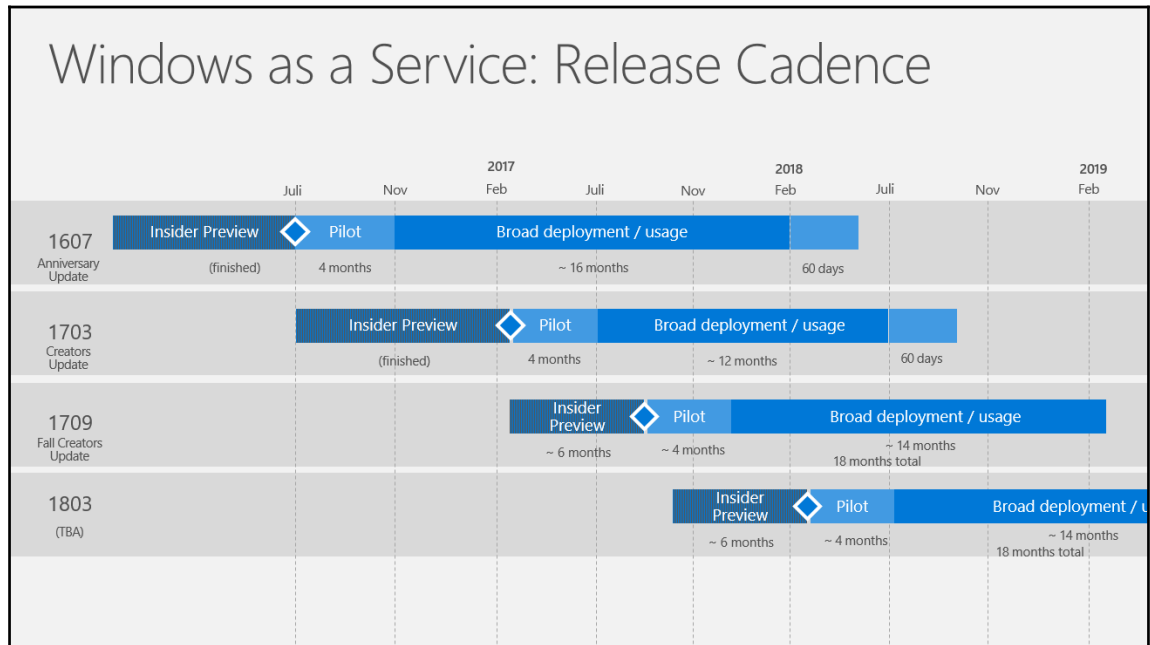
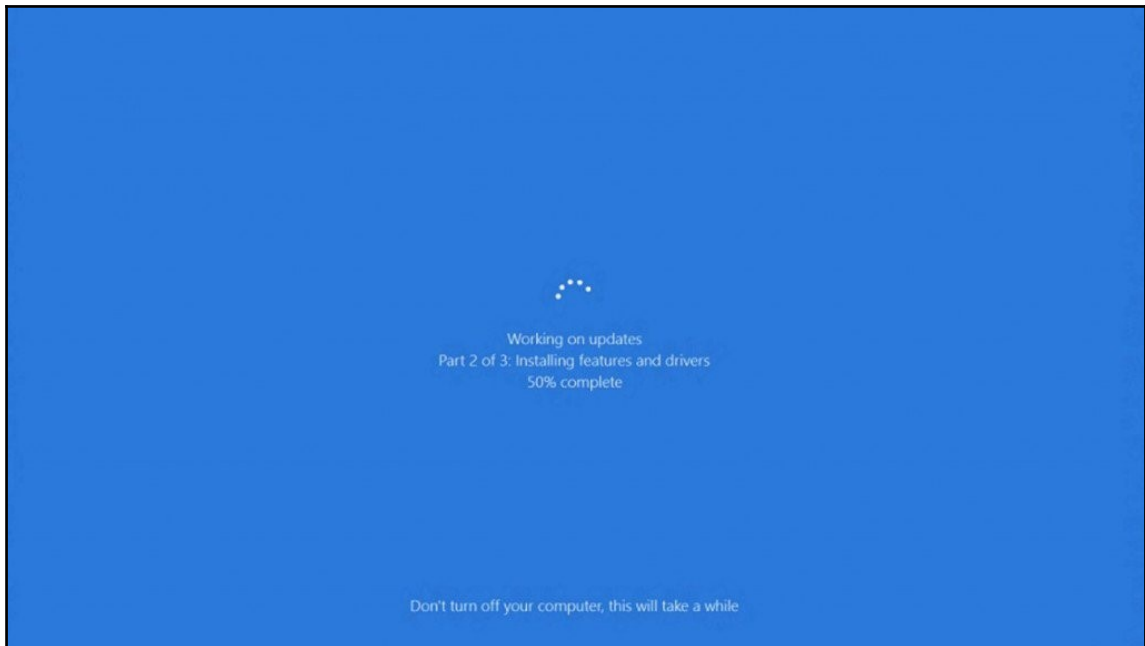
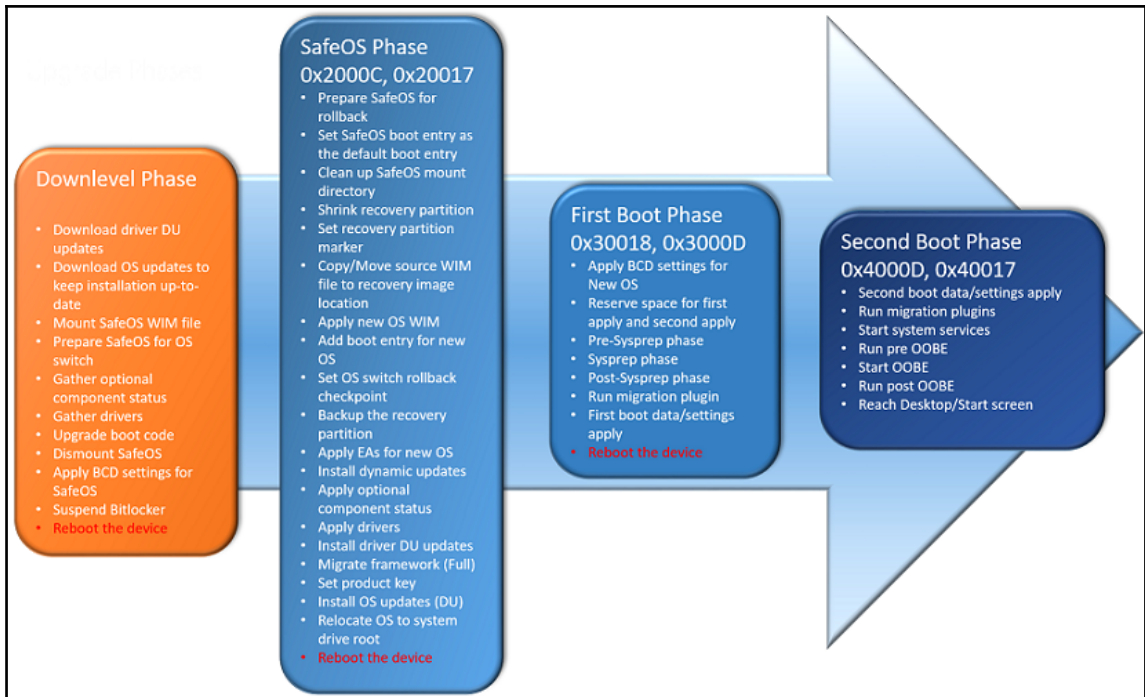


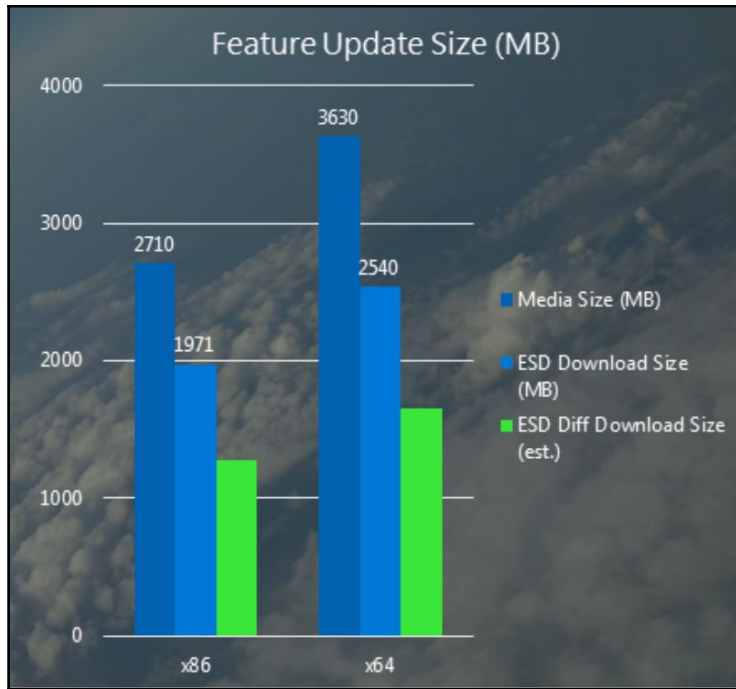
Chapter 01: Installation and Upgrading



Windows 10: Comparing Servicing Choices

Differentiator	Current Branch	Current Branch for Business	Long Term Servicing Branch
Primary purpose	Pilot Deployments	Broad Deployment	Special Devices
Deployment timeline	Soon after release	About 4 months (or more) after release	Any time during lifecycle
Release frequency	About every six months		Approximately every 2-3 years
Updates	All security fixes, moderate bar for other fixes		All security fixes, high bar for other fixes
Apps	All in-box apps		No in-box apps (except system apps)
Browser	Edge and Internet Explorer 11		Internet Explorer 11
Windows features	All		Excludes Cortana, Windows Store
Platform features	Win32, Universal Windows Platform		Win32, Universal Windows Platform





Chapter 02: Configuration and Customization

The screenshot shows the Windows Store interface for the 'Windows Configuration Designer' app. At the top, there are navigation tabs for 'Home', 'Apps', 'Games', 'Music', and 'Movies & TV'. A search bar is located in the top right corner. The main content area features a large blue header for the app, with the title 'Windows Configuration Designer' and the developer 'Microsoft Corporation'. A rating of 'Everyone' is shown. Below the header, it states 'You own this product.' and includes an 'Install' button. A section titled 'People also like' displays a row of eight recommended apps, each with its icon, name, rating, and price. Below this, there are sections for 'Screenshots' (showing four preview images of the app's interface) and 'Description' (providing details about the app's functionality). At the bottom, the 'Available on' section indicates that the app is compatible with 'PC'.

Home Apps Games Music Movies & TV Search

Windows Configuration Designer

Microsoft Corporation

Everyone

You own this product.

Install

People also like

Show all

App Name	Rating	Price
Delve	★★★★★	Free
UWP Community Toolkit Sample App	★★★★★	Free
Page Analyzer	★★★★★	Free
Microsoft HoloLens	★★★★★	Free
MicrosoftPrinttoPDF Settings	★★★★★	Free
Field Service Mobile	★★★★★	Free
Set up School PCs	★★★★★	Free
Microsoft Dynamics 365	★★★★★	Free

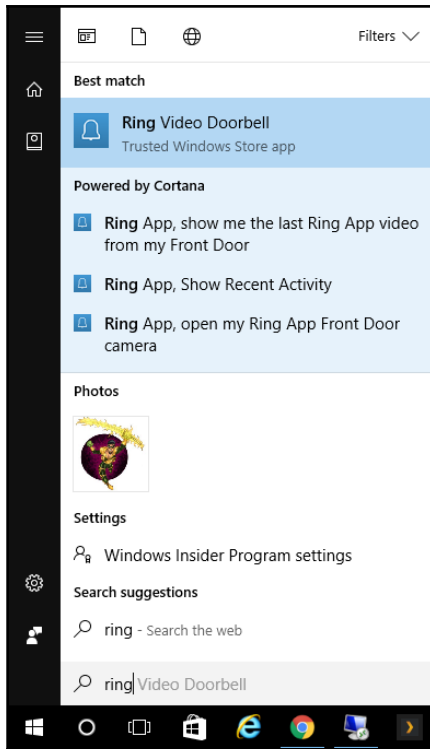
Screenshots

Description

Configure Windows devices without imaging. Use the Windows Configuration Designer App to simplify deployment of Windows devices at your organization. WCD allows configuration of many aspects of Windows devices including - Active Directory or Azure Active Directory domain join, Device name, Connect to Wi-Fi, enroll into Management, and install applications.

Available on

PC



I pulled up some info on factorization.

N 643456 (DCXLMMMCDLVI)

Factorization:
 $643456 = 2^7 \times 11 \times 457$

Divisors: 1, 2, 4, 8, 11, 16, ... (See all 32 divisors)

Categorization:

Characteristics:

Parity	Prime	Happy	Weird	Triangula
Even	X	X	X	X

Number line:

is 643456 a prime number

Tree **Filter** Copy Misc United Kingdom (English)

- toggle status -

Policy

- Internet Explorer 10
- Internet Explorer 11
- Internet Explorer 5/6
- Internet Explorer 7
- Internet Explorer 8
- Internet Explorer 9
- Machine Policy Settings Only
- Microsoft Edge
- Miscellaneous
- Office 2007
- Office 2010
- Office 2013
- Office 2016
- User Policy Settings Only
- Windows 10**
- Windows 2000
- Windows 7/2008R2
- Windows 8.1/Server 2012R2
- Windows 8/2012
- Windows Server 2003
- Windows Vista/2008
- Windows XP

Details Like Share

Policy	
Category Path	
Supported On	
Registry Key	
Value	
Admx	

Explanation


News

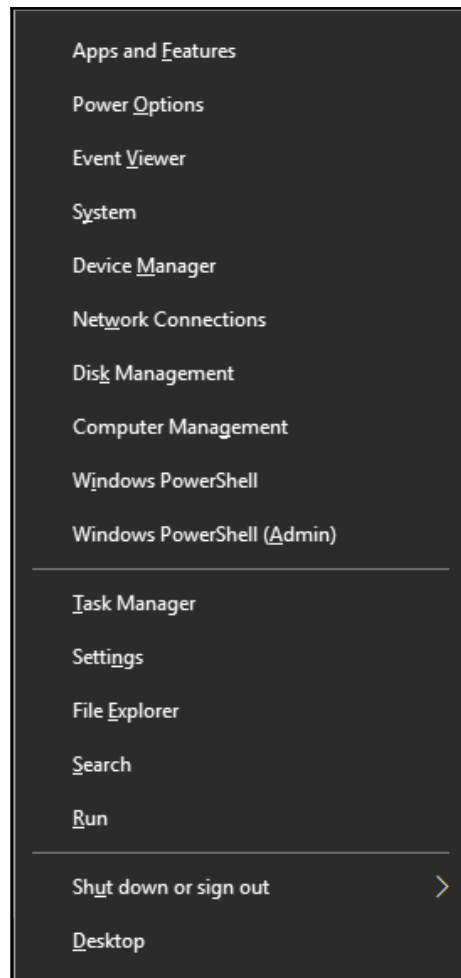
Facebook

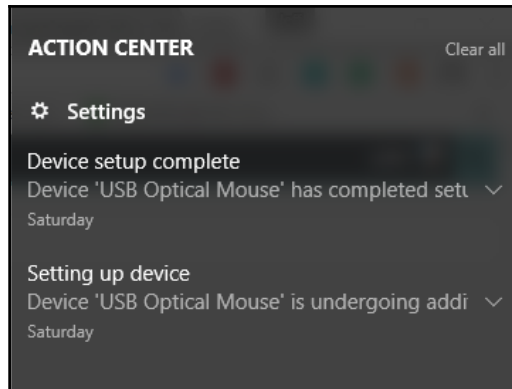
We have created a [Facebook page](#) to have a two-way communication channel. So feel free to provide any feedback, ask questions and get information about new releases and features:
<http://aka.ms/GPSatFB>

Cheers

Stephanus

© 2010-2016 Microsoft Corporation. All rights reserved [Terms of use](#) [Privacy & Cookies](#) [Contact](#) 





Apply policies to improve sign-in time

When a user is configured with a mandatory profile, Windows 10 starts as though it was the first sign-in each time the user signs in. To improve sign-in performance for users with mandatory user profiles, apply the Group Policy settings shown in the following table. (The table shows which operating system versions each policy setting can apply to.)

Group Policy setting	Windows 10	Windows Server 2016	Windows 8.1	Windows Server 2012
Computer Configuration > Administrative Templates > System > Logon > Show first sign-in animation = Disabled	✓	✓	✓	✓
Computer Configuration > Administrative Templates > Windows Components > Search > Allow Cortana = Disabled	✓	✓	✗	✗
Computer Configuration > Administrative Templates > Windows Components > Cloud Content > Turn off Microsoft consumer experience = Enabled	✓	✗	✗	✗

Set up assigned access


Assigned access

You can restrict a local standard user account so that it only has access to one Windows app. Choose an app that is designed to work properly in assigned access.


[Learn more](#)

To exit assigned access, press Ctrl+Alt+Del.

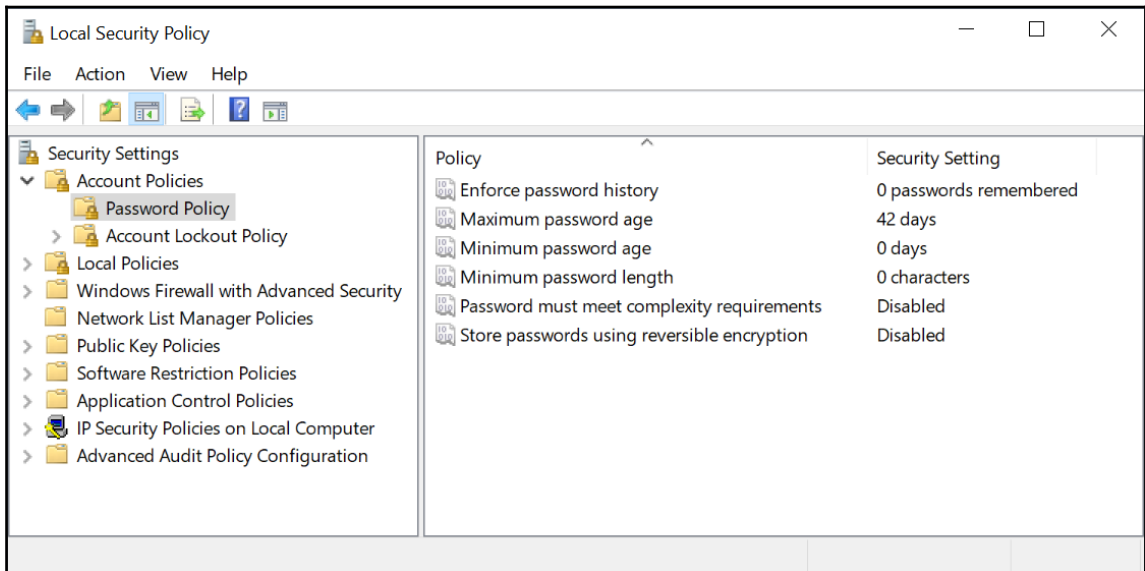
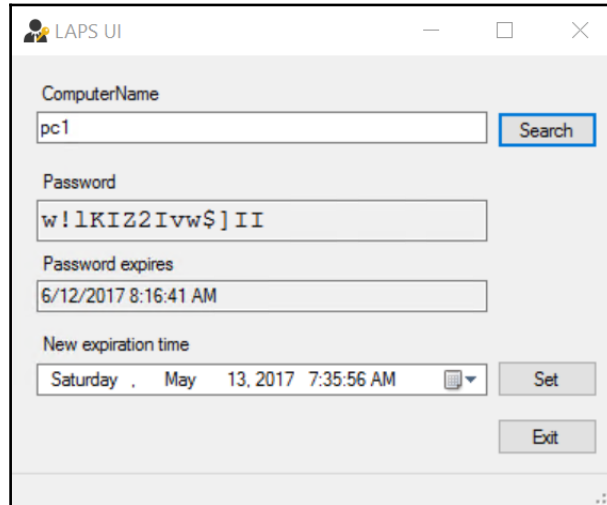
Choose which account will have assigned access

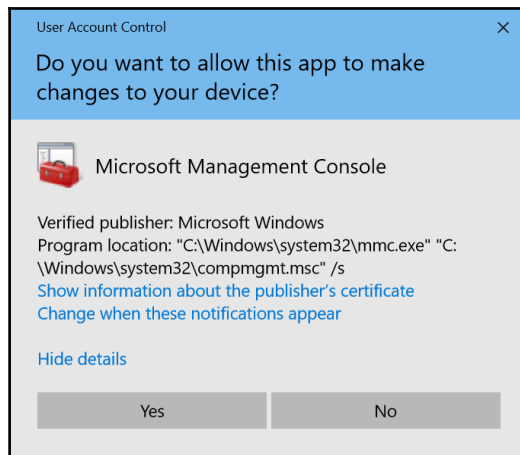
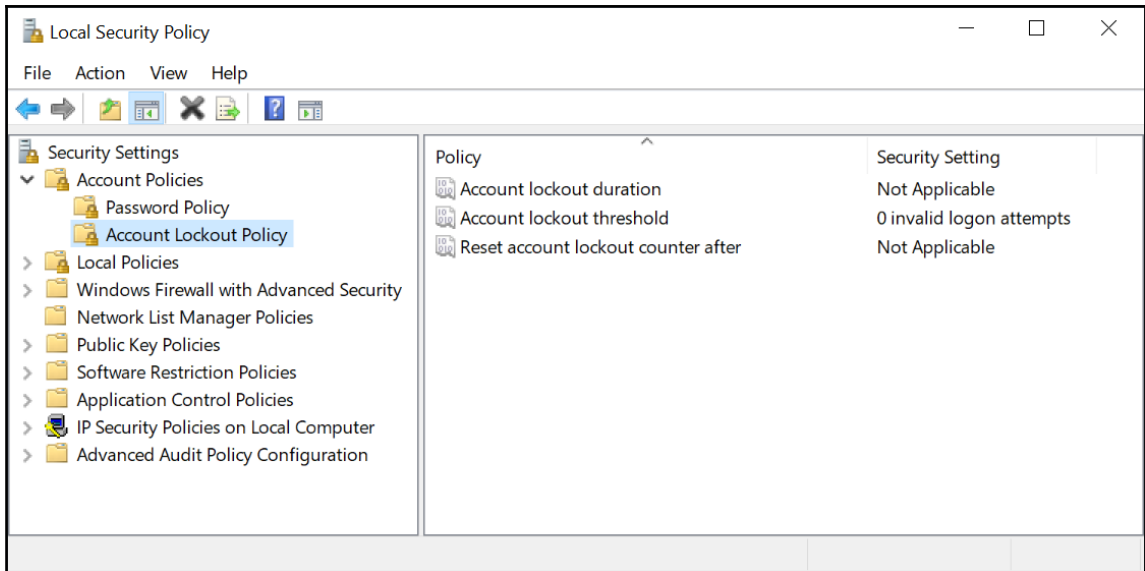
 Choose an account

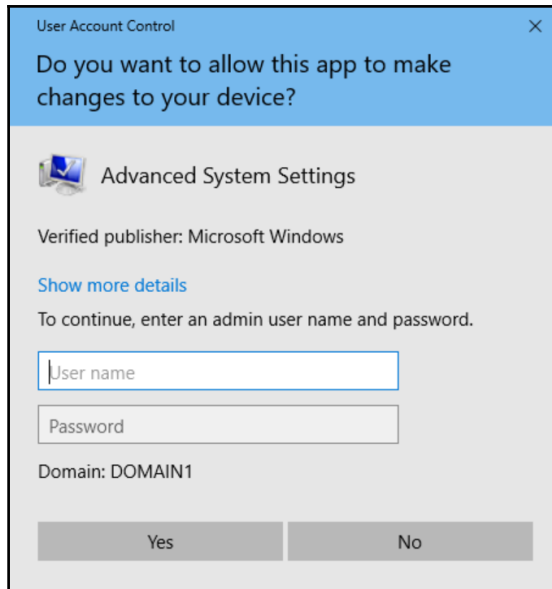
Choose which app this account can access

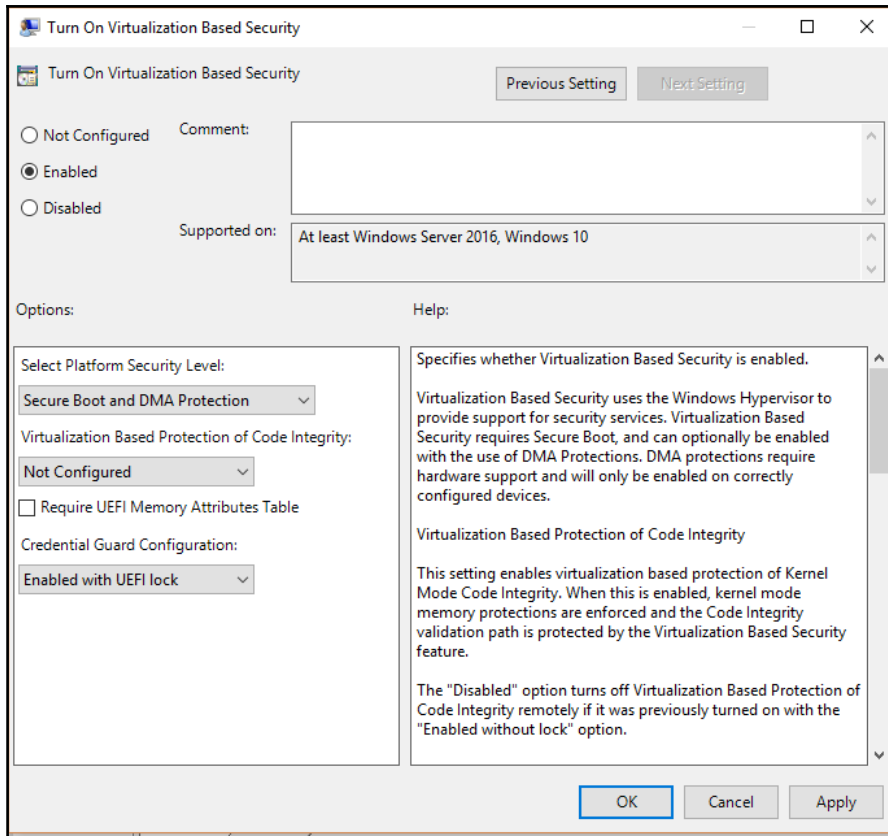
 Choose an app

Chapter 03: User Account Administration

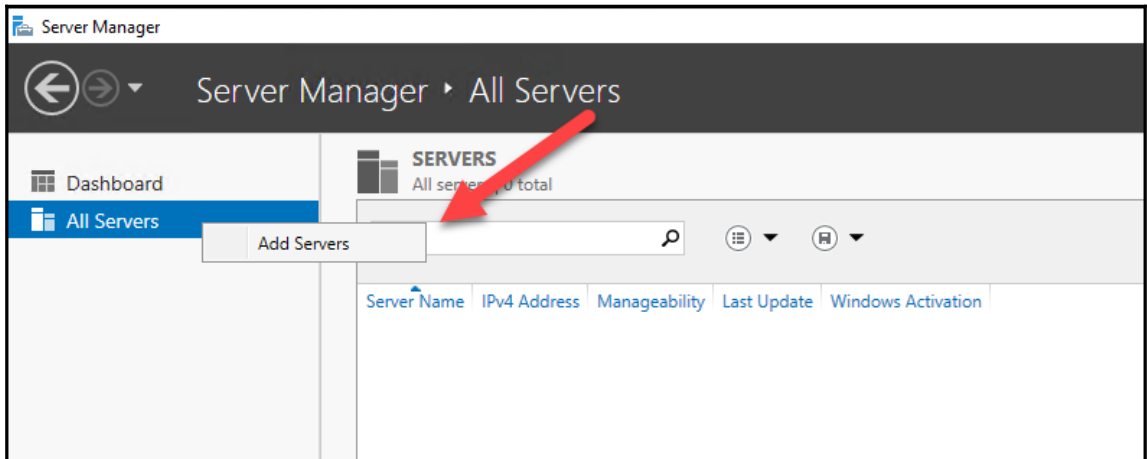
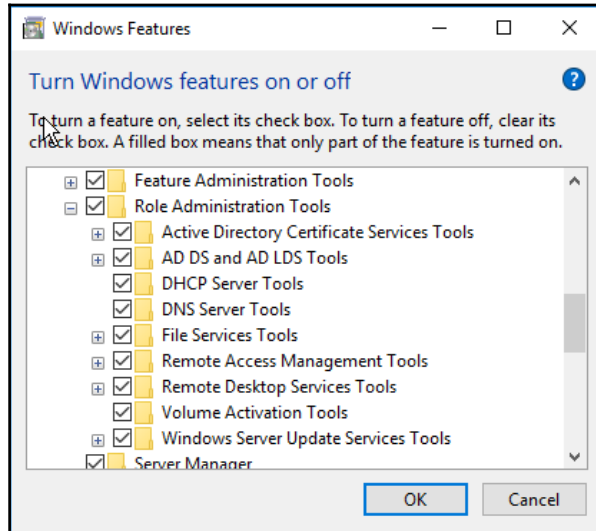


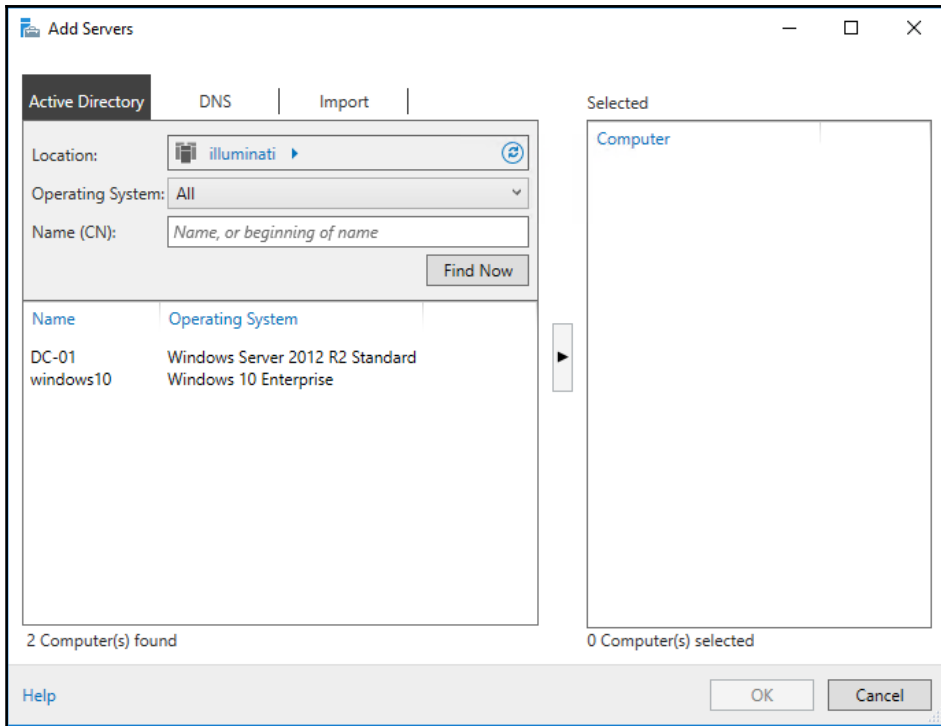


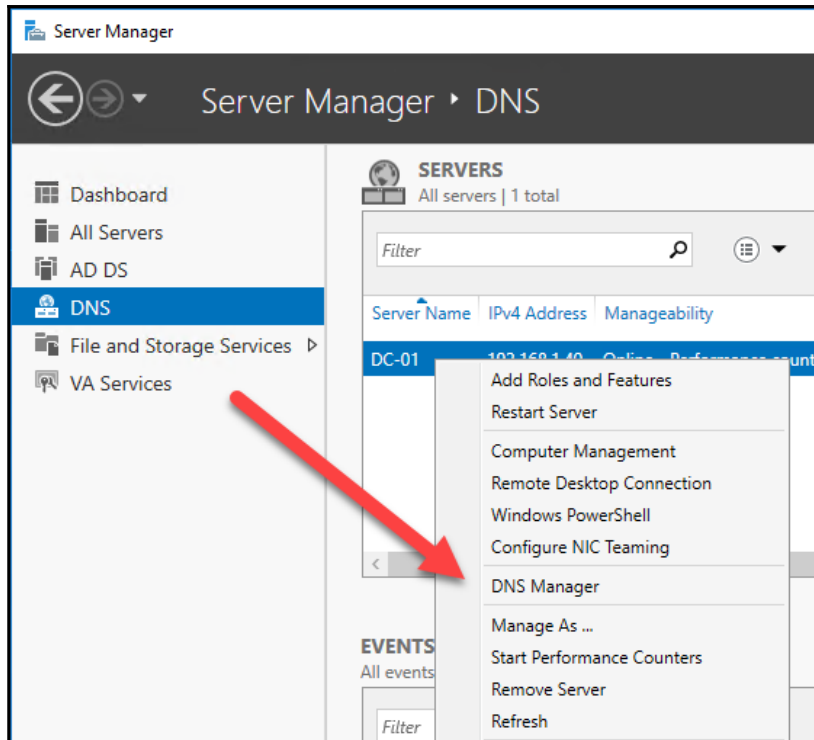




Chapter 04: Remote Administration Tools







Server Manager ▸ All Servers

SERVERS
All servers | 1 total

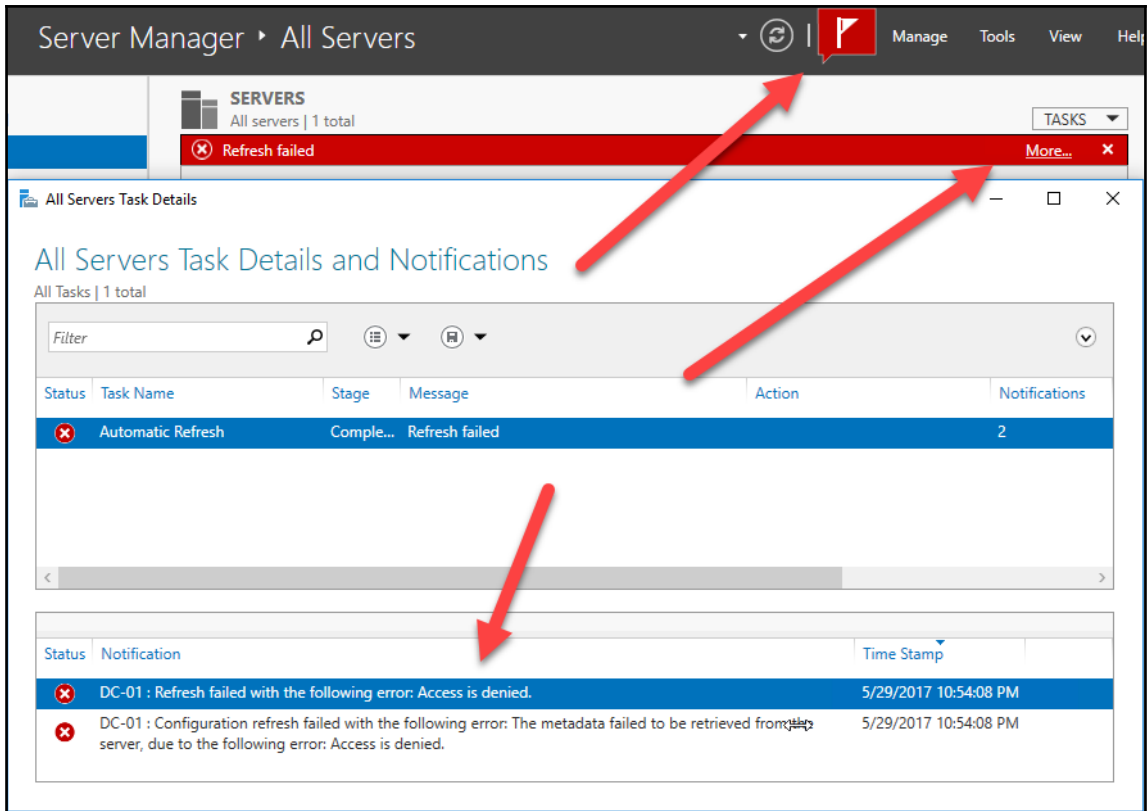
Refresh failed More...

All Servers Task Details and Notifications

All Tasks | 1 total

Status	Task Name	Stage	Message	Action	Notifications
✖	Automatic Refresh	Comple...	Refresh failed		2

Status	Notification	Time Stamp
✖	DC-01 : Refresh failed with the following error: Access is denied.	5/29/2017 10:54:08 PM
✖	DC-01 : Configuration refresh failed with the following error: The metadata failed to be retrieved from the server, due to the following error: Access is denied.	5/29/2017 10:54:08 PM



SERVERS
All servers | 1 total

Refresh failed

Filter

Server Name	IPv4 Address	Manageability	Last Update	Window
DC-01	192.168.1.40	Online - Performance counters not started	5/29/2017 10:54:08 PM	

- Add Roles and Features
- Restart Server
- Computer Management
- Remote Desktop Connection
- Windows PowerShell
- Configure NIC Teaming
- Manage As ...
- Remove Server
- Refresh
- Copy

SERVERS
All servers | 1 total

Filter

Server Name	ID	Severity	Source	Log	Date and Time
-------------	----	----------	--------	-----	---------------

SERVERS
All servers | 1 total

Filter

Server Name	IPv4 Address	Manageability	Last Update
DC-01	192.168.1.40	Online - Performance counters not started	5/29/2017 11:00:15 PM

Dashboard

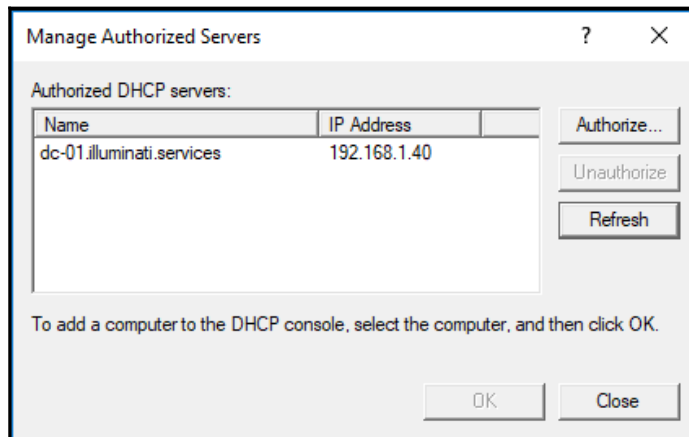
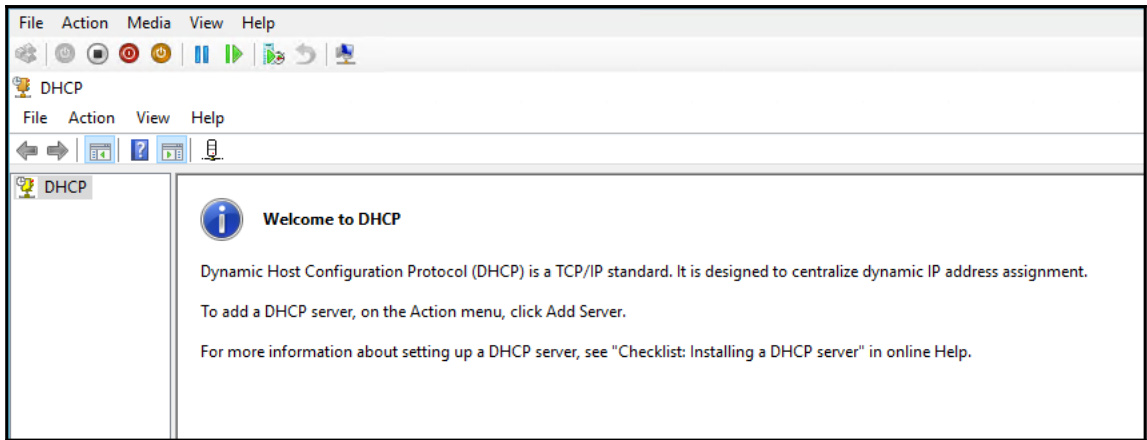
All Servers

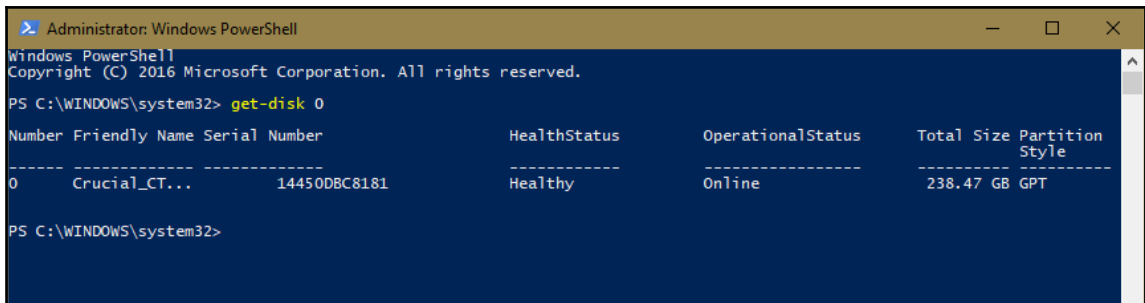
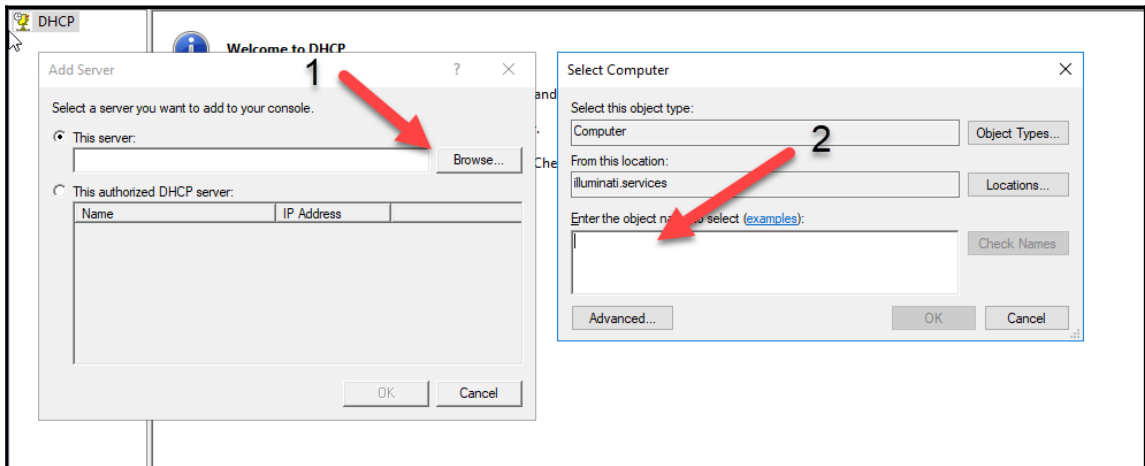
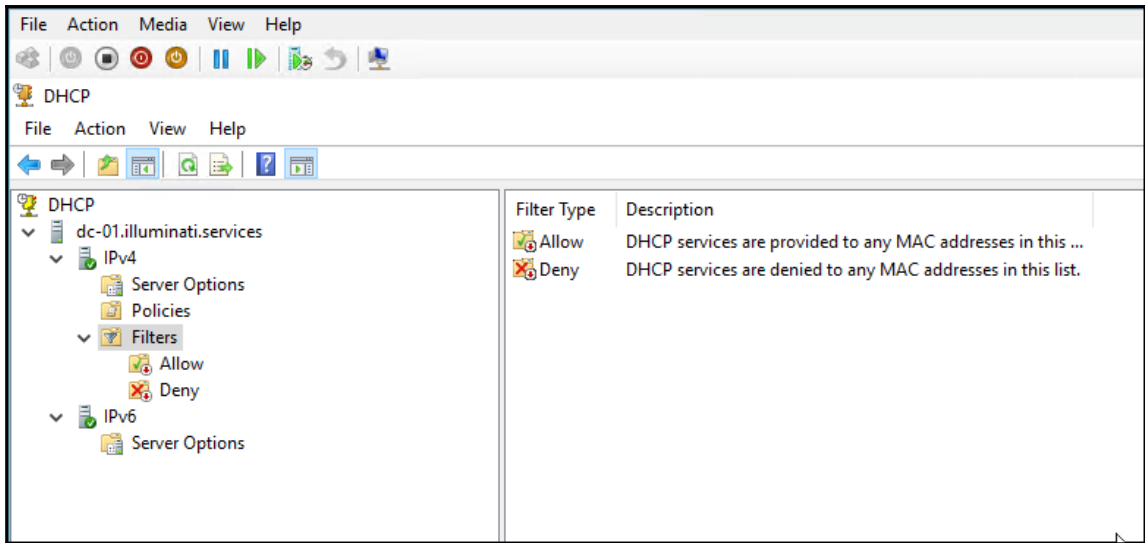
AD DS

DNS

File and Storage Services

VA Services





```
Administrator: Windows PowerShell

PS C:\WINDOWS\system32> get-disk 0 | Get-StorageReliabilityCounter

DeviceId Temperature ReadErrorsUncorrected Wear PowerOnHours
-----
0          0          0          14206

PS C:\WINDOWS\system32>
```

```
Administrator: Windows PowerShell

PS C:\WINDOWS\system32> get-help html

NAME
    ConvertTo-Html

SYNOPSIS
    Converts Microsoft .NET Framework objects into HTML that can be displayed in a Web browser.

SYNTAX
    ConvertTo-Html [[-Property] <Object[]>] [[-Head] <String[]>] [[-Title] <String>] [[-Body] <String[]>] [-As {Table
| List}] [-CssUri <Uri>] [-InputObject <PSObject>] [-PostContent <String[]>] [-PreContent <String[]>]
[<CommonParameters>]

    ConvertTo-Html [[-Property] <Object[]>] [-As {Table | List}] [-Fragment] [-InputObject <PSObject>] [-PostContent
<String[]>] [-PreContent <String[]>] [<CommonParameters>]

DESCRIPTION
    The ConvertTo-Html cmdlet converts .NET Framework objects into HTML that can be displayed in a Web browser. You
    can use this cmdlet to display the output of a command in a Web page.

    You can use the parameters of ConvertTo-Html to select object properties, to specify a table or list format, to
    specify the HTML page title, to add text before and after the object, and to return only the table or list
    fragment, instead of a strict DTD page.

    When you submit multiple objects to ConvertTo-Html , Windows PowerShell creates the table (or list) based on the
    properties of the first object that you submit. If the remaining objects do not have one of the specified
    properties, the property value of that object is an empty cell. If the remaining objects have additional
    properties, those property values are not included in the file.

RELATED LINKS
    Online Version: http://go.microsoft.com/fwlink/?LinkId=821758
    ConvertTo-Csv
    ConvertTo-Json
    ConvertTo-Xml
    Export-Clixml
    Import-Clixml

REMARKS
    To see the examples, type: "get-help ConvertTo-Html -examples".
    For more information, type: "get-help ConvertTo-Html -detailed".
    For technical information, type: "get-help ConvertTo-Html -full".
    For online help, type: "get-help ConvertTo-Html -online"
```



```
PS C:\Users\richa.RICHARD-SURFACE> get-dscresource
```

ImplementedAs	Name	ModuleName	Version	Properties
Binary	File			{DestinationPath, Attributes, Ch...
Binary	SignatureValidation			{SignedItemType, TrustedStorePath}
PowerShell	Archive			{Destination, Path, Checksum, Cr...
PowerShell	Environment	PSDesiredStateConfiguration	1.1	{Name, DependsOn, Ensure, Path...}
PowerShell	Group	PSDesiredStateConfiguration	1.1	{GroupName, Credential, Dependo...
Composite	GroupSet	PSDesiredStateConfiguration	1.1	{DependsOn, PsDscRunAsCredential...}
Binary	Log	PSDesiredStateConfiguration	1.1	{Message, DependsOn, PsDscRunASC...
PowerShell	Package	PSDesiredStateConfiguration	1.1	{Name, Path, ProductId, Argument...
Composite	ProcessSet	PSDesiredStateConfiguration	1.1	{DependsOn, PsDscRunAsCredential...}
PowerShell	Registry	PSDesiredStateConfiguration	1.1	{Key, ValueName, DependsOn, Ensu...
PowerShell	Script	PSDesiredStateConfiguration	1.1	{GetScript, SetScript, TestScrip...
PowerShell	Service	PSDesiredStateConfiguration	1.1	{Name, BuiltInAccount, Credentia...
Composite	ServiceSet	PSDesiredStateConfiguration	1.1	{DependsOn, PsDscRunAsCredential...}
PowerShell	User	PSDesiredStateConfiguration	1.1	{UserName, DependsOn, Descriptio...
PowerShell	WaitForAll	PSDesiredStateConfiguration	1.1	{NodeName, ResourceName, Depend...
PowerShell	WaitForAny	PSDesiredStateConfiguration	1.1	{NodeName, ResourceName, Depend...
PowerShell	WaitForSome	PSDesiredStateConfiguration	1.1	{NodeCount, NodeName, ResourceNa...
PowerShell	WindowsFeature	PSDesiredStateConfiguration	1.1	{Name, Credential, DependsOn, En...
Composite	WindowsFeatureSet	PSDesiredStateConfiguration	1.1	{DependsOn, PsDscRunAsCredential...}
PowerShell	WindowsOptionalFeature	PSDesiredStateConfiguration	1.1	{Name, DependsOn, Ensure, LogLev...
Composite	WindowsOptionalFeatureSet	PSDesiredStateConfiguration	1.1	{DependsOn, PsDscRunAsCredential...}
PowerShell	WindowsPackageCab	PSDesiredStateConfiguration	1.1	{Ensure, Name, SourcePath, Depen...
PowerShell	windowsProcess	PSDesiredStateConfiguration	1.1	{Arguments, Path, Credential, De...

Define New Field X

Identifier:

Replace identifier with:

Environment variable
 Registry value
 64-bit registry view
 WMI Query

Version information for a file
 Time stamp of a file
 Contents of a file
 VB Script file

Path:

```

Administrator: Command Prompt - psexec
06/04/2017 09:19 PM          202,400 pslist64.exe
06/04/2017 09:19 PM          151,728 PsLoggedon.exe
06/04/2017 09:19 PM          170,160 PsLoggedon64.exe
06/04/2017 09:19 PM          178,040 psloglist.exe
06/04/2017 09:19 PM          149,664 pspasswd.exe
06/04/2017 09:19 PM          168,616 pspasswd64.exe
06/04/2017 09:19 PM          255,648 psping.exe
06/04/2017 09:19 PM          293,032 psping64.exe
06/04/2017 09:19 PM          188,584 PsService.exe
06/04/2017 09:19 PM          210,608 PsService64.exe
06/04/2017 09:19 PM          207,664 pssutdown.exe
06/04/2017 09:19 PM          289,448 pssuspend.exe
06/04/2017 09:19 PM          321,704 pssuspend64.exe
06/04/2017 09:19 PM          66,582 PsTools.chm
06/04/2017 09:19 PM              37 pswersion.txt
06/04/2017              27 File(s)    5,955,125 bytes
                                2 Dir(s)    963,455,971,328 bytes free

D:\ISO\PsTools>psexec

PsExec v2.2 - Execute processes remotely
Copyright (C) 2001-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

```

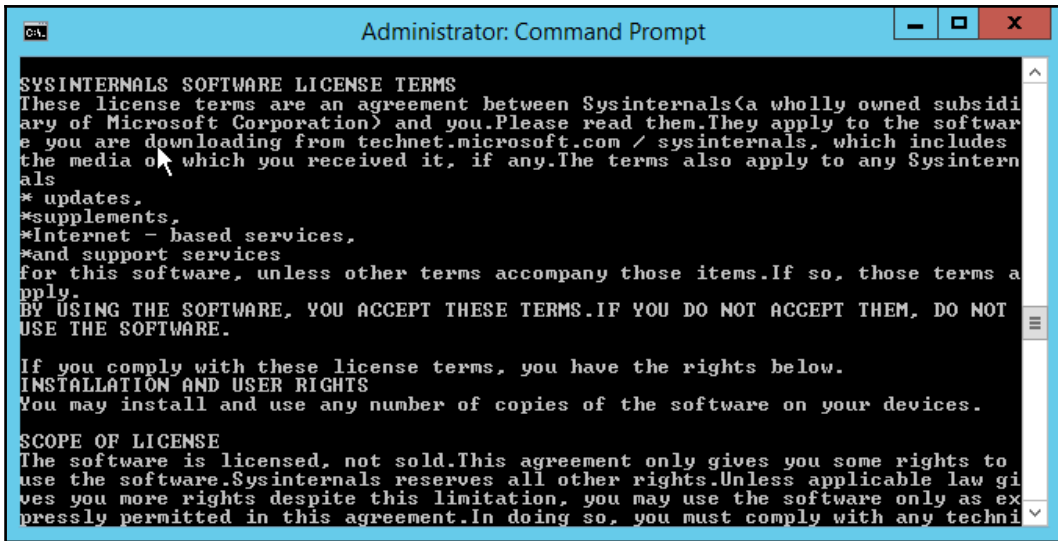
PsExec License Agreement X

You can also use the /accepteula command-line switch to accept the EULA.

SYSINTERNALS SOFTWARE LICENSE TERMS

These license terms are an agreement between Sysinternals (a wholly owned subsidiary of Microsoft Corporation) and you. Please read them. They apply to the software you are downloading from Systinternals.com, which includes the media on which you received it, if any. The terms also apply to any Sysinternals

- updates,
- supplements,
- Internet-based services, and



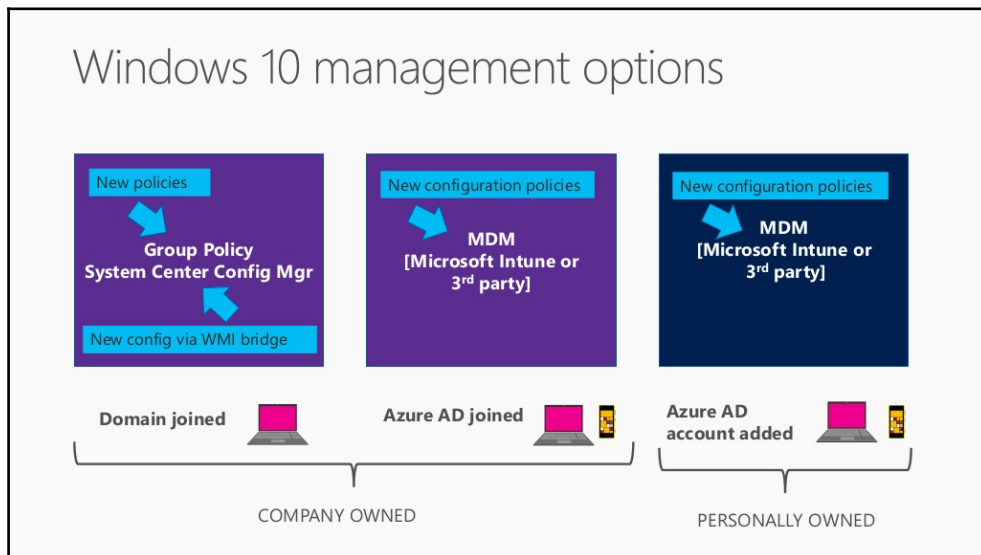
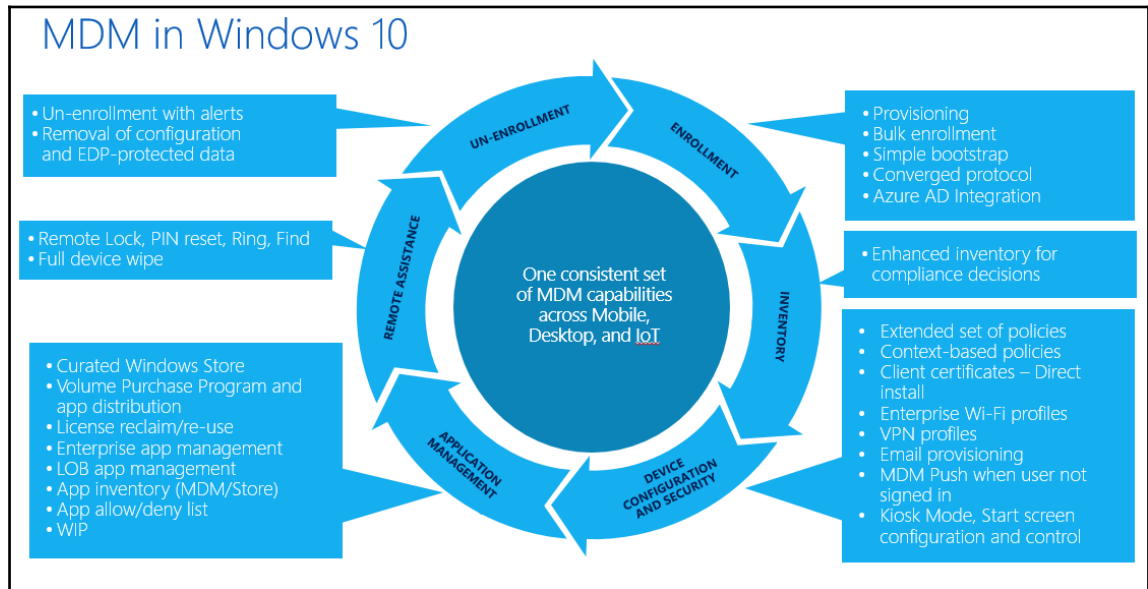
The image shows a screenshot of a Windows Command Prompt window titled "Administrator: Command Prompt". The window has a blue title bar with standard minimize, maximize, and close buttons. The main content area is black with white text. The text displays the Sysinternals Software License Terms, including sections for updates, installation rights, and the scope of the license. A mouse cursor is visible over the text.

```
C:\>
SYSINTERNALS SOFTWARE LICENSE TERMS
These license terms are an agreement between Sysinternals (a wholly owned subsidiary of Microsoft Corporation) and you. Please read them. They apply to the software you are downloading from technet.microsoft.com / sysinternals, which includes the media on which you received it, if any. The terms also apply to any Sysinternals
* updates,
* supplements,
* Internet - based services,
* and support services
for this software, unless other terms accompany those items. If so, those terms apply.
BY USING THE SOFTWARE, YOU ACCEPT THESE TERMS. IF YOU DO NOT ACCEPT THEM, DO NOT USE THE SOFTWARE.

If you comply with these license terms, you have the rights below.
INSTALLATION AND USER RIGHTS
You may install and use any number of copies of the software on your devices.

SCOPE OF LICENSE
The software is licensed, not sold. This agreement only gives you some rights to use the software. Sysinternals reserves all other rights. Unless applicable law gives you more rights despite this limitation, you may use the software only as expressly permitted in this agreement. In doing so, you must comply with any techni
```

Chapter 05: Device Management



Add or edit OMA-URI Setting ✕

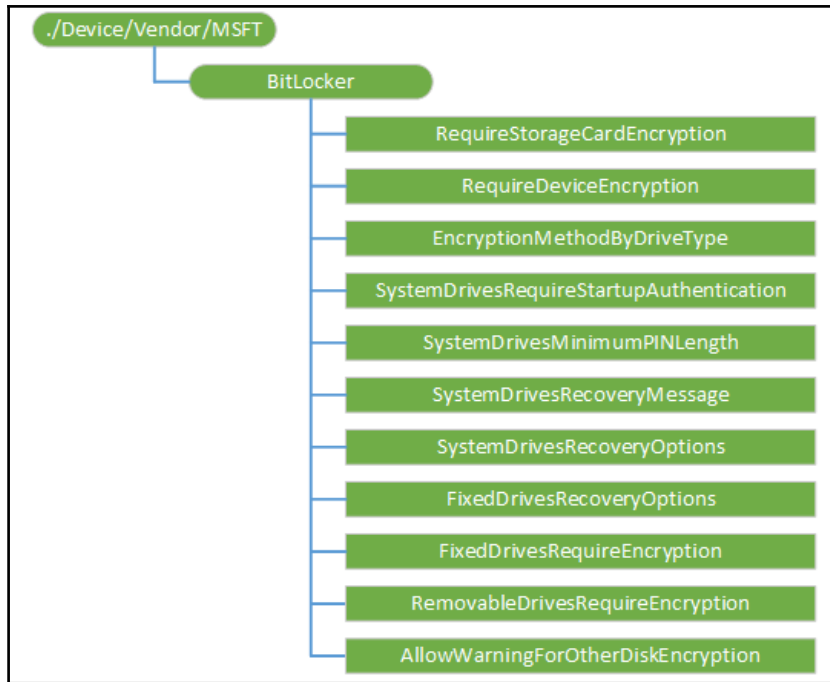
*** Setting name:**

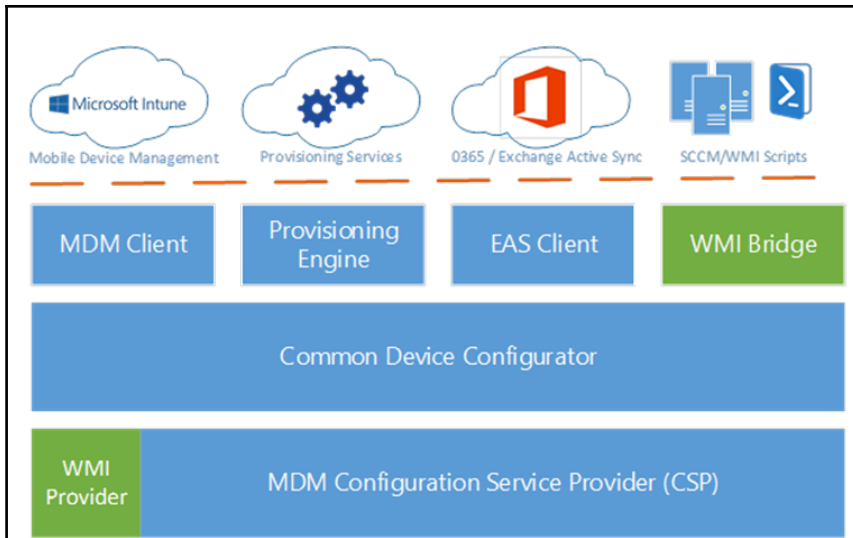
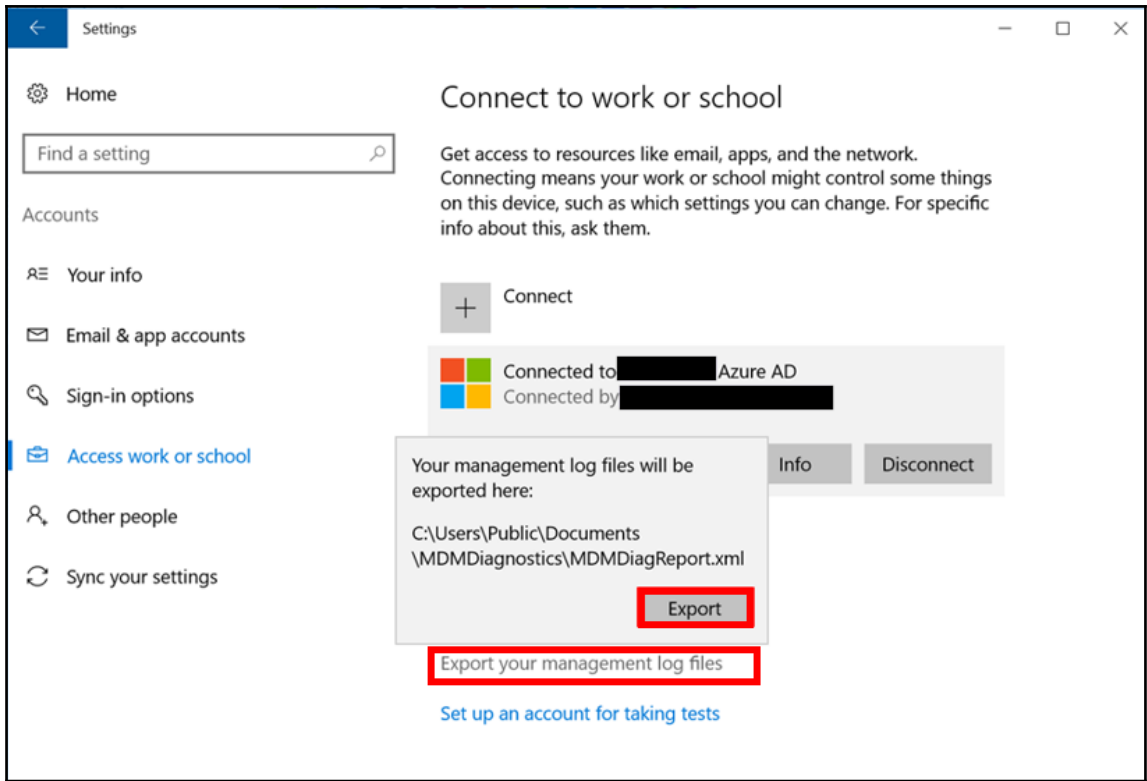
Setting description:

*** Data type:**

*** OMA-URI (case sensitive):**

*** Value:**





User Configuration (Enabled) [hide](#)

Policies [hide](#)

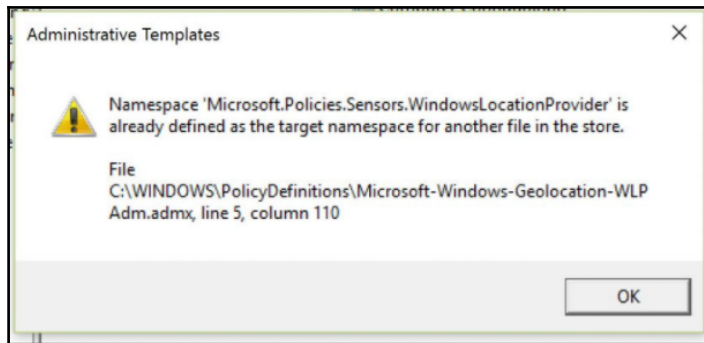
Administrative Templates [hide](#)

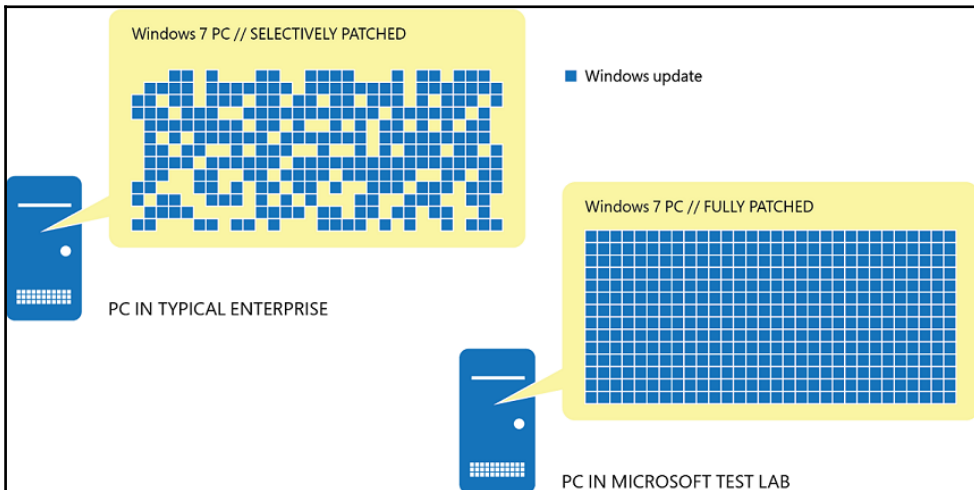
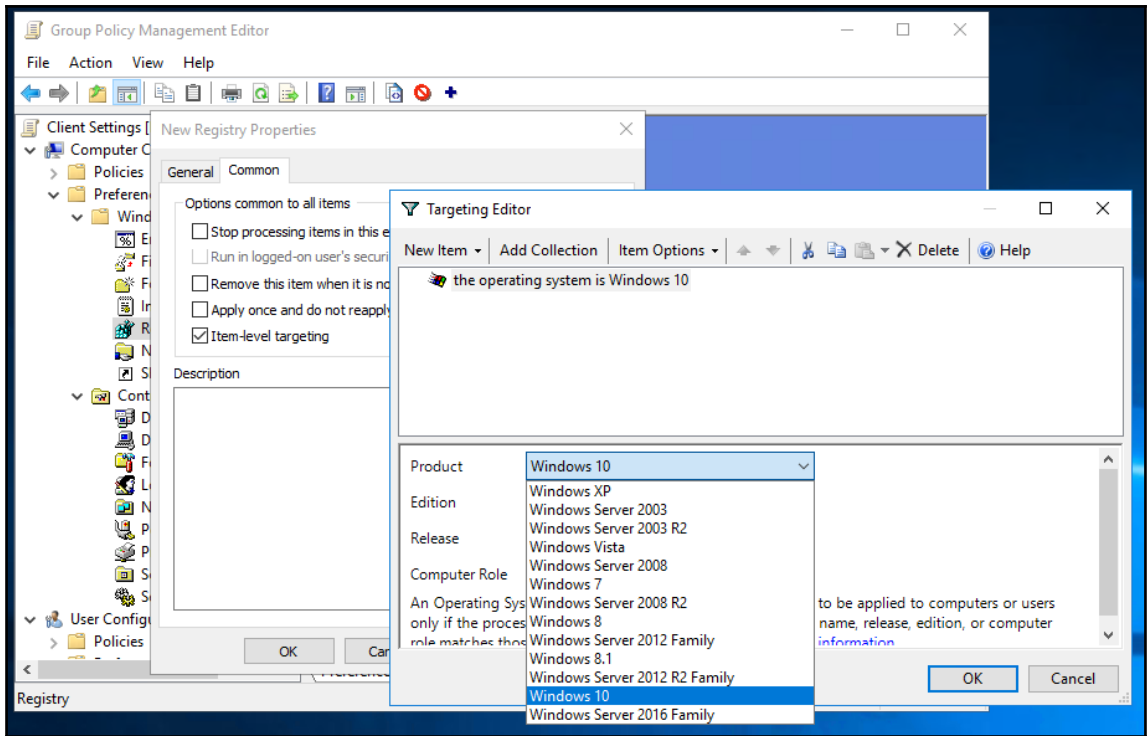
Policy definitions (ADMX files) retrieved from the local computer.

Extra Registry Settings [hide](#)

Display names for some settings cannot be found. You might be able to resolve this issue by updating the .ADM files used by Group Policy Management.

Setting	State
---------	-------





⚙️ Update history

[Uninstall updates](#)

[Recovery options](#)

Update history

- ▼ Feature Updates (1)
 - Windows 10 Insider Preview 15063 (rs2_release)
Successfully installed on 3/21/2017
- ▼ Quality Updates (2)
 - Cumulative Update for Windows 10 Version 1703 for x64-based Systems (KB4016252)
Successfully installed on 4/4/2017
 - Cumulative Update for Windows 10 Version 1703 for x64-based Systems (KB4016250)
Successfully installed on 4/1/2017

About Windows



Microsoft Windows
Version 1703 (OS Build 15063.540)
© 2017 Microsoft Corporation. All rights reserved.
The Windows 10 Pro operating system and its user interface are protected by trademark and other pending or existing intellectual property rights in the United States and other countries/regions.

This product is licensed under the [Microsoft Software License Terms](#) to:
test

OK

Settings

Advanced options

By default, we're dynamically optimizing the amount of bandwidth your device uses to both download and upload Windows and app updates, and other Microsoft products. But you can set a specific limit if you're worried about data usage.

Download settings

Limit how much bandwidth is used for downloading updates in the background

45%

Upload settings

Limit how much bandwidth is used for uploading updates to other PCs on the Internet

50%

Monthly upload limit

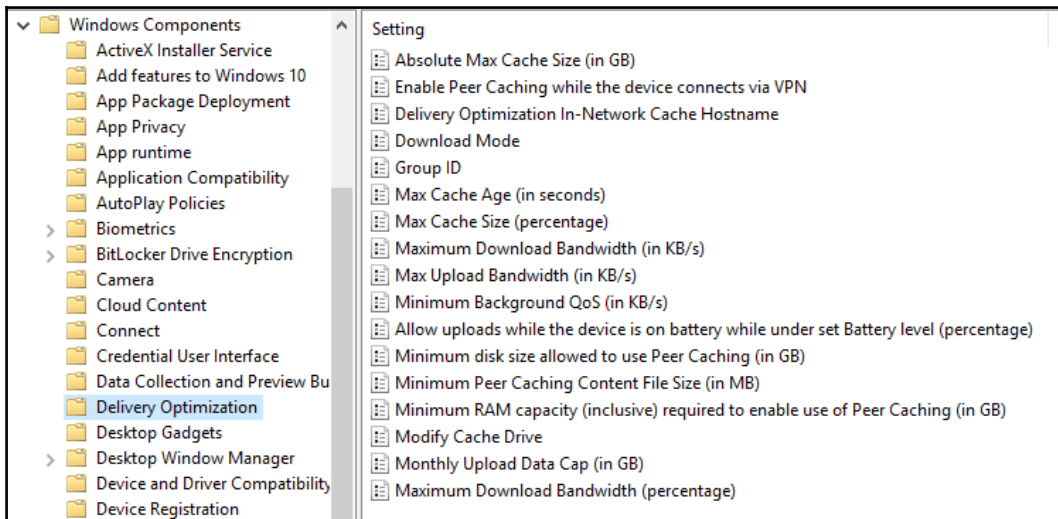
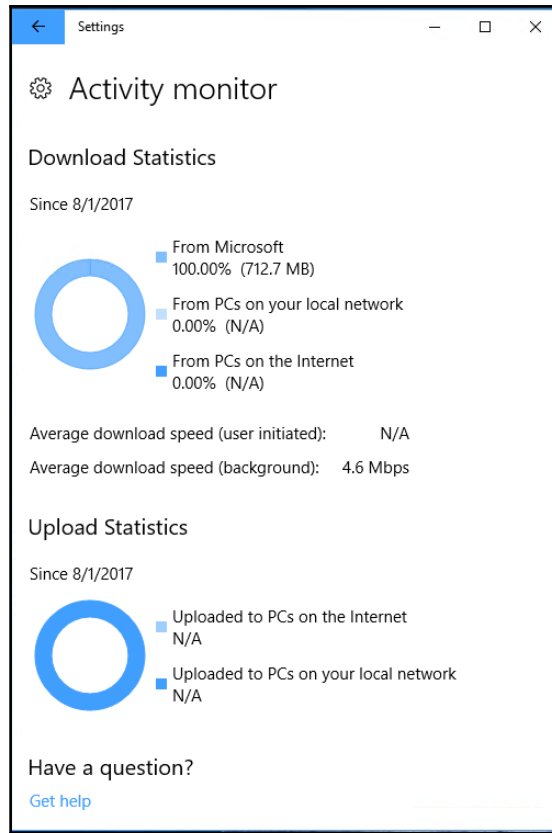
500 GB

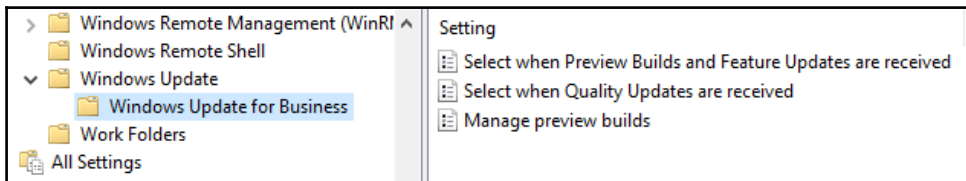
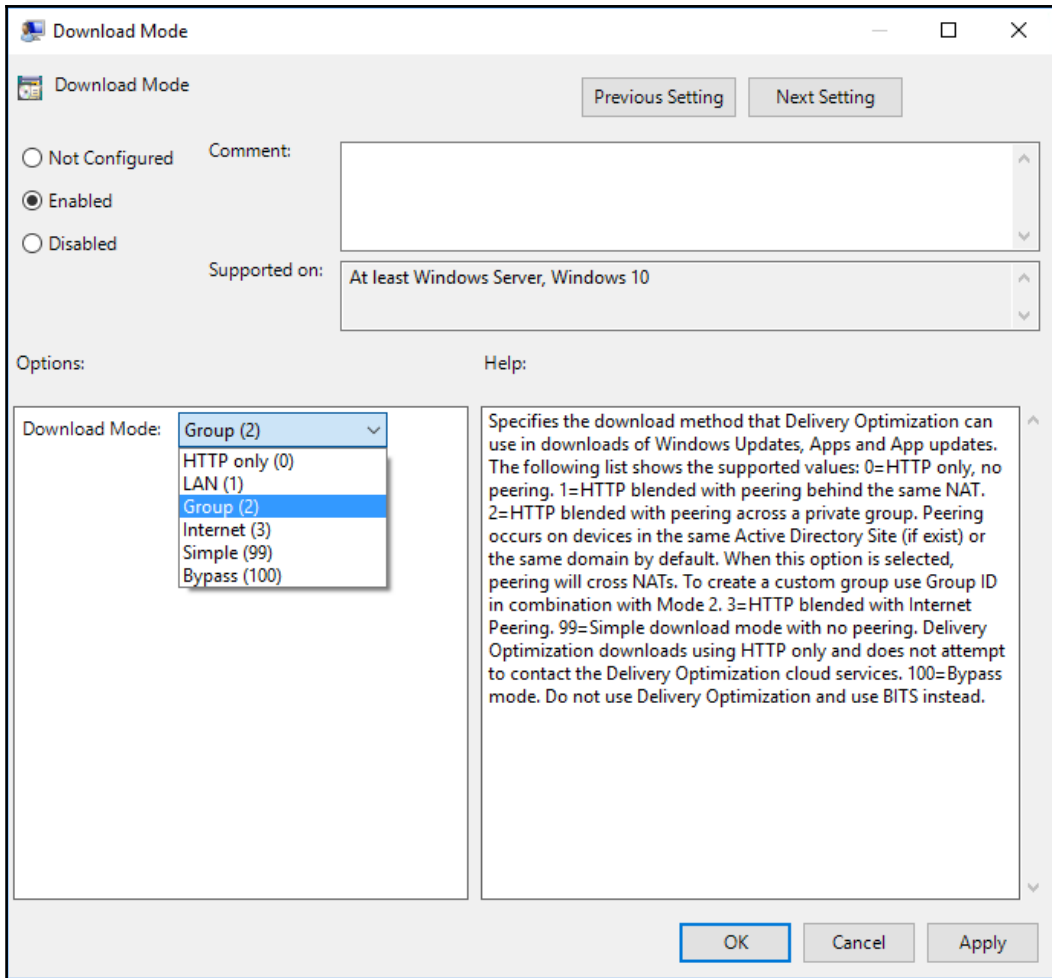
Note: when this limit is reached, your device will stop uploading to other PCs on the Internet.

Monthly upload to date
N/A

Amount left
500.0 GB

Have a question?
[Get help](#)





Select when Quality Updates are received

Select when Quality Updates are received Previous Setting Next Setting

Not Configured Comment:

Enabled

Disabled

Supported on:

Options: Help:

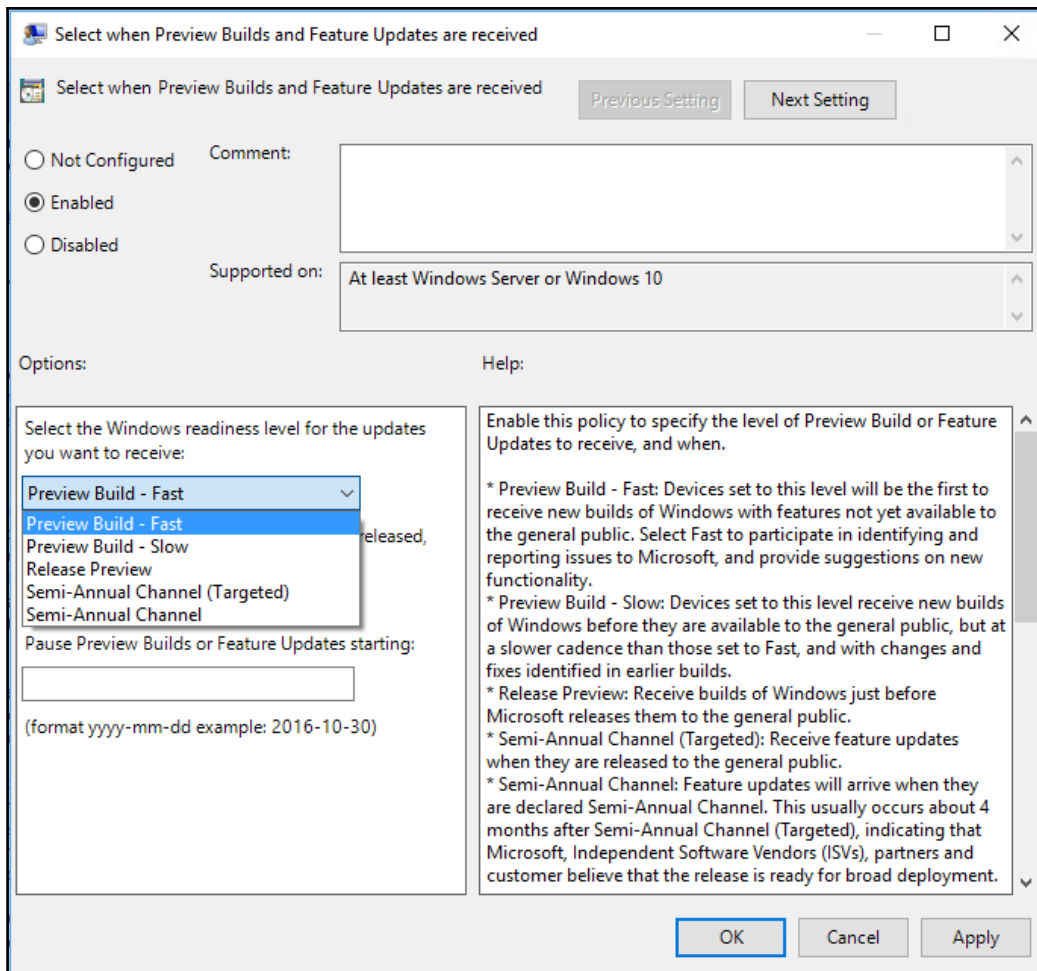
After a quality update is released, defer receiving it for this many days:

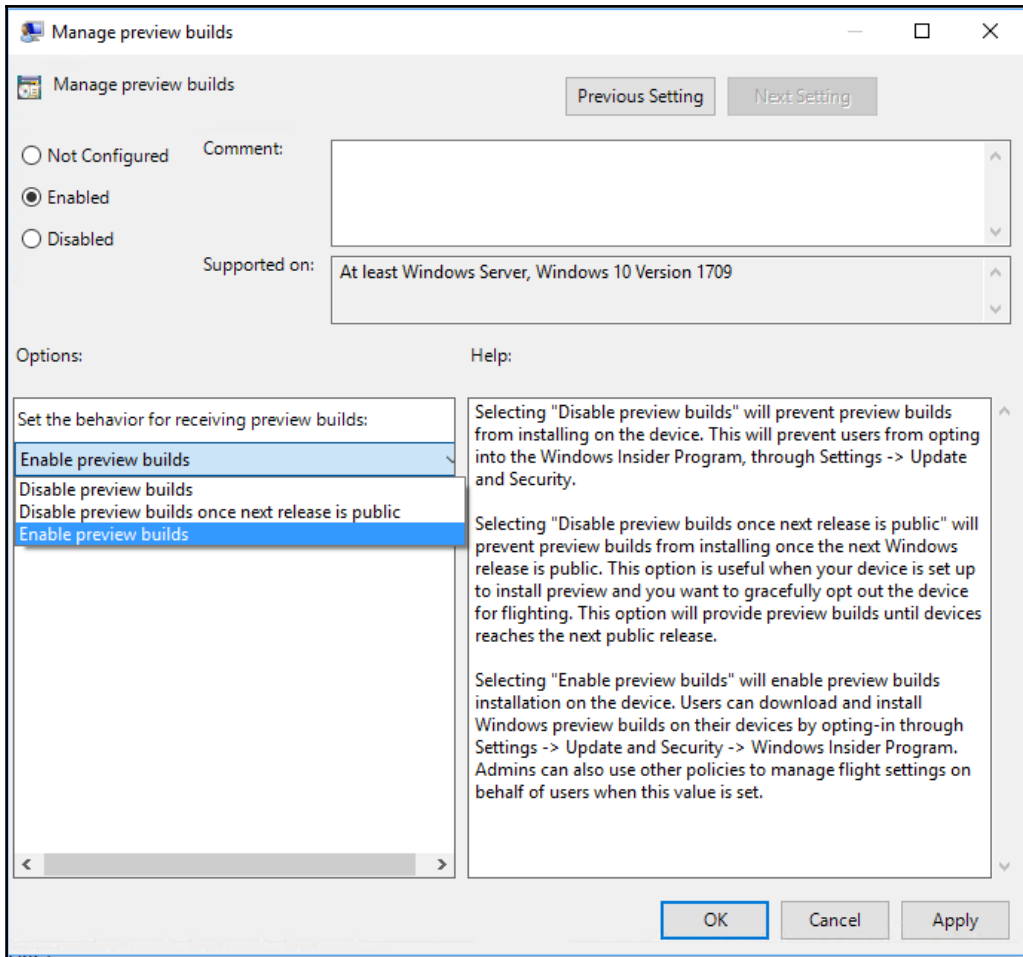
Pause Quality Updates starting

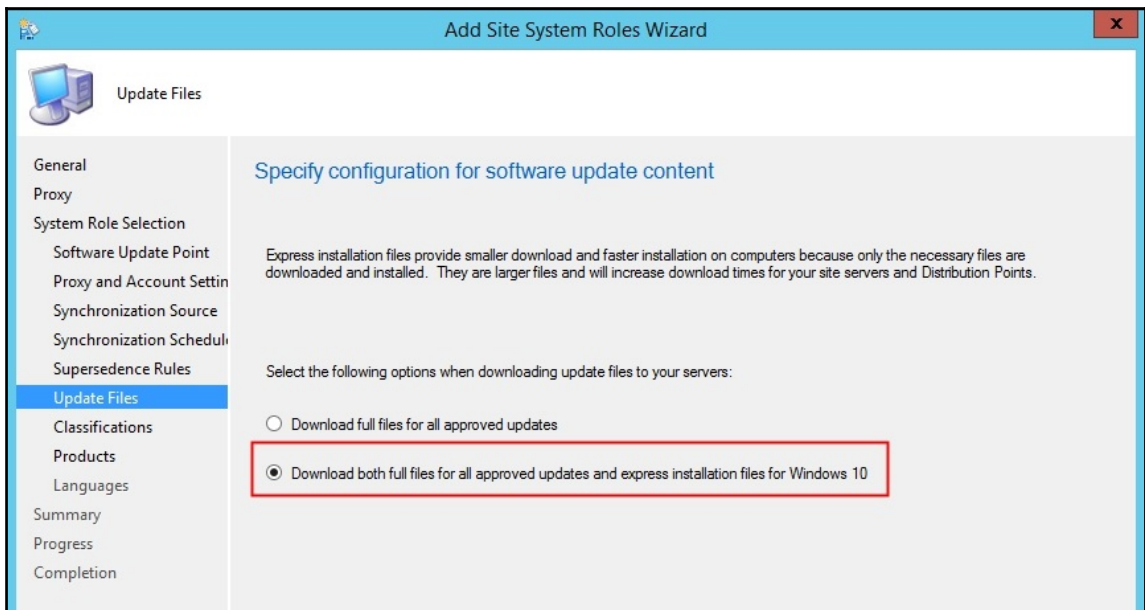
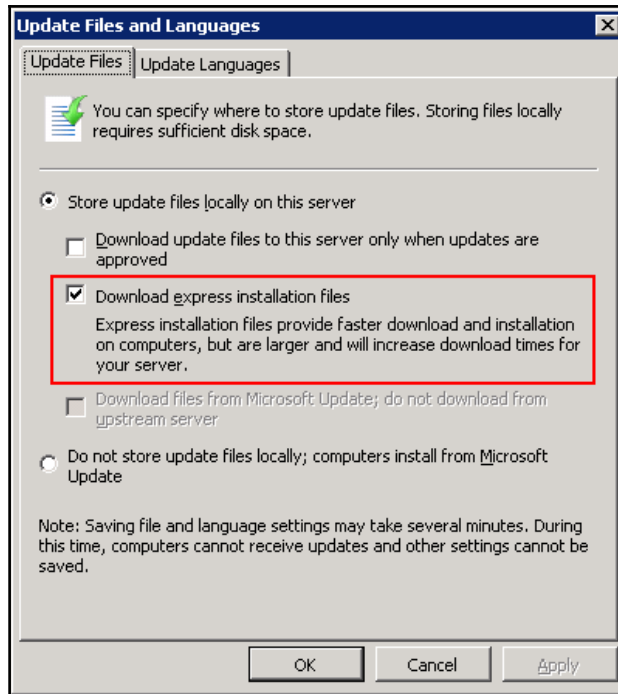
(format yyyy-mm-dd example: 2016-10-30)

Enable this policy to specify when to receive quality updates.
You can defer receiving quality updates for up to 30 days.
To prevent quality updates from being received on their scheduled time, you can temporarily pause quality updates. The pause will remain in effect for 35 days or until you clear the start date field.
To resume receiving Quality Updates which are paused, clear the start date field.
If you disable or do not configure this policy, Windows Update will not alter its behavior.
Note: If the "Allow Telemetry" policy is set to 0, this policy will have no effect.

OK Cancel Apply







Windows 10 release	Configuration Manager 1610	Configuration Manager 1702	Configuration Manager 1706
Enterprise 2015 LTSB	✓	✓	✓
1511 <i>(see editions)</i>	✓	✓	✓
Enterprise 2016 LTSB	✓	✓	✓
1607 Anniversary Update <i>(see editions)</i>	✓	✓	✓
1703 Creators Update <i>(see editions)</i>	✗	BC	✓

Editions: Enterprise, Pro, Education, Pro Education

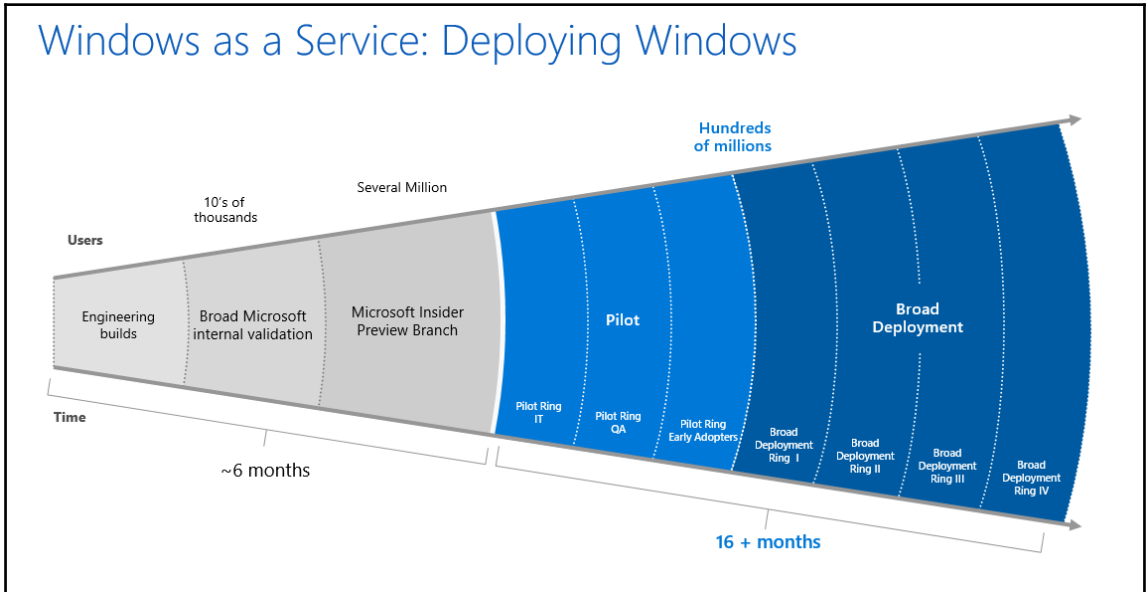
Key

✓ = **Supported**

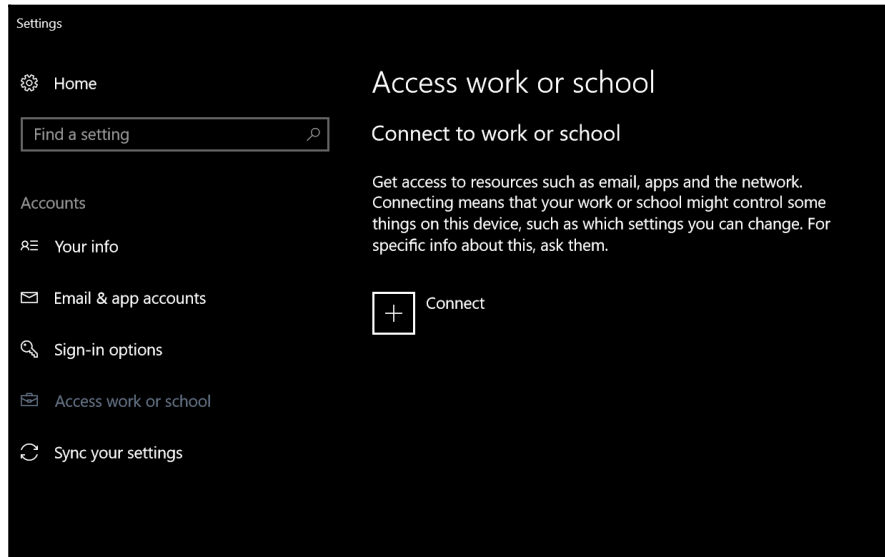
BC = **Backwards compatible** - This means that existing client management features (hardware inventory, software inventory, software updates, etc.) should work with the new Windows 10 release. Any known issues or caveats will be documented.

This approach gives you the ability to deploy and manage new Windows builds on day one with application compatibility support without requiring a new Configuration Manager update version.

✗ = **Not supported**



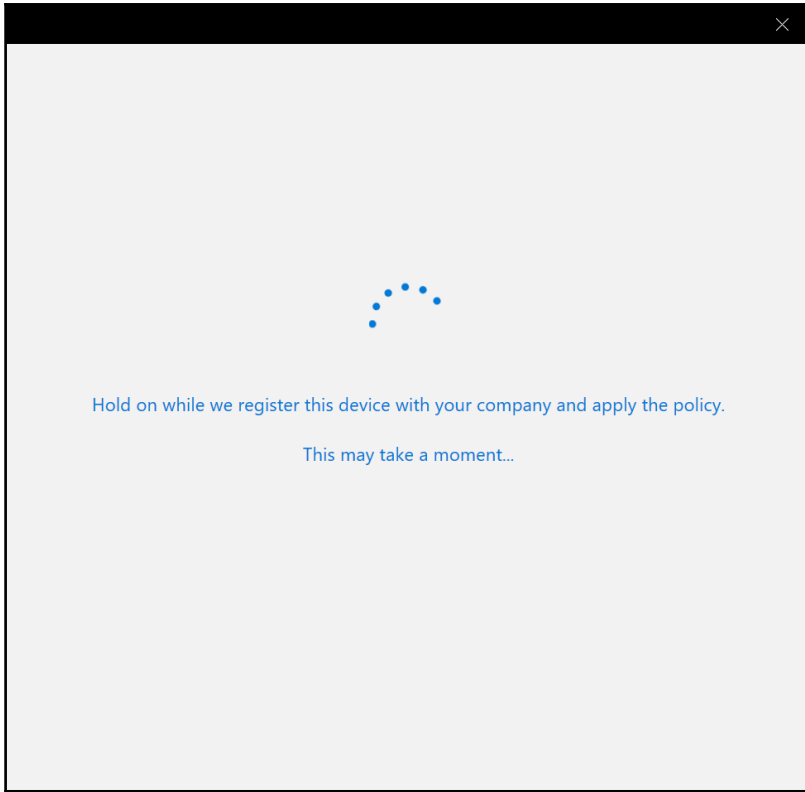
Chapter 06: Protecting Enterprise Data in BYOD Scenarios

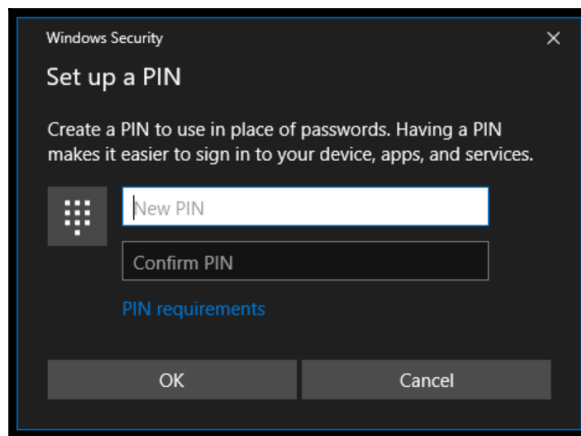
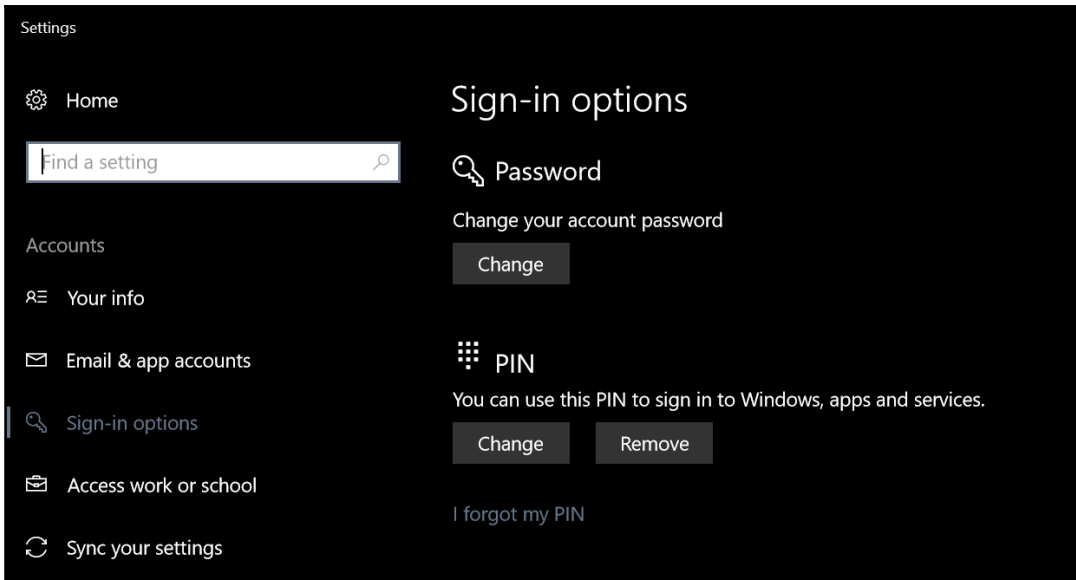


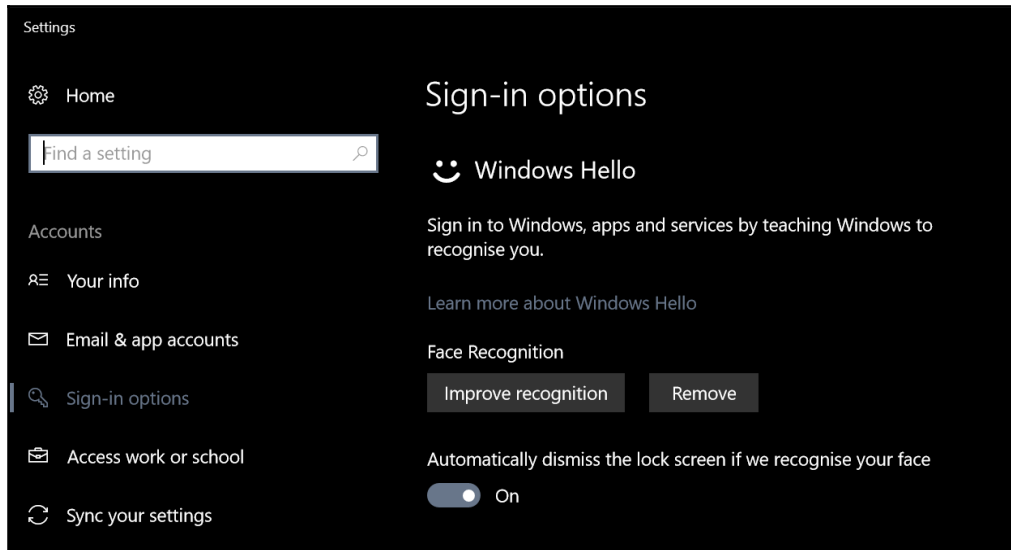
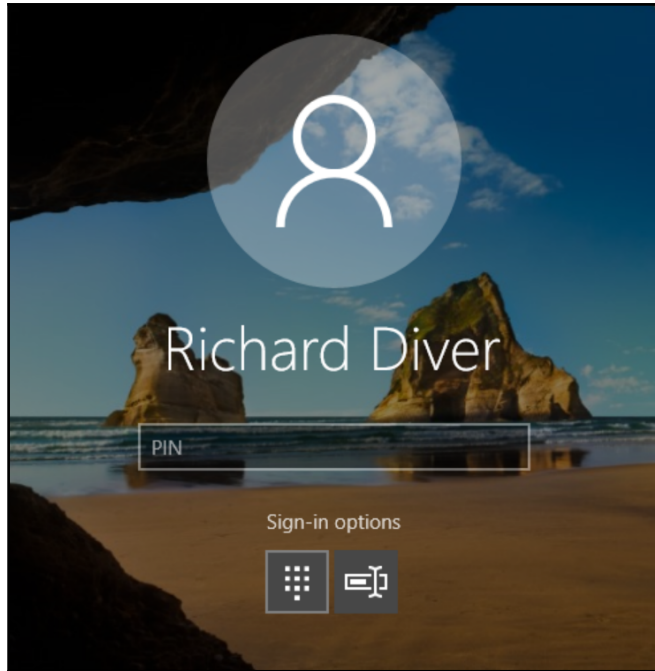
Set up a work or education account

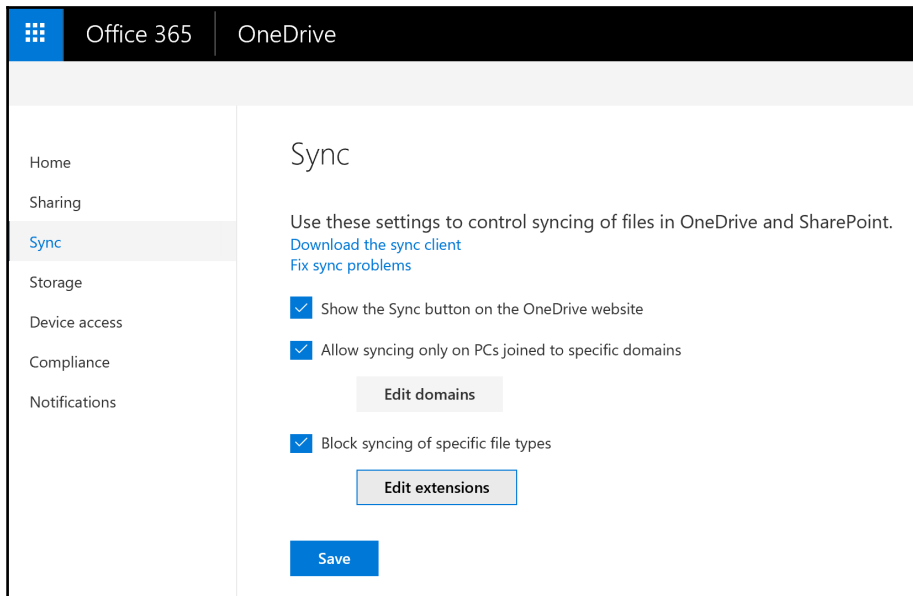
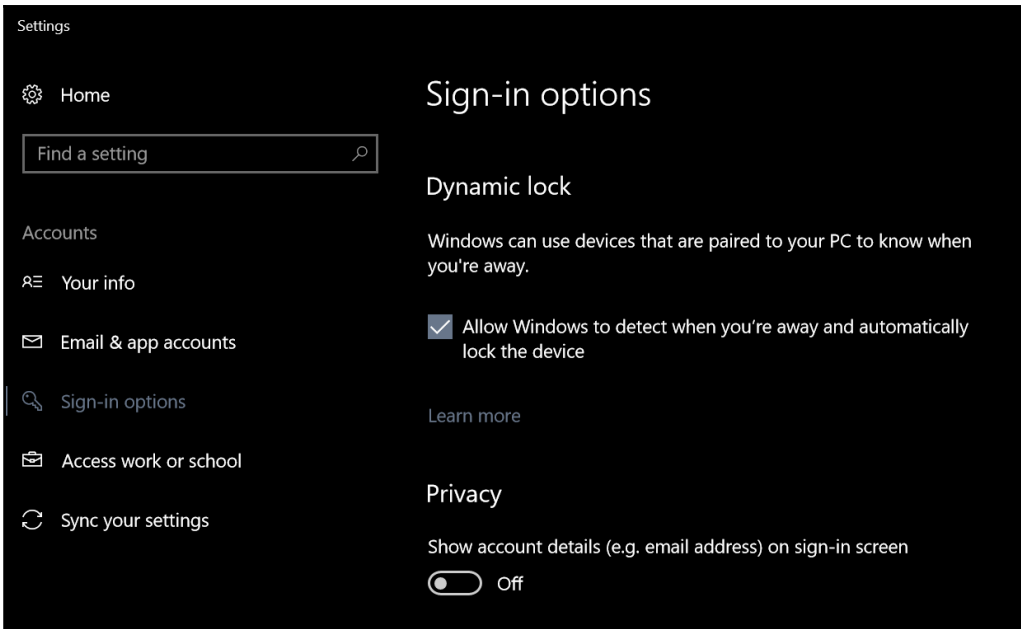
You'll have access to resources such as email, apps and the network. Connecting means that your work or school might control some things on this device, such as which settings you can change. For specific info about this, ask them.

Next









Office 365 OneDrive

Home
Sharing
Sync
Storage
Device access
Compliance
Notifications

Device access

Control access based on network location

Allow access only from specific IP address locations

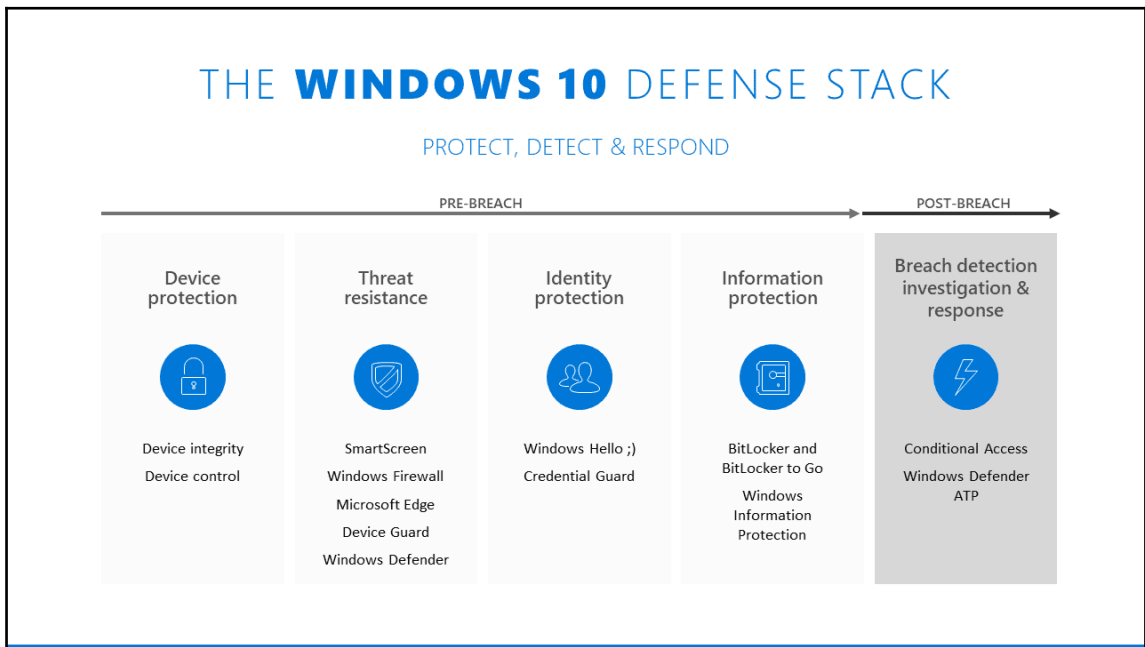
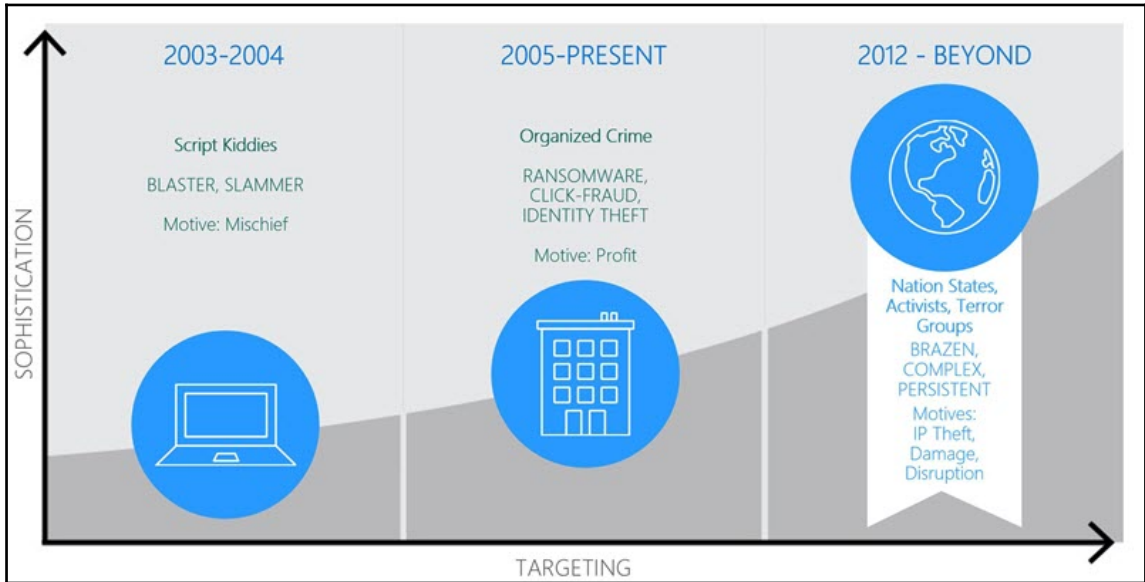
Control access from apps that can't enforce device-based restrictions

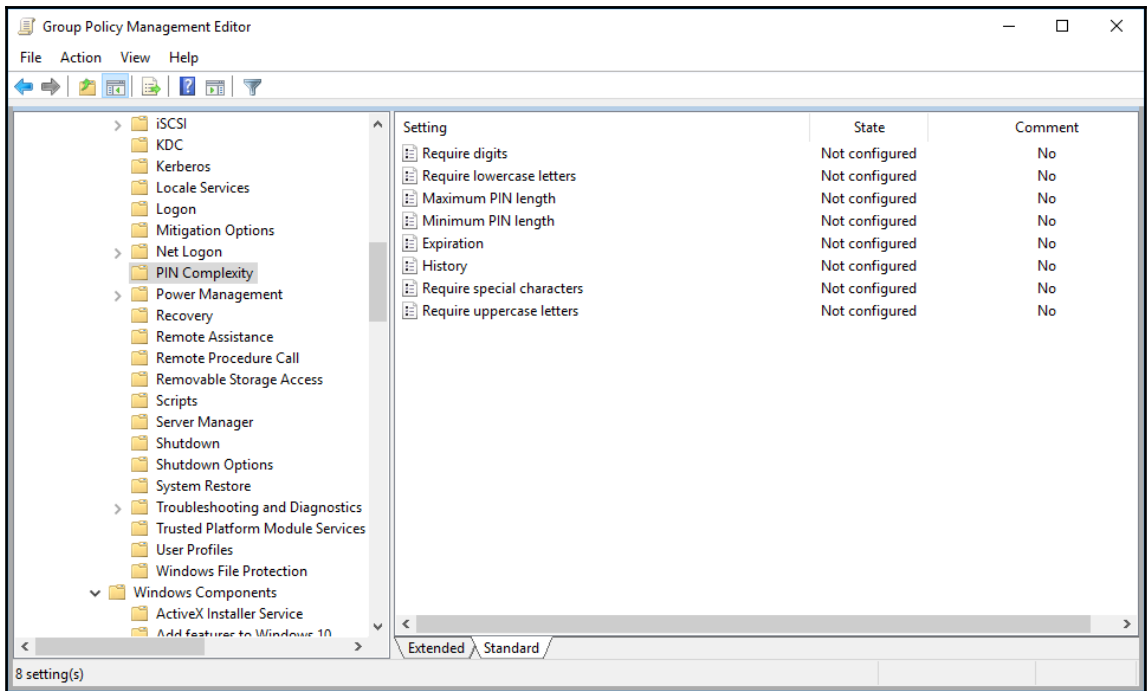
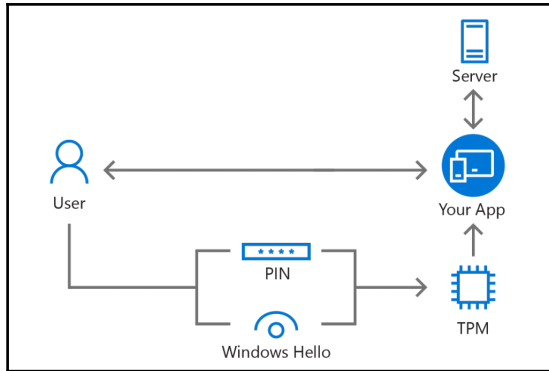
Allow access from apps that don't use modern authentication

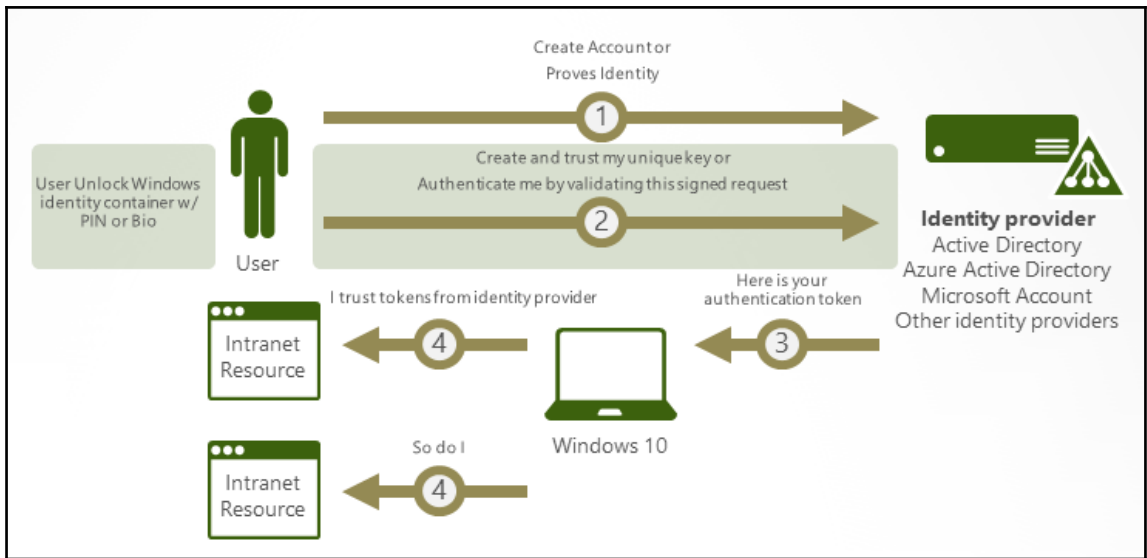
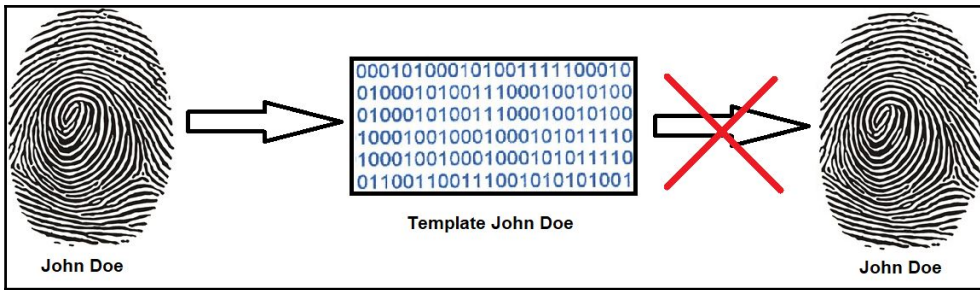
Mobile application management

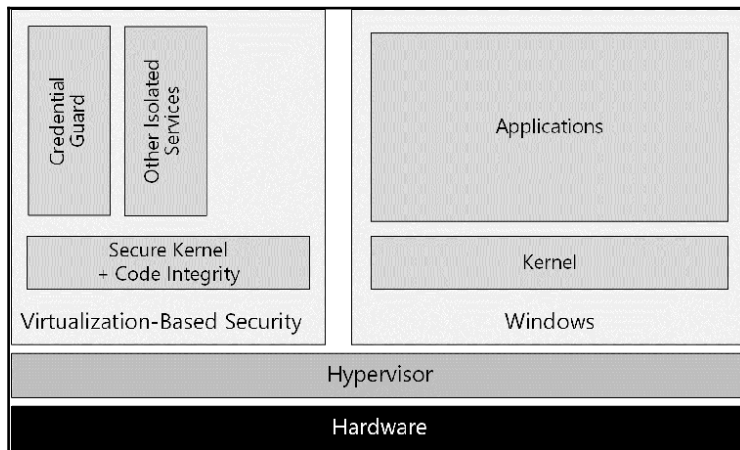
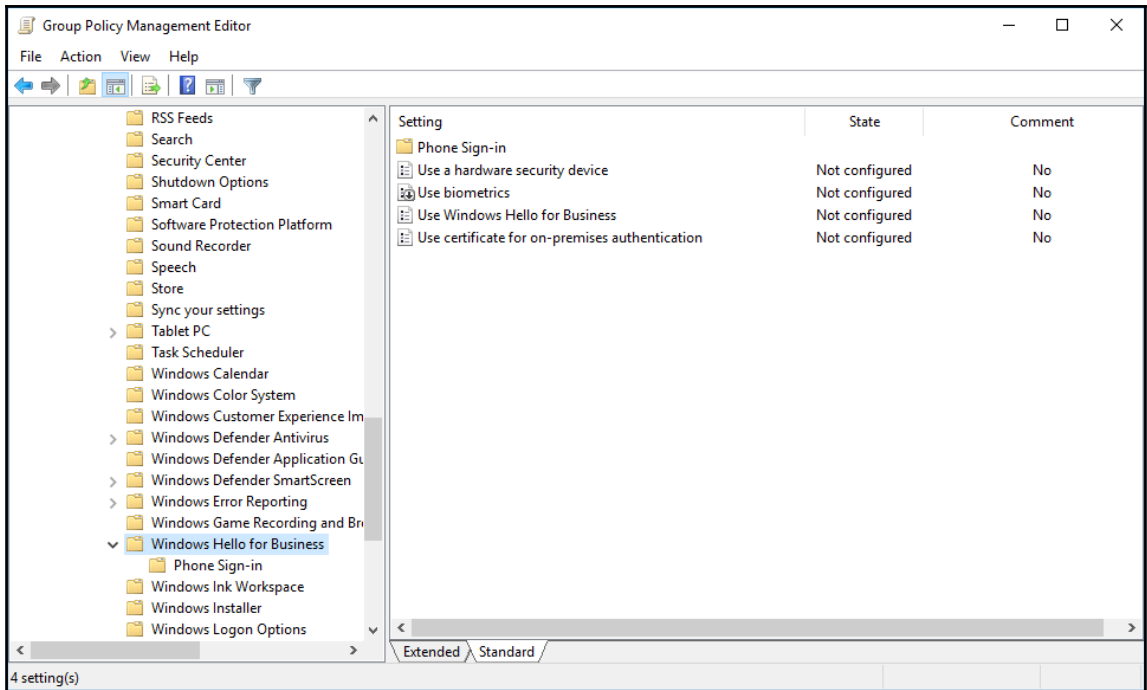
Use these settings to control access to features in the OneDrive and SharePoint mobile apps. If you created other policies in Intune, they will take precedence for the selected users. The settings do not apply to personal accounts that users may have added to the apps.

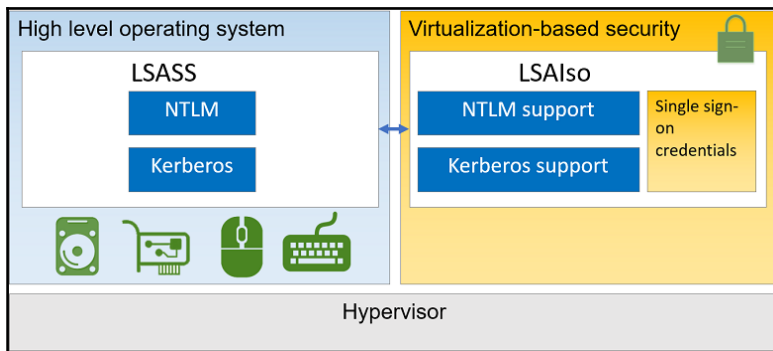
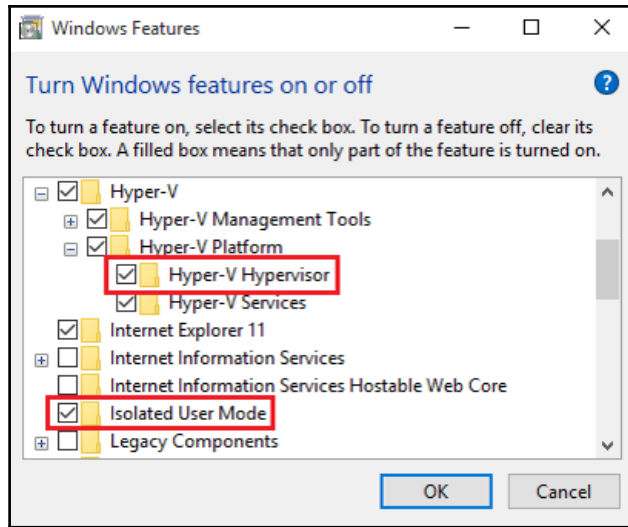
Chapter 07: Windows 10 Security

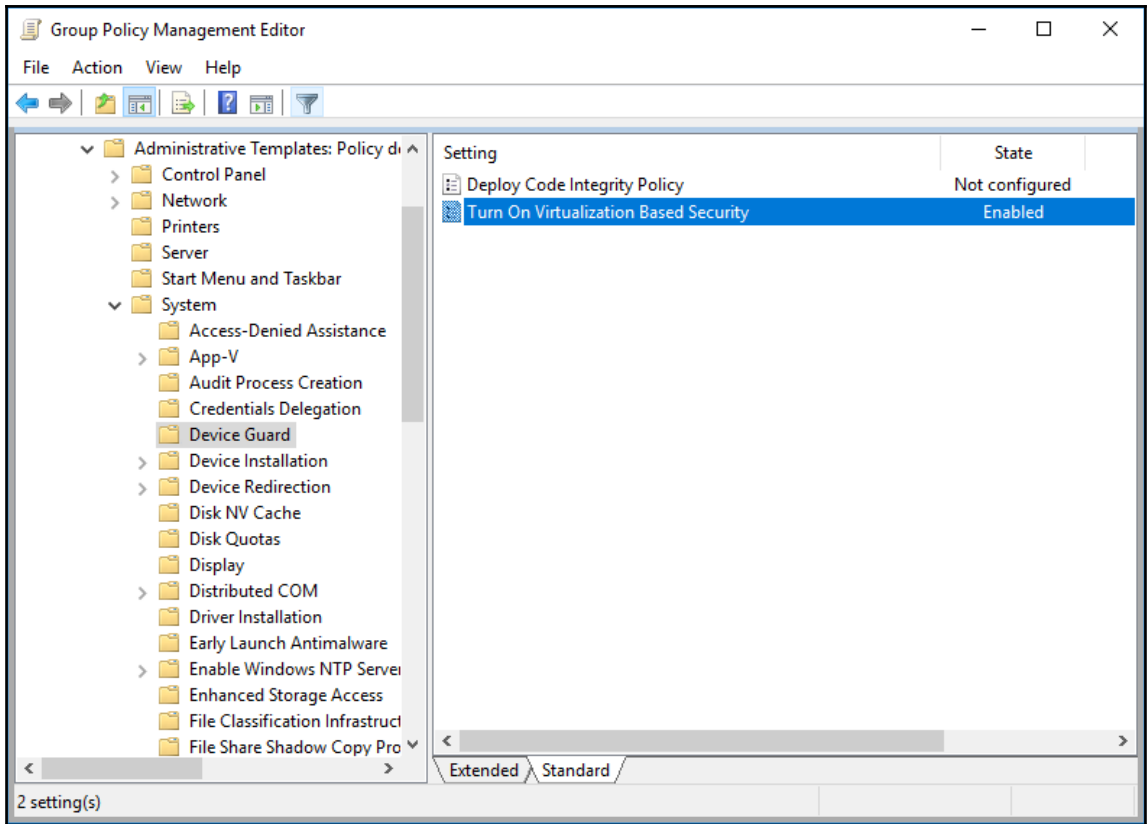


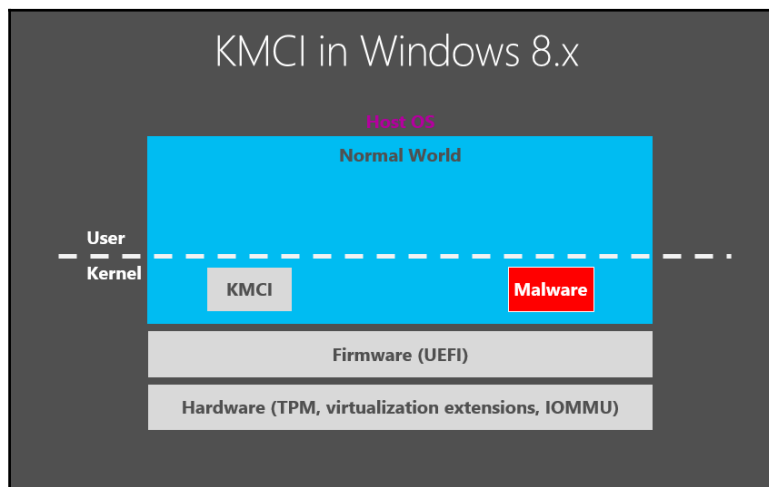
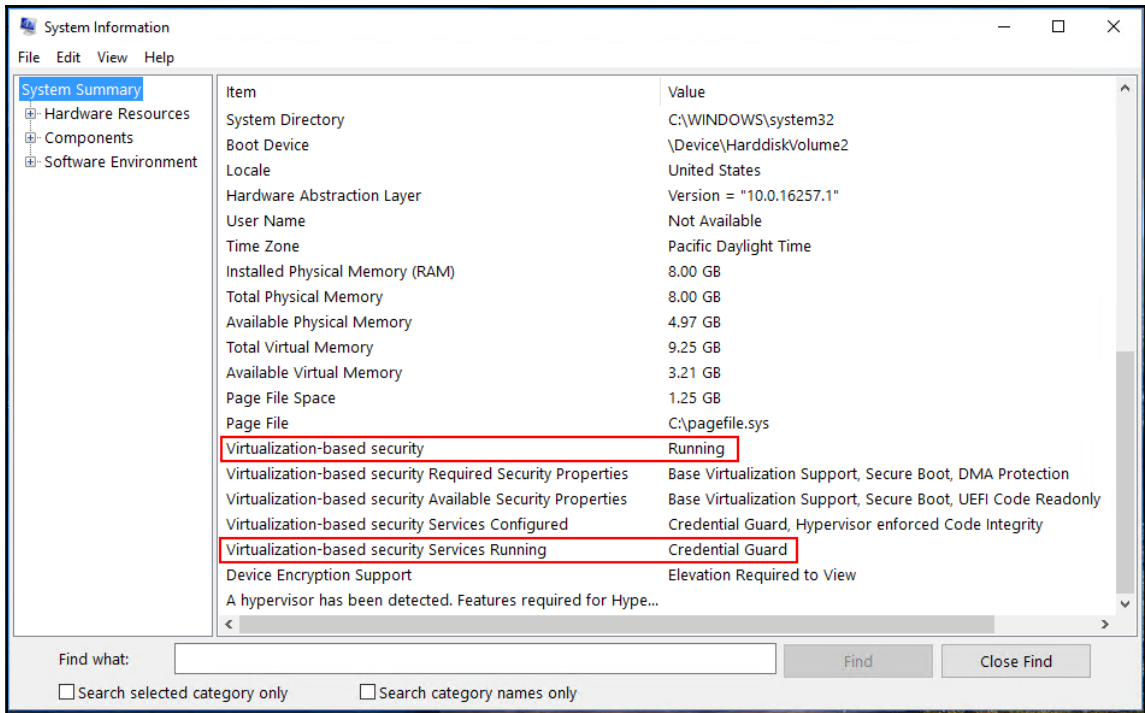




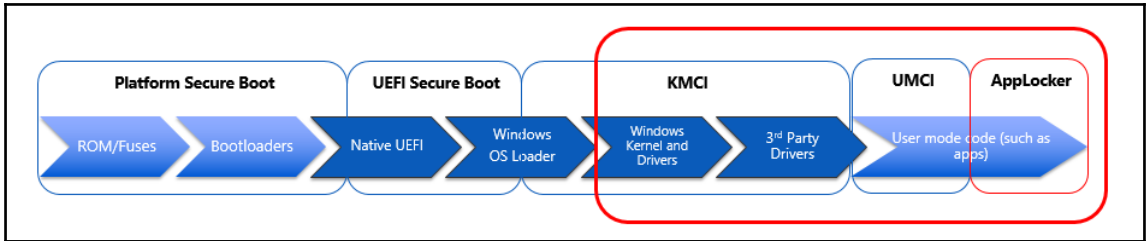
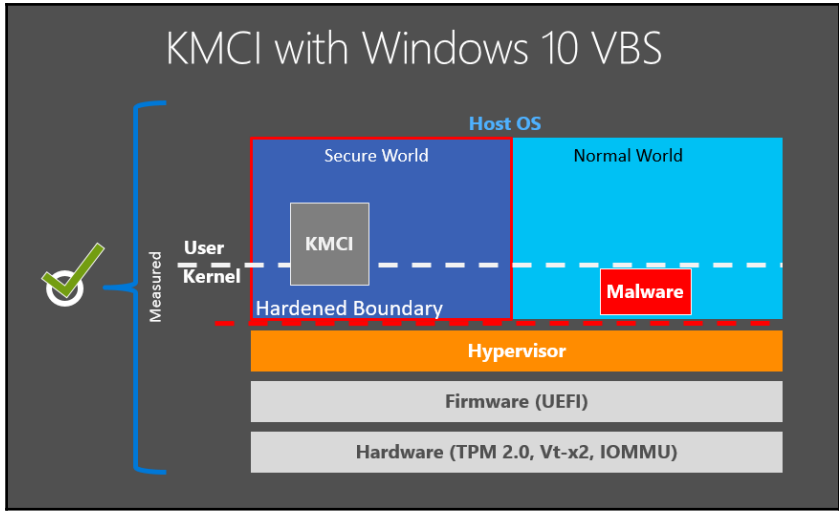


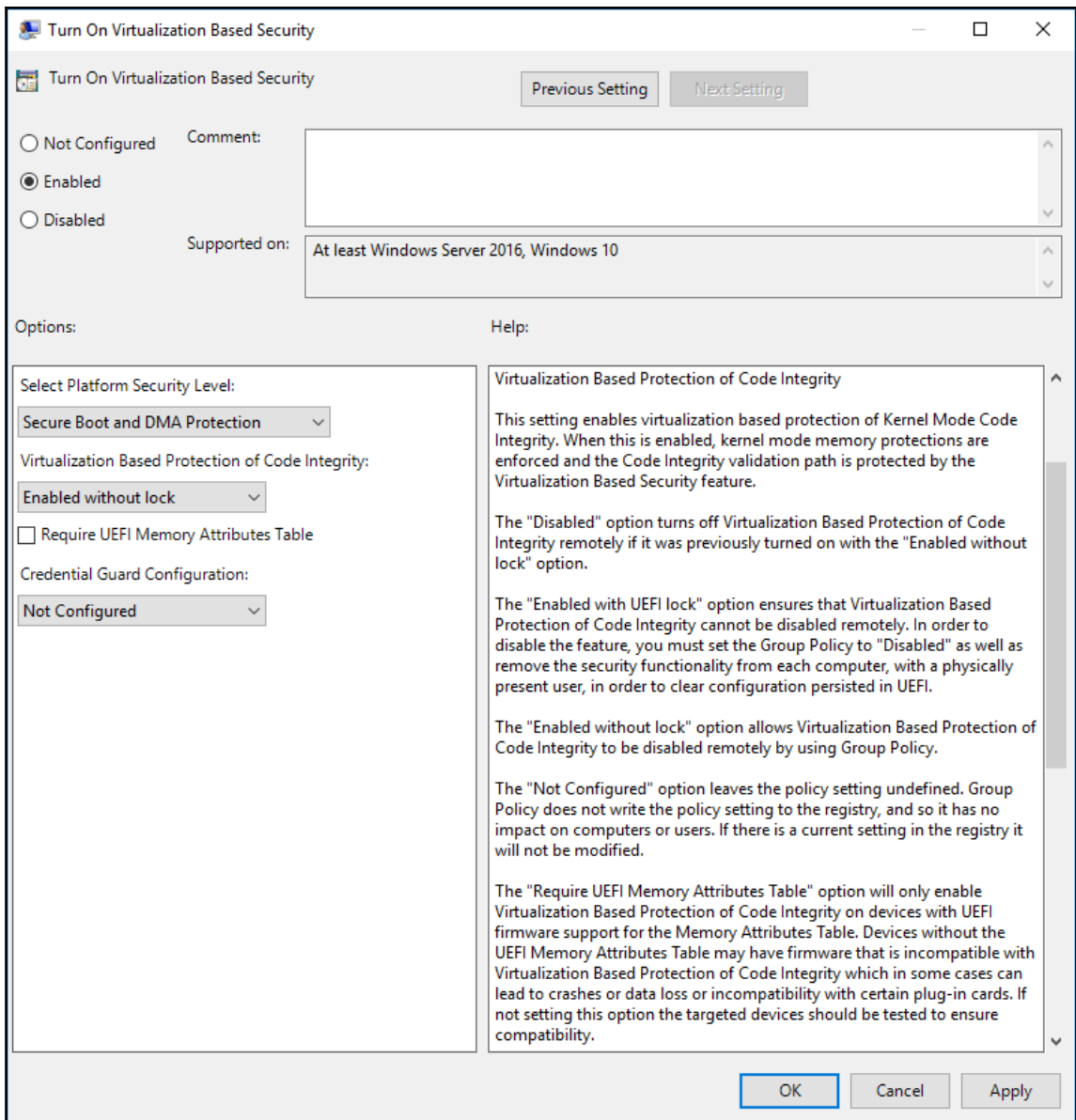






KMCI with Windows 10 VBS

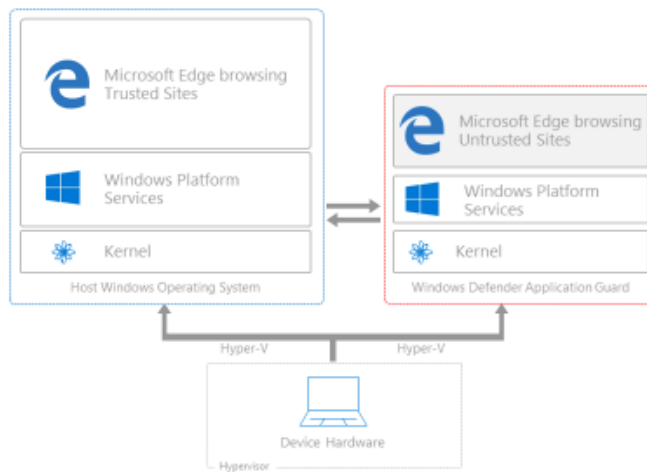


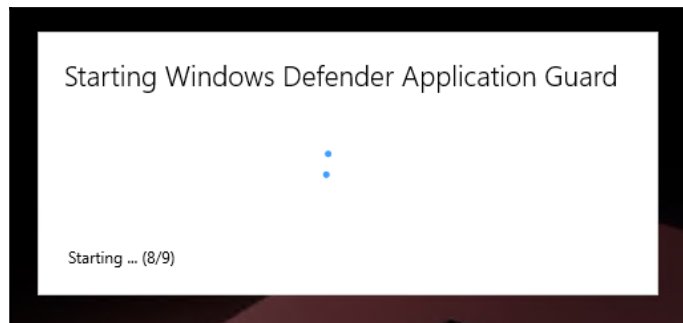
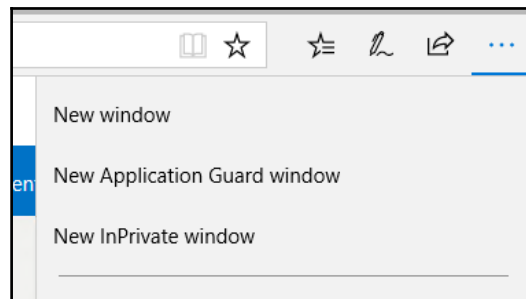
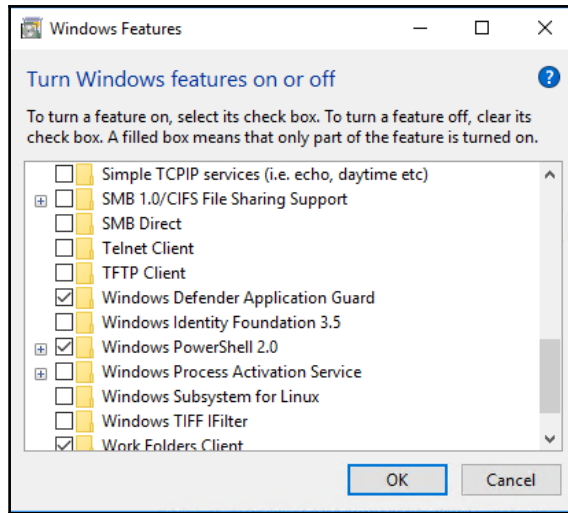


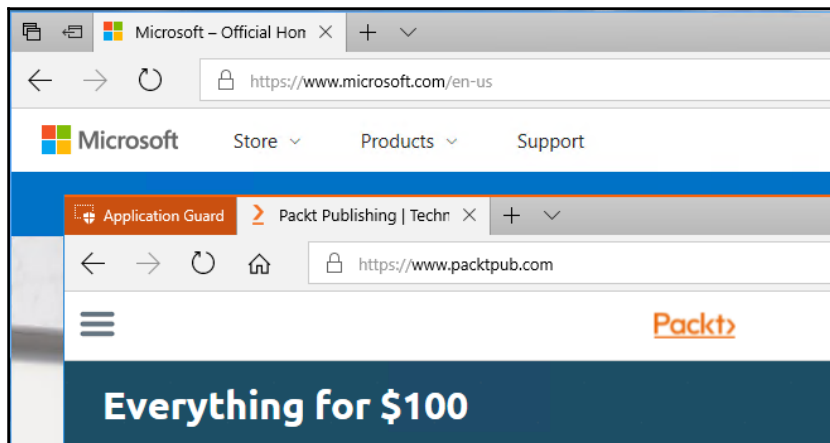
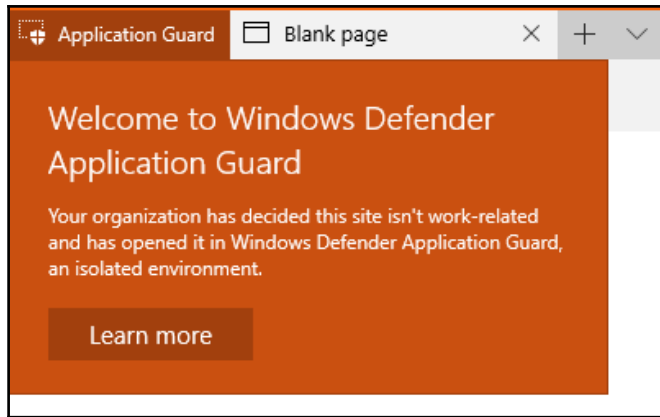


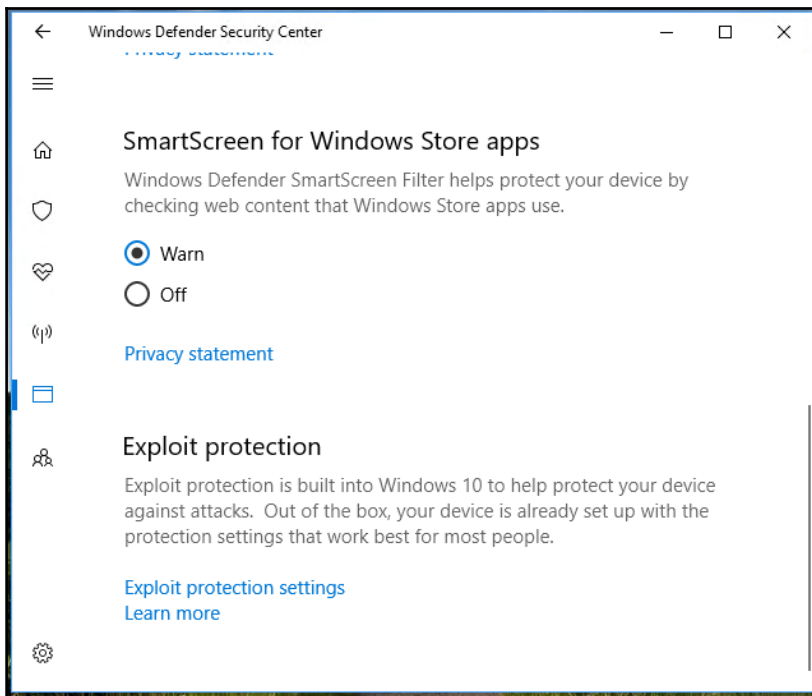
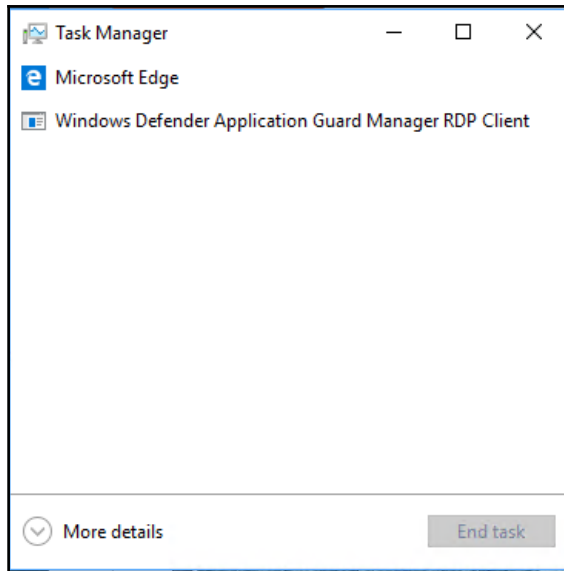
Your PC ran into a problem and needs to restart. We're just collecting some error info, and then we'll restart for you. (0% complete)

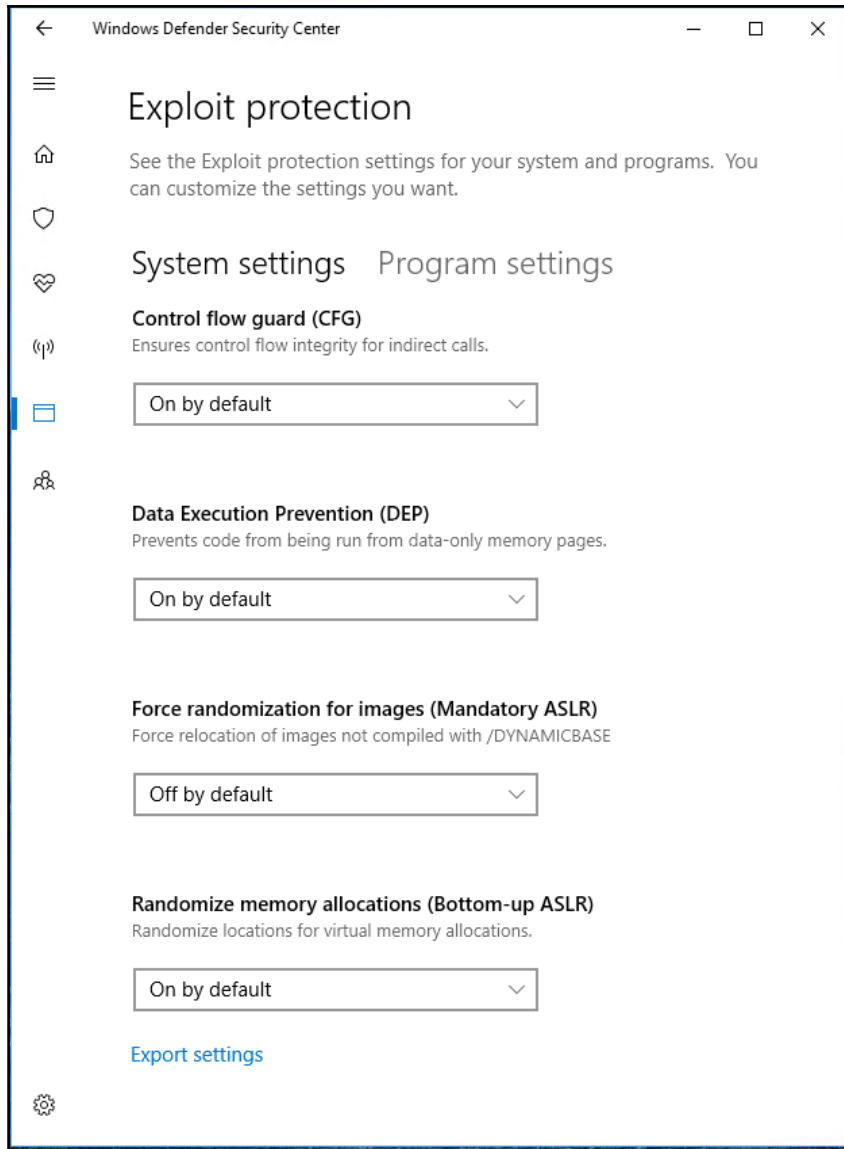
If you'd like to know more, you can search online later for this error: `KERNEL_SECURITY_CHECK_ERROR`

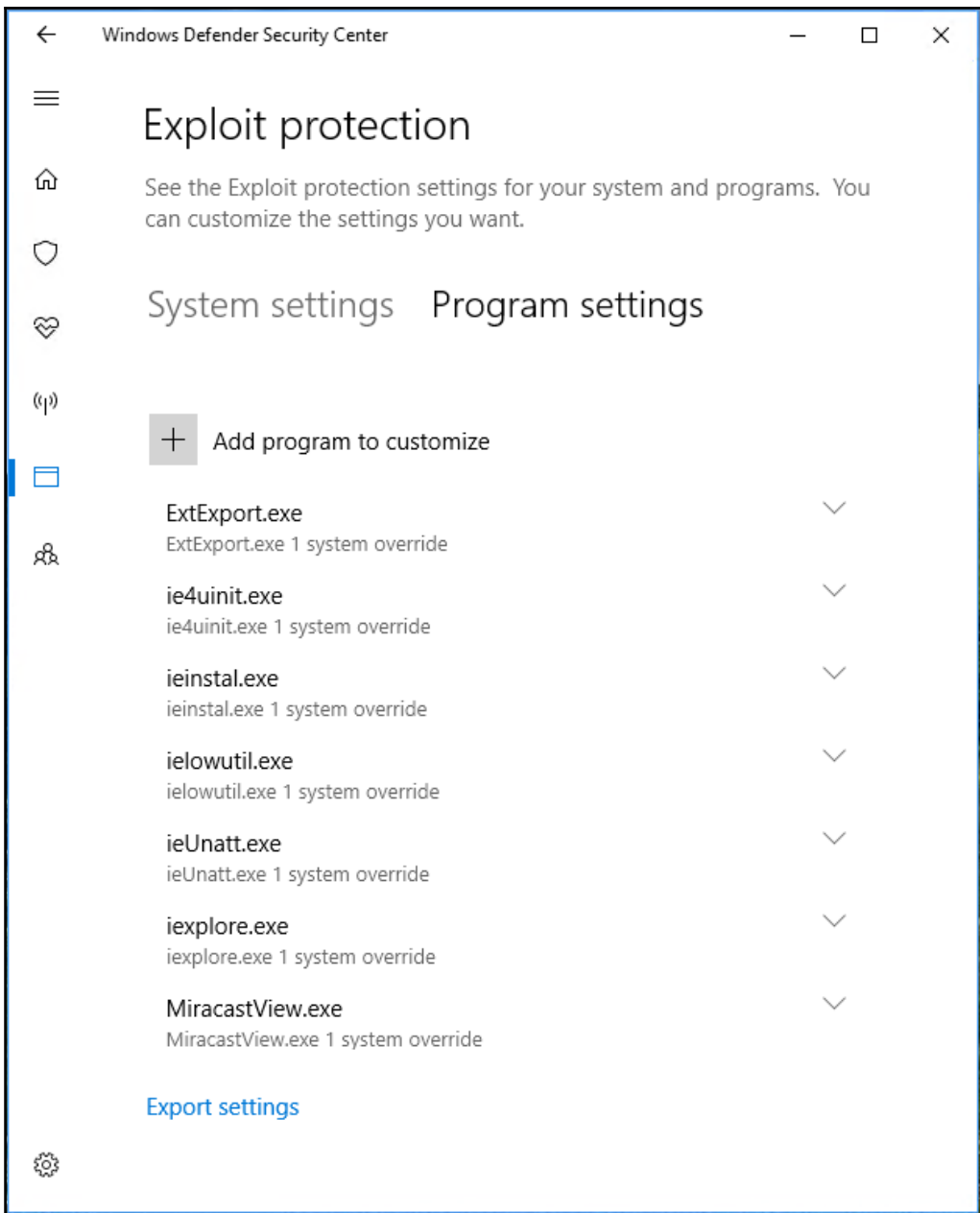












Program settings: iexplore.exe

Arbitrary code guard (ACG)

Prevents non-image backed executable code, and code page modification.

Override system settings

Off

Allow thread opt-out

Audit

Block low integrity images

Prevents loading of images marked with low-integrity.

Override system settings

Off

Audit

Block remote images

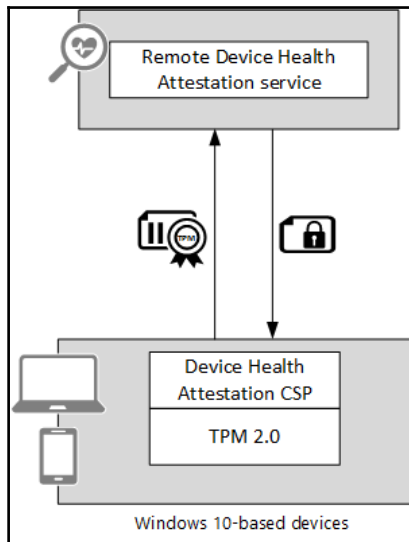
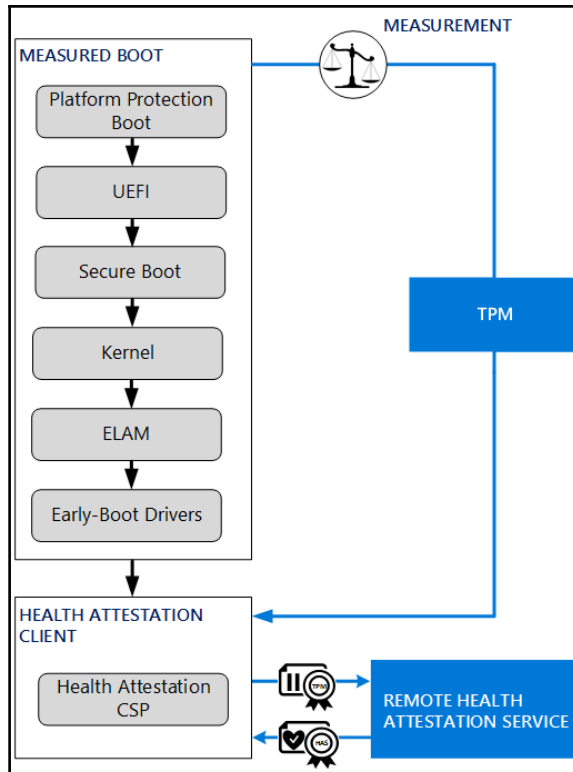
Prevents loading of images from remote devices.

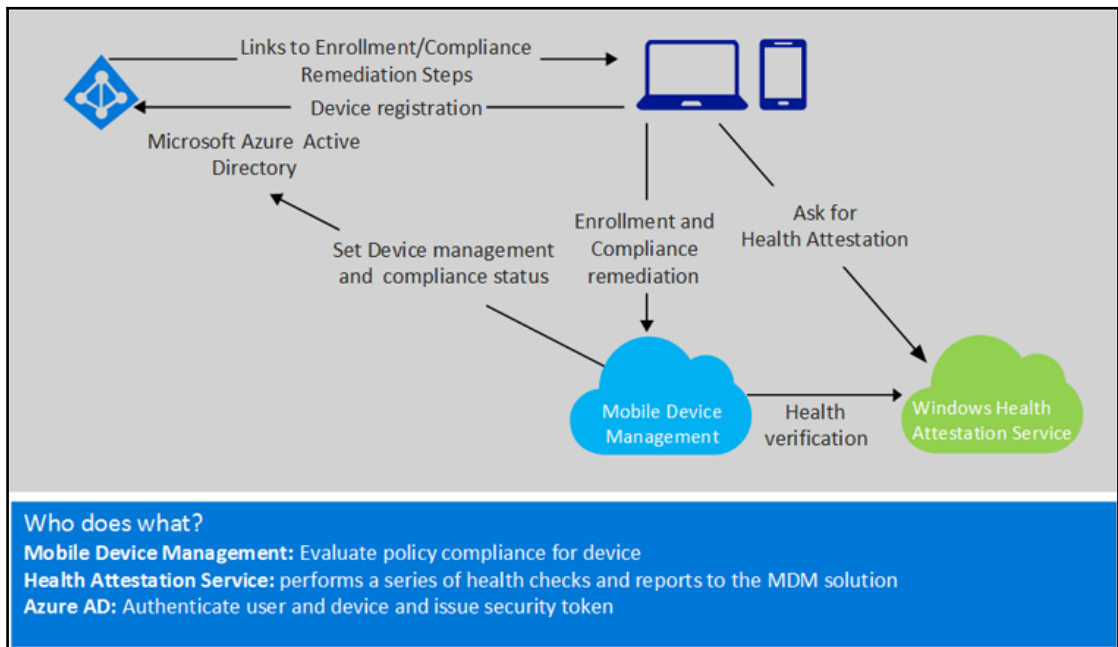
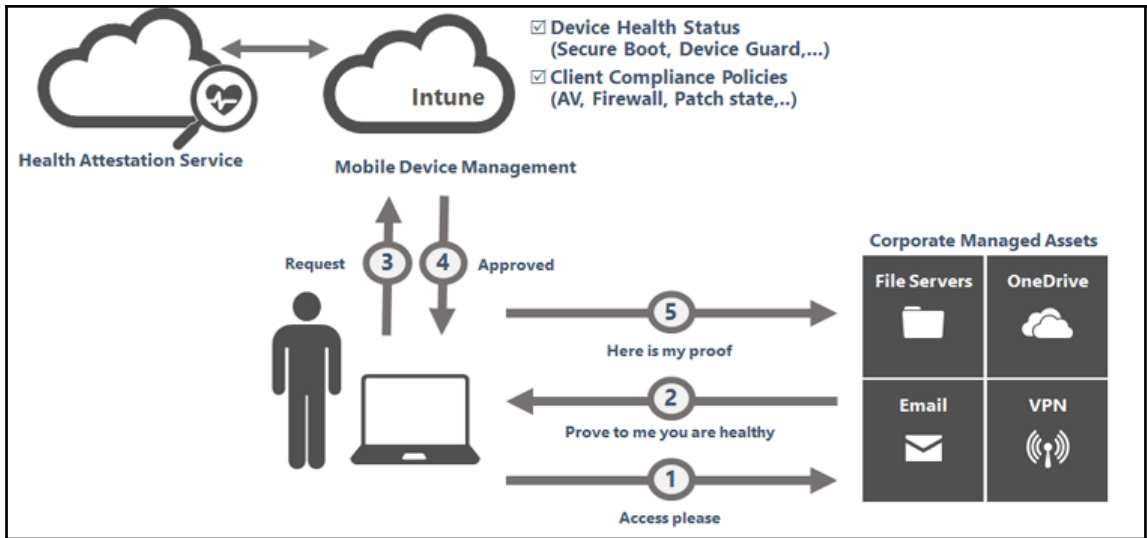
Override system settings

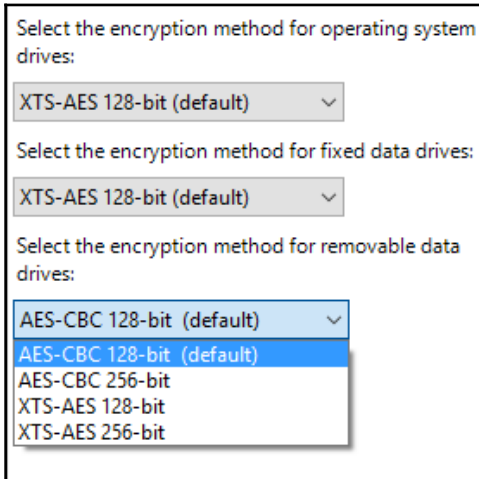
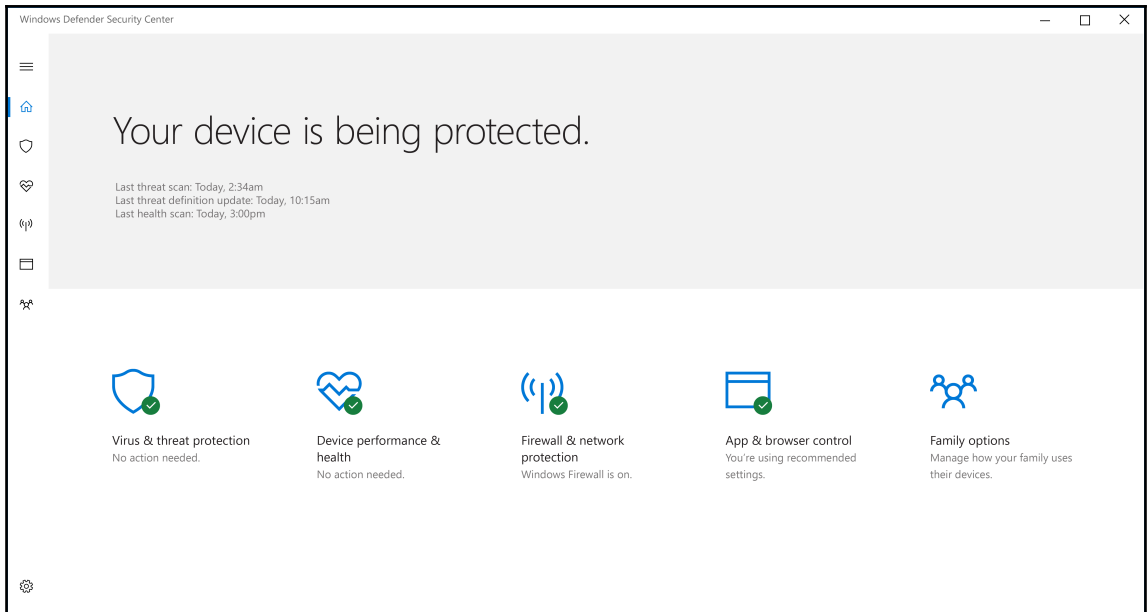
Off

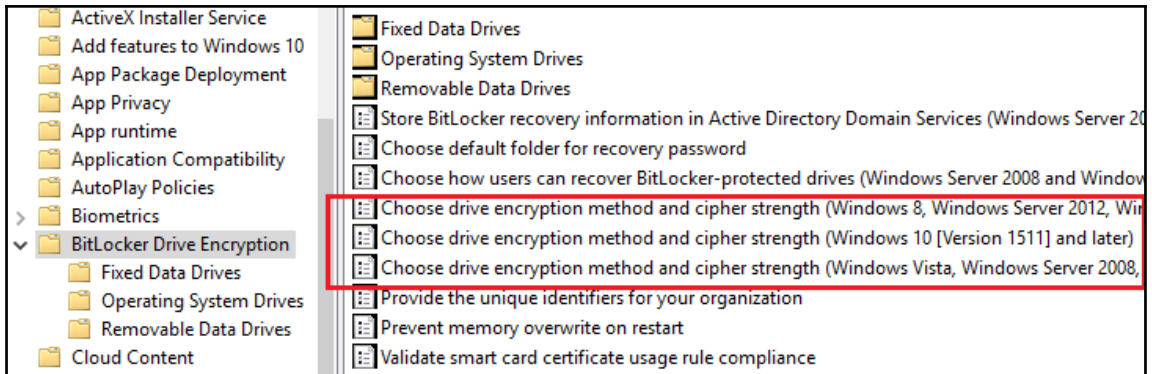
Apply

Cancel

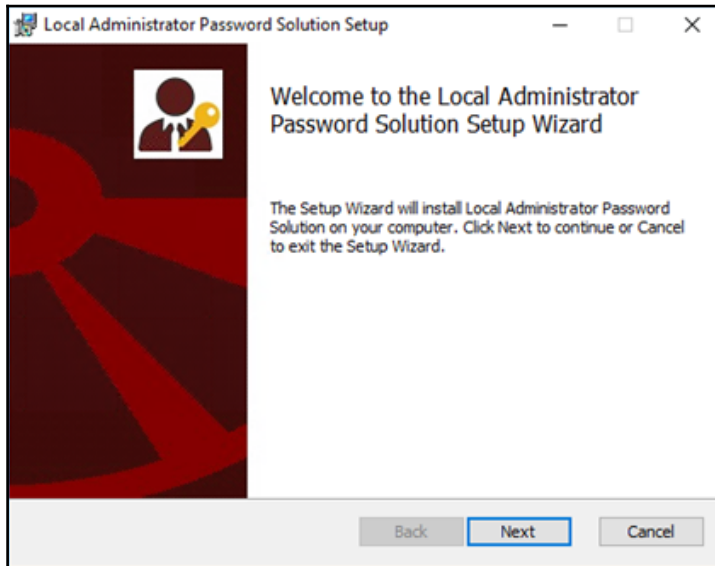


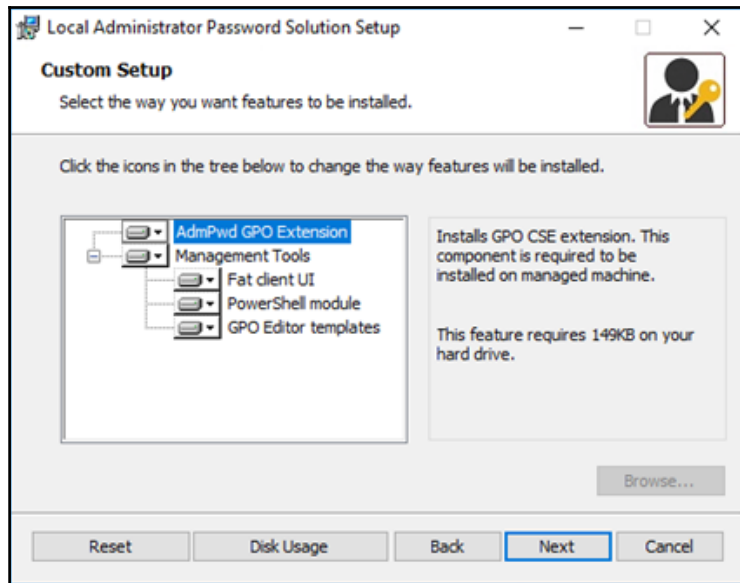
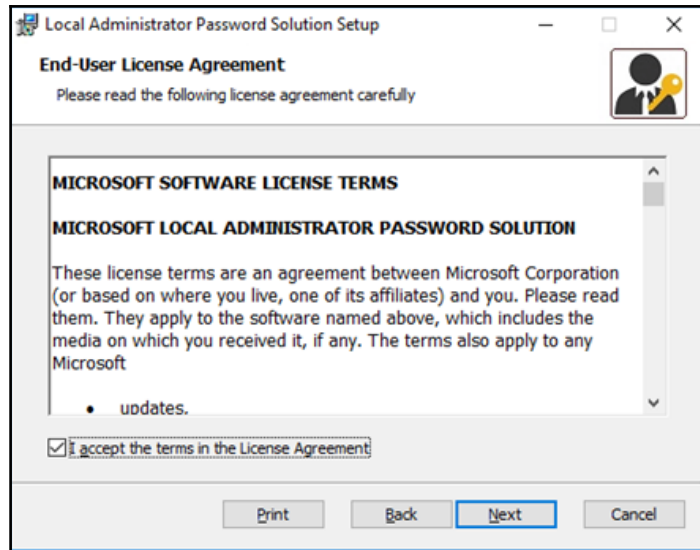


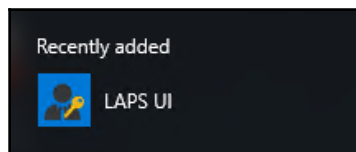
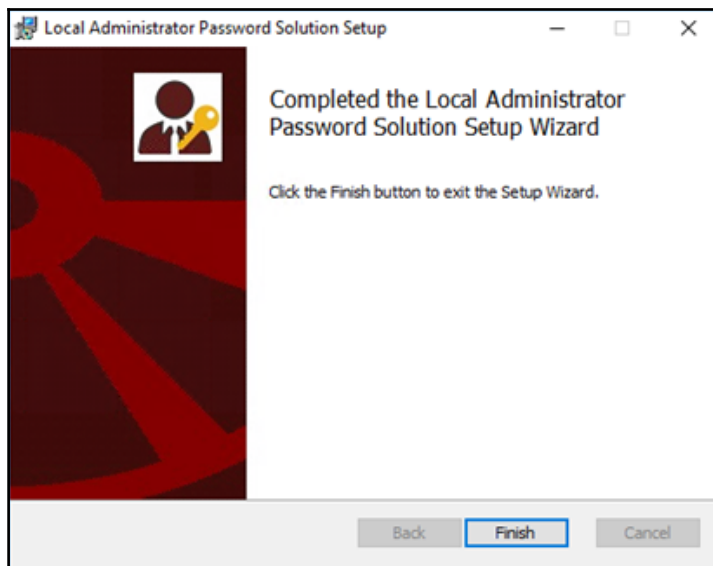
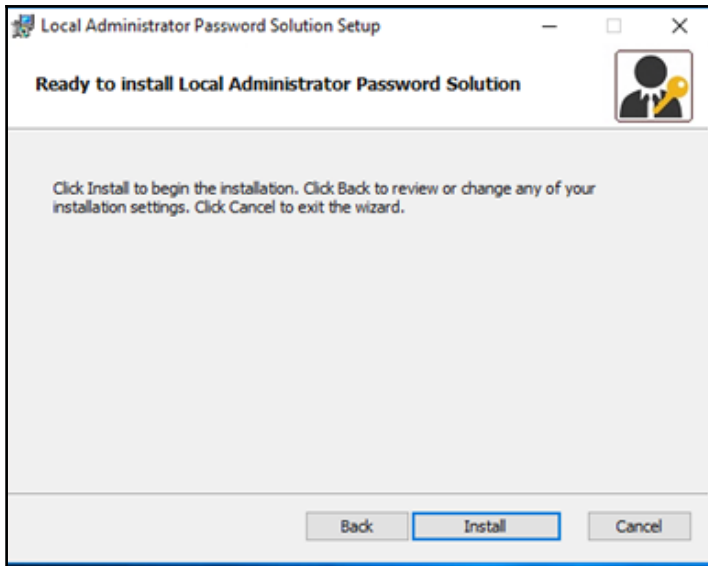


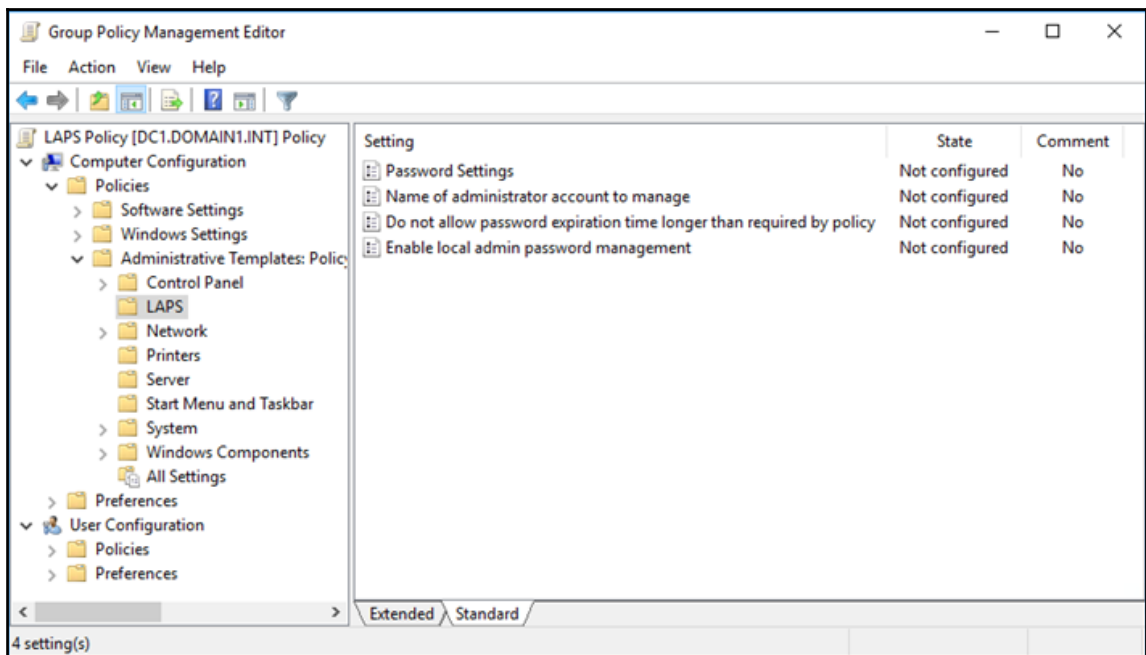
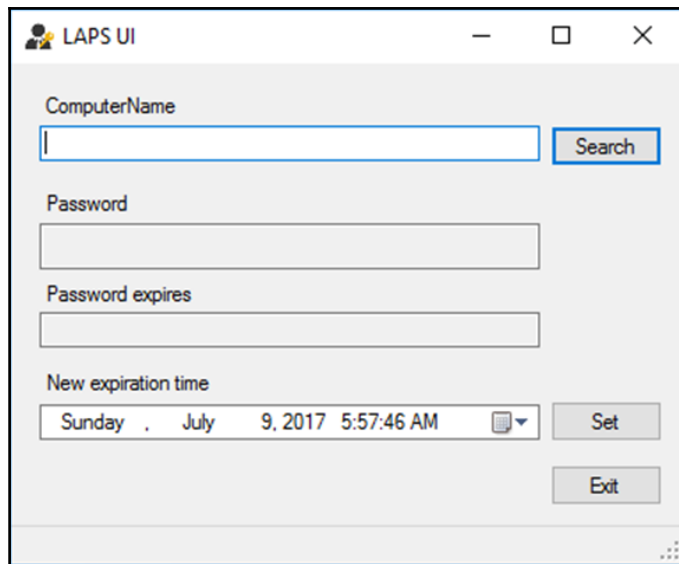


Name	Type	Size
LAPS.x64	Windows Installer Package	996 KB
LAPS.x86	Windows Installer Package	968 KB
LAPS_Datasheet	Microsoft Word Document	100 KB
LAPS_OperationsGuide	Microsoft Word Document	589 KB
LAPS_TechnicalSpecification	Microsoft Word Document	71 KB









Name of administrator account to manage

Previous Setting Next Setting

Not Configured Comment:

Enabled

Disabled

Supported on: At least Microsoft Windows Vista or Windows Server 2003 family

Options:

Administrator account name

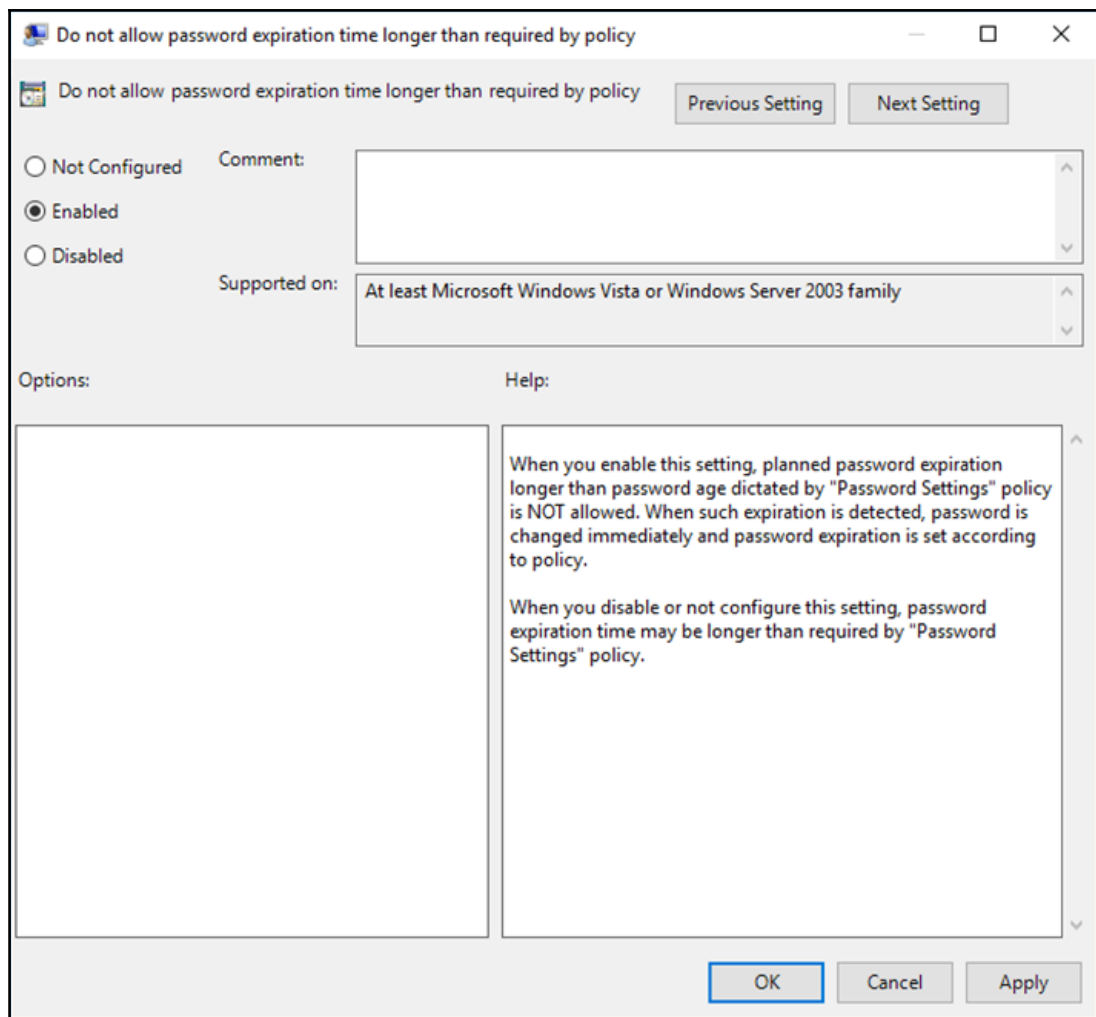
Fred

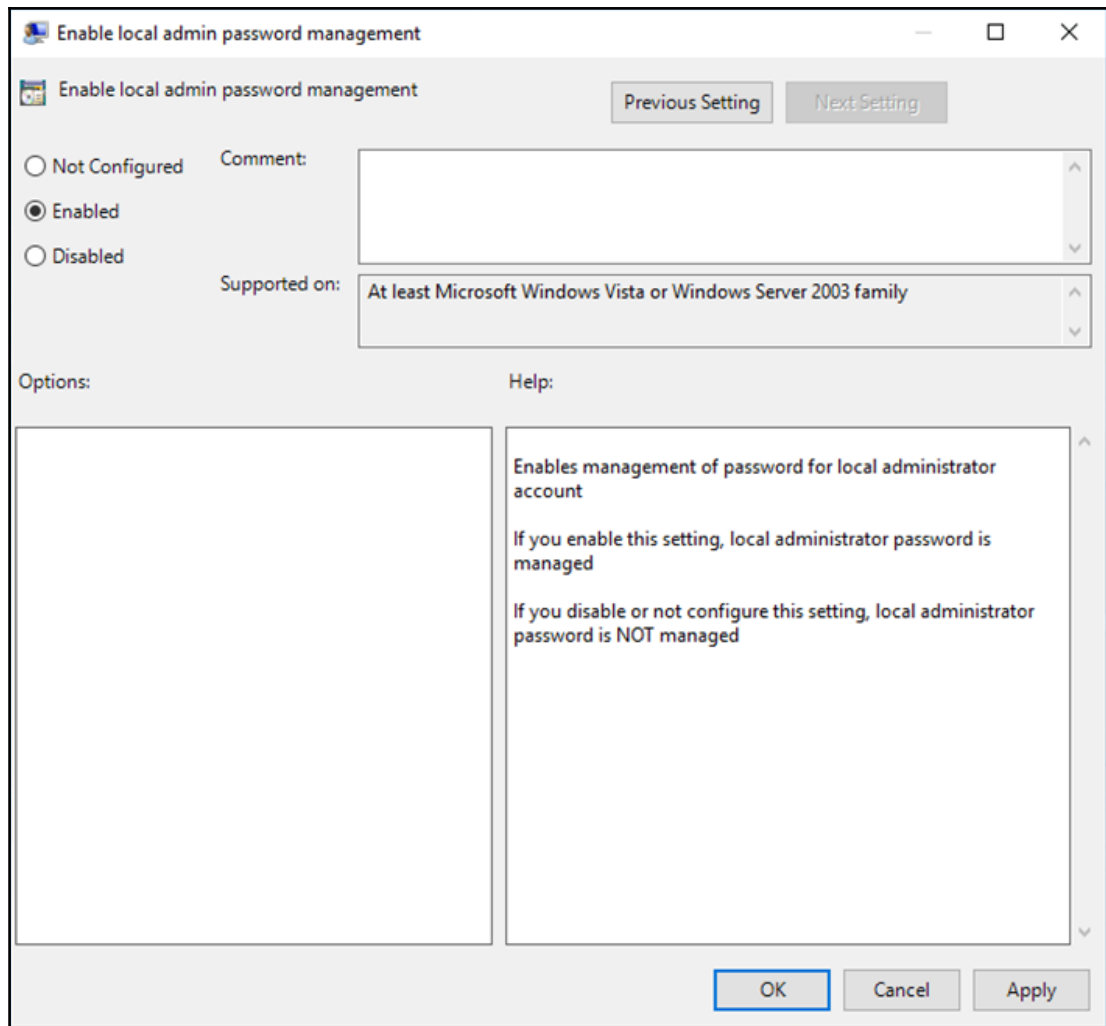
Help:

Administrator account name: name of the local account you want to manage password for.
DO NOT configure when you use built-in admin account. Built-in admin account is auto-detected by well-known SID, even when renamed

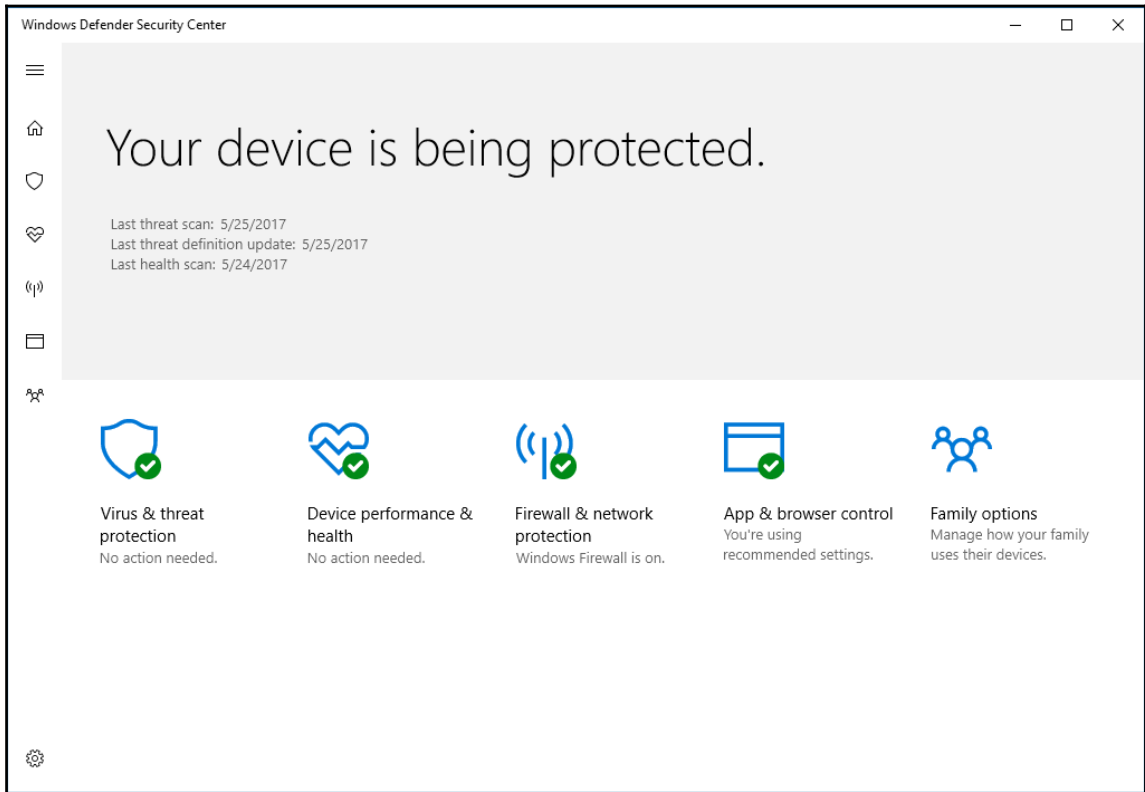
DO configure when you use custom local admin account

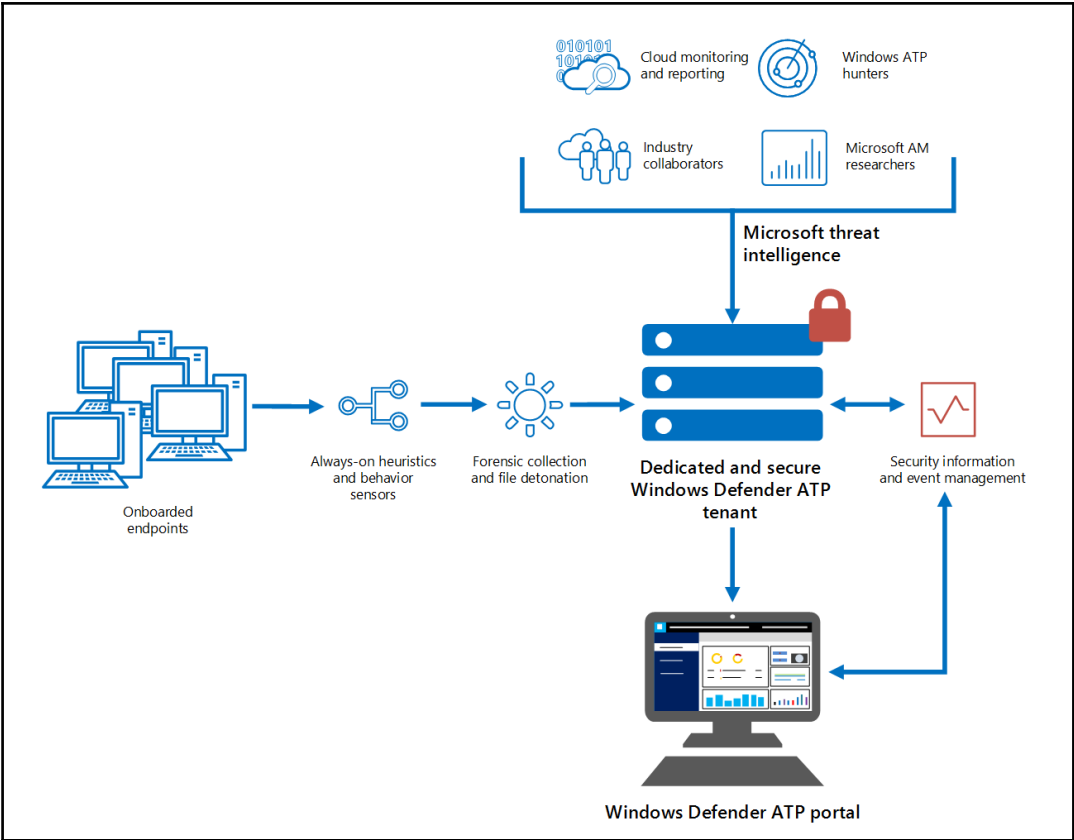
OK Cancel Apply





Chapter 08: Windows Defender Advanced Threat Protection





Windows Defender Security Center | Endpoint management

Client endpoint onboarding

Onboard endpoints in your organization to Windows Defender ATP by downloading the following onboarding configuration package available for a range of deployment tools. Select the one relevant for your organization and follow the instructions. For detailed instructions and additional support see the [Onboard endpoints and set up access](#) section in the [Windows Defender ATP guide](#). Onboarded endpoints will appear in your portal Machines View tab.

Select your deployment tool:

System Center Configuration Manager (current branch) version 1606 and later

Version 1606 and later of System Center Configuration Manager provides an integrated console to deploy Windows Defender ATP policies and monitor the Windows Defender ATP agent health status. For more information on how to configure and monitor Windows Defender ATP endpoints, see [Windows Defender ATP](#) section in the System Center Configuration Manager guide.

Download package

Endpoint onboarding

Windows Defender ATP

Select an item to view its description.

Setting	State
Set client latency mode	Not configured
Enable\Disable Sample collection	Not configured

Windows Defender Security Center | Dashboard

admin1@contoso.com

1

- Dashboard
- Alerts queue
- Machines list
- Service health
- Preferences setup
- Endpoint management

2

Active alerts

30 days

3

Latest active alerts

Date	Alert Description	Severity
05.19.2017	Process hollowing detected	Medium
05.19.2017	Tampering with Windows Defender ATP sensor settings	Medium
05.19.2017	Communication to a malicious network destination	Low
05.19.2017	Communication to a malicious network destination	Low
05.19.2017	Communication to a malicious network destination	Low
05.19.2017	Communication to a malicious network destination	Low
05.19.2017	Communication to a malicious network destination	Low
05.19.2017	Communication to a malicious network destination	Low
05.19.2017	Communication to a malicious network destination	Low
05.19.2017	Communication to a malicious network destination	Low

Machines at risk

machines list

Machine	High	Medium	Low	Informational
machine-z1l	3	12	2	2
machine-01	2	0	0	0
machine-xft	2	0	0	0
machine-1lr	2	0	0	0

Users at risk

30 days

User	High	Medium	Low	Informational
user-1ajL	2	1	1	0
user-aj3L	1	3	0	0
user-7jtr	1	1	0	0
user-fxr	1	0	0	0

Machines with active malware alerts

30 days

Daily machines reporting (Monthly unique machines: 483,725)

30 days

Sensor health

30 days

More info on TechNet

Service health

Service is operating normally

Windows Defender Security Center Machine

Machines view > desktop-d6lncja

desktop-d6lncja

Actions

- Collect investigation package
- Isolate machine
- Action center

Logged on users (last 30 days)

0

Interactive [0]
RemoteInteractive [0]
Other [0]

No Interactive or RemoteInteractive Logon Types observed on machine.

Machine reporting

Last internal IP: 192.168.10.115
Last external IP: [180.216.148.43](#)

First seen: 18 hours ago
Last seen: 16 hours ago

Alerts related to this machine

No alerts found.

Machine timeline

Value: Search in machine timeline

Information level: All

Event type: All

User account: All

Remove all filters

Timeline: Jan 2017, Feb 2017, Mar 2017, Apr 2017, May 2017, Jun 2017, Today (18.06.2017)

Export to CSV 20 events per page

Older Newer

Windows Defender Security Center | Machine

Machines view > desktop-d6lncja

desktop-d6lncja

Actions

Domain: Workgroup
OS: Windows10 32-bit (Build 15063)

Logged in

No Interactive operations on machine

Alerts related to this machine

No alerts found.

Machine timeline

Value: Search in machine timeline Information level: All

Jan 2017 Feb 2017 Mar 2017

Action center

Investigation package collection

Submission time	Status
19.06.2017 14:57:57	Package available
19.06.2017 15:00:15	Package collection is ready
19.06.2017 14:57:57	Package collection submitted a-richard.diver@ignialabs.com.au: testing capability

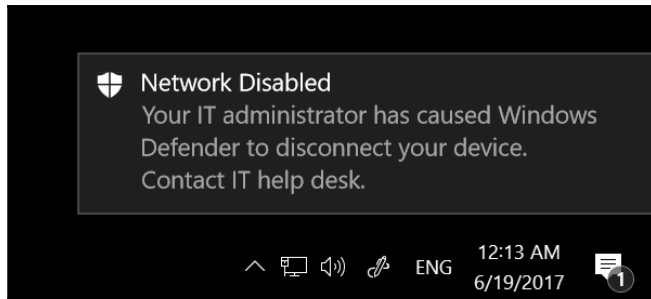
Machine isolation

Submission time	Status
For submitted actions to take effect, machine must be connected to the network.	

Close

WDATP_Investigation_Package.zip

Name	Type
Autoruns	File folder
Installed Programs	File folder
Network Connections	File folder
Prefetch Files	File folder
Processes	File folder
Scheduled Tasks	File folder
Security Event Log	File folder
Services	File folder
SMB Session	File folder
Temp Directories	File folder
Users and Groups	File folder
Forensics Collection Summary.csv	Microsoft Excel Comma Sepa...



Windows Defender Security Center | File | a-richard.diver@

Machines view > desktop-d6lncja > File

File worldwide

<p>File</p> <p>Actions</p> <p>Sha1: b187104076c2cf19788c4d6ba1d8edf0585e82fc</p> <p>MD5: aaf994dd2e79cc6219dba1ace6e57979</p> <p>Sha256: 10293663838e4d78fc611d50eca128fe5ec77140276c33885f778842209ca75c</p> <p>Size: 28.0 KB</p> <p>Signer: Microsoft Windows</p> <p>Issuer: Microsoft Windows Production PCA 2011</p>	<p>Malware detection</p> <p>Virus Total detection ratio:</p> <p>0/60 <small>Virus Total</small></p> <p>Windows Defender AV: No detections found</p>	<p>Prevalence worldwide</p> <p>630</p> <p>First seen: 3 months ago Last seen: 19 minutes ago</p>
--	--	---

Deep analysis

Deep analysis request

File

Actions

- Stop & Quarantine File **df471cf4ddf4c4bfda55463f29fa2**
- Block file **1277ed443ea624**
- Action center **ce5405d3c79c67921b6ec84cbd38dfd2a435e982ff7fbca4**

Issuer: Unknown

Chapter 09: Advanced Configurations

The screenshot shows the Microsoft Store interface for the 'Set up School PCs' application. At the top, there are navigation tabs for Home, Apps, Games, Music, Movies & TV, and Books. A search bar is located in the top right corner. The main content area features the app's icon (a school desk), the title 'Set up School PCs', the developer 'Microsoft Corporation', a 5-star rating with 15 reviews, and the status 'This product is installed.' Below this are 'Launch' and 'Share' buttons. An ESRB rating of 'Everyone' is displayed on the right. The 'Description' section explains that the app simplifies setting up Windows 10 PCs for education using a USB provisioning package. The 'Available on' section shows the app is available on PC. The 'Screenshots' section contains four images: the app's main menu, a 'First step: Let's get you signed in' screen, a 'Configure student PC settings' screen, and a 'Review package summary' screen.

Set up School PCs

Microsoft Corporation
★★★★★ 15
This product is installed.

Launch Share

ESRB Everyone

Description

Set Up School PCs makes it easy to set up Windows 10 PCs with Microsoft's recommended education settings, using a quick USB setup. This app guides you through the creation of a student PC provisioning package and helps you save it to a USB drive. From there, just plug the USB drive into student PCs running Windows 10 Creators Update. Student PCs will automatically join your school network and be configured with settings and apps optimized for education. [More](#)

Available on

PC

Screenshots

1. Create a provisioning package in just a few steps!

2. First step: Let's get you signed in




3. Configure student PC settings

4. Review package summary

Set up School PCs

Create a provisioning package in just a few steps!

Quickly set up school PCs without installing a new version of Windows.
[Learn more](#)



- 1 Create.** Choose preferred settings and apps for student PCs.
- 2 Save.** Use one or more USB drives to save your settings.
- 3 Run.** Plug the USB drive into each student PC. You're done!

[Get started](#)

Set up School PCs

- 1 Create package
- Sign-in**
- 2 Save package
- 3 Run package

First step: Let's get you signed in

Sign in to your school's Office 365 account

This is the best option for setup. Student PCs will automatically be connected to Office 365, Azure Active Directory (Azure AD) and management services like Intune for Education, so managing things will be easier later.

[Need a hand?](#)
[Read this](#)

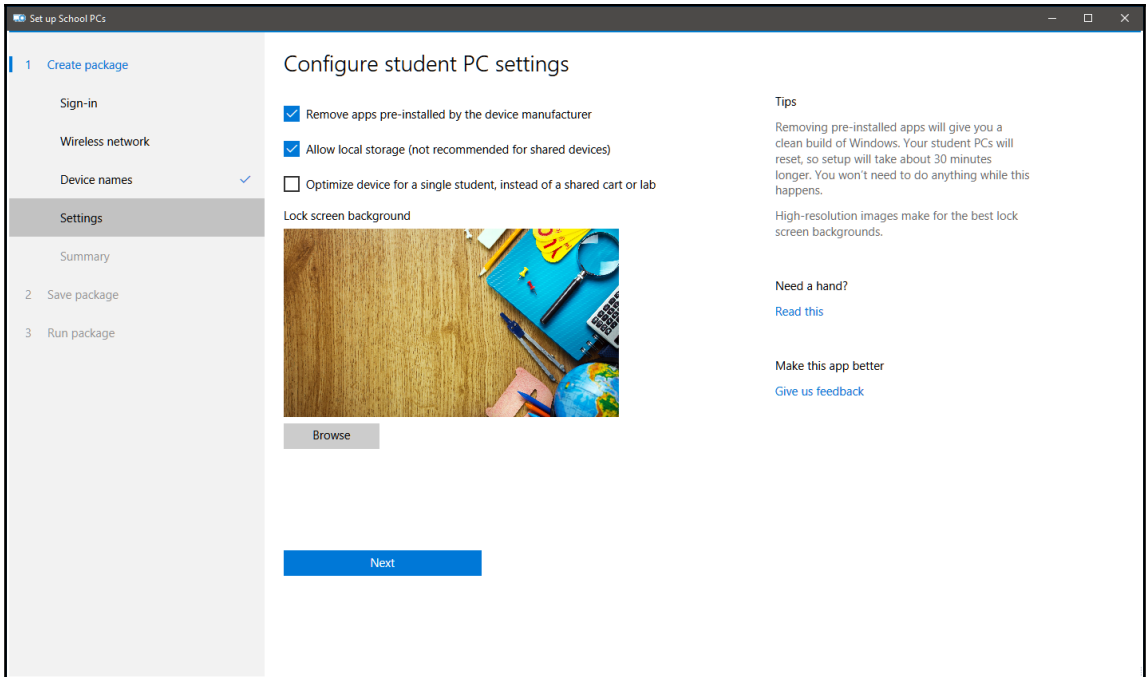
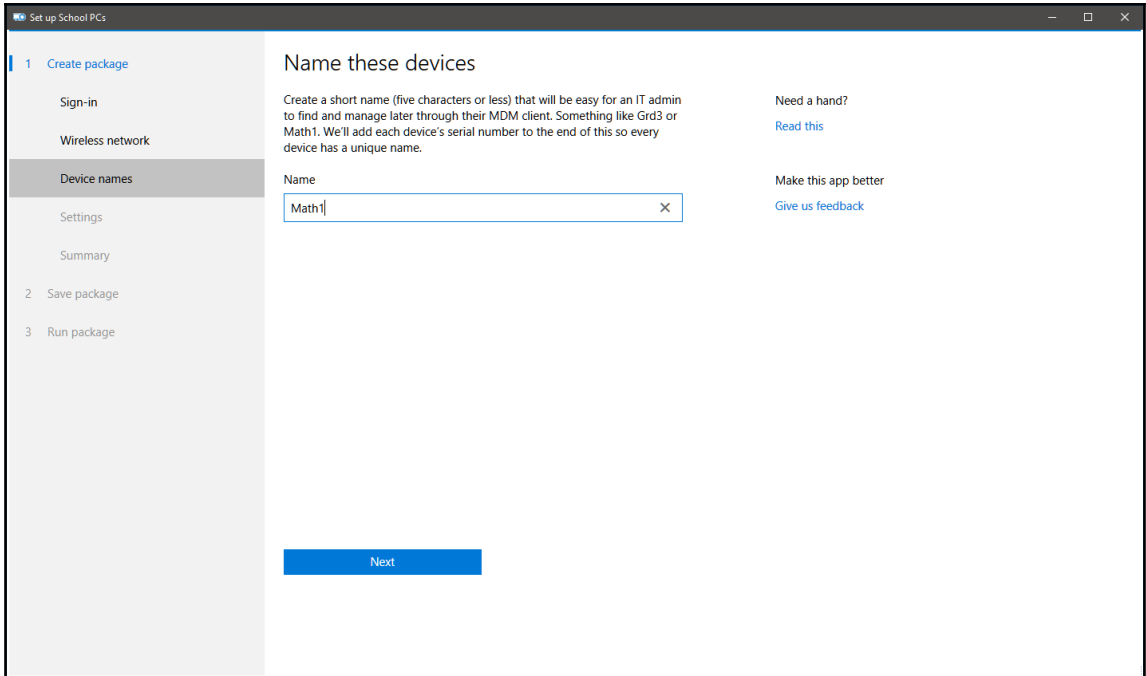
Related products
[Azure Active Directory](#)
[Intune for Education](#)
[Office 365 Education](#)

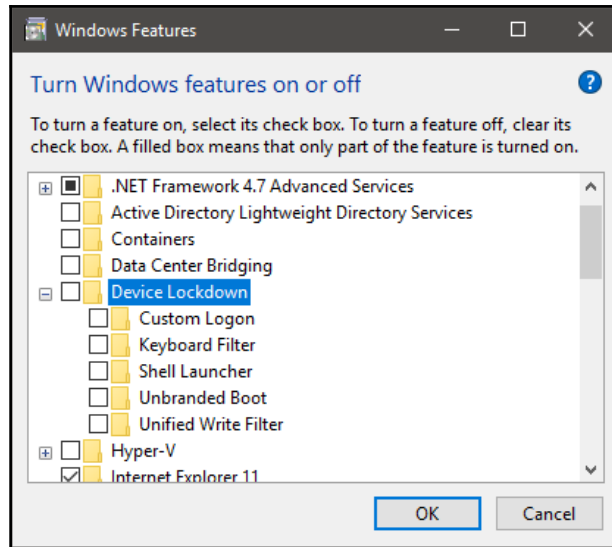
Make this app better
[Give us feedback](#)

Continue without an account

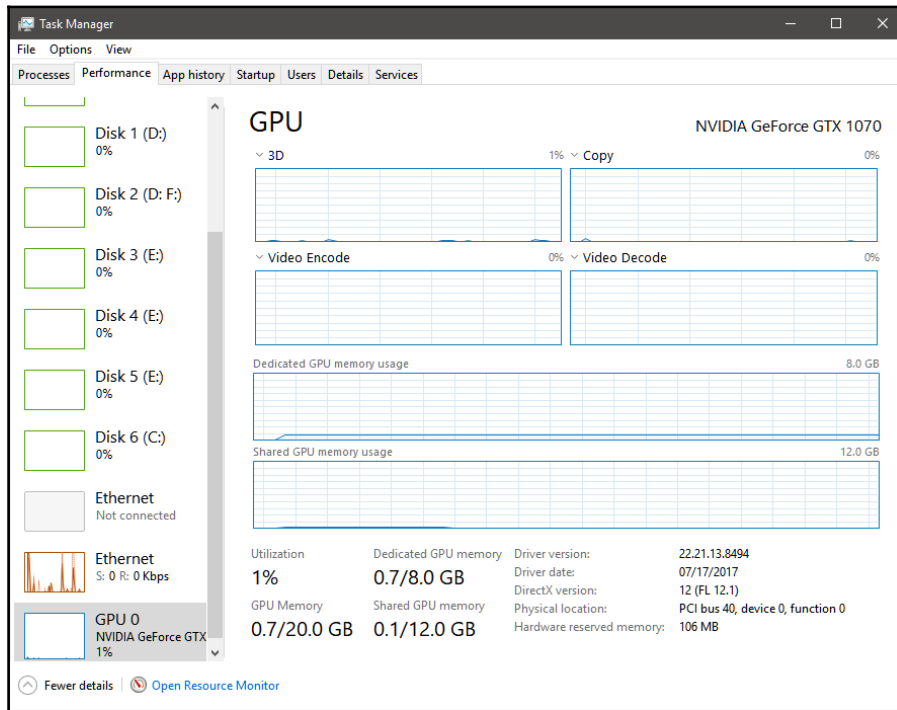
You can complete setup without signing in, but we don't recommend it. Student PCs won't be connected to your school's cloud services, so managing them will be more difficult later.

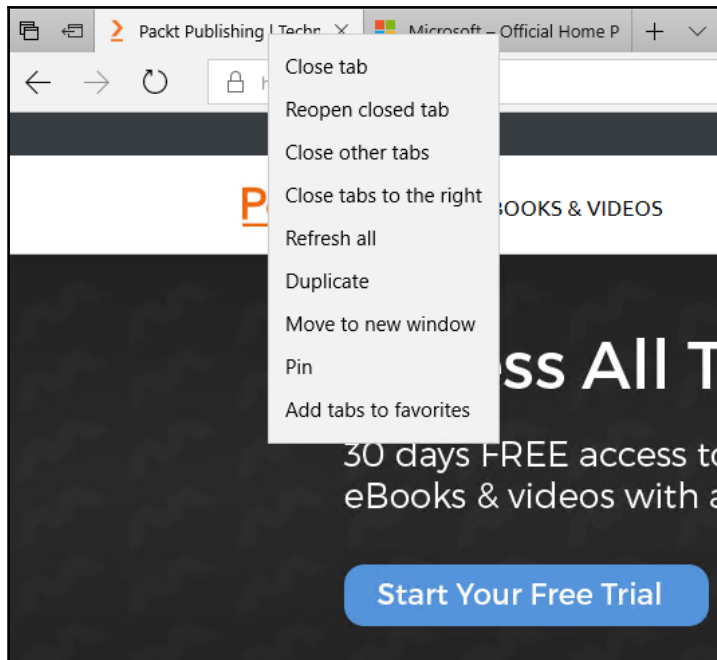
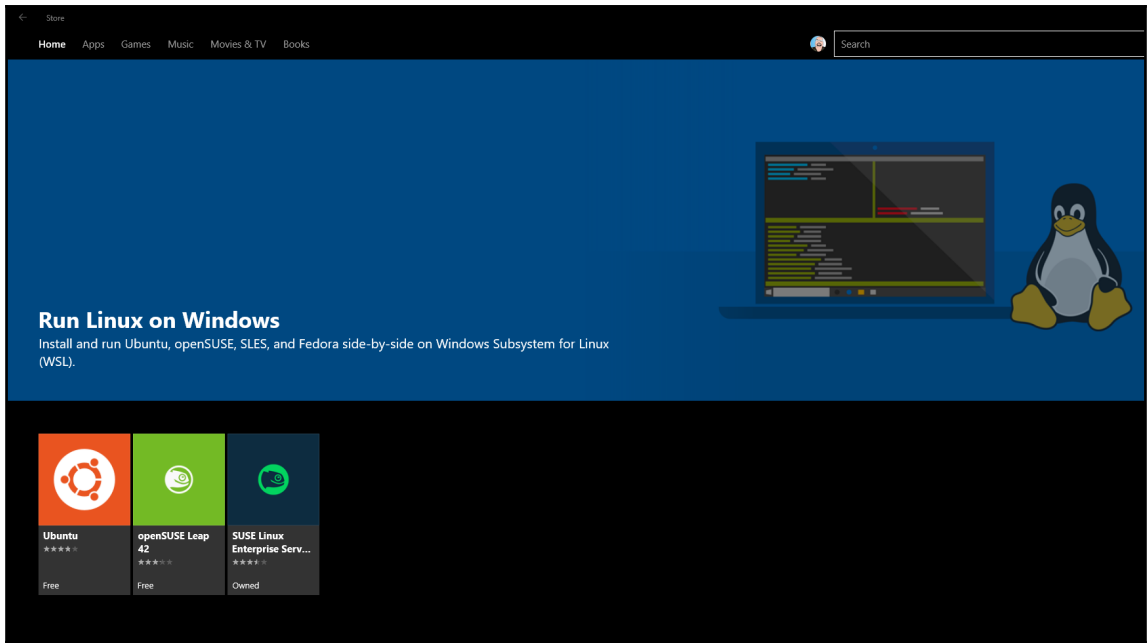
[Sign in](#) [Skip](#)

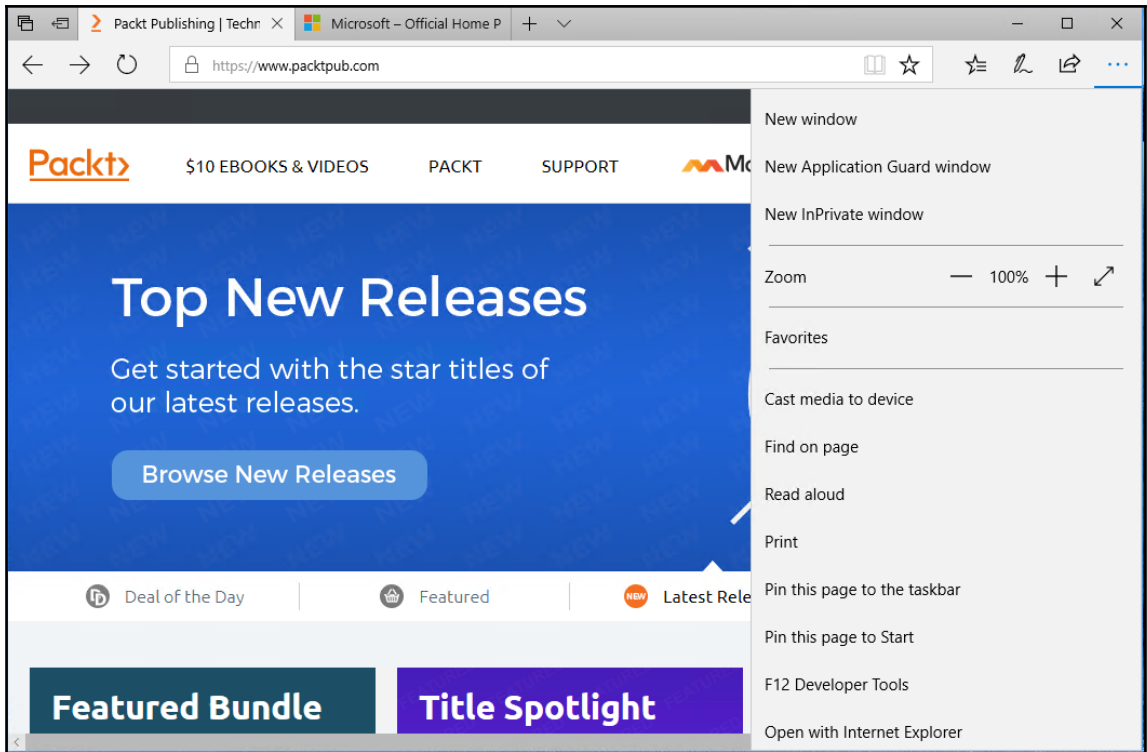


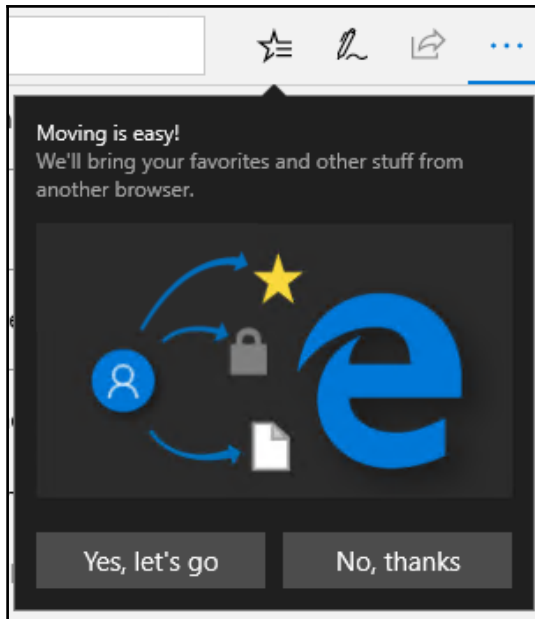


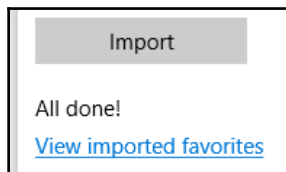
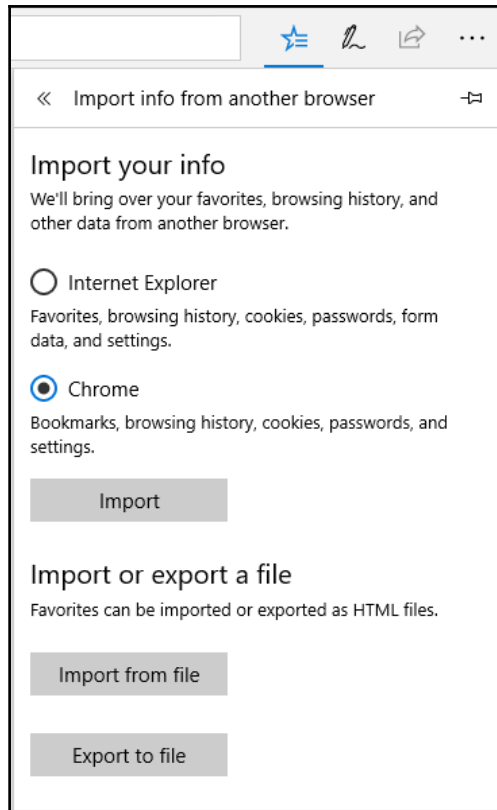
Chapter 10: RedStone 3 Changes

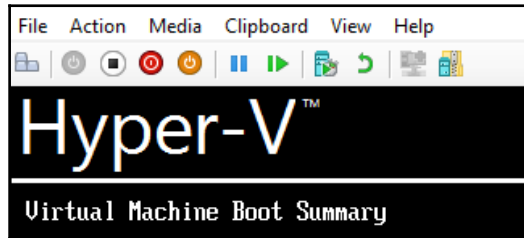
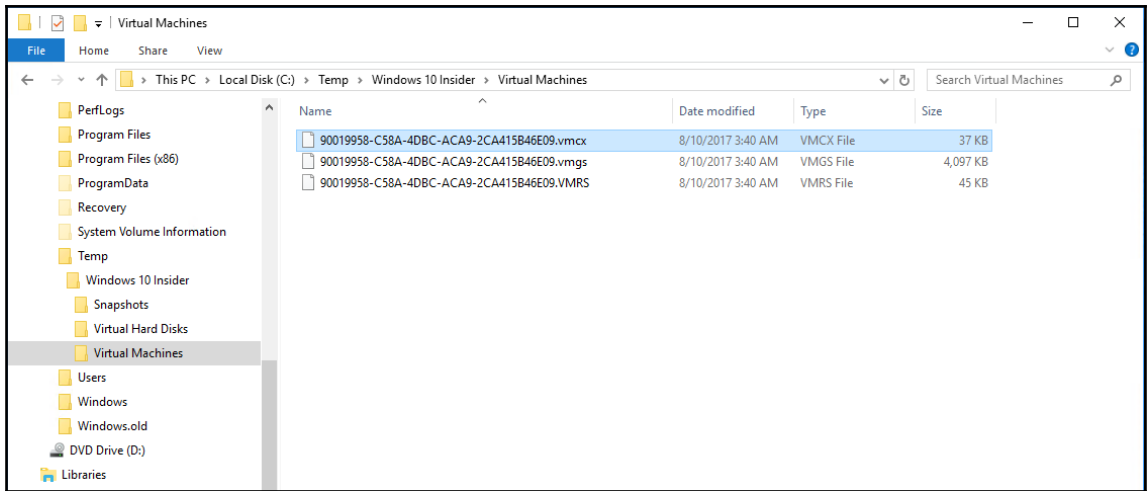


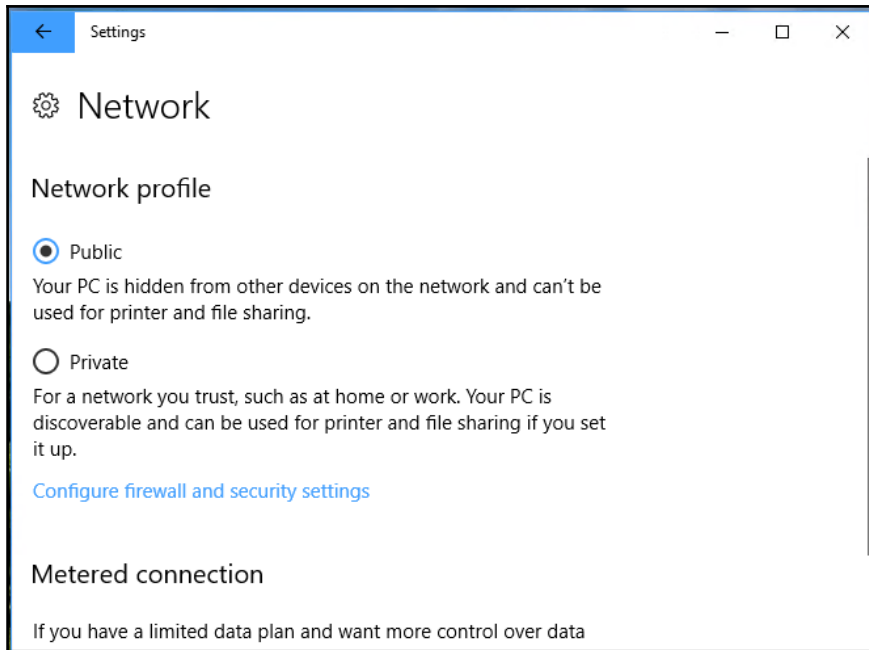












Change how we free up space

Storage sense

On

Storage sense runs automatically when you're low on disk space. We cleaned up 0 bytes of space in the past month.

Temporary Files

- Delete temporary files that my apps aren't using
- Delete files that have been in the recycle bin for over 30 days
- Delete files in the Downloads folder that haven't changed in 30 days

Free up space now

If you're low on space, we can try to clean up files now using the settings on this page.

- Delete previous versions of Windows

These let your PC go back to a previous version of Windows. We delete them automatically after 10 days.

Clean now

