

Lumagate®

We Drive Business Evolution Forward



Planning, Customizing and Deploying Windows 10

about_me - Stefan Schörling

- Chief Technology Officer - Lumagate
- IT Industry Since 1999 – Private-, Public-, Consulting Sector
- Microsoft Certified Trainer since 2007
- Microsoft Most Valuable Professional since 2008

- Specialties
 - Infrastructure
 - Security
 - Client and Enterprise Management

@stefanschorling

www.azuredojo.com

stefan.schorling@lumagate.com

073-396 46 11



about_me - Nickolaj Andersen

- Principal Consultant – Lumagate
- IT Industry Since 2008 – Private and Consulting
- Microsoft Most Valuable Professional since 2016
- PowerShell.org Hero 2015
- Specialties
 - Client and Enterprise Management
 - Mobile Device Management
 - PowerShell / C#

@NickolajA

www.sconfigmgr.com

nickolaj.andersen@lumagate.com

072-200 45 01

System Center User Group



Microsoft®

System Center

User Group Sweden



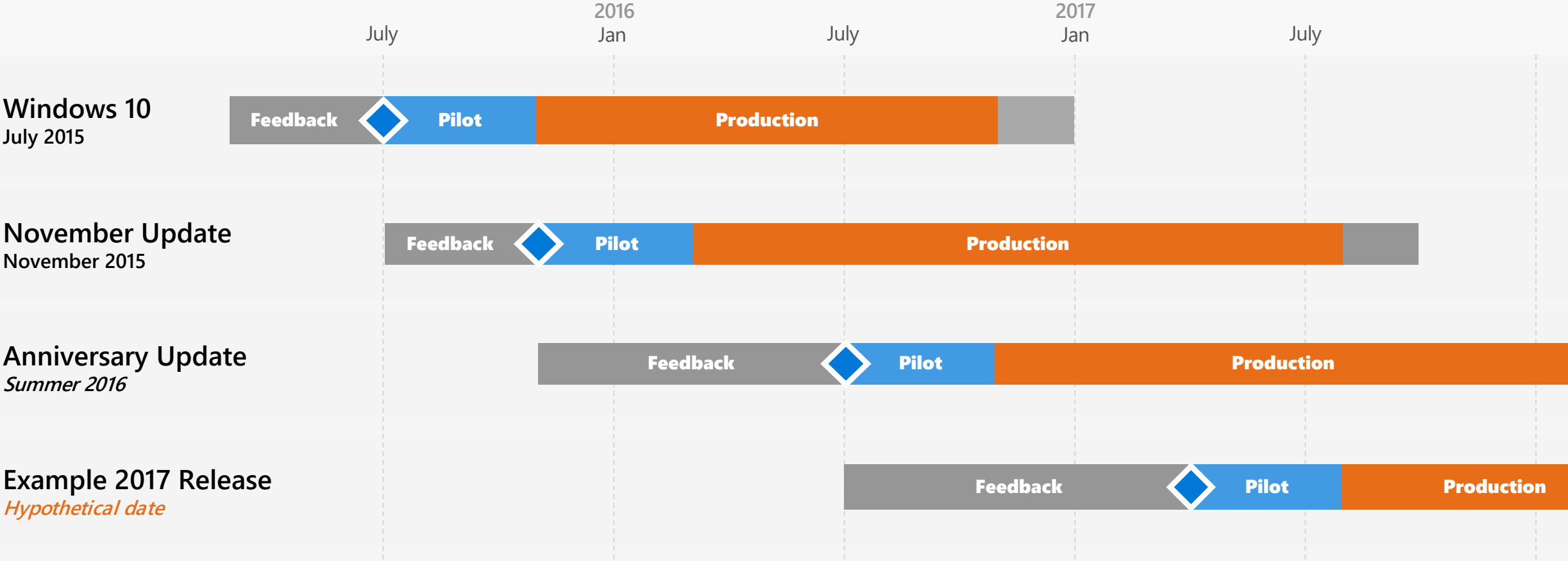
<https://www.facebook.com/groups/241438124169/>

www.scug.se

Planning for Windows 10

- Windows 10 is a Service not a Project
 - You need to add resources
 - Ongoing Maintenance of the Platform

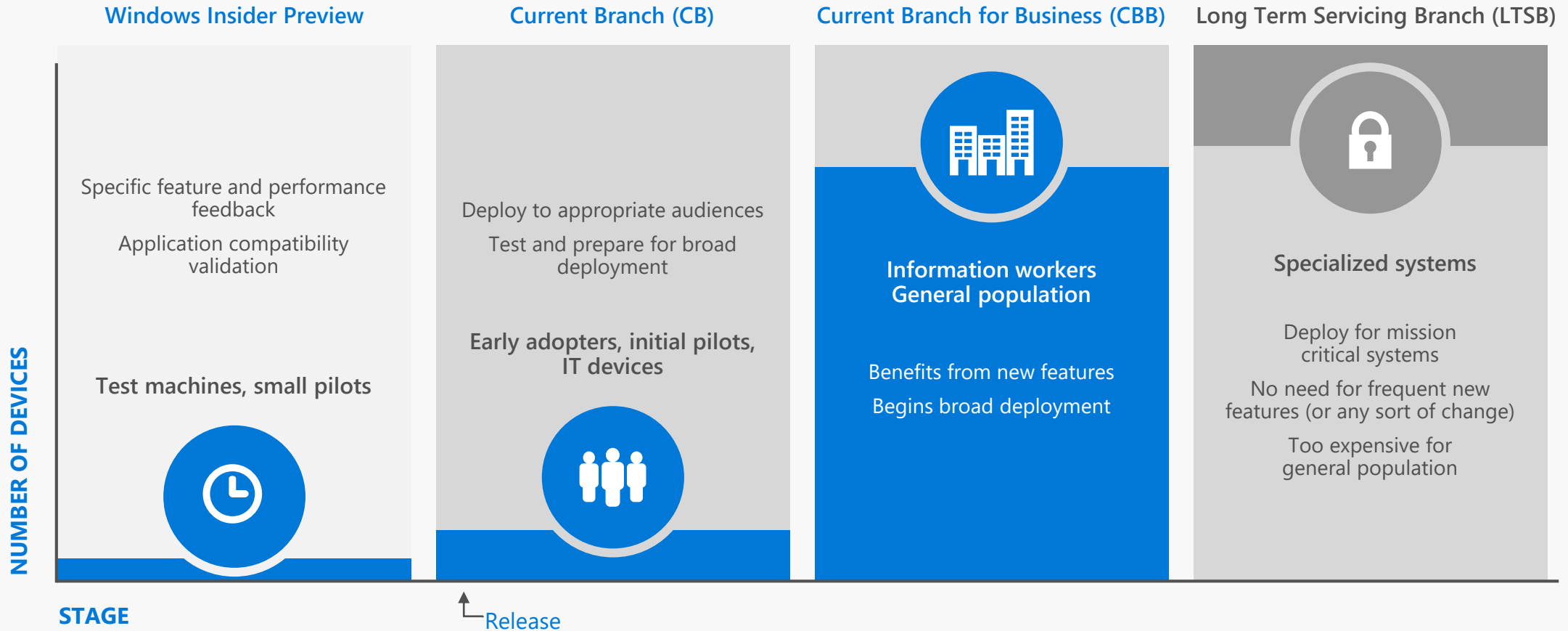
Windows as a Service Cadence



What do I need to think of?

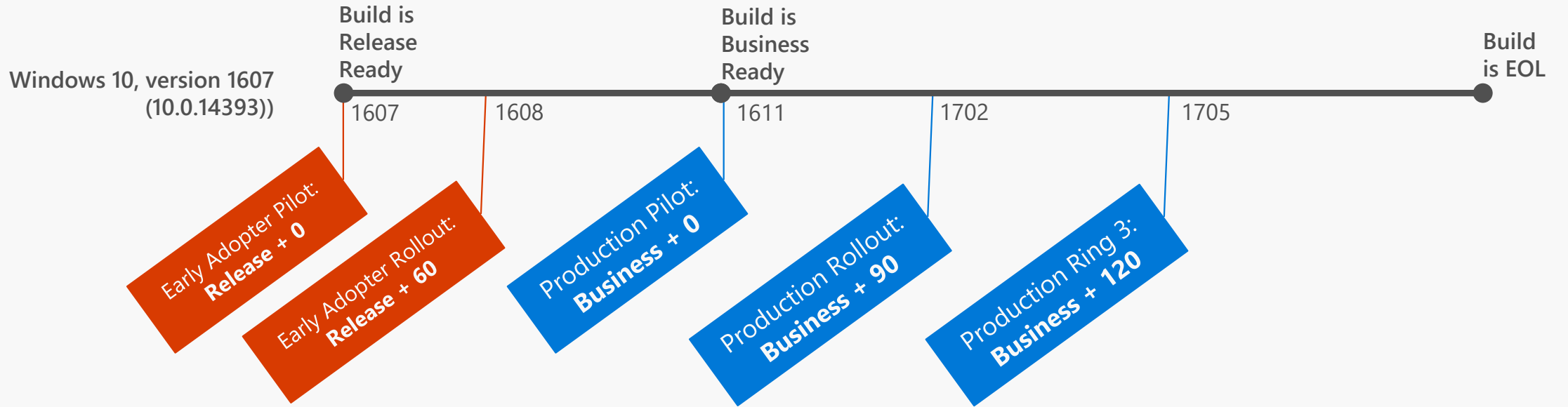
- What features are we going to use
- What deployment rings am I going to be in
- How shall we perform testing of new features
- How shall Application testing be conducted

One Ring to Rule them all





Release Ready & Business Ready Milestones



Define your rings

Easily keep current

Create once,
ongoing monitoring

Do I need to move to Windows 10?

“Windows 7 was designed nearly 10 years ago before any x86/x64 SOCs existed. For Windows 7 to run on any modern silicon, device drivers and firmware need to emulate Windows 7’s expectations for interrupt processing, bus support, and power states, which is challenging for WiFi, graphics, security, and more. As partners make customizations to legacy device drivers, services, and firmware settings, customers are likely to see regressions with Windows 7 ongoing servicing.”

Show all

∨ 16. Where can I read more about Microsoft’s approach to supporting the latest silicon innovation on Windows?

∧ 17. How does Microsoft plan to provide support for new processors and chipsets when they are released?

As new silicon generations are introduced, they will require the latest Windows platform at that time for support. This enables us to focus on deep integration between Windows and the silicon, while maintaining maximum reliability and compatibility with previous generations of platform and silicon. For example, Windows 10 will be the only supported Windows platform on Intel’s upcoming “Kaby lake” silicon, Qualcomm’s upcoming “8996” silicon, and AMD’s upcoming “Bristol Ridge” silicon.



Key Takeaways

- Start Menu
- TaskBar
- Default App Associations
- Branding
- Built-in Applications
- BIOS to UEFI Conversion
- SecureBoot
- Credential Guard



Demo

Deploying Windows 10

- BIOS to UEFI conversion
- Credential Guard
- TPM Owner Password
- Edge browser configuration

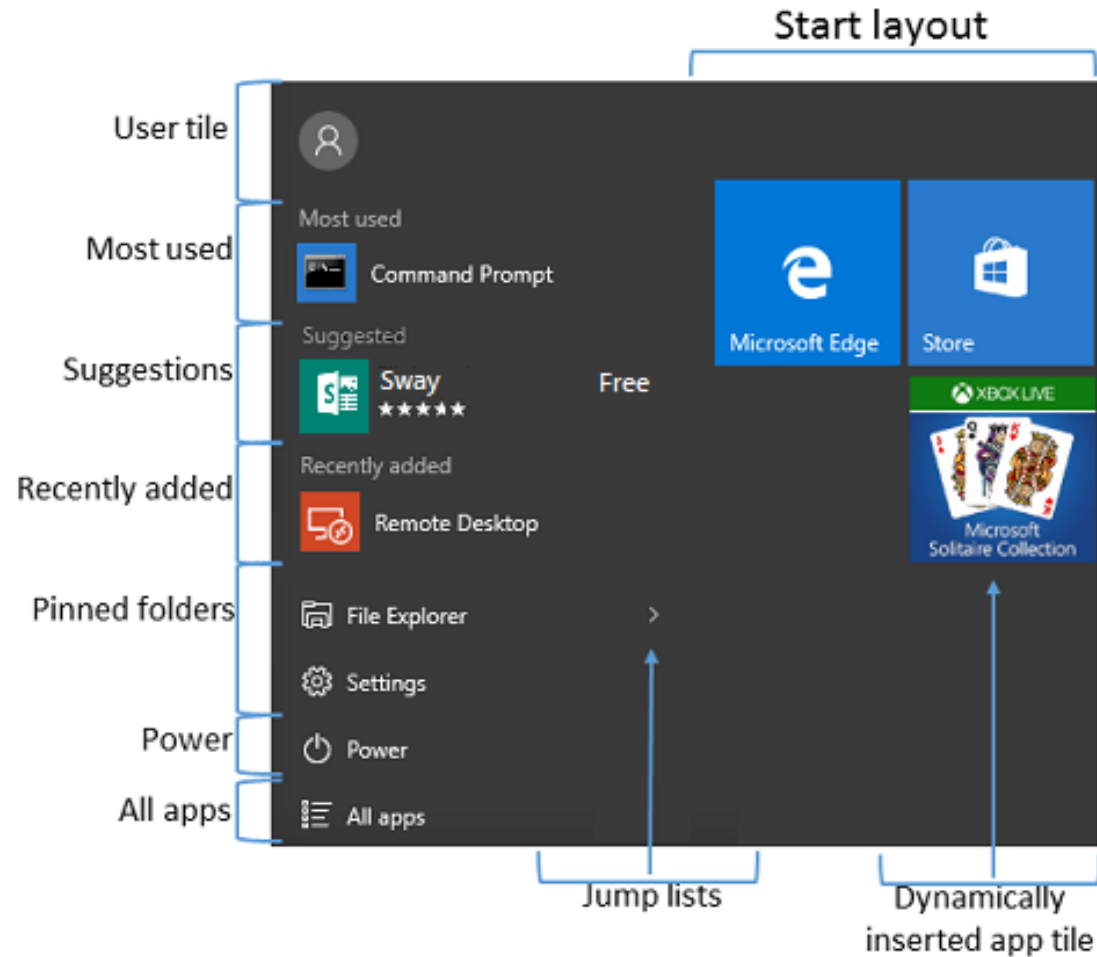
Start Menu

Windows 10



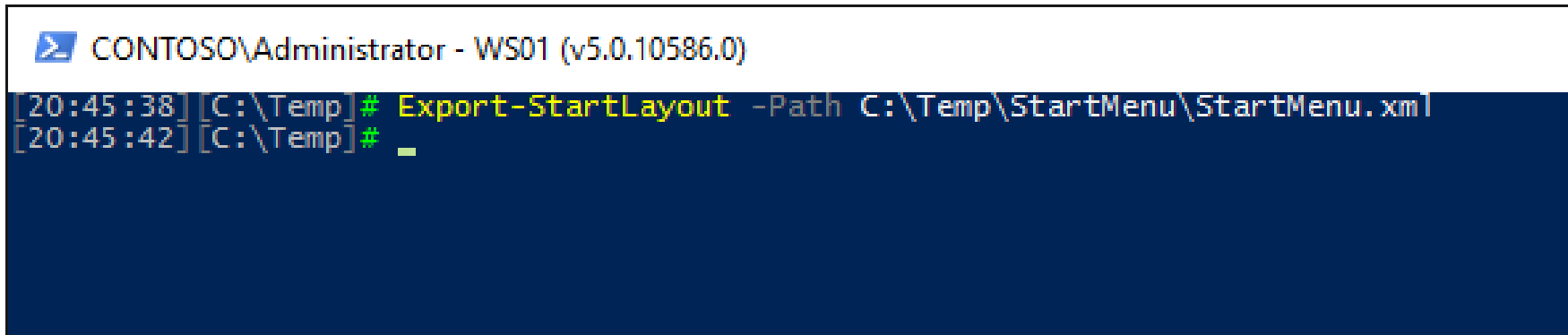
Start Layout Options

- Management Options:
 - Group Policy
 - MDM
- Requires same architecture (32-bit or 64-bit)
- Prevent users from customizing their Start Screen!



Steps to create a Custom Start Layout

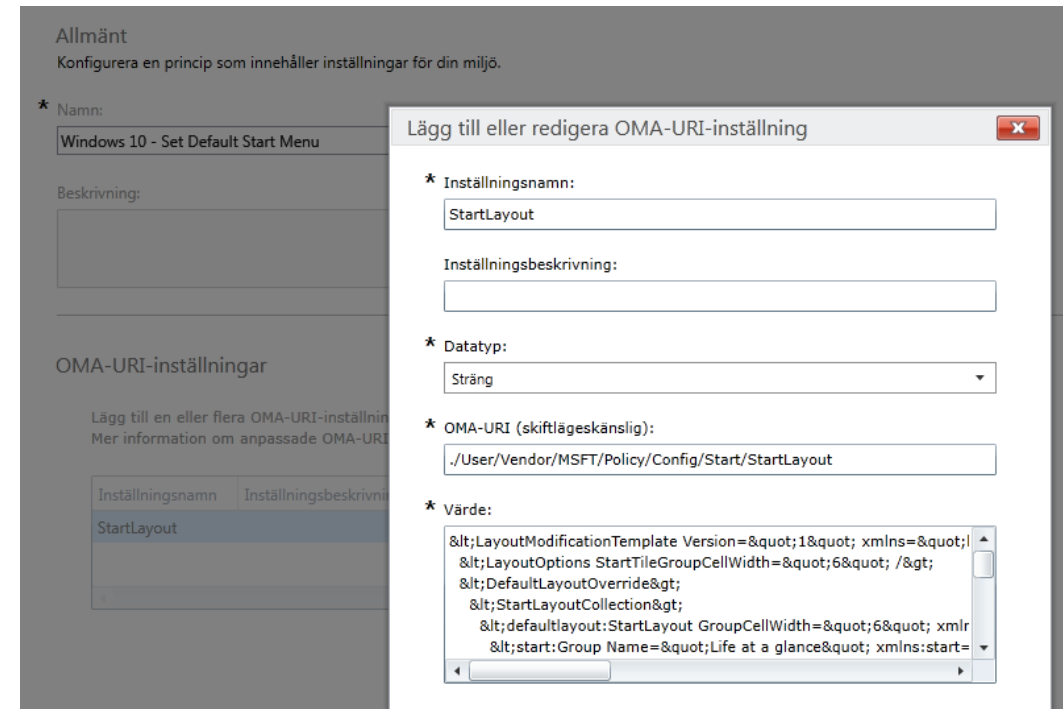
- Reference computer
 - Enterprise or Education SKU
- Customize the Start Layout
- `Export-StartLayout -Path <path>\<file name>.xml`



```
CONTOSO\Administrator - WS01 (v5.0.10586.0)
[20:45:38] [C:\Temp] # Export-StartLayout -Path C:\Temp\StartMenu\StartMenu.xml
[20:45:42] [C:\Temp] #
```

Deploy Start Layout using MDM (Intune)

- Replace markup characters with escape characters:
 - <http://www.freeformatter.com/xml-escape.html>
- Custom Configuration (Windows 10 Desktop and Mobile and later)
- OMA-URI Settings:
 - ./User/Vendor/MSFT/Policy/Config/Start/StartLayout
 - Data type: String
 - Value: <contents of the XML file>



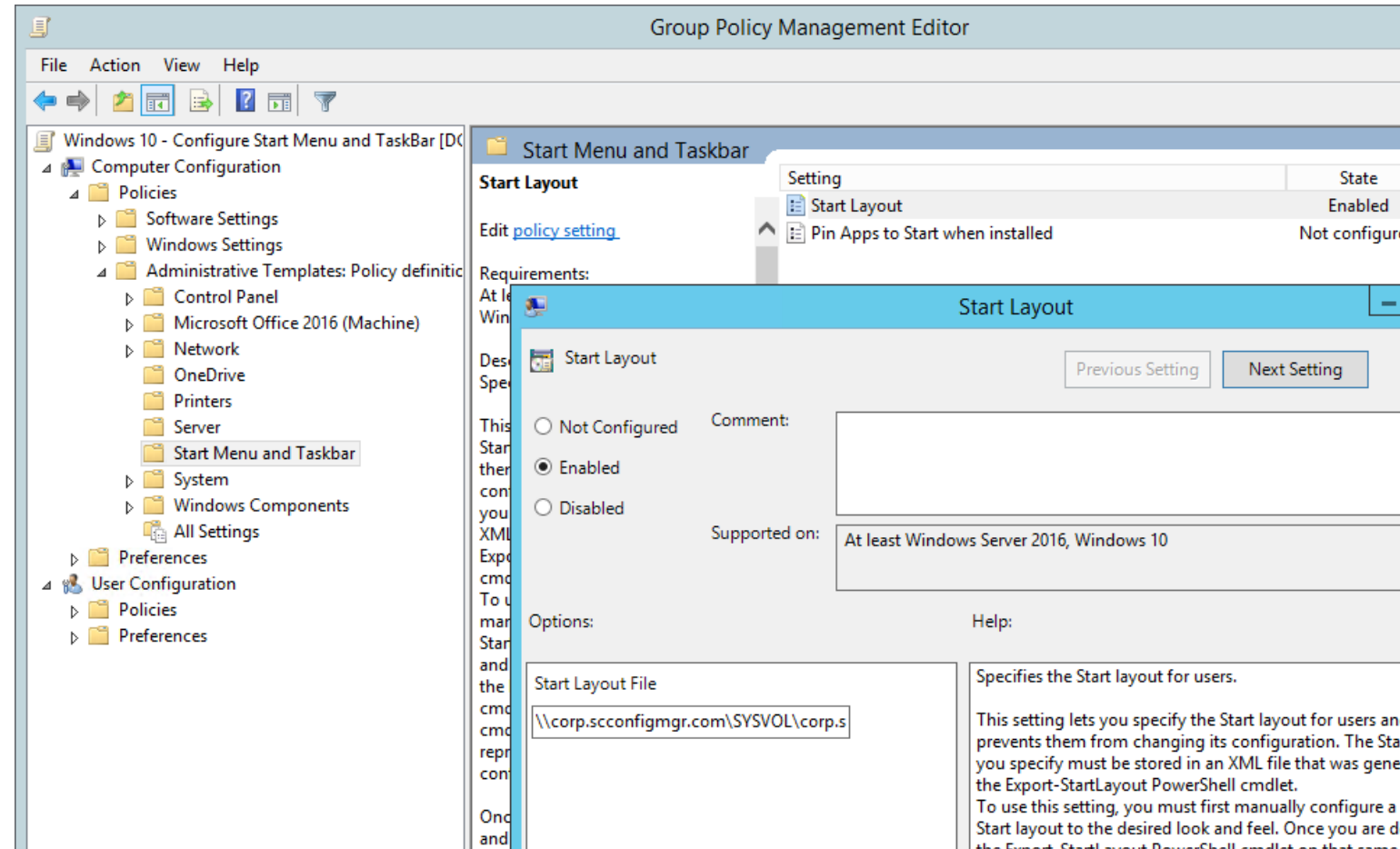
Deploy Start Layout using Group Policy

Same .xml file

- The Start Menu layout is locked

Useful for

- KIOSK computers
- Fixed workloads



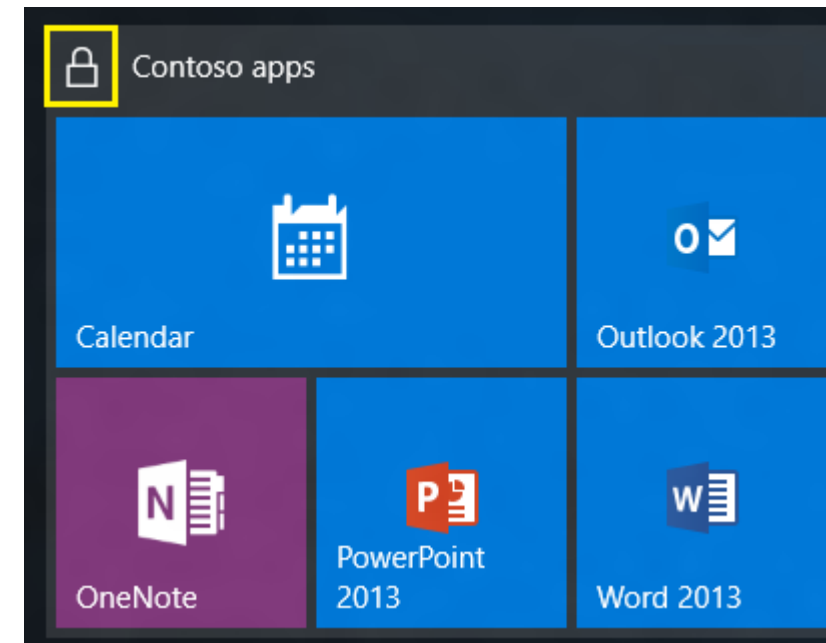
Configure a Partial Start layout

Add one or more customized tile groups

Allow the user to make changes to other parts of the Start layout

Conflicts / Duplicate Apps:

The duplicate app tile is removed from the existing (unlocked) group.



Add an IE link to the Start Menu

- The IE icon under Windows accessories are created when the user signs in.
- Cannot be used as it doesn't exist when startmenu is imported.
- Create an IE shortcut and then alter the .xml file.
- XML can be manually edited (not supported!?)

```
<?xml version="1.0"?>
<LayoutModificationTemplate xmlns="http://schemas.microsoft.com/Start/2014/LayoutModification" Version="1">
  - <DefaultLayoutOverride>
    - <StartLayoutCollection>
      - <defaultlayout:StartLayout xmlns:defaultlayout="http://schemas.microsoft.com/Start/2014/FullDefaultLayout" GroupCellWidth="6">
        - <start:Group xmlns:start="http://schemas.microsoft.com/Start/2014/StartLayout" Name="Ccmexec">
          <start:Tile AppUserModelID="Microsoft.MicrosoftEdge_8wekyb3d8bbwe!MicrosoftEdge" Row="0" Column="0" Size="2x2"/>
          <start:DesktopApplicationTile Row="0" Column="2" Size="2x2" DesktopApplicationLinkPath="%ALLUSERSPROFILE%\Microsoft\Windows\Start Menu\Programs\Accessories\Internet Explorer.lnk"/>
        </start:Group>
        - <start:Group xmlns:start="http://schemas.microsoft.com/Start/2014/StartLayout" Name="Office">
          <start:DesktopApplicationTile Row="0" Column="2" Size="2x2" DesktopApplicationID="{7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\Microsoft Office\Office15\EXCEL.EXE"/>
          <start:DesktopApplicationTile Row="0" Column="4" Size="2x2" DesktopApplicationID="{7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\Microsoft Office\Office15\lync.exe"/>
          <start:DesktopApplicationTile Row="0" Column="0" Size="2x2" DesktopApplicationID="Microsoft.Office.OUTLOOK.EXE.15"/>
          <start:DesktopApplicationTile Row="2" Column="2" Size="2x2" DesktopApplicationID="{7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\Microsoft Office\Office15\POWERPNT.EXE"/>
          <start:DesktopApplicationTile Row="2" Column="4" Size="2x2" DesktopApplicationID="{7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\Microsoft Office\Office15\WINWORD.EXE"/>
        </start:Group>
      </defaultlayout:StartLayout>
    </StartLayoutCollection>
  </DefaultLayoutOverride>
</LayoutModificationTemplate>
```



Demo

Start Menu

TaskBar Configuration

Windows 10



Modify the TaskBar

- Not supported in previous versions Windows 10 1507 and 1511
- Unsupported method:
 - C:\Users\%username%\appdata\roaming\Microsoft\Internet Explorer\Quick Launch
 - HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Taskband



Modify the TaskBar

- Same .xml file as for the Start Menu modification
- During OSD or using a Group Policy
- Must be combined with the customized Start Menu as it will overwrite it otherwise
- Possible to pin apps to the taskbar even after OSD using Group Policy
- Only possible to remove apps that was pinned using the .xml file
- Not possible to remove apps that was pinned by the user.





Demo

Modifying the TaskBar

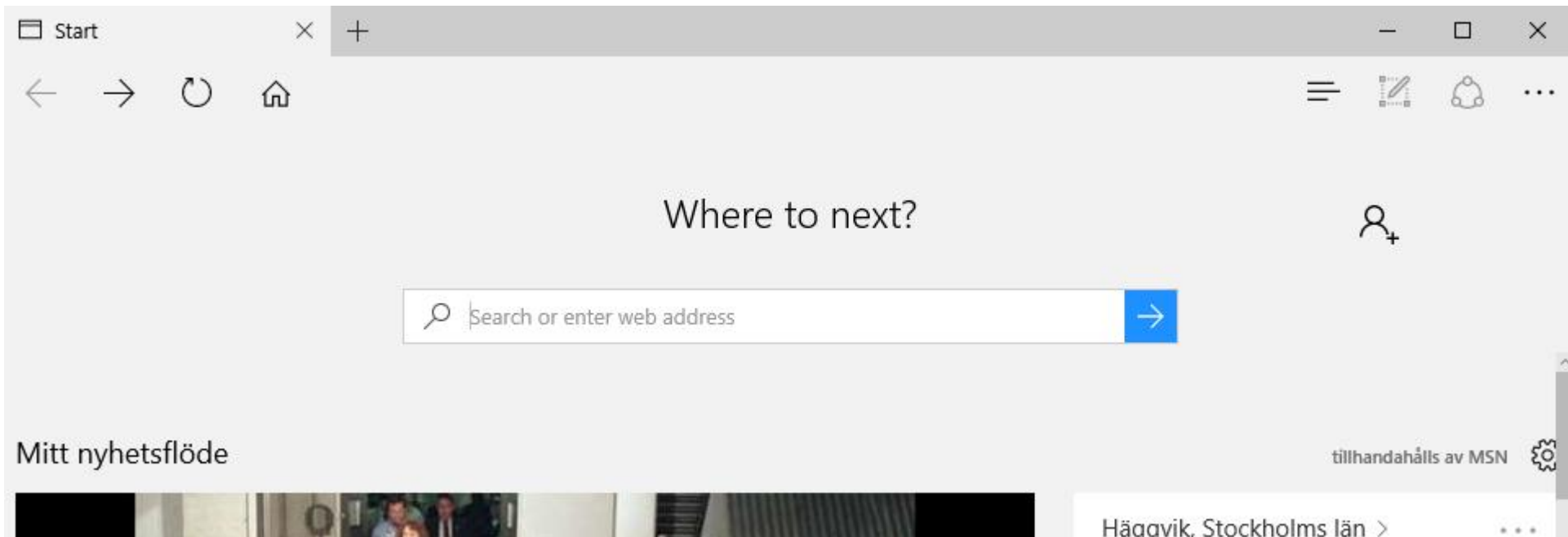
Microsoft Edge configuration

Windows 10



Microsoft Edge

- Enable Home button (with start page)
- Disable Welcome Screen
- PowerShell script during OSD



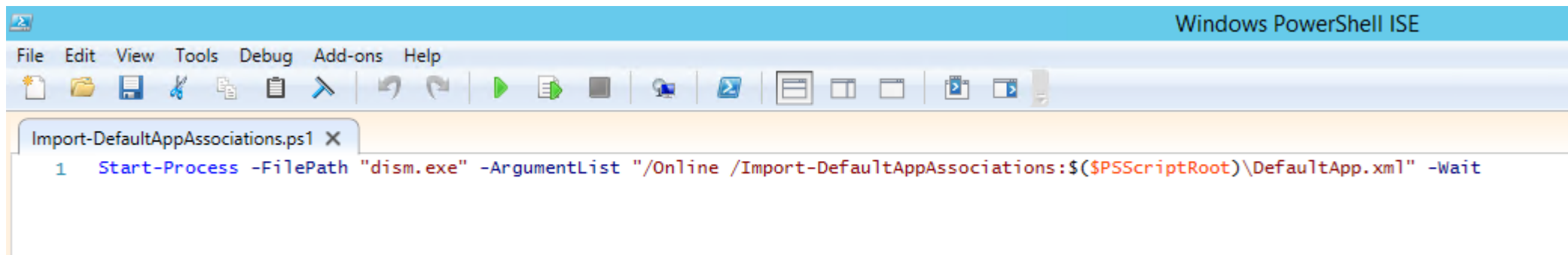
Default File Associations

Windows 10



Modify Default file associations

- Create default app associations on reference computer
- `Dism.exe /Online /Export-DefaultAppAssociations:C:\Temp\DefAppAssociations.xml`
- Applying default app associations
 - Group policy (Mandatory)
 - `Dism.exe` (User Changable)
- `Dism.exe /Online /Import-DefaultAppAssociations:C:\Temp\DefAppAssociations.xml`



The screenshot shows the Windows PowerShell ISE interface. The title bar reads "Windows PowerShell ISE". The menu bar includes "File", "Edit", "View", "Tools", "Debug", "Add-ons", and "Help". The toolbar contains various icons for file operations and execution. The main text area shows a PowerShell script file named "Import-DefaultAppAssociations.ps1" with the following command:

```
1 Start-Process -FilePath "dism.exe" -ArgumentList "/Online /Import-DefaultAppAssociations:$($PSScriptRoot)\DefaultApp.xml" -Wait
```



Demo

Default App Associations

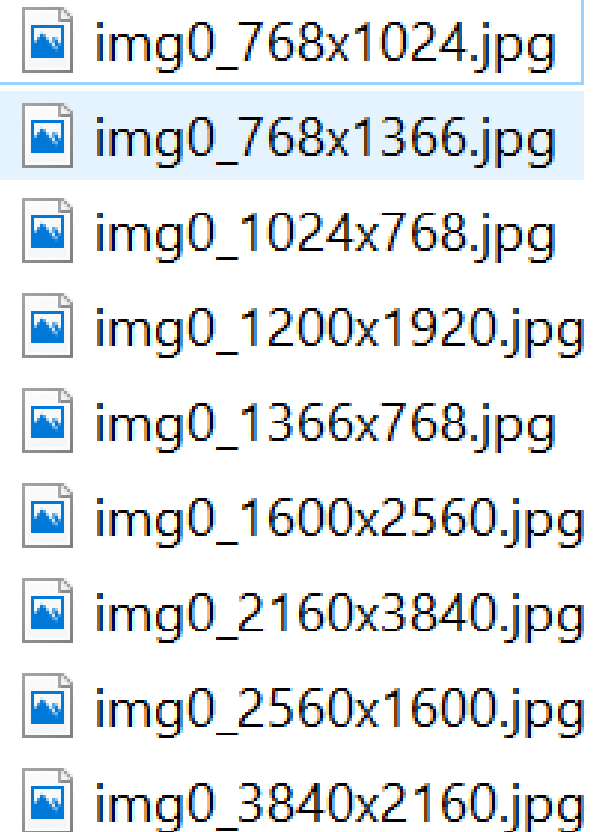
Branding

Windows 10



Set Desktop Wallpaper

- Default Location:
 - %Windir%\Web\4K\Wallpaper\Windows
- All other resolutions:
 - %Windir%\Web\Wallpaper\Windows\img0.jpg
- Files are owned by "TrustedInstaller"
- Use PowerShell to set wallpaper during OSD



Set the Lock Screen

- Script:
xcopy CustomLockScreen.jpg c:\IT\LockScreen\ /Y /S
reg import LockScreen\LockScreen.reg
reg import LockScreen\LockScreen.reg /reg:64
- LockScreen.reg:

Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Personalization]
"LockScreenImage"="C:\\IT\\LockScreen\\CustomLockScreen.jpg"
- Group Policy:
 - Computer Configuration\Administrative Templates\Control Panel\Personalization
 - Force a specific default lock screen image

User Pictures

- Scenario
 - Use the Company logo as User Picture
- Location:
 - "%SystemDrive%\ProgramData\Microsoft\User Account Pictures"
- Format:
 - 32 x 32 (PNG)
 - 40 x 40 (PNG)
 - 48 x 48 (PNG)
 - 192 x 192 (PNG)
 - 448 x 448 (BMP + PNG)



Built-In Applications

Windows 10



Disable Microsoft Consumer Experiences

- Since Windows 10 1511
- End-user apps installed from Windows Store
- Provisioned per user
- Built-In app removal scripts doesn't affect these apps
- Keep the apps from installing:
 - HKLM\SOFTWARE\Policies\Microsoft\Windows\CloudContent
"DisableWindowsConsumerFeatures"=dword:00000001

Remove Built-in Apps

- Remove Built-In apps during reference image creation
- White listing - Remove everything except:
 - Microsoft.WindowsCalculator
 - Microsoft.WindowsStore
 - Microsoft.WindowsSoundRecorder

<http://www.sconfigmgr.com/2016/03/01/remove-built-in-apps-when-creating-a-windows-10-reference-image/>

- Black listing - Remove only:
 - Microsoft.ContactSupport
 - Microsoft.WindowsFeedback
 - Microsoft.Edge

<http://ccmexec.com/2015/08/removing-built-in-apps-from-windows-10-using-powershell/>

Block Built-In Apps using AppLocker

- Not all Built-In apps can be removed:
 - Microsoft Edge
 - Windows Feedback
 - Contact Support
- Workaround:
 - AppLocker policy targeted for computers to block installation
 - Runs before the user logs in for the first time
 - The application is not installed

This app has been blocked by your system administrator.

Contact your system administrator for more info.

Close



Demo

Built-In Applications

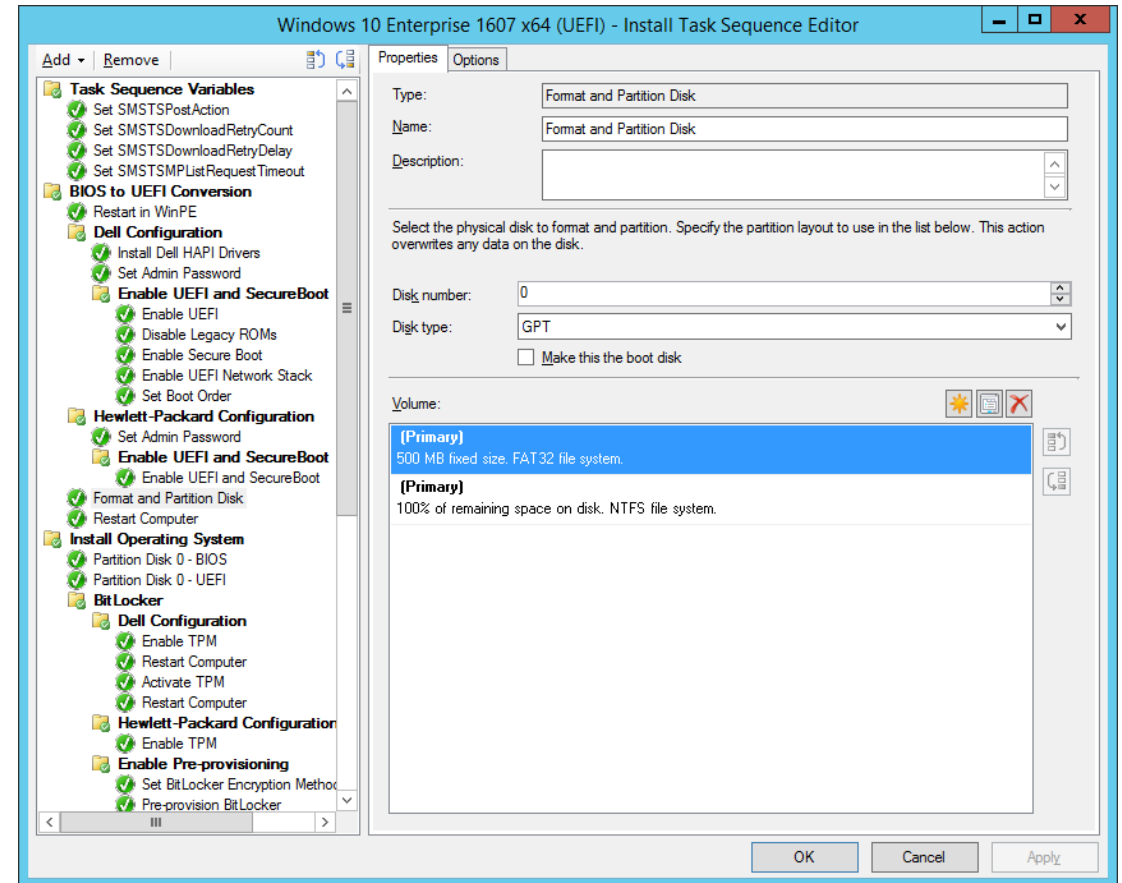
BIOS to UEFI Conversion

Windows 10



BIOS to UEFI Conversion

- Credential Guard and SecureBoot requires UEFI
- Support with ConfigMgr 1610
- TSUEFIDrive



BitLocker and TPM

Windows 10



TPM Owner Password changes

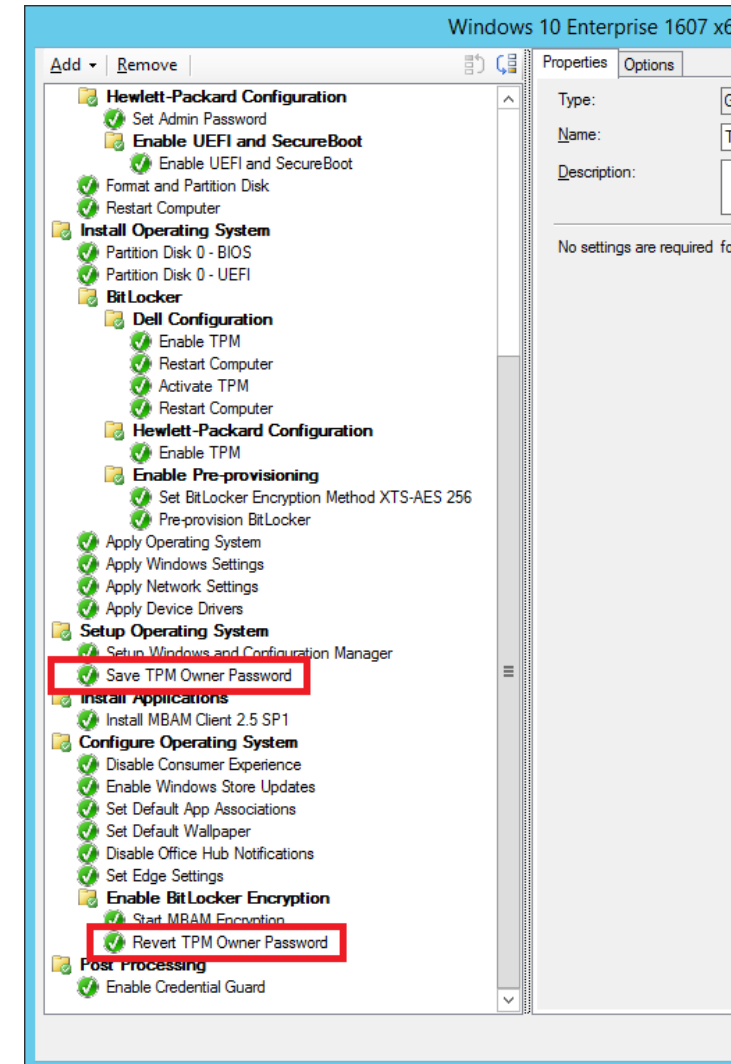
About the TPM owner password

Starting with Windows 10, version 1607, Windows will not retain the TPM owner password when provisioning the TPM. The password will be set to a random high entropy value and then discarded.

In order to retain the TPM owner password, you will need to set the registry key 'HKLM\Software\Policies\Microsoft\TPM' [REG_DWORD] 'OSManagedAuthLevel' to 4. The default value for this key is 2, and unless it is changed to 4 before the TPM is provisioned, the owner password will not be saved. Microsoft strongly recommends that you do not change the default value of this registry key in order to retain the owner password.

Only one owner password exists for each TPM. The TPM owner password allows the ability to enable, disable, or clear the TPM without having physical access to the computer, for example, by using the command-line tools remotely. The TPM owner password also allows manipulation of the TPM dictionary attack logic. Taking ownership of the TPM is performed by Windows as part of the provisioning process on each boot. Ownership can change when you share the password or clear your ownership of the TPM so someone else can initialize it.

Without the owner password you can still perform all the preceding actions by means of a physical presence confirmation from UEFI.

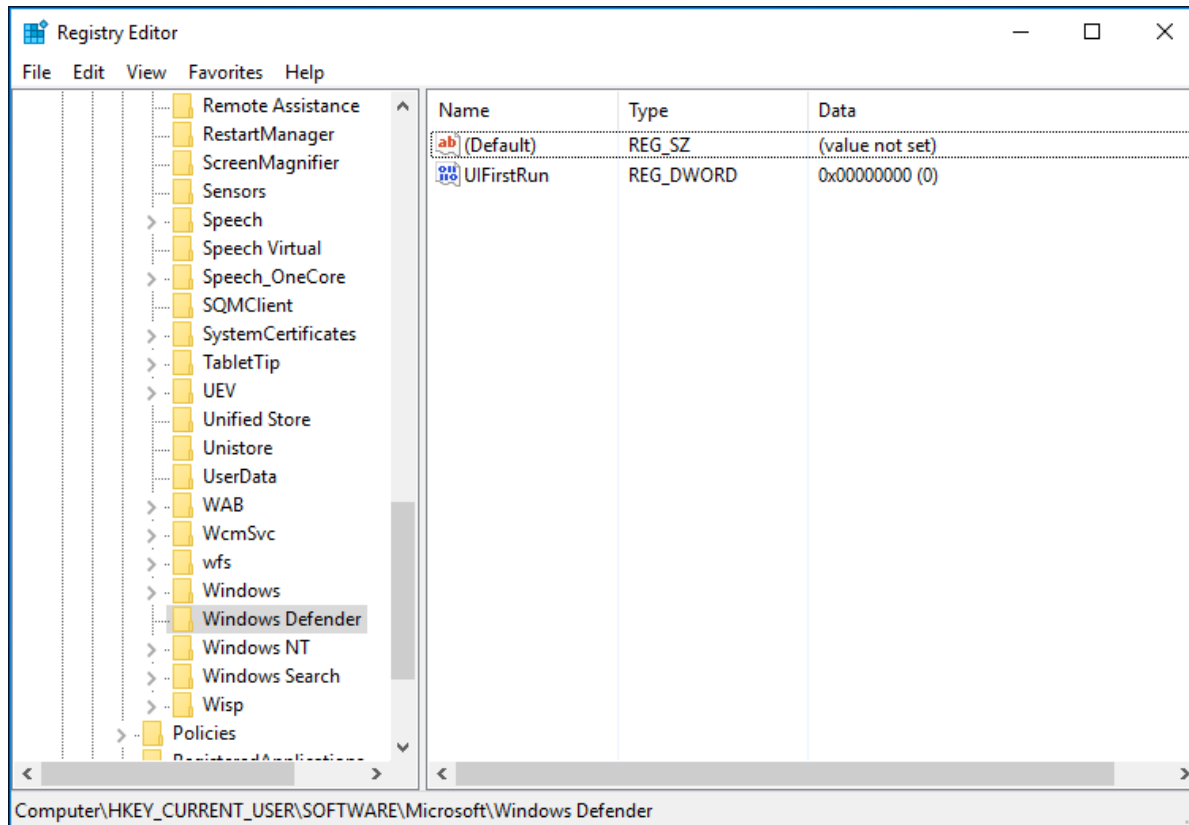


Lessons Learned

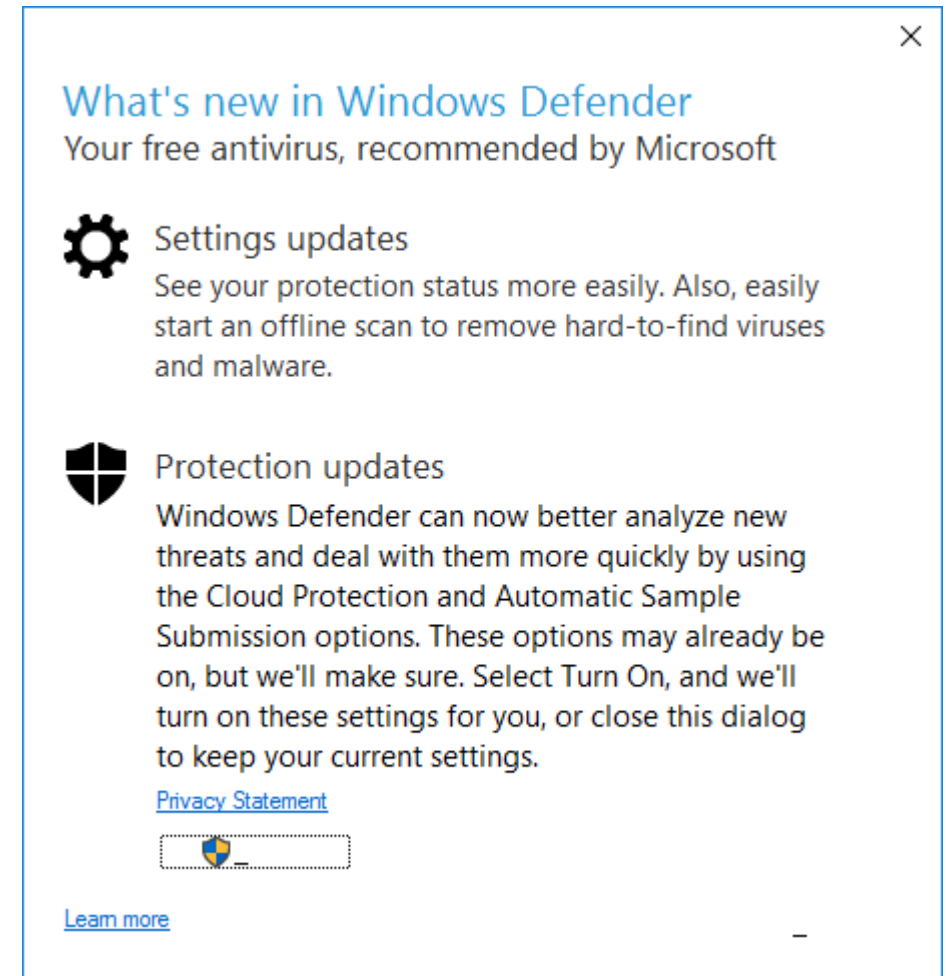
Windows 10



Windows Defender FirstRun Prompt



- HKU\Software\Microsoft\Windows Defender\UIFirstRun



Upgrading from 1507-1511-1607

Feature	Task Sequence	Software Update
Uninstall Built-In Apps	X	
Block apps with AppLocker	X	X
Customize Start Menu	X	X
Customize TaskBar	X	X
Default App Associations	(X)*	(X)*
OS Branding	X	
Internet Explorer on Start Menu	X	

Group Policies

Path	Setting
Computer Configuration\Administrative Templates\Windows Components\Data Collection and Preview Builds	Disable pre-release features or settings Allow Telemetry
Computer Configuration\Administrative Templates\Windows Components\MDM	Disable MDM enrollment
Computer Configuration\Policies\Administrative Templates\Control Panel\Personalization	Force a specific default lock screen image Do not display the lock screen (optional)
User -or Computer Configuration\Administrative Templates\Start Menu and Task Bar	Start Layout

<https://technet.microsoft.com/en-us/itpro/windows/manage/group-policies-for-enterprise-and-education-editions?f=255&MSPPError=-2147217396>

Conclusion

- Keep modifications of Windows 10 to a minimum
- Use defaults
- Invest in end-user training!
- Microsoft is learning
- Customers are learning



Stop "Curla" your users!



Known Issues

- Credential Guard will break many apps
 - (Credential Guard also does not allow unconstrained Kerberos delegation, NTLMv1, MS-CHAPv2, Digest, CredSSP, and Kerberos DES encryption.)
- TPM Hash Changes in 1607
- Kaby Lake
- UE-V in 1607 not fully functioning
- Driver Signing in 1607
- Inconsistency between builds