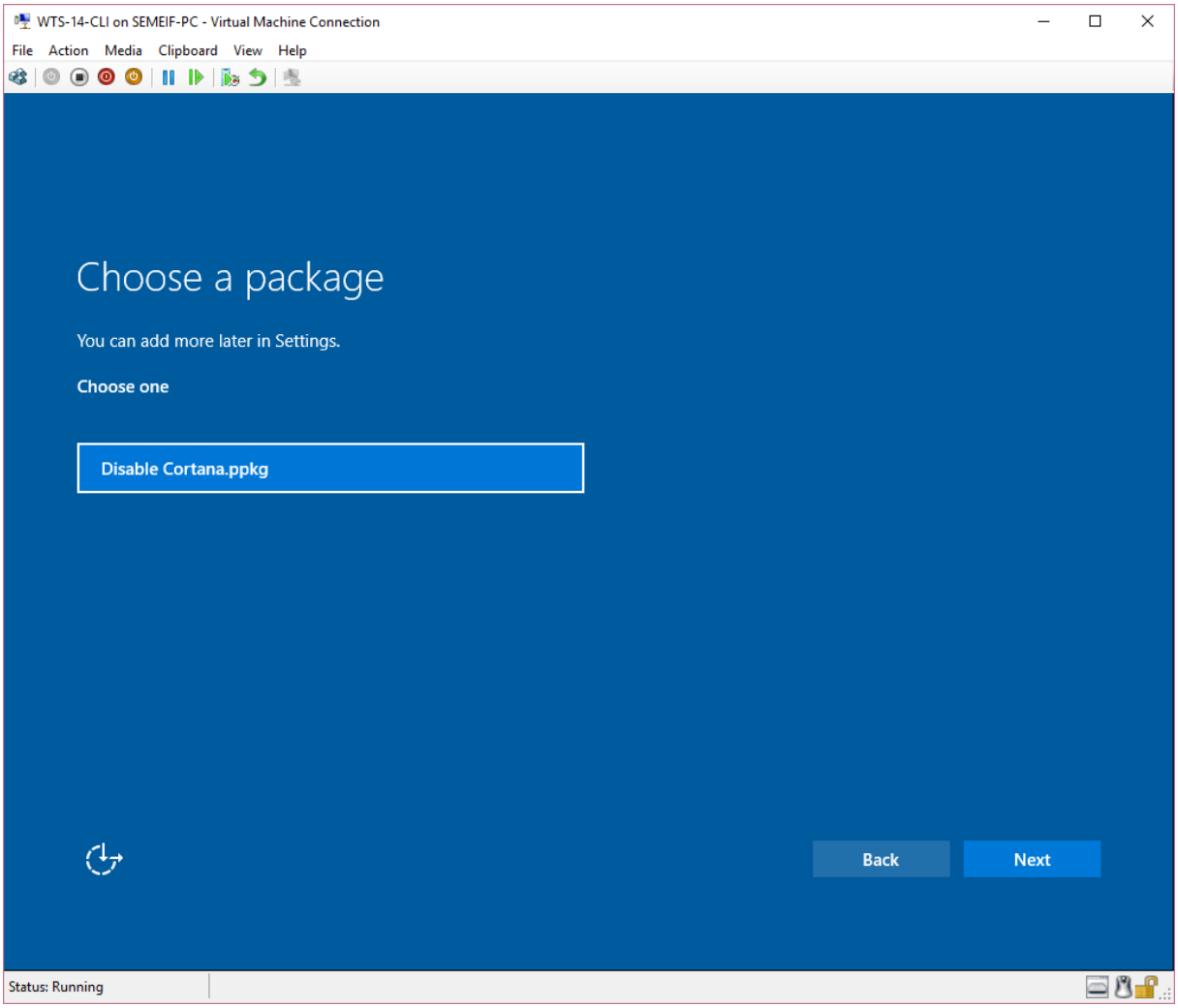


3. Insert USB stick or any other removable media to the machine.

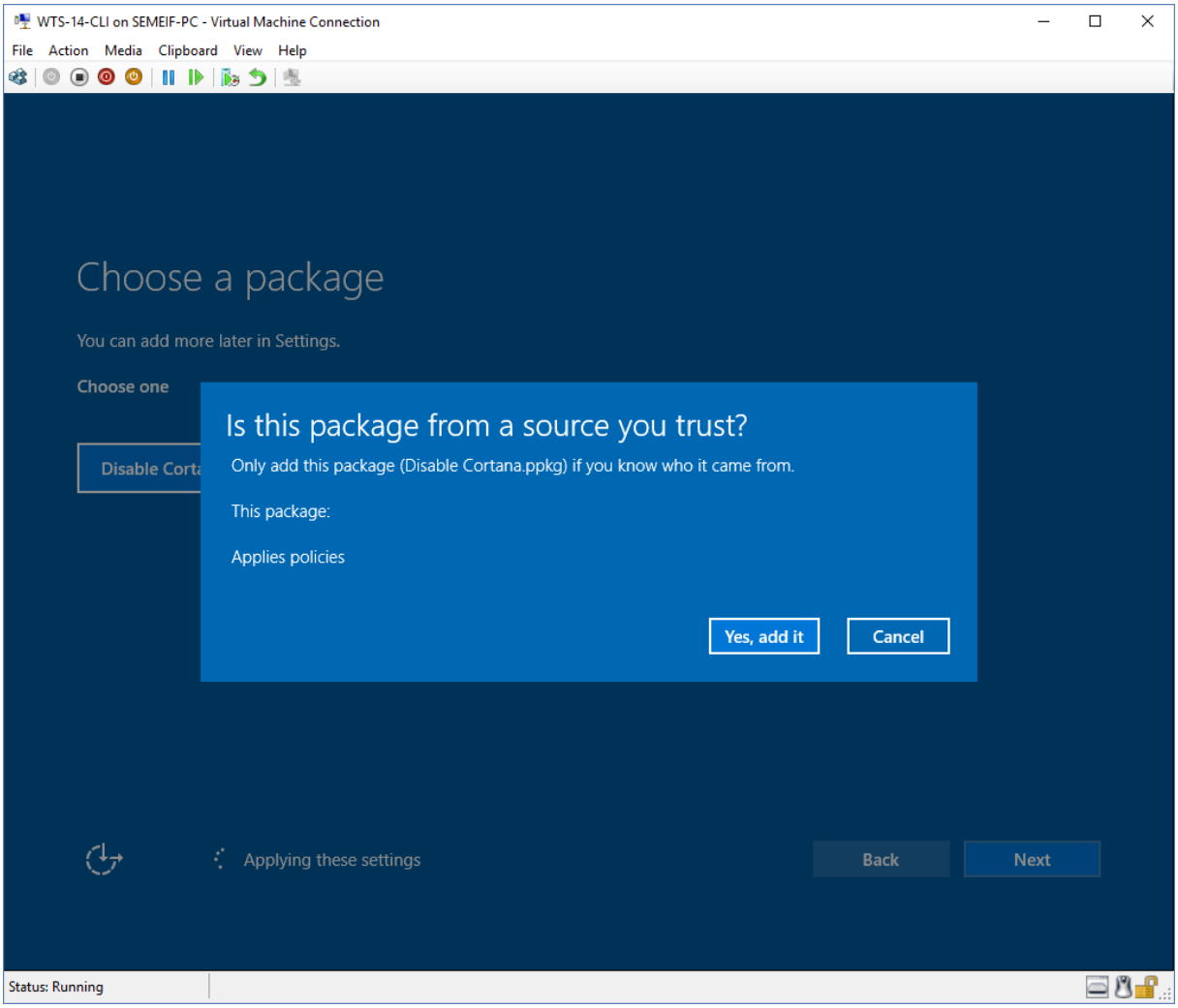
4. Select “Removable Media” and click “Next”.



5. Select the Provisioning package you want to apply and click “Next”.

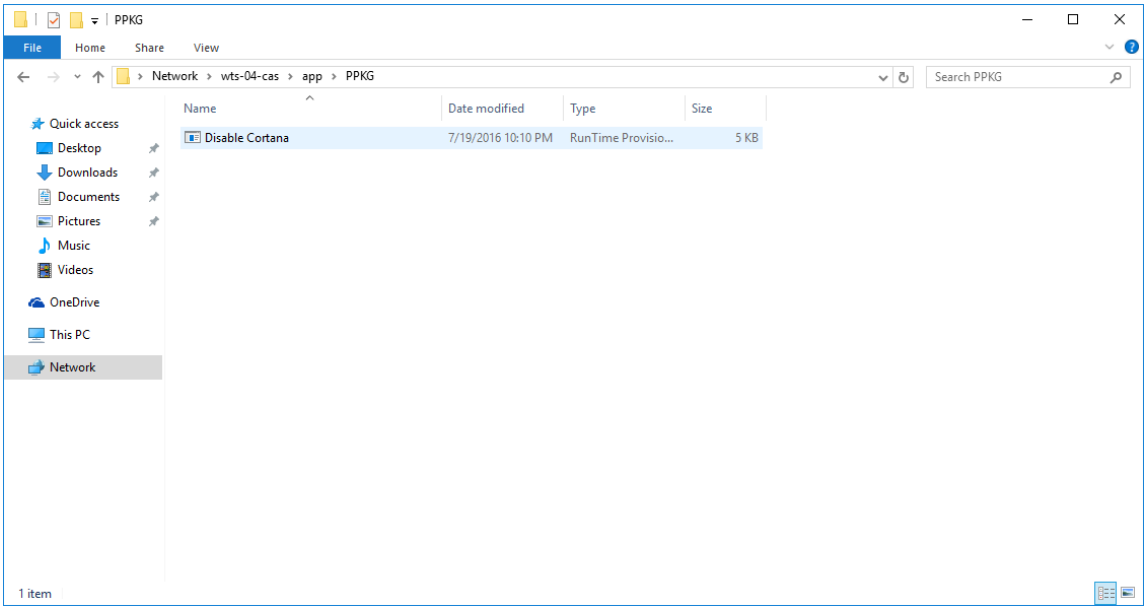


6. When the package is not digitally signed you need to confirm the security warning. Click on “Yes, add it”.

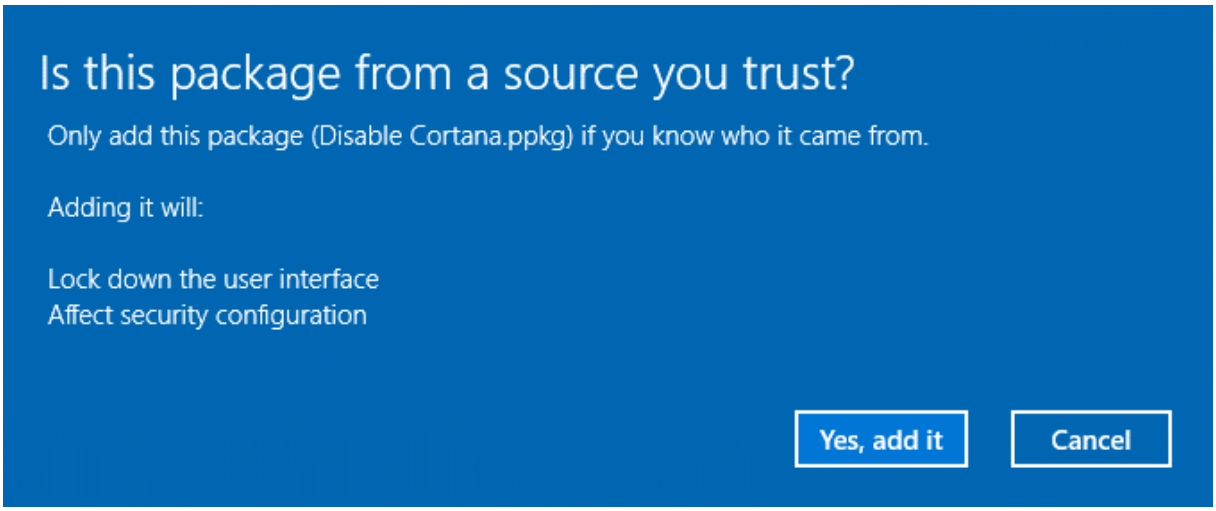


3.3. Apply PPKG while user is already logged on

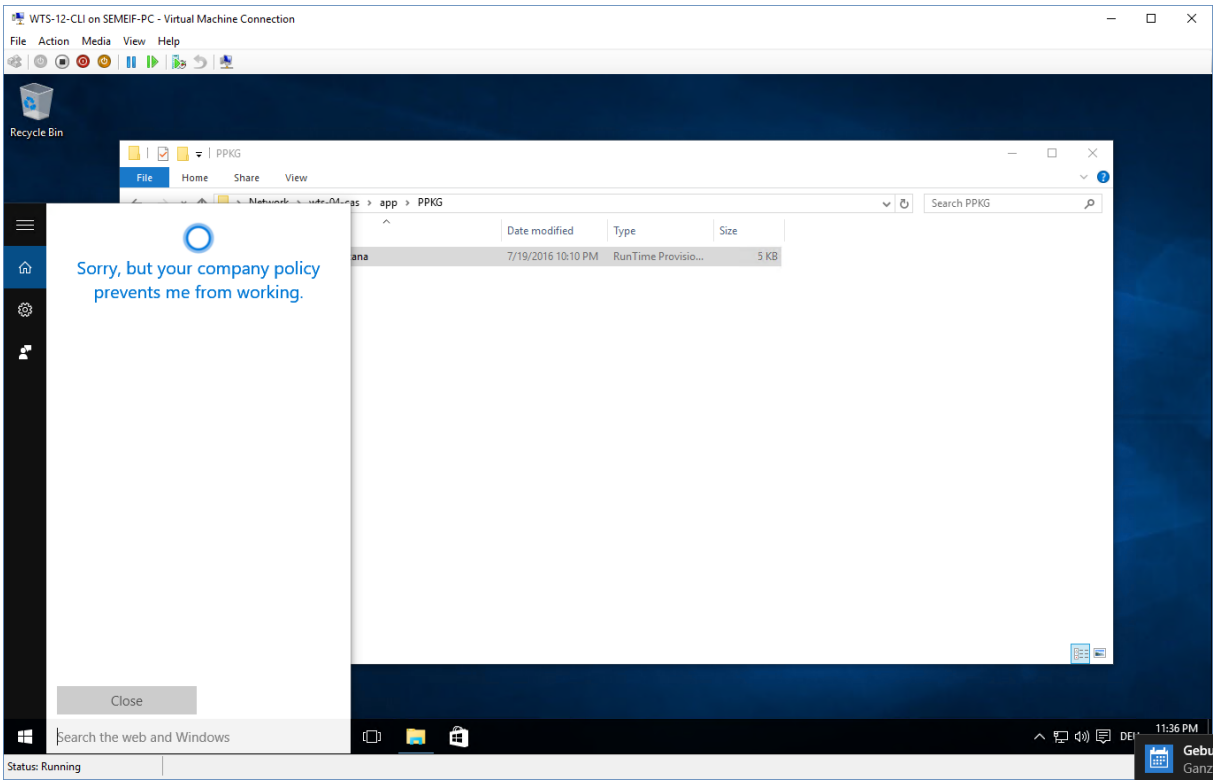
1. On the WTS-12-CLI machine open Cortana and sign in with a Microsoft account.
2. Open “File Explorer” and navigate to \\wts-04-cas\app\PPKG.



3. Double click the “Disable Cortana.ppkg” file.
4. Accept the “UAC” dialog with “Yes”.
5. When the package is not digitally signed you need to confirm the security warning. Click on “Yes, add it”.

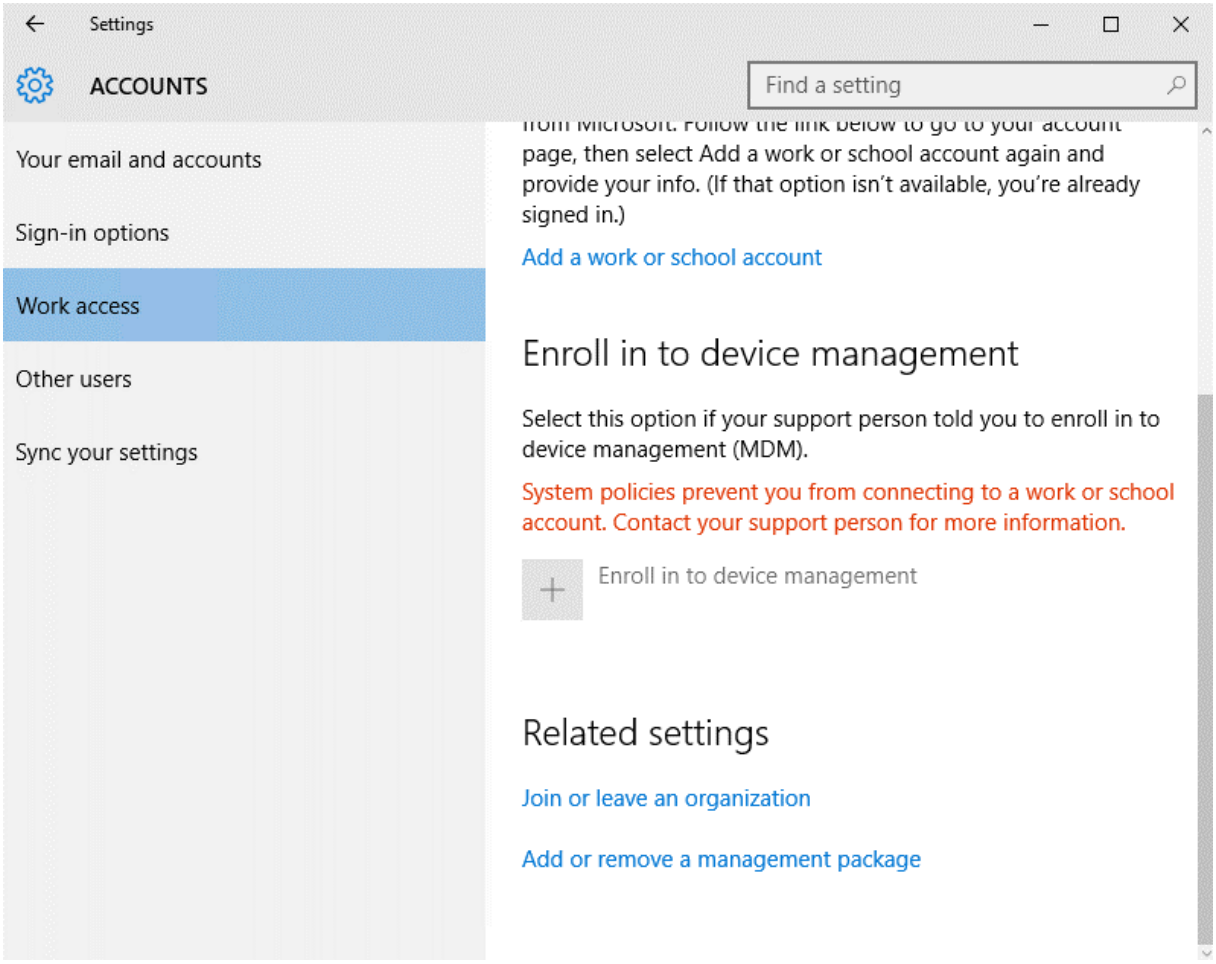


6. Try to open Cortana again and see the result.

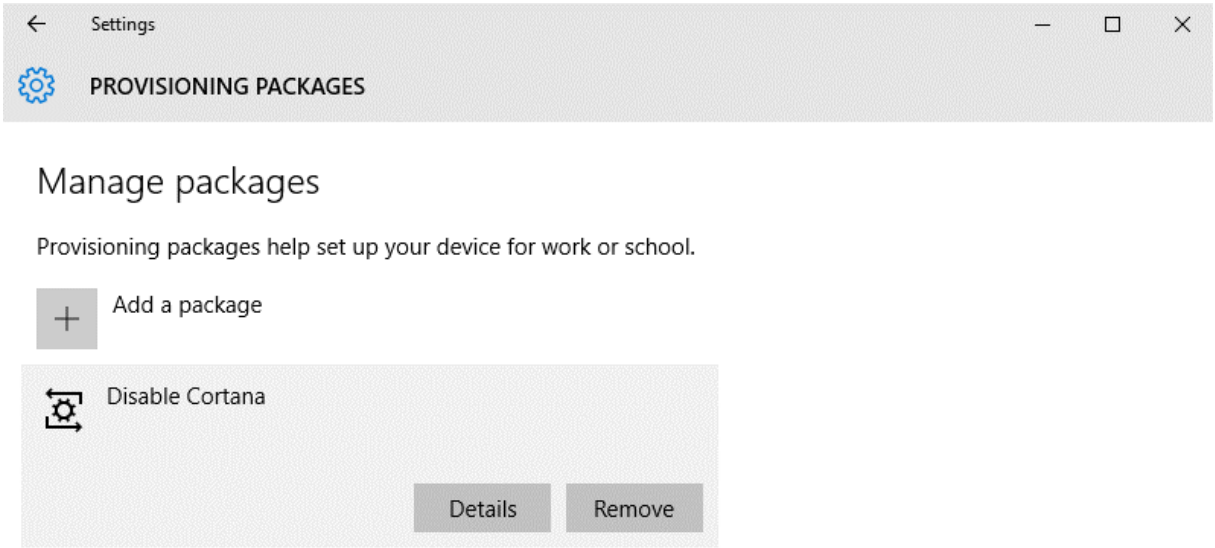


Remove Provisioning package

1. On the WTS-12-CLI machine open "Settings", navigate to "Accounts" → "Work access" and click on "Add or remove a management package".



2. Select the "Disable Cortana" package and click "Remove".



3. On the "UAC" dialog click "Yes" and when it'S removed try Cortana again.
4. Cortana should work.

4. Lab guide part 4 – Device Guard (WTS-14-CLI)

4.1. Verify that hardware and firmware requirements are met.

1. Verify that your client computers possess the necessary hardware and firmware to run these features.
2. Use the hardware readiness tool on the Microsoft Download Center(The tool has **already been downloaded to the Desktop** of WTS_14-CLI and is in the DG_Readiness_Tool_v2.0 folder)
3. Open an elevated PowerShell (ISE) prompt and run the script from the tool: DG_Readiness.ps1 -Capable
4. When the first run is finished reboot the machine and run the script again with the same parameter.

4.2. Create a code integrity policy from a golden computer

!!! Creating a policy from the golden system takes quite some time. Therefore, a policy.bin file has already been created.!!!

1. To create a code integrity policy, copy each of the following commands into an elevated Windows PowerShell session, in order:
2. Initialize variables that you will use. The following example commands use InitialScan.xml and DeviceGuardPolicy.bin for the names of the files that will be created:
   $CIPolicyPath=$env:userprofile+"\Desktop\DG_Policy_Student\"
   $InitialCIPolicy=$CIPolicyPath+"InitialScan.xml"
   $CIPolicyBin=$CIPolicyPath+"DeviceGuardPolicy.bin"
3. Use New-CIPolicy to create a new code integrity policy by scanning the system for installed applications:
   New-CIPolicy -Level PcaCertificate -FilePath $InitialCIPolicy –UserPEs 3> CIPolicyLog.txt
4. Use ConvertFrom-CIPolicy to convert the code integrity policy to a binary format:
   ConvertFrom-CIPolicy $InitialCIPolicy $CIPolicyBin

4.3. Audit code integrity policies

1. Find the *.bin policy file that you have created, for example, the c:\users\admin\Desktop\DG_Policy\DeviceGuardPolicy.bin file that resulted from the steps in the earlier section, Create a code integrity policy from a golden computer. Copy the file to C:\Windows\System32\CodeIntegrity.
2. On the computer you want to run in audit mode, open the Local Group Policy Editor by running GPEdit.msc.

3. Navigate to Computer Configuration\Administrative Templates\System\Device Guard, and then select Deploy Code Integrity Policy. Enable this setting by using the appropriate file path, for example, C:\Windows\System32\CodeIntegrity\DeviceGuardPolicy.bin
4. Restart the reference system for the code integrity policy to take effect.
5. Use the system as you normally would, and monitor code integrity events in the event log. While in audit mode, any exception to the deployed code integrity policy will be logged in the Applications and Services Logs\Microsoft\Windows\CodeIntegrity\Operational event log.

4.4. Create a code integrity policy that captures audit information from the event log (optional)

1. Review the audit information in the event log. From the code integrity policy exceptions that you see, make a list of any applications that should be allowed to run in your environment, and decide on the file rule level that should be used to trust these applications.Although the Hash file rule level will catch all of these exceptions, it may not be the best way to trust all of them. For information about file rule levels, see Code integrity file rule levels in "Deploy code integrity policies: policy rules and file rules." Your event log might also contain exceptions for applications that you eventually want your code integrity policy to block. If these appear, make a list of these also, for a later step in this procedure.
2. In an elevated Windows PowerShell session, initialize the variables that will be used. The example filename shown here is DeviceGuardAuditPolicy.xml:
   $CIPolicyPath=$env:userprofile+"\Desktop\DG_Policy\"
   $CIAuditPolicy=$CIPolicyPath+"DeviceGuardAuditPolicy.xml"
3. Use New-CIPolicy to generate a new code integrity policy from logged audit events. This example uses a file rule level of Hash and includes 3> CIPolicylog.txt, which redirects warning messages to a text file, CIPolicylog.txt.
   New-CIPolicy -Audit -Level Hash -FilePath $CIAuditPolicy –UserPEs 3> CIPolicylog.txt
4. Find and review the Device Guard audit policy .xml file that you created. If you used the example variables as shown, the filename will be DeviceGuardAuditPolicy.xml, and it will be on your desktop. Look for the following:
   a. Any applications that were caught as exceptions, but should be allowed to run in your environment. These are applications that should be in the .xml file. Leave these as-is in the file.
   b. Any applications that actually should not be allowed to run in your environment. Edit these out of the .xml file. If they remain in the .xml file,

and the information in the file is merged into your existing code integrity policy, the policy will treat the applications as trusted, and allow them to run.

4.5. Merge code integrity policies (optional)

1. To merge two code integrity policies, complete the following steps in an elevated Windows PowerShell session:
2. Initialize the variables that will be used:
   $CIPolicyPath=$env:userprofile+"\Desktop\DG_Policy\"
   $InitialCIPolicy=$CIPolicyPath+"InitialScan.xml"
   $AuditCIPolicy=$CIPolicyPath+"DeviceGuardAuditPolicy.xml"
   $MergedCIPolicy=$CIPolicyPath+"MergedPolicy.xml"
   $CIPolicyBin=$CIPolicyPath+"NewDeviceGuardPolicy.bin"
3. Use Merge-CIPolicy to merge two policies and create a new code integrity policy:
   Merge-CIPolicy -PolicyPaths $InitialCIPolicy,$AuditCIPolicy -OutputFilePath $MergedCIPolicy
4. Use ConvertFrom-CIPolicy to convert the merged code integrity policy to binary format:
   ConvertFrom-CIPolicy $MergedCIPolicy $CIPolicyBin

4.6. Enforce code integrity policies (Enforcement does not work in this HOL environment, because the VMs do not have access to a TPM 2.0 Hardware on the Server)

1. Initialize the variables that will be used:
   $CIPolicyPath=$env:userprofile+"\Desktop\DG_Policy\"
   $InitialCIPolicy=$CIPolicyPath+"InitialScan.xml"
   $EnforcedCIPolicy=$CIPolicyPath+"EnforcedPolicy.xml"
   $CIPolicyBin=$CIPolicyPath+"EnforcedDeviceGuardPolicy.bin"
2. Ensure that rule options 9 (“Advanced Boot Options Menu”) and 10 (“Boot Audit on Failure”) are set the way that you intend for this policy. We strongly recommend that you enable these rule options before you run any enforced policy for the first time. Enabling these options provides administrators with a pre-boot command prompt, and allows Windows to start even if the code integrity policy blocks a kernel-mode driver from running. When ready for enterprise deployment, you can remove these options.
   To ensure that these options are enabled in a policy, use Set-RuleOption as shown in the following commands. You can run these commands even if you're not sure whether options 9 and 10 are already enabled—if so, the commands have no effect.

Set-RuleOption -FilePath $InitialCIPolicy -Option 9
Set-RuleOption -FilePath $InitialCIPolicy -Option 10

3. Copy the initial file to maintain an original copy:
   copy $InitialCIPolicy $EnforcedCIPolicy
4. Use Set-RuleOption to delete the audit mode rule option:
   Set-RuleOption -FilePath $EnforcedCIPolicy -Option 3 -Delete
5. Use ConvertFrom-CIPolicy to convert the new code integrity policy to binary format:
   ConvertFrom-CIPolicy $EnforcedCIPolicy $CIPolicyBin
6. Now that this policy is in enforced mode, you can deploy it to your test computers. Rename the policy to SIPolicy.p7b and copy it to C:\Windows\System32\CodeIntegrity for testing, or deploy the policy through Group Policy by following the instructions in Deploy and manage code integrity policies with Group Policy. You can also use other client management software to deploy and manage the policy.

Appendix