



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]

Windows Tech Series – Management

2

MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, our provision of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The descriptions of other companies' products in this document, if any, are provided only as a convenience to you. Any such references should not be considered an endorsement or support by Microsoft. Microsoft cannot guarantee their accuracy, and the products may change over time. Also, the descriptions are intended as brief highlights to aid understanding, rather than as thorough coverage. For authoritative descriptions of these products, please consult their respective manufacturers.

© 2016 Microsoft Corporation. All rights reserved. Any use or distribution of these materials without express authorization of Microsoft Corp. is strictly prohibited.

Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Versions

Version	Author	Changes
1.0	Semeif	
1.1	Semeif	Basic modules finished

Windows Tech Series – Management

3

MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, our provision of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The descriptions of other companies' products in this document, if any, are provided only as a convenience to you. Any such references should not be considered an endorsement or support by Microsoft. Microsoft cannot guarantee their accuracy, and the products may change over time. Also, the descriptions are intended as brief highlights to aid understanding, rather than as thorough coverage. For authoritative descriptions of these products, please consult their respective manufacturers.

© 2016 Microsoft Corporation. All rights reserved. Any use or distribution of these materials without express authorization of Microsoft Corp. is strictly prohibited.

Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Index

Prerequisites	6
1. Lab guide part 1 – Security with EMS	7
1.1. Azure AD & EMS setup and configuration.....	7
1.1.1. Create Microsoft Azure Trial account (Time: 5:00)	7
1.1.2. Create Azure AD (Time: 6:30).....	9
1.1.3. Azure AD in the “old” Portal	10
1.1.4. Configure Azure Active Directory	11
Create Global Administrator.....	11
Assign EMS License to the Global Administrator	13
1.1.5. Intune setup and initial configuration (Time: 5:00)	13
Activate Intune as Mobile Device Management Authority.....	13
Activate Mobile Device Management in Azure Active Directory.....	16
1.2. Set MDM Policies in Intune (EDP, Whitelist Apps..) (Time: 20:00).....	16
Create PIN Policy	16
Create Windows Information Protection Policy.....	19
Enable Passport for Work.....	25
1.3. Conditional access	26
Attach O365 to Azure AD.....	26
Set up “Service to Service” connector.	30
Create a device compliance policy	34
Evaluate the effect of the conditional access policy	35
Set Conditional Access Policy	36
App White-/Blacklisting (Optional).....	39
Check policies on Client.....	Fehler! Textmarke nicht definiert.
2. Lab guide part 2 – Security with Configuration Manager.....	53
2.1. Client Settings in Configuration Manager (Time: 5:00).....	53
Software updates schedule.....	54
Client Policy	54

Default settings	55
Computer restart	55
2.2 Managing Endpoint Protection/Defender with Config Manager	56
2.1.1. Install Endpoint Protection Site System Role	56
2.1.2. Enable Endpoint Protection in client settings	62
2.1.3. Configure Configuration Manager Software Updates to Deliver Definition Updates 64	
2.1.4. Create and deploy antimalware policies for Endpoint Protection.....	79
Modify the default antimalware policy.....	79
Import an antimalware policy	81
Deploy an antimalware policy to client computers	84
Let's have some fun and bring some Malware on a client machine.	86
2.1.5. Monitor Endpoint Protection.....	89
Monitor Endpoint Protection by Using the Endpoint Protection Status Node	89
3. Lab guide part 3 – Security through Provisioning	91
3.1. Create Provisioning Package with ICD (Time: 10:00)	91
3.2. Apply PPKG in OOBE (optional)	96
3.3. Apply PPKG while user is already logged on.....	100
Remove Provisioning package	102
4. Lab guide part 4 – Device Guard.....	103
4.1. Verify that hardware and firmware requirements are met	103
4.2. Create a code integrity policy from a golden computer.....	103
4.3. Audit code integrity policies	103
4.4. Create a code integrity policy that captures audit information from the event log	104
4.5. Merge code integrity policies.....	105
4.6. Enforce code integrity policies.....	105
Appendix.....	107

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 OOB (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.

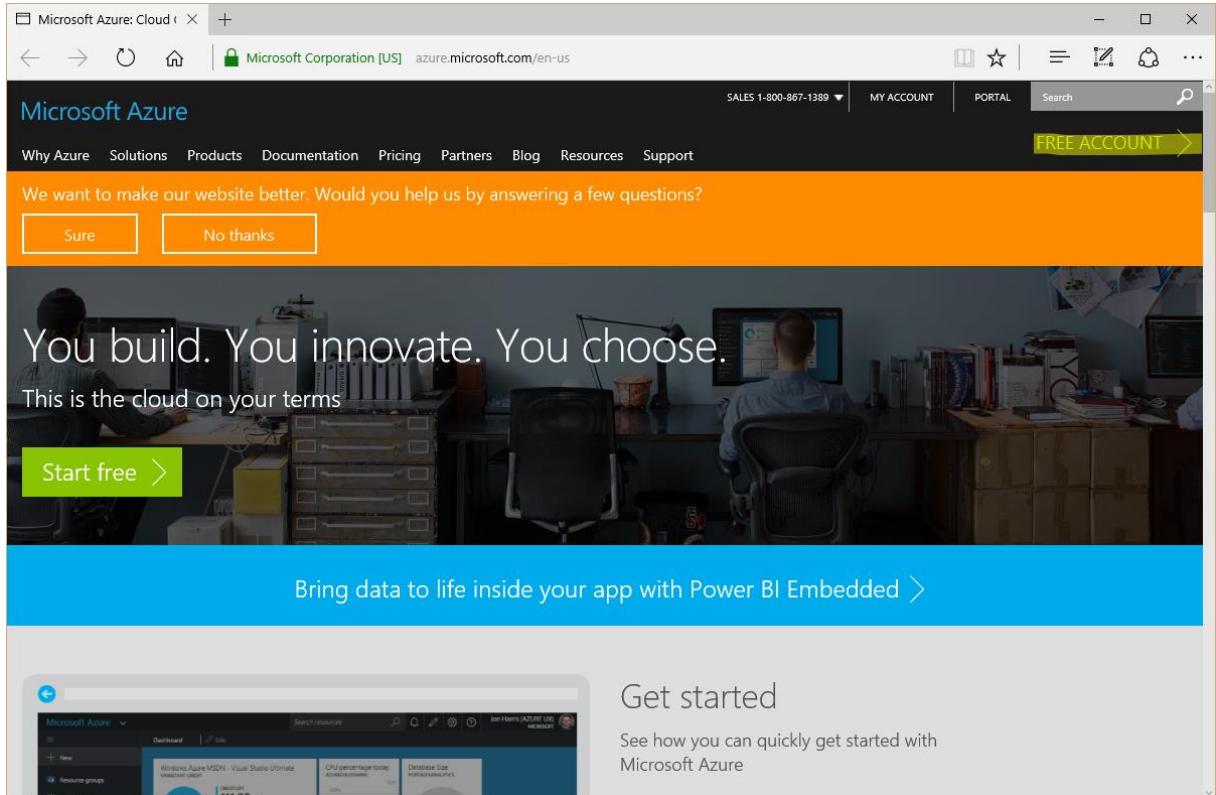
Mobile Phone (for receiving MFA Codes)

1. Lab guide part 1 – Security with EMS

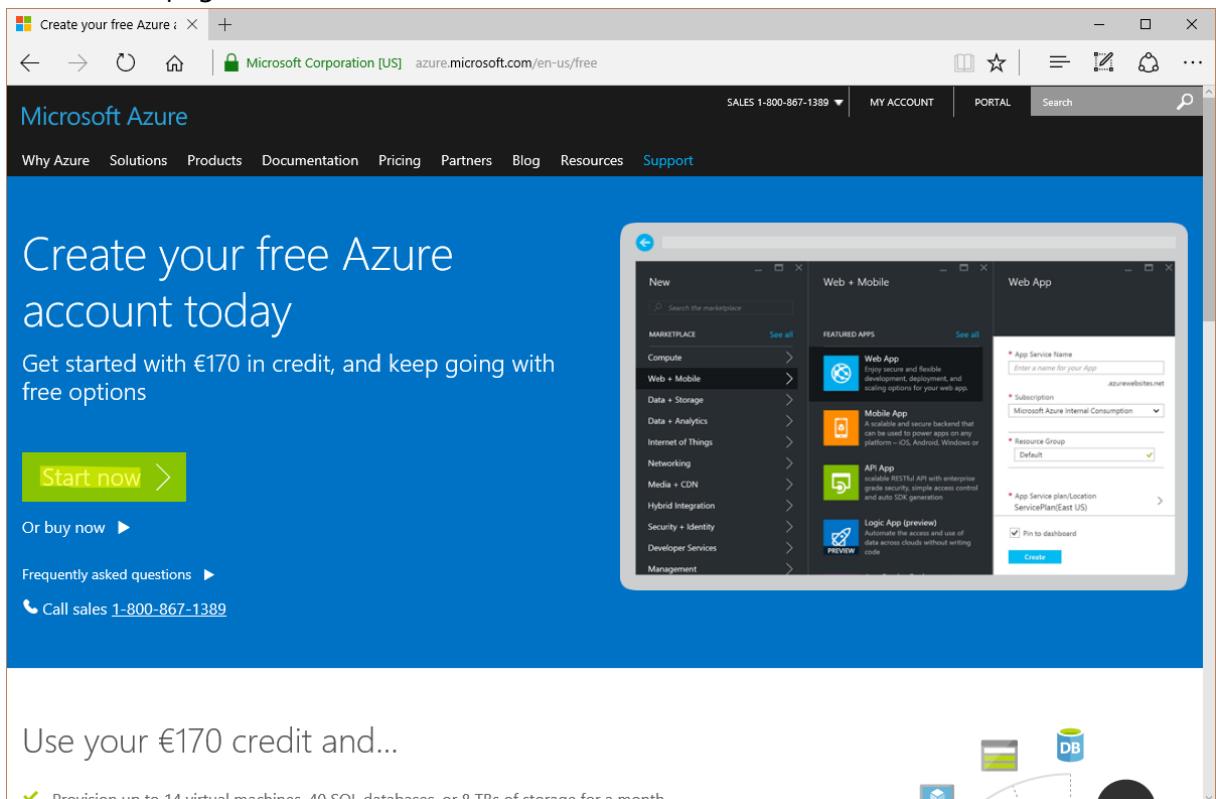
1.1. Azure AD & EMS setup and configuration

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

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



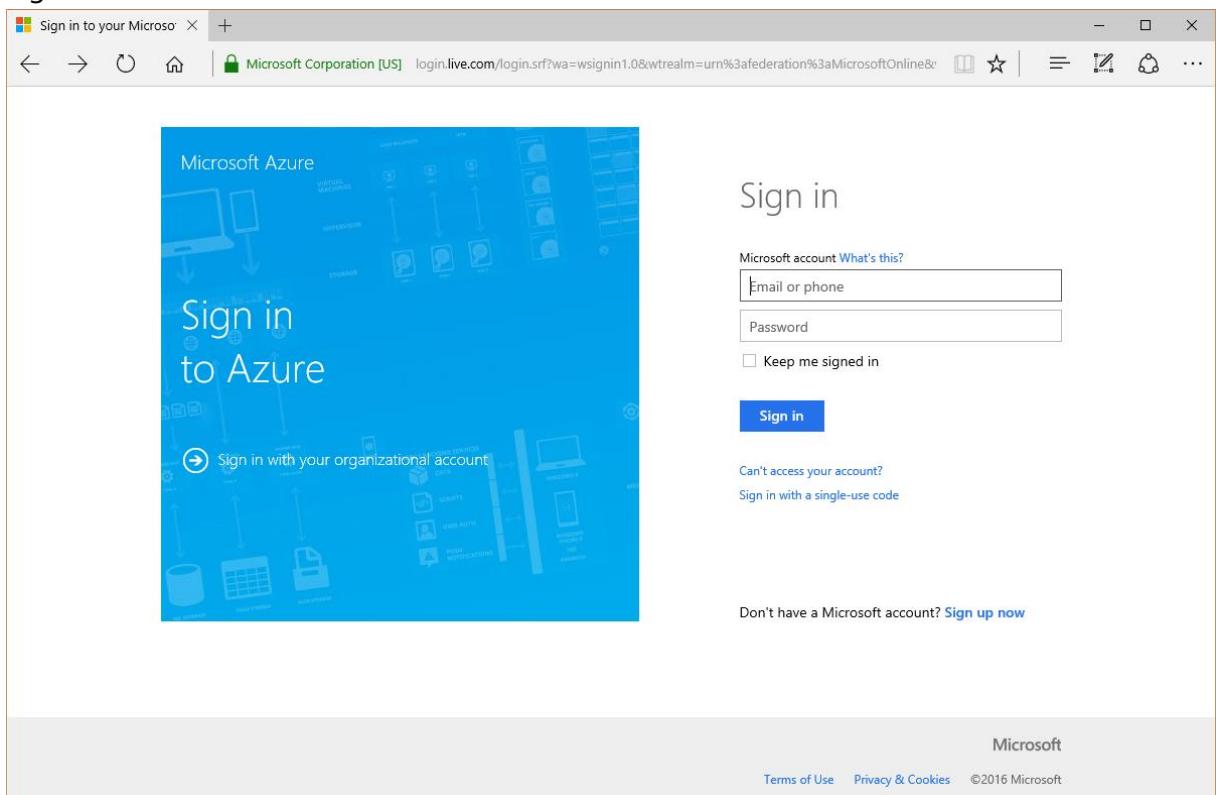
3. On the next page click "Start now".



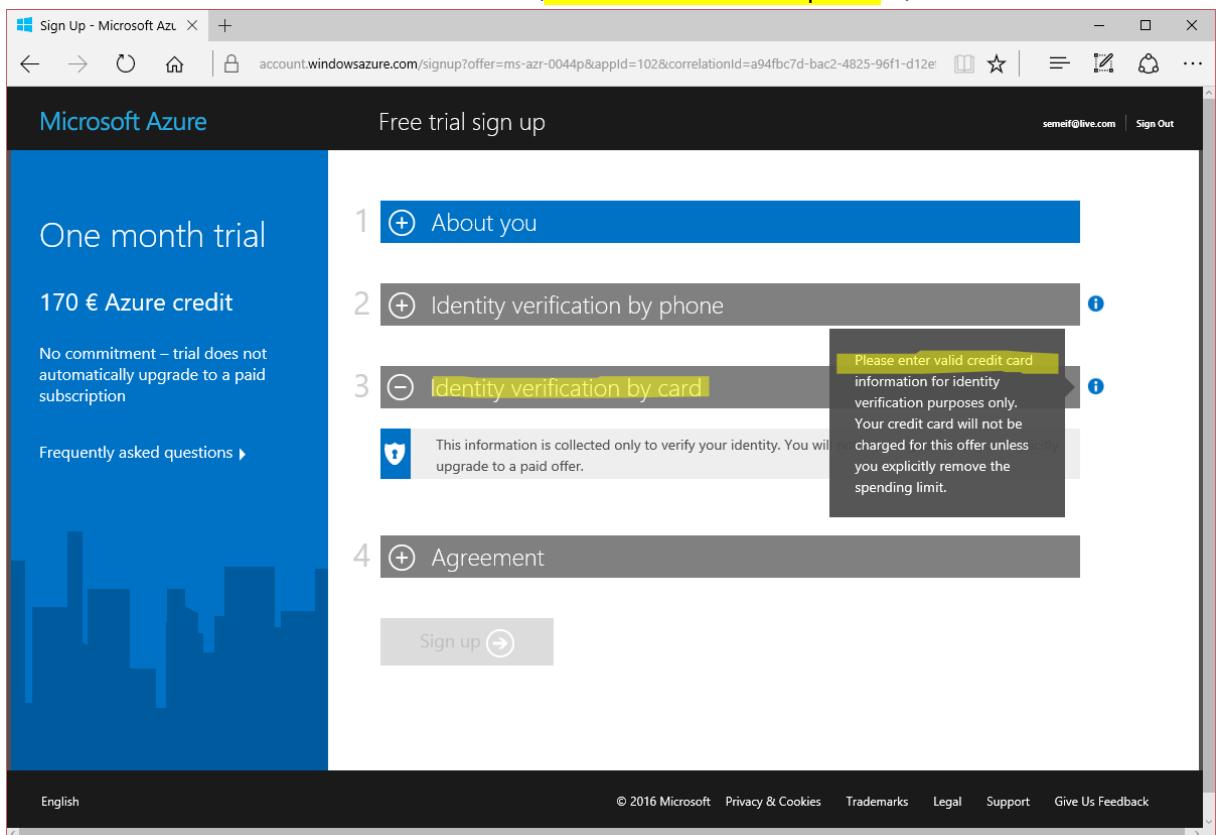
Use your €170 credit and...

✓ Provision up to 14 virtual machines, 40 SQL databases, or 8 TBs of storage for a month

4. Sign-in with a Microsoft Account.



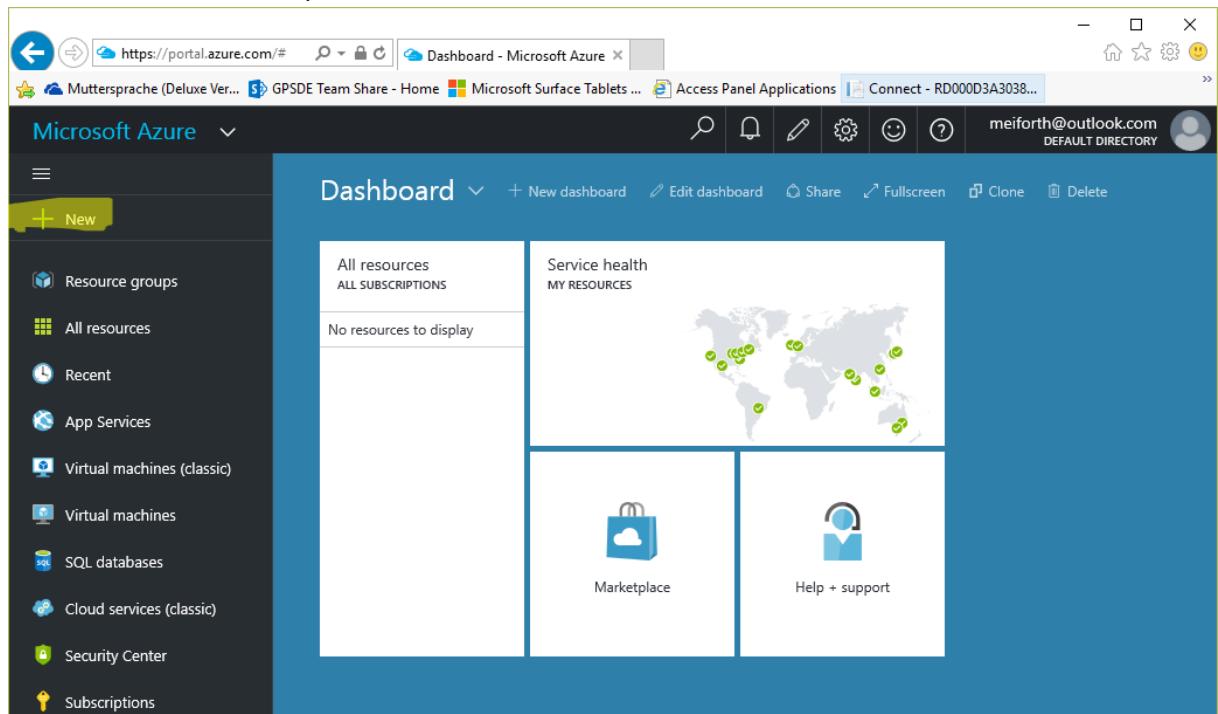
5. Enter additional verification information. (Valid Credit Card required!!!)



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

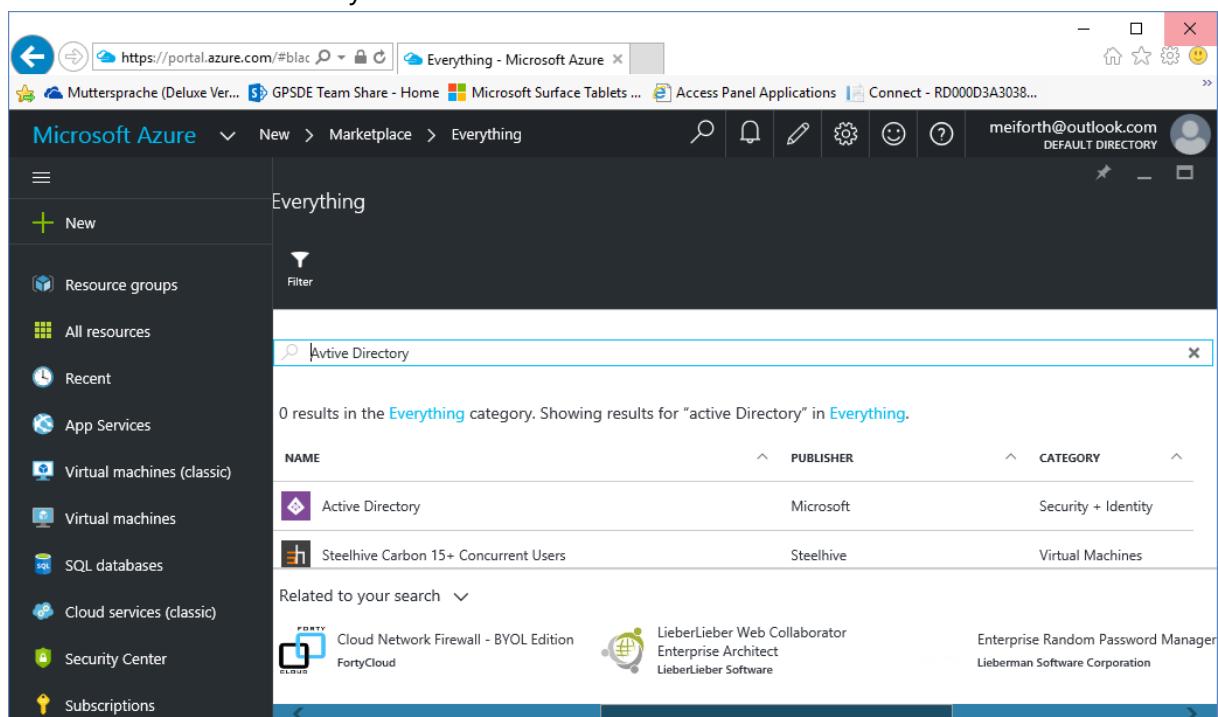
1.1.2. Create Azure AD (Time: 6:30)

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



The screenshot shows the Microsoft Azure dashboard. On the left, there's a sidebar with various navigation options like Resource groups, All resources, Recent, App Services, etc. A green box highlights the "+ New" button. The main area is titled "Dashboard" and shows sections for "All resources ALL SUBSCRIPTIONS" (which says "No resources to display") and "Service health MY RESOURCES" (a world map with green dots). Below these are links for "Marketplace" and "Help + support". At the top right, it shows the user's email (meiforth@outlook.com) and the "DEFAULT DIRECTORY".

3. Search for "Active Directory".



The screenshot shows the Microsoft Azure Marketplace search results for "Active Directory". The search bar at the top contains "Active Directory". The results table has columns for NAME, PUBLISHER, and CATEGORY. Two items are listed:

NAME	PUBLISHER	CATEGORY
Active Directory	Microsoft	Security + Identity
Steelhive Carbon 15+ Concurrent Users	Steelhive	Virtual Machines

Below the table, there's a section titled "Related to your search" with links to "Cloud Network Firewall - BYOL Edition" by FortyCloud, "Enterprise Architect" by LieberLieber Software, and "Enterprise Random Password Manager" by Lieberman Software Corporation.

4. Click on  Active Directory

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”



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

The screenshot shows the "Add directory" page. It includes fields for "NAME" (WTSFY17HOL), "DOMAIN NAME" (WTSFY17HOL.onmicrosoft.com), and "COUNTRY OR REGION" (United States). A checkbox for "This is a B2C directory" is checked. A "PREVIEW" button is visible. A large green checkmark icon is located in the top right corner.

DIRECTORY

Create new directory

NAME

WTSFY17HOL

DOMAIN NAME

WTSFY17HOL .onmicrosoft.com

COUNTRY OR REGION

United States

This is a B2C directory. PREVIEW

3. Now your Active Directory will be created and shows up with the status Active 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 **Get Azure AD Premium** and click on **Try it now**.
6. On the next screen click on TRY ENTERPRISE MOBILITY SUITE NOW
7. To Activate Enterprise Mobility Suite trial, click on .
8. Now the EMS will be attached to your AD.
9. Click on **Please wait while we set up the trial... (Click here to refresh)** to check the status.

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

The screenshot shows the Microsoft Azure Active Directory portal. The left sidebar lists various services: Grid, Network, Compute, Storage, Cloud, Mobile, DB, and Analytics. The main navigation bar includes Microsoft Azure, Check out the new portal, CREDIT STATUS, and a user account (meiforth@outlook.com). The top navigation bar shows the URL https://manage.windows... and tabs for Active Directory - Microsoft Az... and Active Directory - Microsoft... The 'LICENSES' section is selected. It shows the 'Enterprise Mobility Suite' license plan with 100 active units and 0 assigned units. The subscription renewal date is listed as 8/10.

1.1.4. Configure Azure Active Directory

Create Global Administrator

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

The screenshot shows the Microsoft Azure Active Directory portal. The left sidebar lists various services: Grid, Network, Compute, Storage, Cloud, Mobile, DB, and Analytics. The main navigation bar includes Microsoft Azure, Check out the new portal, CREDIT STATUS, and a user account (meiforth@outlook.com). The top navigation bar shows the URL https://manage.windows... and tabs for Active Directory - Microsoft Az... and Active Directory - Microsoft... The 'USERS' section is selected. A message box displays the text "Your directory is ready to use. Here are a few options to get started." with a checkbox for "Skip Quick Start the next time I visit". Below the message box are buttons for "I WANT TO" (Set Up Directory, Manage Access, Develop Applications) and "GET STARTED".



2. Click on **ADD USER**.
3. Select "New user in your organization" and give it a "User Name".

Microsoft Azure

ADD USER

Tell us about this user

TYPE OF USER

New user in your organization

USER NAME

semeif @ WTSFY17HOL.onmicrosoft.com

4. Enter the user profile information and choose „Global Admin“ as a Role. Enter an

alternate email address for account recovery purposes. Then click

Microsoft Azure

ADD USER

user profile

FIRST NAME

Sebastian

LAST NAME

Meiforth

DISPLAY NAME

Sebastian

ROLE

Global Admin

ALTERNATE EMAIL ADDRESS

semeif@microsoft.com

MULTI-FACTOR AUTHENTICATION

Enable Multi-Factor Authentication

5. Click on **create** 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 **ASSIGN**.



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.

The screenshot shows the Microsoft Intune Admin Center interface. On the left is a vertical navigation menu with the following items:

- DASHBOARD
- GROUPS
- ALERTS
- APPS** (highlighted in yellow)
- POLICY
- REPORTS
- ADMIN

The main content area is titled "Administration" and contains the following sections:

- Overview** (highlighted in blue)
- Alerts and Notifications**
 - ▶ Alert Types
 - Recipients
 - Notification Rules
- Administrator Management**
 - Service Administrators
 - Device Enrollment Managers
 - Client Software Download
 - Storage Use
- Mobile Device Management** (highlighted in yellow)
- Company Portal

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

The screenshot shows the "Mobile Device Management" page. At the top, there is a message box:

First Step: Choose to use Microsoft Intune to manage mobile devices.

Below the message box, there is a section titled "Mobile Device Management Authority". It contains the following information:

i No authority set. **Set Mobile Device Management Authority** (highlighted in yellow)

6. Open the „Windows“ section.

The screenshot shows a navigation menu for "Mobile Device Management". The "Windows" section is highlighted with a yellow background. Other sections include "Alerts and Notifications", "Administrator Management", and "Mobile Device Management".

- Administration
 - Overview
 - Alerts and Notifications
 - Alert Types
 - Recipients
 - Notification Rules
 - Administrator Management
 - Service Administrators
 - Device Enrollment Managers
 - Client Software Download
 - Storage Use
 - Mobile Device Management**
 - Windows
 - Windows Phone

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

Set Up Mobile Device Management for Windows

Step 1: Enrollment Server Address

Either specify a verified domain name (such as contoso.com), or tell your users to manually enter manage.microsoft.com as the server name during enrollment.

[Learn more about setting your DNS server for enrollment](#)

WTSFY17HOL.onmicrosoft.com

Test Auto-Detection

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

Test Successful



WTSFY17HOL.onmicrosoft.com

Users can now enroll their Windows devices without typing the server address manually.

[Learn about Windows enrollment.](#)

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”.

wtsfy17hol

The screenshot shows the Azure Active Directory Applications page. At the top, there are navigation links: DASHBOARD, USERS, GROUPS, APPLICATIONS (which is highlighted in blue), DOMAINS, DIRECTORY INTEGRATION, CONFIGURE, REPORTS, and LICENSES. Below the navigation bar is a search bar with the placeholder "Search Application name or Client ID". A dropdown menu above the search bar says "Show Applications my company uses". To the right of the search bar is a checkmark icon. The main table lists two applications:

NAME	PUBLISHER	TYPE	APP URL
Microsoft Intune	Microsoft Corporation	Web application	http://www.microsoft.com/en-us/server-cl...
Office 365 Management APIs	Microsoft Corporation	Web application	

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

The screenshot shows the Microsoft Intune Configure page. On the left, there is a section labeled "APPLY TO" with three buttons: "ALL" (highlighted with a dashed border), "GROUPS", and "NONE". To the right of this is a help icon (a question mark inside a circle). Below this is a note: "You can configure this mobile device management application to distribute apps from Windows Store for Business. [Get Started](#)".



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 "Policy" Workspace in Microsoft Intune and click on "Add Policy"

The screenshot shows the Microsoft Intune interface. The left sidebar has a 'POLICY' button highlighted. The main area is titled 'Policy' and 'Overview'. It displays 'Policy Status' with '0 Issues'. On the right, there are sections for 'TASKS' (Add Policy), 'REPORTS' (View Noncompliant Apps Report), and 'LEARN ABOUT' (Managing Policies, Interaction with Group Policy). Top right buttons include 'Help', 'Sign Out', and a 'W' icon.

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

The screenshot shows the 'Create a New Policy' dialog. The title is 'Select a template for the new policy'. A note says: 'Select the template that includes the settings you want to manage with the new policy. You use a template to create a policy, and then you can configure the settings in that policy. You cannot change a template.' A list of templates is shown on the left, and a detailed description of the selected template is on the right.

Template	Description
Custom Configuration (Windows 10 Desktop and Mobile and later)	This template contains settings for Windows devices that define items like password length. Policies created from this template can be deployed to user or device groups, and will only be applied to devices that are managed by Microsoft Intune.
Custom Configuration (Windows Phone 8.1 and later)	
Edition Upgrade Policy (Windows 10 Desktop and later)	
Edition Upgrade Policy (Windows 10 Holographic and later)	
Edition Upgrade Policy (Windows 10 Mobile and later)	
Email Profile (Windows 10 Desktop and Mobile and later)	
Email Profile (Windows Phone 8 and later)	
Enterprise data protection (Windows 10 Desktop and Mobile and later)	
General Configuration (Windows 10 Desktop and Mobile and later)	How would you like to use the selected template? <input checked="" type="radio"/> Create and Deploy a Policy with the Recommended Settings <input type="radio"/> Create and Deploy a Custom Policy
General Configuration (Windows 10 Team and later)	
General Configuration (Windows 8.1 and later)	
General Configuration (Windows Phone 8.1 and later)	
PKCS #12 (.PFX) Certificate Profile (Windows 10 Desktop and Mobile and later)	

At the bottom are 'Create Policy' and 'Cancel' buttons.

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

* Name:
WTS HoL Demo Policy

Description:
WTS HoL Demo Policy created by semeif

Security

Password

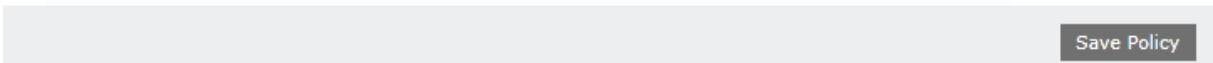
Require a password to unlock devices : [\(i\)](#)
Yes

Required password type : [\(i\)](#)
Numeric

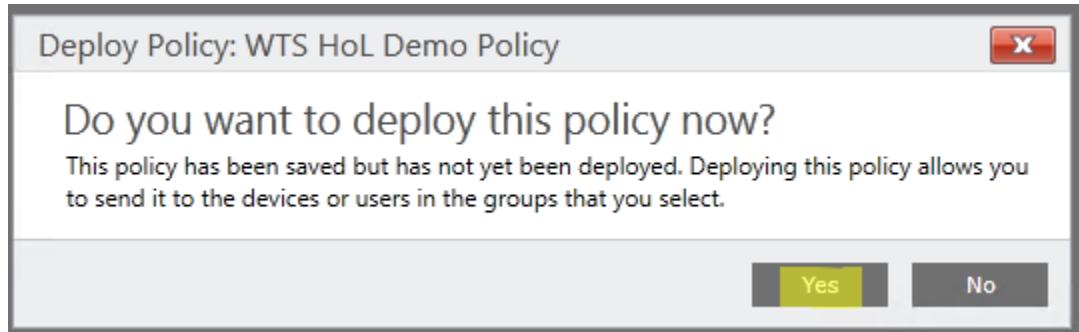
Minimum number of character sets : [\(i\)](#)
1

Minimum password length : [\(i\)](#)
6

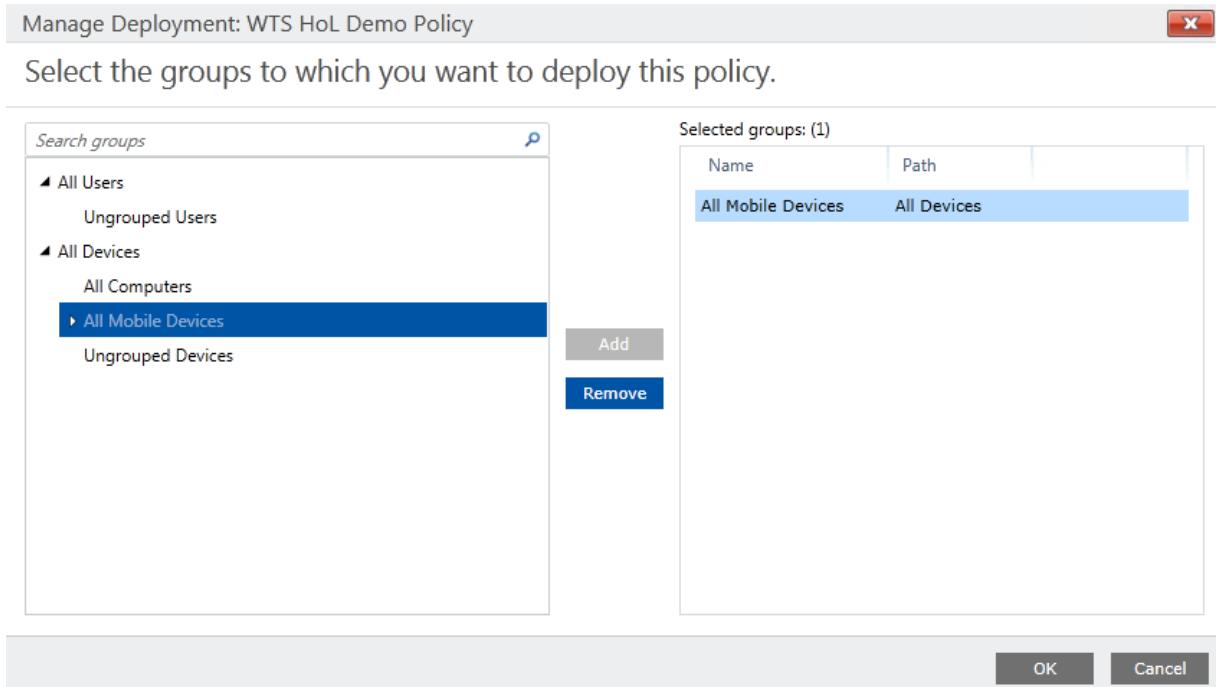
Save Policy



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”.

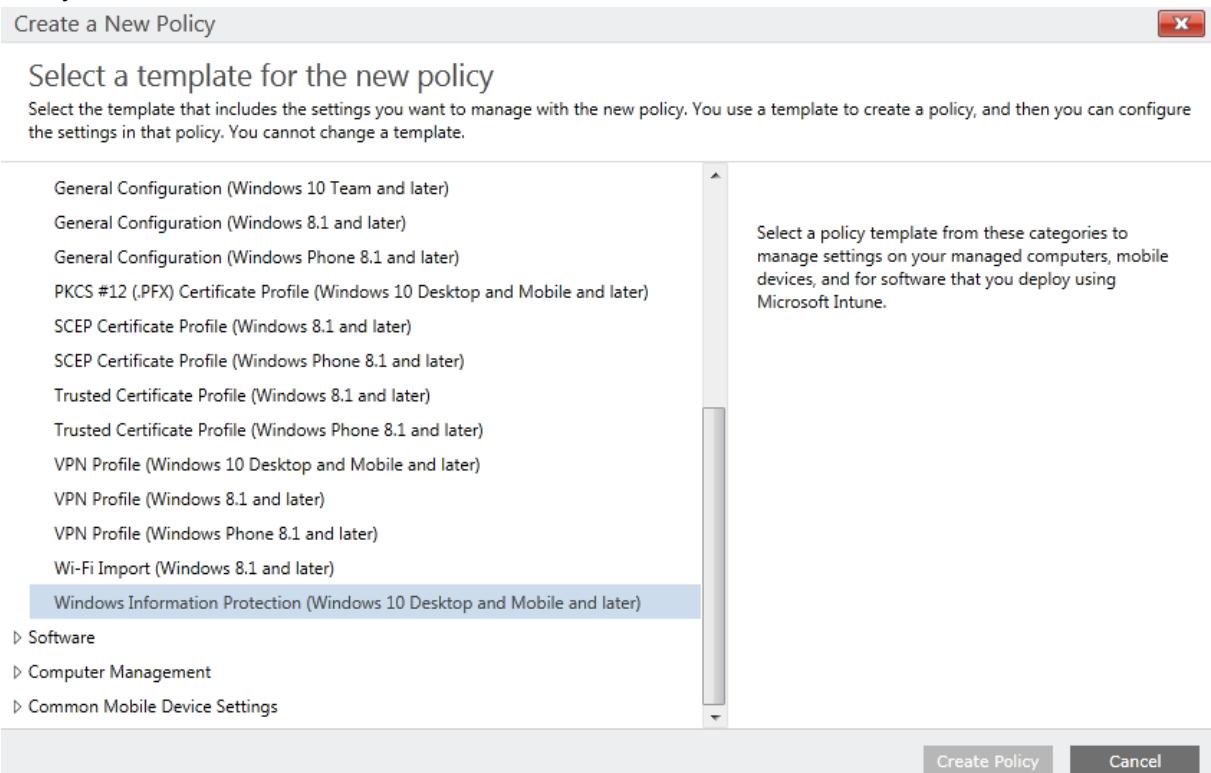


9. Your Policy will now be applied to all systems which are managed through MDM.

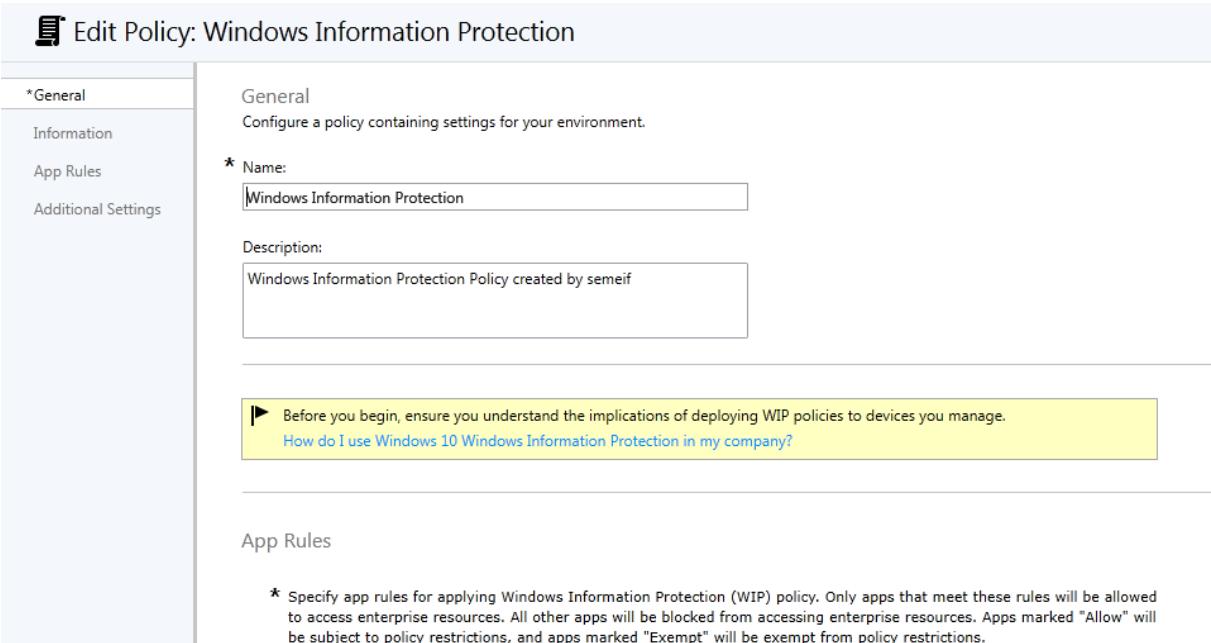
Create Windows Information Protection Policy

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".

App Rules

* Specify app rules for applying Windows Information Protection (WIP) policy. Only apps that meet these rules will be allowed to access enterprise resources. All other apps will be blocked from accessing enterprise resources. Apps marked "Allow" will be subject to policy restrictions, and apps marked "Exempt" will be exempt from policy restrictions.

Rule name	Windows Information Protection mode	Rule template

Add **Edit** **Delete**

* Specify the paste/drop/share restriction mode for apps that meet the app criteria defined in the "App rules" section:

- Block: Blocks paste/drop/share actions when attempting to move data out of enterprise locations and apps.
- Override: Blocks paste/drop/share actions and displays a prompt to the user allowing them to override the block when attempting to move data out of enterprise locations and apps. Override actions are logged for audit.
- Silent: Allows paste/drop/share actions when attempting to move data out of enterprise locations and apps. These actions are logged for audit.
- Off: Turns off Windows Information Protection.

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

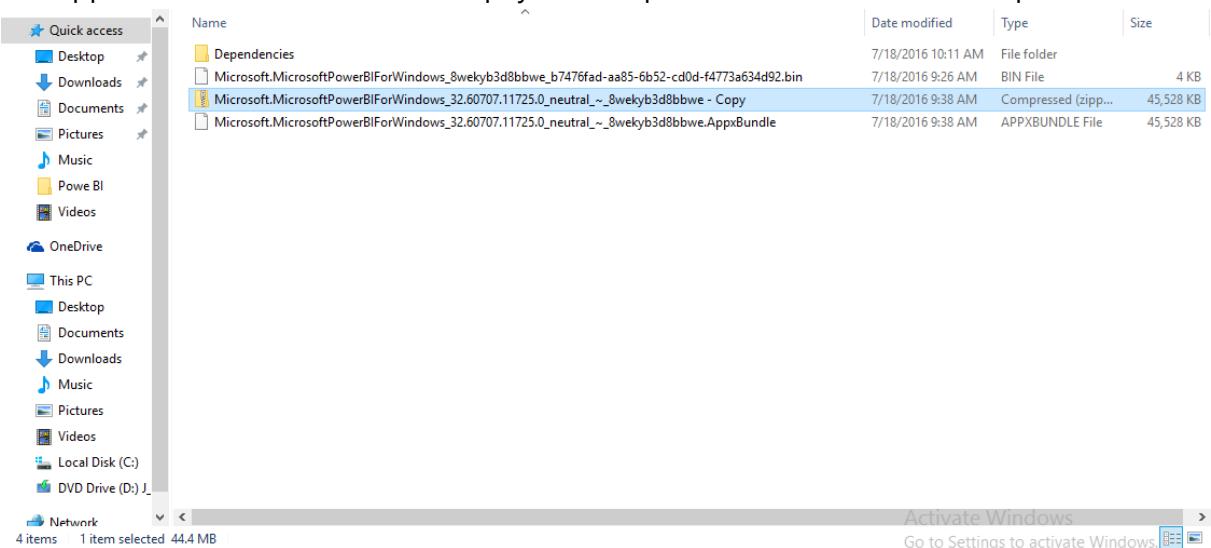
Enterprise data protection mode: Allow

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.

```

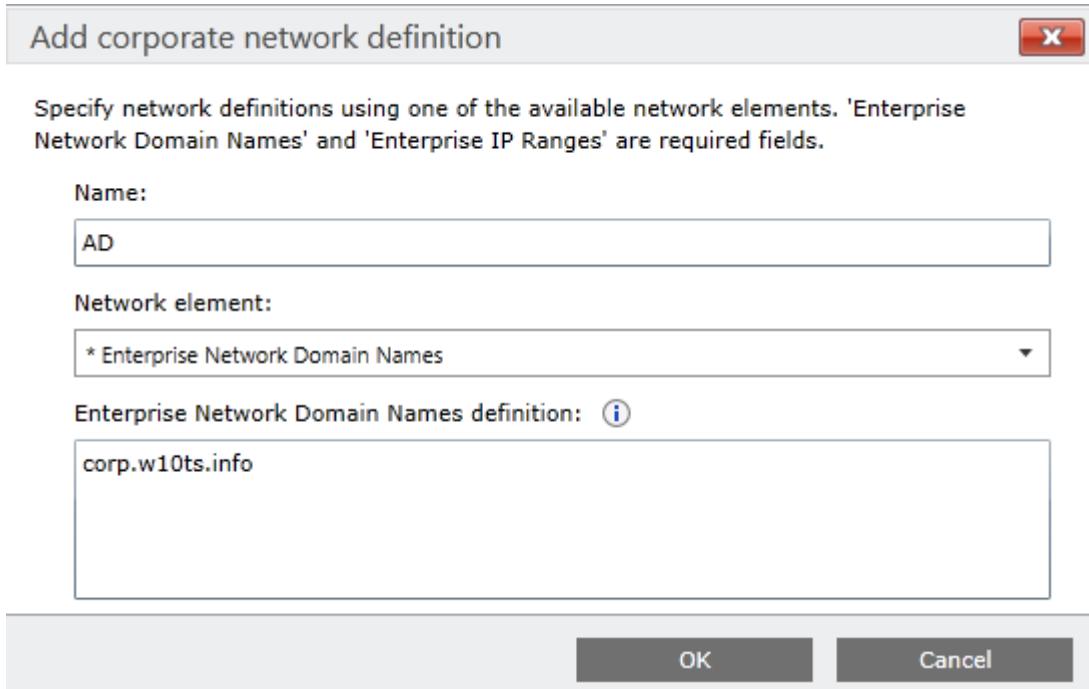
<?xml version="1.0" encoding="UTF-8"?>
- <Bundle xmlns="http://schemas.microsoft.com/appx/2013/bundle" SchemaVersion="2.0">
  <Identity Version="32.60707.11725.0" Publisher="CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US" Name="Microsoft.Msft.PowerBIForWindows"/>
  - <Packages>
    - <Package Version="32.60707.11725.0" Size="71009" Offset="47" FileName="_language-bg.appx" ResourceId="split.language-bg" Type="resource">
      - <Resources>
        <Resource Language="bg-bg"/>
      </Resources>
    </Package>
    - <Package Version="32.60707.11725.0" Size="67403" Offset="71127" FileName="_language-ca.appx" ResourceId="split.language-ca" Type="resource">
      - <Resources>
        <Resource Language="ca-es"/>
      </Resources>
    </Package>
    - <Package Version="32.60707.11725.0" Size="67652" Offset="138601" FileName="_language-cs.appx" ResourceId="split.language-cs" Type="resource">
      - <Resources>
        <Resource Language="cs-cz"/>
      </Resources>
    </Package>
    - <Package Version="32.60707.11725.0" Size="67029" Offset="206324" FileName="_language-da.appx" ResourceId="split.language-da" Type="resource">
      - <Resources>
        <Resource Language="da-dk"/>
      </Resources>
    </Package>
    - <Package Version="32.60707.11725.0" Size="68066" Offset="273424" FileName="_language-de.appx" ResourceId="split.language-de" Type="resource">
      - <Resources>
        <Resource Language="de-de"/>
      </Resources>
    </Package>
  </Packages>
</Bundle>

```

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

* Corporate identity:

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.

```
C:\ Command Prompt
pathname Specifies a pattern, file or directory.
efsfile An encrypted file path.

Used without parameters, CIPHER displays the encryption state of the
current directory and any files it contains. You may use multiple directory
names and wildcards. You must put spaces between multiple parameters.

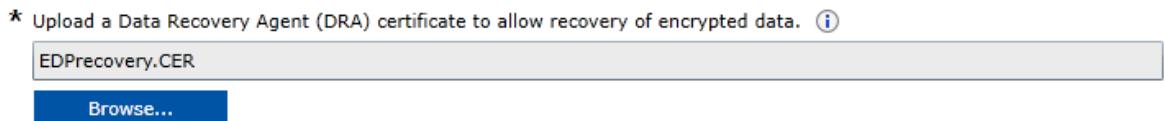
C:\Users\Sebastian>cd Documents

C:\Users\Sebastian\Documents>cipher /r:EDPrecovery
Please type in the password to protect your .PFX file:
Please retype the password to confirm:

Your .CER file was created successfully.
Your .PFX file was created successfully.

C:\Users\Sebastian\Documents>
```

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":

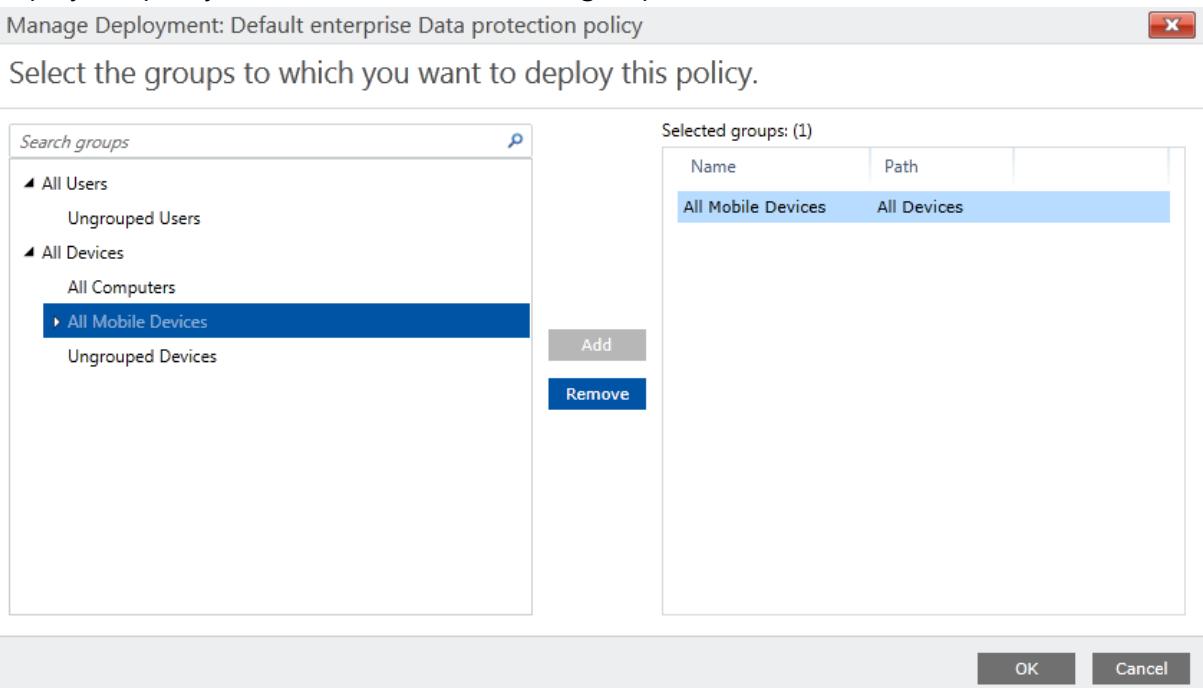
Additional Settings

<input checked="" type="checkbox"/> Show the "Personal" option from the "File ownership" menus in the 'Windows File Explorer' and the 'Windows Save As' dialogs :	(i)
<input type="button" value="No"/>	<input type="button" value="Yes"/>
<input checked="" type="checkbox"/> Prevent corporate data from being accessed by apps when the device is locked. Applies only to Windows 10 Mobile if not configured.	(i)
<input checked="" type="checkbox"/> Revoke encryption keys on unenroll :	(i)
<input type="button" value="Yes"/>	<input type="button" value="No"/>
<input checked="" type="checkbox"/> Allow Windows Search to search encrypted corporate data and Store apps :	(i)
<input type="button" value="Yes"/>	<input type="button" value="No"/>
<input checked="" type="checkbox"/> Show the enterprise data protection icon overlay :	(i)
<input type="button" value="Yes"/>	<input type="button" value="No"/>

Activate Windows
Save Policy Cancel
Go to Settings to activate Windows.

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".

The screenshot shows the Microsoft Intune Admin workspace. The left sidebar has a dark blue header with 'Microsoft Intune' and a light blue footer with 'ADMIN'. The main menu items include DASHBOARD, GROUPS, ALERTS, APPS, POLICY, REPORTS, and ADMIN. Under the ADMIN category, 'Mobile Device Management' is expanded, showing 'Windows' which is also expanded, and 'Hello for Business' is selected. The right panel title is 'Windows Hello for Business'. It contains a brief description: 'Windows Hello for Business is an alternate sign-in method for Windows 10 that uses Active Directory or an Azure Active Directory account to replace password, smart card, or virtual smart card.' Below this, there are three radio buttons: 'Disable Windows Hello for Business on enrolled devices' (unchecked), 'Enable Windows Hello for Business on enrolled devices' (checked), and 'Not configured' (unchecked). A note below says: 'These settings are applied to all Windows 10 and Windows 10 Mobile devices enrolled in Intune.'

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

The screenshot shows the Microsoft Intune Admin workspace. The left sidebar has a dark blue header with 'Microsoft Intune' and a light blue footer with 'ADMIN'. The main menu items include DASHBOARD, GROUPS, ALERTS, APPS, POLICY, REPORTS, and ADMIN. Under the ADMIN category, 'Mobile Device Management' is expanded, showing 'Windows' which is also expanded, and 'Passport for Work' is selected. The right panel title is 'Passport for Work'. It contains a brief description: 'Microsoft Passport for Work is an alternate sign-in method for Windows 10 that uses Active Directory or an Azure Active Directory account to replace password, smart card, or virtual smart card.' Below this, there are three radio buttons: 'Disable Passport for Work on enrolled devices' (unchecked), 'Enable Passport for Work on enrolled devices' (checked), and 'Not configured' (unchecked). A note below says: 'These settings are applied to all Windows 10 and Windows 10 Mobile devices enrolled in Intune.' There are several dropdown menus and input fields for configuring PIN requirements:

- 'Use a Trusted Platform Module (TPM)': Preferred
- 'Require minimum PIN length': 4
- 'Require maximum PIN length': 127
- 'Require lowercase letters in PIN': Not allowed
- 'Require uppercase letters in PIN': Not allowed
- 'Require special characters in PIN': Not allowed
- 'PIN expiration is not configured'

At the bottom right, there are buttons for 'Activate Windows', 'Save', and 'Cancel'.

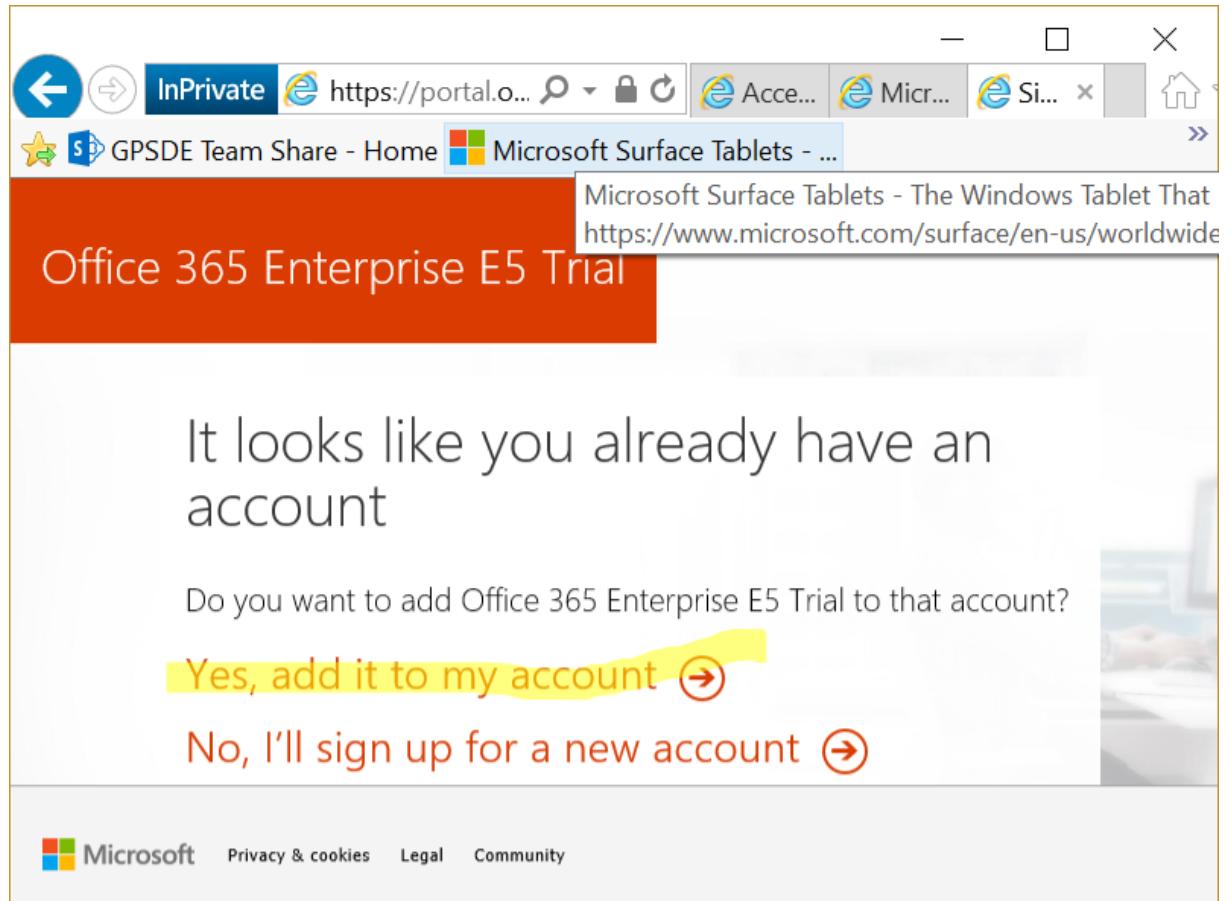
1.3. Conditional access

Attach O365 to Azure AD

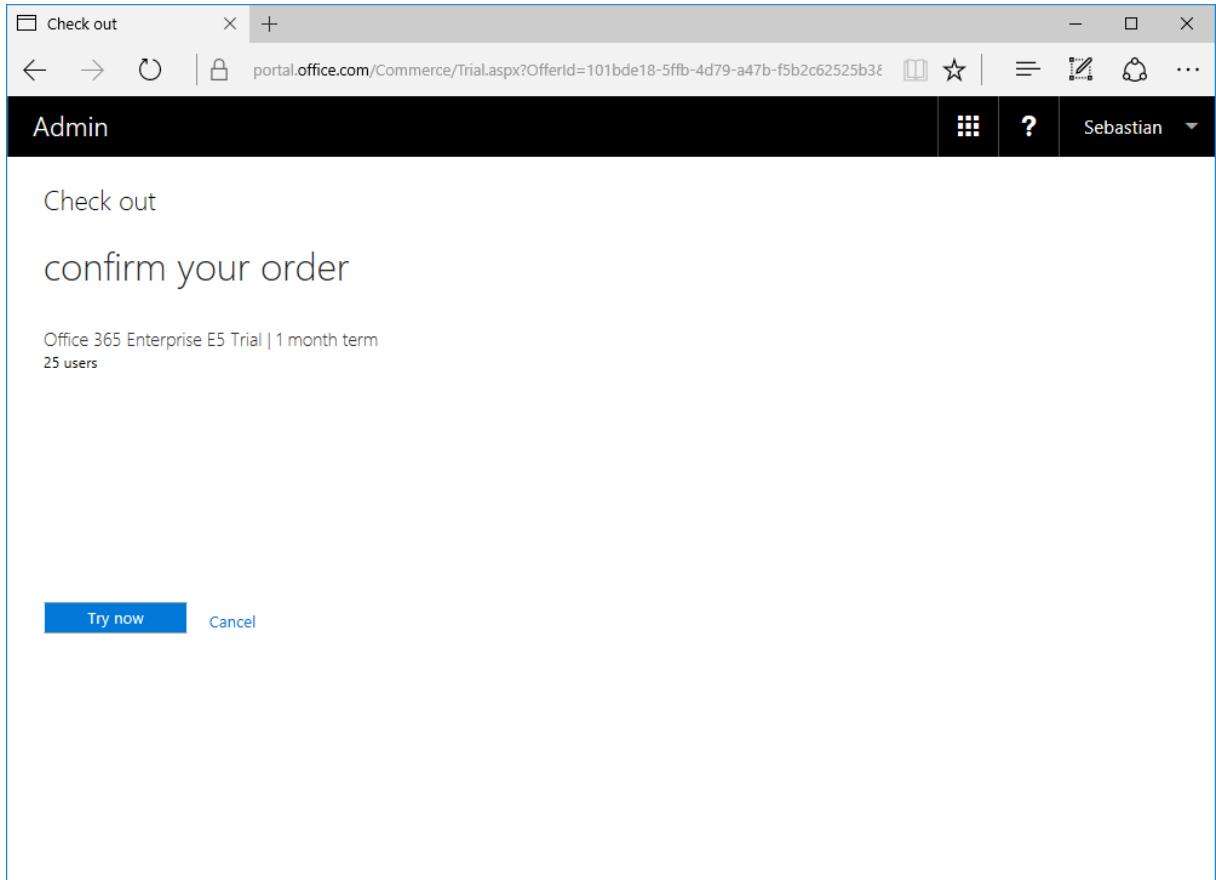
1. On the WTS-12-CLI machine navigate to

<https://go.microsoft.com/fwlink/p/?LinkID=698279&culture=en-US&country=US>

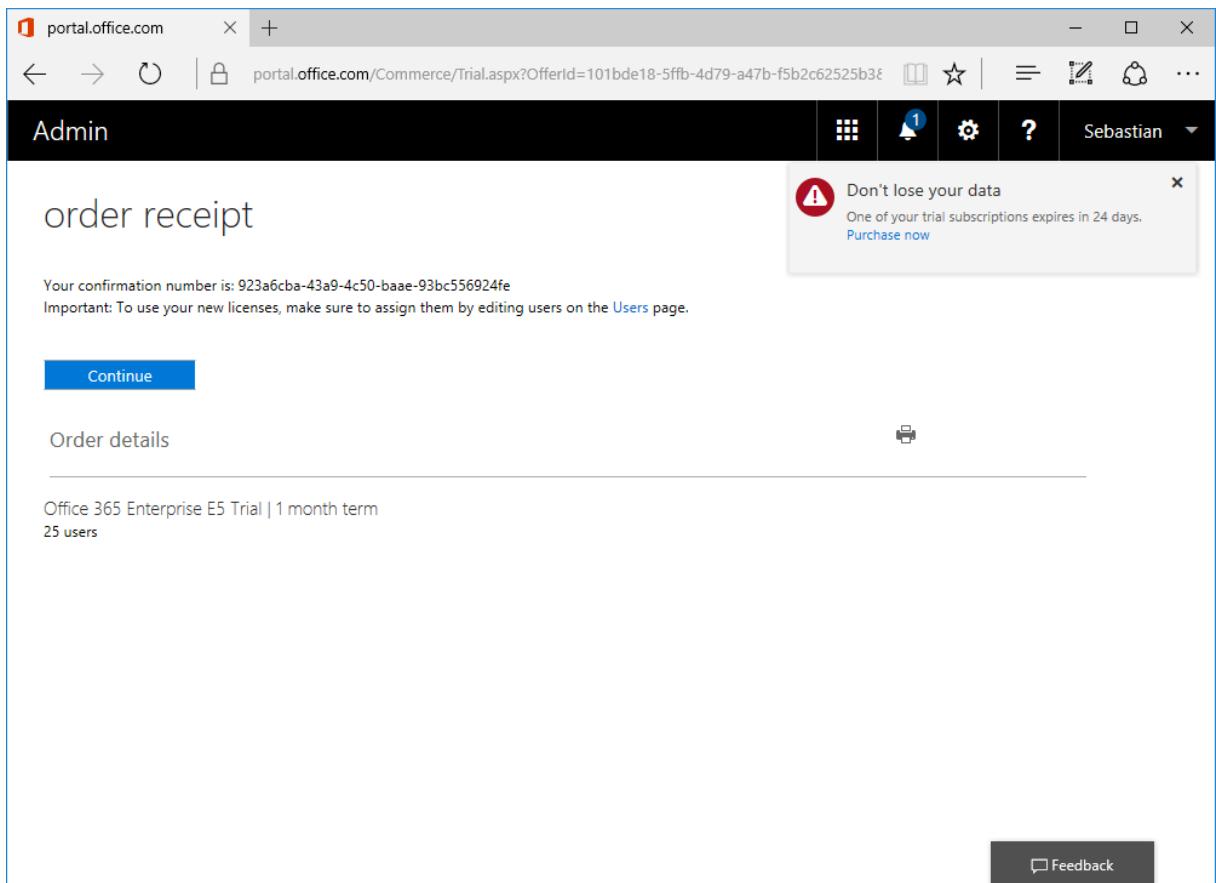
(already as o365 in the Favorites) and click on "Yes, add it to my account".



2. Click on "Try now".



3. Click on "Continue".



4. In the O365 Admin Center Preview navigate to "Users" → "Active Users".

The screenshot shows the Microsoft Admin Center preview interface. The left sidebar has a 'Users' icon selected. Under 'Active users', there are options: 'Add a user', 'Delete a user', 'Edit a user', and 'Reset a password'. On the right, a 'Billing' section displays 'Total balance: None' and 'In trial: Buy now'. A tooltip 'to setup' is shown above the 'Select domain' button.

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

The screenshot shows the 'Active users' list in the Admin Center. It includes columns for 'Display name', 'User name', and 'Status'. Two users are listed: 'Sebastian' (meiforth) and 'Sebastian' (semeif@TimeDemoHOL.onmicrosoft.com). The second user is highlighted with a blue selection bar. Below the list, there are sections for 'User', 'Types of users', and 'Filters'.

6. In the "Product licenses" section click on "Edit".

User name	semeif@TimeDemoHOL.onmicrosoft.com	Edit
Product licenses	Enterprise Mobility Suite	Edit
Group memberships (0)	No groups for the user. Click edit to change group membership.	Edit
Sign-in status	Sign-in allowed	Edit
Roles	Global administrator	Edit
Mailbox permissions	This user doesn't have an Exchange Online license.	Edit
Email forwarding	This user doesn't have an Exchange Online license.	Edit
Email apps	This user doesn't have an Exchange Online license.	Edit
Display name	Sebastian	Edit
Office phone		

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

Location *	United States
Office 365 Enterprise E5	On
25 of 25 licenses available	
Office 365 Advanced Security Management	On
Office 365 Advanced eDiscovery	On
Customer Lockbox	On
Delve Analytics	On
Sway	On
Exchange Online Advanced Threat Protection	On

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.

The screenshot shows the Microsoft Intune Admin workspace. The left sidebar has a blue 'ADMIN' tab selected. The main content area displays the 'Administration Overview' page. It includes sections for 'Account Details' (Name of account: TimeDemoHOL, Status of account: Active, Account hosted on: North America 02), 'Number of devices enrolled: 3', 'Version: 5.0.7000.0', and 'Manage Your Account'. Below this is a 'Cloud Storage Status' section showing 'Space used: 0.05 GB of 20 GB (0.25% used)' and a green checkmark indicating 'No issues. Manage storage'. The right sidebar has links for 'Learn About Administration Overview' and 'Licensing'.

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

The screenshot shows the Microsoft Intune Admin workspace with the 'Administration Overview' page. The left sidebar's 'ADMIN' tab is selected. In the 'Mobile Device Management' section, the 'Microsoft Exchange' item has its 'Set Up Exchange Connection' sub-item highlighted with a blue selection bar. The right sidebar contains 'Learn About' links for 'Administration Overview' and 'Licensing'.

3. Click on "Set Up Service to Service Connector".

The screenshot shows the Microsoft Intune web interface. On the left, there's a navigation sidebar with icons for Groups, Updates, Protection, Alerts, Apps, Licenses, Policy, Reports, and Admin. Under the Admin section, 'Set Up Exchange Connection' is highlighted. The main content area has a title 'Set Up Exchange Connection' and a numbered list of steps:

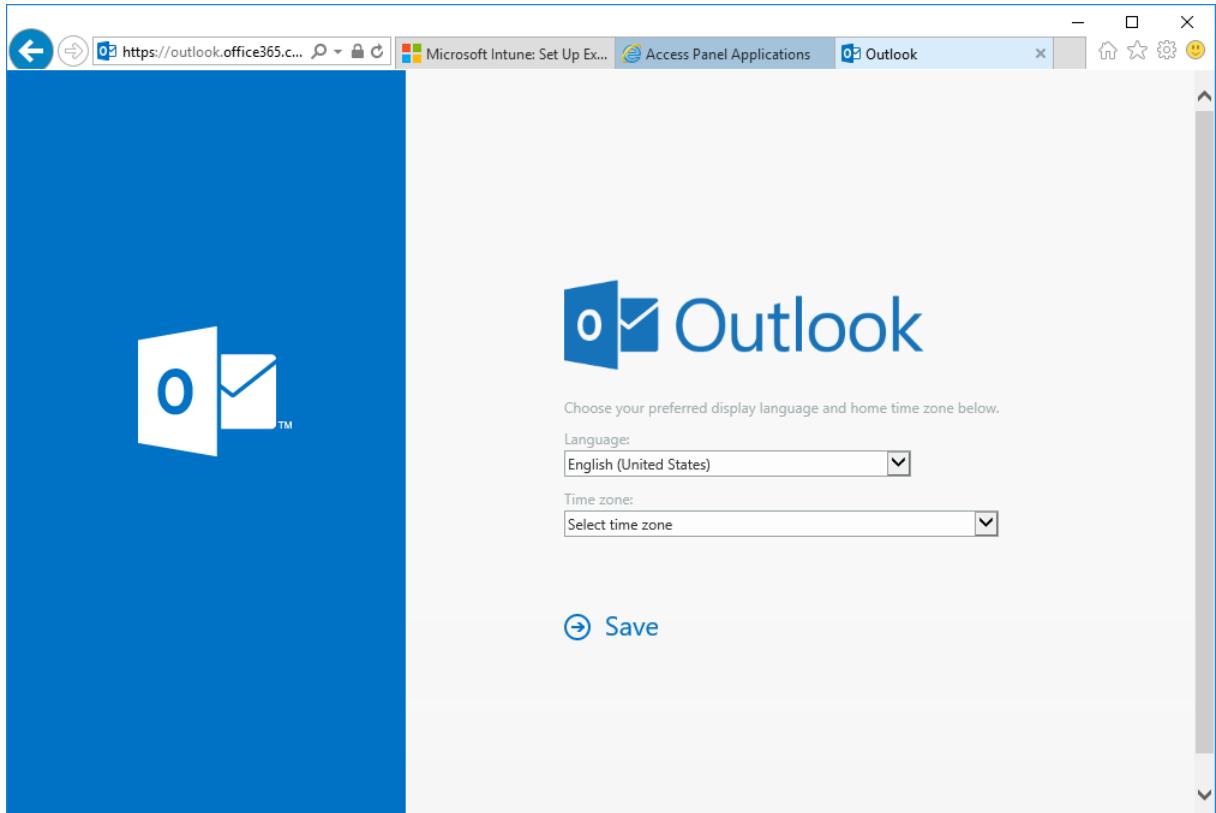
1. Prepare a computer that has access to your Exchange environment and complies with the On-Premises Connector system requirements. [Learn about the system requirements](#)
2. Create a user account in Active Directory that has permission to run the required Exchange cmdlets. For Hosted Exchange environments, either create a user in Active Directory or MSDOS that has permission to run the required Exchange cmdlets, or use an existing tenant administrator that has these permissions. [Learn about the Exchange cmdlet requirements](#)
3. Download the On-Premises Connector software, extracting the contents into a secure location on the computer you prepared. Install and configure the On-Premises Connector using the user account from step 2.

A 'Download On-Premises Connector' button is visible. Below this, a section titled 'Microsoft Intune Service to Service Connector for Hosted Exchange' contains a link 'Click Set Up Service to Service Connector to set up a connection to your Exchange hosted environment. An Office 365 account that has an Exchange 2013 tenant is required.' and a 'Set Up Service to Service Connector' button.

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".

The screenshot shows the Microsoft Azure Access Panel Applications interface. At the top, there are tabs for 'applications', 'groups', 'approvals', and 'profile'. A search bar is at the top right. Below, there's a message 'New look coming soon!' and a 'Try it out' button. Two application tiles are shown: 'Office 365 SharePoint Online' and 'Office 365 Exchange Online'. The 'Office 365 Exchange Online' tile is highlighted with a white border. At the bottom, it says 'Showing 2 of 2'.

- Fill out the form on the next page and click "Save".



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

The screenshot shows the Microsoft Intune interface for setting up an Exchange connection. On the left, there is a sidebar with icons for GROUPS, UPDATES, PROTECTION, ALERTS, APPS, LICENSES, POLICY, and REPORTS. The main content area is titled "Set Up Exchange Connection" and describes the Microsoft Intune On-Premises Connector for On-Premises or Hosted Exchange. It lists three steps: 1. Prepare a computer that has access to your Exchange environment and complies with the On-Premises Connector system requirements. 2. Create a user account* in Active Directory that has permission to run the required Exchange cmdlets. For Hosted Exchange, this user must be a host administrator that has permission to run the required Exchange cmdlets. 3. Download the On-Premises Connector and install it on the computer that will run the On-Premises Connector using the provided setup file. A "Download On-Premises Connector" button is visible.

A modal dialog box titled "Set Up Service To Service Connector" is overlaid on the page. It contains the following text: "To work correctly, the Service to Service Connector must be set up by a user with Exchange admin rights. Microsoft Intune will use the email address of the currently logged in user to set the connection. To Specify another account, log out and log in again with the desired account." Below this, it says "Your hosted Exchange connection will be configured using semeif@TimeDemoHOL.onmicrosoft.com. Would you like to continue?". At the bottom of the dialog are "OK" and "Cancel" buttons.

At the bottom of the main page, there is a link "Set Up Service to Service Connector". The footer of the page includes the Microsoft logo, copyright information (© 2016 Microsoft. All rights reserved), and links for Privacy & Cookies and Feedback. The status bar at the bottom right shows "Remote Tasks (2)".

8. Now the connector gets validated against Exchange Online.

The screenshot shows the Microsoft Intune Administration interface. On the left, there's a navigation sidebar with icons for Groups, Updates, Protection, Alerts, Apps, Licenses, Policy, Reports, and Admin. The 'Admin' icon is highlighted. The main content area is titled 'Microsoft Exchange Mobile Device Management'. It shows a warning message: 'Microsoft Exchange' with a yellow exclamation mark icon, stating 'Connection pending validation of hosted Exchange account. No sync has been run.' Below this, there's a blue link 'Run quick sync' with an info icon. To the right, there's a 'Tasks' section with links for Run Quick Sync, Run Full Sync, Delete Connection, and Change Hosted Exchange. Below that is an 'Exchange Connection Information' section with details: Exchange organization: TimeDemoHOL.onmicrosoft.com, Exchange Connector type: Microsoft Intune Service to Service Connector for Hosted Exchange, and Hosted Exchange Account: semeif@TimeDemoHOL.onmicrosoft.com. There are also 'Learn About' links for Mobile Device Management and Synchronizing Mobile.

9. Click on "Run quick sync".

This screenshot is identical to the previous one, showing the Microsoft Intune Administration interface. The 'Run quick sync' link in the 'Microsoft Exchange' section is now highlighted in green, indicating it has been clicked. The rest of the interface remains the same, including the warning message, tasks, and exchange connection information.

Create a device compliance policy

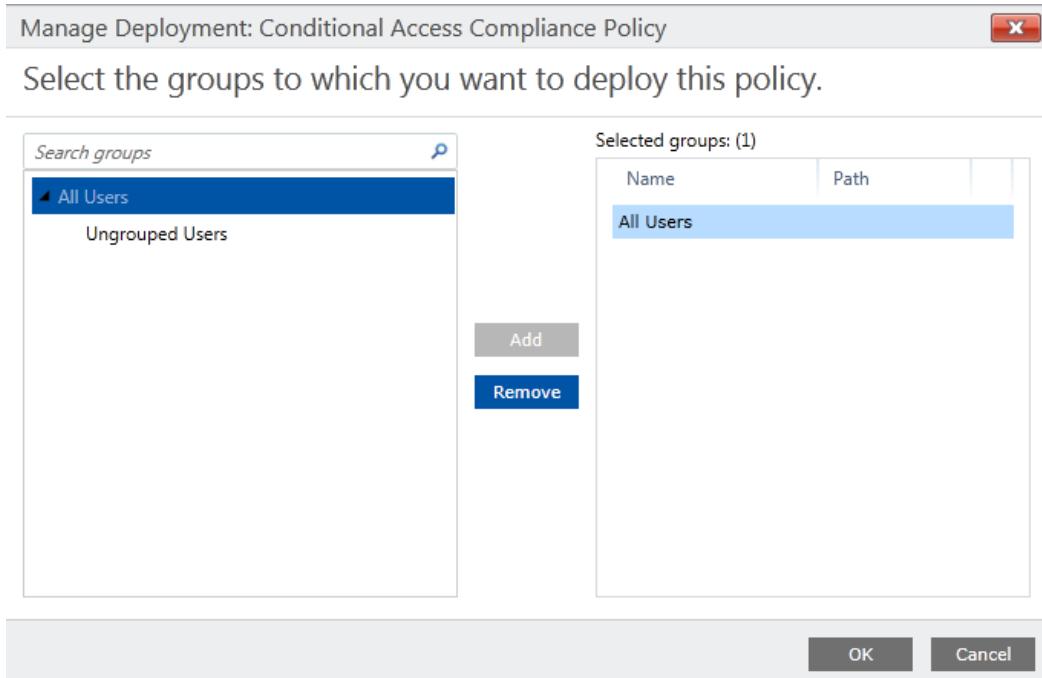
1. Go to the "Policy" workspace → "Compliance Policies" and click on "Add...".

The screenshot shows the Microsoft Intune Policy workspace. On the left, there's a vertical navigation bar with icons for GROUPS, UPDATES, PROTECTION, ALERTS, APPS, LICENSES, POLICY (which is selected), REPORTS, and ADMIN. The main area has a title 'Policy' and a sidebar with 'Overview', 'Policy Conflicts', 'Configuration Policies', and 'Compliance Policies' (which is selected). Below this is a section titled 'Conditional Access' with options like Dynamics CRM Online Policy, Exchange Online Policy, Exchange On-premises Policy, SharePoint Online Policy, Skype for Business Online Policy, Exchange ActiveSync, Corporate Device Enrollment, and Terms and Conditions. To the right is a table titled 'Policies (0)' with columns 'Name' and 'Last Updated'. A message 'No items to show' is displayed. At the bottom, there's a footer with Microsoft branding and a 'Remote Tasks (2)' link.

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.

The screenshot shows the 'Create Policy: Conditional Access Compliance Policy' dialog. It has tabs for 'General' (selected) and 'System Security'. Under 'General', there's a 'Name' field with 'Conditional Access Compliance Policy' and a 'Description' field with 'Conditional Access Compliance Policy by semeif'. A note says 'Some settings in this policy are not configured. If you want to configure all settings, click this switch.' with a link 'Learn about configuring policy settings'. Under 'System Security', there's a 'Password' field. At the bottom are 'Save Policy' and 'Cancel' buttons. The background shows the same Microsoft Intune Policy workspace as the previous screenshot.

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.

	Model	Management Channel	AAD Registered	Compliant	EAS Activated	EAS Activation ID
Virtual Machine	Managed by Microsoft Intune	Yes	Yes	No		
Virtual Machine	Managed by Microsoft Intune	Yes	Yes	No		

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".

Microsoft Intune

Policy

- Overview
- Policy Conflicts
- Configuration Policies
- Compliance Policies
- Conditional Access
 - Dynamics CRM Online Policy
 - Exchange Online Policy** (selected)
 - Exchange On-premises Policy
 - SharePoint Online Policy
 - Skype for Business Online Policy
 - Exchange ActiveSync
 - Corporate Device Enrollment
 - Terms and Conditions

Exchange Online Policy

Use conditional access to help secure access to Exchange Online, so that only managed and compliant devices can access email. To create a compliance policy for devices, go to the Compliance Policies node.

Enable conditional access policy

Learn About

- Configure Exchange access by platform
- Learn which email clients will be blocked

Save **Cancel**

Microsoft Intune

Policy

- Overview
- Policy Conflicts
- Configuration Policies
- Compliance Policies
- Conditional Access
 - Dynamics CRM Online Policy
 - Exchange Online Policy** (selected)
 - Exchange On-premises Policy
 - SharePoint Online Policy
 - Skype for Business Online Policy
 - Exchange ActiveSync
 - Corporate Device Enrollment
 - Terms and Conditions

Exchange Online Policy

Use conditional access to help secure access to Exchange Online, so that only managed and compliant devices can access email. To create a compliance policy for devices, go to the Compliance Policies node.

Enable conditional access policy

Application access

- Outlook and other apps that use modern authentication
 - iOS
 - Android
- Outlook Web Access (OWA)
 - Block non-compliant devices on same platforms as Outlook
 - 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

Save **Cancel**

The screenshot shows the Microsoft Intune web interface. The left sidebar has a 'Policy' icon highlighted. The main content area is titled 'Policy' and contains the following sections:

- Overview**
- Policy Conflicts**
- Configuration Policies**
- Compliance Policies**
- Conditional Access**
 - Dynamics CRM Online Policy
 - Exchange Online Policy** (selected)
 - Exchange On-premises Policy
 - SharePoint Online Policy
 - Skype for Business Online Policy
 - Exchange ActiveSync
 - Corporate Device Enrollment
 - Terms and Conditions

Platform Configuration (checkboxes):

- iOS
- Android
- Outlook Web Access (OWA)**
- Block non-compliant devices on same platforms as Outlook
- Exchange ActiveSync apps that use basic authentication
- 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

Buttons at the bottom right: Save, Cancel.

Page footer: Microsoft © 2016 Microsoft. All rights reserved Privacy & Cookies Feedback Remote Tasks (2)

5.

App White-/Blacklisting (Optional)

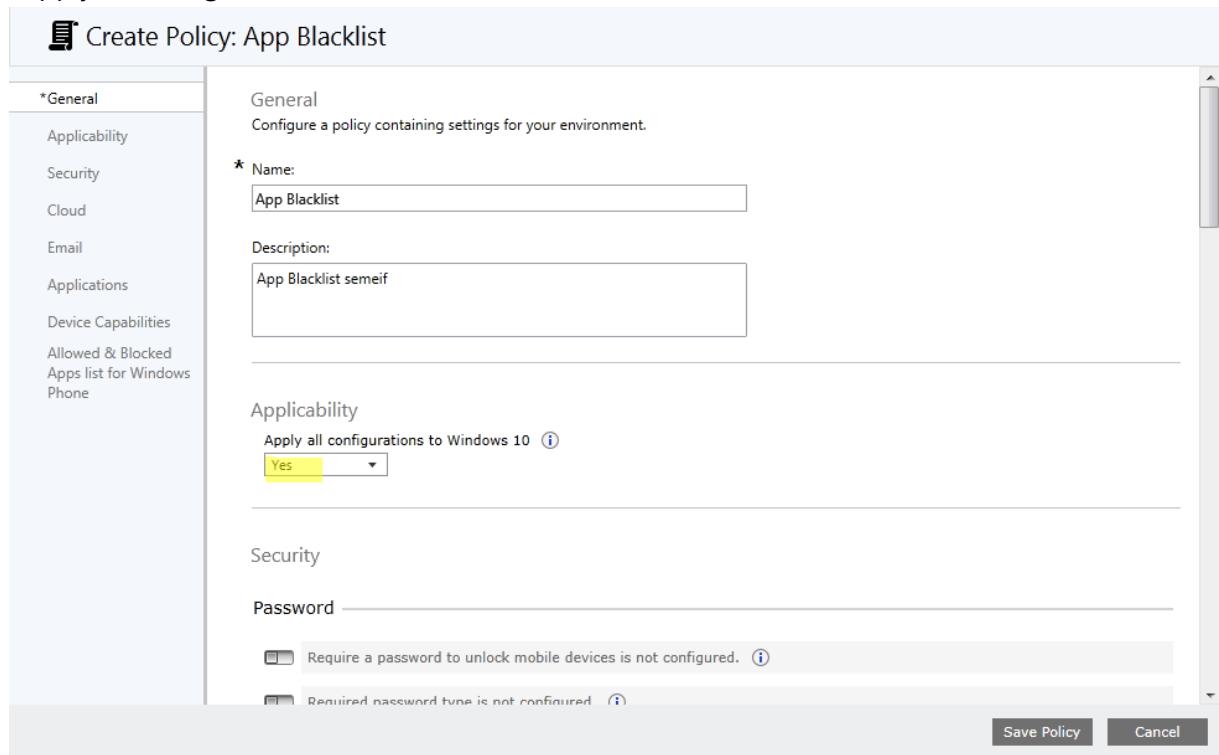
1. On WTS-12-CLI.
2. Open <http://manage.microsoft.com>
3. Log on with the Global Administrator created in the Azure Active Directory section.
Navigate to the "Policy" workspace and click on "Add Policy".

The screenshot shows the Microsoft Intune Policy workspace. The left sidebar has a 'POLICY' icon selected. The main area displays 'Policy Status' with 1 device with settings errors. A prominent blue button labeled 'Add Policy' with a plus sign is visible, along with a description: 'Control features and settings on computers and mobile devices.' Below it are sections for 'REPORTS' (View Noncompliant Apps Report) and 'LEARN ABOUT' (Managing Policies, Interaction with Group Policy). The bottom of the screen shows standard navigation links and a copyright notice.

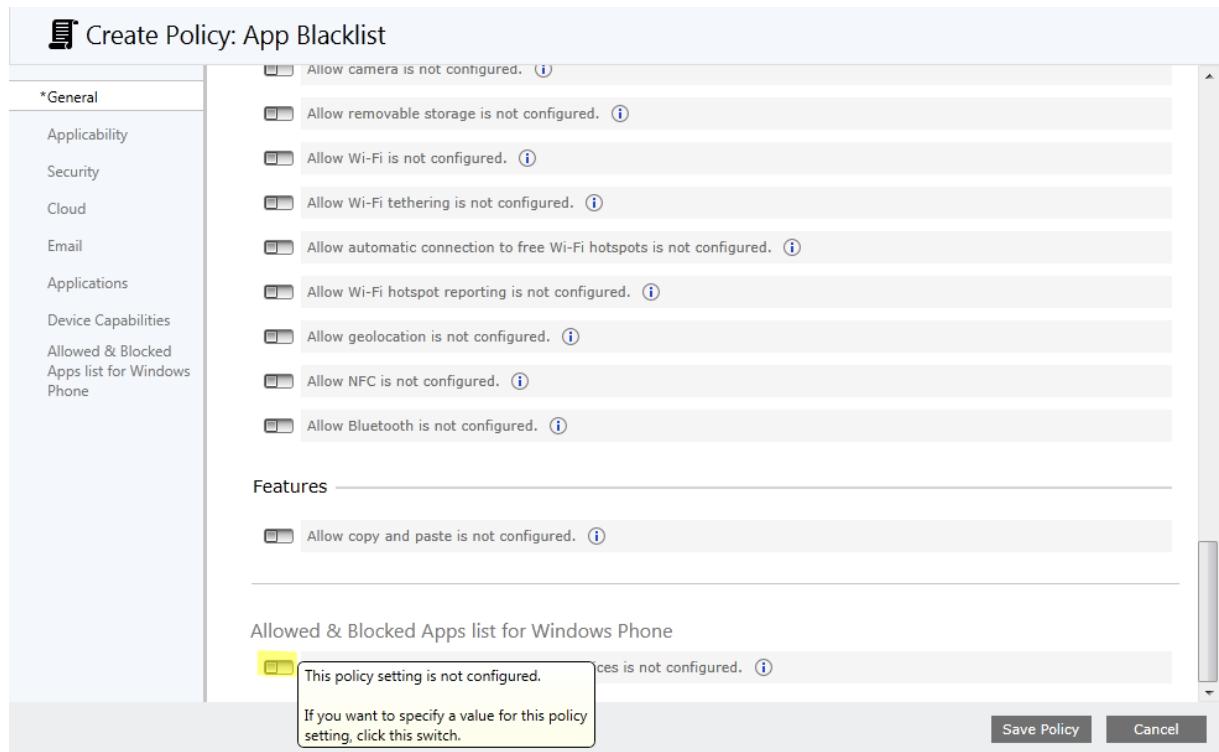
4. Expand Windows and select "General Configuration (Windows Phone 8.1 and later)" and click on "Create Policy".

The screenshot shows the 'Create a New Policy' dialog. The title bar says 'Create a New Policy'. The main area is titled 'Select a template for the new policy' with a sub-instruction: 'Select the template that includes the settings you want to manage with the new policy. You use a template to create a policy, and then you can configure the settings in that policy. You cannot change a template.' A list of templates is shown, with 'General Configuration (Windows Phone 8.1 and later)' highlighted. To the right, a sidebar provides instructions: 'Select a policy template from these categories to manage settings on your managed computers, mobile devices, and for software that you deploy using Microsoft Intune.' At the bottom are 'Create Policy' and 'Cancel' buttons.

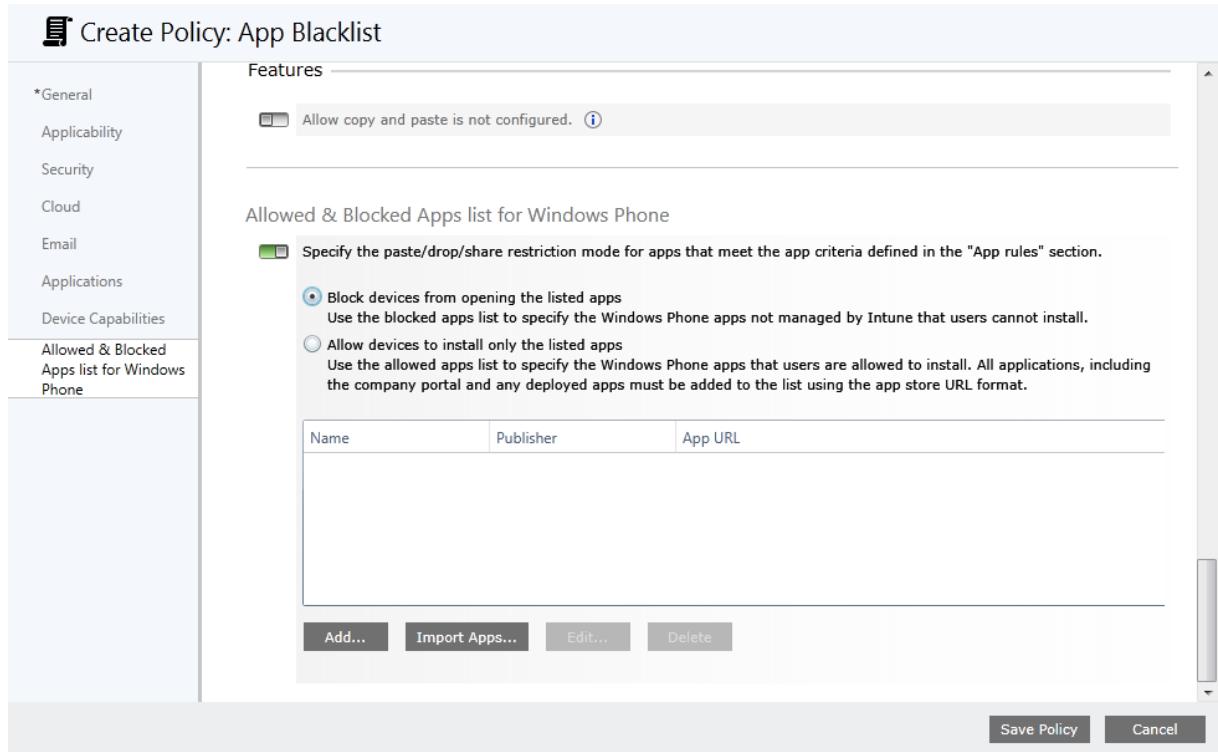
5. Enter a name and description for the policy and make shure that under "Applicability" "Apply all configurations to windows 10" is set to "Yes".



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...".

A screenshot of the "Create Policy: App Blacklist" dialog box. The left sidebar shows navigation options: *General, Applicability, Security, Cloud, Email, Applications, Device Capabilities, and Allowed & Blocked Apps list for Windows Phone. The main area is titled "Features" and contains a note: "Allow copy and paste is not configured." Below this is a section titled "Allowed & Blocked Apps list for Windows Phone" with a note: "Specify the paste/drop/share restriction mode for apps that meet the app criteria defined in the 'App rules' section." Two radio button options are shown: "Block devices from opening the listed apps" (selected) and "Allow devices to install only the listed apps". A table below lists apps with columns for Name, Publisher, and App URL. At the bottom are buttons for Add..., Import Apps..., Edit..., Delete..., Save Policy, and Cancel.

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/9wzdngrfjb13>

Add App to blocked list X

*Name:	Fresh Paint
Publisher:	Microsoft Corporation
*App URL :	www.microsoft.com/en-us/store/apps/fresh-paint/9wzdngrfjb13

[Learn more about allowing and blocking apps.](#)

OK Cancel

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/9wzdngrdfwbs>

Name: Twitter

Publisher: Twitter Inc.

App URL: <https://www.microsoft.com/en-us/store/apps/twitter/9wzdngrfj140>

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”.

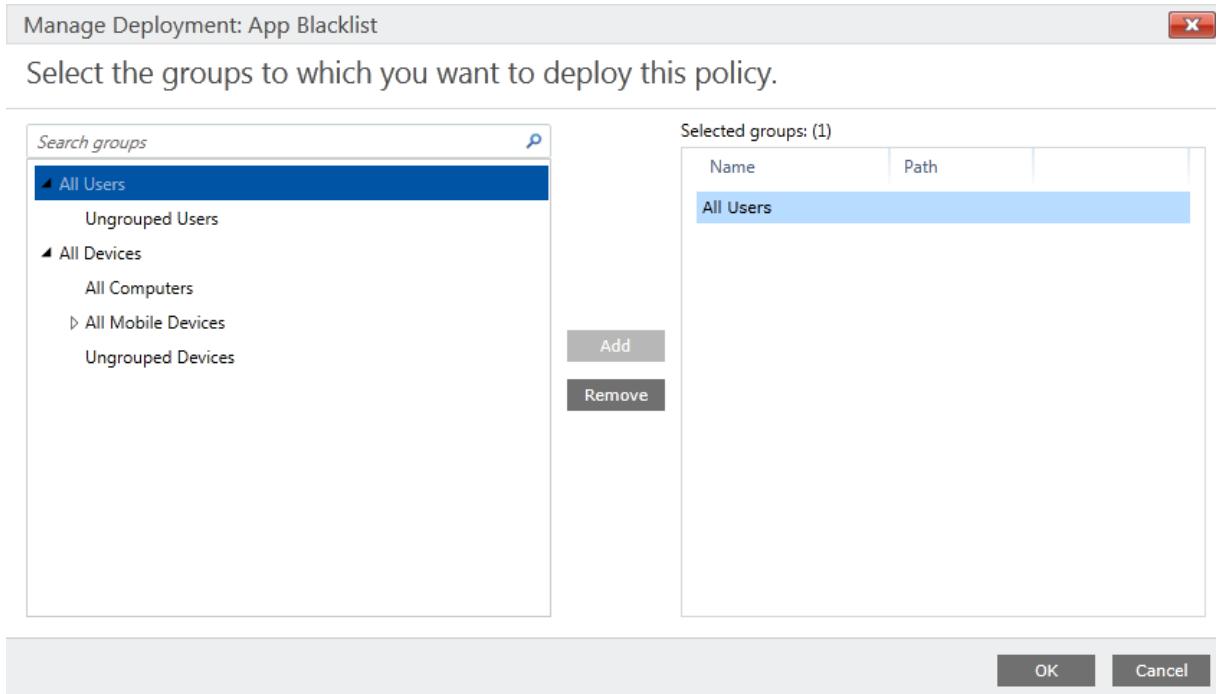
Deploy Policy: App Blacklist X

Do you want to deploy this policy now?

This policy has been saved but has not yet been deployed. Deploying this policy allows you to send it to the devices or users in the groups that you select.

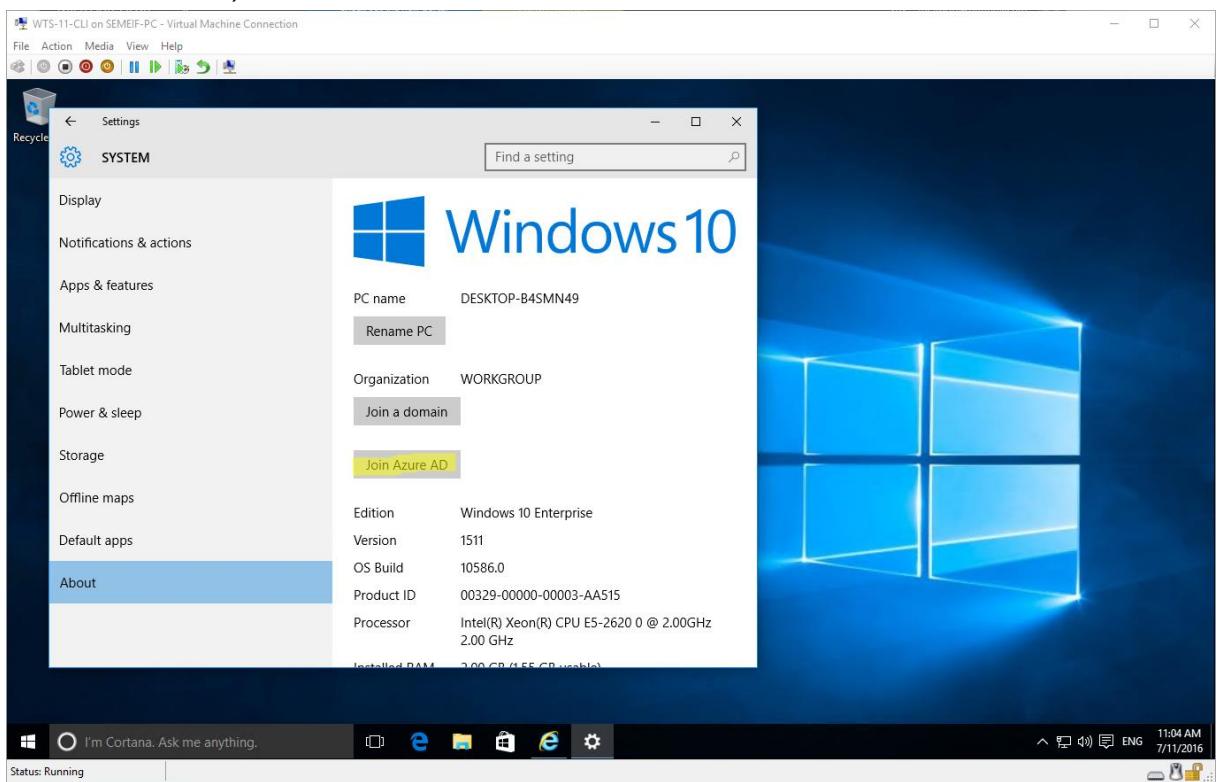
Yes No

11. Add the "All Users" group and click "OK".

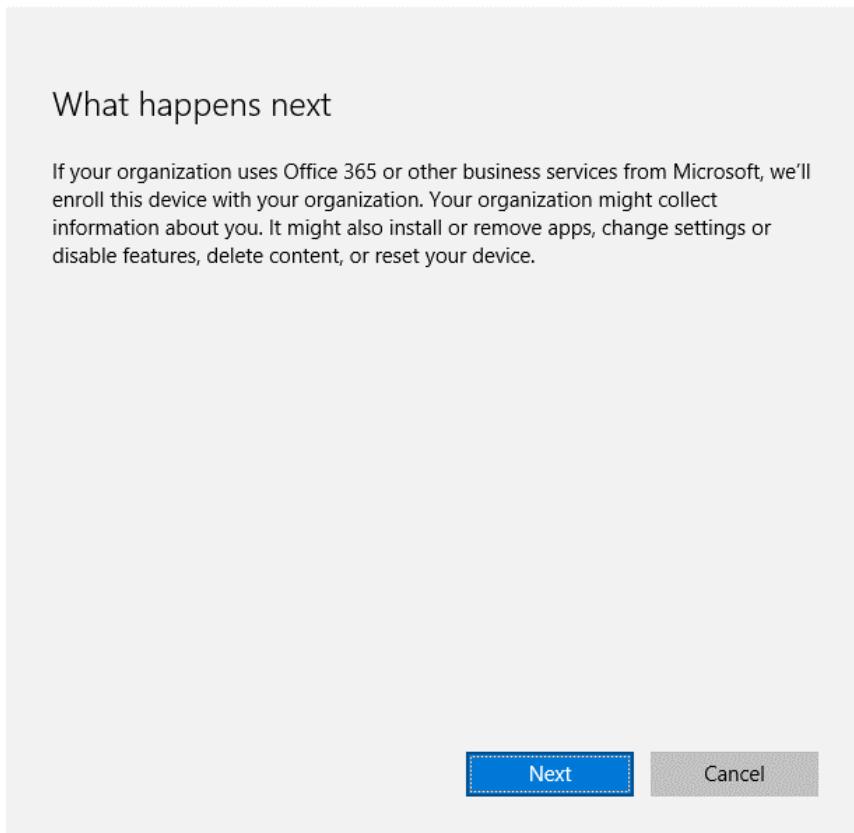


Azure Active Directory Domain join

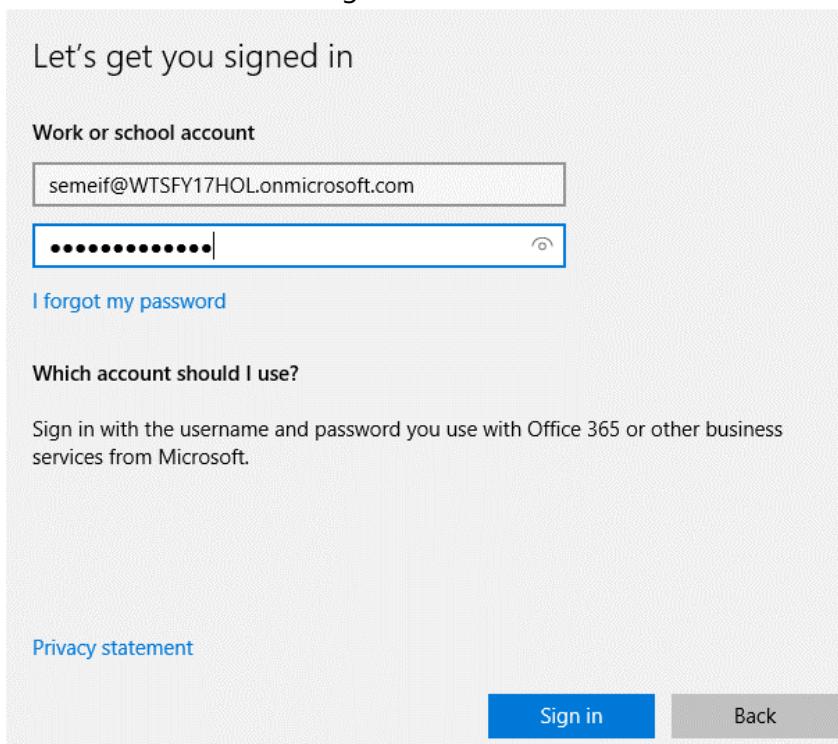
1. On the Client Lab machine WTS-12-CLI click on Start → Settings → System → About → Join Azure AD. (This sometimes takes **multiple attempts!!!** Cause of NAT→NAT→NAT)



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" screen review the information and click "Join".

Make sure this is your organization

Make sure this is your organization

If you continue, system policies might be turned on or other changes might be made to your PC.
Is this the right organization?

Connecting to: WTSFY17HOL.onmicrosoft.com
User name: semeif@WTSFY17HOL.onmicrosoft.com
User type: Administrator

Cancel

Join

5. On the "All finished!" screen click "Finish".

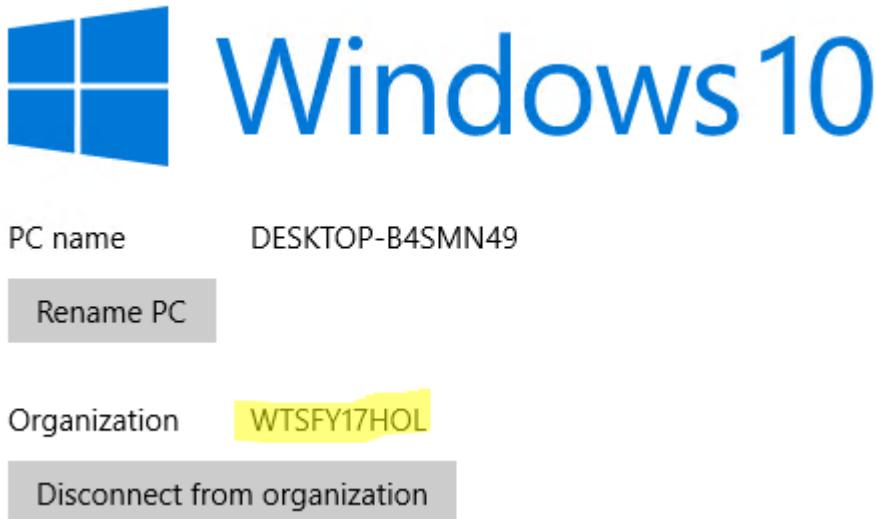
All finished!

Your device is now joined to your organization in Azure AD.

Finish

Verify Azure AD Connection

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



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

Enroll in to device management

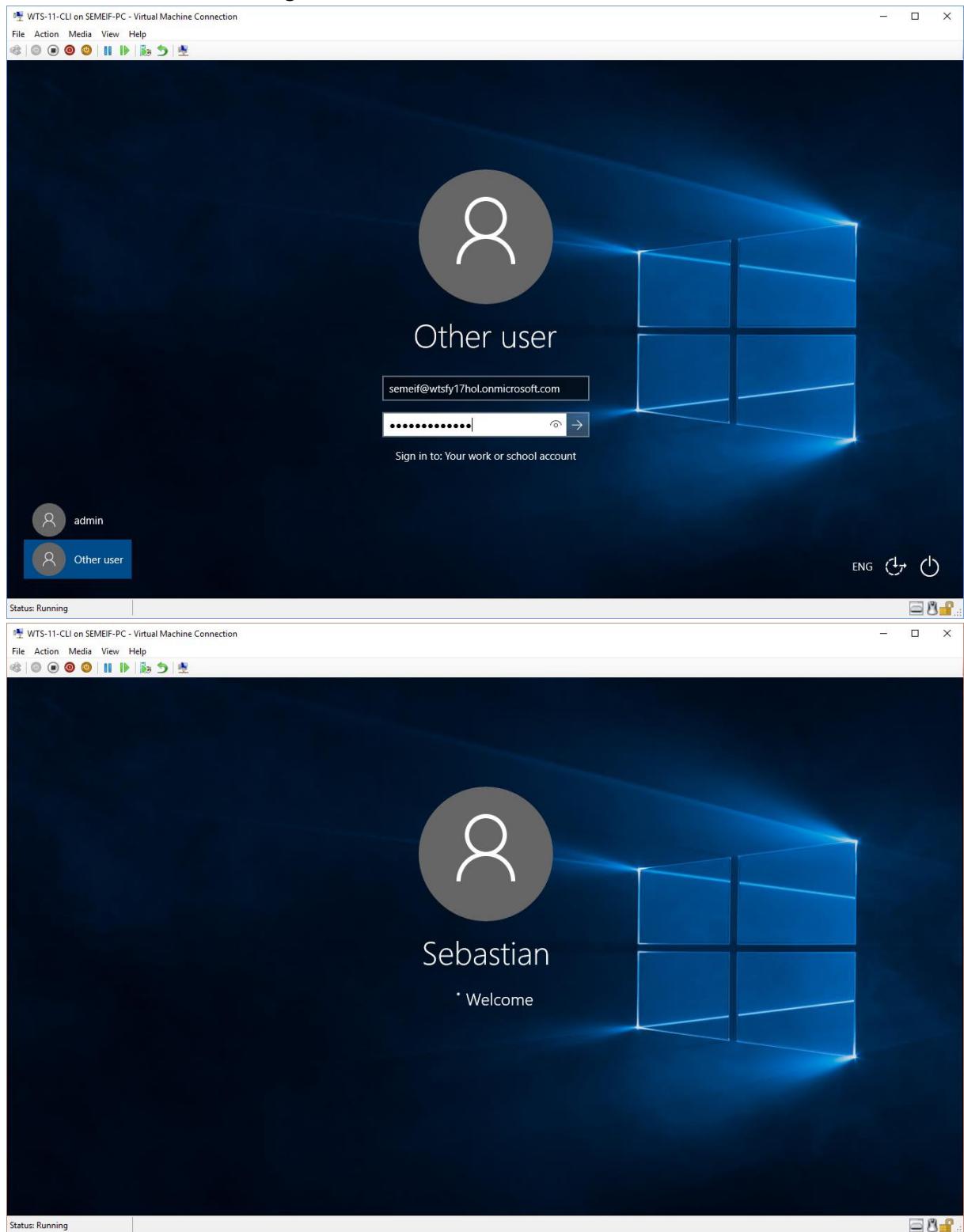
Select this option if your support person told you to enroll in to device management (MDM).



WTSFY17HOL

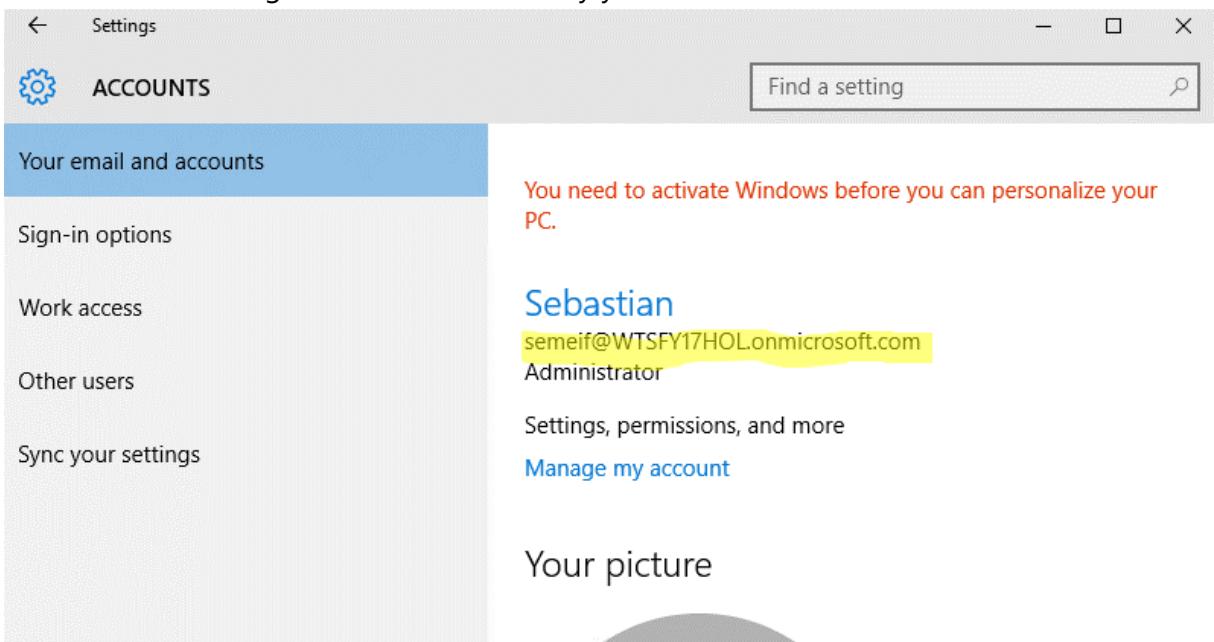
semeif@WTSFY17HOL.onmicrosoft.com

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 prompt with the command "whoami".

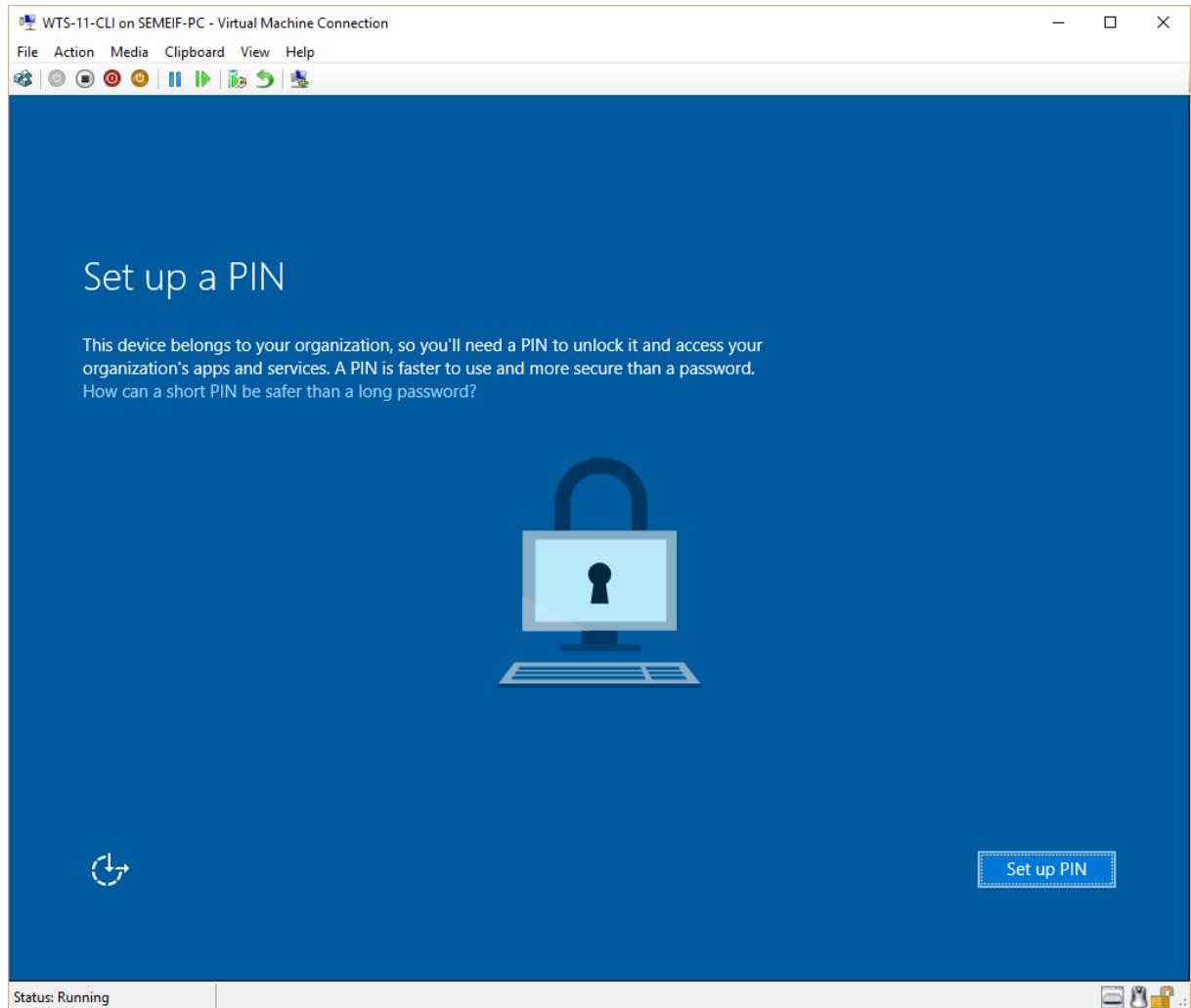
```
cmd: Command Prompt
Microsoft Windows [Version 10.0.10586]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Sebastian>whoami
azuread\sebastian

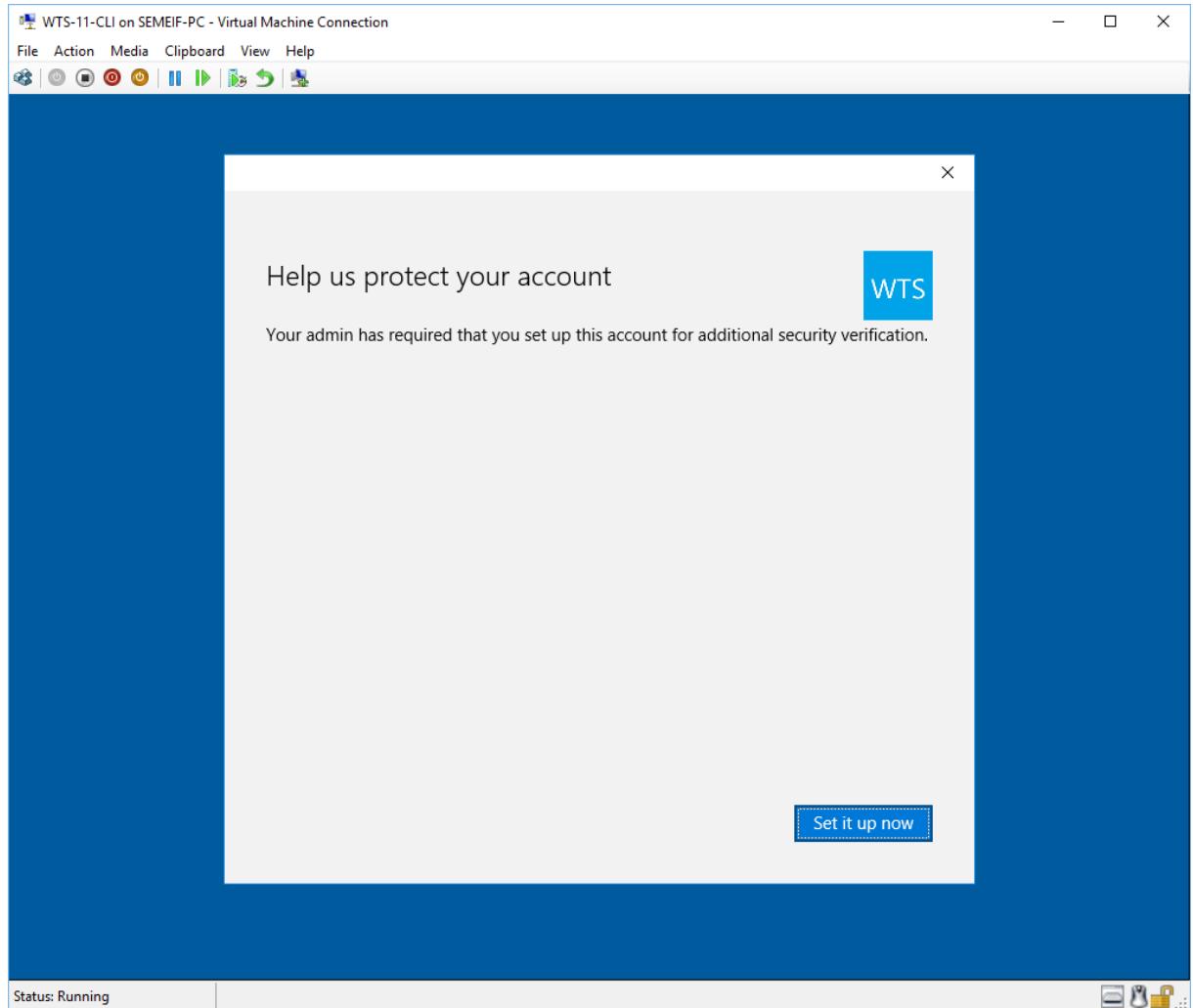
C:\Users\Sebastian>
```

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)

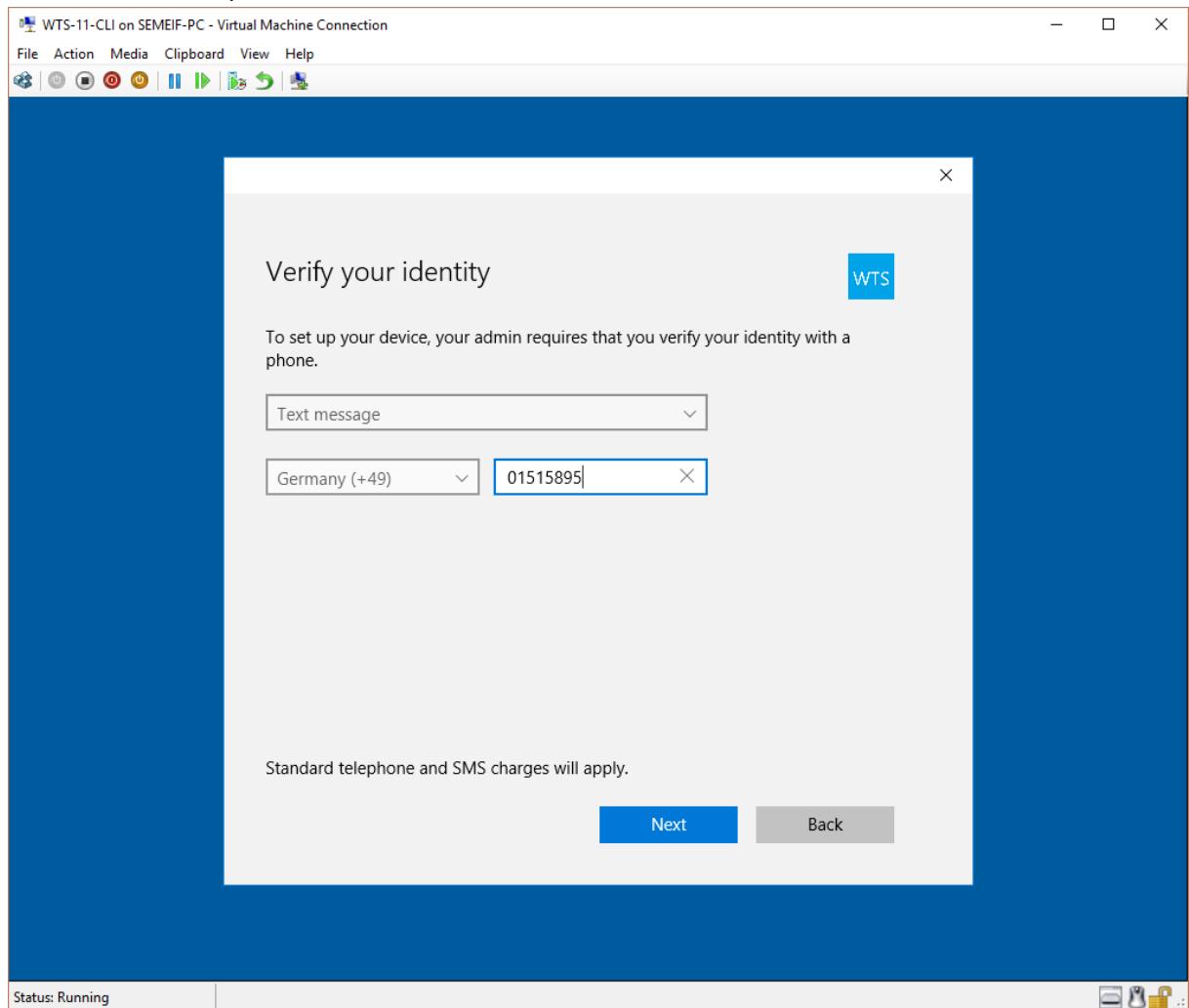
1. When you log on the machine you will get the "Set up a pin" dialogue. Click on "Set-up PIN".



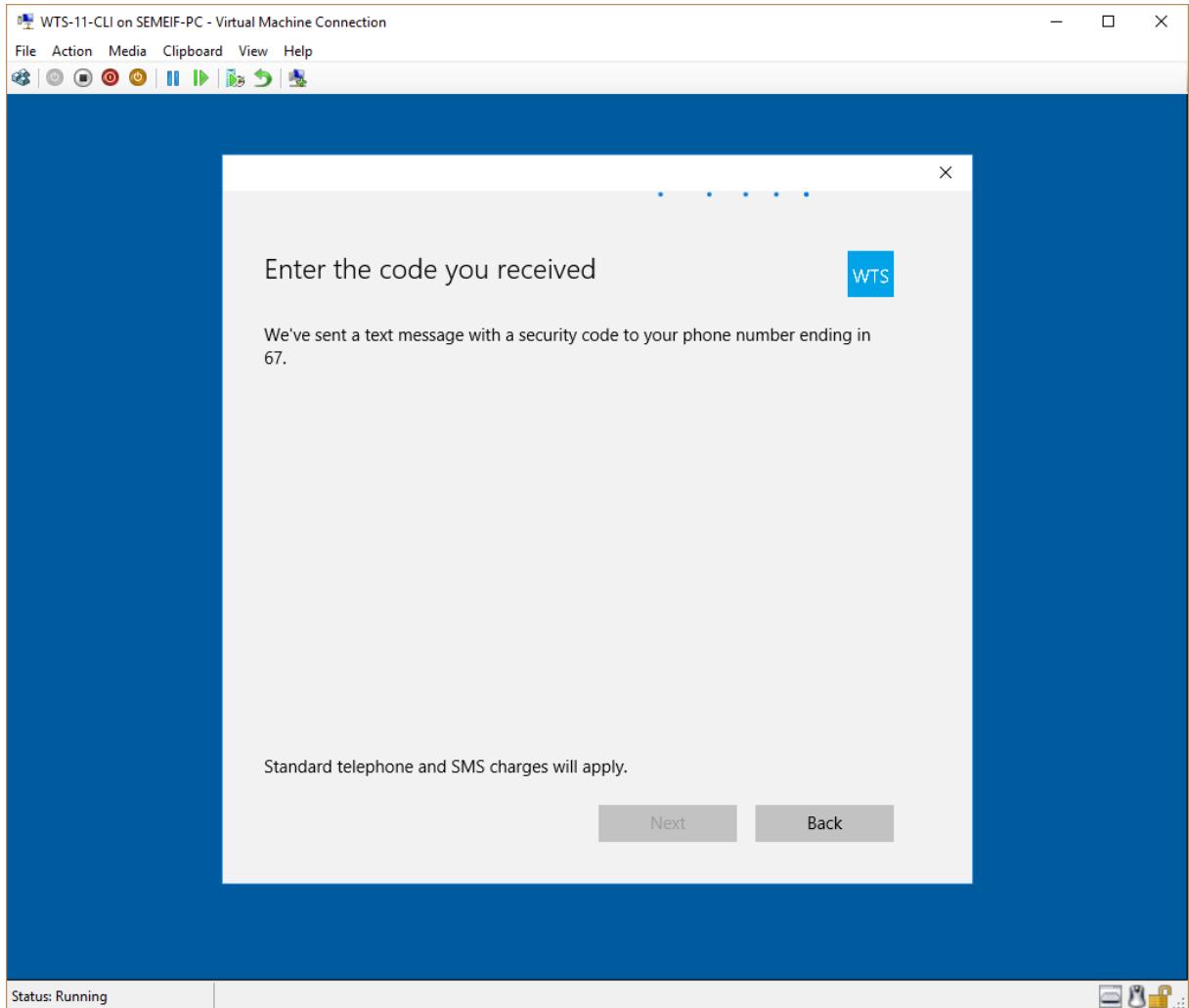
2. On the „Help us protect your account“ screen click „Set it up now“.



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"

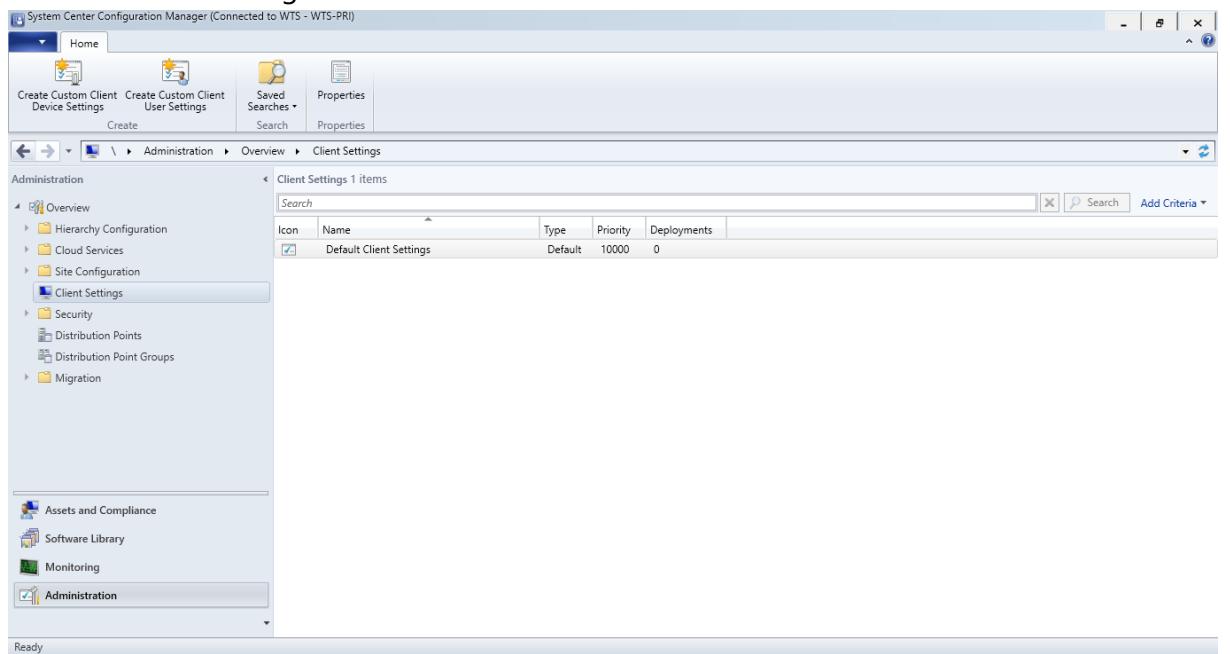


5. Now you can set-up your PIN.

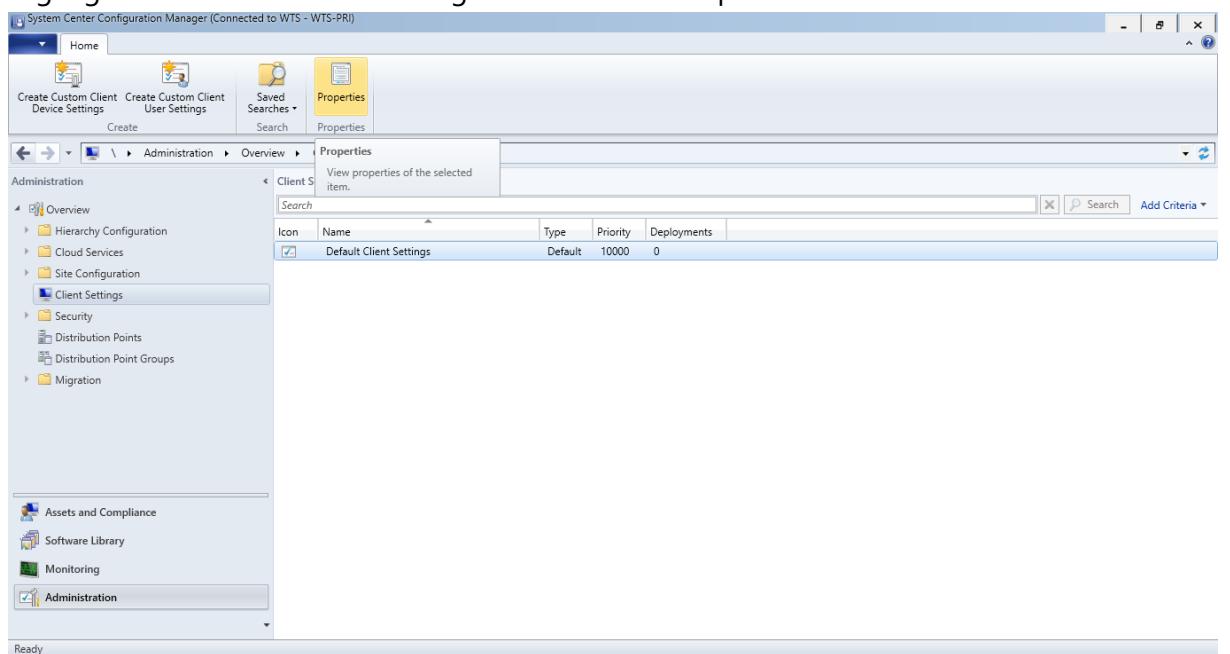
2. Lab guide part 2 – Security with Configuration Manager

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".

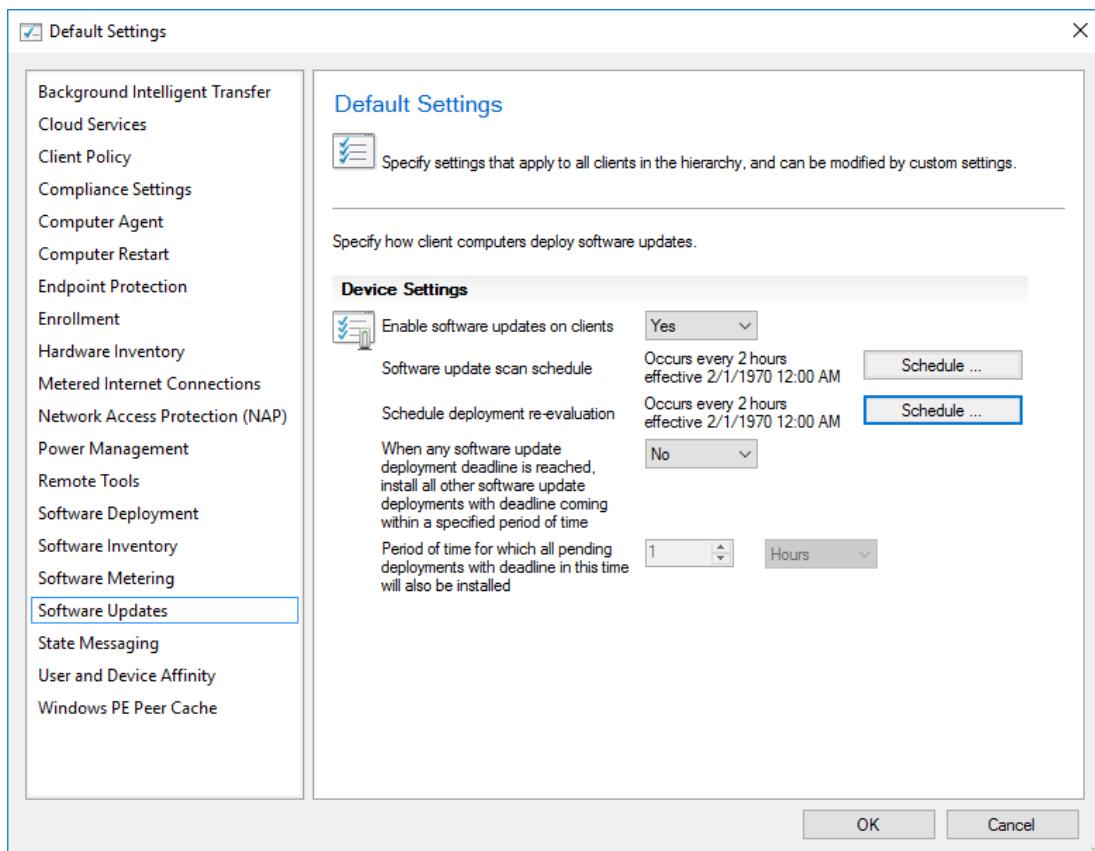


3. Highlight the "Default client Settings" and click on "Properties".

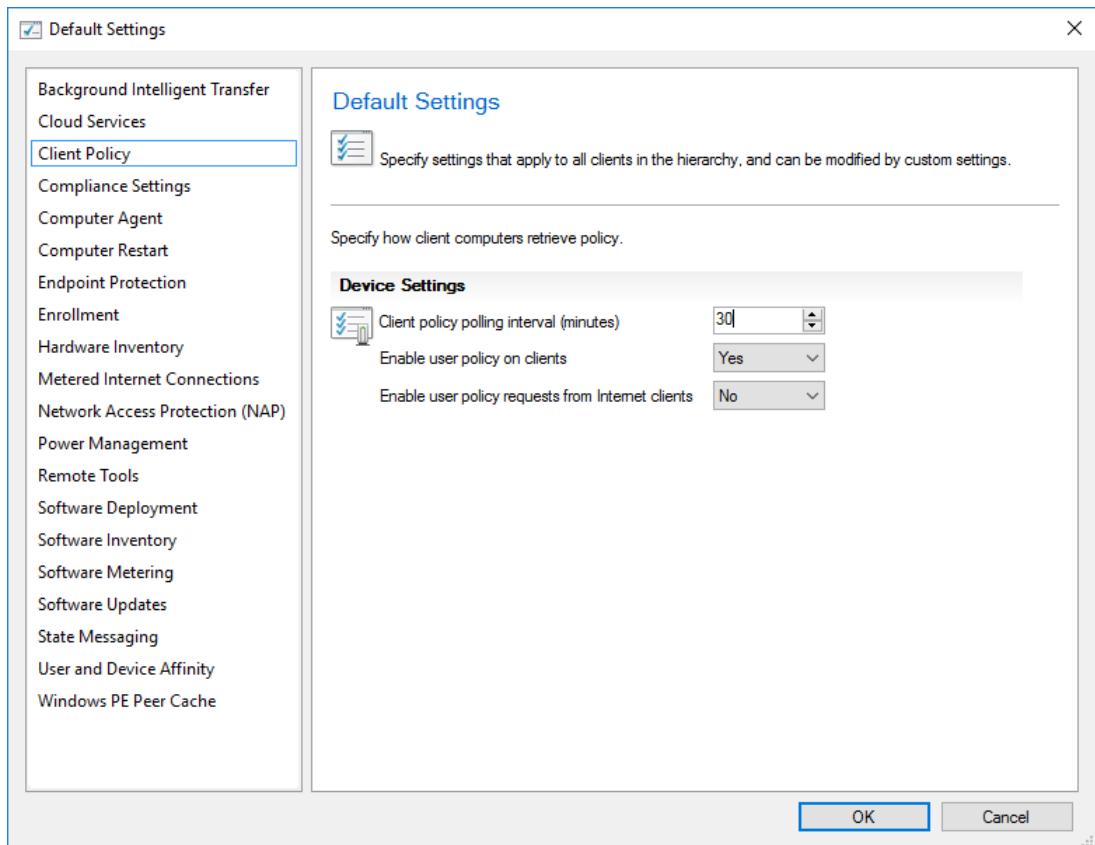


4. Edit the Client Settings as the following:

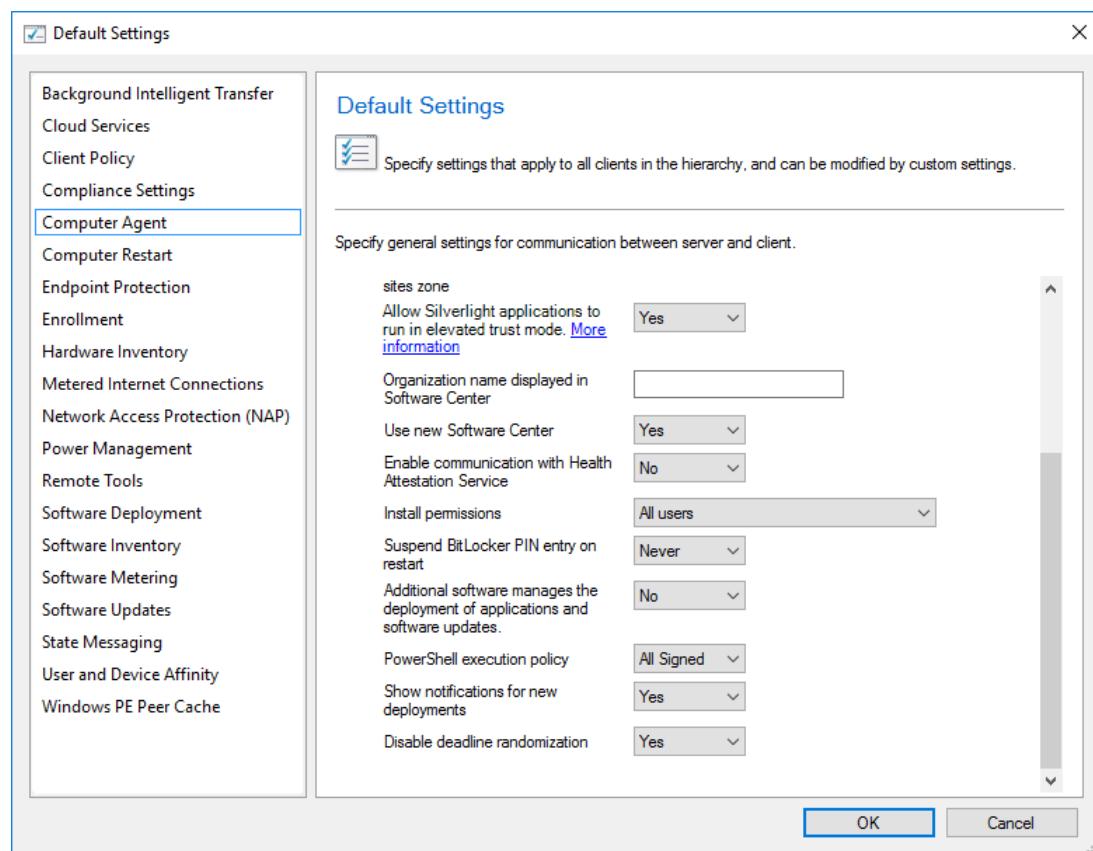
Software updates schedule



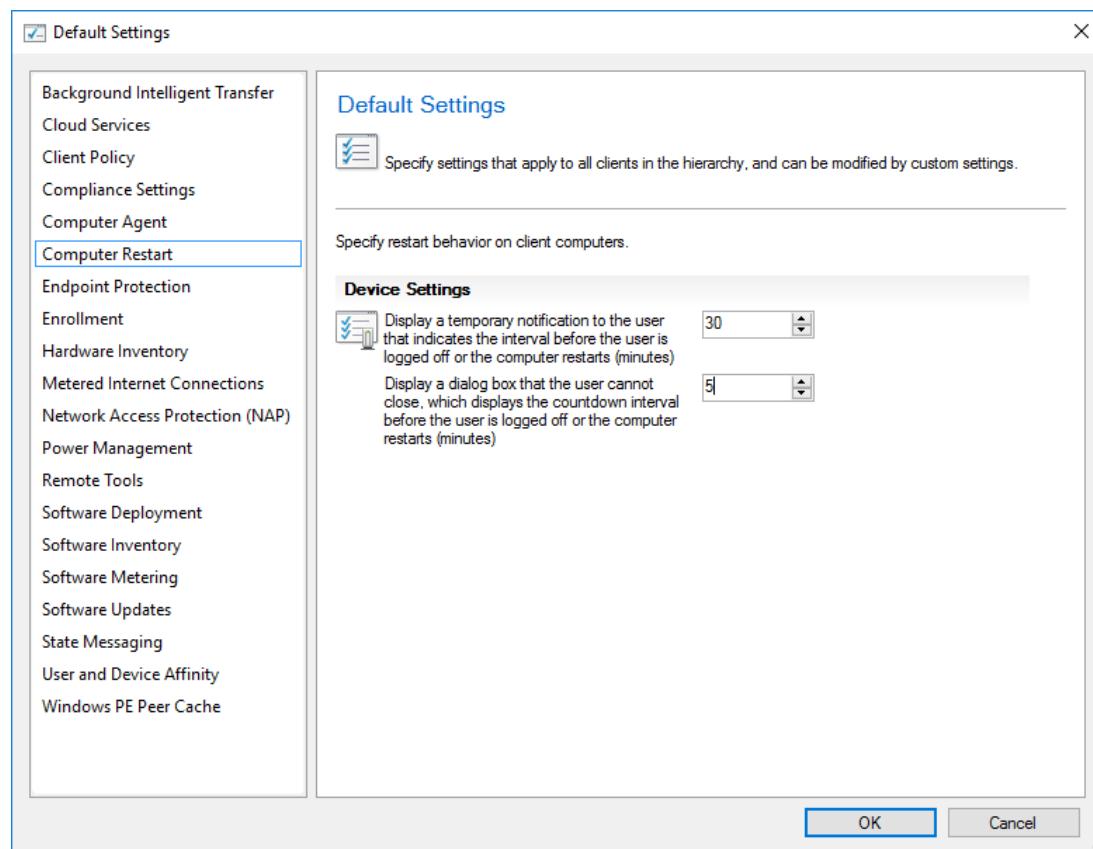
Client Policy



Default settings



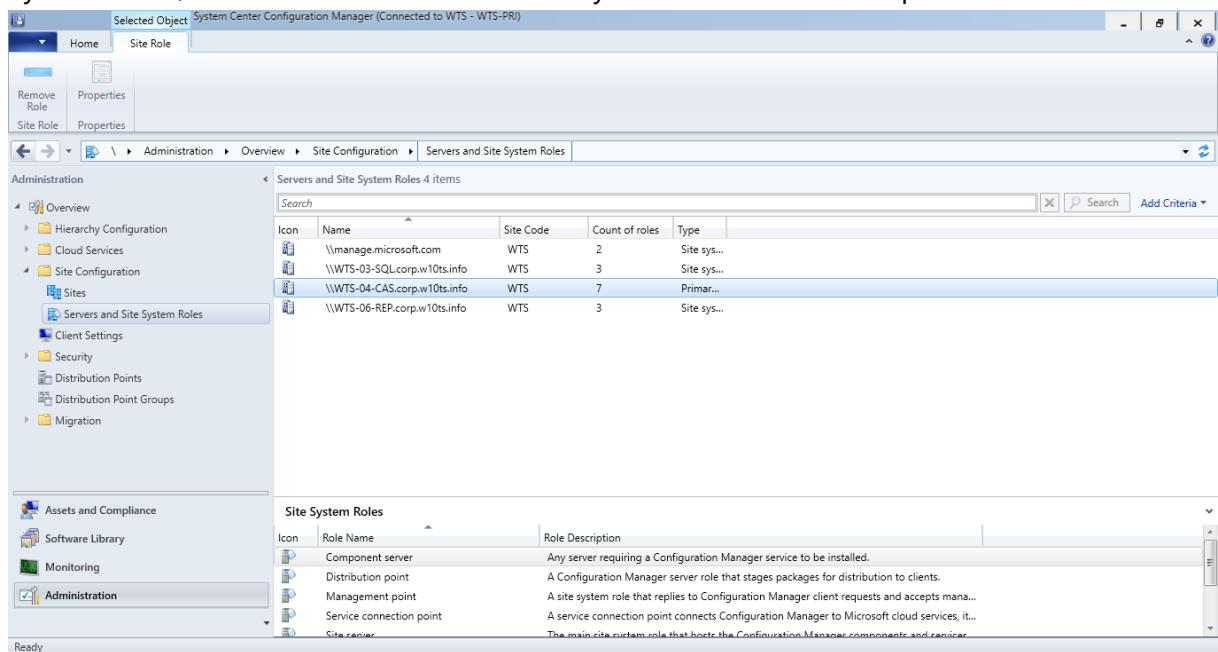
Computer restart



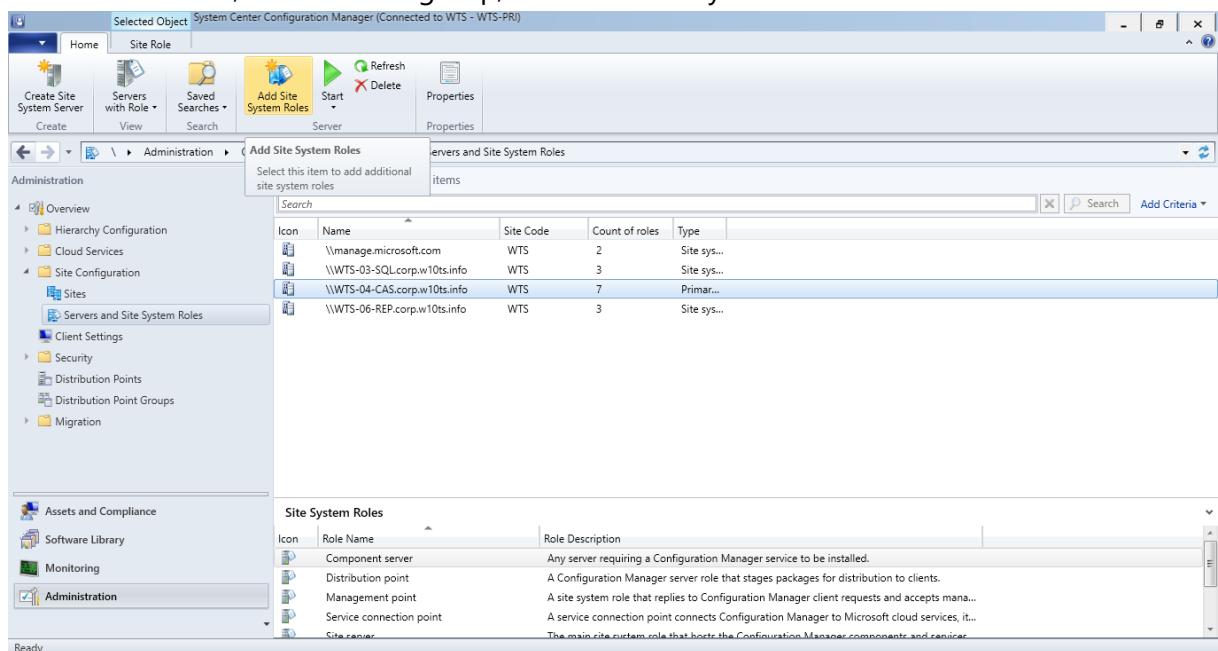
2.2 Managing Endpoint Protection/Defender with Config Manager

2.1.1. Install Endpoint Protection Site System Role

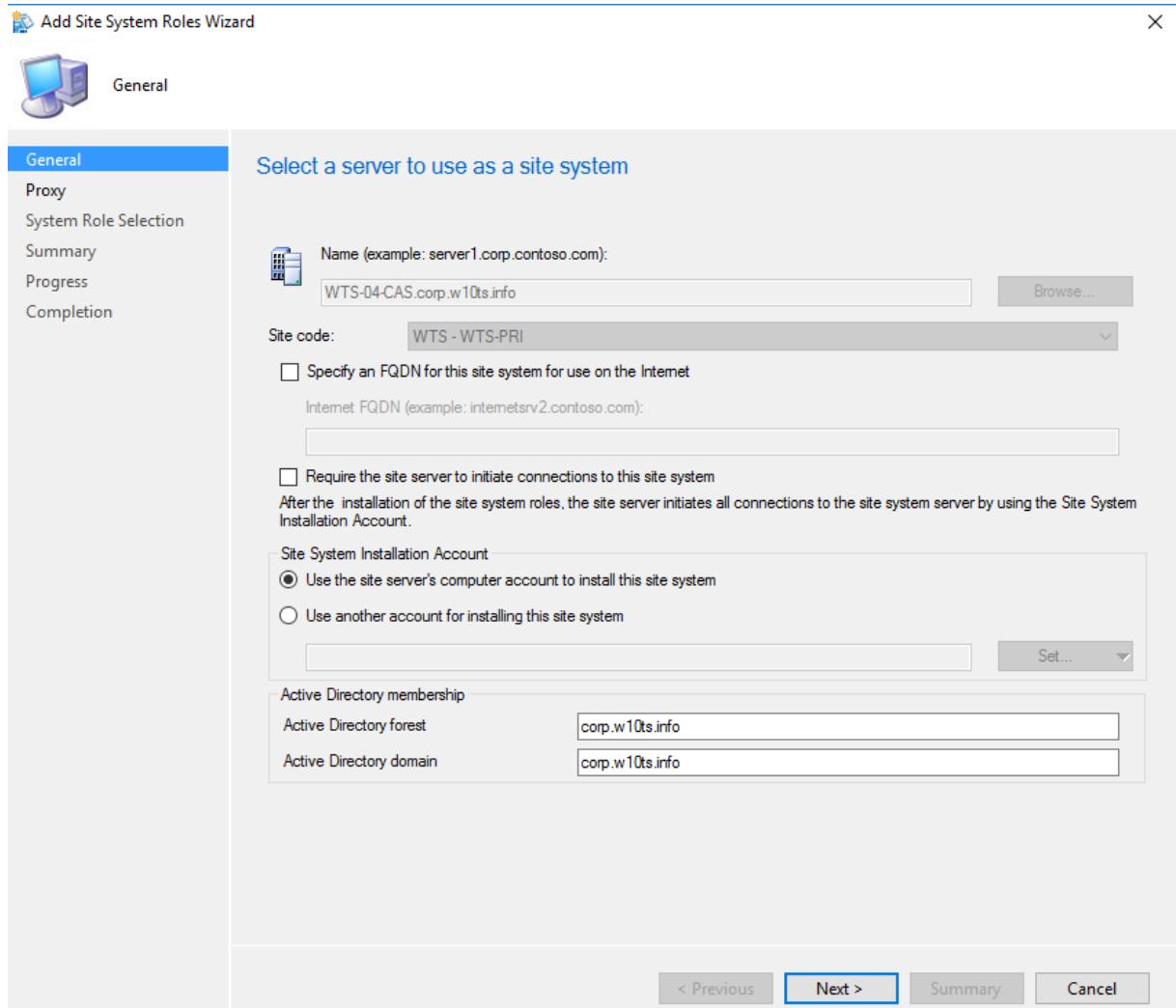
1. In the Configuration Manager console, click Administration.
2. In the Administration workspace, expand Site Configuration, click Servers and Site System Roles, and then select the server that you want to use for Endpoint Protection.



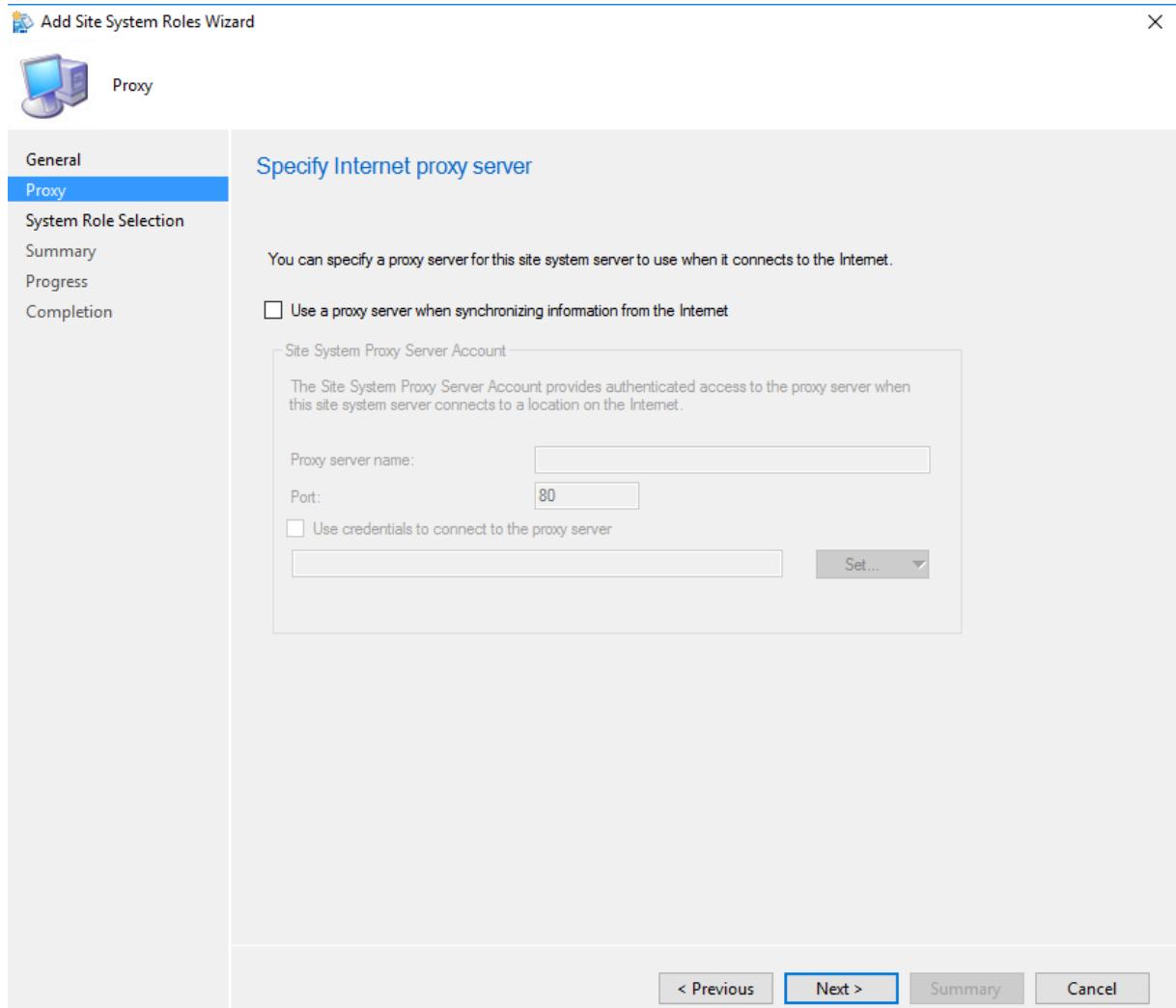
3. On the Home tab, in the Server group, click Add Site System Roles.



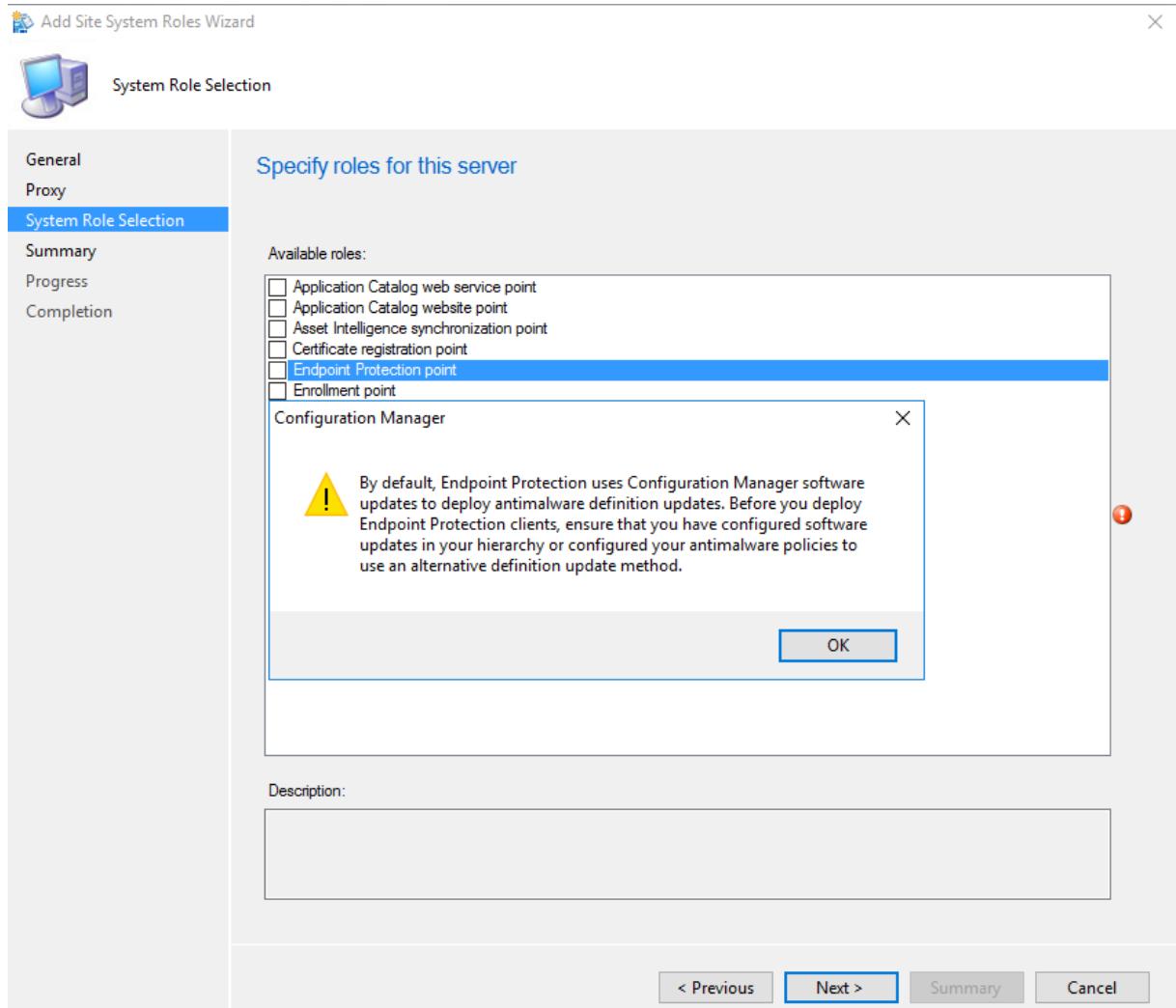
4. On the General page, leave the defaults and then click "Next".



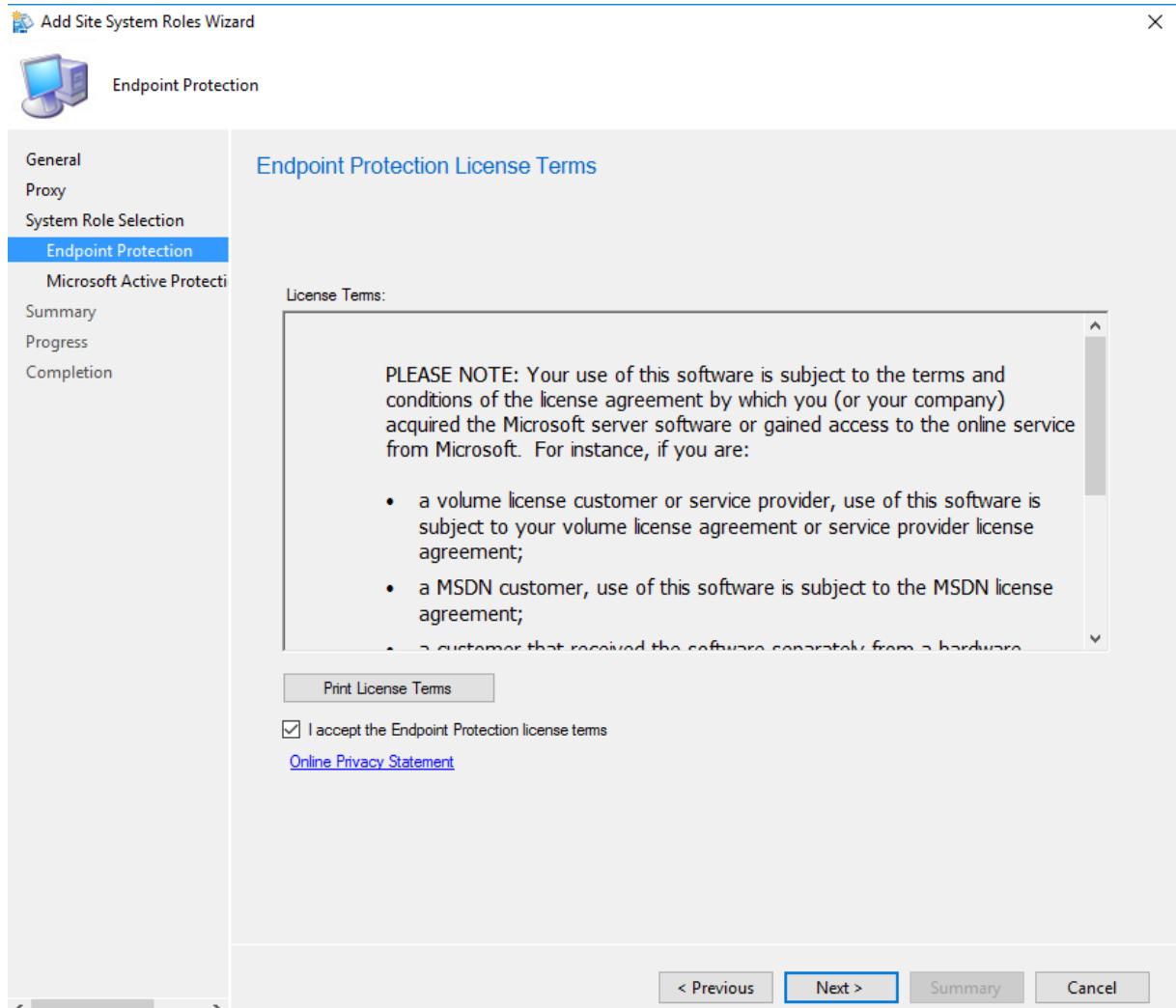
5. On the Proxy page, leave the defaults and then click "Next".



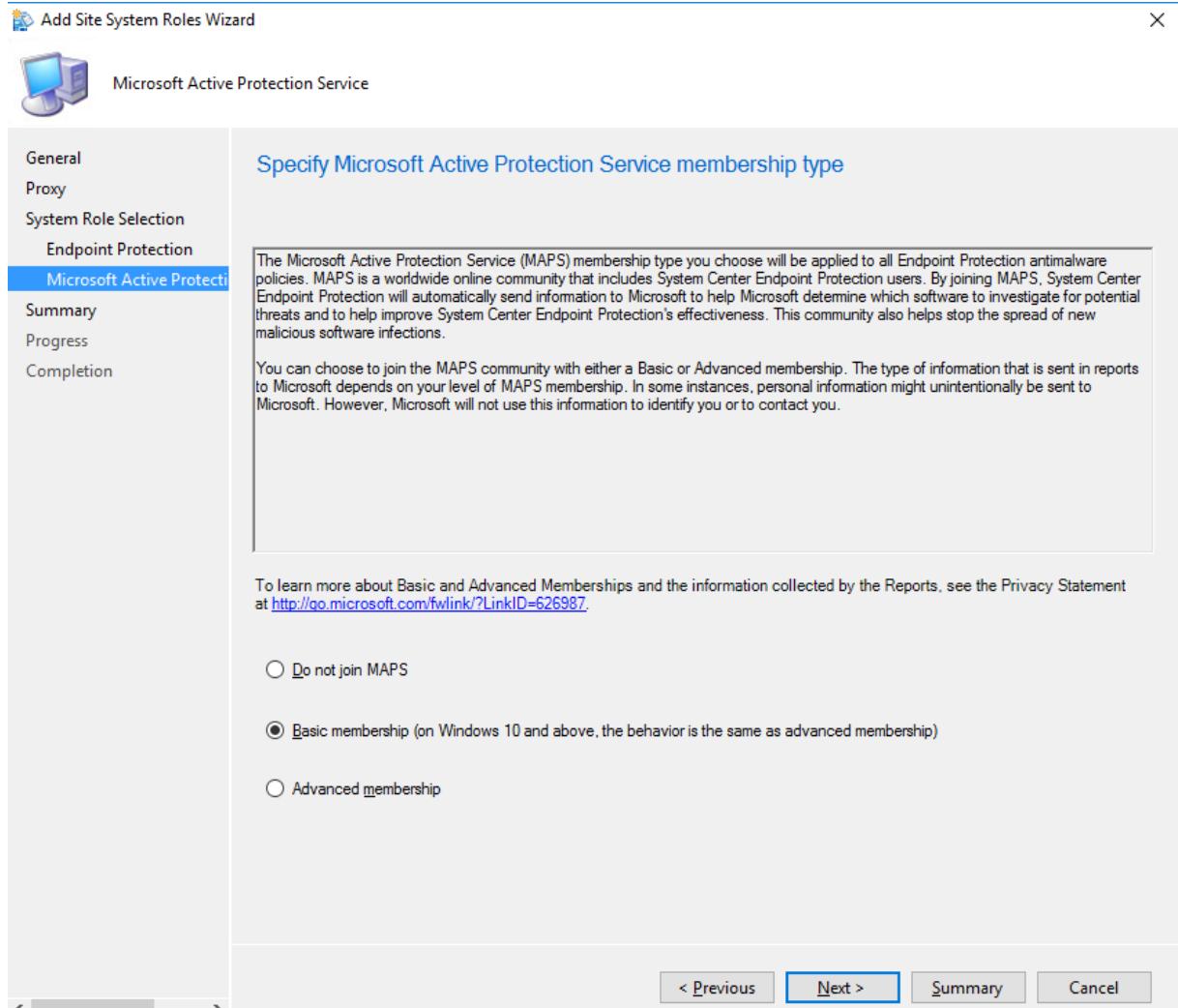
6. On the System Role Selection page, select Endpoint Protection point in the list of available roles, confirm the warning dialog and then click "Next".



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



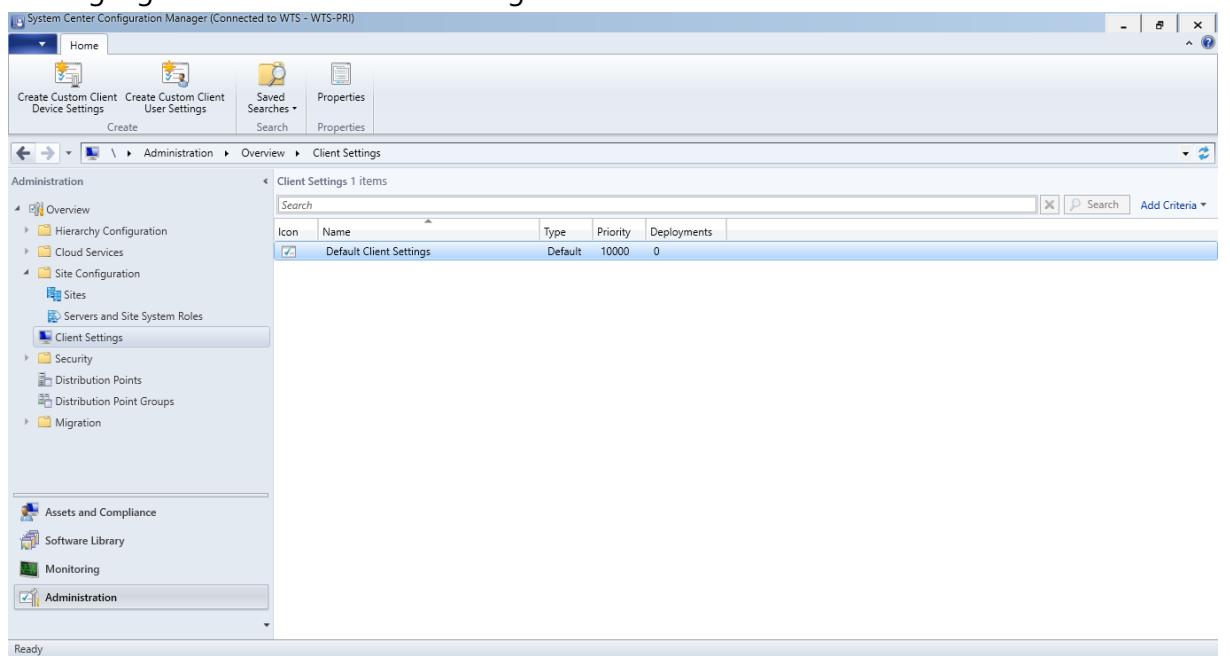
8. On the Microsoft Active Protection Service page, select the level of information that you want to send to Microsoft to help develop new definitions, and then click "Next".



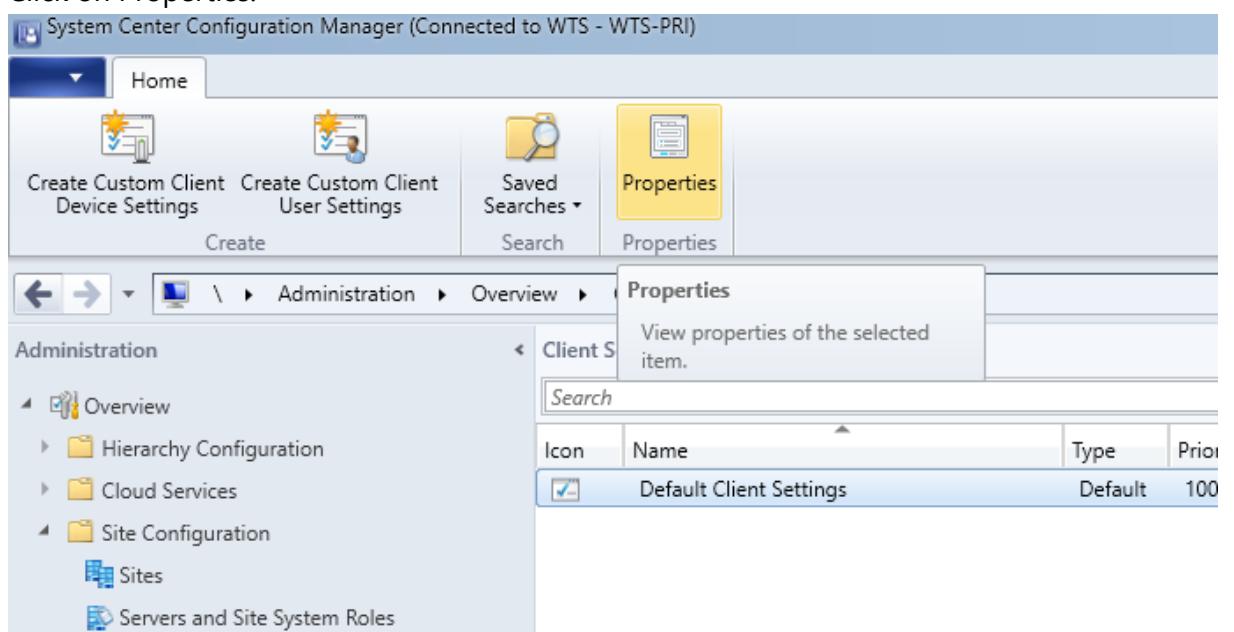
9. Complete the wizard and click on "Close".

2.1.2. Enable Endpoint Protection in client settings

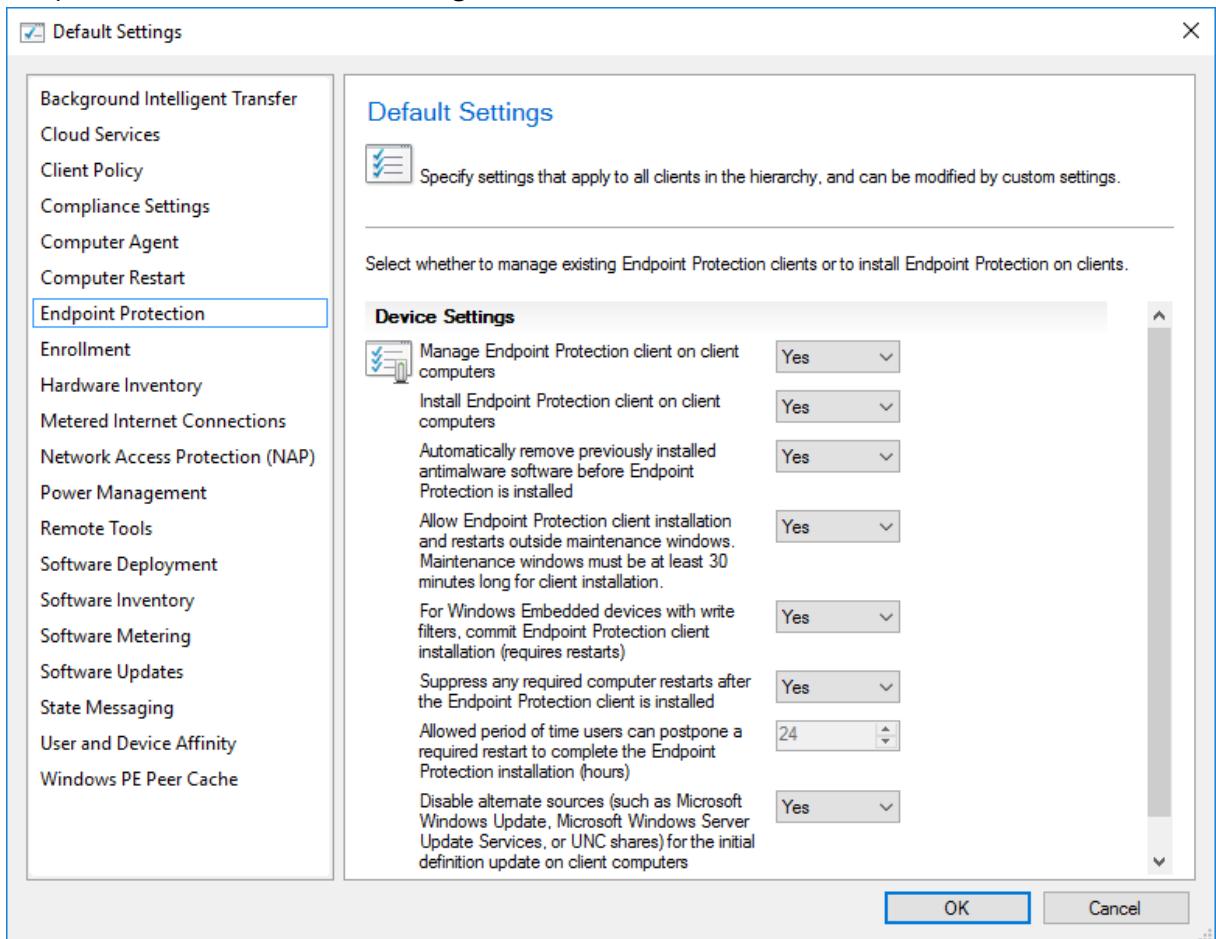
1. In the Administration workspace, expand "Site Configuration", select "Client Settings" and highlight the "Default Client Settings".



2. Click on Properties.



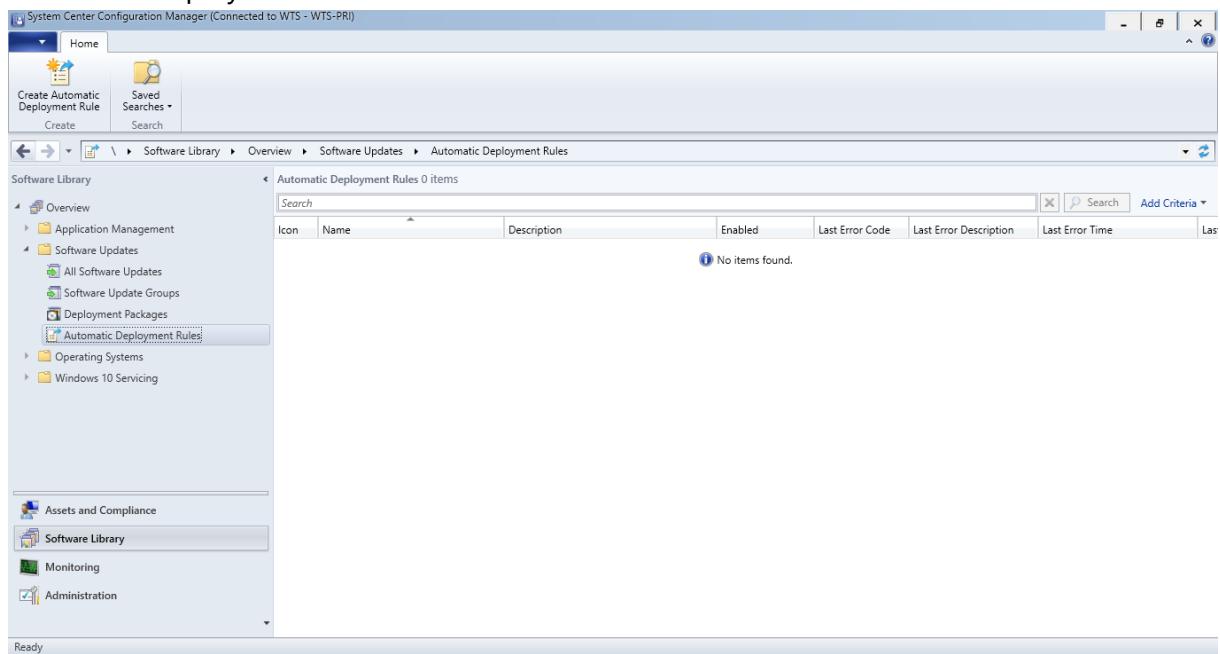
3. Select "Yes" at "Manage Endpoint Protection client on client computers" in the Endpoint Protection "Device Settings".



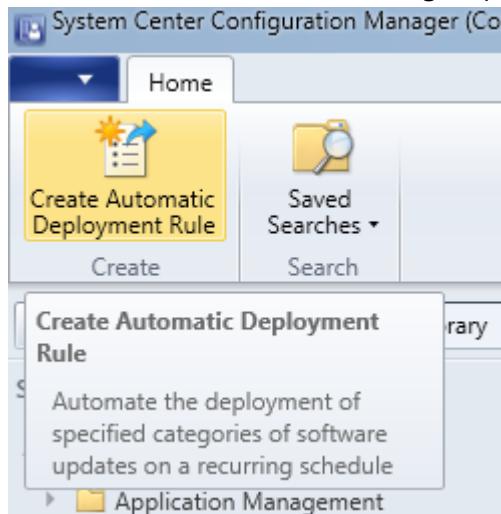
4. Click "OK".

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

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

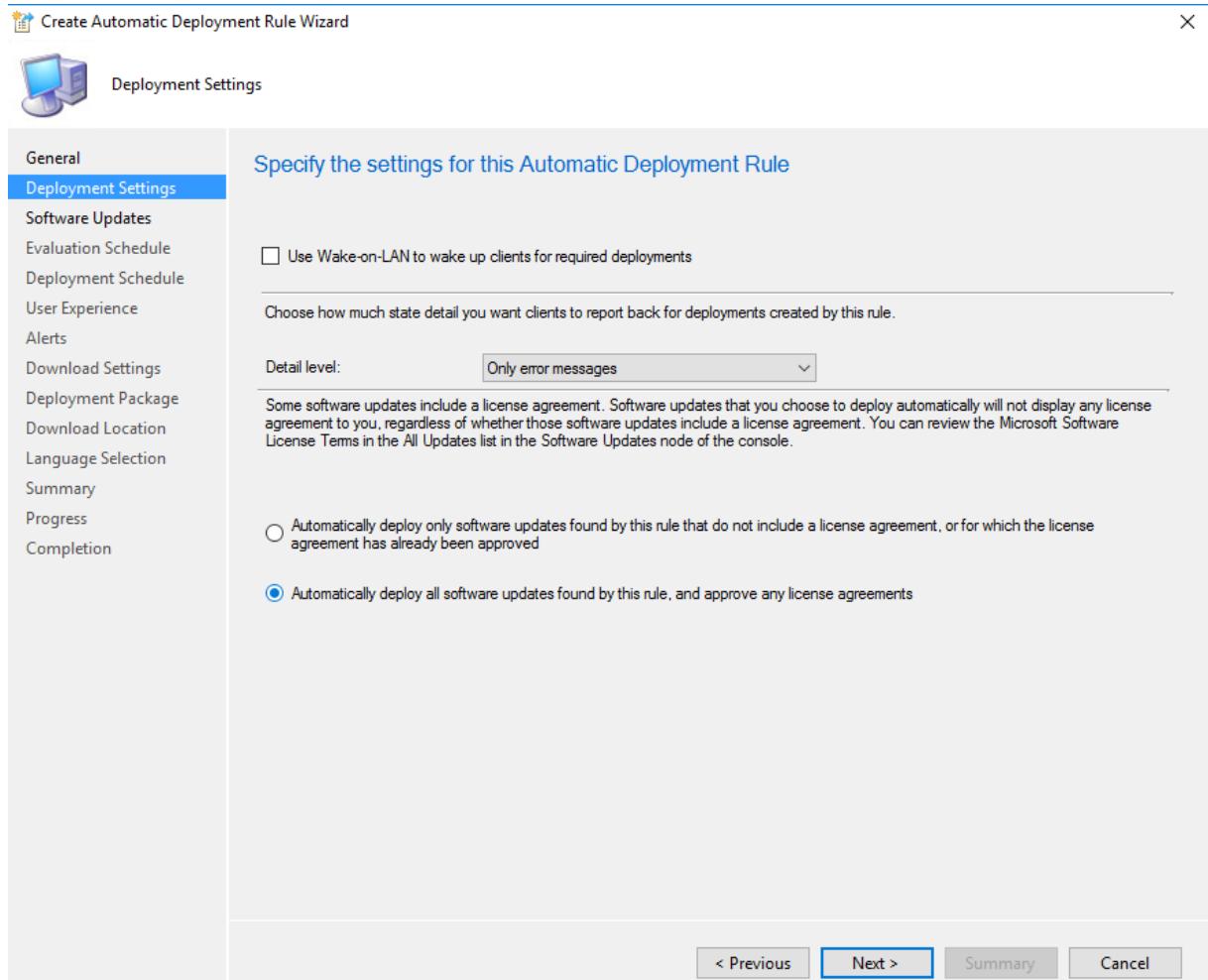
Create a new Software Update Group

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

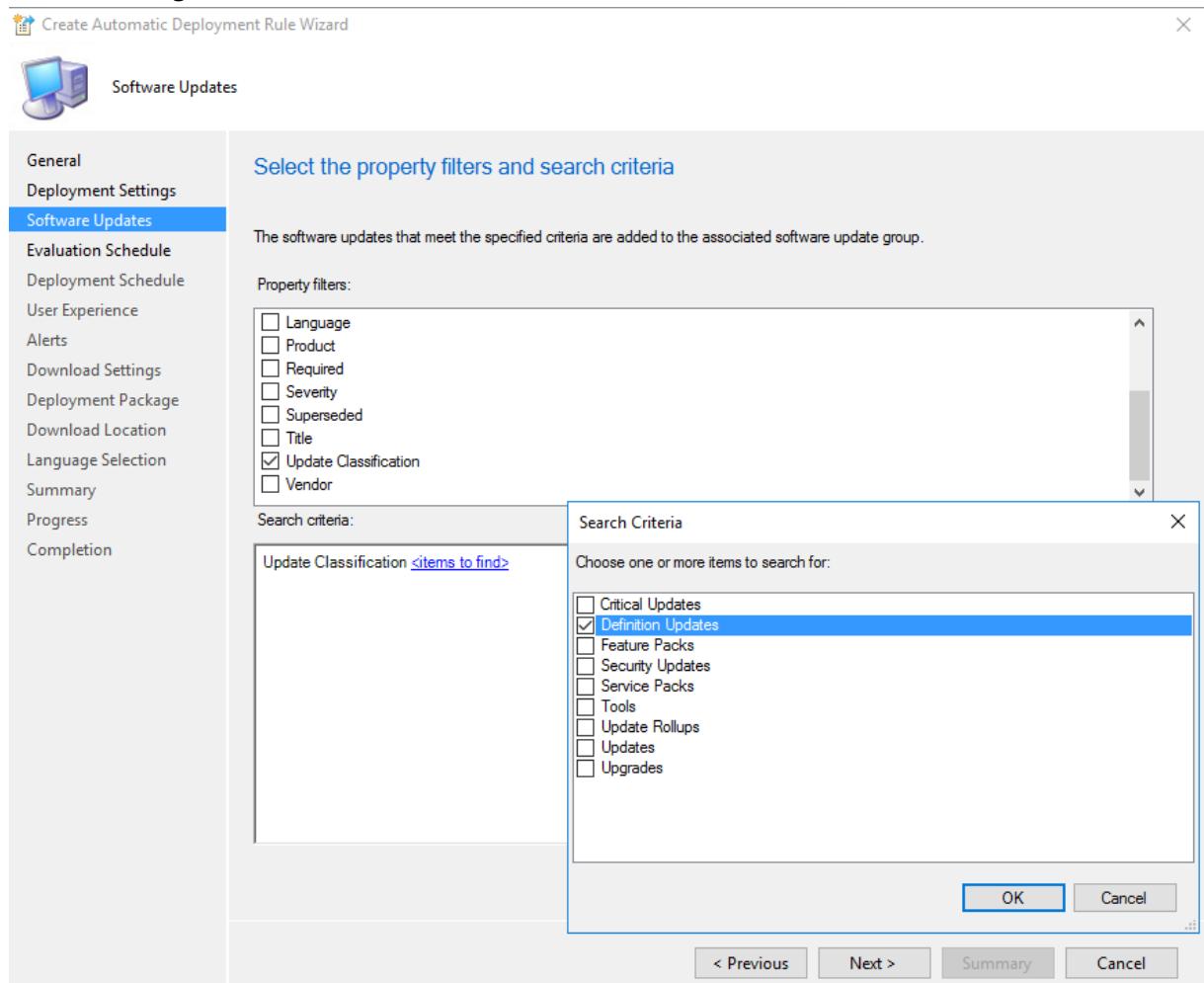
< Previous Next > Summary Cancel

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



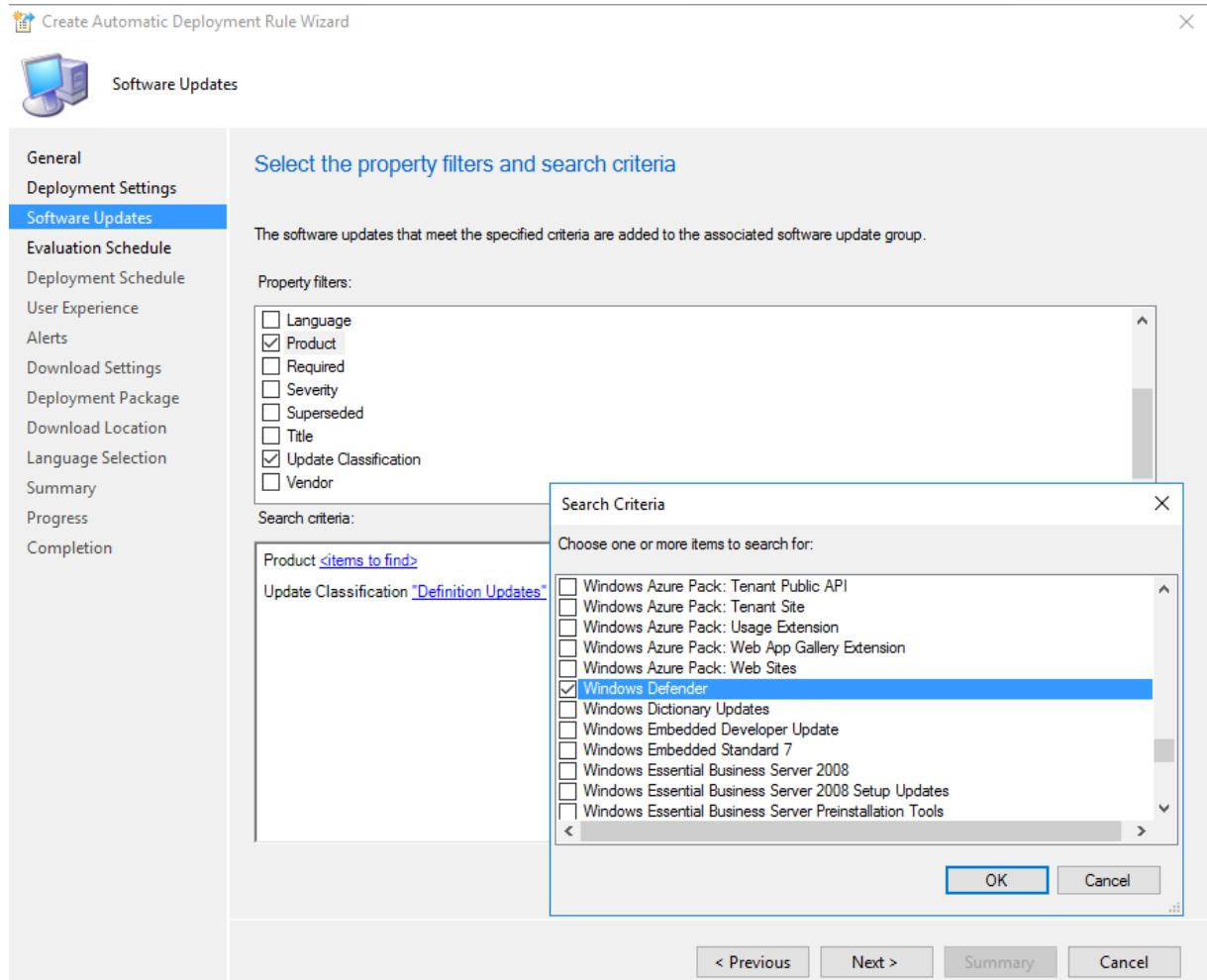
6. In the Property filters list, select the Update Classification check box and in the Search criteria list, click <items to find>. Then, in the Search Criteria dialog box, in the Specify the value to search for list, select Definition Updates. Click OK to close the Search

Criteria dialog box.



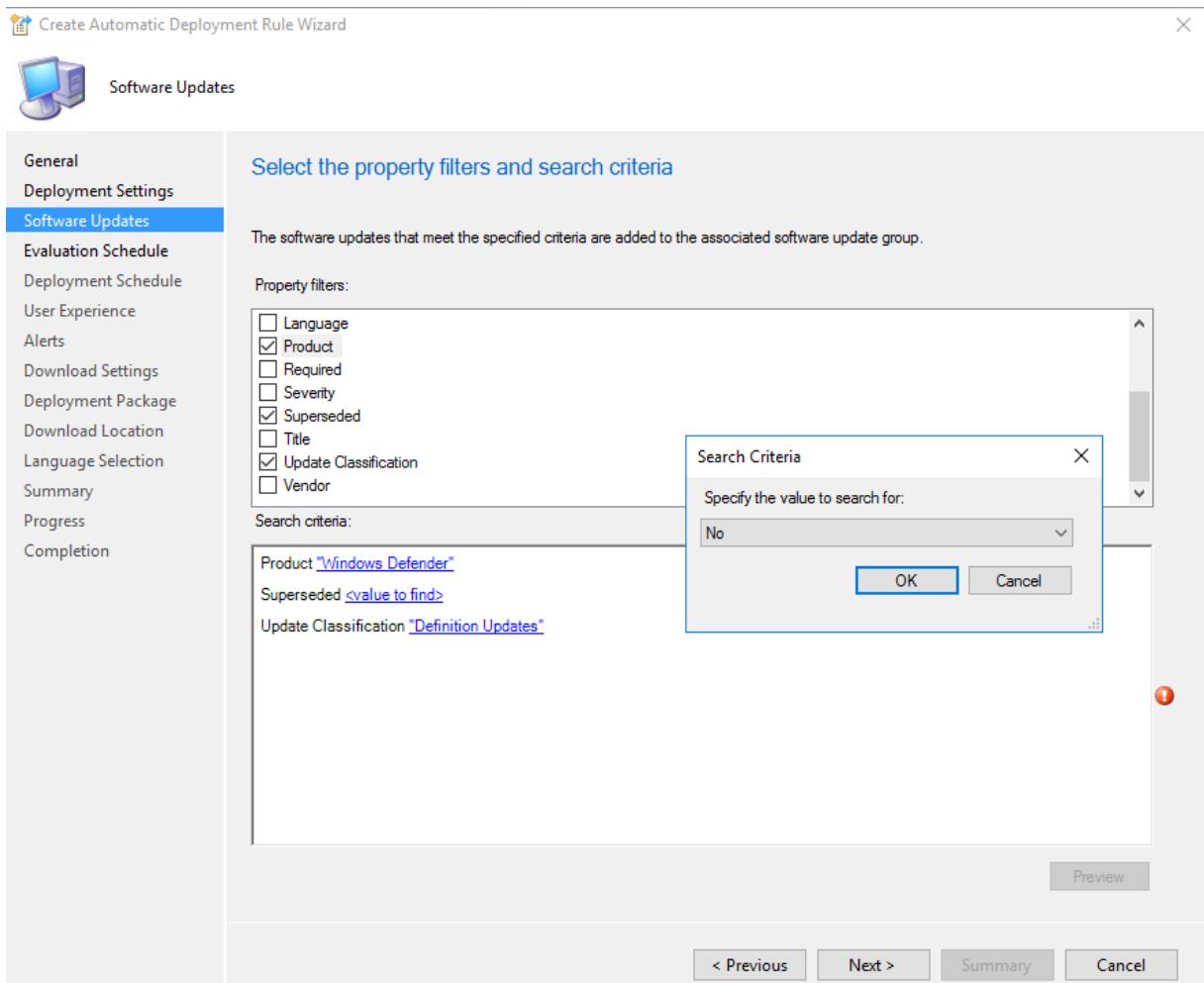
7. In the Property filters list, select the Product check box and in the Search criteria list, click <items to find>. Then, in the Search Criteria dialog box, in the Specify the value to search for list, select "Windows Defender" for Windows 10 and later. Click OK to

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



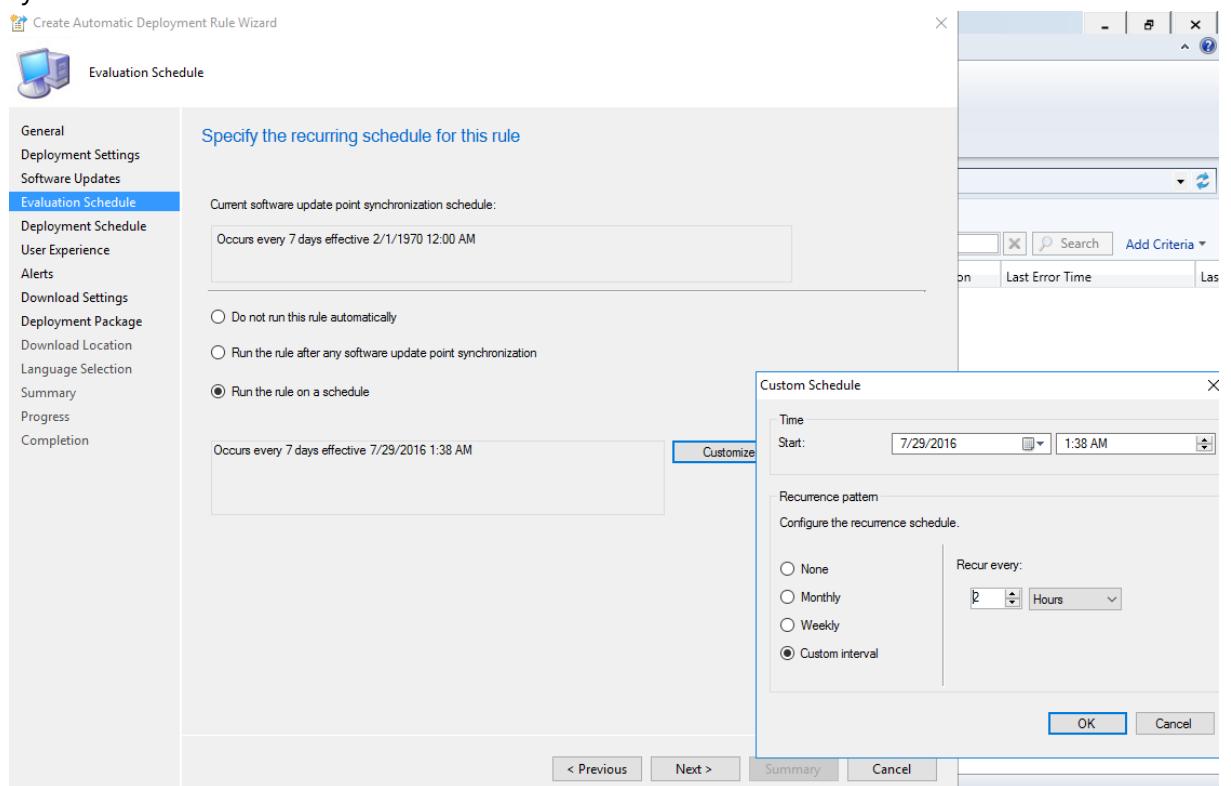
8. In the Property filters list, select the Superseded check box and in the Search criteria list, click <items to find>. Then, in the Search Criteria dialog box, in the Specify the value to search for list, select No. Click OK to close the Search Criteria dialog box, and

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

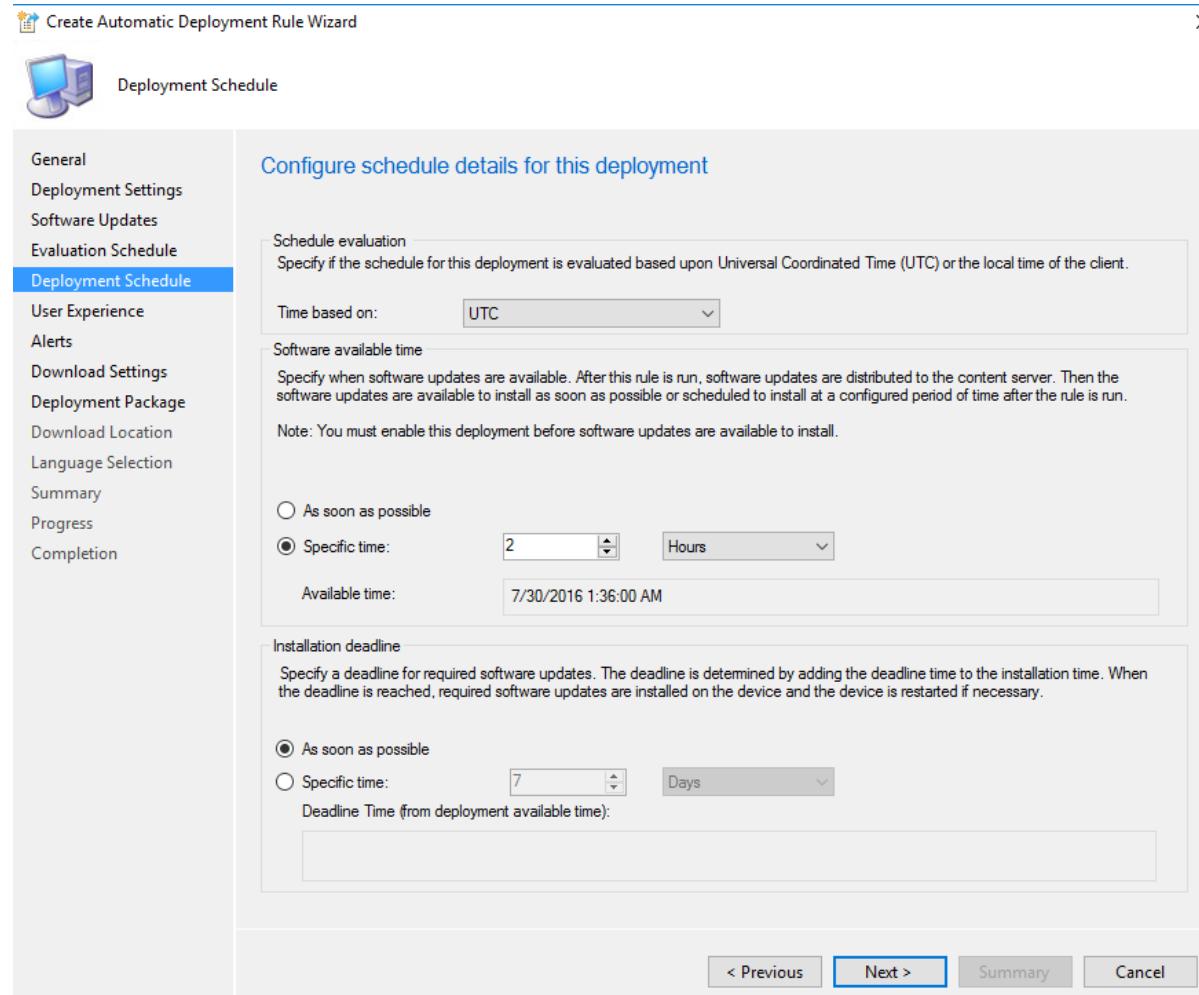
synchronization. Click "Next".



10. On the Deployment Schedule page of the wizard, configure the following settings and then click "Next":

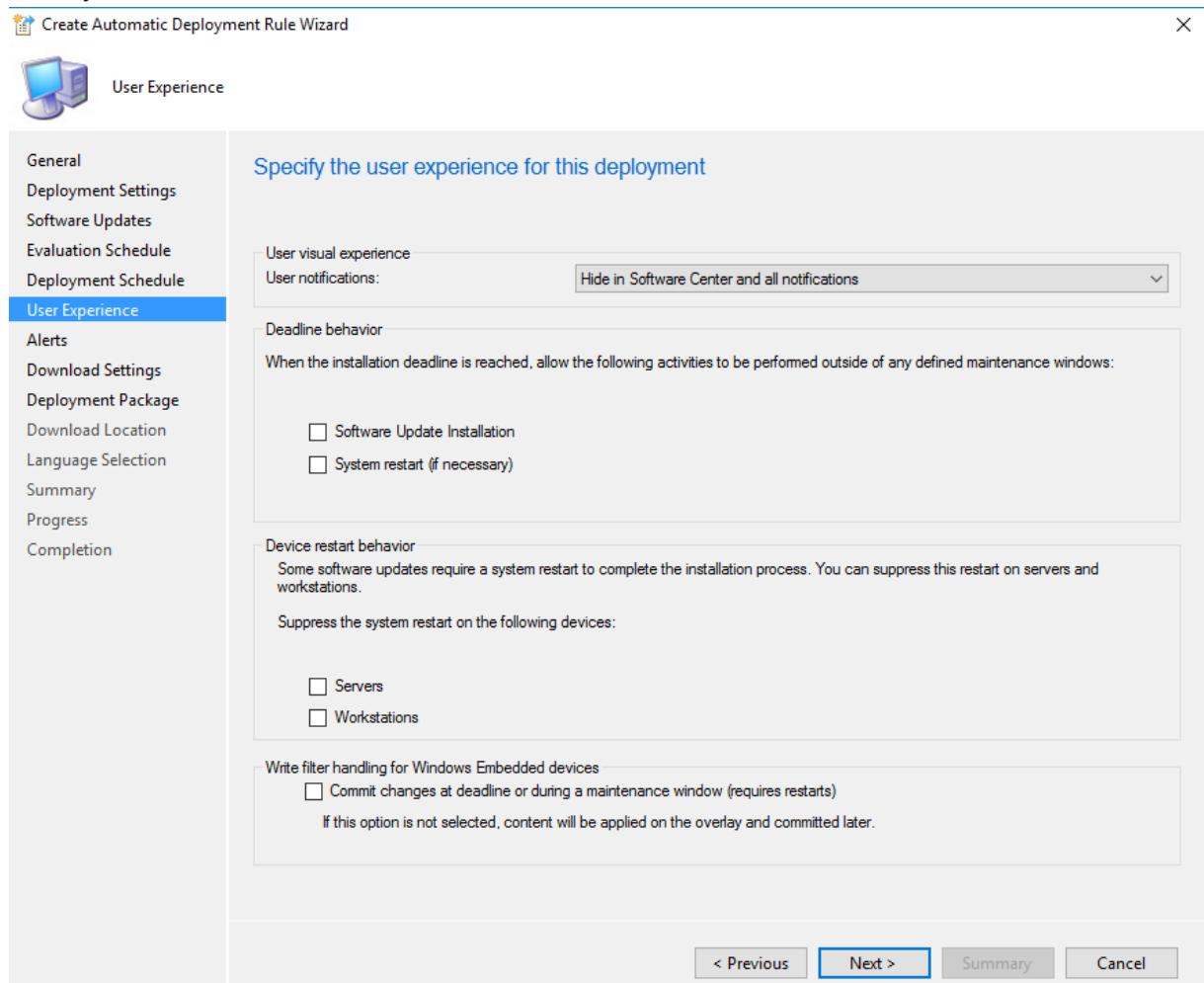
- a. Time based on: Select UTC if you want all clients in the hierarchy to install the latest definitions at the same time. The actual installation time will vary within a two-hour window. This setting is a recommended best practice.
- b. Software available time: Specify the available time for the deployment 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: Days

Offset from the deadline: Days

Alerts are generated after the installation deadline is reached.
Deadline time:

Operations Manager alerts

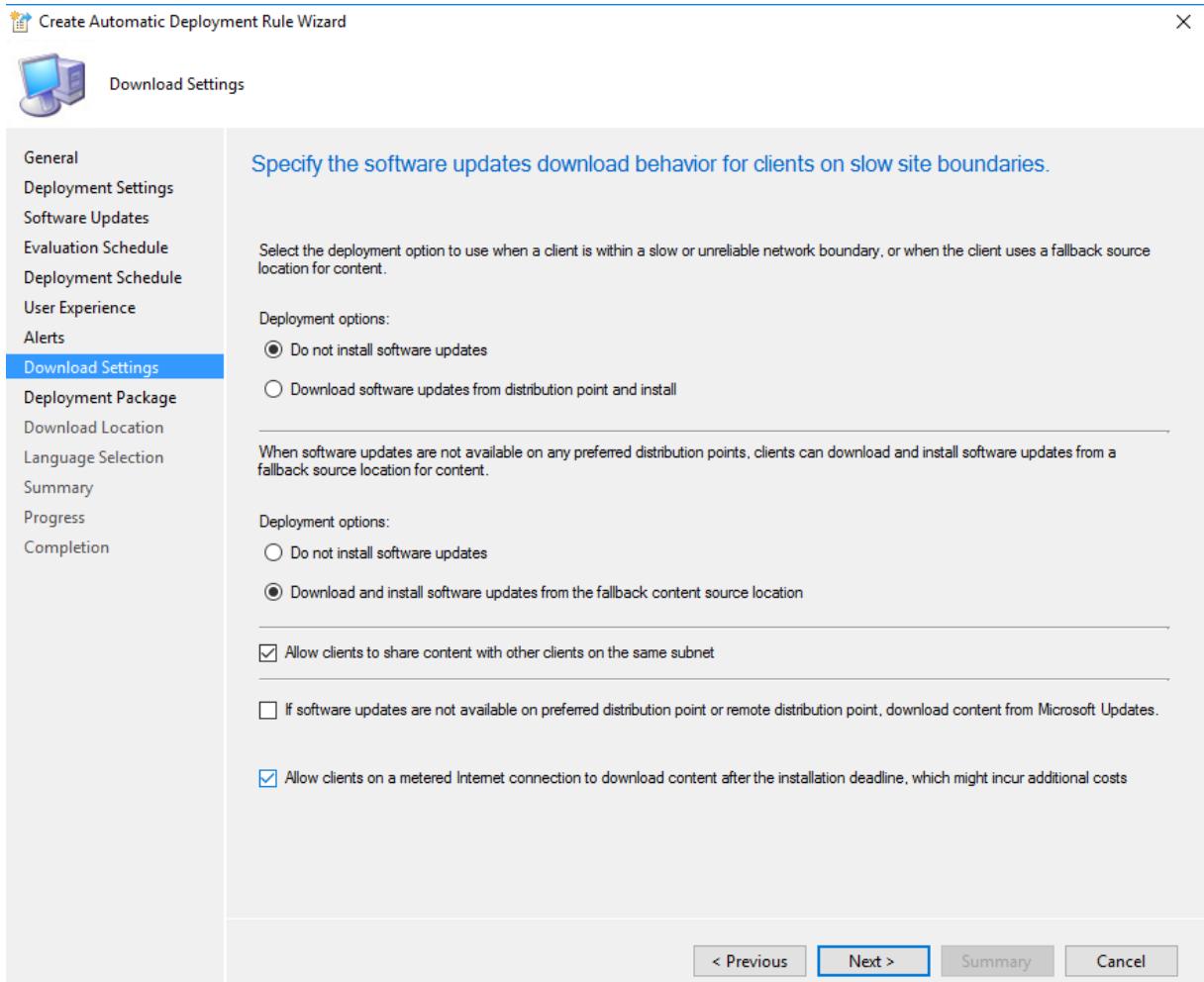
System Center Operations Manager might generate alerts when a device installs a software update. To avoid receiving alerts for planned maintenance, you can disable these alerts during the duration of the software update installation process.

Disable Operations Manager alerts while software updates run

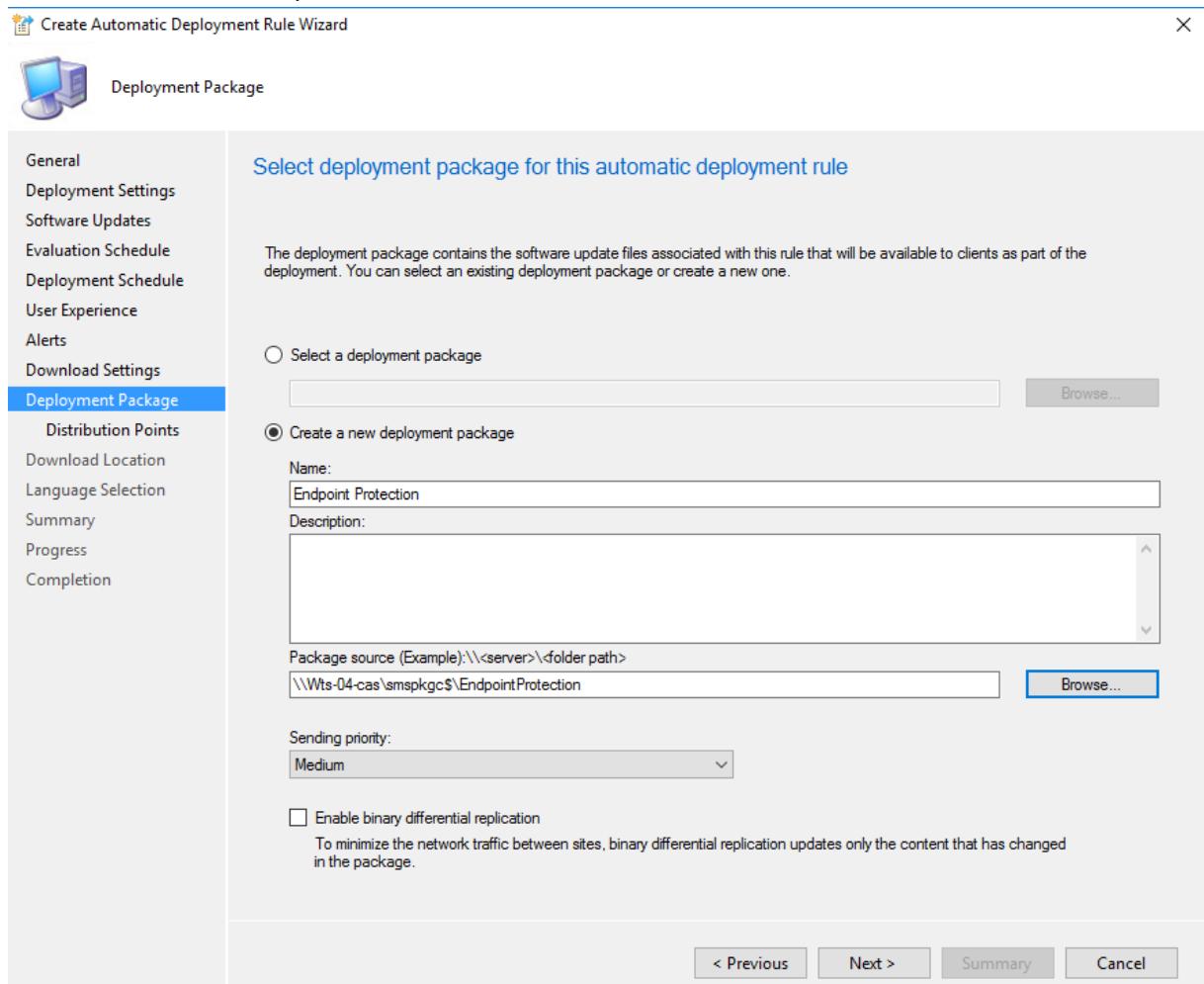
Generate Operations Manager alert when a software update installation fails

< Previous **Next >** Summary Cancel

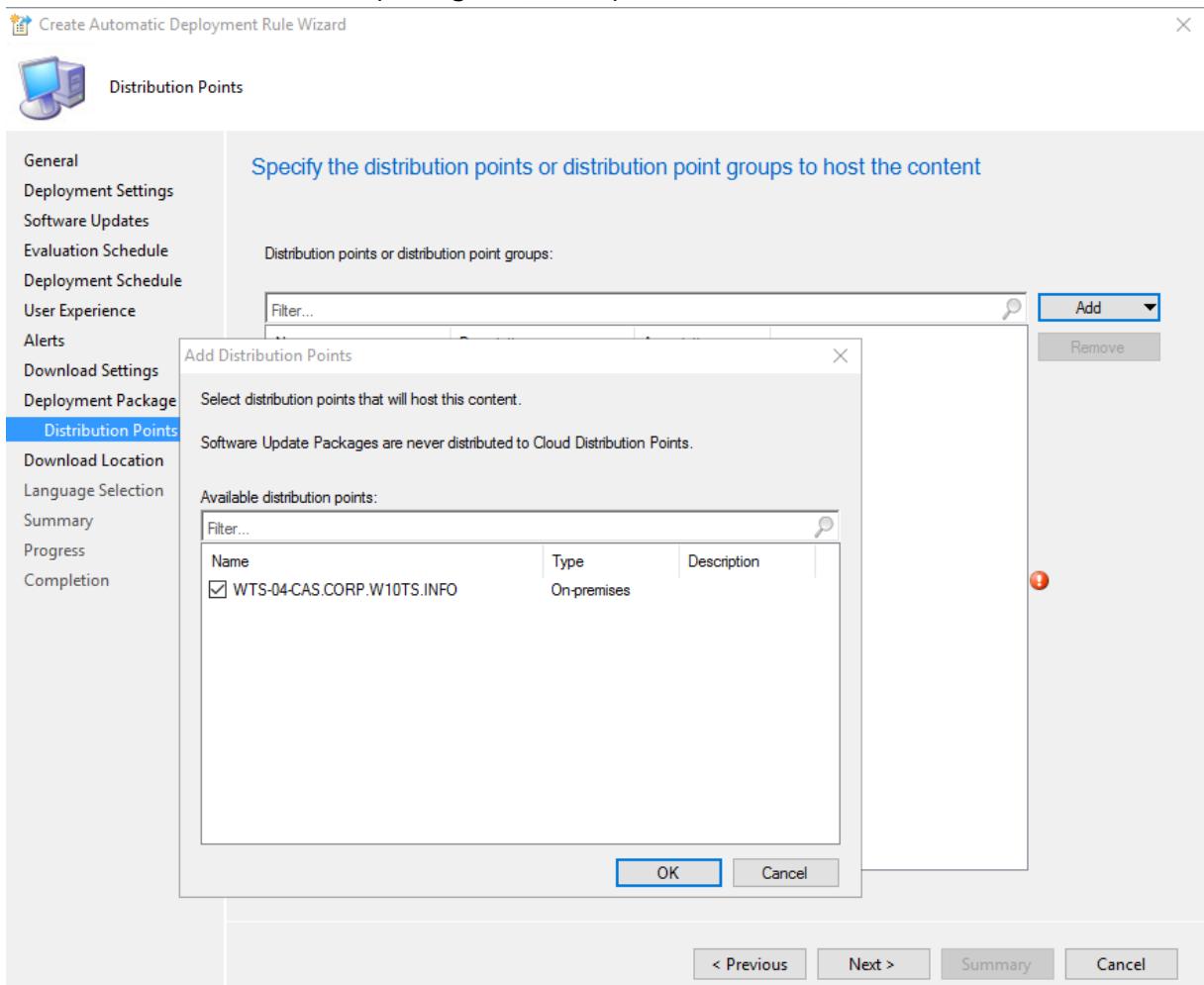
13. On the Download Settings page of the wizard, select the necessary software updates download behavior, and then click "Next".



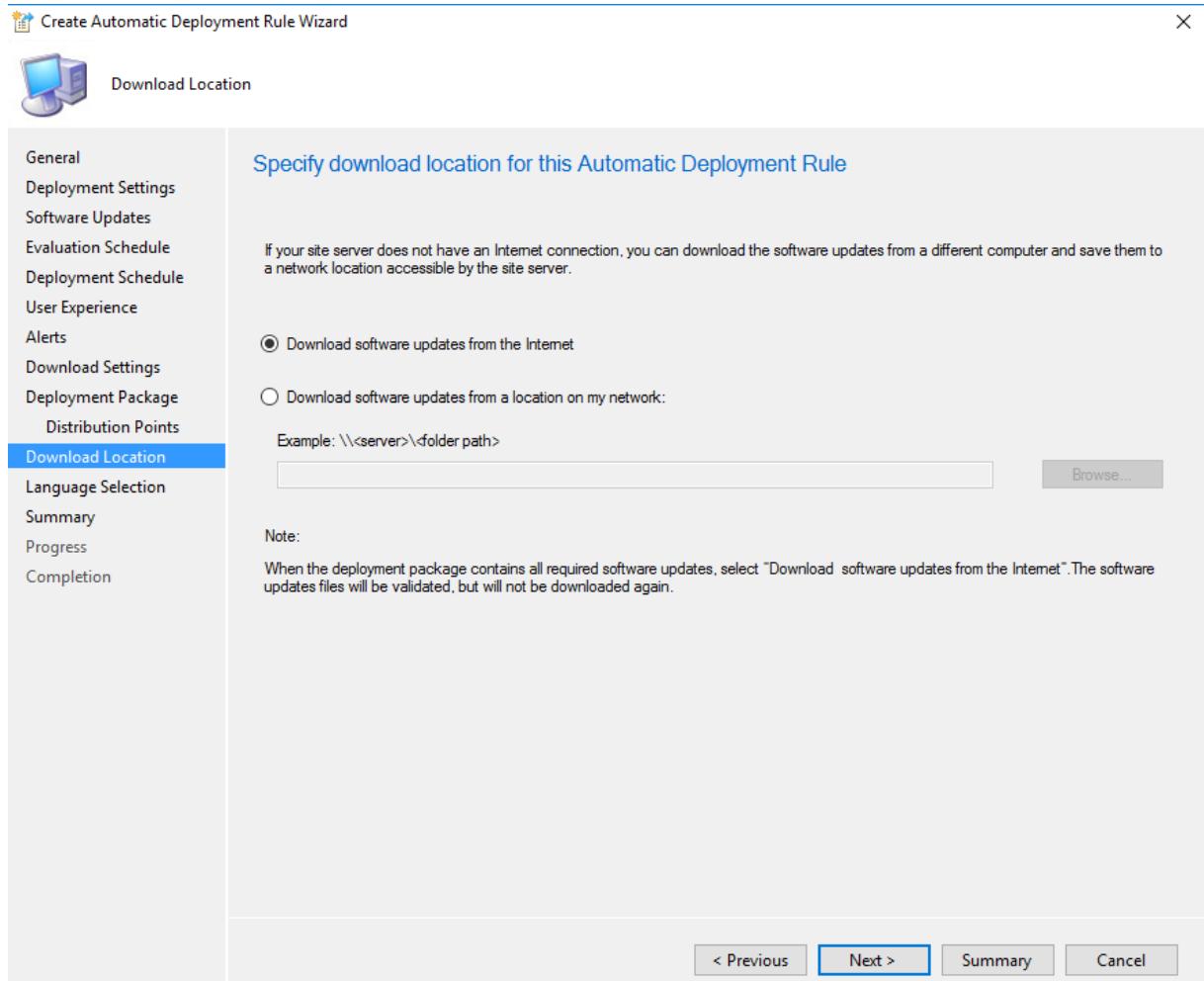
14. On the Deployment Package page of the wizard, create a new deployment package to contain the software update files associated with the rule and click "Next".



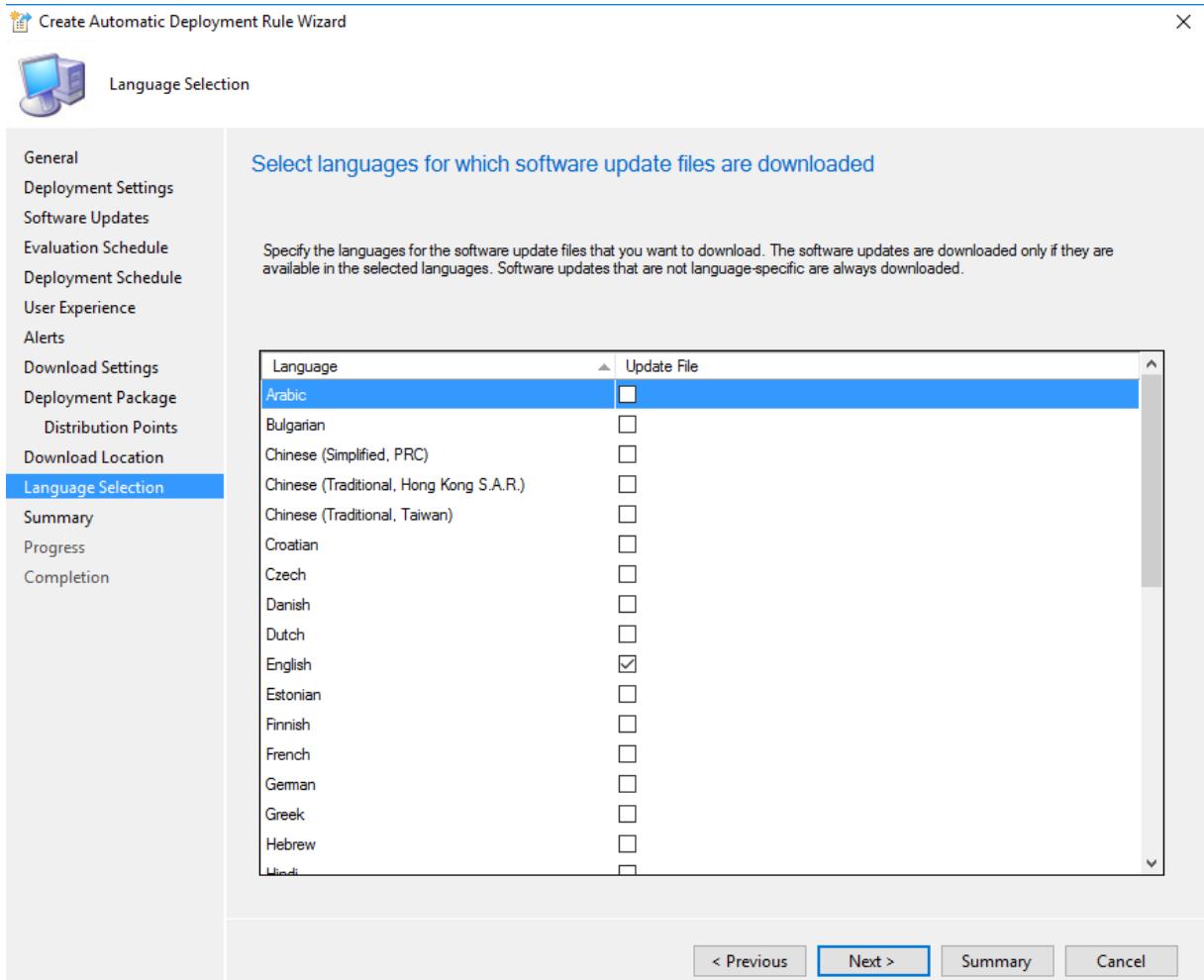
15. On the Distribution Points page of the wizard, select one or more distribution points to which the content for this package will be copied, and then click "Next".



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".

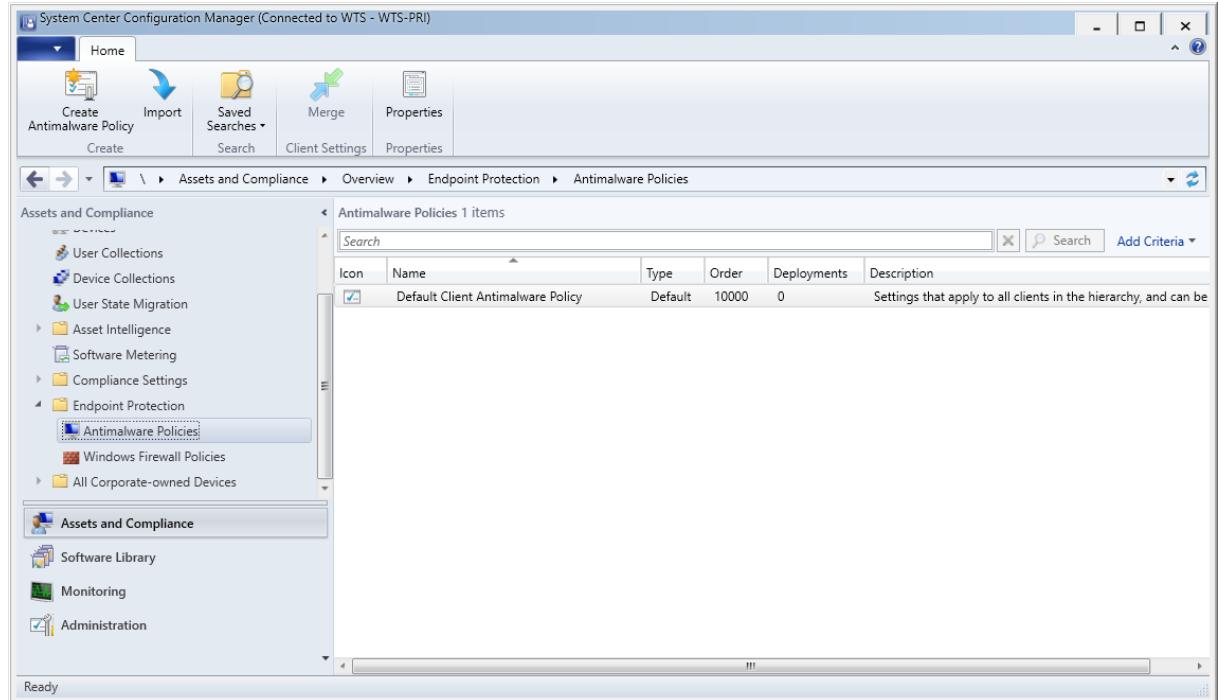


18. Complete the Create Automatic Deployment Rule Wizard.

2.1.4. Create and deploy antimalware policies for Endpoint Protection

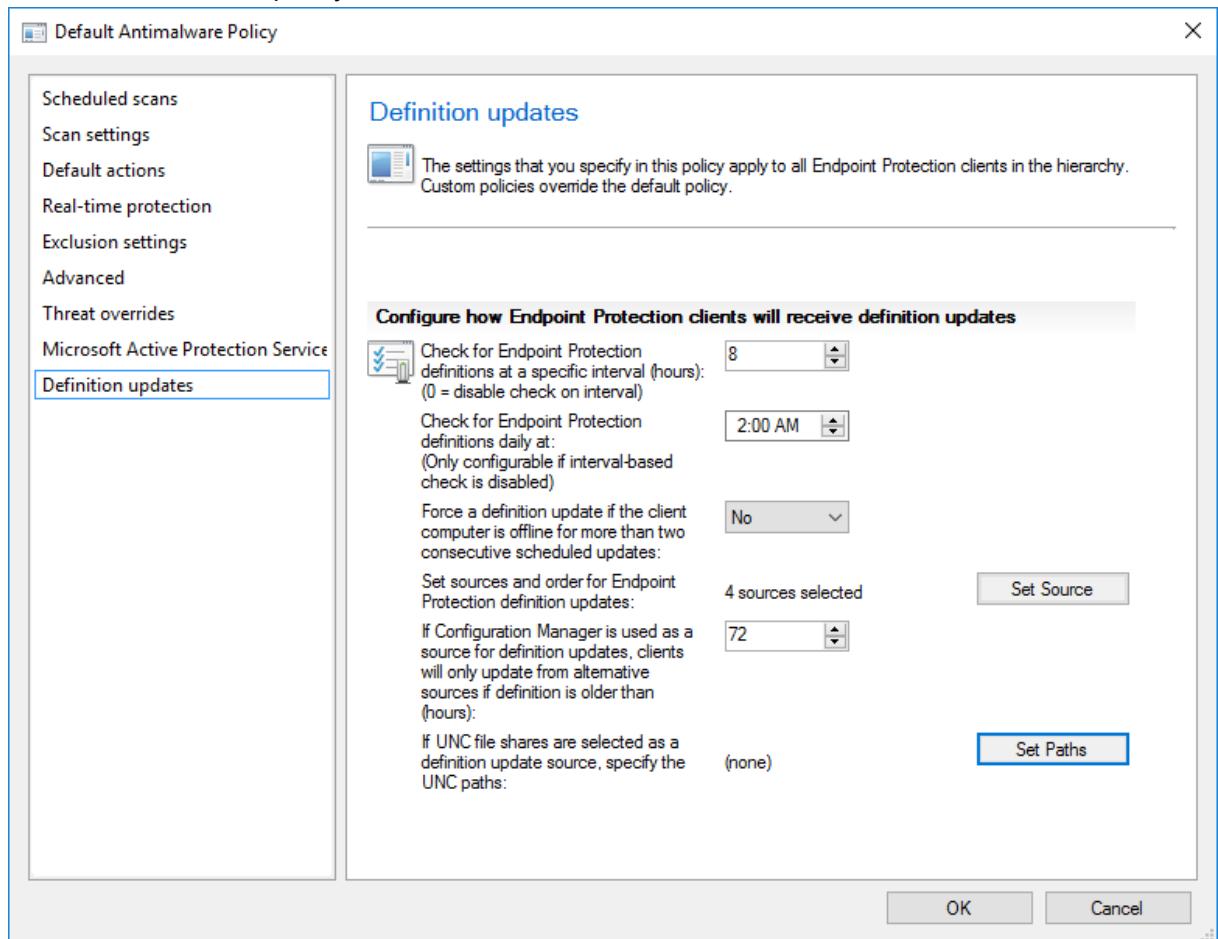
Modify the default antimalware policy

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



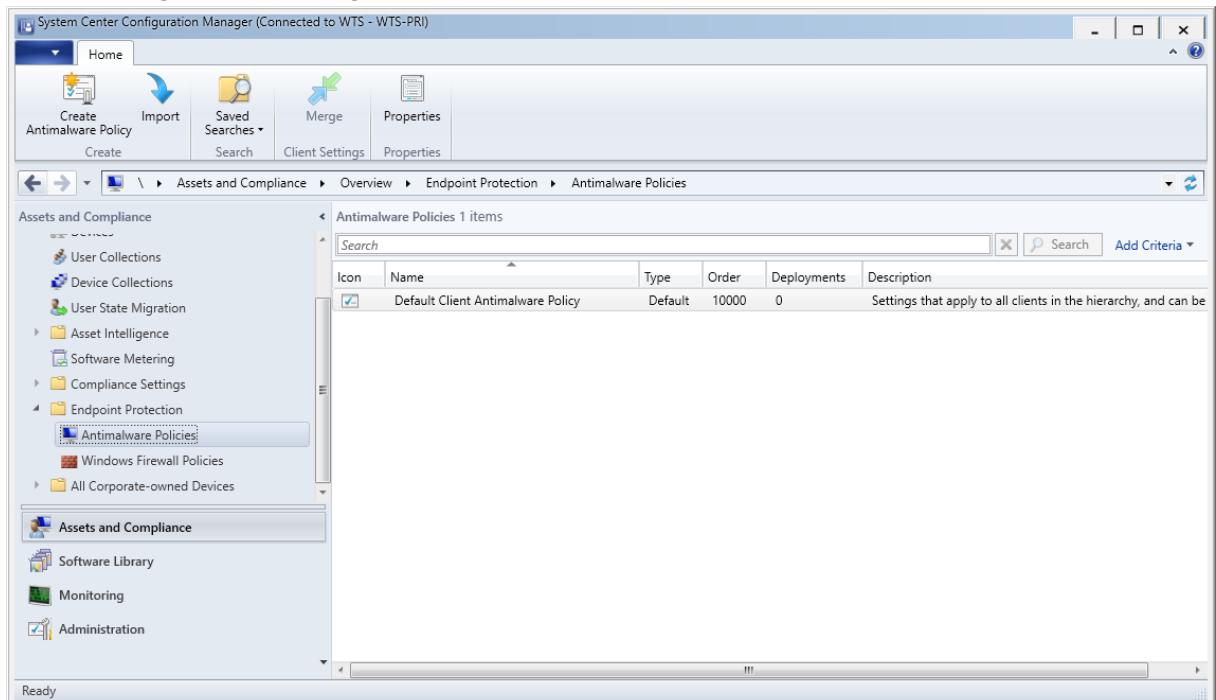
2. Select the antimalware policy Default Client Antimalware Policy and then, on the Home tab, in the Properties group, click Properties.

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

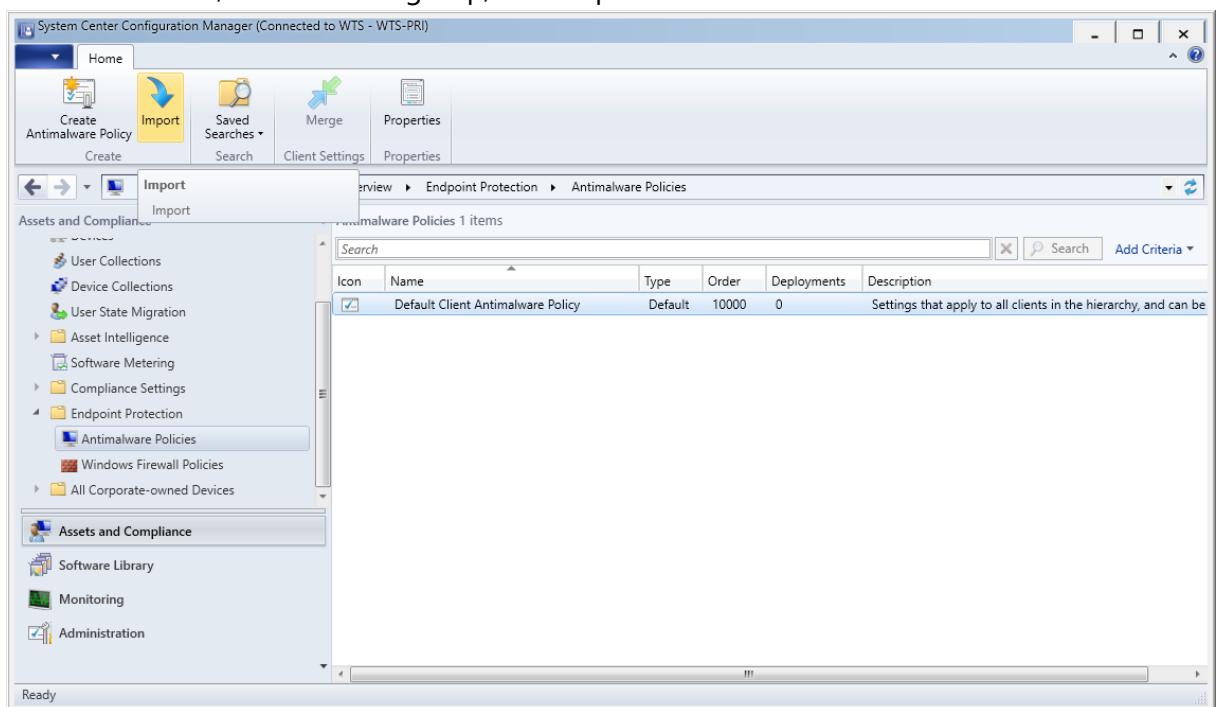


Import an antimalware policy

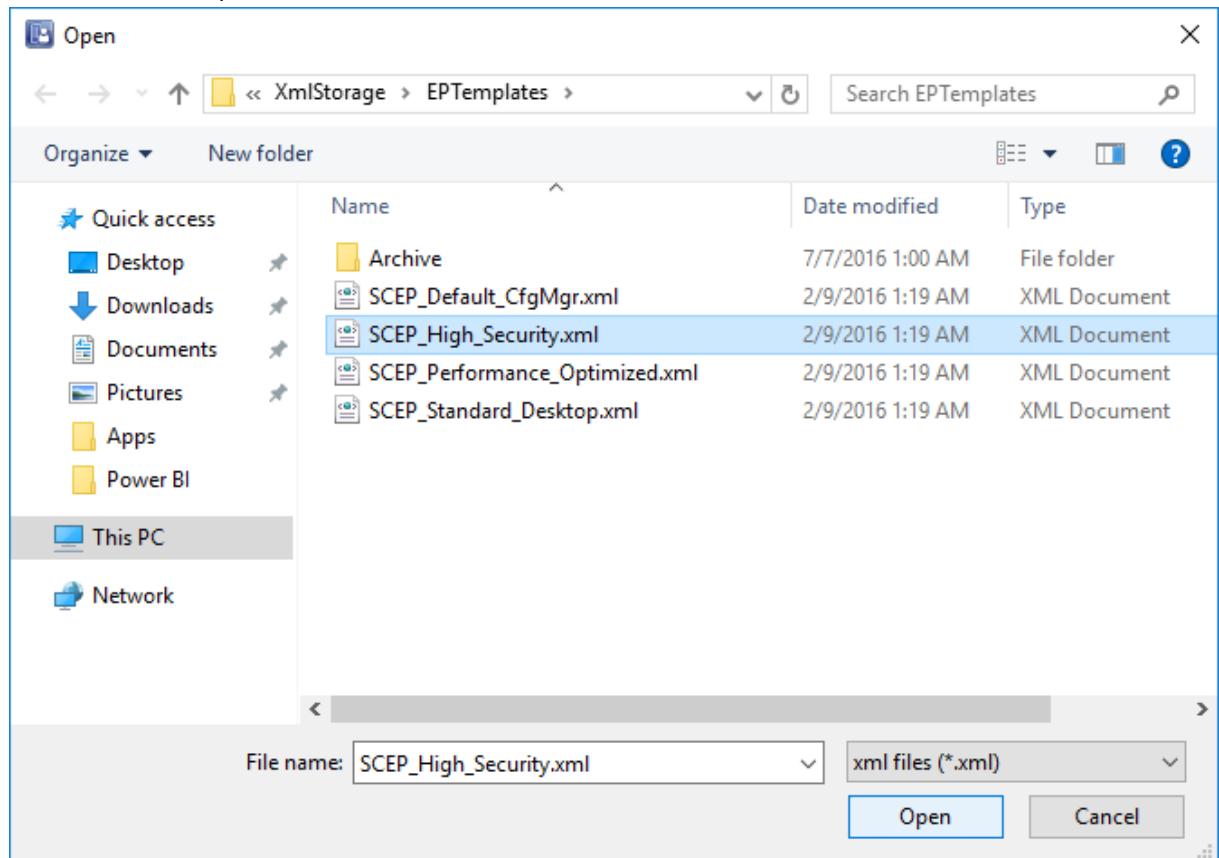
1. In the Configuration Manager console, click Assets and Compliance.



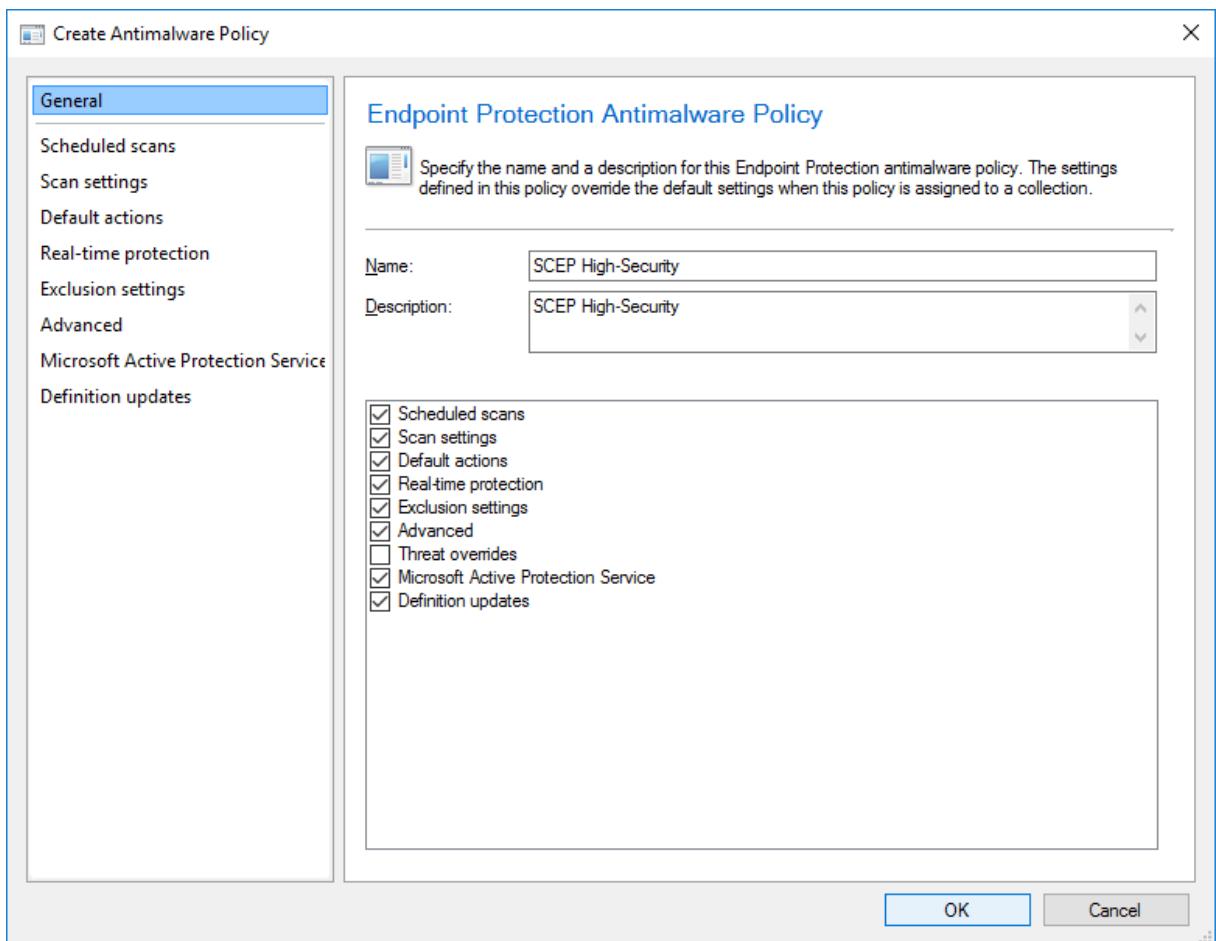
2. In the Assets and Compliance workspace, expand Endpoint Protection, and then click Antimalware Policies.
3. In the Home tab, in the Create group, click Import.



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.

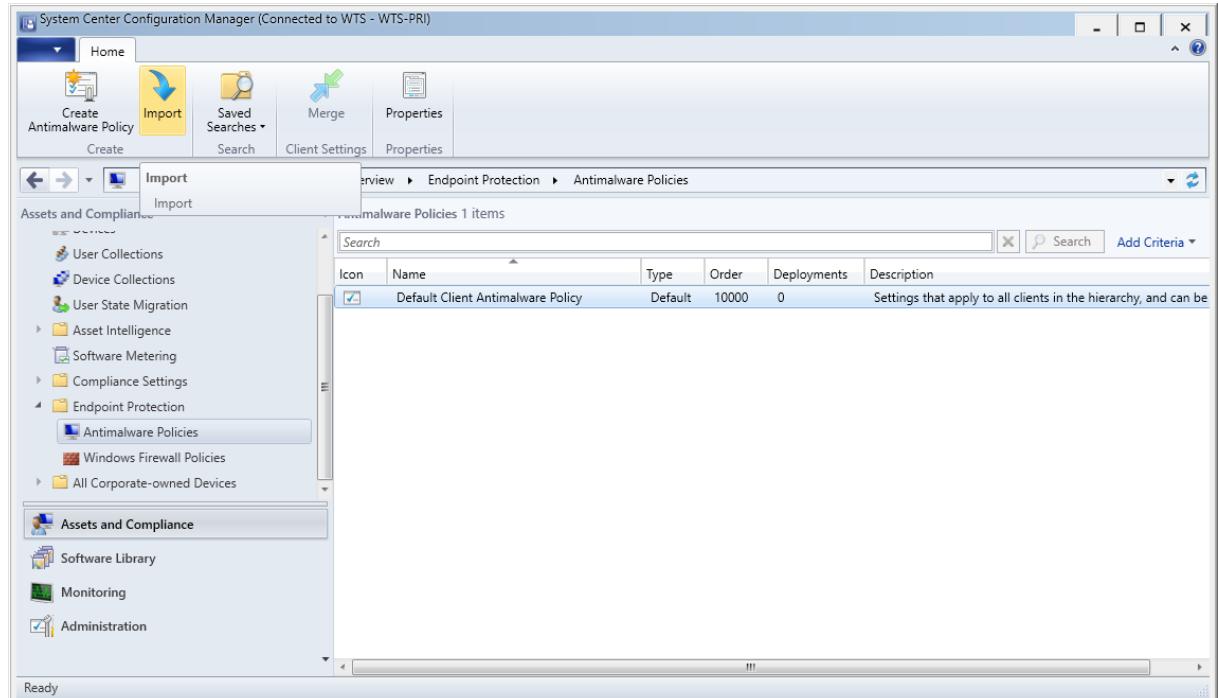


6. Verify that the new antimalware policy is displayed in the Antimalware Policies list.

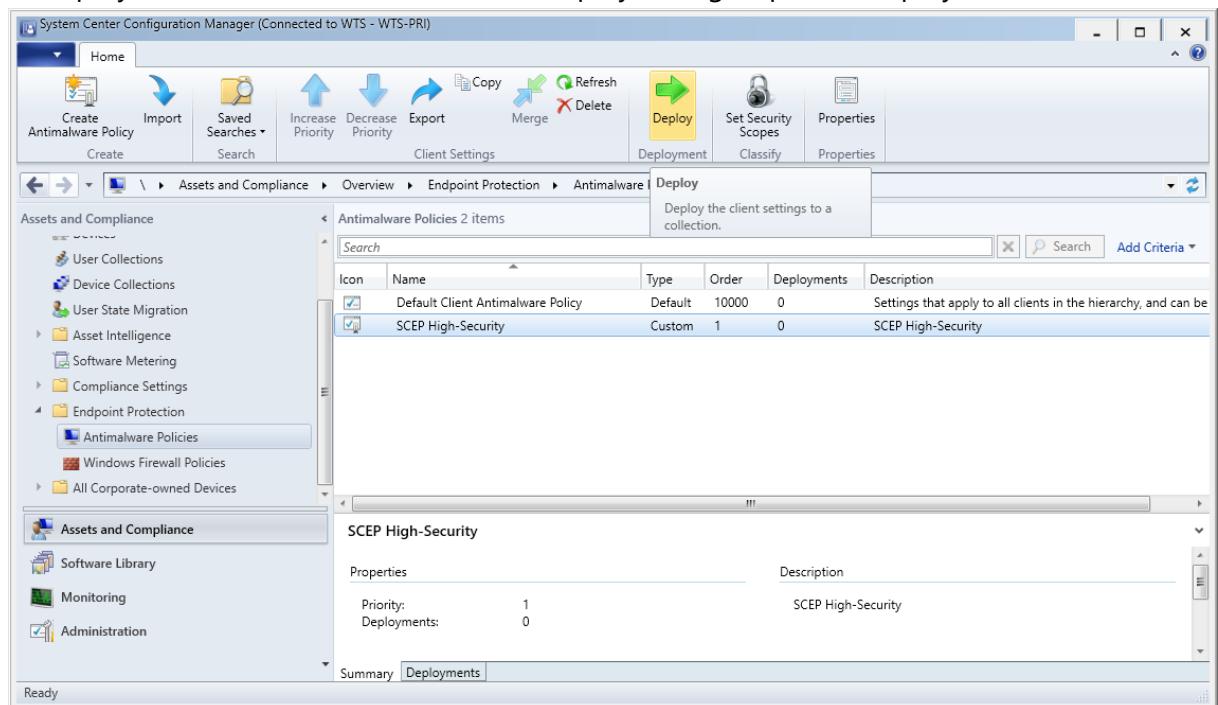
Icon	Name	Type	Order	Deployments	Description
<input checked="" type="checkbox"/>	Default Client Antimalware Policy	Default	10000	0	Settings that apply to all clients in the hierarchy, and can be
<input checked="" type="checkbox"/>	SCEP High-Security	Custom	1	0	SCEP High-Security

Deploy an antimalware policy to client computers

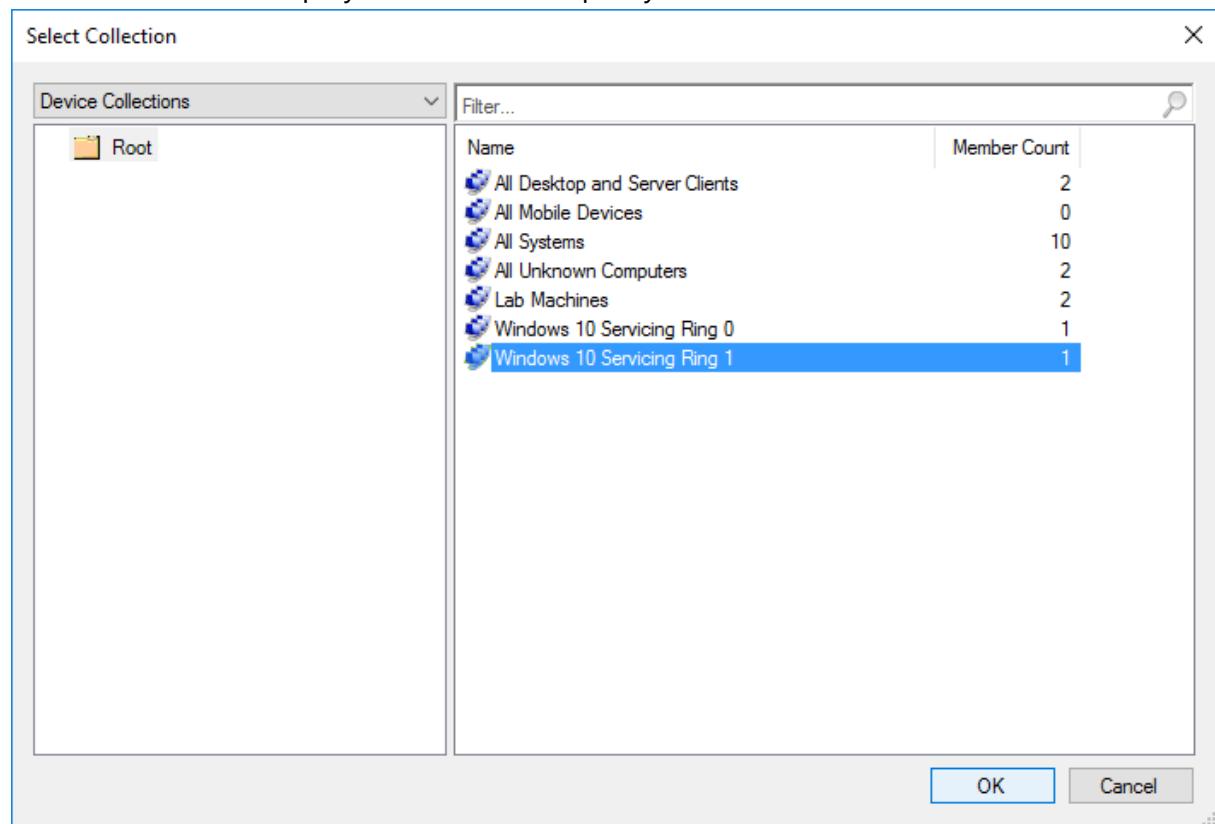
1. In the Configuration Manager console, click Assets and Compliance.
2. In the Assets and Compliance workspace, expand Endpoint Protection, and then click Antimalware Policies.



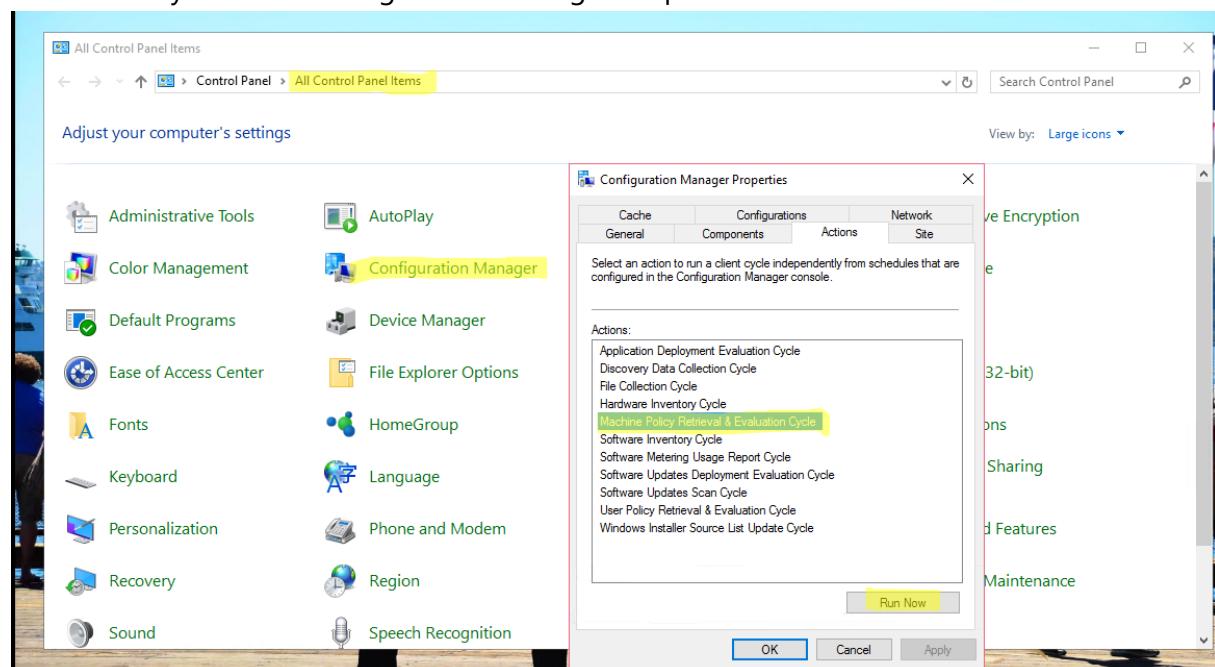
3. In the Antimalware Policies list, select the "SCEP High-Security" antimalware policy to deploy. Then, on the Home tab, in the Deployment group, click Deploy.



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.

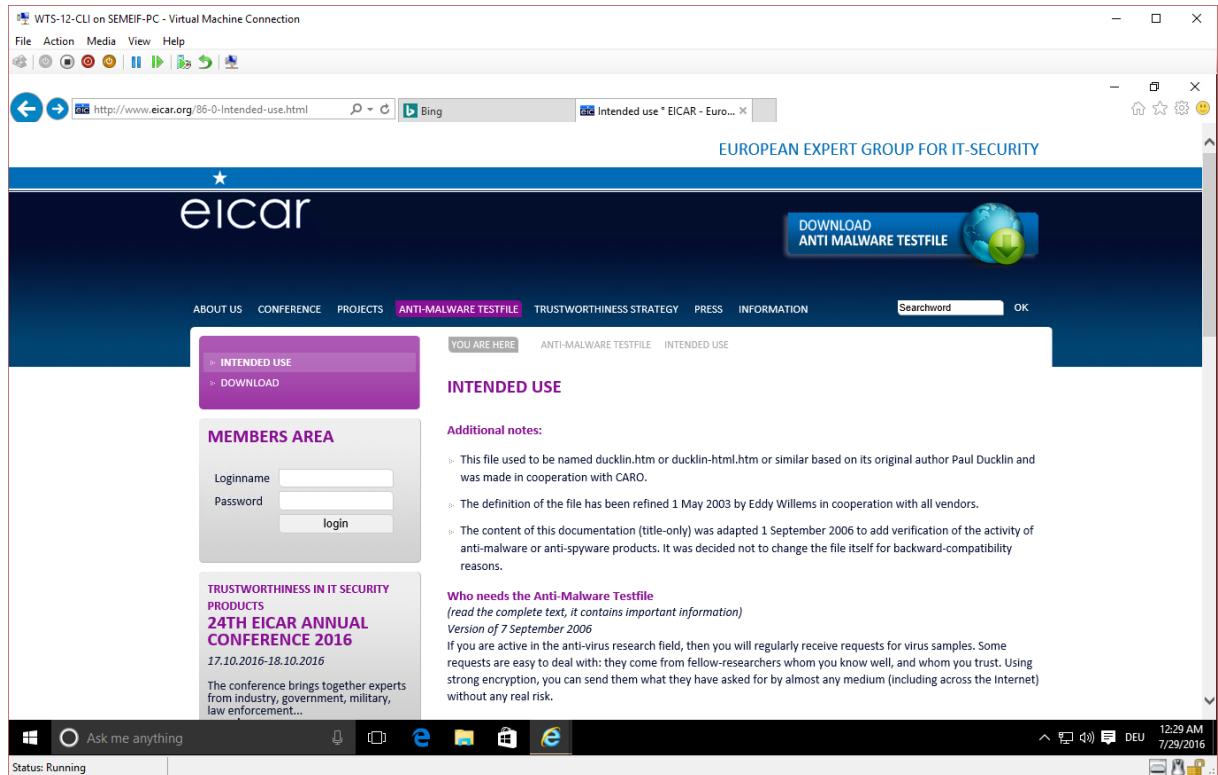


5. Log on as corp\admin to the WTS-10-CLI and run the Machine Policy Retrieval & Evaluation Cycle in the Configuration Manager Properties on the Actions tab.

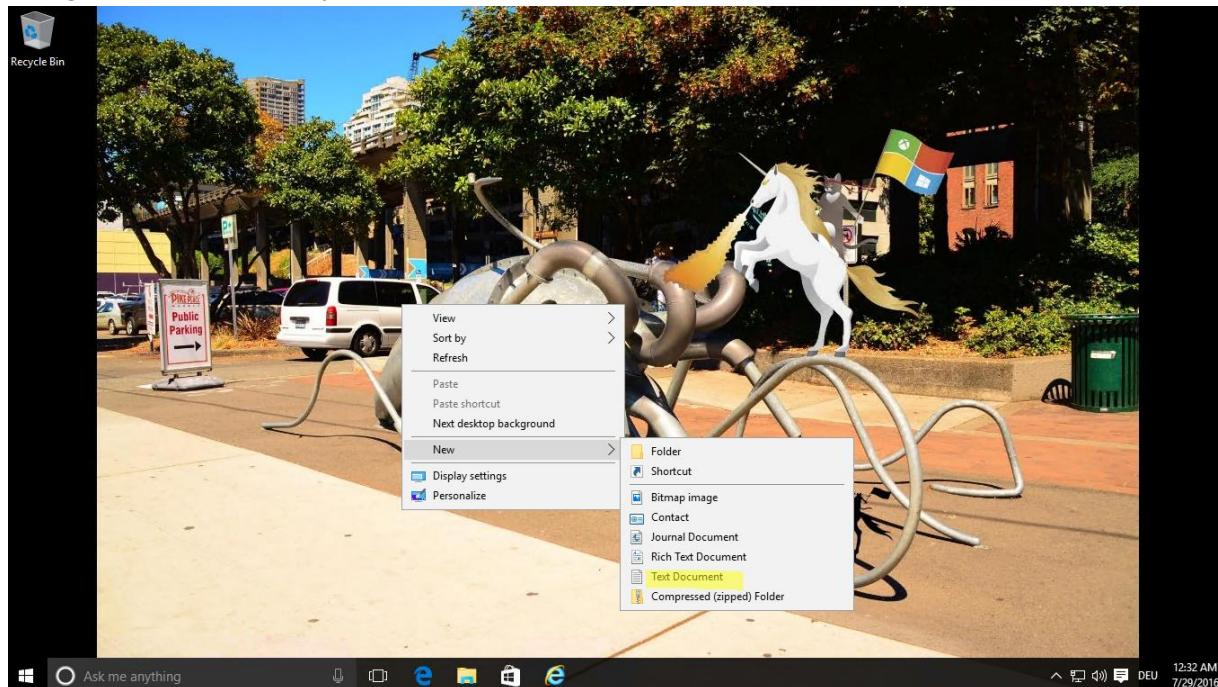


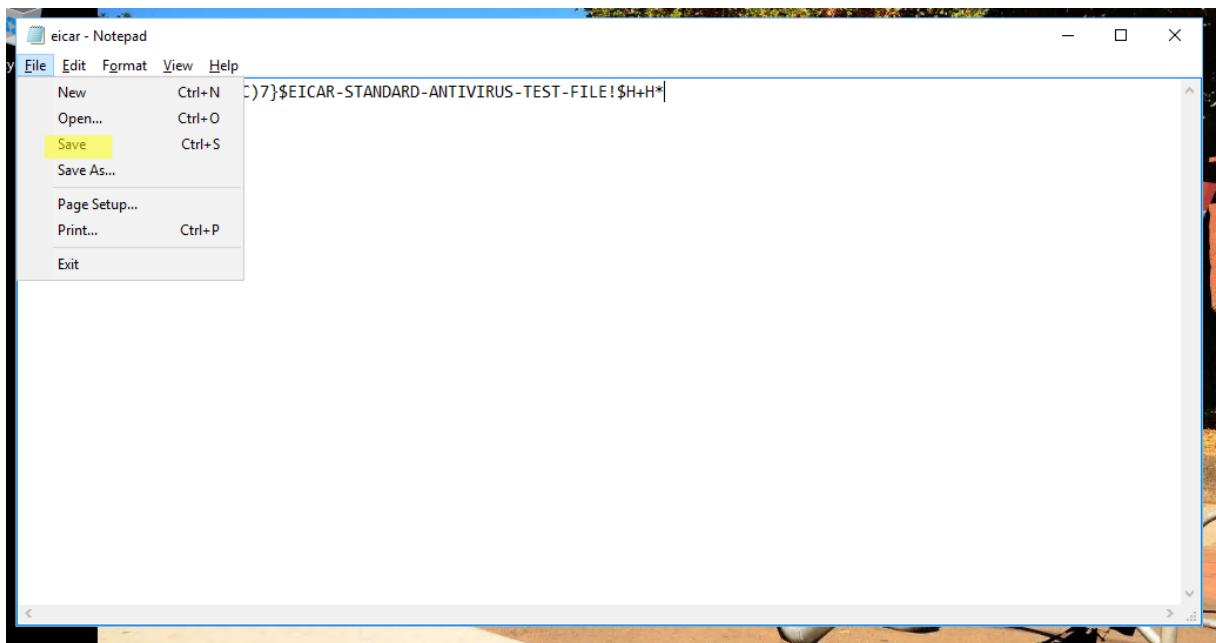
Let's have some fun and bring some Malware on a client machine.

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

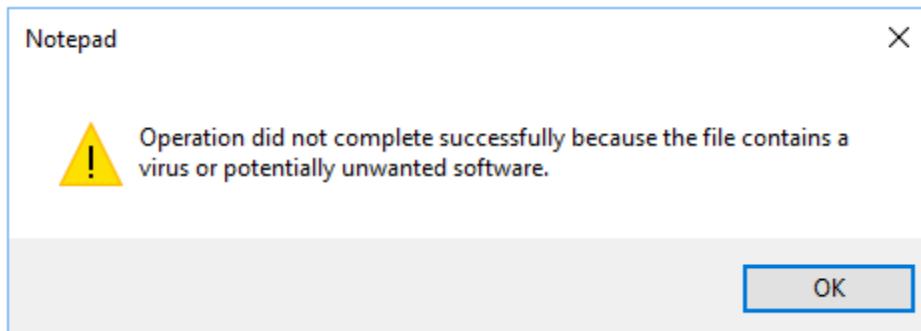


2. Scroll down to until you see the eicar Test String which starts with "X5O!P%@AP[4]\".
3. Copy the string into your clipboard, create a text document on the desktop, paste the string into the file and try to save it.





- 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".

A screenshot of the eicar.org website. The header reads "EUROPEAN EXPERT GROUP FOR IT-SECURITY". Below the header is a large blue button with the text "DOWNLOAD ANTI MALWARE TESTFILE" and a globe icon with a green downward arrow. At the bottom of the page, there is a navigation bar with links for "DISHINNESS STRATEGY", "PRESS", "INFORMATION", a search bar, and an "OK" button. The footer contains the text "LWARE TESTFILE INTENDED USE".

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

Download area using the standard protocol http

eicar.com	eicar.com.txt	eicar_com.zip	eicarcom2.zip
68 Bytes	68 Bytes	184 Bytes	308 Bytes

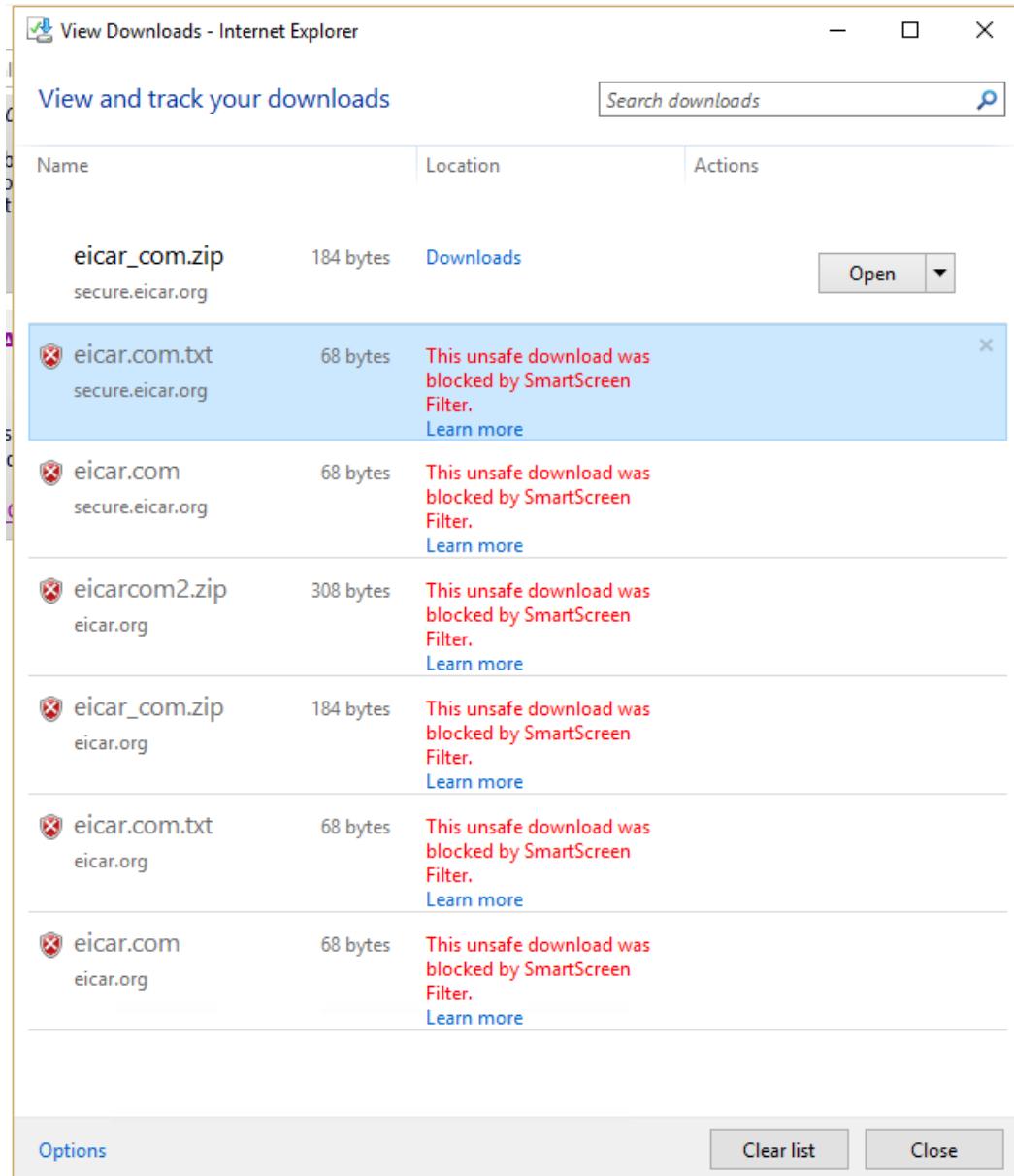
Download area using the secure, SSL enabled protocol https

eicar.com	eicar.com.txt	eicar_com.zip	eicarcom2.zip
68 Bytes	68 Bytes	184 Bytes	308 Bytes

8. There will be several warnings like this.

The screenshot shows a Windows file download dialog titled "1 Interrupted Action". It displays an error message: "An unexpected error is keeping you from copying the file. If you continue to receive this error, you can use the error code to search for help with this problem. Error 0x800700E1: Operation did not complete successfully because the file contains a virus or potentially unwanted software." Below the message, there is a preview of the file "eicar[1]" which is identified as an "MS-DOS Application" with a size of 68 bytes, last modified on 7/29/2016 at 12:37 AM. Three buttons are visible: "Try Again", "Skip", and "Cancel". To the right of the dialog, a sidebar titled "Download area using the standard protocol http" and "Download area using the secure, SSL enabled protocol https" lists the same four EICAR test files with their respective sizes: eicar.com (68 Bytes), eicar.com.txt (68 Bytes), eicar_com.zip (184 Bytes), and eicarcom2.zip (308 Bytes). A link "to delete the test file from your PC" is present. At the bottom of the sidebar, a note explains that EICAR cannot provide AV scanner support and directs users to contact their vendor's support. A footer at the bottom of the screen states "© 1998-2016 - EICAR - European Institute for Computer Anti-Virus Research e.V." and "realized by trivent media & design".

9. At the end 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.

The screenshot shows the System Center Configuration Manager interface. The title bar says "System Center Configuration Manager (Connected to WTS - WTS-PRI)". The left navigation pane is expanded, showing "Monitoring" as the selected category. Under "Monitoring", "Endpoint Protection Status" is selected. The main content area is titled "System Center Endpoint Protection Status". A dropdown menu labeled "Collection:" shows "Windows 10 Servicing Ring 1". Below this, a section titled "Security State - Last Updated 7/29/2016 2:12:05 AM" displays various statistics:

Category	Value
Total active clients in this collection protected with Endpoint Protection:	100.0%
Active clients protected with Endpoint Protection:	1 / 1 (100.0%) affected by malware. Clients can be in multiple states.
Total devices in this collection:	1
Endpoint Protection clients in this collection that are active:	1
Active clients protected with Endpoint Protection:	1
Active clients at risk:	0
Clients in this collection that are inactive or not installed:	0
Endpoint Protection agent not yet installed:	0
Endpoint Protection agent not supported on platform:	0
Malware remediation status:	0 Remediation failed, 0 Full scan required, 0 Restart required, 0 Offline scan required, 0 Client settings modified by malware, 1 Malware remediated in the last 24 hours.

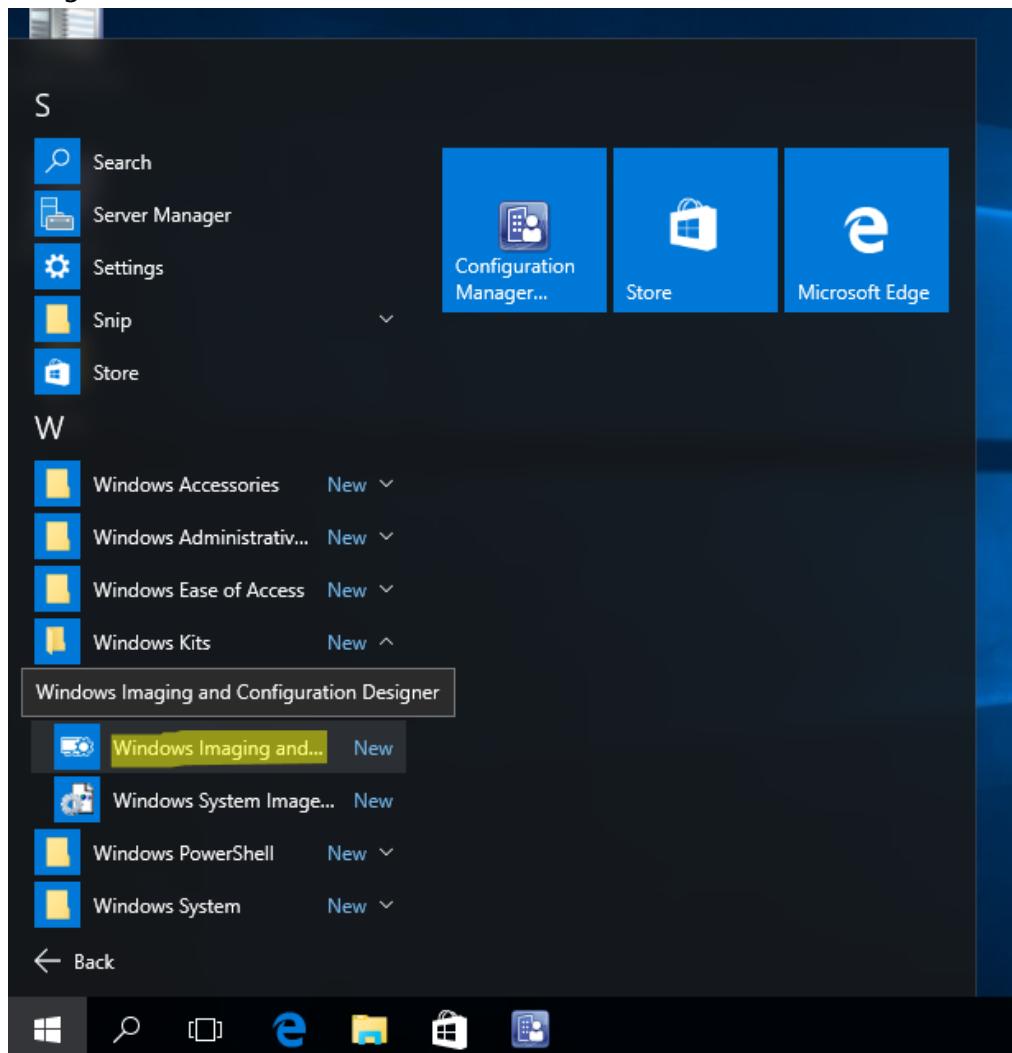
4. Review Status. If the status is empty, click on "Run Summarization".

The screenshot shows the System Center Configuration Manager interface. The title bar says "System Center Configuration Manager". The left navigation pane is collapsed, showing "Monitoring" as the selected category. The main content area has a large green "Run Summarization" button. Below it, there is some text: "Endpoint Protection Status" and "Monitoring". The bottom of the screen shows a taskbar with icons for "Start", "File Explorer", "Task View", and "Search".

3. Lab guide part 3 – Security through Provisioning

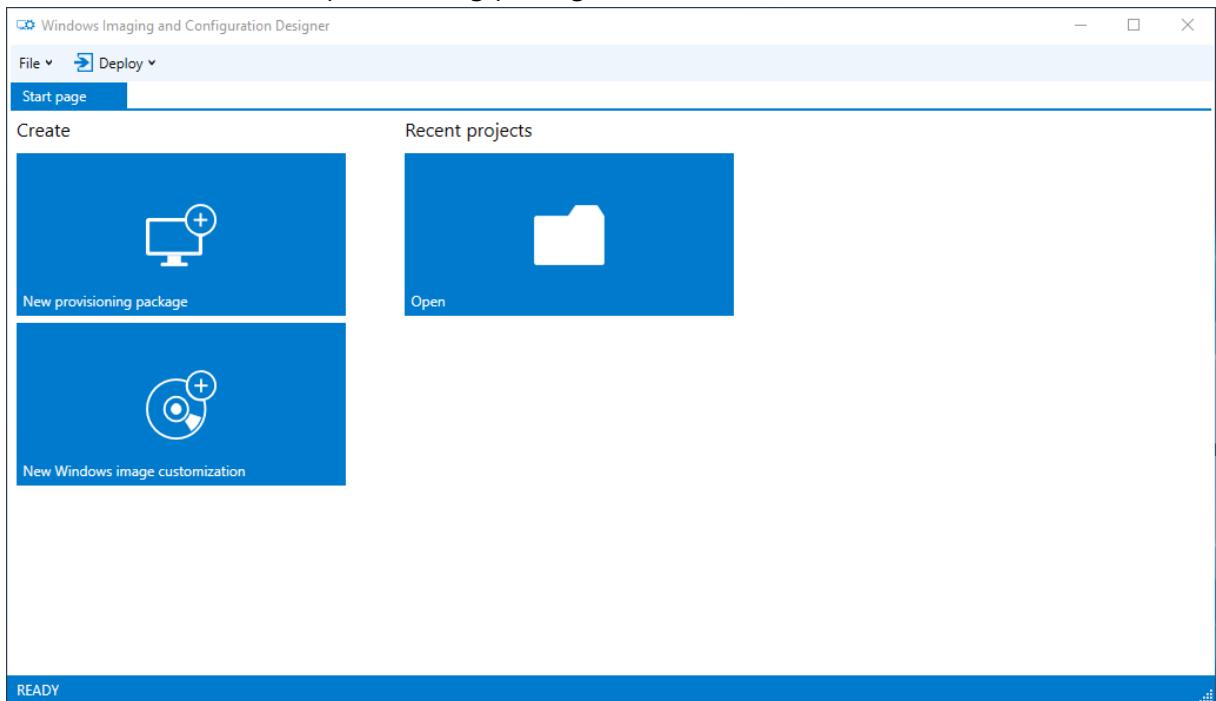
3.1. Create Provisioning Package with ICD (Time: 10:00)

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.

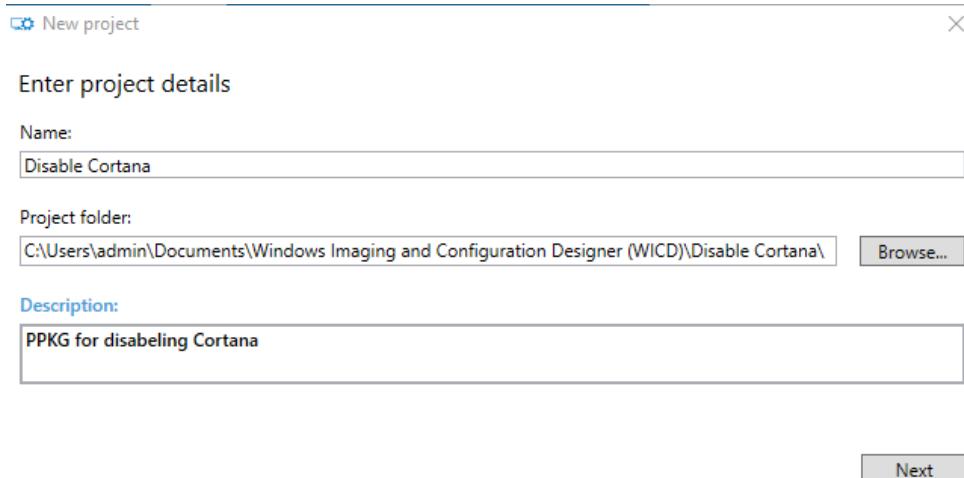


2. Click "Yes" on the UAC prompt.

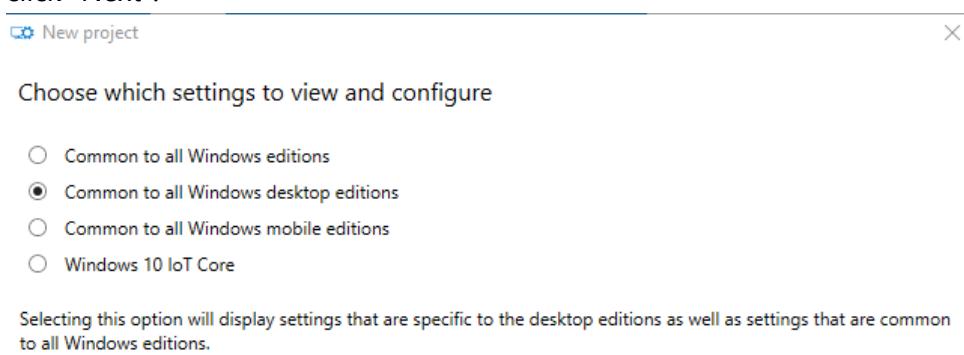
3. In the ICD click on “New provisioning package”.



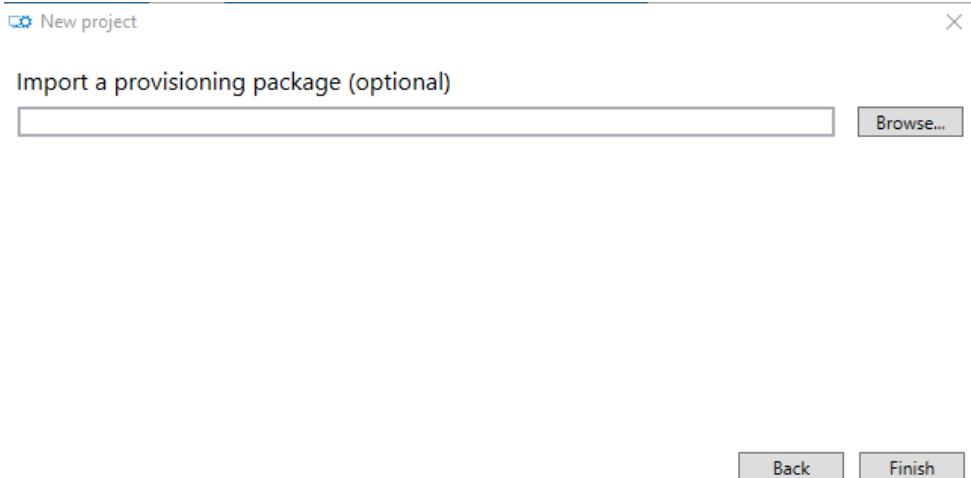
4. Enter the project details and click “Next”.



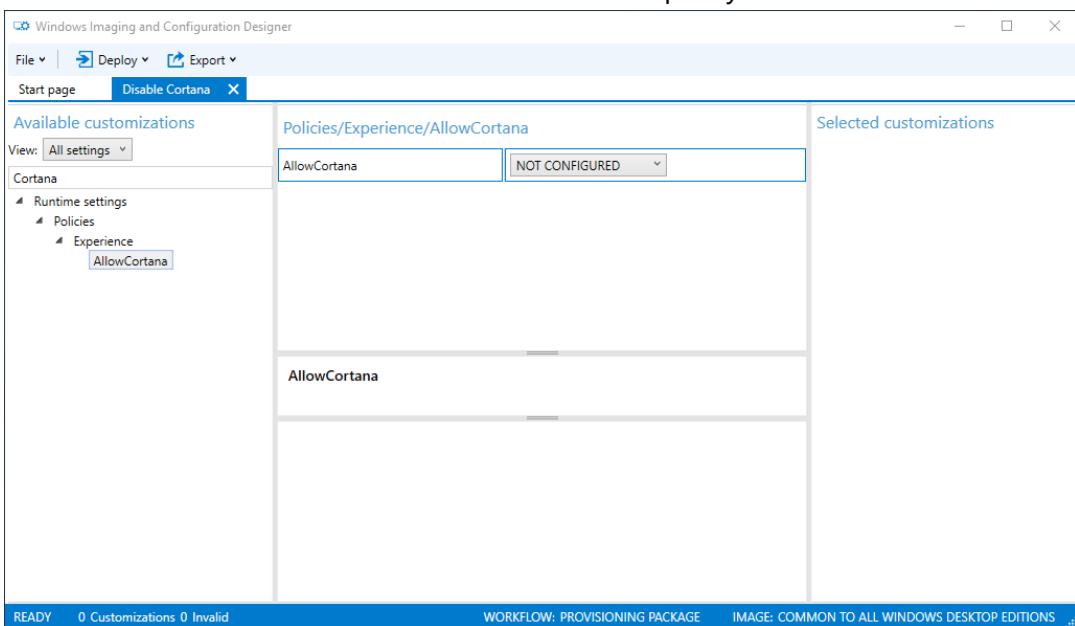
5. On the Edition selection screen select “Common to all Windows desktop editions” and click “Next”.



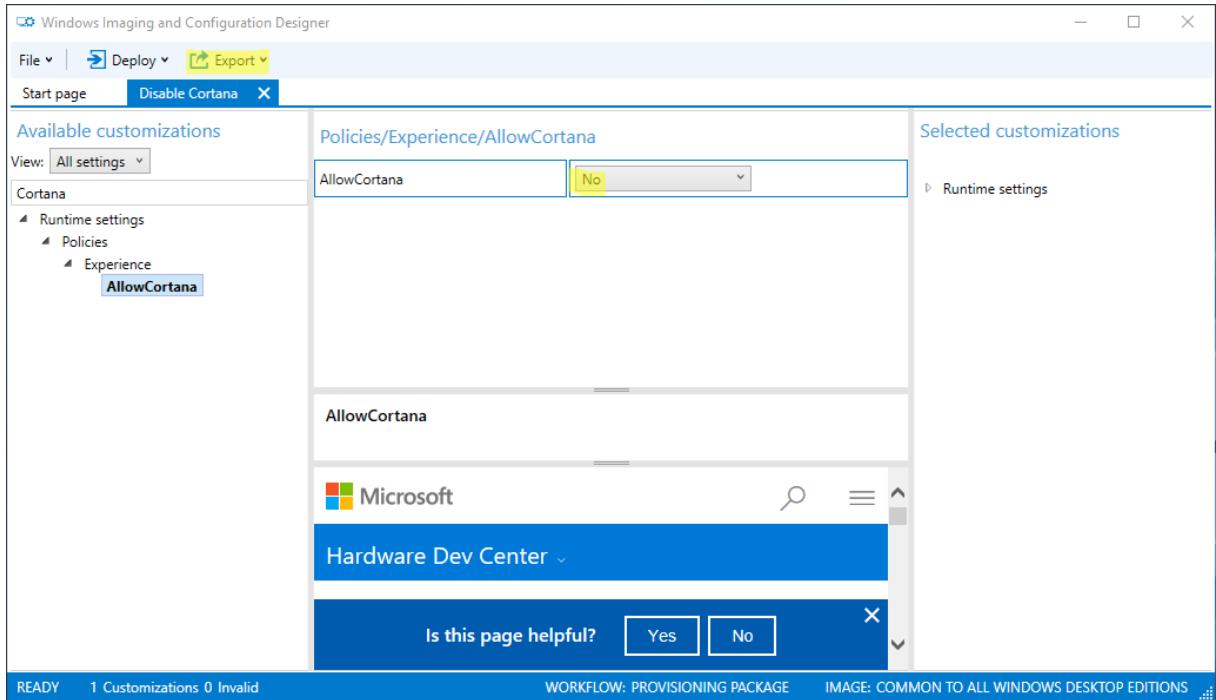
6. On the “Import a provisioning package” screen click “Finish”.



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



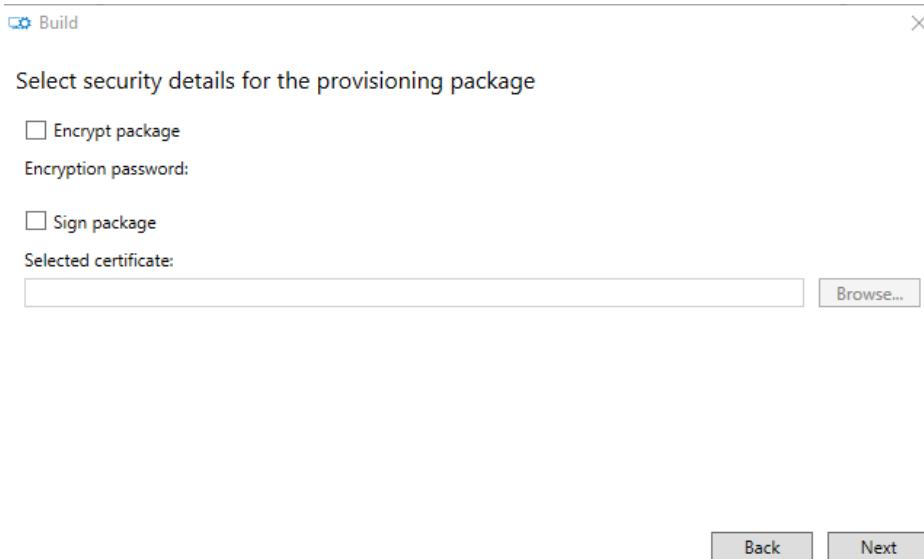
8. Set the policy to "No" and click on "Export" → "Provisioning Package".



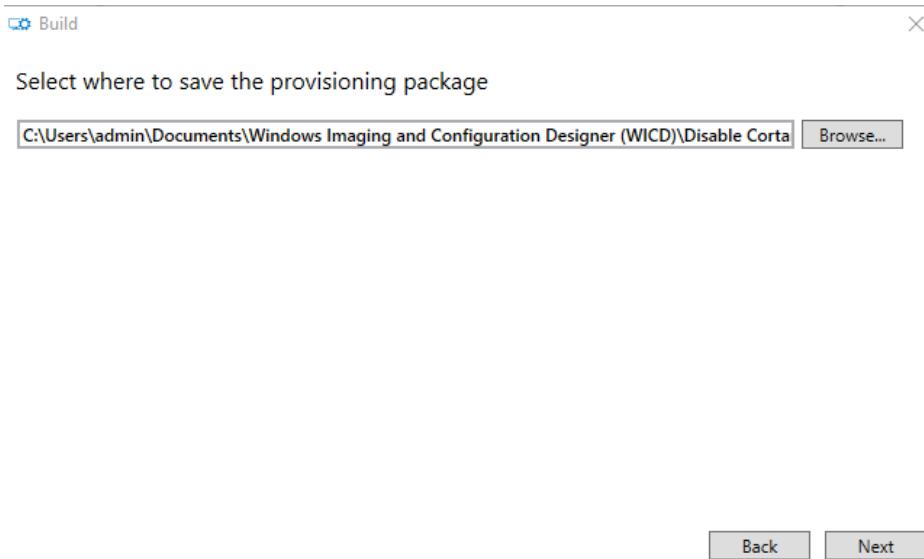
9. Select "IT Admin" as owner and click "Next".

This screenshot shows a configuration dialog for a provisioning package. It includes fields for 'Name' (set to 'Disable Cortana'), 'ID' (set to 'ad6c4e93-45fb-4786-b563-72d19579f969'), 'Version (in Major.Minor format)' (set to '1.0'), 'Owner:' (set to 'IT Admin'), and 'Rank (between 0 - 99):' (set to '0'). At the bottom right is a 'Next' button.

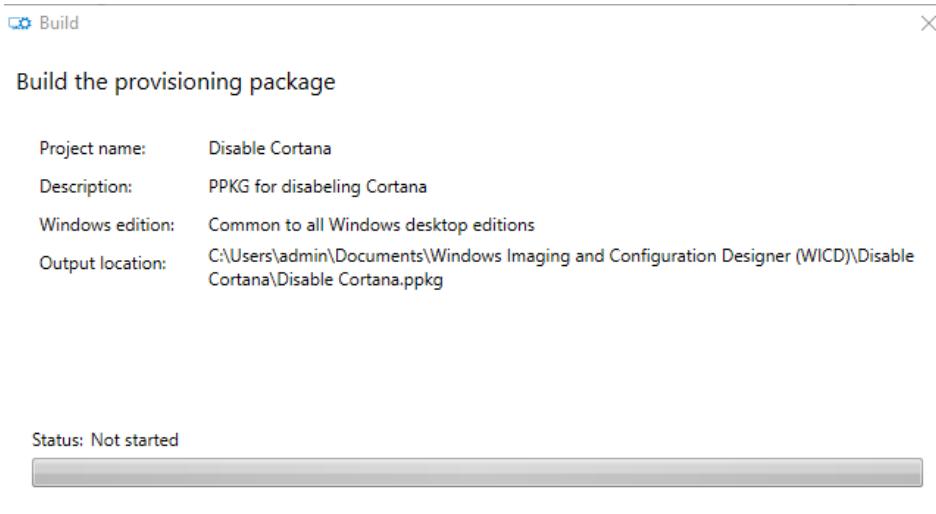
10. On the "Select security details" screen leave the defaults and click "Next".



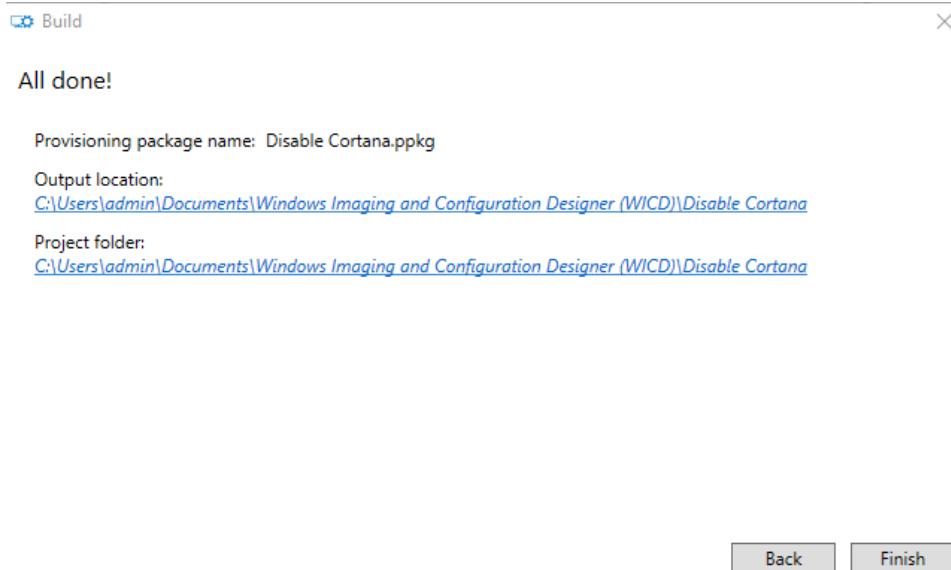
11. Remember the path where the package is stored and click "Next".



12. On the "Build the provisioning package" click "Build".



13. Open the output location.

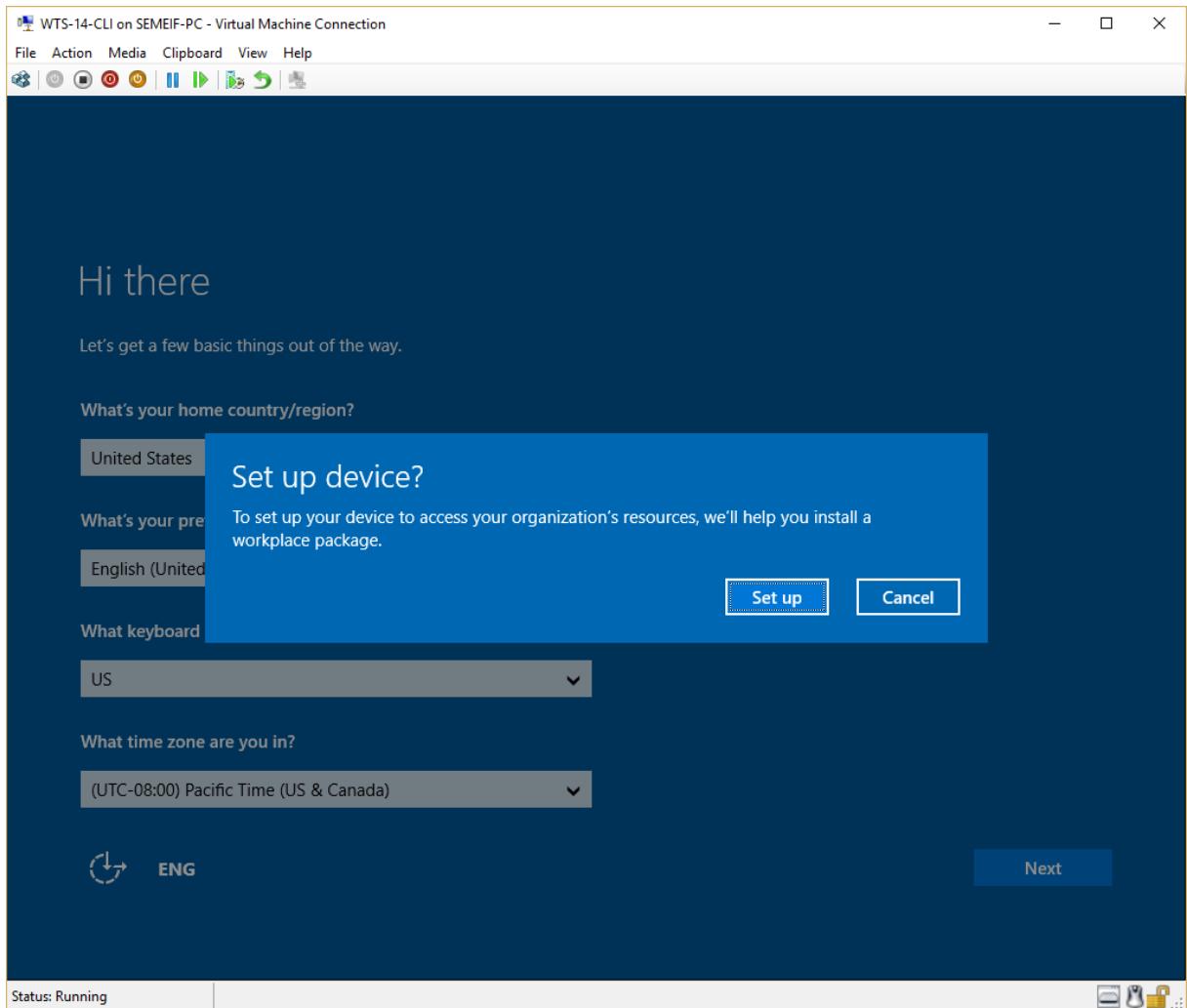


14. And copy the file <Disable Cortana.ppkg> to the App folder on the desktop of the WTS-04-CAS machine.

3.2. Apply PPKG in OOBE (optional)

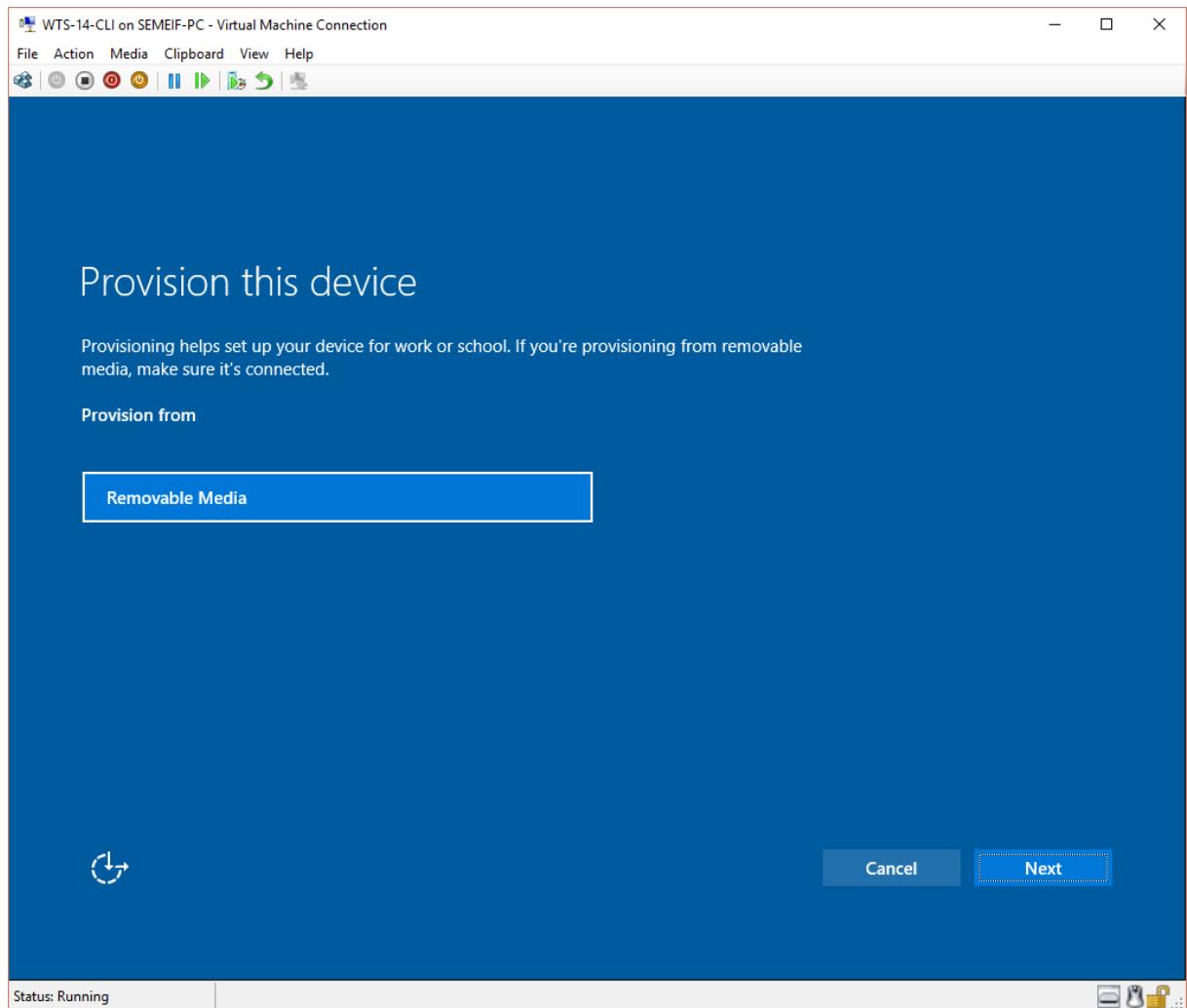
1. Due to the restrictions that you can't insert a USB stick to VM during the OOBE this part of the Module will only describe the theory.

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

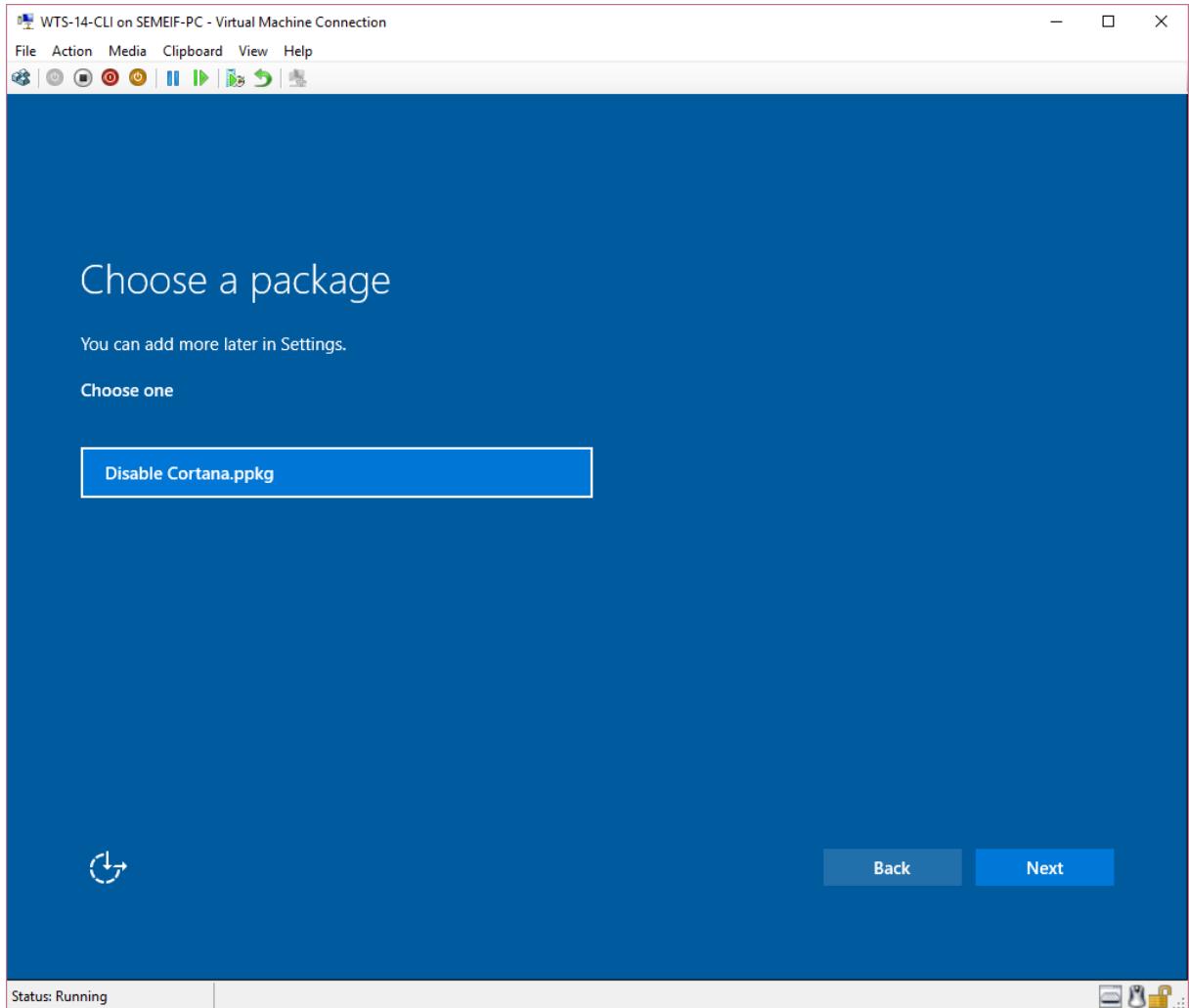


3. Insert USB stick or any other removable media to the machine.

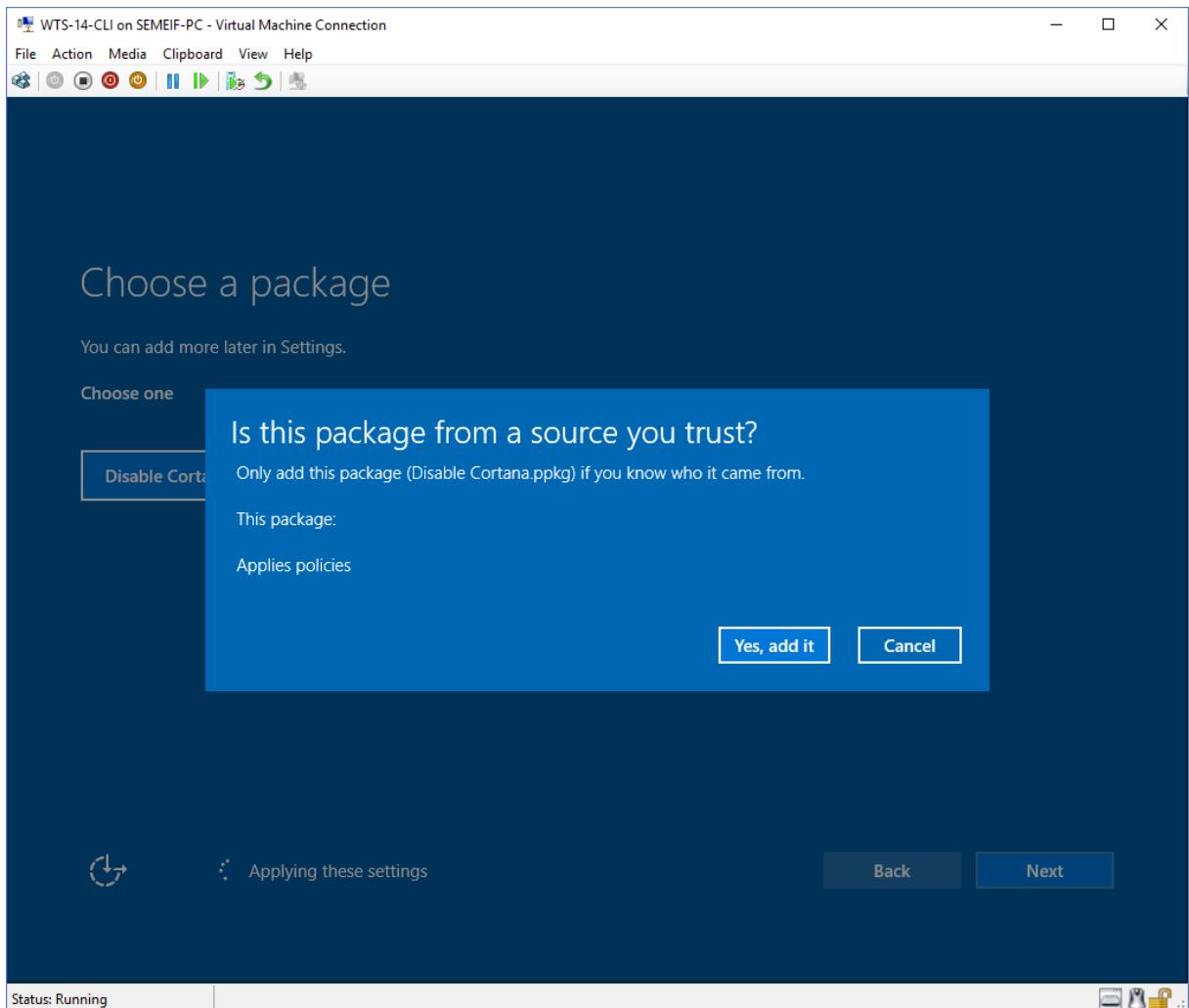
4. Select "Removable Media" and click "Next".



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

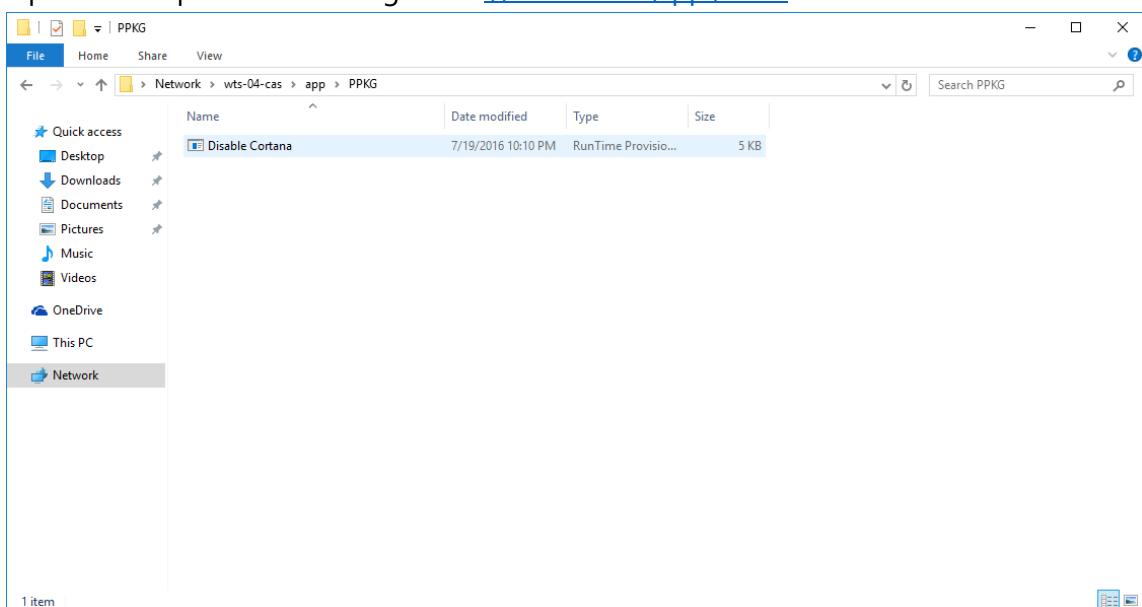


- When the package is not digitally signed you need to confirm the security warning.
Click on "Yes, add it".

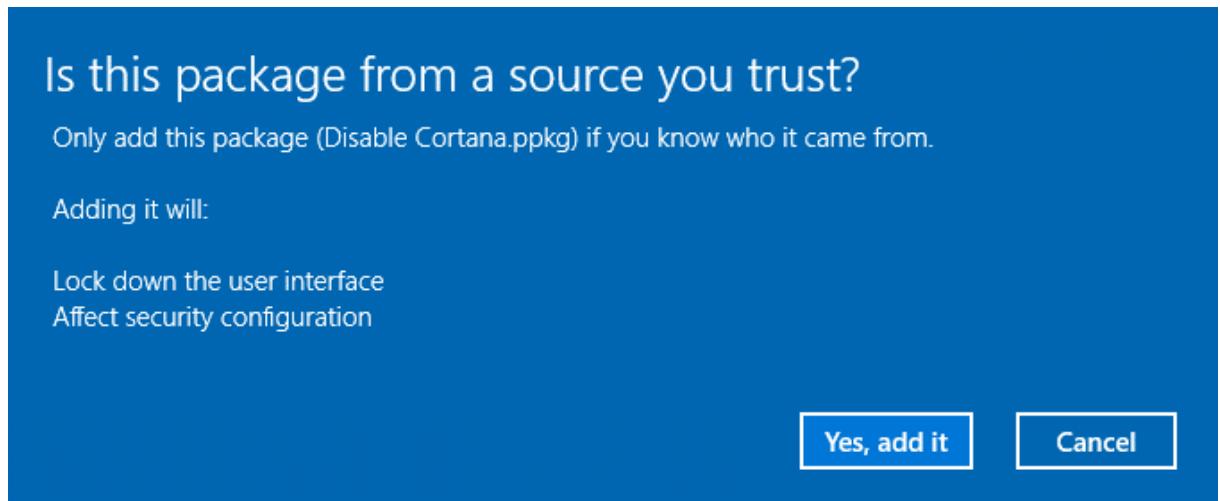


3.3. Apply PPKG while user is already logged on

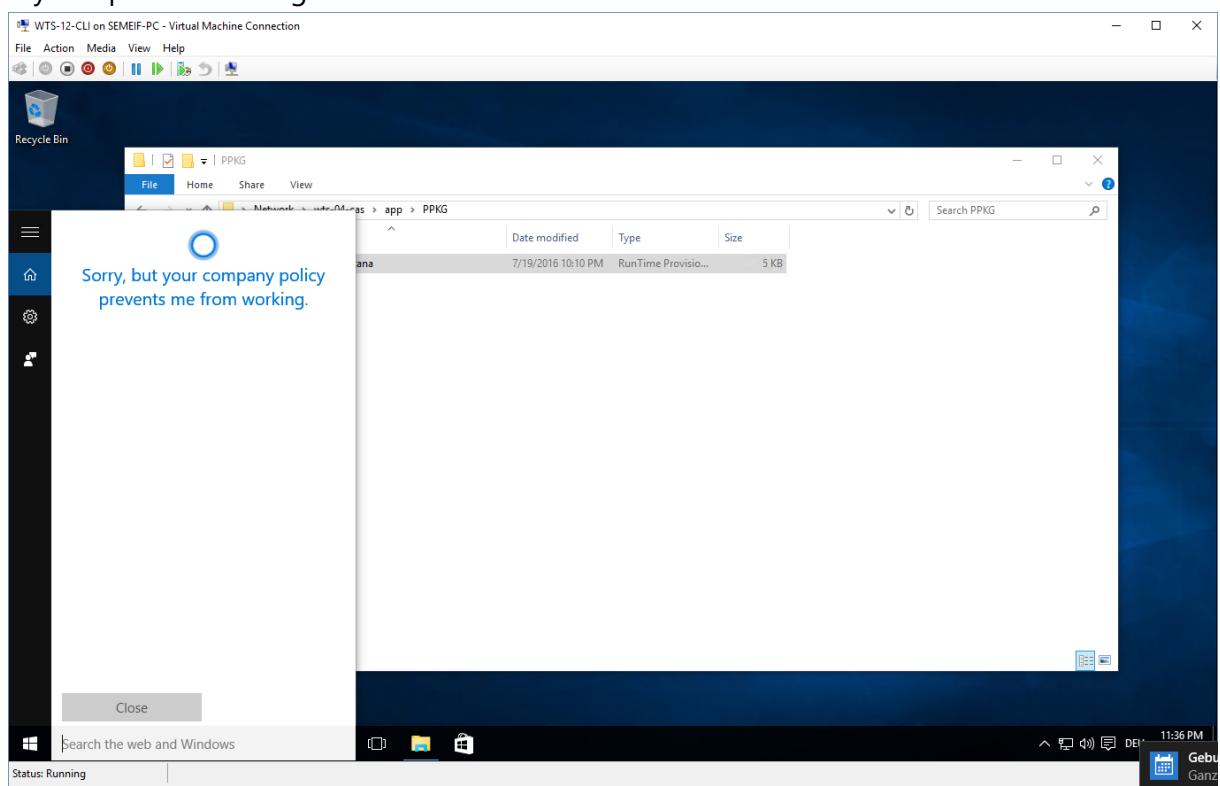
- On the WTS-12-CLI machine open Cortana and sign in with a Microsoft account.
- Open "File Explorer" and navigate to <\\wts-04-cas\app\PPKG>.



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".

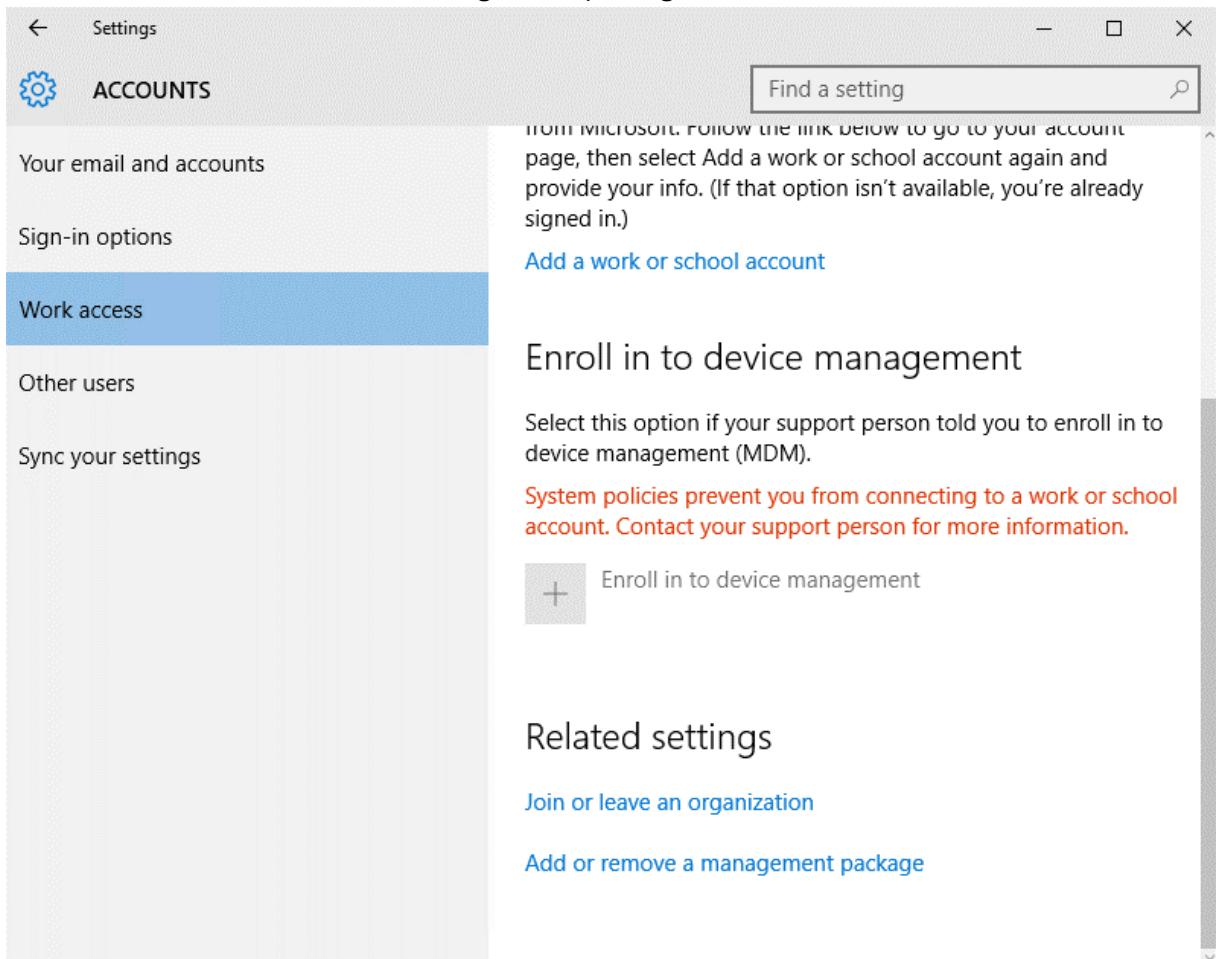


6. Try to open Cortana again and see the result.

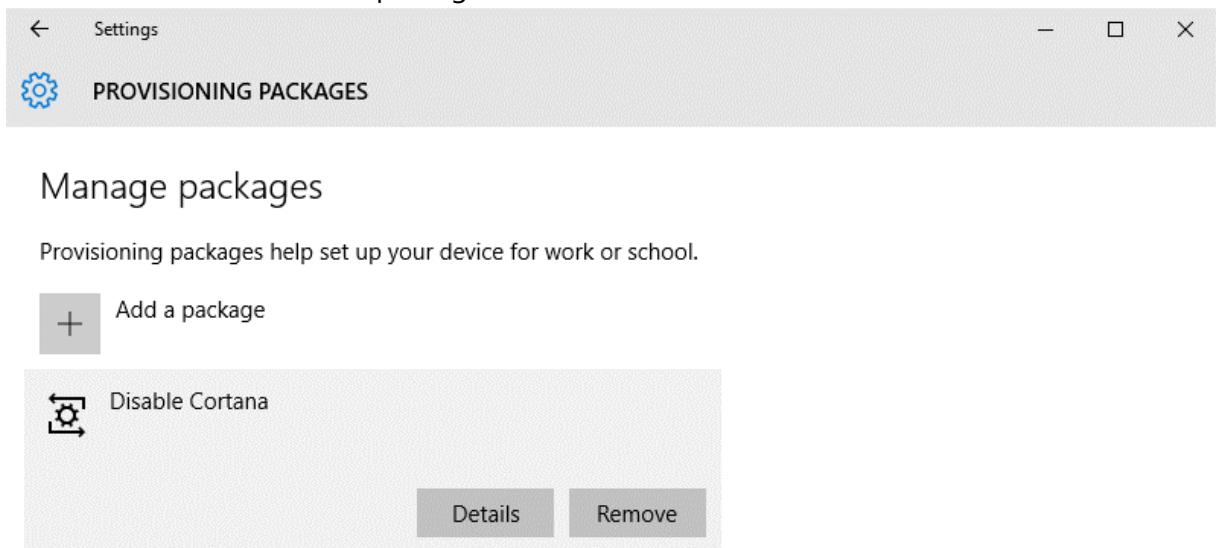


Remove Provisioning package

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