



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

Lumagate[®]

- Infrastructure
- Security
- Client and Enterprise Management

@stefanschorling <u>www.azuredojo.com</u> <u>stefan.schorling@lumagate.com</u> 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.scconfigmgr.com

nickolaj.andersen@lumagate.com

072-200 45 01

System Center User Group



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

silicon.

➤ 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"



Key Takeways

- 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



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>

A	Allmänt Konfigurera en princip so	om innehåller inställning	ıar för din miljö.				
*	Namn:						
Windows 10 - Set Default Start Menu			Lägg till eller redigera OMA-URI-inställning	x			
			* Inställningsnamn:				
Contraction of the second seco			StartLayout				
			Inställningsbeskrivning:				
			* Datatyp:				
(JMA-URI-Instalinii	ngar	Sträng 👻				
	Lägg till en eller fle Mer information on	era OMA-URI-inställnin	* OMA-URI (skiftlägeskänslig):				
Mer Mormation on anpassade OMA-UKI			./User/Vendor/MSFT/Policy/Config/Start/StartLayout				
		Inställningsbeskrivni	* Värde.				
	StartLayout		<layoutmodificationtemplate 6"="" version="1" xmlns="1 <LayoutOptions StartTileGroupCellWidth="></layoutmodificationtemplate> <defaultlayoutoverride> <startlayoutcollection> <defaultlayout:startlayout <defaultlayout:startlayout="" <start:group="" groupcellwidth="6" name="Life at a glance" xmlns:start="</td" xmlr=""><td></td></defaultlayout:startlayout></startlayoutcollection></defaultlayoutoverride>				

Deploy Start Layout using Group Policy

Same .xml file

• The Start Menu layout is locked

Useful for

- KIOSK computers
- Fixed workloads

J Group Policy Management Editor						
File Action View Help						
 Windows 10 - Configure Start Menu and TaskBar [D(▲ Computer Configuration ▲ Policies ▷ Conftware Settings ▷ Windows Settings 	Star Edit	Start Menu and Ta t Layout policy setting	askbar	Settin E Sta	ting Sta Start Layout Enab Pin Apps to Start when installed Not con	te oled figur
 Administrative Templates: Policy definitic Control Panel Microsoft Office 2016 (Machine) 	Requ At le Win	uirements:			Start Layout	_
 Network OneDrive Printers 	Desi Spei	📷 Start Layout			Previous Setting Next Setting]
 Server Start Menu and Taskbar System Windows Components 	This Star ther con	 Not Configured Enabled Disabled 	Commer	nt:		
 Il Settings ▶ I Preferences ✓ User Configuration 	XML Expo cmc		Support	ed on:	1: At least Windows Server 2016, Windows 10	
▷ Control Policies ▷ Control Preferences	Star	Options:			Help:	
	the cmc cmc repr con	Start Layout File	com\SYSV	OL\corp	Specifies the Start layout for users. This setting lets you specify the Start layout for use prevents them from changing its configuration. Th you specify must be stored in an XML file that was the Export-StartLayout PowerShell cmdlet. To use this setting, you must first manually configu	rs an ie Sta gene ure a
	and				Start layout to the desired look and feel. Once you the Export-Start avout DowerShell condict on that s	are d

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 exists 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 AppUserModeIID="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

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





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

🔊 img0_768x1024.jpg 🖾 img0_768x1366.jpg img0_1024x768.jpg 🔟 img0_1200x1920.jpg 🔊 img0_1366x768.jpg 🛋 img0_1600x2560.jpg 🖾 img0_2160x3840.jpg 🖾 img0_2560x1600.jpg 🖾 img0 3840x2160.jpg

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:0000001

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.scconfigmgr.com/2016/03/01/remove-built-in-apps-when-creating-a-windows-10reference-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.

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

Windows	10 Enterprise 1607 x64 (UEFI) - Install Task Sequence Editor	x
Add - Remove	Properties Options	
Add * Kemove Task Sequence Variables Set SMSTSPostAction Set SMSTSDownloadRetryDelay Set SMSTSDownloadRetryDelay Set SMSTSDownloadRetryDelay Set SMSTSDOwnloadRetryDelay Set SMSTSDOwnloadRetryDelay Set SMSTSDOwnloadRetryDelay Set SMSTSDOwnloadRetryDelay Set SMSTSDOwnloadRetryDelay Set SMSTSDOwnloadRetryDelay Set Admin Password Enable UEF1 Set Admin Password Enable UEF1 Set Secure Rods Enable Secure Rods Set Secure Rods Secure Rods Sec	Properties Options Type: Format and Partition Disk Name: Format and Partition Disk Description: ^ Select the physical disk to format and partition. Specify the partition layout to use in the list below. This action overwrites any data on the disk. Disk number: 0 Disk type: GPT V Make this the baset disk.	
Enable UEFI Network Stack Set Boot Order Hewlett-Packard Configuration Set Admin Password Enable UEFI and SecureBoot Format and Partition Disk Restart Computer Install Operating System Partition Disk 0 - BIOS Partition Disk 0 - UEFI	Make this the boot disk Volume: (Primary) 500 MB fixed size. FAT32 file system. (Primary) 100% of remaining space on disk. NTFS file system.	
BitLocker Dell Configuration Enable TPM Restart Computer Activate TPM Restart Computer Enable Pre-provisioning Set BitLocker Encyption Methor Pre-provision BitLocker </th <th></th> <th></th>		
	OK Cancel Apply	

BitLocker and TPM

Windows 10

TPM Owner Password changes

About the TPM owner password

🛃 Lumagate

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

Window Defender FirstRun Prompt

	Remote Assistance	Name	Туре	Data	
	RestartManager	(Default)	REG_SZ	(value not set)	
	ScreenMagnifier	100 UlFirstRun	REG_DWORD	0x0000000 (0)	
	Sensors		-		
> -	Speech				
	Speech Virtual				
> -	Speech_OneCore				
	SQMClient				
> -	SystemCertificates				
> -	TabletTip				
> -	UEV				
	Unified Store				
	Unistore				
	UserData				
> -	WAB				
> -	WcmSvc				
> -	wfs				
> -	Windows				
	Windows Defender				
> -	Windows NT				
> -	Windows Search				
> -	Wisp				
> - <mark> </mark> P	olicies				
· · · D	>	<			

HKU\Software\Microsoft\Windows Defender\UIFirstRun

What's new in Windows Defender Your free antivirus, recommended by Microsoft Settings updates See your protection status more easily. Also, easily start an offline scan to remove hard-to-find viruses and malware. Protection updates Windows Defender can now better analyze new threats and deal with them more quickly by using the Cloud Protection and Automatic Sample Submission options. These options may already be on, but we'll make sure. Select Turn On, and we'll turn on these settings for you, or close this dialog to keep your current settings. Privacy Statement Learn more

×

Lumagate[®]

Upgrading from 1507-1511-1607

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

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-andeducation-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