Windows 10 – Why?!

@iJackWilson

Introduction

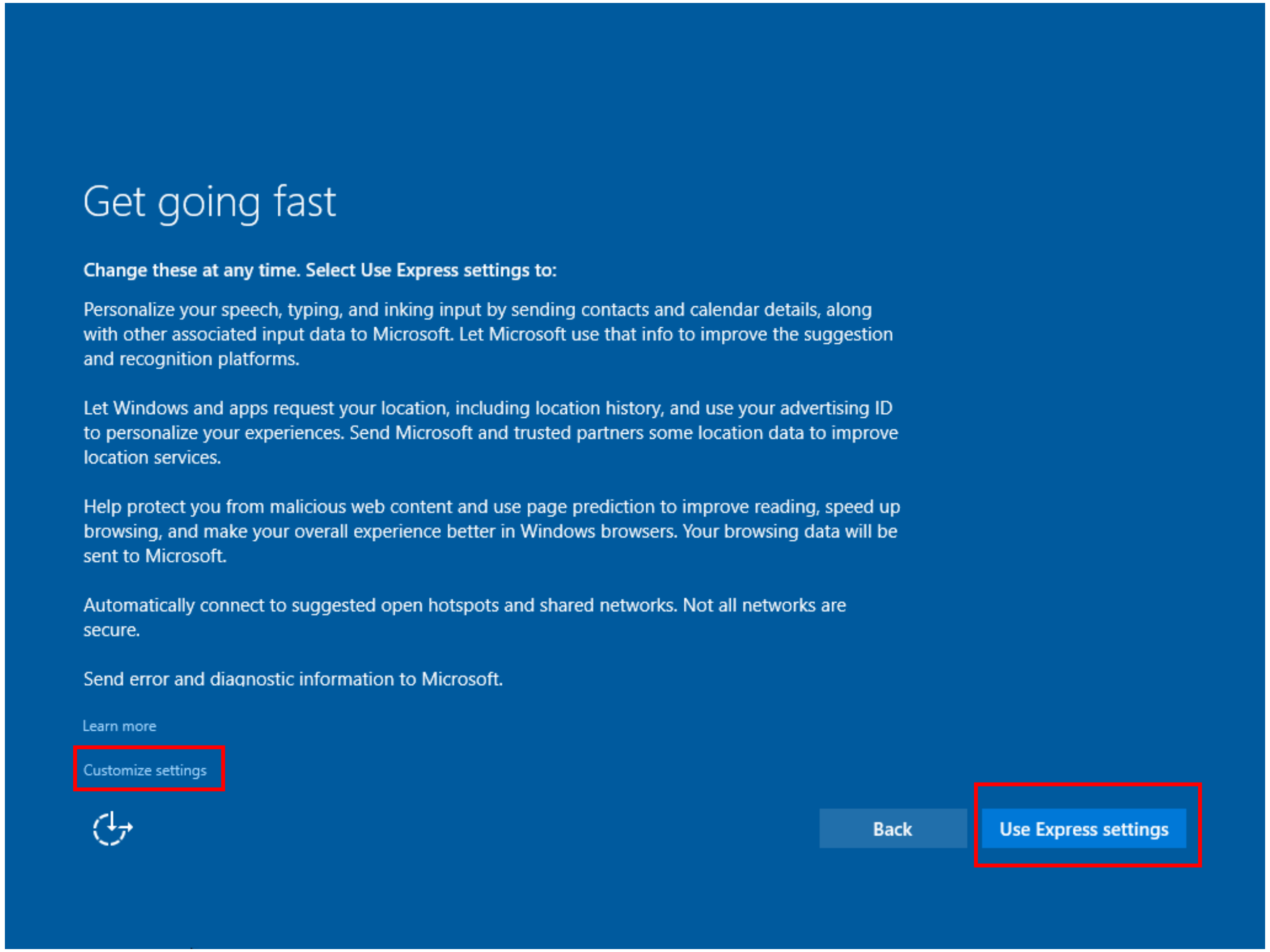
- Microsoft has an 88% market share
- Windows 10 is the “end-all OS”
  - Continuous updates
  - No successor
- Some great new features added
- Some features that make you think the devs were huffing glue
- Aggressive techniques to force upgrade

Express vs Custom

- Two virtual machines used for testing
- One with Express settings, one with Custom
- Everything left default with Express
- Everything turned off/disabled with Custom
- Comparison of how much was actually changed within settings

Express vs Custom

- I found the options to be quite hard to distinguish



Get going fast

Change these at any time. Select Use Express settings to:

Personalize your speech, typing, and inking input by sending contacts and calendar details, along with other associated input data to Microsoft. Let Microsoft use that info to improve the suggestion and recognition platforms.

Let Windows and apps request your location, including location history, and use your advertising ID to personalize your experiences. Send Microsoft and trusted partners some location data to improve location services.

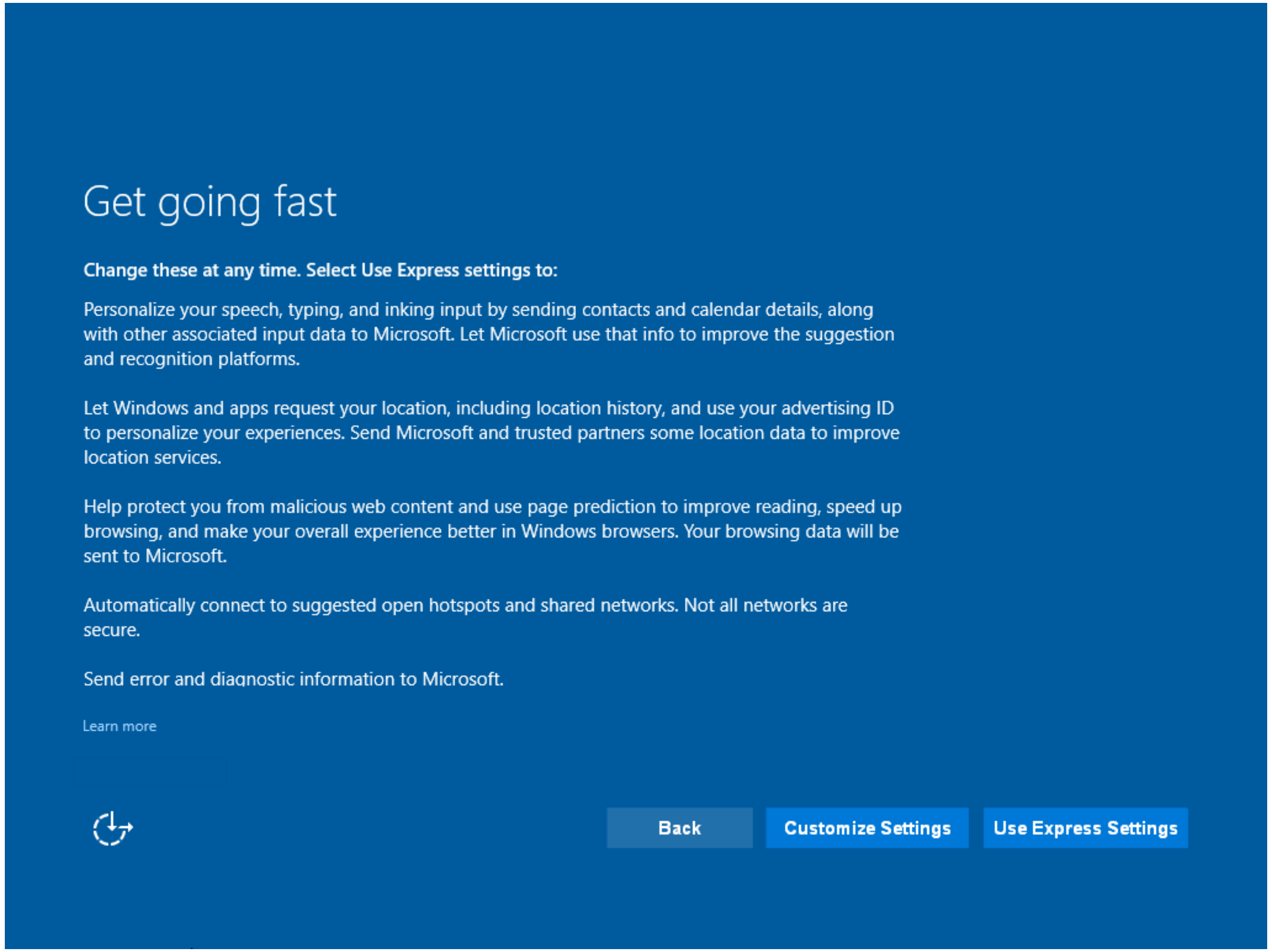
Help protect you from malicious web content and use page prediction to improve reading, speed up browsing, and make your overall experience better in Windows browsers. Your browsing data will be sent to Microsoft.

Automatically connect to suggested open hotspots and shared networks. Not all networks are secure.

Send error and diagnostic information to Microsoft.

Express vs Custom

- How it should be?



Get going fast

Change these at any time. Select Use Express settings to:

Personalize your speech, typing, and inking input by sending contacts and calendar details, along with other associated input data to Microsoft. Let Microsoft use that info to improve the suggestion and recognition platforms.

Let Windows and apps request your location, including location history, and use your advertising ID to personalize your experiences. Send Microsoft and trusted partners some location data to improve location services.

Help protect you from malicious web content and use page prediction to improve reading, speed up browsing, and make your overall experience better in Windows browsers. Your browsing data will be sent to Microsoft.

Automatically connect to suggested open hotspots and shared networks. Not all networks are secure.

Send error and diagnostic information to Microsoft.

Express

All enabled by default:

- Advertising ID
- Smartscreen filter
- Language list
- Location services
- Camera
- Microphone
- Speech, Inking and Typing
- Account info
- Contacts
- Calendar
- Messaging
- Radios
- Other devices
- Feedback and diagnostics
- Background apps

Express

All enabled by default:

- Advertising ID
- Smartscreen filter
- Language list
- **Location services**
- Camera
- Microphone
- Speech, Inking and Typing
- **Account info**
- Contacts
- Calendar
- Messaging
- **Radios**
- **Other devices**
- Feedback and diagnostics
- Background apps

Master settings were enabled
Sub-settings for individual apps were disabled

Express

All enabled by default:

- Advertising ID
- Smartscreen filter
- Language list
- Location services
- **Camera**
- **Microphone**
- Speech, Inking and Typing
- Account info

- Contacts
- **Calendar**
- **Messaging**
- Radios
- Other devices
- Feedback and diagnostics
- Background apps

Master settings were enabled
Sub-settings for individual apps were enabled

Express

All enabled by default:

- Advertising ID
- Smartscreen filter
- Language list
- Location services
- Camera
- Microphone
- Speech, Inking and Typing
- Account info
- **Contacts**
- Calendar
- Messaging
- Radios
- Other devices
- Feedback and diagnostics
- **Background apps**

No master settings – managed on a per-app basis

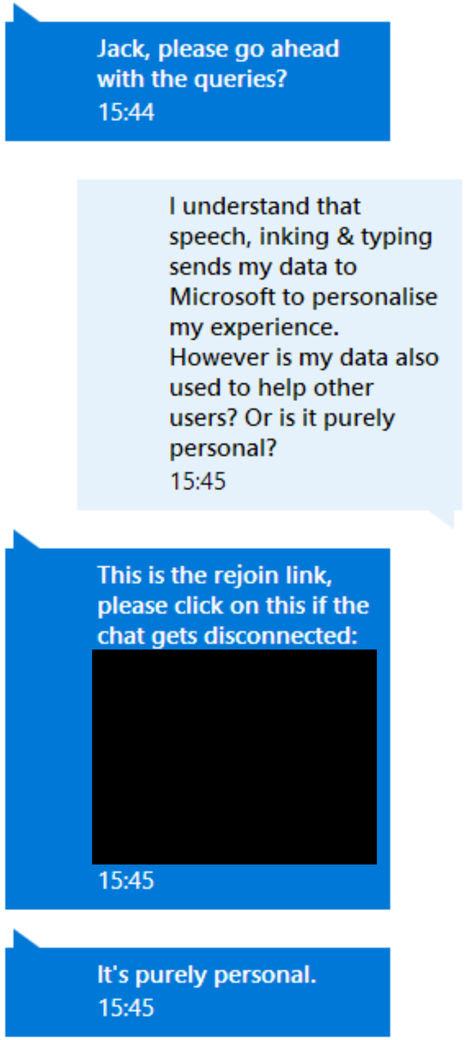
Express

Speech, Inking and Typing

This setting sends:

- Everything the user says
- Everything the user writes
- Everything the user types

To Microsoft for analysis if the word isn't detected correctly.



Jack, please go ahead with the queries?
15:44

I understand that speech, inking & typing sends my data to Microsoft to personalise my experience. However is my data also used to help other users? Or is it purely personal?
15:45

This is the rejoin link, please click on this if the chat gets disconnected:
[redacted]
15:45

It's purely personal.
15:45

Express

Feedback and Diagnostics

- Feedback was asked for by default. Could be changed to:
  - Always
  - Once a day
  - Once a week
  - Never
- Diagnostics and usage data could be changed to:
  - Full (default)
  - Enhanced
  - Basic

Custom

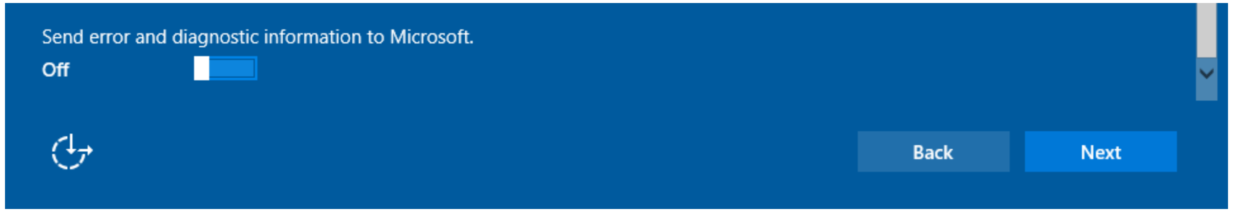
Remained enabled on custom setup

- Advertising ID
- Smartscreen filter
- Language list
- Location services
- Camera
- Microphone
- Speech, Inking and Typing
- **Account info**
- **Contacts**
- **Calendar**
- **Messaging**
- **Radios**
- **Other devices**
- Feedback and diagnostics
- Background apps

Custom

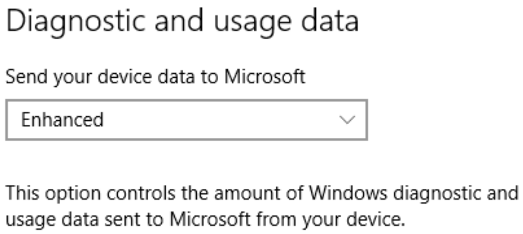
Feedback and Diagnostics

- Feedback remained enabled (no option to disable at setup)
- Diagnostics and usage data was turned off, yet only downgraded from “Full” to “Enhanced”
- Not only was it not disabled, it wasn’t even turned down to the lowest setting



Send error and diagnostic information to Microsoft.

Off



Diagnostic and usage data

Send your device data to Microsoft

Enhanced

This option controls the amount of Windows diagnostic and usage data sent to Microsoft from your device.

Traffic Analysis

- With Express Settings, lots of data was being sent to Microsoft
  - Everything typed was stored in temporary files and sent every 30 minutes to three different servers
  - Telemetry was sent every 5 minutes to eight servers
  - Searching for a movie would index every file on the PC and send that to five servers
  - If webcam was enabled ~35mb of data was sent to five servers
  - Everything said into the microphone was sent to 10 servers, even with Cortana disabled
- Data being used for different purposes was often sent to the same servers, meaning data was only sent to 18 unique servers

Wifi-Sense

- Enabled by default
- Automatically signed user into open wifi networks
- If the user had a Outlook, Skype or Facebook contact who had signed into the network previously, it would sign in unauthenticated, so long as the contact also had Wifi-Sense enabled
- Restricted access – No access to other PC's/devices on network
- Still vulnerable to man-in-the-middle and metasploit attacks
- This feature was removed in the Anniversary Update
    - Lack of use, not worth time to develop

P2P Updates

- Enabled by default
- Added user to a P2P network
- Send and receive Windows updates from other users on home network or across the world
- Reduce server load when update is released
- Not ideal for users with limited bandwidth/data caps

Automatic Updates

- Windows 10 would automatically install updates - whether a small bug or a security patch
- Would automatically update when computer is typically not in use (i.e. at 3am)
- Could also be notified when updates were available
  - Install at that moment
  - Or wait 10 minutes to finish and save work

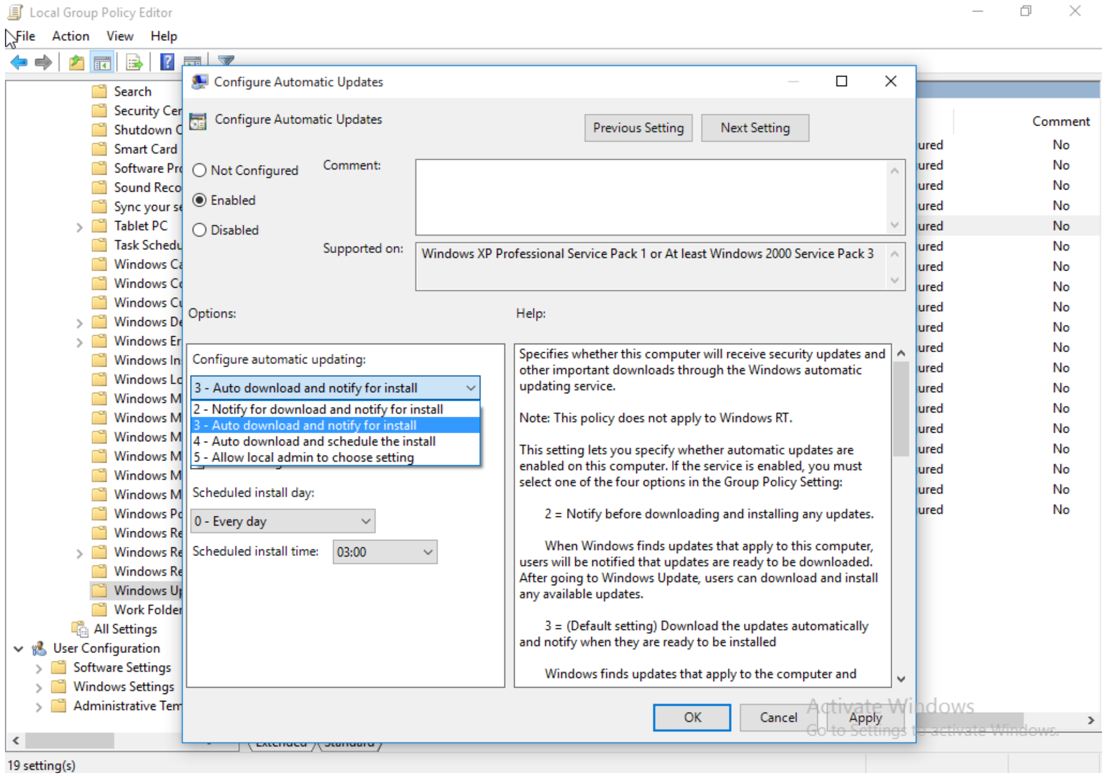
Automatic Updates

- It’s common to leave a computer unattended for purposes such as:
  - Rendering
  - Brute-force attacks
  - Running errands
- Windows restarting without permission can (and did in my case) lead to data loss
- Automatic updates aren’t ideal in a production environment
  - Testing may be required for compatibility before being deployed
- Or when in a CS:GO competitive match…

Automatic Updates

Automatic Updates

- Automatic updates could be disabled (kind of)
  - Required a group-policy edit (which required Windows 10 Pro)
- Called “Notify for download, notify for install”
  - Couldn’t do anything on your computer until you at least opened Windows Update



Configure Automatic Updates

Configure Automatic Updates

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: Windows XP Professional Service Pack 1 or At least Windows 2000 Service Pack 3

Options:

Configure automatic updating:

3 - Auto download and notify for install

2 - Notify for download and notify for install
3 - Auto download and notify for install
4 - Auto download and schedule the install
5 - Allow local admin to choose setting

Scheduled install day: 0 - Every day

Scheduled install time: 03:00

Help:

Specifies whether this computer will receive security updates and other important downloads through the Windows automatic updating service.

Note: This policy does not apply to Windows RT.

This setting lets you specify whether automatic updates are enabled on this computer. If the service is enabled, you must select one of the four options in the Group Policy Setting:

2 = Notify before downloading and installing any updates.

When Windows finds updates that apply to this computer, users will be notified that updates are ready to be downloaded. After going to Windows Update, users can download and install any available updates.

3 = (Default setting) Download the updates automatically and notify when they are ready to be installed

Windows finds updates that apply to the computer and

ured	No
ured	No
ured	No
ured	No
ured	No
ured	No
ured	No
ured	No
ured	No
ured	No
ured	No
ured	No
ured	No
ured	No
ured	No
ured	No
ured	No
ured	No
ured	No

What has changed?

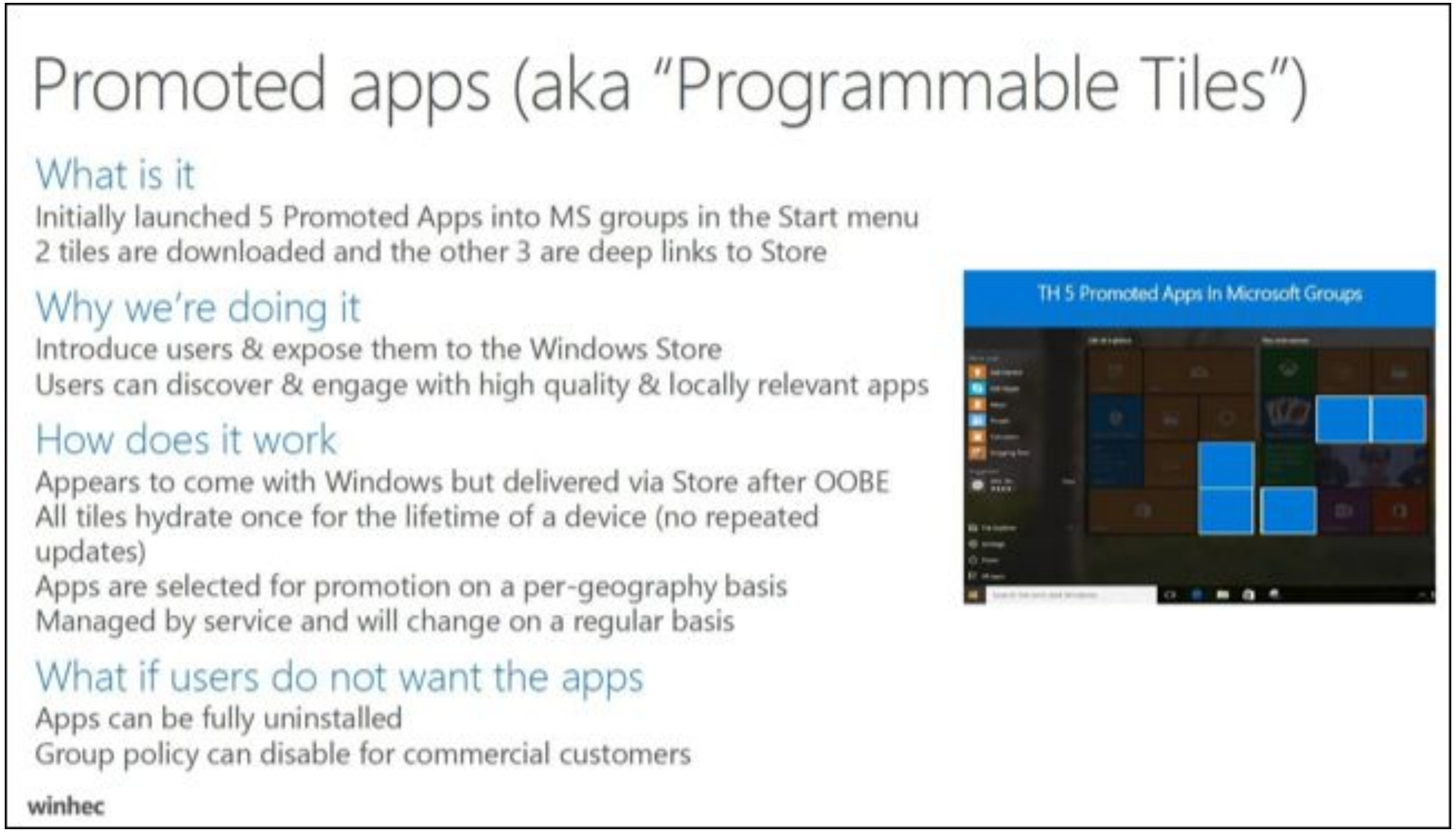
The paper was written before the 1-year "Anniversary Update"

- Cortana is even harder to disable
  - Requires registry edit or group policy setting
- Some Win 10 Pro group policies now require Enterprise edition
- Wifi credential sharing is gone
- Support for bash
- "Refresh Windows"
  - Remove OEM bloatware
- Easier to manage updates
  - Set "Active hours" and Windows won't restart during those times
- QR code on BSOD

http://goo.gl/1TgVd7

What has changed?

- More advertising!



Promoted apps (aka "Programmable Tiles")

What is it

Initially launched 5 Promoted Apps into MS groups in the Start menu
2 tiles are downloaded and the other 3 are deep links to Store

Why we're doing it

Introduce users & expose them to the Windows Store
Users can discover & engage with high quality & locally relevant apps

How does it work

Appears to come with Windows but delivered via Store after OOBE
All tiles hydrate once for the lifetime of a device (no repeated updates)
Apps are selected for promotion on a per-geography basis
Managed by service and will change on a regular basis

What if users do not want the apps

Apps can be fully uninstalled
Group policy can disable for commercial customers

TH 5 Promoted Apps In Microsoft Groups

winhec

Summary

- Don’t let this put you off upgrading to Windows 10
  - Still lots of great features added
- It’s important to understand what Windows is doing and know how to manage it
- OS X isn’t better, you shouldn’t “Just buy a Mac”
  - Before Kyle/Mikey suggest it

Future Work

- More-in depth look at OS X
- Comparison of a few Linux distro’s
- Look at Windows Defender Advanced Threat Protection Service
  - Added in Anniversary Update (Enterprise Only)

Questions?

Full Paper/References/OS X Comparison: jackw.info/blog