Operating System Telemetry

Configuring privacy protection in Windows 10

Klaus Möller
WP8-T1

Webinar, 3rd of August 2020

Public

www.geant.org

Windows 10

- Change: “Windows as a Service”
  - Feature Upgrades: Rolling updates 2x/year (spring, fall)
  - No “next” Windows version
  - No more Service Packs
- Primary business: sale of services
  - Office 365, OneDrive, games, apps, etc.
  - Still sale of software
- Additionally: Advertising
  - Like Apple, Google, etc.
- Fewer options to configure telemetry/tracking on cheaper editions
  - Enterprise – Edu – Pro – Home (least)
- Not “privacy by design/default”

Why is this important?

- Concerns with regards to Privacy Protection
  - Tracking of users → Privacy
  - Telemetry → sensitive/personal information transferred to MS (servers outside organisation)
  - No transparency (What is tracked, why, where is it transferred to …)
  - In professional use: Organisation is data controller and therefore legally responsible for transmission)
- Guiding question
  - Can Windows 10 be used in public administrations?
  - TLDR: Yes, but tracking/telemetry has to be turned off
  - Recent EU court rulings have voided Privacy Shield → probably not anymore
- Scope
  - Office/Administration PCs/Laptops
  - Windows 10 Enterprise 1909

Problem Fields, Agenda

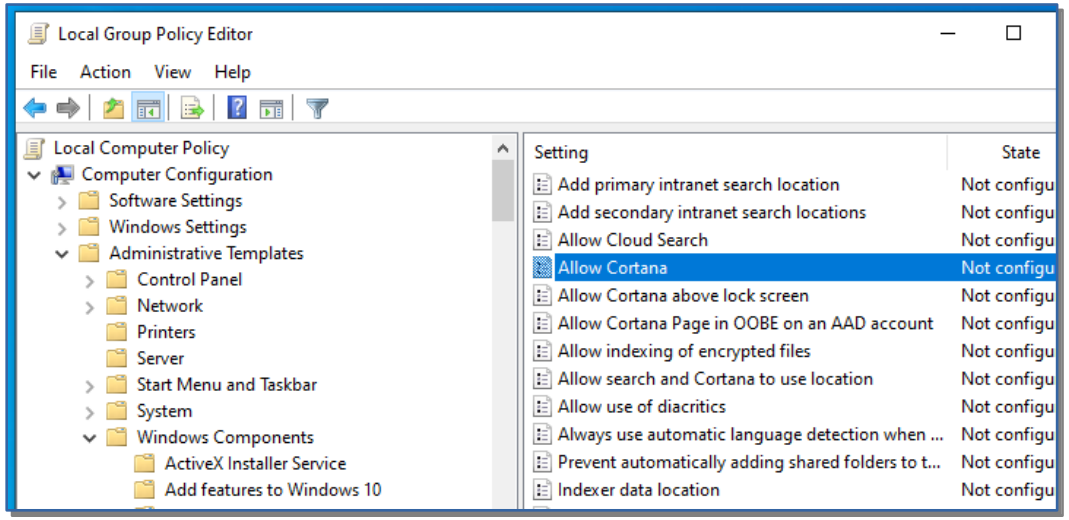
- Cortana
- Taskbar web search
- Advertising ID
- Updates
- Microsoft Account
- Telemetry
- Former issues:
  - WLAN password sharing function (WiFi-Sense)
  - Disabled for encrypted WLANs since 1607

Cortana: Features – Issues – Recommendation

- Virtual Assistant
  - Voice interface to search, notes, etc.
    - Like Google, Siri, Alexa, …
  - Also for Android (needs MS account to sync)
- Problems
  - Voice samples send to MS for analysis
  - May leak personal/sensitive/confidential information
  - Can interact to voice commands even when screen/system is locked, tracks all the time
- Recommendation: Deactivate

Cortana: Deactivation

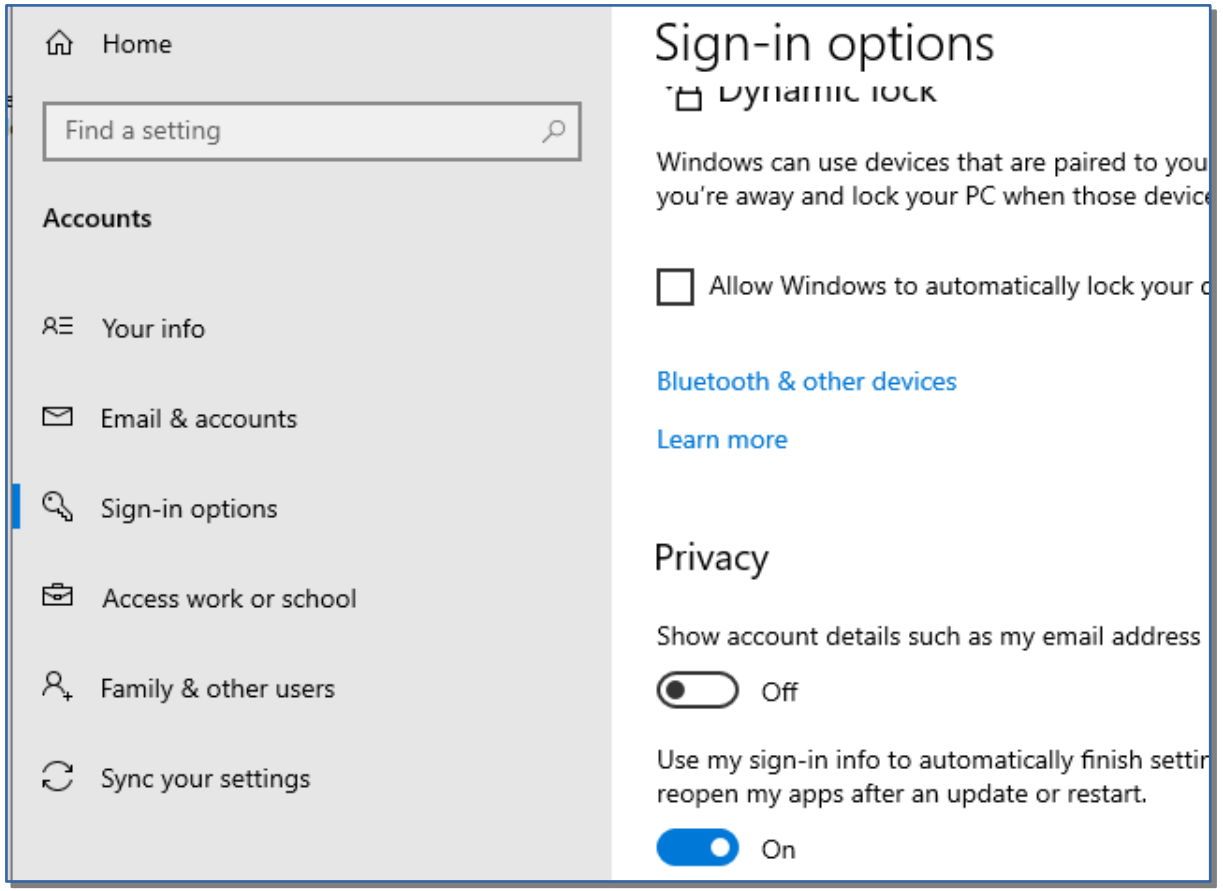
- Group Policy (Enterprise, Edu, Pro):
  - Computer Configuration→Administrative Templates→Windows Components→Search →Allow Cortana
    - Set to „Disabled“



- Registry edit:
  - Key: `HKLM\Software\Policies\Microsoft\Windows\Windows Search`
  - Value: `AllowCortana = 0` (DWORD)
  - Per user key: `HKCU\SOFTWARE\Policies\Microsoft\Windows\Windows Search`

Cortana: Email address control

- Don‘t show email address on lock screen when using MS account



Taskbar web search: Features – Issues – Recommendation

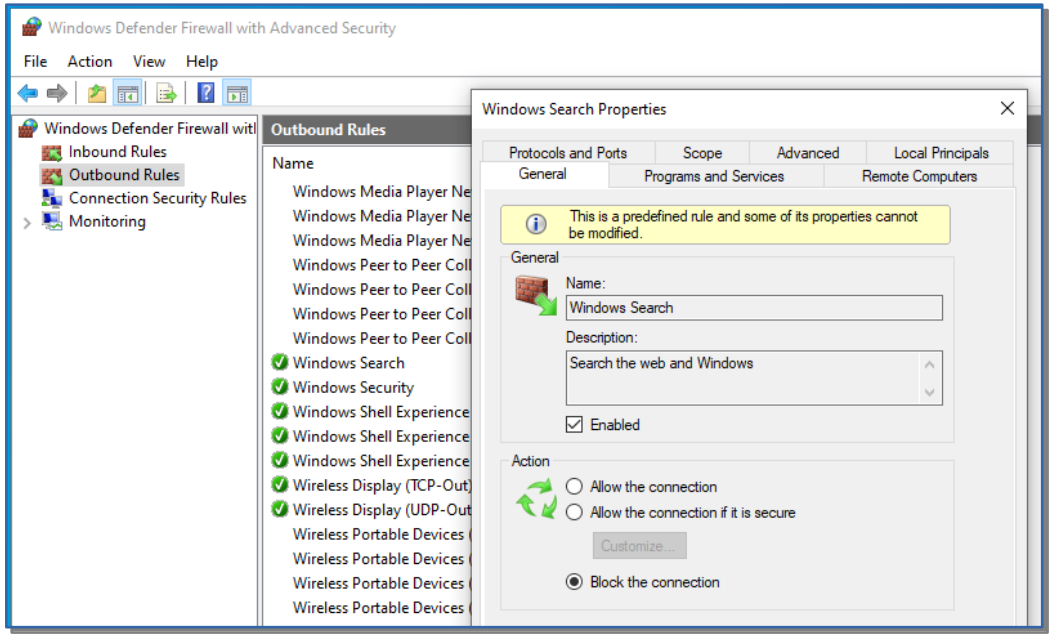
- Web search
  - Hitting the Windows + S key or when typing in taskbar search window
  - Incremental web search as in browsers
  - I.e. sends search term while you type to the search engine which offers suggestions
  - Here: Edge & Bing
- Problem
  - Advertising/profiling through search engine
  - Hardcoded - can‘t choose other search engines or browsers
- Recommendation: Deactivate
  - Registry (recommended)
  - Or blocking in the local firewall

Taskbar web search: Deactivation (1)

- Registry keys change with Windows 10 Feature Upgrades
- Versions 1803 – 1909:
  - Key: `HKCU\Software\Microsoft\CurrentVersion\Search`
  - Values:
    - `BingEnabled = 0` (DWORD)
    - `CortanaConsent = 0` (DWORD)
- Versions 2004 – ??:
  - Key: `HKLM\Software\Policies\Microsoft\Windows\Windows Search`
  - Value: `ConnectedSearchUseWeb = 0` (DWORD)
  - Enterprise & Edu only

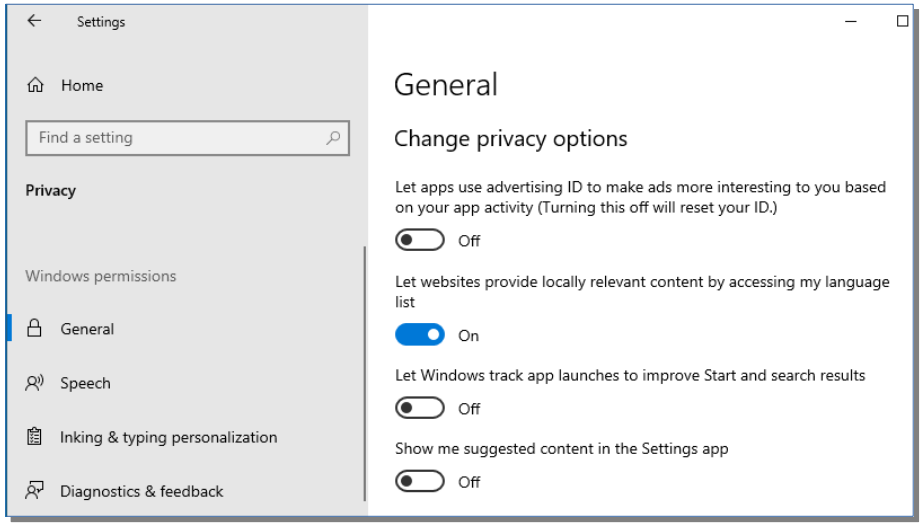
Taskbar web search: Deactivation (2)

- Through personal firewall
  - Powershell or cmd.exe (as admin):
    - `netsh advfirewall firewall add rule name="Block Cortana Outbound Traffic“ dir=out action=block program=“%windir%\systemapps\Microsoft.Windows.Cortana_cw5n1h2txyewy\SearchUI.exe" enable=yes profile=any`
- GUI:
  - Settings →
  - „Windows Defender with
  - Advanced Security“

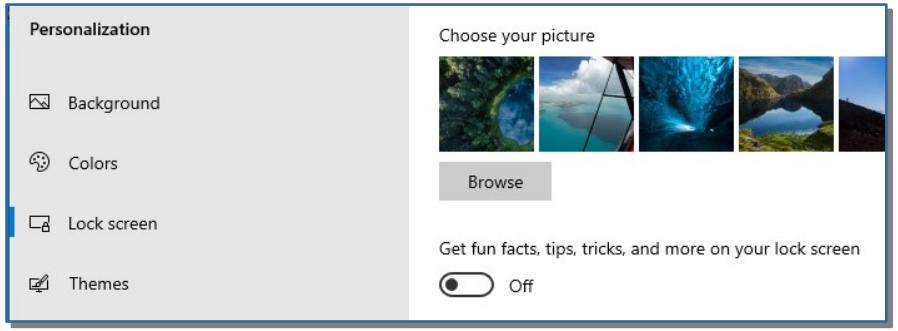


Advertising (ID): Issues & Recommendations

- Allows cross device tracking
- Deactivate
- Keep only language access



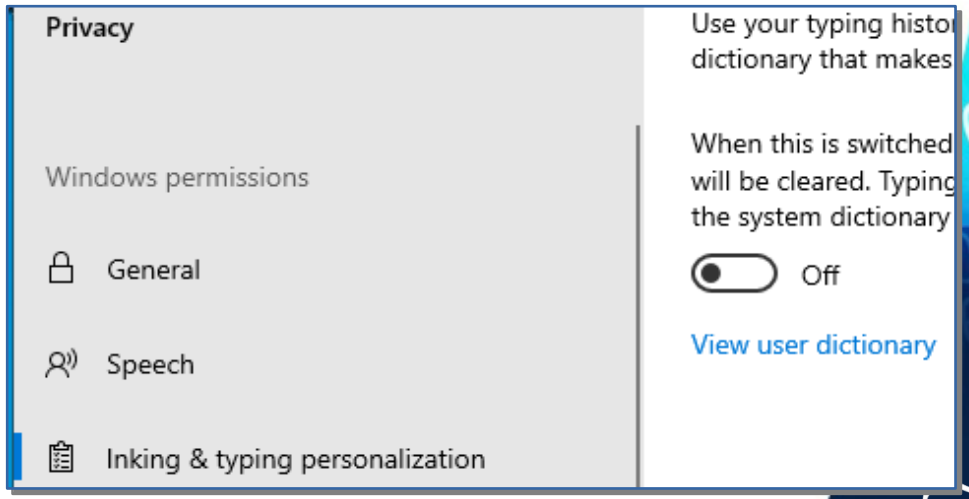
- Also turn off additional information on the lock screen



Advertising: Speech & Inking

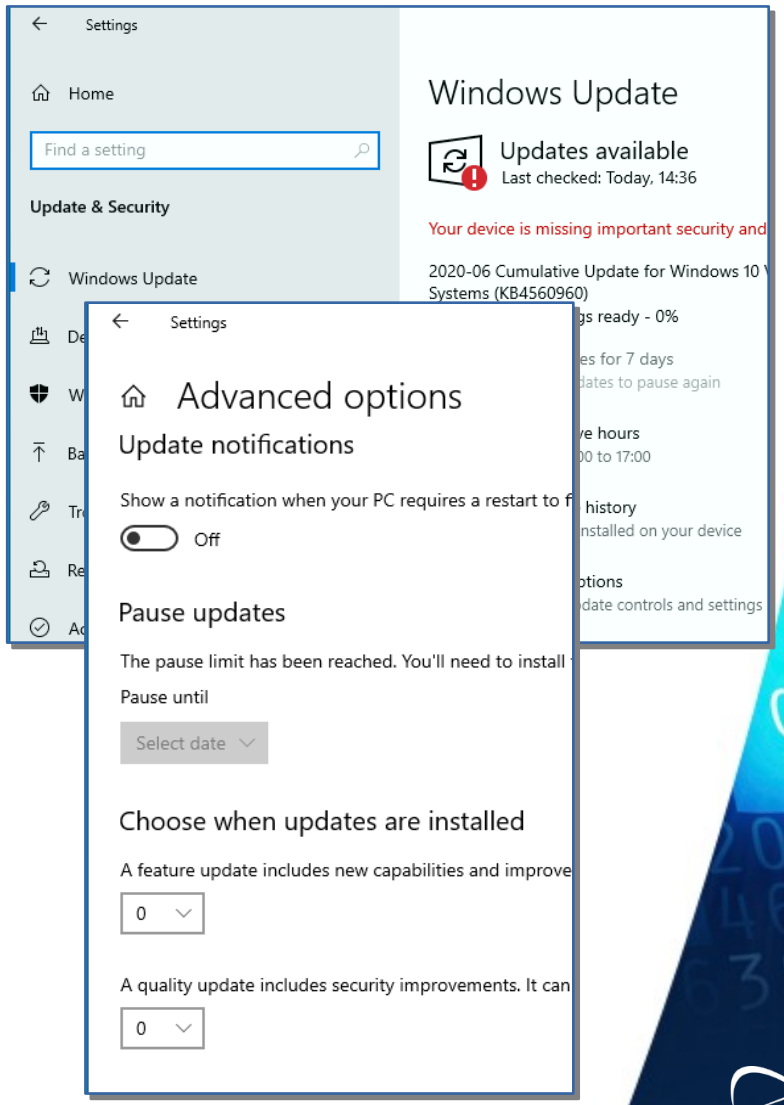
- Online Speech recognition
  - Uploads voice samples to MS cloud
    - Apps only: Cortana & dictation
    - Not the Windows voice recogniation
  - Some users may depend on it!
    - Disabilities?

- Inking & typing
  - Uploads handwriting samples to MS cloud
  - If turned off, local handwriting dict still works
  - Not needed, especially if no supporting hardware present



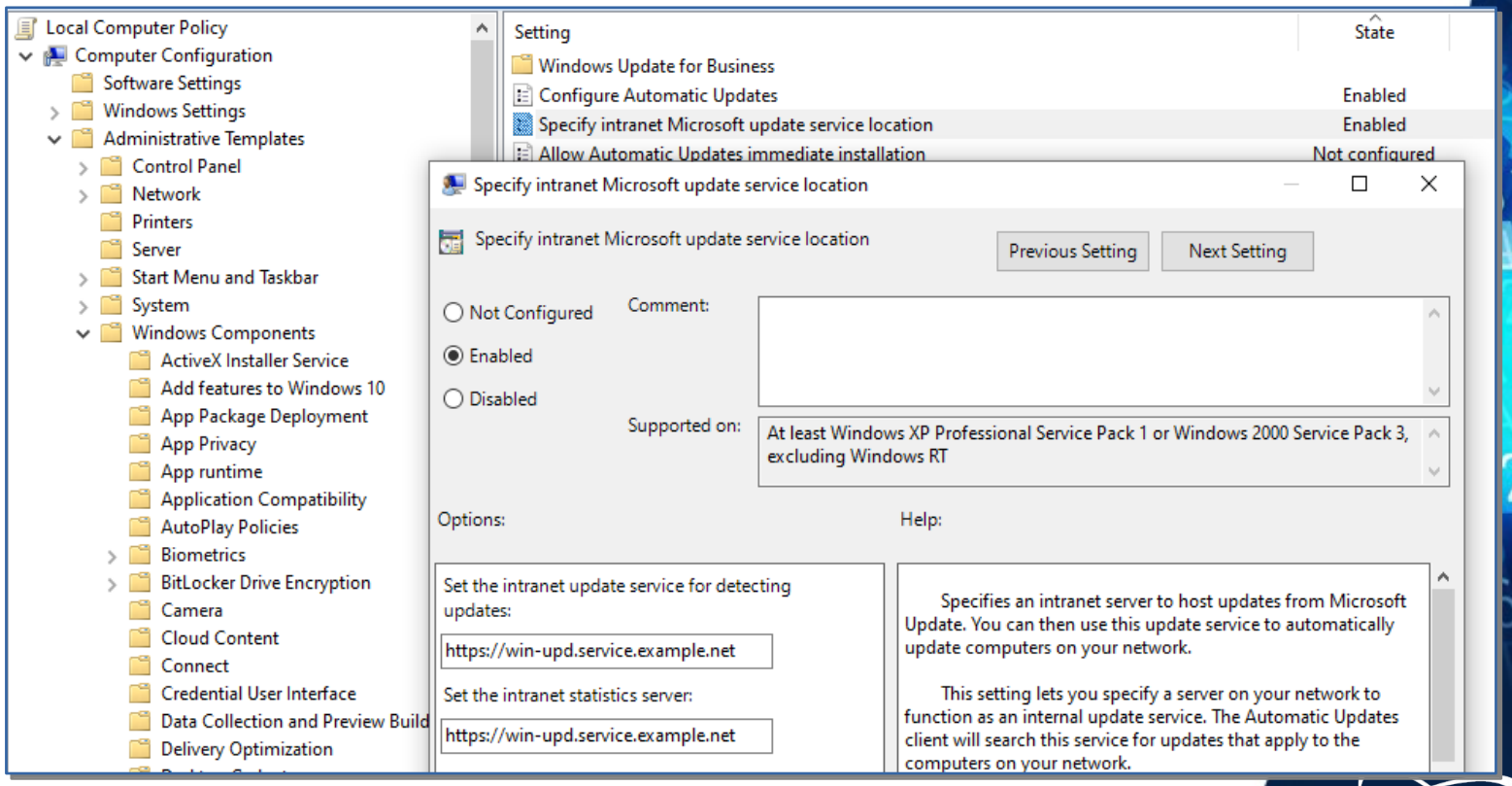
Updates

- Installing updates can‘t be turned off
- Feature Upgrades
  - Require maintenance work to adjust to personal preferences
    - Can be hold back up to one year
- Quality (Security) Updates
  - Install as fast as you can!
  - If stability is critical, wait a few days to see if MS pulls back an update
  - Can be delayed up to one month
- Reboots can be delayed until after work hours



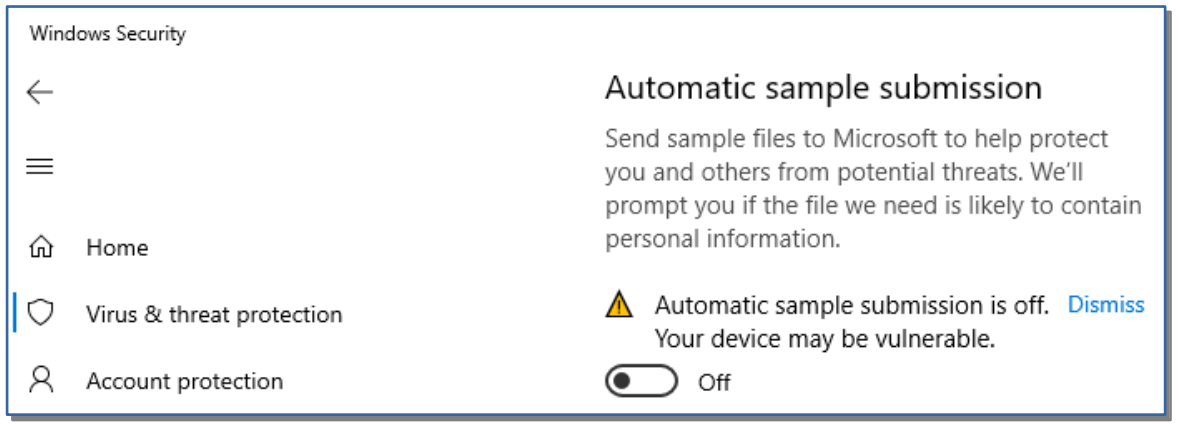
Updates: Update server

- More options with update server managed by the organisation
  - WSUS or Endpoint Manager
  - GPO object
  - Enterprise & Edu only



Updates: Windows Defender

- Windows Defender
  - Needs regular (signature) updates
  - Also uploads files assessed as suspicious
  - May process and upload personal/sensitive/confidential information/files
- Recommendation:
  - Turn off **automatic** sample submission
  - Settings → Update & Security → Virus & threat protection

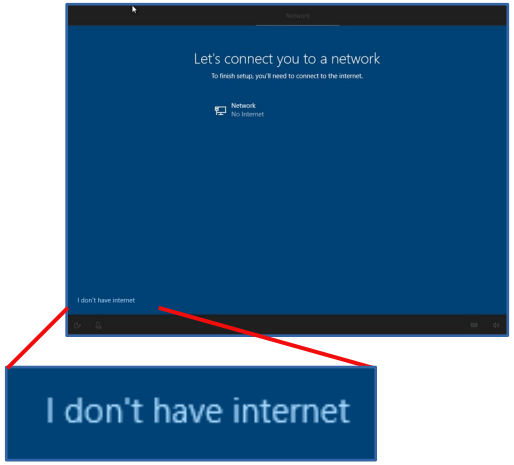


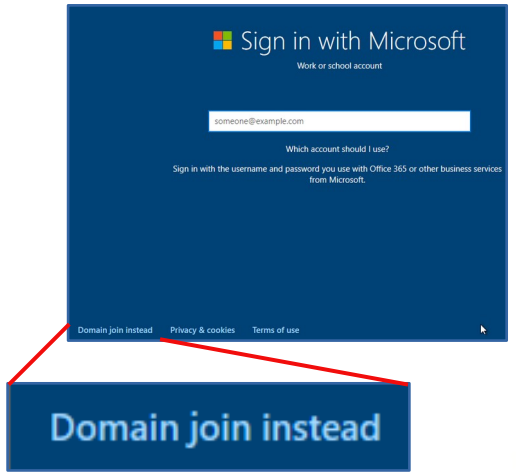
Defender Sample Submission Complete Deactivation

- Per registry key
  - `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Spynet`
  - Values:
    - `SubmitSamplesConsent = 2 (DWORD)`
    - `SpynetReporting = 0 (DWORD)`
- Per GPO:
  - `Computer Configuration → Administrative Templates → Windows Components → Windows Defender → MAPS`
    - `Send file samples when further analysis is required`
    - Set to `Enabled`
    - Select `Never send`

Local Account vs. Microsoft Account

- Default:
  - Use of MS (Cloud) account(s)
  - Almost hidden option to use local account
- Features:
  - (+) Single-sign-on to OS and Cloud
  - (+) Enables restore of OS license
  - (-) Makes tracking easier
  - (-) Password transferred in clear text to MS (once)
- Recommendation:
  - Install with local account
  - Add (cloud) accounts later if needed
  - Store/Cloud accounts don‘t need to be the same as host account





Any questions so far?

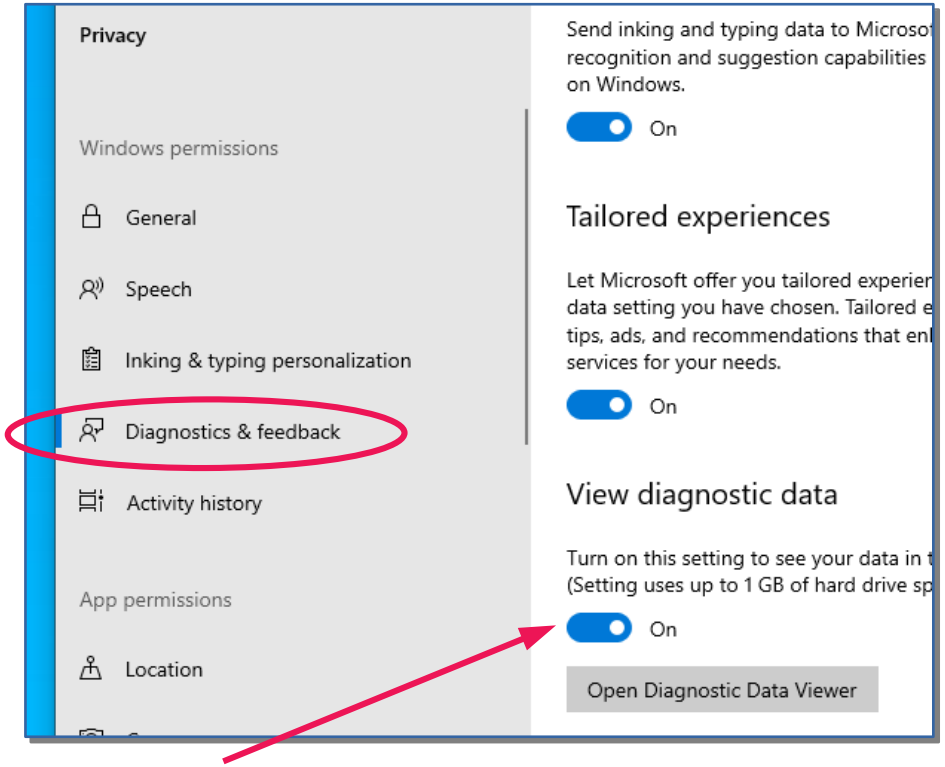
www.geant.org

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 731122 (GN4-2).

Telemetry: What it is – What it does – Issues

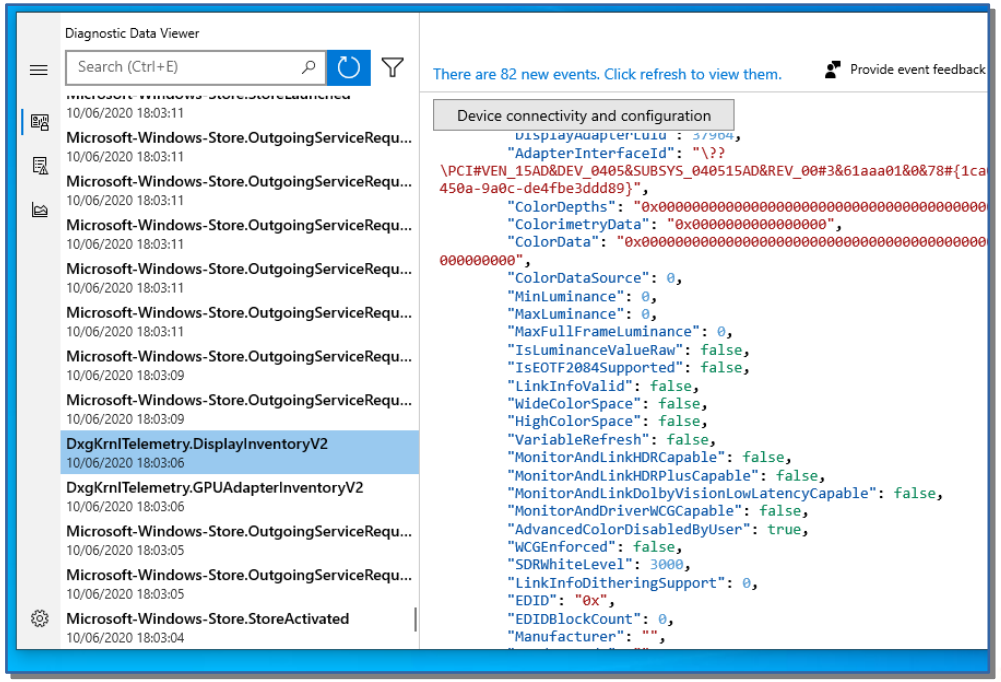
- System data uploaded by the *Connected User Experience and Telemetry* component
  - Aka Universal Telemetry Client (UTC) service, aka **Diagtrack** Service
- What is collected
  - Crash and usage data
  - Inspection of system & applications
  - System/platform information
- If “collect more information” is enabled
  - Inspection of running processes
    - Libraries loaded from DiagTrack service
  - Collection of system & platform information
    - Queries of registry & setup logs
- This may include sensitive/personal information!
  - Usage data can be used in behaviour analysis by Microsoft

Telemetry: Diagnostic Data Viewer



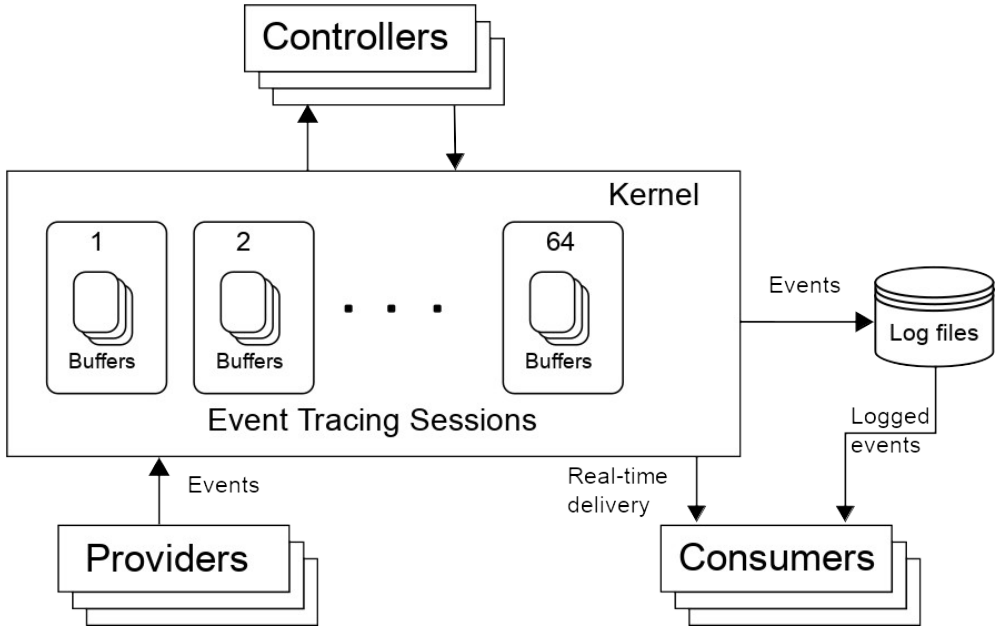
- Switch is off by default
- Requires free of charge App
- MS account required

- Diagnostic data on your system
- View only, no delete or filter



Excourse: Event Tracing for Windows

- Framework/API to build application logging
- DiagTrack & Eventlog based on it
- Controllers
  - Manage sessions
  - Create/delete
  - Activate/deactivate
  - Add/remove providers/consumers
- Providers
  - Produce (i.e. log, write logs) events
- Consumers
  - Consume (i.e. read) events
  - From log files or directly from kernel buffers (real-time)



Telemetry: Configuration (1)

- Tracking Level set in registry key:
  - `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\DataCollection\AllowTelemetry (DWORD)`
- Configuration defines providers for given tracking level
  - Downloaded from Microsoft at regular intervals
  - `%ProgramData%\Microsoft\Diagnosis\DownloadedSettings\utc.app.json`

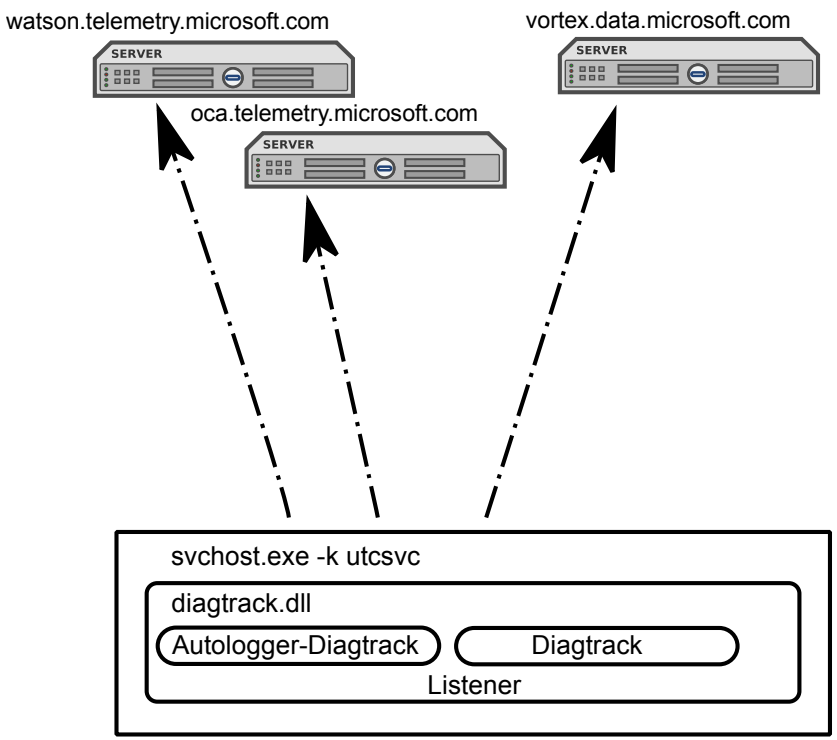
```
#{
 "queryUrl": "/settings/v3.0/utc/app",
 "settings": {
   "UTC:::ENDPOINT.TELEMETRY.ASM-WINDOWSSQ": "telemetry.0",
   "UTC:::PROVIDERDEFINITION.MICROSOFT.WINDOWS.SHELL.SYSTEMSETTINGS.SETTINGSAPPACTIVITY":
"b7afa6af-aaab-4f50-b7dc-b61d4ddbe34f",
   "UTC:::COMMONSCHEMAVERSION": "3.0",
   "UTC:::TENANT": "dedb3435bceb4d2d9f40bcb2139e6562-4de2fa0d-3dbd-4e46-a2dd-
f158b62f510a-7933",
…
```

Telemetry: Configuration (2)

Level	No of Providers for Listener		Data logged KBytes/day	Available for	Default Level
	AutoLogger-Diagtrack	Diagtrack			
0: Security	9	4		Ent, Edu	
1: Basic	93	410	~150 – 250	All	
2: Enhanced	105	418	~250 – 350	All	Ent
3: Full	112	422		All	Home, Pro

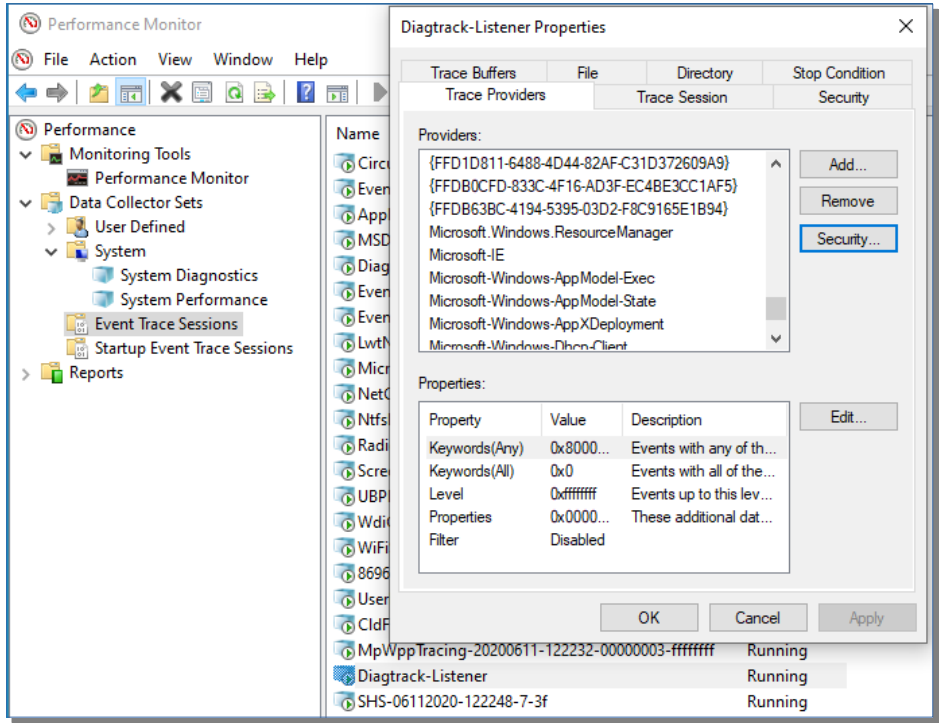
Telemetry: Transmission

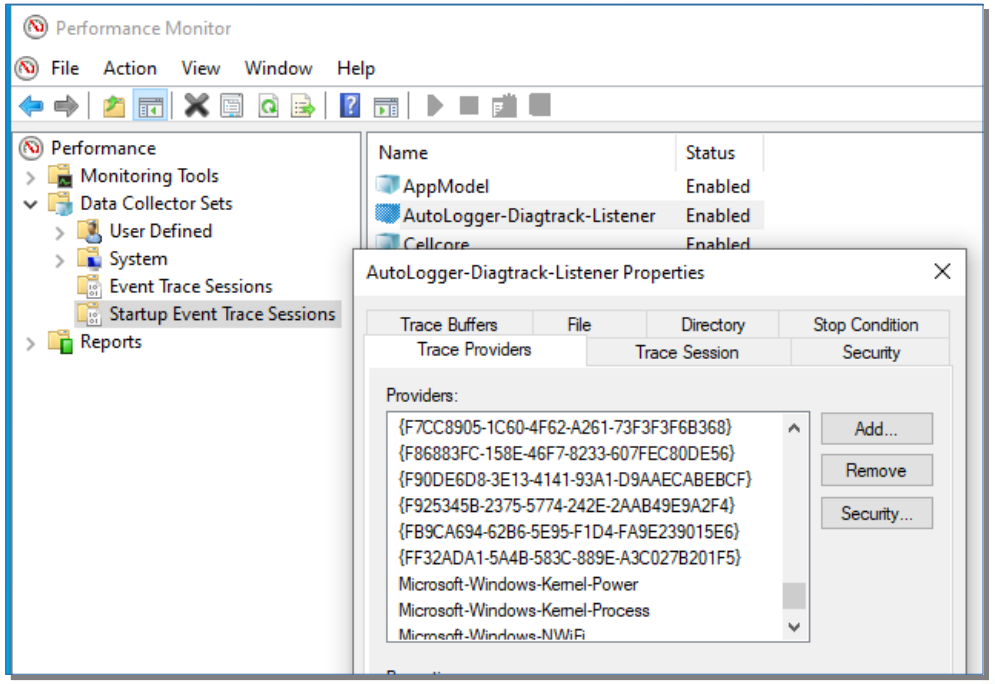
- Network: Telemetry servers
  - Names change with Windows 10 version
  - CDN, region etc. dependant
  - TLS, certificate pinned
  - Connects around every 15-20min
    - Less on metered links
- Locally: Diagtrack-Listener
  - `%ProgramData%\Windows\Diagnostic`
  - Hidden folder
- Listeners:
  - Autologger-Diagtrack for early boot events aka Startup Event Trace Sessions
  - Diagtrack for normal operation, aka Event Trace Sessions



Telemetry: perfmon.exe

- Control/inspection of telemetry sessions





Telemetry: Control (1)

- Local system:
  1. Set `AllowTelemetry` Key to `0`
  2. Deactivate `DiagTrack` Service
  3. Disallow network access to MS data collection servers (local firewall)
  4. Manipulate system name resolution for MS data collection servers (i.e. `%SystemRoot%\System32\etc\hosts`)
- Network:
  5. Disallow network access to MS data collection servers (network firewall)
  6. Manipulate DNS responses for MS data collection server names (local nameserver)

Telemetry: Control (2)

- 1) & 2) work best
  - Easy to setup through Scripts, GPOs, etc.
- 2) only solution on Pro, Home editions
- 3) – 6) problematic
  - IP addresses may change often

```
> dig  +noall +answer watson.telemetry.microsoft.com
watson.telemetry.microsoft.com. 10 IN   CNAME   umwatson.trafficmanager.net.
umwatson.trafficmanager.net.    10 IN       A   51.143.111.7
```

  - DNS names may change with Feature Upgrades
  - MS might opt to ignore etc/hosts in the future
  - Firewalls rules may not allow DNS names
  - Scripts & cronjobs for workarounds

Summary

- Telemetry/Data collection cannot be turned off completely
  - From an organisation/global security perspective, this is not entirely bad
- Trade-off between
  - Local security needs
  - Users‘ privacy
  - Users‘ convenience
  - Support from Microsoft/local admins
  - Legal: GDPR, other local laws, contracts (maintenance, warranties), etc.
- There are no patent solutions
- Only scratching the surface
  - See the links

Thank you

Any questions?

Next module: ***Logging and Audit***, 5th of August 2020

www.geant.org

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 731122 (GN4-2).

References (1)

- Privacy Protection Authorities
  - European Data Protection Supervisor
    - https://edps.europa.eu/press-publications/press-news/press-releases/2019/edps-investigates-contractual-agreements_en
  - France
    - https://www.zdnet.com/article/french-authorities-serve-notice-to-microsoft-for-windows-10-privacy-failings/
    - https://www.cnil.fr/en/windows-10-official-closure-formal-notice-procedure-served-microsoft-corporation
  - Netherlands
    - https://autoriteitpersoonsgegevens.nl/en/news/dutch-dpa-microsoft-breaches-data-protection-law-windows-10

References (2)

- Privacy Protection Authorities
  - German Federal Office for Information Security (BSI) SiSyPhus (English, with German summaries)
    - https://www.bsi.bund.de/EN/Topics/Cyber-Security/Recommendations/SiSyPHuS_Win10/SiSyPHuS_node.html
  - Bavaran Data Protection Authority for the Private Sector Windows 10 Investigation Report (English)
    - https://www.lda.bayern.de/media/windows_10_report.pdf
  - Max-Planck-Society (MPG): Orientation help (Orientierungshilfe) Windows 10 (German)
    - https://www.it-sicherheit.mpg.de/Orientierungshilfe_Windows10.pdf

References (3)

- The Court of Justice of the European Union
  - Ruling in case C-311/18 - Facebook Ireland und Schrems
    - http://curia.europa.eu/juris/liste.jsf?num=C-311/18
- Windows Defender blocking entries in .../etc/hosts
  - https://www.bleepingcomputer.com/news/microsoft/windows-10-hosts-file-blocking-telemetry-is-now-flagged-as-a-risk/
  - https://support.microsoft.com/en-us/help/2764944/hosts-file-is-detected-as-malware-in-windows-defender

References (4)

- Microsoft privacy statement
  - https://privacy.microsoft.com/en-us/privacystatement
- More explanation about data collection in Windows 10
  - https://privacy.microsoft.com/en-US/windows10privacy
- **Which Windows 10 components connect to Microsoft servers**
  - https://docs.microsoft.com/en-us/windows/privacy/manage-connections-from-windows-operating-system-components-to-microsoft-services
- **Which (Microsoft) servers Windows 10 connects to**
  - https://docs.microsoft.com/en-us/windows/privacy/manage-windows-2004-endpoints
- Cortana & privacy
  - https://support.microsoft.com/en-us/help/4468233/cortana-and-privacy-microsoft-privacy
- Cortana deactivation
  - https://www.howtogeek.com/265027/how-to-disable-cortana-in-windows-10/

Further reading

- “Windows Internals, Part 1” 7th Ed.
  - Pavel Yosifovich, Mark E. Russionvich, and David A. Solomon
  - Microsoft Press 2017
  - ISBN: 978-0-7356-8418-8 (Book), 978-13-398648-8 (eBook)
  - Part 2 was scheduled for 9/2019 :(
- “Troubleshooting with the Windows Sysinternals Tools”, 2nd Ed.
  - Mark. E. Russinovich, and Aaron Margosis
  - Microsoft Press 2016
  - ISBN: 978-0-7356-8444-7 (Book), 978-13-398653-2 (eBook)
- “Digital Privacy and Security Using Windows: A Practical Guide”
  - Nihad A. Hassan, and Rami Hijazi
  - Apress 2017
  - ISBN 9-78148227985