Ryerson University | Computing & Communications Services

Windows 10 Security and Policy Settings

Due to many changes Microsoft has made in Windows 10, users are encouraged to adopt some recommended settings to increase security and privacy.

It requires a higher level of computing knowledge than Windows 7 to change these settings. It is strongly recommended that you have CCS or your departmental IT make these changes to your Windows 10 computer. If you decide to make these changes yourself, please follow these settings carefully (If you are running a different or older version of Windows 10, you may not see some of the settings listed below.):

Group Policies & Registry Settings

1. To turn off **Let apps use advertising ID** to make ads more interesting to you based on your app usage (turning this off will reset your ID) use **one** of the following methods:

    a. Navigate to **Computer Configuration > Administrative Templates > System > User Profiles > Turn off the advertising ID** and set it to **Enabled**

    b. Navigate to **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\AdvertisingInfo** and set your registry values to:
    Name: Enabled
    Data: 0 (zero)
    Type: REG_DWORD

2. To turn off **Let websites provide locally relevant content by accessing my language list.** You will need to login with **each user** separately to make this change.

    a. Navigate to **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\AdvertisingInfo** and set your registry values to:
    Name: HttpAcceptLanguageOptOut
    Data: 1 (one)
    Type: REG_DWORD

3. In the **Feedback & Diagnostics** area, you can choose how often you are asked for feedback and how much diagnostic and usage information is sent to Microsoft.
   This modifies the Feedback policy, use **one** of the following methods:

   a. Navigate to **Computer Configuration > Administrative Templates > Windows Components > Data Collection and Preview Builds > Do not show feedback notifications** and set it to **Enabled**

   b. Navigate to **HKEY_LOCAL_MACHINE\Policies \Microsoft\Windows\DataCollection** and set your registry values to:
   Name: DoNotShowFeedbackNotifications
   Data: 1 (one)
   Type: REG_DWORD

4. This modifies the **Diagnostic and usage data policy**, use **one** of the following methods:

   a. Navigate to **Computer Configuration > Administrative Templates > Windows Components > Data Collection And Preview Builds > Allow Telemetry** and set it to **Enabled.** Under options, select “0 - Security [Enterprise Only].”

   b. Navigate to **HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\DataCollection** and set your registry values to:
   Name: Allow Telemetry
   Data: 0 (zero)
   Type: REG_DWORD

5. To **Disable Autoplay** complete **all** of the following:

   a. Navigate to **Computer Configuration > Administrative Templates > Windows Components > AutoPlay Policies** and set it to **Enabled.**

   b. Navigate to **Computer Configuration > Administrative Templates > Windows Components > Disallow AutoPlay for non-volume devices** and set it to **Enabled.**

   c. Navigate to **Computer Configuration > Administrative Templates > Windows Components > Set the default behavior for Autorun** and set it to **Enabled.** For Default Autorun Behavior, select “Do not execute any autorun commands”

6. To **Prevent Enabling Lock Screen Camera** complete the following:

    a. Navigate to **Computer Configuration > Administrative Templates > Control Panel > Personalization > Prevent enabling lock screen camera** and set it to **Enabled.**

7. **Microsoft Edge** settings, complete the following:

    a. Navigate to **Computer Configuration > Administrative Templates > Windows Components > Microsoft Edge > Configure Password Manager** and set it to **Disabled.**

    b. Navigate to **Computer Configuration > Administrative Templates > Windows Components > Microsoft Edge > Configure SmartScreen Filter** and set it to **Enabled.**

    c. Navigate to **Computer Configuration > Administrative Templates > Windows Components > Microsoft Edge > Configure Cookies** and set it to **Enabled.** Set Configure Cookies option to “Block 3rd-party cookie.”

8. To disable the feature that allows **Remote Desktop Connection Client** to save passwords

    a. Navigate to **Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Connection Client > Do not allow passwords to be saved** and set it to **Enabled.**

9. Disable the feature that signs in the last interactive user after a system restart,

    a. Navigate to **Computer Configuration > Administrative Templates > Windows Components > Windows Logon Options > Sign-in last interactive user automatically after a system-initiated restart** and set it to **Disabled.**

10. To set Group policy for Windows updates,

    a. Navigate to **Computer Configuration > Administrative Templates > Windows Components > Delivery Optimization > Download Mode** and set it to **Enabled.** For Download Mode, select “HTTP only”

Privacy Settings

From the Start menu, select **Settings** then select **Privacy**

Location	Recommended Settings
General	Turn off all options except for Turn on SmartScreen Filter to check web content (URLs) that Windows Store apps use.
Location	Turn off all listed apps and turn off the General location option.
Camera	Set Let apps use my camera to On and for Choose apps that can use your camera to On, for Microsoft Edge, and OneNote.
Microphone	Set Let apps use my microphone to On and Choose apps that can use your microphone to On, for Microsoft Edge, OneNote and Voice Recorder
Notifications	Set Let apps access to my notification to On.
Speech, inking and typing	Strongly suggest that you do not use this feature as info goes to Microsoft.
Account info	Set Let apps access my name, picture and other account info to Off.
Contacts	Set Let apps access my contacts to Off.
Calendar	Set Let apps access my calendar to On. Turn off all apps, except for Windows.
Call History	Set Let apps access my call history to Off.
Email	Set Let apps access and send email to Off.
Messaging	Set Let apps read or send messages (text or MMS) to Off.
Radios	Set Let apps read or send messages (text or MMS) to Off.
Other Devices	Set Sync with devices to Off.
Background Apps	Allow the following apps to run in the background; Alarms & Clock, Microsoft Edge, Settings.

Microsoft Provisioned Apps

Do not use and uninstall **Microsoft Mail client and Calendar** as items are made public.

Other provisioned apps and features that should be uninstalled are:

- Get Office, Get Skype, Get Started, Windows Insider Hub, Microsoft WiFi, Bing Finance, Bing Sports, Movies & TV, Music, People, Phone, Phone Companion, CandyCrush Soda Saga, Twitter & Xbox.

** Please note: Many of the above Apps/Features cannot be uninstalled in the normal manner and Powershell scripts must be used to remove them.