TAS Research Report:
Desktop Windows Security and Optimisation

Version: 2.0

Date: 2023-06-27

Notice

Document enquiries may be directed to:

Records Management Office
SITA SOC Ltd
PO Box 26100, Monument Park, 0105, South Africa
Tel: +27 12 482 3000
www.sita.co.za

TAS Research Report: Desktop Windows optimisation
Document No: **TASRR40-2023**
Author: **Izak de Villiers**, izak.devilliers@sita.co.za, +27 12 482 2749

Approval

The signatories hereof, being duly authorised thereto, by their signatures, hereto authorise the execution of the work detailed herein, or confirm their acceptance of the contents hereof and authorise the implementation/adoption thereof, as the case may be, for and on behalf of the parties represented by them.

Tshayhu Mukhodobwane
HOD: Norms Standards and Quality
Corporate and Digital Strategy

2023-07-04
Date

Deon Nel
Senior Specialist: TAS

2023-07-04
Date

Izak de Villiers
Senior Specialist: TAS

2023-07-04
Date

Foreword

To support Government ICT operations, a solid, reliable and stable desktop operating system is required. Unfortunately Microsoft's Windows platform does not support this requirement as fully as could be expected. This report identifies issues with the default configuration of Windows 10 and 11, highlighting problematic behaviours, bundled apps, services and settings that need to be fixed, uninstalled, disabled or changed to improve performance, security and efficiency. The research was done in conjunction with the GITOC TTT and other subject matter experts. The report will be shared with Microsoft to hopefully create awareness resulting in an improved, optimised or properly-positioned desktop OS in future. Alternatively, making Government aware of the issues may precipitate a move towards open-source alternatives.

Contents

Tables

Figures

1. Introduction and background

Following recent changes in the end-user computing market and technology landscape, Microsoft has placed a heavy emphasis on consumer and cloud technologies starting with the introduction of Windows 10. This emphasis has became stronger with Windows 11, including the bundling of games and consumer cloud services into desktop Windows – even in the Professional version used in business and enterprise. Due to this, the default security stance of Windows is problematic, with dozens of open firewall ports and unwanted services increasing the system's attack surface significantly.

TAS believes that many performance and other issues experienced with new Windows systems can be attributed to the consumer-focussed configuration of Windows. Consumer apps and functionality in Windows waste RAM and CPU cycles, cause unwanted internet traffic and impacts system performance and security. These issues can only be avoided by proper configuration of the standard Government desktop OS. An inefficient desktop OS reduces user productivity and wastes computing resources, requiring replacement of hardware earlier than necessary.

This report lists issues found with the configuration of off-the-shelf Windows, highlighting unnecessary apps, services and settings that need to be disabled or changed to improve security, performance and efficiency.

It is a fact that with Windows 10 and 11 Microsoft has delivered brilliant and advanced new features such as PowerShell, Windows Terminal, Hyper-V and the Windows Linux subsystem (WSL). The possibility of simply installing Linux on a Windows desktop from the Microsoft Store would have been unthinkable a few years ago. However, 99% of Windows users will never need these advanced features – they will just struggle with the advertisements and other UI distractions while trying to do their work without having to pay attention to the OS.

In the final analysis, a more secure and effective Windows desktop environment will contribute towards lower TCO (total cost of ownership) by eliminating unnecessary consumer-focussed features, and reducing risk by presenting a smaller attack surface to malicious actors.

2. Goals of an enterprise desktop OS

Before diving into the detail of where modern Windows falls short of what it should deliver, it will be useful to identify a set of goals that a desktop OS should achieve in order to be successful in the enterprise.

- Strong security: system must be hardened by default
- Low TCO: no negative cost or productivity impacts
- Reliability: the OS is available at all times
- Support the user in fulfilling their task, with minimum distractions or inefficiencies
- Direct and intuitive access to user applications and data
- Stability, with long periods between significant changes or feature updates
- Good performance: support user productivity with minimum delays
- Efficient use of hardware, software and network resources
- Unambiguous, easy-to-use UI to maximise user productivity
- Support the enterprise's business, not the OS vendor's
- Customisable and advanced functionality for specialist users (while keeping the basic OS simple to use for normal users)
- No unwanted "features"

- Provide tools to the user to access their data and applications in the most effective and direct way (this could include icons on the desktop, pins on the Taskbar, or an effective Start Menu)

We believe this report shows that very few of these goals are met by current versions of Windows, leading us to the conclusion that these goals are not shared by Microsoft, despite the claims they make. This forces enterprise users of Windows to spend significant time and resources to harden the system and address built-in inefficiencies, instead of just being able to implement and use the OS to do their work.

3. Desktop Windows issues

TAS has done a considerable amount of research on desktop optimisation throughout the lifespan of Microsoft Windows, starting as early as Windows 98 and XP. Over this time, and with the introduction of cloud services and consumer apps, the focus and design of Windows has changed to the extent that much of the baseline functionality and UI principles have been eroded.

Input from the Government end-user community, including SITA clients and the GITOC TTT has been incorporated into these findings and recommendations.

3.1 Performance indicators

An idle Windows system exhibits significant CPU utilisation and network traffic, which seems to implicate the unnecessary bundled apps and services for wasting so many resources. Multiply the amount of unnecessary network traffic by hundreds of systems in a typical organisation, and user experience will definitely be impacted, not to mention other enterprise systems.

TCO is also affected by higher power consumption and consequent generation of heat, requiring more cooling. On mobile systems battery life is negatively affected by every unwanted Windows component that wastes CPU cycles and energy.

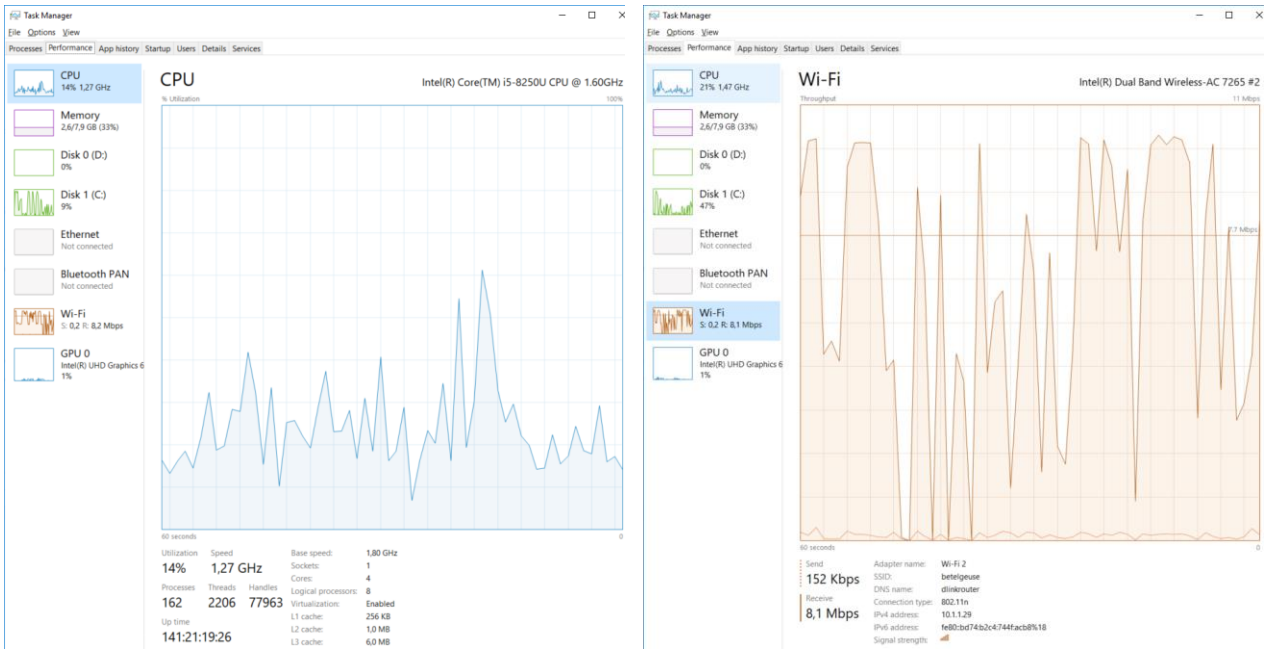


Figure 1: High CPU and network activity on idle system

3.2 Windows Explorer

3.2.1 Start Menu

The area where Microsoft's inappropriate focus on consumers in Windows Pro is most evident is the Start Menu. The majority of live tiles on the default Windows 10 Start Menu are either games or consumer apps – and they update over the internet every time the Start Menu is opened.

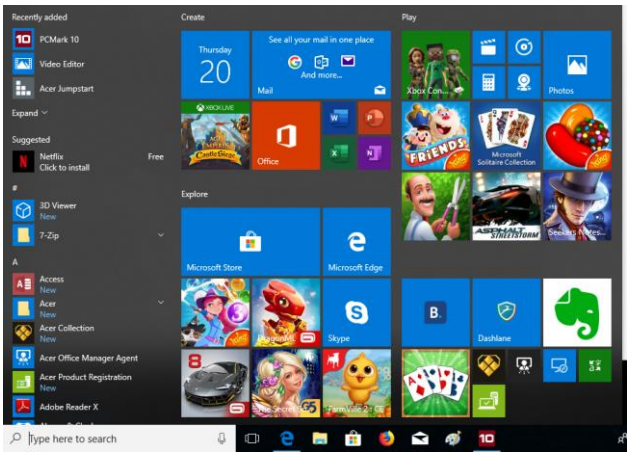


Figure 2: Consumer apps in Windows Start Menu

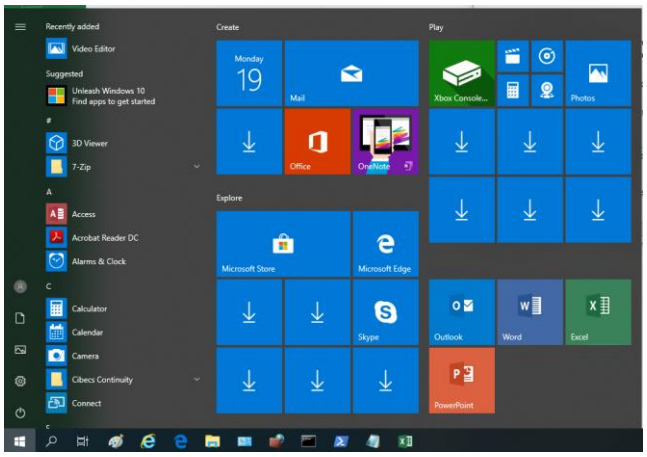


Figure 3: Start Menu when not connected

When the device is not connected to the Internet, all these tiles are inactive, and show "downloading" icons. Imagine the impact on the enterprise network when hundreds of PCs all update their icons over the internet at the same time. These unwanted network connections could also represent potential security issues, since future changes to apps or settings could introduce new vulnerabilities.

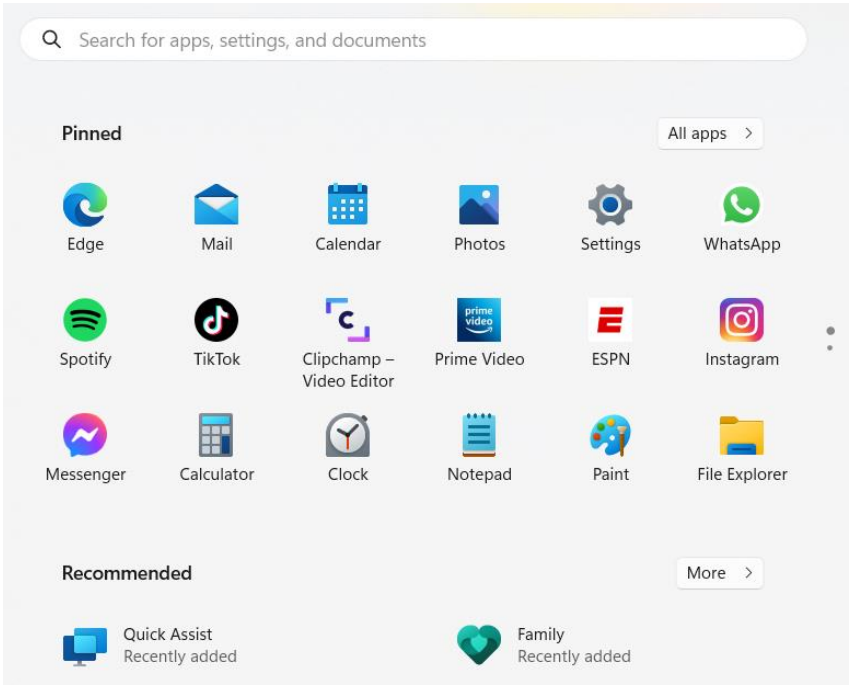


Figure 4: Windows 11 Start Menu

Having done away with the "live tiles" concept, the Windows 11 Start Menu probably causes less unnecessary network traffic. However, it seems that Win11 has even more consumer applications installed by default (e.g. ESPN, Prime Video, Spotify) – some of which (especially TikTok) can represent serious security and productivity risks for an enterprise desktop.

It would take very little effort by Microsoft to remove these apps from the Pro version of Windows. Why do they insist on bundling these apps, even though they are surely aware that they cause problems in work environments?

3.2.2 Built-in advertisements

Following the theme of implementing UI elements and "features" that fit better in a consumer space, Windows also shows the user product advertisements. During an update in 2018, Microsoft introduced "sync provider notifications" into the file explorer. These will periodically show "suggestions" for apps and services that Microsoft wants to introduce to the user. The Start Menu's "suggested" section has the same purpose. No true enterprise OS vendor would show unsolicited content to end-users, and no proactive IT department would allow it.

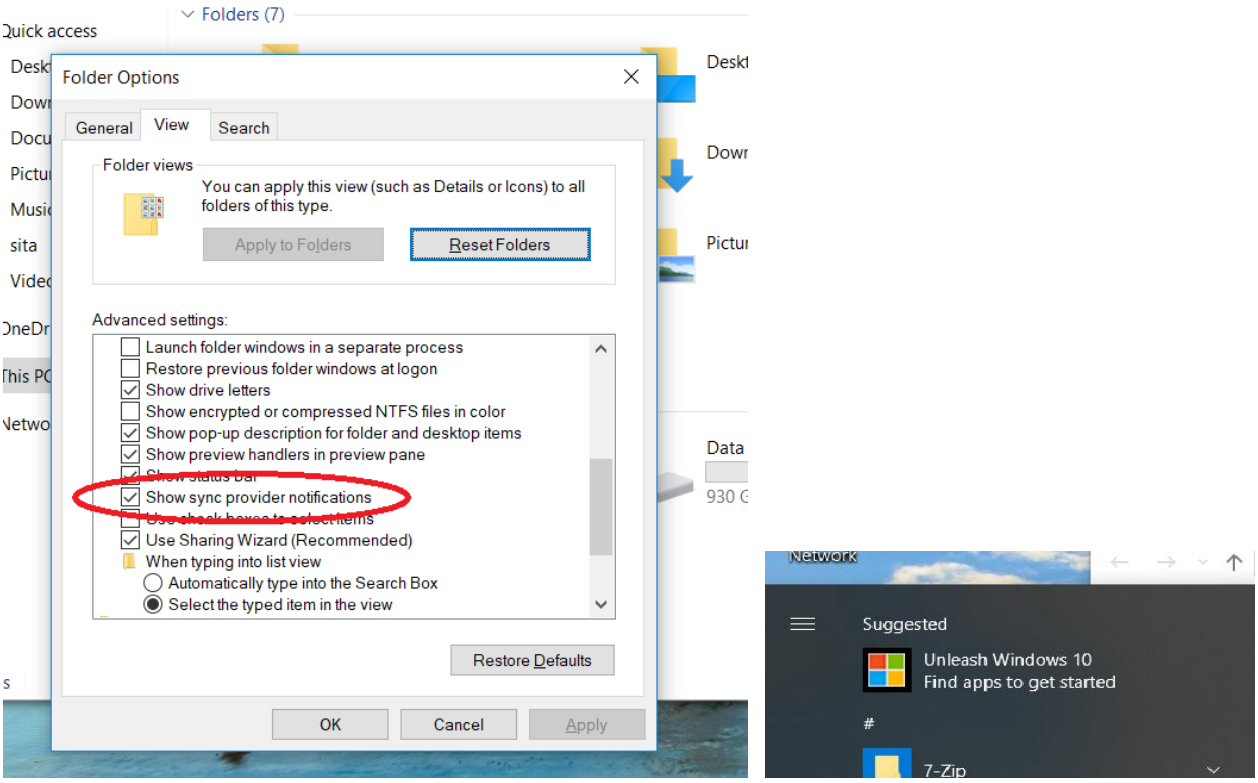


Figure 5: Sync provider notifications: advertisements in Explorer and Start Menu

3.3 Consumer-focussed apps

The consumer apps and games installed in Windows by default need to be disabled, since these communicate over the network (even receiving incoming messages through the firewall!) and interfere with day-to-day operations. One such example is the **Xbox** app, Microsoft's gaming platform, which has no place an enterprise PC.

Likewise, apps such as Groove Music, Maps, Solitaire and Mixed Reality serve no purpose in Government. Microsoft has even added advertisements and cloud-based data collection to the new version of Solitaire.

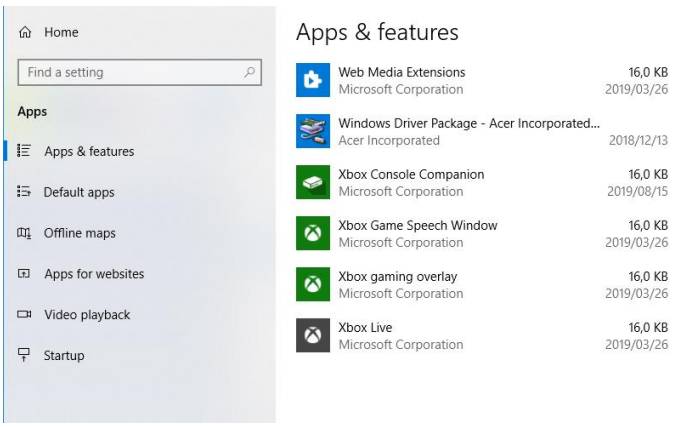


Figure 6: Consumer and gaming apps installed by default

3.3.1 Embedded and bundled apps

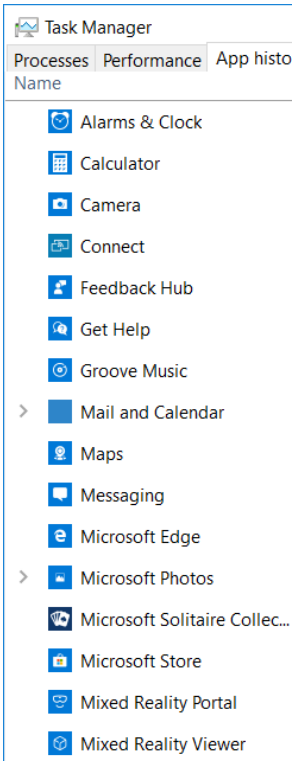


Figure 7: Unneeded apps installed in Win10

In the 1990s Microsoft's anti-competitive practices were the subject of a lengthy legal trial[1] in the USA. The complaint was that Windows forced users to use Microsoft's web browser (Internet Explorer), not allowing customers to choose alternative products, or even to remove of the default browser from the system. Microsoft's argument was that IE was integrated into Windows, and could not be removed without breaking important functionality. This claim was refuted during the trial, and, even though MS won an eventual appeal, they were forced to allow alternative web browsers, paving the way for significantly better products to gain market share. Since then IE market share dropped from 95% down to less than 10% in 2014, perhaps showing why Microsoft feels the need to compete unfairly.

With Windows 11 we have come full circle, with Microsoft again embedding applications into the OS (e.g. Edge and Teams) with no readily accessible way of removing them, and various unsubtle prompts and encouragements for the user to switch away from their preferred competing products.

For example, the **Chat app** (Teams) is front and centre on the Windows 11 taskbar, but it's not even listed as an installed app, and cannot be removed without using the Windows Terminal and PowerShell. As was the case with IE, users would just naturally follow the path of least resistance, and start using Teams as their default messaging app. Thus Microsoft effectively eliminates competition by exploiting default OS behaviour and the reluctance of users to install an alternative. This could easily end up in another monopoly situation as was the case with IE achieving more than 90% market share in the early 2000s due to unfair bundling practices. Unlike with a web browser, though, a messaging app also affects the services used by the people that the user communicates with, making one user's choice cascade to others.

The **Edge browser** on the other hand is listed as an installed app, but the option to remove or uninstall it is not exposed to the user. Edge also egregiously modifies search engine behaviour to steer users away from competing products, and promotes itself through various mechanisms as being better than the alternatives w.r.t. performance, battery life or security. Whenever the user is prompted by Windows to switch to Edge, the options are typically "Yes" or "Skip for now". There is often no option to permanently choose, so the prompts keep reappearing.

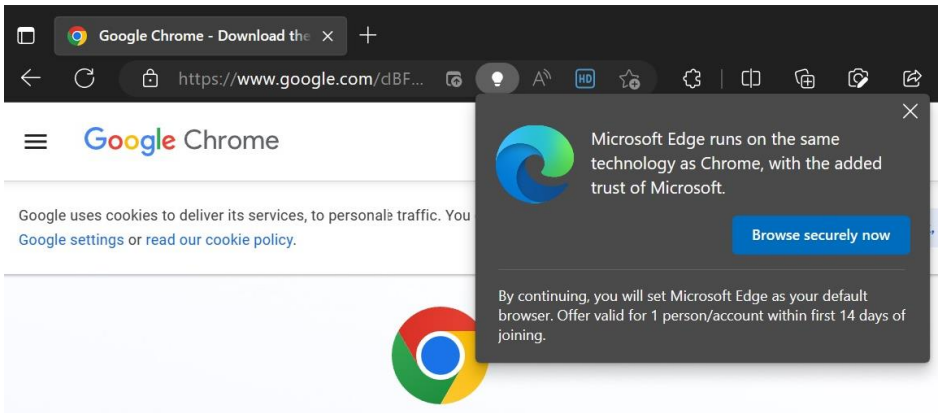


Figure 8: Edge uses several mechanisms to discourage users from switching

[1] Microsoft antitrust case https://corporatefinanceinstitute.com/resources/management/microsoft-antitrust-case/

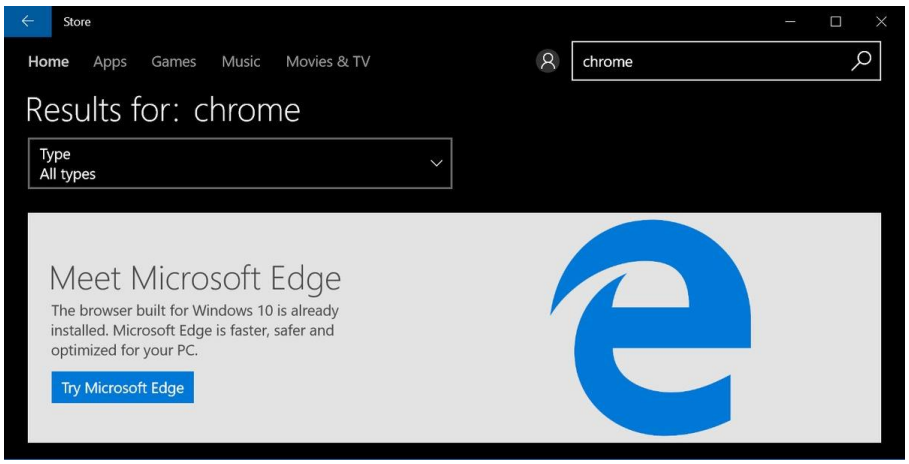


Figure 9: Even the Microsoft Store manipulates search results to mislead users

Xbox, Microsoft's cross-platform gaming app, is another egregious example of the company's lack of enterprise focus: every Windows desktop comes loaded with several Xbox components, most of which can't be uninstalled. It's safe to say that most organisations do not need to have these apps running on their desktops, and they should have the ability to remove them – or preferably Microsoft should not preload them in the first place.

According to an Xbox ambassador on Microsoft's Answers forum:

> *There is no ability to completely remove Xbox from Windows 10 even with the Powershell commands. The component itself is tiny, removing it will not release a significant amount of storage on your laptop.*
>
> *Xbox does not come with games installed by default. Any games that are somehow installed on your machine can be removed via the Settings screen.*
>
> *In addition, the Xbox component of Windows 10 uses no extra processing cycles and will not slow down your laptop, regardless of its specifications.*

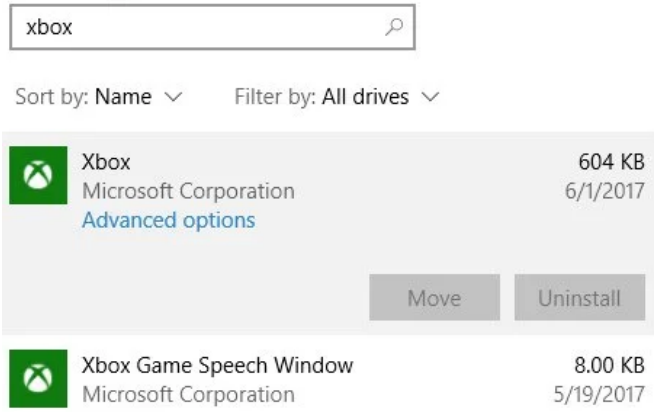


Figure 10: Components of the Xbox app cannot be uninstalled

Lastly, Microsoft bundles a trial version of Microsoft Office with every Windows PC. Even when organisations install their own version of Microsoft Office, these default components remain on the system, causing confusion for users and consuming resources. The upside for Microsoft is that users may accidentally be persuaded to provide their personal information to register this version unnecessarily.

Government Departments have complained to SITA that users select this version of Office instead of the correct, licenced one, resulting in unnecessary support calls to resolve issues.

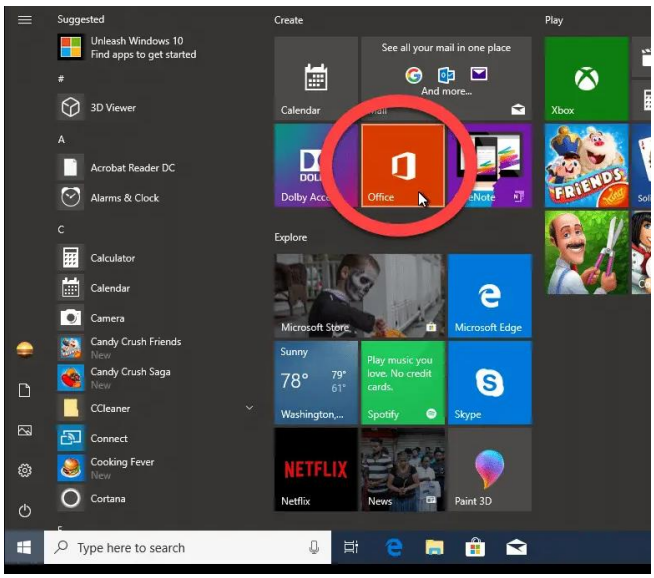


Figure 11: Office bundled with Windows

3.3.2 Default applications and file associations

To further cause confusion and impair user productivity, Windows regularly loses previously set application preferences (file associations), forcing the user to either go with the Microsoft option, or to laboriously fix the associations manually. In many cases the choice cannot be made permanent: the "always use this app" option is disabled, leaving the user with no choice but to use the Microsoft option.

Either Microsoft is not aware that 3rd-party applications exist (unlikely) or they do not want these apps to be available to the user. More recent versions of Windows have been actively blocking users from changing the defaults to open their preferred applications. To make matters worse, user preferences are often reset after Windows is updated. In many cases, restoring the user's preference is blocked – as shown in the screenshot.

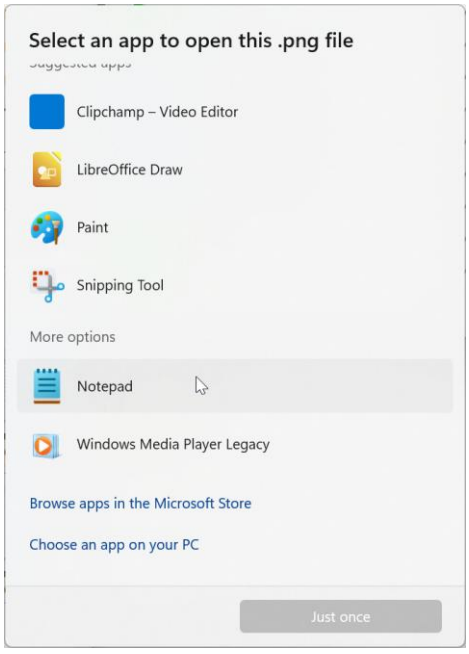


Figure 12: User-selected app preferences are reset regularly

As in the 1990s Microsoft is clearly still abusing its position as the OS vendor to unfairly promote its own products and stifle competition.

3.3.3 Startup settings

Apps such as Microsoft OneDrive and Windows Defender are configured to start by default at boot. In most cases Windows Defender is not needed, since enterprises have their own anti-malware system. Having a second anti-malware service running is not efficient, and could be seriously detrimental, since these often clash with each other, duplicate functionality and even sometimes "detect" each other as malware.

Intel's Graphics Settings utility, installed on more than 95% of desktops, can be disabled, since it uses resources without providing significant benefit to the user. Microsoft's consumer-focussed OneDrive is not appropriate for enterprise use, but uses resources, causes end-user distraction, and communicates with the cloud continually. Whenever an app or service is specifically required by a user, it can be enabled on a case-by-case basis. However, the default state should be "Disabled", or it should be uninstalled.

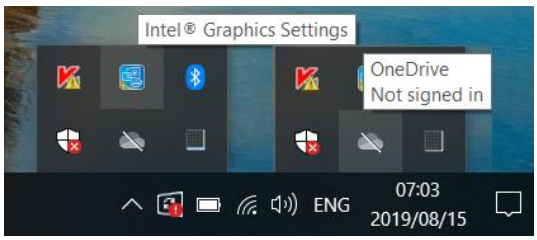


Figure 13: Intel Graphics Settings and OneDrive running by default

3.3.4 Cloud-based and gaming apps

One of the most hyped features of Windows 10 has been the voice-activated **Cortana** service that promises advanced AI-driven search and automation functionality. However in South Africa this service is only partially available, and it needs real-time cloud access in order to work at all. Voice-driven personal assistants have been proven over and over to listen in to conversations without being activated by the user. This is obviously a serious security risk for Government and other enterprises. Cortana has since been deprecated by Microsoft, with plans to replace it with a different AI-enabled service based on Bing Chat. Needless to say, in an enterprise environment with high security requirements this can only cause problems.

OneDrive is a consumer cloud file-sharing app, which typically should not be allowed inside an enterprise network, both for performance and security/confidentiality reasons. Microsoft does have an Enterprise version of OneDrive if this type of functionality is needed – but it must be properly implemented and secured.

Lastly, as noted above, the pervasive **Xbox** gaming app and related services has no place on an enterprise system.

All of these components have corresponding firewall rules which open ports by default on all Windows installations, possibly exposing users to serious vulnerabilities. The firewall settings are discussed elsewhere in the report.

Figure 14: Cortana, OneDrive cloud and Xbox components

3.4 Data collection

With the introduction of Windows 10, Microsoft started to place considerable emphasis on collecting user data. It started with users being encouraged to create a Windows ID to log into Microsoft cloud services, and has culminated in a situation where the current version of Win11 **does not allow the user to boot** into their PC without first signing into Microsoft. Previously this step could be bypassed, but that is no longer possible, leaving the user vulnerable to data collection, and even **denying them access** to the computer they purchased.

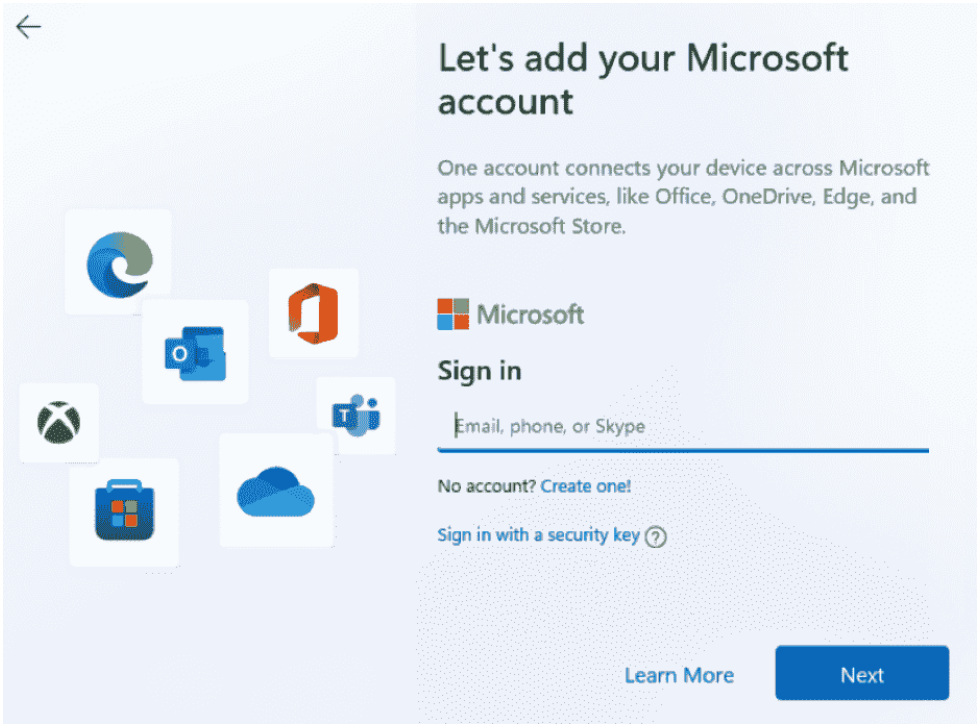


Figure 15: Users have to sign in before being allowed to use Win11

Another example of this, with an added consumer twist, is that built-Windows in apps sometimes ask the user to "rate" them. While this may provide useful information to Microsoft, it does not belong in a work environment. The user is interested in getting the output from the app and continuing with their work as quickly and efficiently as possible. The OS must not interrupt that process.

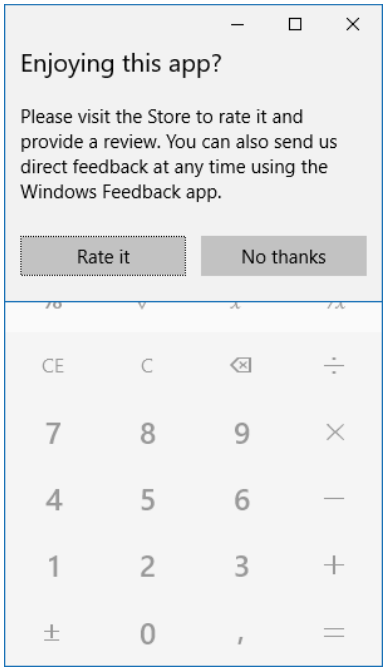


Figure 16: Apps asking for user ratings

Windows also constantly prompts users to "finish setting up your PC"[2] – presumably because the "correct" Microsoft default applications or data collection settings were not chosen. This is another productivity drain and source of confusion and frustration for end-users. This data collection could represent or enable spyware, which is a serious privacy[3] and data security risk for enterprises and government. Like many other Windows prompts, the "finish setting up prompt" often comes at the most inconvenient time for the user. Being a modal dialogue box, it **cannot** be switched away from or bypassed, therefore blocking all productive work on the PC until the user submits to Microsoft's demands. Selecting "Remind me later" only means the user to has to revisit this unwanted interruption later, at another inconvenient time.

According to the Electronic Frontier Foundation, a non-exhaustive list of user data collected by Windows includes:

- Location data
- Text, voice and touch input
- Webpages visited
- Telemetry data regarding general computer usage, including which programs are run and for how long

[2] www.tipsdotcom.com/lets-finish-setting-up-your-device.html
[3] www.eff.org/deeplinks/2016/08/windows-10-microsoft-blatantly-disregards-user-choice-and-privacy-deep-dive

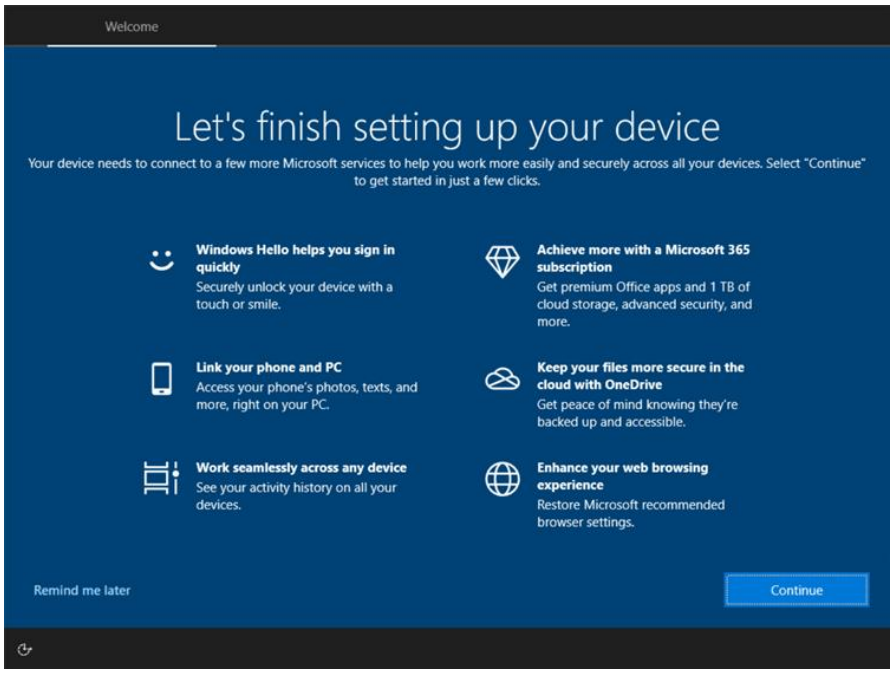


Figure 17: Initial setup, revisited repeatedly

The German Federal Office for Information Security has released a tool that checks how much telemetry date an unsecured Windows 10 or Windows 11 sends to Microsoft.[4] The linked article concludes that it is unclear how the transmitted data is being used by Microsoft, but it is a major concern nonetheless.

Apparently the data collection and other issues with Windows 11 has prompted the developers of **Rufus**, a very well-known utility app for creating a boot disk from an ISO image, to allow users to disable all these "features" up-front:

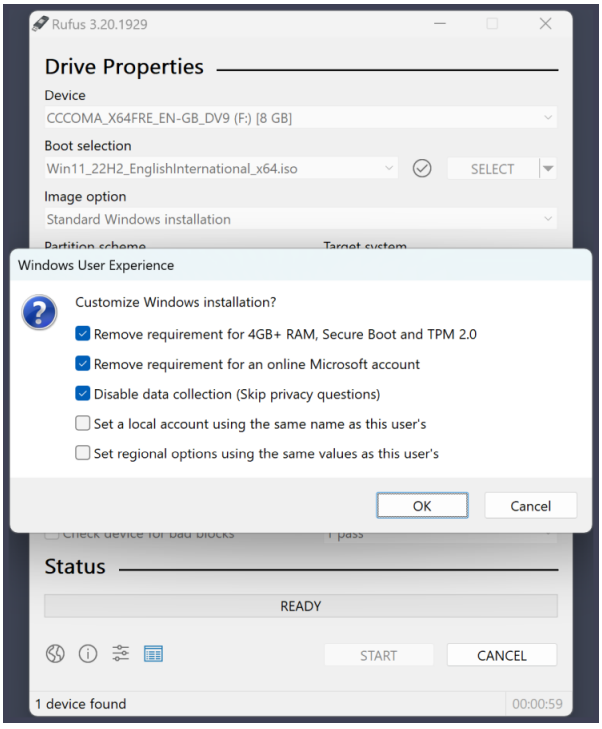


Figure 18: Rufus boot disk creator can change Win11 installation options

[4] www.fb-pro.com/windows-telemetry-information-test

As part of our engagement with Microsoft, TAS will inquire what feedback they have received from other organisations around the world (e.g. US DoD) regarding user data collection in Windows.

3.5 Windows Services

The Windows Services infrastructure provides vital functionality to keep Windows running properly. This includes anti-malware, network and configuration services. However, this infrastructure is sometimes used inappropriately, and needs to be configured correctly to make Windows more efficient.

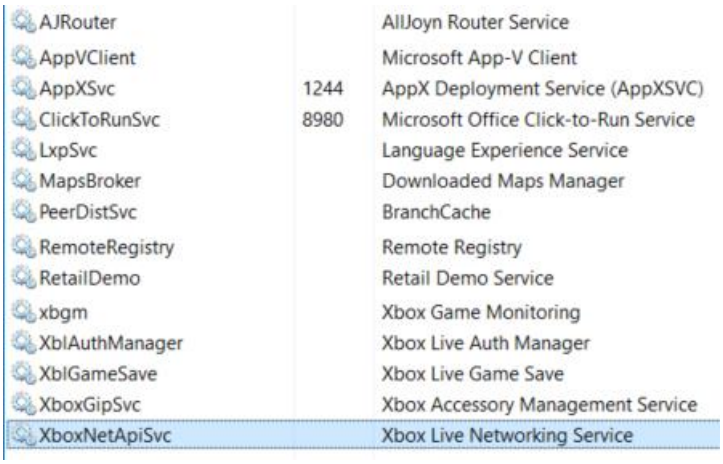


Figure 19: Example of unnecessary services enabled by default

The large number of services running by default is a concern – every one of these makes demands on system resources. In some environments some services may be required or can add value, while in other environments they just use up computing resources. The basic principle is, if a service is not needed, it should not be running.

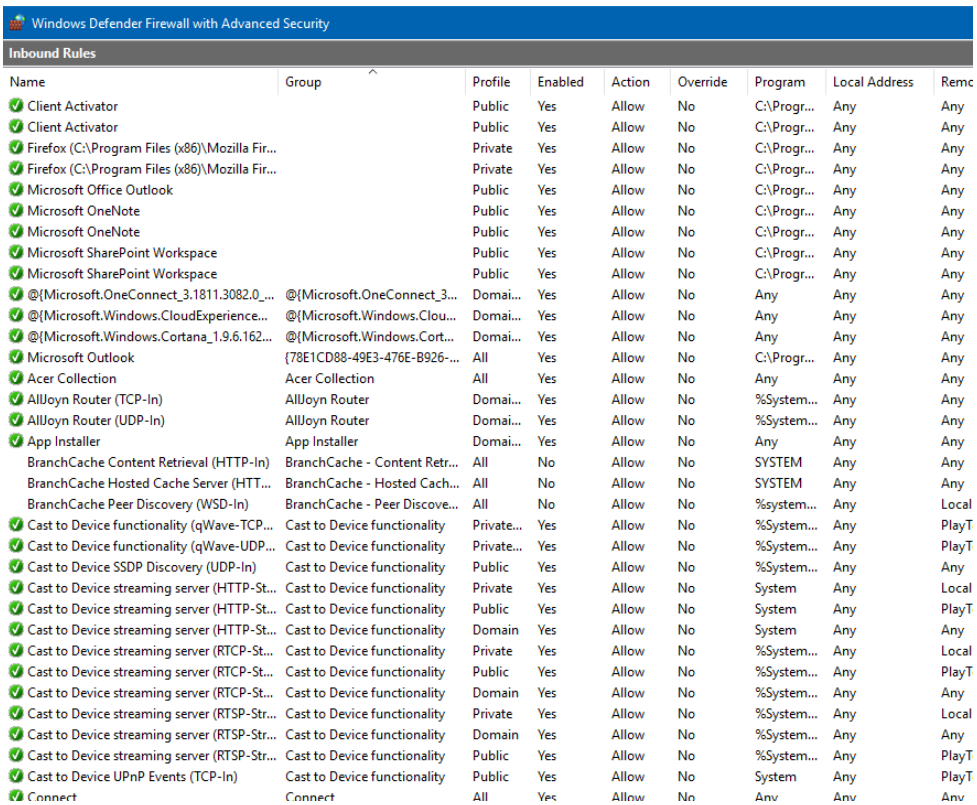
The optimum Services configuration will need to be determined for each group of devices, but shown here is an extract of services that are either definitely not needed, or represent performance issues and security risks. Each of these should be considered carefully, given the possible impact on scarce resources or information security. Some of these enable disturbing functionality in Windows, such as **Remote Registry**. A full list of services that are enabled by default is included in the Annex.

3.6 Firewall configuration

An important component of a Windows system's security is the local firewall. However, Microsoft appears to have subverted the firewall settings to enable many of its consumer technologies, sacrificing security for convenience or ease of use. This has been a pattern of behaviour from Microsoft throughout its history.

In general, any device that is not a server should only have the **bare minimum** of inbound firewall rules enabled. However, in Windows 10 and 11 Microsoft registers hundreds of default rules, most of which point to their consumer applications. Needless to say, **any** open firewall port is a significant security risk. With the number of open ports in Windows, Microsoft is opening their users to possible zero-day vulnerabilities or other risks.

Government systems must be security-hardened by default, and the first step towards this goal is to disable as many open firewall ports as possible. The screenshot below shows just the first few dozen lines of **several pages** of enabled inbound firewall rules in Windows. The concern here is the large number of **inbound** rules, most of which are for Microsoft consumer applications. However, **any** inbound firewall rule represents an unacceptable security risk, and these should be minimised to only those specifically needed in the environment. It is conceivable that malware could scan through all the open access points until it finds a vulnerability. Allowing so many external communications through the firewall is foolish at best, and malicious at worst.



Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remc
Client Activator		Public	Yes	Allow	No	C:\Progr...	Any	Any
Client Activator		Public	Yes	Allow	No	C:\Progr...	Any	Any
Firefox (C:\Program Files (x86)\Mozilla Fir...		Private	Yes	Allow	No	C:\Progr...	Any	Any
Firefox (C:\Program Files (x86)\Mozilla Fir...		Private	Yes	Allow	No	C:\Progr...	Any	Any
Microsoft Office Outlook		Public	Yes	Allow	No	C:\Progr...	Any	Any
Microsoft OneNote		Public	Yes	Allow	No	C:\Progr...	Any	Any
Microsoft OneNote		Public	Yes	Allow	No	C:\Progr...	Any	Any
Microsoft SharePoint Workspace		Public	Yes	Allow	No	C:\Progr...	Any	Any
Microsoft SharePoint Workspace		Public	Yes	Allow	No	C:\Progr...	Any	Any
@{Microsoft.OneConnect_3.1811.3082.0_...	@{Microsoft.OneConnect_3...	Domai...	Yes	Allow	No	Any	Any	Any
@{Microsoft.Windows.CloudExperience...	@{Microsoft.Windows.Clou...	Domai...	Yes	Allow	No	Any	Any	Any
@{Microsoft.Windows.Cortana_1.9.6.162...	@{Microsoft.Windows.Cort...	Domai...	Yes	Allow	No	Any	Any	Any
Microsoft Outlook	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progr...	Any	Any
Acer Collection	Acer Collection	All	Yes	Allow	No	Any	Any	Any
AllJoyn Router (TCP-In)	AllJoyn Router	Domai...	Yes	Allow	No	%System...	Any	Any
AllJoyn Router (UDP-In)	AllJoyn Router	Domai...	Yes	Allow	No	%System...	Any	Any
App Installer	App Installer	Domai...	Yes	Allow	No	Any	Any	Any
BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retr...	All	No	Allow	No	SYSTEM	Any	Any
BranchCache Hosted Cache Server (HTT...	BranchCache - Hosted Cach...	All	No	Allow	No	SYSTEM	Any	Any
BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discove...	All	No	Allow	No	%system...	Any	Local
Cast to Device functionality (qWave-TCP...	Cast to Device functionality	Private...	Yes	Allow	No	%System...	Any	PlayT
Cast to Device functionality (qWave-UDP...	Cast to Device functionality	Private...	Yes	Allow	No	%System...	Any	PlayT
Cast to Device SSDP Discovery (UDP-In)	Cast to Device functionality	Public	Yes	Allow	No	%System...	Any	Any
Cast to Device streaming server (HTTP-St...	Cast to Device functionality	Private	Yes	Allow	No	System	Any	Local
Cast to Device streaming server (HTTP-St...	Cast to Device functionality	Public	Yes	Allow	No	System	Any	PlayT
Cast to Device streaming server (HTTP-St...	Cast to Device functionality	Domain	Yes	Allow	No	System	Any	Any
Cast to Device streaming server (RTCP-St...	Cast to Device functionality	Private	Yes	Allow	No	%System...	Any	Local
Cast to Device streaming server (RTCP-St...	Cast to Device functionality	Public	Yes	Allow	No	%System...	Any	PlayT
Cast to Device streaming server (RTCP-St...	Cast to Device functionality	Domain	Yes	Allow	No	%System...	Any	Any
Cast to Device streaming server (RTSP-Str...	Cast to Device functionality	Private	Yes	Allow	No	%System...	Any	Local
Cast to Device streaming server (RTSP-Str...	Cast to Device functionality	Domain	Yes	Allow	No	%System...	Any	Any
Cast to Device streaming server (RTSP-Str...	Cast to Device functionality	Public	Yes	Allow	No	%System...	Any	PlayT
Cast to Device UPnP Events (TCP-In)	Cast to Device functionality	Public	Yes	Allow	No	System	Any	PlayT
Connect	Connect	All	Yes	Allow	No	Any	Any	Any

Figure 20: Example of inbound firewall rules

A full list of default enabled firewall rules is included in **Annex B**. Both inbound and outbound rules need to be reviewed urgently, since any open firewall port is a security vulnerability that increases the system's attack surface.

3.7 Lack of accessibility

Enabling accessibility to applications for people with disabilities is a major focus for SITA and Government. Unfortunately every successive version of Windows over the past decade has **decreased** the ability of vision- or movement- impaired users to access all the functions of the OS via the keyboard, for example. Currently very few functions in the general OS UI (mainly Explorer) are still capable of effective keyboard access. Why these regressive changes have been made over time by Microsoft is not clear, given their own stated commitment to inclusion and catering for differently-abled users.

In previous versions of Windows, pull-down menus allowed universal keyboard access via a logical, hierarchical structure that was easily visible in the UI. As menus have disappeared from the UI, keyboard access has either been made less logical, more difficult or has been removed entirely. The old pull-down menus had a simple mnemonic and structured design with built-in keyboard accelerators. Today's Ribbon has lost this functionality, it is organised seemingly at random, and requires long, arbitrary strings of keys to be pressed for keyboard access (where this is even allowed). When comparing the two systems, it is clear just how much poorer the OS is in terms of support for keyboard navigation. The question is why Microsoft deliberately **removed** accessibility from recent versions of products.

A comparison between the Windows 7 and Windows 10 Explorer is illustrated below: notice the logical mnemonic keyboard accelerators, economy of space usage and hierarchy in the older product.

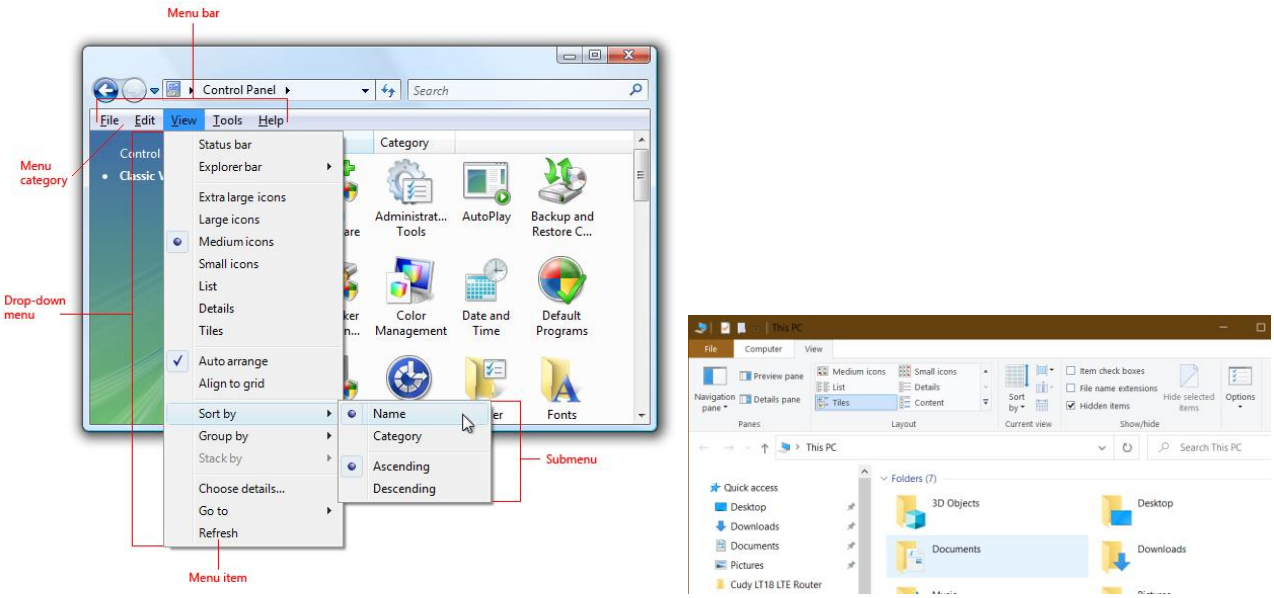


Figure 21: Simplicity of access: Win7 drop-down menu[5] compared to Win10 Ribbon

The old Windows Control Panel was also thoroughly accessible via the keyboard, while its (partial) replacement Settings allows almost **no** keyboard interaction, other than the Search box. Every applet in the Control Panel had keyboard accelerators for most elements (e.g. the Region dialogue below), while Settings has no or very limited keyboard access. To make matters worse, Settings is a monolithic UI that can't be replicated or duplicated like most other windows, so if the user moves to a different area in Settings, existing context is lost immediately.

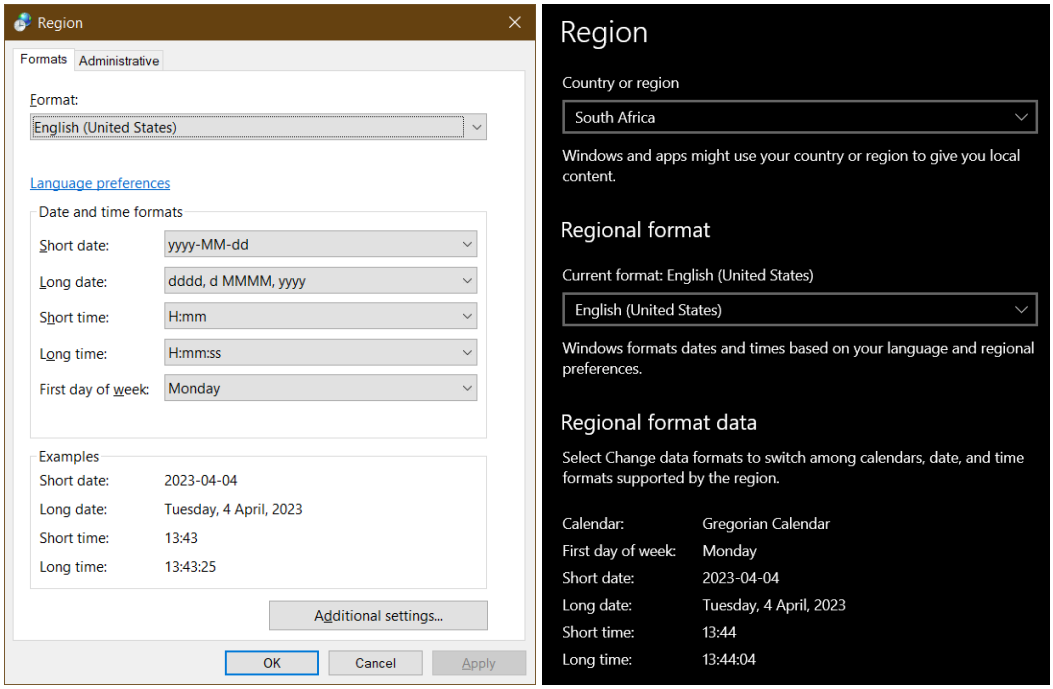


Figure 22: Accessibility in Control Panel vs. Win10 Settings – underlines show keyboard accelerators

[5] Screenshot from Microsoft's *Windows 7 Menus design guide* https://learn.microsoft.com/en-us/windows/win32/uxguide/cmd-menus

3.8 Forced Windows updates and upgrades

Microsoft has a proven track record of forcing its customers to upgrade to the latest OS, largely for the benefit of the vendor – typically there is very limited or no benefit to the end user to adopt a new desktop environment when their requirements, software or business processes have not changed.

A 2016 article by The Verge documents criticisms by the Electronic Freedom Frontier (EFF) on how Windows 10 was forced on users, disregarding choice and privacy concerns.[6] According to an EFF employee the tactics Microsoft employed to get users to upgrade to Windows 10 "went from annoying to downright malicious." Microsoft's upgrade prompts triggered a backlash after the company tweaked its notification to schedule Windows 10 upgrades even after users dismissed the prompt. In one case Microsoft was forced to pay a user $10 000 in damages due to an unwanted upgrade.

How forced upgrades can still be a problem after Windows 10 is a mystery, since Microsoft stated in 2015 that Windows 10 was to be the "last version of Windows". Windows 11 is therefore in the strange position of an OS that should not exist, but yet Windows 10 desktops across the world have been urging their users to upgrade anyway. As with all recent Windows versions, Microsoft uses advertisements, incentives and veiled threats to induce users to upgrade or update their OS, or face (unspecified) dire consequences.[7] In many cases these ads cannot be blocked or bypassed.

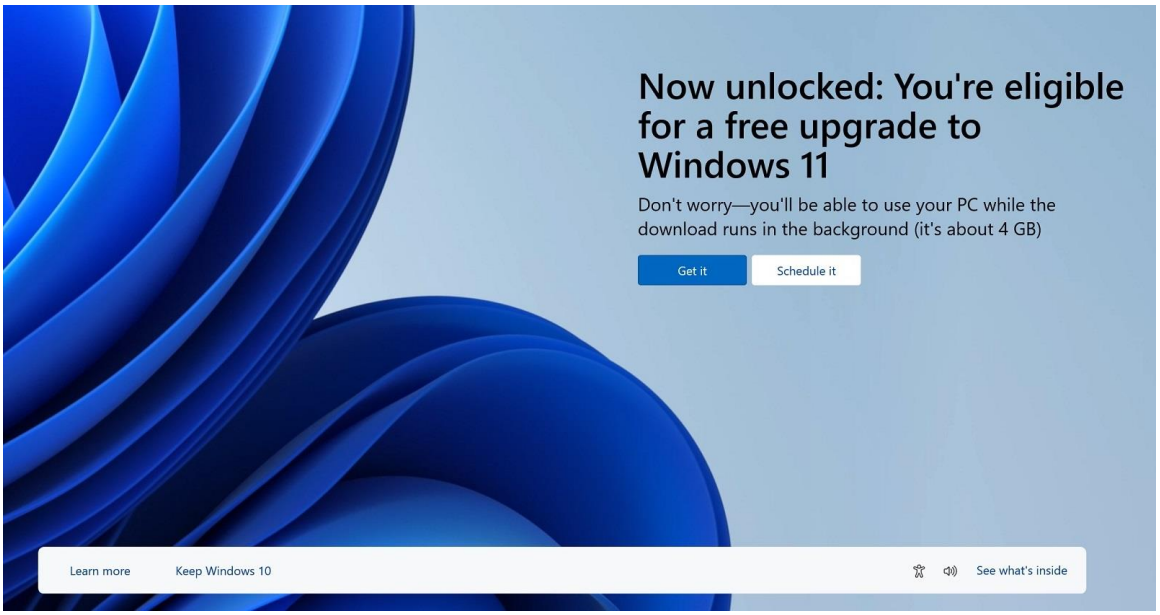


Figure 23: Win11 upgrade advertisement shown to Win10 users

For many end users Windows 11 is not a compelling upgrade, due to decreased performance, increased risk, familiar functionality that was removed, or possible incompatibilities introduced by the new version, whether hardware or software.

In principle TCO is one of the most important factors in any IT environment. A stable desktop platform with minimal disruptions, limited security risks and maximised performance is the holy grail in a world of scarce resources. At least the owner of the desktop hardware should be allowed to have the final say w.r.t. what OS version is allowed to operate within their environment without being forced to upgrade.

While having a fully updated desktop OS is very important, Windows Update needs to be managed at an organisational level, with updates only pushed down to desktops once fully tested and validated. Most

[6] www.theverge.com/2016/8/22/12582622/eff-microsoft-windows-10-privacy-concerns
[7] www.windowslatest.com/2023/05/15/microsoft-bombards-windows-10-users-with-full-screen-windows-11-upgrade-offer-pop-ups

organisations have WSUS or a similar service running to perform updates in an orderly way. What must **not** be allowed is for every individual PC to download its updates whenever most convenient for itself.

The fact that Microsoft forces organisations that use desktop Windows (even those in mission-critical roles) to accept automatic updates without proper testing and validation shows a complete disregard of its responsibilities as an enterprise vendor. Forcing Windows to update itself and reboot without the user being able to stop it is a terrible situation forced on its clients by a vendor that seems to be out of touch with enterprise requirements and processes. How and why businesses and governments worldwide put up with this is a mystery.

An even bigger concern is that Windows updates have in the past **caused** compatibility problems, security vulnerabilities or even data loss, and therefore enterprises simply **cannot** allow Microsoft to determine when the best time is for their desktop OS to be updated.

3.9 User interface issues

To expand on an earlier section about accessibility, Microsoft has made several arbitrary and sub-optimal changes to the Windows UI over time, causing problems for existing users, requiring retraining at best, and a loss of productivity at worst. In our opinion, the removal of pull-down menus in almost all contexts is the best example of this. According to Microsoft's Design Basics training online[8], the following guidelines should be followed:

> *Hide the menu bar instead of removing it completely, because menu bars are more accessible for keyboard users.*
>
> *Don't make a shortcut key the only way to perform a task. Users should also be able to use the mouse or the keyboard with Tab, arrow, and access keys.*

These are older guidelines that seem to have lost favour inside Microsoft, but we believe they should be revived, since. pull-down menus and keyboard access are the most effective UI elements for desktop use.

Other examples of this issue include:

- The mouse right-click function is not supported anymore in "modern" apps. This is a fundamental change for the worse in UI functionality, made to support touch functionality that is not used in 99% of desktops.
- Making needless visual changes to the UI, such as moving the Start Button to the middle of the Task Bar in Windows 11. In Windows 8 Microsoft removed the Start Menu completely, only to have to reverse course in subsequent UI iterations due to customer backlash.
- Removing useful functionality that has been part of Windows for decades, such as being able to change the properties of the Task Bar, changing keyboard support, removing menus.

These UI changes deny users the continuity between product versions needed to maintain or enhance productivity. The changes cause cost increases for organisations due to increased help desk calls and the need for retraining. Even though there are sometimes improvements in functionality, almost every new version of Windows results in a worse UI experience for experienced users. When upgrading to a new version, customers are often forced to trade needed existing functionality for a set of new features that may not be useful to them.

[8] https://learn.microsoft.com/en-us/windows/win32/uxguide/cmd-menus

3.10 Network protocol optimisation

Internet Protocol version 6 (IPv6) is enabled by default on all Windows installations. This protocol is not currently being used in SA Government networks and most corporate environments, since techniques such as NAT have enabled organisations to remain on IPv4 for longer. However, having desktop systems continually attempt communication over IPv6 has an adverse effect on network utilisation.

As stated before, the fundamental configuration principle should be that anything that is not **specifically** needed should be disabled, in order to make more resources available for needed operations. Disabling unneeded protocols and services is even more important from a security perspective.

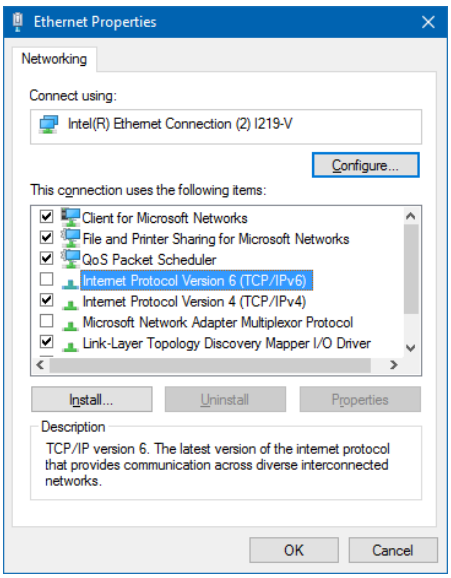


Figure 24: Disable IPv6

4. Windows optimisation process

Optimising desktop Windows should improve performance and security in the following ways:

- Reduce resource footprint (RAM, CPU and storage) by removing or disabling unnecessary Windows components
- Reduce unnecessary communication across the network (especially over the internet) by removing cloud-dependent and consumer-focussed services and applications
- Reduce security vulnerabilities by minimising the attack surface through proper firewall configuration

4.1 Proposed changes

In order to address Windows performance, security and usability issues, the following changes to the Windows default configuration are proposed:

- Uninstall or disable **unnecessary apps** (specifically many consumer-focussed packages such as games and games platforms)
- Disable unused **Windows services** running in the background
- Optimise **firewall rules** to reduce security vulnerabilities and optimise network communication
- Disable unneeded protocols and settings in the **network configuration**
- Disable cloud-dependent services such as **Cortana**
- Disable the **Windows Stor**e
- Manage **Windows updates** properly

5. GITOC request for optimised Windows

In January 2021, TAS directed an official request to Microsoft on behalf of the GITO Council for an optimised version of Windows for use by Government:

> The South African Government is committed to service delivery for the broader community in our country. Computer equipment plays a vital role in assisting citizens. Most of our devices are preloaded with Windows 10.

> Unfortunately, Microsoft appears in some cases to be more focussed on the consumer than they are on the corporate/government user (specifically w.r.t. Windows 10 Professional). This means that Government users often receive devices that appear to be set up for home users or gamers, rather than aimed at government or corporate use.
>
> Government ICT personnel feel that the current builds of Windows 10 hamper service delivery to our citizens due to their emphasis on non-enterprise use cases. Additionally, integration into Microsoft's non-enterprise cloud services is not allowed by our security policy, but with Windows 10 PCs our users usually don't have a choice.
>
> We therefore hereby request Microsoft to provide us with a build of Windows 10 that removes all the unnecessary components, specifically consumer, gaming, telemetry and advertising, that hinder rather than help us in fulfilling our service delivery mandate.

No official response has been received from Microsoft to date, but TAS is of the opinion that Microsoft will earn the gratitude of clients around the world if they granted this request.

6. Conclusion

It would be preferable if Microsoft delivered a version of Windows that can function as a true enterprise-class OS without the gamification, consumer features and security risks. Unfortunately as things stand, Windows users are forced to rectify these issues themselves. In order to achieve this, TAS recommends that organisations such as SITA and Government Departments set up default OS images for Windows with the required optimisations for their end-user computers. These images can then be installed at the OEM factory when a batch of systems is procured to save time and effort when commissioning new systems.

Building an OS image takes significant effort and background knowledge, but a single image can be applied to many devices (dozens or even hundreds), and this has great efficiency benefits over the lifespan of end-user devices. Unfortunately this image must usually be recreated with every Windows update, resulting in a high workload for scarce technical resources.

We trust this report will provide some guidance in configuring Government desktops to a more secure, efficient and effective standard. Any comments, corrections or inputs are welcome, and can be forwarded to TAS for inclusion in future versions of the document.

Note: With Microsoft aggressively pursuing a Software as a Service (SaaS) policy with Windows, the issues listed in this document are a moving target. Some of them may have been resolved since the publication date, or new issues may have been introduced with new Windows updates.

Annex A: List of installed apps: Windows 10

This list was generated on a fresh installation of Windows 10 Pro with the following PowerShell cmdlet:

```
Get-AppxPackage
```

Although some of these are necessary components, please note the large number of apps clearly inappropriate for enterprise environments.

Name
1527c705-839a-4832-9118-54d4Bd6a0c89
c5e2524a-ea46-4f67-841f-6a9465d9d515
E2A4F912-2574-4A75-9BB0-0D023378592B
F46D4000-FD22-4DB4-AC8E-4E1DDDE828FE
Microsoft.3DBuilder
Microsoft.549981C3F5F10
Microsoft.AAD.BrokerPlugin
Microsoft.AccountsControl
Microsoft.Advertising.Xaml
Microsoft.Appconnector
Microsoft.AsyncTextService
Microsoft.BingFinance
Microsoft.BingNews
Microsoft.BingSports
Microsoft.BingWeather
Microsoft.BioEnrollment
Microsoft.CredDialogHost
Microsoft.DesktopAppInstaller
Microsoft.ECApp
Microsoft.GetHelp
Microsoft.Getstarted
Microsoft.HEIFImageExtension
Microsoft.LockApp
Microsoft.Media.PlayReadyClient.2
Microsoft.Microsoft3DViewer
Microsoft.MicrosoftEdge
Microsoft.MicrosoftEdge.Stable
Microsoft.MicrosoftEdgeDevToolsClient
Microsoft.MicrosoftOfficeHub
Microsoft.MicrosoftSolitaireCollection
Microsoft.MicrosoftStickyNotes
Microsoft.MixedReality.Portal
Microsoft.MSPaint
Microsoft.NET.Native.Framework.1.0
Microsoft.NET.Native.Framework.1.3
Microsoft.NET.Native.Framework.1.6
Microsoft.NET.Native.Framework.1.7
Microsoft.NET.Native.Framework.2.2
Microsoft.NET.Native.Runtime.1.0
Microsoft.NET.Native.Runtime.1.3
Microsoft.NET.Native.Runtime.1.4
Microsoft.NET.Native.Runtime.1.6
Microsoft.NET.Native.Runtime.1.7
Microsoft.NET.Native.Runtime.2.2
Microsoft.Office.OneNote
Microsoft.People
Microsoft.ScreenSketch
Microsoft.Services.Store.Engagement
Microsoft.SkypeApp
Microsoft.StorePurchaseApp

Name
Microsoft.VCLibs.110.00
Microsoft.VCLibs.120.00
Microsoft.VCLibs.140.00
Microsoft.VCLibs.140.00.UWPDesktop
Microsoft.VP9VideoExtensions
Microsoft.Wallet
Microsoft.WebMediaExtensions
Microsoft.WebpImageExtension
Microsoft.Win32WebViewHost
Microsoft.Windows.Apprep.ChxApp
Microsoft.Windows.AssignedAccessLockApp
Microsoft.Windows.CallingShellApp
Microsoft.Windows.CapturePicker
Microsoft.Windows.CloudExperienceHost
Microsoft.Windows.ContentDeliveryManager
Microsoft.Windows.NarratorQuickStart
Microsoft.Windows.OOBENetworkCaptivePortal
Microsoft.Windows.OOBENetworkConnectionFlow
Microsoft.Windows.ParentalControls
Microsoft.Windows.PeopleExperienceHost
Microsoft.Windows.Photos
Microsoft.Windows.PinningConfirmationDialog
Microsoft.Windows.Search
Microsoft.Windows.SecHealthUI
Microsoft.Windows.SecureAssessmentBrowser
Microsoft.Windows.ShellExperienceHost
Microsoft.Windows.StartMenuExperienceHost
Microsoft.Windows.XGpuEjectDialog
Microsoft.WindowsAlarms
Microsoft.WindowsAppRuntime.1.3
Microsoft.WindowsCalculator
Microsoft.WindowsCamera
microsoft.windowscommunicationsapps
Microsoft.WindowsFeedbackHub
Microsoft.WindowsMaps
Microsoft.WindowsSoundRecorder
Microsoft.WindowsStore
Microsoft.WinJS.2.0
Microsoft.Xbox.TCUI
Microsoft.XboxApp
Microsoft.XboxGameCallableUI
Microsoft.XboxGameOverlay
Microsoft.XboxGamingOverlay
Microsoft.XboxIdentityProvider
Microsoft.XboxSpeechToTextOverlay
Microsoft.YourPhone
Microsoft.ZuneMusic
Microsoft.ZuneVideo
MicrosoftWindows.Client.CBS
MicrosoftWindows.UndockedDevKit

Name	Name
Microsoft.UI.Xaml.2.0	NcsiUwpApp
Microsoft.UI.Xaml.2.1	Windows.CBSPreview
Microsoft.UI.Xaml.2.3	windows.immersivecontrolpanel
Microsoft.UI.Xaml.2.4	Windows.PrintDialog
Microsoft.UI.Xaml.2.7	
Microsoft.UI.Xaml.2.8	

Table 1: Installed apps, Win10

Annex B: List of default running services, Windows 10

This list was generated on a fresh installation of Windows 10 Pro with the following PowerShell cmdlet:

```
Get-Service | Where-Object {$_.Status -EQ "Running"}
```

Status	Name	DisplayName
Running	Appinfo	Application Information
Running	AppXSvc	AppX Deployment Service (AppXSVC)
Running	AudioEndpointBuilder	Windows Audio Endpoint Builder
Running	Audiosrv	Windows Audio
Running	BFE	Base Filtering Engine
Running	BITS	Background Intelligent Transfer Service
Running	BrokerInfrastructure	Background Tasks Infrastructure Service
Running	camsvc	Capability Access Manager Service
Running	cbdhsvc_3123d	Clipboard User Service_3123d
Running	CDPSvc	Connected Devices Platform Service
Running	CDPUserSvc_3123d	Connected Devices Platform User Service_3123d
Running	CertPropSvc	Certificate Propagation
Running	CoreMessagingRegistrar	CoreMessaging
Running	CryptSvc	Cryptographic Services
Running	DcomLaunch	DCOM Server Process Launcher
Running	Dhcp	DHCP Client
Running	DiagTrack	Connected User Experiences and Telemetry
Running	DispBrokerDesktopSvc	Display Policy Service
Running	Dnscache	DNS Client
Running	DPS	Diagnostic Policy Service
Running	DsSvc	Data Sharing Service
Running	DusmSvc	Data Usage
Running	EventLog	Windows Event Log
Running	EventSystem	COM+ Event System
Running	FontCache	Windows Font Cache Service
Running	gpsvc	Group Policy Client
Running	InstallService	Microsoft Store Install Service
Running	iphlpsvc	IP Helper
Running	KeyIso	CNG Key Isolation
Running	LanmanServer	Server
Running	LanmanWorkstation	Workstation
Running	lfsvc	Geolocation Service
Running	LicenseManager	Windows License Manager Service
Running	lmhosts	TCP/IP NetBIOS Helper
Running	LSM	Local Session Manager
Running	mpssvc	Windows Defender Firewall
Running	NcbService	Network Connection Broker
Running	netprofm	Network List Service
Running	NlaSvc	Network Location Awareness
Running	nsi	Network Store Interface Service
Running	OneSyncSvc_3123d	Sync Host_3123d
Running	PcaSvc	Program Compatibility Assistant Service
Running	PimIndexMaintenanceSvc_3123d	Contact Data_3123d
Running	PlugPlay	Plug and Play
Running	Power	Power
Running	ProfSvc	User Profile Service
Running	RmSvc	Radio Management Service
Running	RpcEptMapper	RPC Endpoint Mapper
Running	RpcSs	Remote Procedure Call (RPC)
Running	SamSs	Security Accounts Manager
Running	ScDeviceEnum	Smart Card Device Enumeration Service
Running	Schedule	Task Scheduler
Running	SecurityHealthService	Windows Security Service
Running	SEMgrSvc	Payments and NFC/SE Manager

Status	Name	DisplayName
Running	SENS	System Event Notification Service
Running	SessionEnv	Remote Desktop Configuration
Running	SgrmBroker	System Guard Runtime Monitor Broker
Running	ShellHWDetection	Shell Hardware Detection
Running	Spooler	Print Spooler
Running	SSDPSRV	SSDP Discovery
Running	StateRepository	State Repository Service
Running	StorSvc	Storage Service
Running	swprv	Microsoft Software Shadow Copy Provider
Running	SysMain	SysMain
Running	SystemEventsBroker	System Events Broker
Running	TabletInputService	Touch Keyboard and Handwriting Panel Service
Running	TermService	Remote Desktop Services
Running	Themes	Themes
Running	TimeBrokerSvc	Time Broker
Running	TokenBroker	Web Account Manager
Running	TrkWks	Distributed Link Tracking Client
Running	UmRdpService	Remote Desktop Services UserMode Port Redirector
Running	UnistoreSvc_3123d	User Data Storage_3123d
Running	UserDataSvc_3123d	User Data Access_3123d
Running	UserManager	User Manager
Running	UsoSvc	Update Orchestrator Service
Running	VaultSvc	Credential Manager
Running	vmicheartbeat	Hyper-V Heartbeat Service
Running	vmickvpexchange	Hyper-V Data Exchange Service
Running	vmicrdv	Hyper-V Remote Desktop Virtualization Service
Running	vmicshutdown	Hyper-V Guest Shutdown Service
Running	vmictimesync	Hyper-V Time Synchronization Service
Running	vmicvss	Hyper-V Volume Shadow Copy Requestor
Running	VSS	Volume Shadow Copy
Running	WaaSMedicSvc	Windows Update Medic Service
Running	Wcmsvc	Windows Connection Manager
Running	WdiServiceHost	Diagnostic Service Host
Running	WdiSystemHost	Diagnostic System Host
Running	WdNisSvc	Microsoft Defender Antivirus Network Inspection Service
Running	WinDefend	Microsoft Defender Antivirus Service
Running	WinHttpAutoProxySvc	WinHTTP Web Proxy Auto-Discovery Service
Running	Winmgmt	Windows Management Instrumentation
Running	WpnService	Windows Push Notifications System Service
Running	WpnUserService_3123d	Windows Push Notifications User Service_3123d
Running	Wscsvc	Security Center
Running	Wsearch	Windows Search

Table 2: Default running services, Win10

Annex C: Inbound firewall rules, Windows 10

According to the well-understood security principle of reducing the attack surface of a computer, 90% of the default Windows firewall rules increase risk significantly. Again, the question needs to be asked why Microsoft allows consumer apps such as Xbox (gaming) and Zune (music) to open ports in the firewall on enterprise desktops. Note also that these are all **inbound** rules, i.e. access is allowed from **outside** the organisation.

This list was generated on a fresh installation of Windows 10 Pro with the following PowerShell cmdlet:

```
Get-NetFirewallRule | out-GridView
```

Firewall Rule Name	Address	Direction	Action
@{Microsoft.AAD.BrokerPlugin_1000.19041.1.0_neutral_neutral_cw5n1h2txyewy ?ms-resource://Microsoft.AAD.BrokerPlugin/resources/PackageDisplayName}	Domain, Private	Inbound	Allow
@{Microsoft.MicrosoftEdge_44.19041.1.0_neutral__8wekyb3d8bbwe?ms-resource://Microsoft.MicrosoftEdge/Resources/AppName}	Domain, Private	Inbound	Allow
@{Microsoft.MicrosoftEdge_44.19041.423.0_neutral__8wekyb3d8bbwe?ms-resource://Microsoft.MicrosoftEdge/Resources/AppName}	Domain, Private	Inbound	Allow
@{Microsoft.Win32WebViewHost_10.0.19041.1_neutral_neutral_cw5n1h2txyewy?ms-resource://Windows.Win32WebViewHost/resources/DisplayName}	Domain, Private, Public	Inbound	Allow
@{Microsoft.Windows.CloudExperienceHost_10.0.10240.16384_neutral_neutral_cw5n1h2txyewy?ms-resource://Microsoft.Windows.CloudExperienceHost/resources/appDescription}	Domain, Private	Inbound	Allow
@{Microsoft.Windows.CloudExperienceHost_10.0.19041.1_neutral_neutral_cw5n1h2txyewy?ms-resource://Microsoft.Windows.CloudExperienceHost/resources/appDescription}	Domain, Private	Inbound	Allow
@{Microsoft.Windows.Search_1.14.0.19041_neutral_neutral_cw5n1h2txyewy?ms-resource://Microsoft.Windows.Search/resources/PackageDisplayName}	Domain, Private	Inbound	Allow
@{Microsoft.Windows.StartMenuExperienceHost_10.0.19041.1_neutral_neutral_cw5n1h2txyewy?ms-resource://Microsoft.Windows.StartMenuExperienceHost/StartMenuExperienceHost/PkgDisplayName}	Domain, Private	Inbound	Allow
@{Windows.ContactSupport_10.0.10240.16384_neutral_neutral_cw5n1h2txyewy ?ms-resource://Windows.ContactSupport/Resources/appDisplayName}	Any	Inbound	Allow
@FirewallAPI.dll,-80200	Any	Inbound	Allow
@FirewallAPI.dll,-80200	Any	Inbound	Allow
3D Builder	Domain, Private	Inbound	Allow
AllJoyn Router	Domain, Private	Inbound	Allow
AllJoyn Router	Domain, Private	Inbound	Allow
App Installer	Domain, Private	Inbound	Allow
BranchCache - Content Retrieval (Uses HTTP)	Any	Inbound	Allow
BranchCache - Hosted Cache Server (Uses HTTPS)	Any	Inbound	Allow
BranchCache - Peer Discovery (Uses WSD)	Any	Inbound	Allow
Cast to Device functionality	Private, Public	Inbound	Allow
Cast to Device functionality	Private, Public	Inbound	Allow
Cast to Device functionality	Public	Inbound	Allow
Cast to Device functionality	Private	Inbound	Allow
Cast to Device functionality	Domain	Inbound	Allow
Cast to Device functionality	Public	Inbound	Allow
Cast to Device functionality	Private	Inbound	Allow
Cast to Device functionality	Domain	Inbound	Allow
Cast to Device functionality	Public	Inbound	Allow
Cast to Device functionality	Private	Inbound	Allow
Cast to Device functionality	Domain	Inbound	Allow
Cast to Device functionality	Public	Inbound	Allow
Cast to Device functionality	Public	Inbound	Allow
Connected Devices Platform	Public	Inbound	Allow
Connected Devices Platform	Domain, Private	Inbound	Allow
Connected Devices Platform	Domain, Private	Inbound	Allow
Core Networking	Any	Inbound	Allow

Firewall Rule Name	Address	Direction	Action
Core Networking	Any	Inbound	Allow
Core Networking	Any	Inbound	Allow
Core Networking	Any	Inbound	Allow
Core Networking	Any	Inbound	Allow
Core Networking	Any	Inbound	Allow
Core Networking	Any	Inbound	Allow
Core Networking	Any	Inbound	Allow
Core Networking	Any	Inbound	Allow
Core Networking	Any	Inbound	Allow
Core Networking	Any	Inbound	Allow
Core Networking	Any	Inbound	Allow
Core Networking	Any	Inbound	Allow
Core Networking	Any	Inbound	Allow
Core Networking	Any	Inbound	Allow
Core Networking	Any	Inbound	Allow
Core Networking	Any	Inbound	Allow
Core Networking	Any	Inbound	Allow
Core Networking	Any	Inbound	Allow
Core Networking Diagnostics	Private, Public	Inbound	Allow
Core Networking Diagnostics	Domain	Inbound	Allow
Core Networking Diagnostics	Private, Public	Inbound	Allow
Core Networking Diagnostics	Domain	Inbound	Allow
Cortana	Domain, Private, Public	Inbound	Allow
Delivery Optimization	Any	Inbound	Allow
Delivery Optimization	Any	Inbound	Allow
Desktop App Web Viewer	Domain, Private, Public	Inbound	Allow
DIAL protocol server	Private	Inbound	Allow
DIAL protocol server	Domain	Inbound	Allow
Distributed Transaction Coordinator	Private, Public	Inbound	Allow
Distributed Transaction Coordinator	Domain	Inbound	Allow
Distributed Transaction Coordinator	Private, Public	Inbound	Allow
Distributed Transaction Coordinator	Domain	Inbound	Allow
Distributed Transaction Coordinator	Private, Public	Inbound	Allow
Distributed Transaction Coordinator	Domain	Inbound	Allow
File and Printer Sharing	Private, Public	Inbound	Allow
File and Printer Sharing	Domain	Inbound	Allow
File and Printer Sharing	Private, Public	Inbound	Allow
File and Printer Sharing	Domain	Inbound	Allow
File and Printer Sharing	Any	Inbound	Allow
File and Printer Sharing	Private, Public	Inbound	Allow
File and Printer Sharing	Domain	Inbound	Allow
File and Printer Sharing	Private, Public	Inbound	Allow
File and Printer Sharing	Domain	Inbound	Allow
File and Printer Sharing	Private, Public	Inbound	Allow
File and Printer Sharing	Domain	Inbound	Allow
File and Printer Sharing	Private, Public	Inbound	Allow
File and Printer Sharing	Domain	Inbound	Allow
File and Printer Sharing	Private, Public	Inbound	Allow
File and Printer Sharing	Domain	Inbound	Allow
File and Printer Sharing	Private, Public	Inbound	Allow
File and Printer Sharing	Domain	Inbound	Allow
File and Printer Sharing over SMBDirect	Any	Inbound	Allow
Get Office	Any	Inbound	Allow
HomeGroup	Private	Inbound	Allow
HomeGroup	Private	Inbound	Allow
Remote Shutdown	Any	Inbound	Allow
Remote Shutdown	Any	Inbound	Allow
iSCSI Service	Private, Public	Inbound	Allow
iSCSI Service	Domain	Inbound	Allow

Firewall Rule Name	Address	Direction	Action
Key Management Service	Private, Public	Inbound	Allow
Key Management Service	Domain	Inbound	Allow
Mail and Calendar	Domain, Private, Public	Inbound	Allow
mDNS	Domain	Inbound	Allow
mDNS	Private	Inbound	Allow
mDNS	Public	Inbound	Allow
Media Center Extenders	Any	Inbound	Allow
Media Center Extenders	Any	Inbound	Allow
Media Center Extenders	Any	Inbound	Allow
Media Center Extenders	Any	Inbound	Allow
Media Center Extenders	Any	Inbound	Allow
Media Center Extenders	Any	Inbound	Allow
Media Center Extenders	Any	Inbound	Allow
Media Center Extenders	Any	Inbound	Allow
Microsoft Edge	Domain, Private	Inbound	Allow
Microsoft Edge	Any	Inbound	Allow
Microsoft Edge WebView2 Runtime	Any	Inbound	Allow
Microsoft Photos	Domain, Private, Public	Inbound	Allow
Microsoft Solitaire Collection	Domain, Private	Inbound	Allow
Microsoft Sticky Notes	Domain, Private	Inbound	Allow
Microsoft Store	Domain, Private, Public	Inbound	Allow
Movies & TV	Domain, Private	Inbound	Allow
MSN Weather	Domain, Private	Inbound	Allow
Netlogon Service	Any	Inbound	Allow
Netlogon Service	Any	Inbound	Allow
Network Discovery	Domain, Public	Inbound	Allow
Network Discovery	Private	Inbound	Allow
Network Discovery	Public	Inbound	Allow
Network Discovery	Private	Inbound	Allow
Network Discovery	Domain	Inbound	Allow
Network Discovery	Public	Inbound	Allow
Network Discovery	Private	Inbound	Allow
Network Discovery	Domain	Inbound	Allow
Network Discovery	Domain, Public	Inbound	Allow
Network Discovery	Private	Inbound	Allow
Network Discovery	Domain, Public	Inbound	Allow
Network Discovery	Private	Inbound	Allow
Network Discovery	Public	Inbound	Allow
Network Discovery	Private	Inbound	Allow
Network Discovery	Domain	Inbound	Allow
Network Discovery	Public	Inbound	Allow
Network Discovery	Private	Inbound	Allow
Network Discovery	Domain	Inbound	Allow
Network Discovery	Public	Inbound	Allow
Network Discovery	Private	Inbound	Allow
Network Discovery	Domain	Inbound	Allow
Network Discovery	Domain, Public	Inbound	Allow
Network Discovery	Private	Inbound	Allow
Network Discovery	Domain, Public	Inbound	Allow
Network Discovery	Private	Inbound	Allow
Network Discovery	Public	Inbound	Allow
Network Discovery	Public	Inbound	Allow
OneNote for Windows 10	Domain, Private	Inbound	Allow
Performance Logs and Alerts	Private, Public	Inbound	Allow
Performance Logs and Alerts	Domain	Inbound	Allow
Performance Logs and Alerts	Private, Public	Inbound	Allow
Performance Logs and Alerts	Domain	Inbound	Allow
Proximity Sharing	Any	Inbound	Allow

Firewall Rule Name	Address	Direction	Action
Remote Assistance	Domain	Inbound	Allow
Remote Assistance	Public	Inbound	Allow
Remote Assistance	Domain, Private	Inbound	Allow
Remote Assistance	Domain	Inbound	Allow
Remote Assistance	Domain, Private	Inbound	Allow
Remote Assistance	Domain, Private	Inbound	Allow
Remote Assistance	Public	Inbound	Allow
Remote Assistance	Domain, Private	Inbound	Allow
Remote Desktop (WebSocket)	Any	Inbound	Allow
Remote Desktop (WebSocket)	Any	Inbound	Allow
Remote Desktop	Any	Inbound	Allow
Remote Desktop	Any	Inbound	Allow
Remote Desktop	Any	Inbound	Allow
Remote Event Log Management	Private, Public	Inbound	Allow
Remote Event Log Management	Domain	Inbound	Allow
Remote Event Log Management	Private, Public	Inbound	Allow
Remote Event Log Management	Domain	Inbound	Allow
Remote Event Log Management	Private, Public	Inbound	Allow
Remote Event Log Management	Domain	Inbound	Allow
Remote Event Monitor	Any	Inbound	Allow
Remote Event Monitor	Any	Inbound	Allow
Remote Scheduled Tasks Management	Private, Public	Inbound	Allow
Remote Scheduled Tasks Management	Domain	Inbound	Allow
Remote Scheduled Tasks Management	Private, Public	Inbound	Allow
Remote Scheduled Tasks Management	Domain	Inbound	Allow
Remote Service Management	Private, Public	Inbound	Allow
Remote Service Management	Domain	Inbound	Allow
Remote Service Management	Private, Public	Inbound	Allow
Remote Service Management	Domain	Inbound	Allow
Remote Service Management	Private, Public	Inbound	Allow
Remote Service Management	Domain	Inbound	Allow
Remote Volume Management	Private, Public	Inbound	Allow
Remote Volume Management	Domain	Inbound	Allow
Remote Volume Management	Private, Public	Inbound	Allow
Remote Volume Management	Domain	Inbound	Allow
Remote Volume Management	Private, Public	Inbound	Allow
Remote Volume Management	Domain	Inbound	Allow
Routing and Remote Access	Any	Inbound	Allow
Routing and Remote Access	Any	Inbound	Allow
Routing and Remote Access	Any	Inbound	Allow
Secure Socket Tunneling Protocol	Any	Inbound	Allow
{78E1CD88-49E3-476E-B926-580E596AD309}	Any	Inbound	Allow
{78E1CD88-49E3-476E-B926-580E596AD309}	Any	Inbound	Allow
Skype	Domain, Private	Inbound	Allow
SNMP Trap	Private, Public	Inbound	Allow
SNMP Trap	Domain	Inbound	Allow
Solitaire & Casual Games	Domain, Private	Inbound	Allow
Start	Domain, Private	Inbound	Allow
TPM Virtual Smart Card Management	Private, Public	Inbound	Allow
TPM Virtual Smart Card Management	Domain	Inbound	Allow
TPM Virtual Smart Card Management	Private, Public	Inbound	Allow
TPM Virtual Smart Card Management	Domain	Inbound	Allow
Virtual Machine Monitoring	Any	Inbound	Allow
Virtual Machine Monitoring	Any	Inbound	Allow
Virtual Machine Monitoring	Any	Inbound	Allow
Virtual Machine Monitoring	Any	Inbound	Allow
Virtual Machine Monitoring	Any	Inbound	Allow
WLAN Service - WFD Application Services Platform Coordination Protocol (Uses UDP)	Any	Inbound	Allow
WLAN Service - WFD Services Kernel Mode Driver Rules	Any	Inbound	Allow
WLAN Service - WFD Services Kernel Mode Driver Rules	Any	Inbound	Allow

Firewall Rule Name	Address	Direction	Action
Wi-Fi Direct Network Discovery	Public	Inbound	Allow
Wi-Fi Direct Network Discovery	Public	Inbound	Allow
Wi-Fi Direct Network Discovery	Public	Inbound	Allow
Windows Clock	Domain, Private	Inbound	Allow
Windows Collaboration Computer Name Registration Service	Any	Inbound	Allow
Windows Collaboration Computer Name Registration Service	Any	Inbound	Allow
Windows Defender Firewall Remote Management	Private, Public	Inbound	Allow
Windows Defender Firewall Remote Management	Domain	Inbound	Allow
Windows Defender Firewall Remote Management	Private, Public	Inbound	Allow
Windows Defender Firewall Remote Management	Domain	Inbound	Allow
Windows Management Instrumentation (WMI)	Private, Public	Inbound	Allow
Windows Management Instrumentation (WMI)	Domain	Inbound	Allow
Windows Management Instrumentation (WMI)	Private, Public	Inbound	Allow
Windows Management Instrumentation (WMI)	Domain	Inbound	Allow
Windows Management Instrumentation (WMI)	Private, Public	Inbound	Allow
Windows Management Instrumentation (WMI)	Domain	Inbound	Allow
Windows Media Player	Domain, Private	Inbound	Allow
Windows Media Player	Any	Inbound	Allow
Windows Media Player Network Sharing Service	Private, Public	Inbound	Allow
Windows Media Player Network Sharing Service	Domain	Inbound	Allow
Windows Media Player Network Sharing Service	Private, Public	Inbound	Allow
Windows Media Player Network Sharing Service	Domain	Inbound	Allow
Windows Media Player Network Sharing Service	Private, Public	Inbound	Allow
Windows Media Player Network Sharing Service	Domain	Inbound	Allow
Windows Media Player Network Sharing Service	Any	Inbound	Allow
Windows Media Player Network Sharing Service	Private, Public	Inbound	Allow
Windows Media Player Network Sharing Service	Domain	Inbound	Allow
Windows Media Player Network Sharing Service	Private, Public	Inbound	Allow
Windows Media Player Network Sharing Service	Domain	Inbound	Allow
Windows Media Player Network Sharing Service	Private, Public	Inbound	Allow
Windows Media Player Network Sharing Service	Domain	Inbound	Allow
Windows Media Player Network Sharing Service	Any	Inbound	Allow
Windows Media Player	Any	Inbound	Allow
Windows Peer to Peer Collaboration Foundation	Any	Inbound	Allow
Windows Peer to Peer Collaboration Foundation	Any	Inbound	Allow
Windows Peer to Peer Collaboration Foundation	Any	Inbound	Allow
Windows Peer to Peer Collaboration Foundation	Any	Inbound	Allow
Windows Remote Management (Compatibility)	Private, Public	Inbound	Allow
Windows Remote Management (Compatibility)	Domain	Inbound	Allow
Windows Remote Management	Public	Inbound	Allow
Windows Remote Management	Domain, Private	Inbound	Allow
Windows Search	Domain, Private	Inbound	Allow
Windows Security	Domain, Private	Inbound	Allow
Wireless Display	Any	Inbound	Allow
Wireless Display	Any	Inbound	Allow
Wireless Portable Devices	Any	Inbound	Allow
Wireless Portable Devices	Any	Inbound	Allow
Work or school account	Domain, Private	Inbound	Allow
Xbox Console Companion	Domain, Private, Public	Inbound	Allow
Xbox Game Bar	Domain, Private, Public	Inbound	Allow
Your account	Domain, Private	Inbound	Allow

Table 3: Inbound firewall rules, Win10

Annex D: List of installed apps: Windows 11

This list was generated on a fresh installation of Windows 11 Pro with the following PowerShell cmdlet:

```
Get-AppxPackage
```

Although some of these are necessary components, please note the large number of apps clearly inappropriate for enterprise environments.

Name	Name
1527c705-839a-4832-9118-54d4Bd6a0c89	Microsoft.UI.Xaml.2.8
c5e2524a-ea46-4f67-841f-6a9465d9d515	Microsoft.UI.Xaml.CBS
Clipchamp.Clipchamp	Microsoft.VCLibs.140.00
E2A4F912-2574-4A75-9BB0-0D023378592B	Microsoft.VCLibs.140.00
F46D4000-FD22-4DB4-AC8E-4E1DDDE828FE	Microsoft.VCLibs.140.00.UWPDesktop
Microsoft.549981C3F5F10	Microsoft.VCLibs.140.00.UWPDesktop
Microsoft.AAD.BrokerPlugin	Microsoft.VP9VideoExtensions
Microsoft.AccountsControl	Microsoft.WebMediaExtensions
Microsoft.AsyncTextService	Microsoft.WebpImageExtension
Microsoft.BingNews	Microsoft.Win32WebViewHost
Microsoft.BingWeather	Microsoft.Windows.Apprep.ChxApp
Microsoft.BioEnrollment	Microsoft.Windows.AssignedAccessLockApp
Microsoft.CredDialogHost	Microsoft.Windows.CallingShellApp
Microsoft.DesktopAppInstaller	Microsoft.Windows.CapturePicker
Microsoft.ECApp	Microsoft.Windows.CloudExperienceHost
Microsoft.GamingApp	Microsoft.Windows.ContentDeliveryManager
Microsoft.GetHelp	Microsoft.Windows.NarratorQuickStart
Microsoft.Getstarted	Microsoft.Windows.OOBENetworkCaptivePortal
Microsoft.HEIFImageExtension	Microsoft.Windows.OOBENetworkConnectionFlow
Microsoft.HEVCVideoExtension	Microsoft.Windows.ParentalControls
Microsoft.LockApp	Microsoft.Windows.PeopleExperienceHost
Microsoft.MicrosoftEdge	Microsoft.Windows.Photos
Microsoft.MicrosoftEdge.Stable	Microsoft.Windows.PinningConfirmationDialog
Microsoft.MicrosoftEdgeDevToolsClient	Microsoft.Windows.PrintQueueActionCenter
Microsoft.MicrosoftOfficeHub	Microsoft.Windows.SecureAssessmentBrowser
Microsoft.MicrosoftSolitaireCollection	Microsoft.Windows.ShellExperienceHost
Microsoft.MicrosoftStickyNotes	Microsoft.Windows.StartMenuExperienceHost
Microsoft.NET.Native.Framework.2.2	Microsoft.Windows.XGpuEjectDialog
Microsoft.NET.Native.Framework.2.2	Microsoft.WindowsAlarms
Microsoft.NET.Native.Runtime.2.2	Microsoft.WindowsCalculator
Microsoft.NET.Native.Runtime.2.2	Microsoft.WindowsCamera
Microsoft.Paint	microsoft.windowscommunicationsapps
Microsoft.People	Microsoft.WindowsFeedbackHub
Microsoft.PowerAutomateDesktop	Microsoft.WindowsMaps
Microsoft.RawImageExtension	Microsoft.WindowsNotepad
Microsoft.ScreenSketch	Microsoft.WindowsSoundRecorder
Microsoft.SecHealthUI	Microsoft.WindowsStore
Microsoft.Services.Store.Engagement	Microsoft.WindowsTerminal
Microsoft.Services.Store.Engagement	Microsoft.Xbox.TCUI
Microsoft.StorePurchaseApp	Microsoft.XboxGameCallableUI
Microsoft.Todos	Microsoft.XboxGameOverlay
Microsoft.UI.Xaml.2.4	Microsoft.XboxGamingOverlay
Microsoft.UI.Xaml.2.7	

Table 4: Installed apps, Win11

Annex E: List of default running services, Windows 11

As with Windows 10, the sheer number of running services in Windows 11 shows a complete lack of concern for security and performances on the part of Microsoft.

This list was generated on a fresh installation of Windows 11 Pro with the following PowerShell cmdlet:

```
Get-Service | Where-Object {$_.Status -EQ "Running"}.
```

Status	Name	DisplayName
Running	AMD Crash Defender Service	AMD Crash Defender Service
Running	AMD External Events Utility	AMD External Events Utility
Running	AppIDSvc	Application Identity
Running	Appinfo	Application Information
Running	AppReadiness	App Readiness
Running	AppXSvc	AppX Deployment Service (AppXSVC)
Running	AudioEndpointBuilder	Windows Audio Endpoint Builder
Running	Audiosrv	Windows Audio
Running	BFE	Base Filtering Engine
Running	BITS	Background Intelligent Transfer Service
Running	BrokerInfrastructure	Background Tasks Infrastructure Service
Running	BthAvctpSvc	AVCTP service
Running	camsvc	Capability Access Manager Service
Running	cbdhsvc_1ef6f0	Clipboard User Service_1ef6f0
Running	CDPSvc	Connected Devices Platform Service
Running	CDPUserSvc_1ef6f0	Connected Devices Platform User Service_1ef6f0
Running	ClipSVC	Client License Service (ClipSVC)
Running	CoreMessagingRegistrar	CoreMessaging
Running	CryptSvc	Cryptographic Services
Running	DcomLaunch	DCOM Server Process Launcher
Running	DeviceInstall	Device Install Service
Running	Dhcp	DHCP Client
Running	DiagTrack	Connected User Experiences and Telemetry
Running	DispBrokerDesktopSvc	Display Policy Service
Running	DisplayEnhancementService	Display Enhancement Service
Running	Dnscache	DNS Client
Running	DoSvc	Delivery Optimization
Running	DPS	Diagnostic Policy Service
Running	DusmSvc	Data Usage
Running	EventLog	Windows Event Log
Running	EventSystem	COM+ Event System
Running	fhsvc	File History Service
Running	FontCache	Windows Font Cache Service
Running	hidserv	Human Interface Device Service
Running	InstallService	Microsoft Store Install Service
Running	iphlpsvc	IP Helper
Running	KeyIso	CNG Key Isolation
Running	LanmanServer	Server
Running	LanmanWorkstation	Workstation
Running	lfsvc	Geolocation Service
Running	LicenseManager	Windows License Manager Service
Running	lmhosts	TCP/IP NetBIOS Helper
Running	LSM	Local Session Manager
Running	mpssvc	Windows Defender Firewall
Running	NcbService	Network Connection Broker
Running	netprofm	Network List Service
Running	NPSMSvc_1ef6f0	NPSMSvc_1ef6f0
Running	nsi	Network Store Interface Service
Running	OneSyncSvc_1ef6f0	Sync Host_1ef6f0
Running	PcaSvc	Program Compatibility Assistant Service

Status	Name	DisplayName
Running	PlugPlay	Plug and Play
Running	Power	Power
Running	ProfSvc	User Profile Service
Running	RmSvc	Radio Management Service
Running	RpcEptMapper	RPC Endpoint Mapper
Running	RpcSs	Remote Procedure Call (RPC)
Running	SamSs	Security Accounts Manager
Running	Schedule	Task Scheduler
Running	SDRSVC	Windows Backup
Running	SecurityHealthService	Windows Security Service
Running	SENS	System Event Notification Service
Running	SgrmBroker	System Guard Runtime Monitor Broker
Running	ShellHWDetection	Shell Hardware Detection
Running	Spooler	Print Spooler
Running	SSDPSRV	SSDP Discovery
Running	StateRepository	State Repository Service
Running	StorSvc	Storage Service
Running	SysMain	SysMain
Running	SystemEventsBroker	System Events Broker
Running	TextInputManagementService	Text Input Management Service
Running	Themes	Themes
Running	TimeBrokerSvc	Time Broker
Running	TokenBroker	Web Account Manager
Running	TrkWks	Distributed Link Tracking Client
Running	UdkUserSvc_1ef6f0	Udk User Service_1ef6f0
Running	UserManager	User Manager
Running	UsoSvc	Update Orchestrator Service
Running	VaultSvc	Credential Manager
Running	W32Time	Windows Time
Running	WaaSMedicSvc	WaaSMedicSvc
Running	Wcmsvc	Windows Connection Manager
Running	WdiSystemHost	Diagnostic System Host
Running	WdNisSvc	Microsoft Defender Antivirus Network Inspection Service
Running	webthreatdefsvc	Web Threat Defense Service
Running	webthreatdefusersvc_1ef6f0	Web Threat Defense User Service_1ef6f0
Running	WinDefend	Microsoft Defender Antivirus Service
Running	WinHttpAutoProxySvc	WinHTTP Web Proxy Auto-Discovery Service
Running	Winmgmt	Windows Management Instrumentation
Running	wlidsvc	Microsoft Account Sign-in Assistant
Running	WpnService	Windows Push Notifications System Service
Running	WpnUserService_1ef6f0	Windows Push Notifications User Service_1ef6f0
Running	wscsvc	Security Center
Running	WSearch	Windows Search
Running	wuauserv	Windows Update

Table 5: Default running services, Win11

Annex F: Firewall rules, Windows 11

As with Windows 10, the sheer number of allowed (i.e. open) firewall (and specifically more than 200 **inbound**) connections in Windows 11 shows a complete lack of concern for security on the part of Microsoft.

This list was generated on a fresh installation of Windows 11 Pro with the following PowerShell cmdlet:

```
Get-NetFirewallRule | out-GridView
```

Firewall Rule Name	Address	Direction	Action
AllJoyn Router (TCP-In)	Domain, Private	Inbound	Allow
AllJoyn Router (UDP-In)	Domain, Private	Inbound	Allow
App Installer	Domain, Private	Inbound	Allow
BranchCache Content Retrieval (HTTP-In)	Any	Inbound	Allow
BranchCache Hosted Cache Server (HTTP-In)	Any	Inbound	Allow
BranchCache Peer Discovery (WSD-In)	Any	Inbound	Allow
Cast to Device functionality (qWave-TCP-In)	Private, Public	Inbound	Allow
Cast to Device functionality (qWave-UDP-In)	Private, Public	Inbound	Allow
Cast to Device SSDP Discovery (UDP-In)	Public	Inbound	Allow
Cast to Device streaming server (HTTP-Streaming-In)	Private	Inbound	Allow
Cast to Device streaming server (HTTP-Streaming-In)	Domain	Inbound	Allow
Cast to Device streaming server (HTTP-Streaming-In)	Public	Inbound	Allow
Cast to Device streaming server (RTCP-Streaming-In)	Private	Inbound	Allow
Cast to Device streaming server (RTCP-Streaming-In)	Domain	Inbound	Allow
Cast to Device streaming server (RTCP-Streaming-In)	Public	Inbound	Allow
Cast to Device streaming server (RTSP-Streaming-In)	Private	Inbound	Allow
Cast to Device streaming server (RTSP-Streaming-In)	Domain	Inbound	Allow
Cast to Device streaming server (RTSP-Streaming-In)	Public	Inbound	Allow
Cast to Device UPnP Events (TCP-In)	Public	Inbound	Allow
Connected Devices Platform - Wi-Fi Direct Transport (TCP-In)	Public	Inbound	Allow
Connected Devices Platform (TCP-In)	Domain, Private	Inbound	Allow
Connected Devices Platform (UDP-In)	Domain, Private	Inbound	Allow
Core Networking - Destination Unreachable (ICMPv6-In)	Any	Inbound	Allow
Core Networking - Destination Unreachable Fragmentation Needed (ICMPv4-In)	Any	Inbound	Allow
Core Networking - Dynamic Host Configuration Protocol (DHCP-In)	Any	Inbound	Allow
Core Networking - Dynamic Host Configuration Protocol for IPv6(DHCPV6-In)	Any	Inbound	Allow
Core Networking - Internet Group Management Protocol (IGMP-In)	Any	Inbound	Allow
Core Networking - IPHTTPS (TCP-In)	Any	Inbound	Allow
Core Networking - IPv6 (IPv6-In)	Any	Inbound	Allow
Core Networking - Multicast Listener Done (ICMPv6-In)	Any	Inbound	Allow
Core Networking - Multicast Listener Query (ICMPv6-In)	Any	Inbound	Allow
Core Networking - Multicast Listener Report (ICMPv6-In)	Any	Inbound	Allow
Core Networking - Multicast Listener Report v2 (ICMPv6-In)	Any	Inbound	Allow
Core Networking - Neighbor Discovery Advertisement (ICMPv6-In)	Any	Inbound	Allow
Core Networking - Neighbor Discovery Solicitation (ICMPv6-In)	Any	Inbound	Allow
Core Networking - Packet Too Big (ICMPv6-In)	Any	Inbound	Allow
Core Networking - Parameter Problem (ICMPv6-In)	Any	Inbound	Allow
Core Networking - Router Advertisement (ICMPv6-In)	Any	Inbound	Allow
Core Networking - Router Solicitation (ICMPv6-In)	Any	Inbound	Allow
Core Networking - Teredo (UDP-In)	Any	Inbound	Allow
Core Networking - Time Exceeded (ICMPv6-In)	Any	Inbound	Allow
Core Networking Diagnostics - ICMP Echo Request (ICMPv4-In)	Private, Public	Inbound	Allow
Core Networking Diagnostics - ICMP Echo Request (ICMPv4-In)	Domain	Inbound	Allow
Core Networking Diagnostics - ICMP Echo Request (ICMPv6-In)	Private, Public	Inbound	Allow
Core Networking Diagnostics - ICMP Echo Request (ICMPv6-In)	Domain	Inbound	Allow
Cortana	Domain, Private, Public	Inbound	Allow
Delivery Optimization (TCP-In)	Any	Inbound	Allow
Delivery Optimization (UDP-In)	Any	Inbound	Allow
Desktop App Web Viewer	Domain, Private, Public	Inbound	Allow
DIAL protocol server (HTTP-In)	Private	Inbound	Allow

Firewall Rule Name	Address	Direction	Action
DIAL protocol server (HTTP-In)	Domain	Inbound	Allow
Distributed Transaction Coordinator (RPC)	Private, Public	Inbound	Allow
Distributed Transaction Coordinator (RPC)	Domain	Inbound	Allow
Distributed Transaction Coordinator (RPC-EPMAP)	Private, Public	Inbound	Allow
Distributed Transaction Coordinator (RPC-EPMAP)	Domain	Inbound	Allow
Distributed Transaction Coordinator (TCP-In)	Private, Public	Inbound	Allow
Distributed Transaction Coordinator (TCP-In)	Domain	Inbound	Allow
File and Printer Sharing (Echo Request - ICMPv4-In)	Private, Public	Inbound	Allow
File and Printer Sharing (Echo Request - ICMPv4-In)	Domain	Inbound	Allow
File and Printer Sharing (Echo Request - ICMPv6-In)	Private, Public	Inbound	Allow
File and Printer Sharing (Echo Request - ICMPv6-In)	Domain	Inbound	Allow
File and Printer Sharing (LLMNR-UDP-In)	Any	Inbound	Allow
File and Printer Sharing (NB-Datagram-In)	Private, Public	Inbound	Allow
File and Printer Sharing (NB-Datagram-In)	Domain	Inbound	Allow
File and Printer Sharing (NB-Name-In)	Private, Public	Inbound	Allow
File and Printer Sharing (NB-Name-In)	Domain	Inbound	Allow
File and Printer Sharing (NB-Session-In)	Private, Public	Inbound	Allow
File and Printer Sharing (NB-Session-In)	Domain	Inbound	Allow
File and Printer Sharing (SMB-In)	Private, Public	Inbound	Allow
File and Printer Sharing (SMB-In)	Domain	Inbound	Allow
File and Printer Sharing (Spooler Service - RPC)	Private, Public	Inbound	Allow
File and Printer Sharing (Spooler Service - RPC)	Domain	Inbound	Allow
File and Printer Sharing (Spooler Service - RPC-EPMAP)	Private, Public	Inbound	Allow
File and Printer Sharing (Spooler Service - RPC-EPMAP)	Domain	Inbound	Allow
File and Printer Sharing over SMBDirect (iWARP-In)	Any	Inbound	Allow
Inbound Rule for Remote Shutdown (RPC-EP-In)	Any	Inbound	Allow
Inbound Rule for Remote Shutdown (TCP-In)	Any	Inbound	Allow
iSCSI Service (TCP-In)	Private, Public	Inbound	Allow
iSCSI Service (TCP-In)	Domain	Inbound	Allow
Key Management Service (TCP-In)	Private, Public	Inbound	Allow
Key Management Service (TCP-In)	Domain	Inbound	Allow
Mail and Calendar	Domain, Private, Public	Inbound	Allow
mDNS (UDP-In)	Domain	Inbound	Allow
mDNS (UDP-In)	Private	Inbound	Allow
mDNS (UDP-In)	Public	Inbound	Allow
Media Center Extenders - HTTP Streaming (TCP-In)	Any	Inbound	Allow
Media Center Extenders - Media Streaming (TCP-In)	Any	Inbound	Allow
Media Center Extenders - qWave (TCP-In)	Any	Inbound	Allow
Media Center Extenders - qWave (UDP-In)	Any	Inbound	Allow
Media Center Extenders - RTSP (TCP-In)	Any	Inbound	Allow
Media Center Extenders - SSDP (UDP-In)	Any	Inbound	Allow
Media Center Extenders - WMDRM-ND/RTP/RTCP (UDP-In)	Any	Inbound	Allow
Media Center Extenders - XSP (TCP-In)	Any	Inbound	Allow
Microsoft Edge	Domain, Private	Inbound	Allow
Microsoft Edge (mDNS-In)	Any	Inbound	Allow
Microsoft Edge (mDNS-In)	Any	Inbound	Allow
Microsoft Media Foundation Network Source IN [TCP 554]	Any	Inbound	Allow
Microsoft Media Foundation Network Source IN [UDP 5004-5009]	Any	Inbound	Allow
Microsoft Solitaire Collection	Domain, Private	Inbound	Allow
Microsoft Store	Domain, Private, Public	Inbound	Allow
Microsoft Teams	Any	Inbound	Allow
Microsoft Teams	Any	Inbound	Allow
Microsoft To Do	Domain, Private	Inbound	Allow
Movies & TV	Domain, Private	Inbound	Allow
Netlogon Service (NP-In)	Any	Inbound	Allow
Netlogon Service Authz (RPC)	Any	Inbound	Allow
Network Discovery (LLMNR-UDP-In)	Domain, Public	Inbound	Allow
Network Discovery (LLMNR-UDP-In)	Private	Inbound	Allow
Network Discovery (NB-Datagram-In)	Public	Inbound	Allow
Network Discovery (NB-Datagram-In)	Private	Inbound	Allow
Network Discovery (NB-Datagram-In)	Domain	Inbound	Allow

Firewall Rule Name	Address	Direction	Action
Network Discovery (NB-Name-In)	Public	Inbound	Allow
Network Discovery (NB-Name-In)	Private	Inbound	Allow
Network Discovery (NB-Name-In)	Domain	Inbound	Allow
Network Discovery (Pub-WSD-In)	Domain, Public	Inbound	Allow
Network Discovery (Pub-WSD-In)	Private	Inbound	Allow
Network Discovery (SSDP-In)	Domain, Public	Inbound	Allow
Network Discovery (SSDP-In)	Private	Inbound	Allow
Network Discovery (UPnP-In)	Public	Inbound	Allow
Network Discovery (UPnP-In)	Private	Inbound	Allow
Network Discovery (UPnP-In)	Domain	Inbound	Allow
Network Discovery (WSD Events-In)	Public	Inbound	Allow
Network Discovery (WSD Events-In)	Private	Inbound	Allow
Network Discovery (WSD Events-In)	Domain	Inbound	Allow
Network Discovery (WSD EventsSecure-In)	Public	Inbound	Allow
Network Discovery (WSD EventsSecure-In)	Private	Inbound	Allow
Network Discovery (WSD EventsSecure-In)	Domain	Inbound	Allow
Network Discovery (WSD-In)	Domain, Public	Inbound	Allow
Network Discovery (WSD-In)	Private	Inbound	Allow
Network Discovery (WSD-In)	Domain, Public	Inbound	Allow
Network Discovery (WSD-In)	Private	Inbound	Allow
Network Discovery for Teredo (SSDP-In)	Public	Inbound	Allow
Network Discovery for Teredo (UPnP-In)	Public	Inbound	Allow
Performance Logs and Alerts (DCOM-In)	Private, Public	Inbound	Allow
Performance Logs and Alerts (DCOM-In)	Domain	Inbound	Allow
Performance Logs and Alerts (TCP-In)	Private, Public	Inbound	Allow
Performance Logs and Alerts (TCP-In)	Domain	Inbound	Allow
Proximity sharing over TCP (TCP sharing-In)	Any	Inbound	Allow
Remote Assistance (DCOM-In)	Domain	Inbound	Allow
Remote Assistance (PNRP-In)	Public	Inbound	Allow
Remote Assistance (PNRP-In)	Domain, Private	Inbound	Allow
Remote Assistance (RA Server TCP-In)	Domain	Inbound	Allow
Remote Assistance (SSDP TCP-In)	Domain, Private	Inbound	Allow
Remote Assistance (SSDP UDP-In)	Domain, Private	Inbound	Allow
Remote Assistance (TCP-In)	Public	Inbound	Allow
Remote Assistance (TCP-In)	Domain, Private	Inbound	Allow
Remote Desktop - (TCP-WS-In)	Any	Inbound	Allow
Remote Desktop - (TCP-WSS-In)	Any	Inbound	Allow
Remote Desktop - Shadow (TCP-In)	Any	Inbound	Allow
Remote Desktop - User Mode (TCP-In)	Any	Inbound	Allow
Remote Desktop - User Mode (UDP-In)	Any	Inbound	Allow
Remote Event Log Management (NP-In)	Private, Public	Inbound	Allow
Remote Event Log Management (NP-In)	Domain	Inbound	Allow
Remote Event Log Management (RPC)	Private, Public	Inbound	Allow
Remote Event Log Management (RPC)	Domain	Inbound	Allow
Remote Event Log Management (RPC-EPMAP)	Private, Public	Inbound	Allow
Remote Event Log Management (RPC-EPMAP)	Domain	Inbound	Allow
Remote Event Monitor (RPC)	Any	Inbound	Allow
Remote Event Monitor (RPC-EPMAP)	Any	Inbound	Allow
Remote Scheduled Tasks Management (RPC)	Private, Public	Inbound	Allow
Remote Scheduled Tasks Management (RPC)	Domain	Inbound	Allow
Remote Scheduled Tasks Management (RPC-EPMAP)	Private, Public	Inbound	Allow
Remote Scheduled Tasks Management (RPC-EPMAP)	Domain	Inbound	Allow
Remote Service Management (NP-In)	Private, Public	Inbound	Allow
Remote Service Management (NP-In)	Domain	Inbound	Allow
Remote Service Management (RPC)	Private, Public	Inbound	Allow
Remote Service Management (RPC)	Domain	Inbound	Allow
Remote Service Management (RPC-EPMAP)	Private, Public	Inbound	Allow
Remote Service Management (RPC-EPMAP)	Domain	Inbound	Allow
Remote Volume Management - Virtual Disk Service (RPC)	Private, Public	Inbound	Allow
Remote Volume Management - Virtual Disk Service (RPC)	Domain	Inbound	Allow
Remote Volume Management - Virtual Disk Service Loader (RPC)	Private, Public	Inbound	Allow

Firewall Rule Name	Address	Direction	Action
Remote Volume Management - Virtual Disk Service Loader (RPC)	Domain	Inbound	Allow
Remote Volume Management (RPC-EPMAP)	Private, Public	Inbound	Allow
Remote Volume Management (RPC-EPMAP)	Domain	Inbound	Allow
Routing and Remote Access (GRE-In)	Any	Inbound	Allow
Routing and Remote Access (L2TP-In)	Any	Inbound	Allow
Routing and Remote Access (PPTP-In)	Any	Inbound	Allow
Secure Socket Tunneling Protocol (SSTP-In)	Any	Inbound	Allow
SNMP Trap Service (UDP In)	Private, Public	Inbound	Allow
SNMP Trap Service (UDP In)	Domain	Inbound	Allow
Start	Domain, Private	Inbound	Allow
TPM Virtual Smart Card Management (DCOM-In)	Private, Public	Inbound	Allow
TPM Virtual Smart Card Management (DCOM-In)	Domain	Inbound	Allow
TPM Virtual Smart Card Management (TCP-In)	Private, Public	Inbound	Allow
TPM Virtual Smart Card Management (TCP-In)	Domain	Inbound	Allow
Virtual Machine Monitoring (DCOM-In)	Any	Inbound	Allow
Virtual Machine Monitoring (Echo Request - ICMPv4-In)	Any	Inbound	Allow
Virtual Machine Monitoring (Echo Request - ICMPv6-In)	Any	Inbound	Allow
Virtual Machine Monitoring (NB-Session-In)	Any	Inbound	Allow
Virtual Machine Monitoring (RPC)	Any	Inbound	Allow
WFD ASP Coordination Protocol (UDP-In)	Any	Inbound	Allow
WFD Driver-only (TCP-In)	Any	Inbound	Allow
WFD Driver-only (UDP-In)	Any	Inbound	Allow
Wi-Fi Direct Network Discovery (In)	Public	Inbound	Allow
Wi-Fi Direct Scan Service Use (In)	Public	Inbound	Allow
Wi-Fi Direct Spooler Use (In)	Public	Inbound	Allow
Windows Collaboration Computer Name Registration Service (PNRP-In)	Any	Inbound	Allow
Windows Collaboration Computer Name Registration Service (SSDP-In)	Any	Inbound	Allow
Windows Defender Firewall Remote Management (RPC)	Private, Public	Inbound	Allow
Windows Defender Firewall Remote Management (RPC)	Domain	Inbound	Allow
Windows Defender Firewall Remote Management (RPC-EPMAP)	Private, Public	Inbound	Allow
Windows Defender Firewall Remote Management (RPC-EPMAP)	Domain	Inbound	Allow
Windows Feature Experience Pack	Domain, Private	Inbound	Allow
Windows Feature Experience Pack	Domain, Private	Inbound	Allow
Windows Management Instrumentation (ASync-In)	Private, Public	Inbound	Allow
Windows Management Instrumentation (ASync-In)	Domain	Inbound	Allow
Windows Management Instrumentation (DCOM-In)	Private, Public	Inbound	Allow
Windows Management Instrumentation (DCOM-In)	Domain	Inbound	Allow
Windows Management Instrumentation (WMI-In)	Private, Public	Inbound	Allow
Windows Management Instrumentation (WMI-In)	Domain	Inbound	Allow
Windows Media Player	Domain, Private	Inbound	Allow
Windows Media Player (UDP-In)	Any	Inbound	Allow
Windows Media Player Network Sharing Service (HTTP-Streaming-In)	Private, Public	Inbound	Allow
Windows Media Player Network Sharing Service (HTTP-Streaming-In)	Domain	Inbound	Allow
Windows Media Player Network Sharing Service (qWave-TCP-In)	Private, Public	Inbound	Allow
Windows Media Player Network Sharing Service (qWave-TCP-In)	Domain	Inbound	Allow
Windows Media Player Network Sharing Service (qWave-UDP-In)	Private, Public	Inbound	Allow
Windows Media Player Network Sharing Service (qWave-UDP-In)	Domain	Inbound	Allow
Windows Media Player Network Sharing Service (SSDP-In)	Any	Inbound	Allow
Windows Media Player Network Sharing Service (Streaming-UDP-In)	Private, Public	Inbound	Allow
Windows Media Player Network Sharing Service (Streaming-UDP-In)	Domain	Inbound	Allow
Windows Media Player Network Sharing Service (TCP-In)	Private, Public	Inbound	Allow
Windows Media Player Network Sharing Service (TCP-In)	Domain	Inbound	Allow
Windows Media Player Network Sharing Service (UDP-In)	Private, Public	Inbound	Allow
Windows Media Player Network Sharing Service (UDP-In)	Domain	Inbound	Allow
Windows Media Player Network Sharing Service (UPnP-In)	Any	Inbound	Allow
Windows Media Player x86 (UDP-In)	Any	Inbound	Allow
Windows Peer to Peer Collaboration Foundation (PNRP-In)	Any	Inbound	Allow
Windows Peer to Peer Collaboration Foundation (SSDP-In)	Any	Inbound	Allow
Windows Peer to Peer Collaboration Foundation (TCP-In)	Any	Inbound	Allow
Windows Peer to Peer Collaboration Foundation (WSD-In)	Any	Inbound	Allow
Windows Remote Management - Compatibility Mode (HTTP-In)	Private, Public	Inbound	Allow

Firewall Rule Name	Address	Direction	Action
Windows Remote Management - Compatibility Mode (HTTP-In)	Domain	Inbound	Allow
Windows Remote Management (HTTP-In)	Public	Inbound	Allow
Windows Remote Management (HTTP-In)	Domain, Private	Inbound	Allow
Windows Security	Domain, Private	Inbound	Allow
Wireless Display (TCP-In)	Any	Inbound	Allow
Wireless Display Infrastructure Back Channel (TCP-In)	Any	Inbound	Allow
Wireless Portable Devices (SSDP-In)	Any	Inbound	Allow
Wireless Portable Devices (UPnP-In)	Any	Inbound	Allow
Work or school account	Domain, Private	Inbound	Allow
Xbox Game Bar	Domain, Private, Public	Inbound	Allow
Your account	Domain, Private	Inbound	Allow

Table 6: Inbound firewall rules, Win11

Annex G: Abbreviations, Terms and Definitions

CPU	Central Processing Unit
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Services
GITOC	Government IT Officers Council
GUI	Graphical user interface
ICT	Information and Communications Technology
HTML	Hypertext Markup Language
IpvX	Internet Protocol version (e.g. IPv6)
ISO	International Standards Organisation
ISV	Independent Software Vendor
ICT	Information and Communications Technology
IT	Information Technology
LAN	Local Area Network
MIOS	Minimum Interoperability Standards
MISS	Minimum Information Security Standards
MTBF	Mean Time Before Failure: measured for entire system with all mandatory components
MTTR	Mean Time To Repair: measured with engineer on-site with spares in-hand; swap-out of components are acceptable
NAT	Network Address Translation
OEM	Original Equipment Manufacturer
OS	Operating system
RAM	Random Access Memory
SCM	Supply Chain Management
SITA	State Information Technology Agency
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
TAS	Technology Advisory Services
TCO	Total Cost of Ownership: all costs associated with an ICT solution, including capital, labour, services, running costs, etc.
TCP/IP	Transmission Control Protocol/Internet Protocol
TTT	Technical Task Team, a sub-committee of the GITOC SCProc.
UI	User interface
USB	Universal Serial Bus
WAN	Wide Area Network
WiFi	Wireless LAN (IEEE 802.11)
WLAN	Wireless LAN (IEEE 802.11)
WSUS	Windows Server Update Services