Windows 10 Enterprise UIT Security Recommended Settings

In Windows 10, Microsoft has implemented several features that are designed to increase the personalization of the user experience. Many of these features require information to be sent from the user's computer to Microsoft servers for analysis. While the University of Houston does not have a specific policy yet for Windows 10 configurations, the following recommendations should be followed to minimize the risk of exposure to sensitive University data and to bring Windows 10 computers into best alignment with SAM 07.A.08 – Data Classification and Protection.

This document applies to:

- All University-owned desktops, laptops, and mobile devices that are running Windows 10.
- All personally-owned desktops, laptops, and mobile devices that are running Windows 10 and that either store or manipulate Level One data as defined by SAM 07.A.08.

UIT Security Recommends that the only version of Windows 10 used on University-owned devices is Windows 10 Enterprise. Windows 10 Home and Windows 10 Professional do not have all of the desired configuration settings.

This document is broken up according to three distinct system types and configurations:

- University-owned devices managed in an Active Directory environment (i.e Cougarnet).
- University-owned devices managed as standalone systems.
- Personally-owned devices for which a department's IT support does not have authority.

University-owned Devices Managed in an Cougarnet Environment

System Administrators should consider setting the follow settings as detailed in group policy objects assigned to their Organizational Units in Active Directory for domain-managed computers. It assumes that the Windows 10 Administrative Templates have been added to the domain. (These have been added in Cougarnet.)

As some policy names are phrased in the positive (e.g. "Turn On") and others in the negative (e.g. "Turn Off") take care to make sure that the appropriate value (e.g. "enabled" or "disabled") is chosen to get the desired effect.

For all of the settings listed below, the root is Computer Configuration > Policies. It is important to edit GPOs on a Windows 10 computer, otherwise all of these setting may not be seen.

Policy Name	Location	UH Recommended Setting	Description
Allow Cortana	Administrative Templates > Windows Components > Search	Disabled	Turns off Cortana, which transmits a wide and varied amount of user data to Microsoft.
Allow Telemetry	Administrative Templates > Windows Components > Data Collection and Preview Builds	Enabled Set Options to "0 – Off [Enterprise Only]"	Turns off reporting of system usage to Microsoft. (The setting of Enabled is not a misprint.)
Turn Off Application Telemetry	Administrative Templates > Windows Components > Application Compatibility	Enabled	Turns off reporting of application usage to Microsoft.
Allow Input Personalization	Administrative Templates > Control Panel > Regional and Language Options	Disabled	Turns off remote analysis of typing history, contacts, calendar, and e-mail information.
Turn Off Picture Password Sign-In	Administrative Templates > System > Logon	Enabled	Picture-based logons are not complaint with UH Policy.
Turn on PIN Sign-on	Administrative Templates > System > Logon	Disabled	For domain-joined computers, PIN sign-on is not possible. For other computers, it is recommended that PIN sign-on be disabled to restrict users from choosing essentially what is a short password.
Turn Off Advertising ID	Administrative Templates > System > User Profiles	Enabled	Should be turned off to better protect user privacy, unless a user explicitly requests the functionality be enabled.
Use Microsoft Passport for Work	Administrative Templates > Windows Components > Microsoft Passport for Work	Disabled	As UH does not yet have a policy covering the use of biometrics and PINs for authentication, this feature should be disabled.

Accounts: Block Microsoft Accounts	Windows Settings > Security Settings > Local Policies > Security Options	Select the "Define this policy setting" and then choose "Users can't add or log on with Microsoft Accounts"	Personal Microsoft accounts should not be used to store University data.

In Group Policy, two important Windows 10 settings are managed by editing registry preferences. For *domain-joined* computers (i.e. computers in Cougarnet) this may be done by using a Registry Preference file. For those not comfortable or familiar with registry preferences in Group Policy, the same may be done by pushing out *.REG files. Below are the keys.

Registry Values			
Download Mode	Preferences > Windows Settings > Registry	ACTION: Replace KEY: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DeliveryOptimization VALUE NAME: DODownloadMode VALUE TYPE: REG_DWORD VALUE DATA: 0 (For Group Policy Registry Preference deployment only: On the Common tab, check "Remove this item when it is no longer applied")	Disables peer-to-peer updating of Windows Updates to prevent issues with inappropriate use of State of Texas equipment.
WIFI Sense	Preferences > Windows Settings > Registry	ACTION: Replace KEY: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WcmSvc\wifinetworkmanager\config\ VALUE NAME: AutoConnectAllowedOEM VALUE TYPE: REG_DWORD VALUE DATA: 0	Disables WIFI Sense.

University-owned Devices Managed Outside of an Active Directory Environment

For computers not joined to a domain (i.e. not members of Cougarnet), system administrators should set the settings in the computer's Local Security Policy. All policy settings are under the Computer Configuration. Run gpedit.msc to access them.

As some policy names are phrased in the positive (e.g. "Turn On") and others in the negative (e.g. "Turn Off") take care to make sure that the appropriate value (e.g. "enabled" or "disabled") is chosen to get the desired effect.

The root of all of the settings is Computer Configuration.

Policy Name	Location	UH Recommended Setting	Description
Allow Cortana	Administrative Templates > Windows Components > Search	Disabled	Turns off Cortana, which transmits a wide and varied amount of user data to Microsoft.
Allow Telemetry	Administrative Templates > Windows Components > Data Collection and Preview Builds	Enabled Set Options to "0 – Off [Enterprise Only]"	Turns off reporting of system usage to Microsoft. (The setting of Enabled is not a misprint.)
Turn Off Application Telemetry	Administrative Templates > Windows Components > Application Compatibility	Enabled	Turns off reporting of application usage to Microsoft.
Allow Input Personalization	Administrative Templates > Control Panel > Regional and Language Options	Disabled	Turns off remote analysis of typing history, contacts, calendar, and e-mail information.
Turn Off Picture Password Sign-In	Administrative Templates > System > Logon	Enabled	Picture-based logons are not complaint with UH Policy.
Turn on PIN Sign-on	Administrative Templates > System > Logon	Disabled	For domain-joined computers, PIN sign-on is not possible. For other computers, it is recommended that PIN sign-on be disabled to restrict users from choosing essentially what is a short password.
Turn Off Advertising ID	Administrative Templates > System > User Profiles	Enabled	Should be turned off to better protect user privacy, unless a user explicitly requests the functionality be enabled.
Use Microsoft Passport for Work	Administrative Templates > Windows Components > Microsoft Passport for Work	Disabled	As UH does not yet have a policy covering the use of biometrics and PINs for authentication, this feature should be disabled.
Accounts: Block Microsoft Accounts	Windows Settings > Security Settings > Local Policies > Security Options	Choose "Users can't add or log on with Microsoft Accounts"	Personal Microsoft accounts should not be used to store University data.

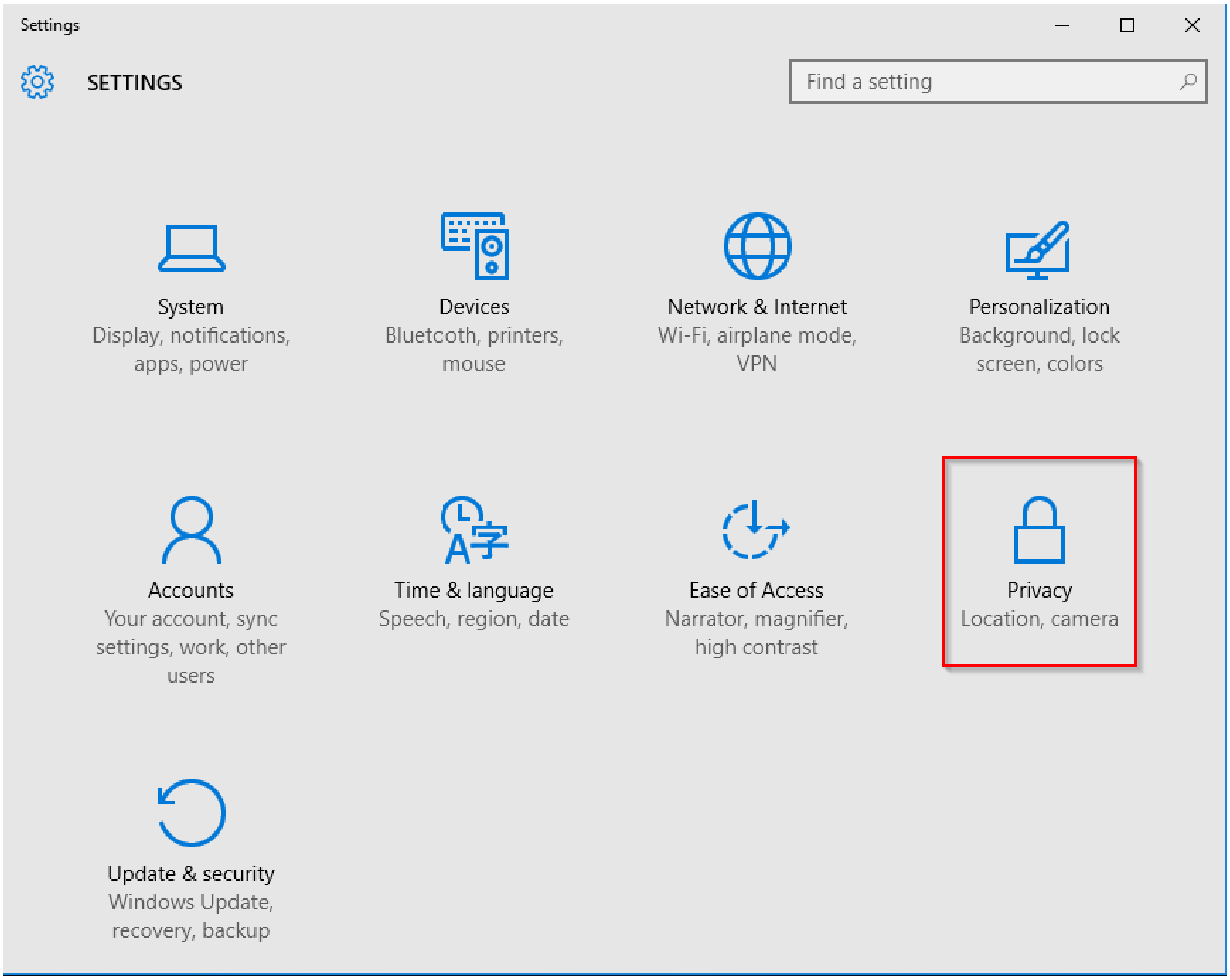
Two important Windows 10 settings are managed by editing the registry. For *non-domain joined* computers this must be done by running individual *.REG files or editing the registry directly on the computer itself. Below are the keys.

Registry Values			
Download Mode	Preferences > Windows Settings > Registry	KEY: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DeliveryOptimization NAME: DODownloadMode DATA: 0 TYPE: DWORD	Disables peer-to-peer updating of Windows Updates to prevent issues with inappropriate use of State of Texas equipment.
WIFI Sense	Preferences > Windows Settings > Registry	KEY: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WcmSvc\wifinetworkmanager\config\ NAME: AutoConnectAllowedOEM DATA: 0 TYPE: DWORD	Disables WIFI Sense.

Recommendations for Personally-Owned Devices

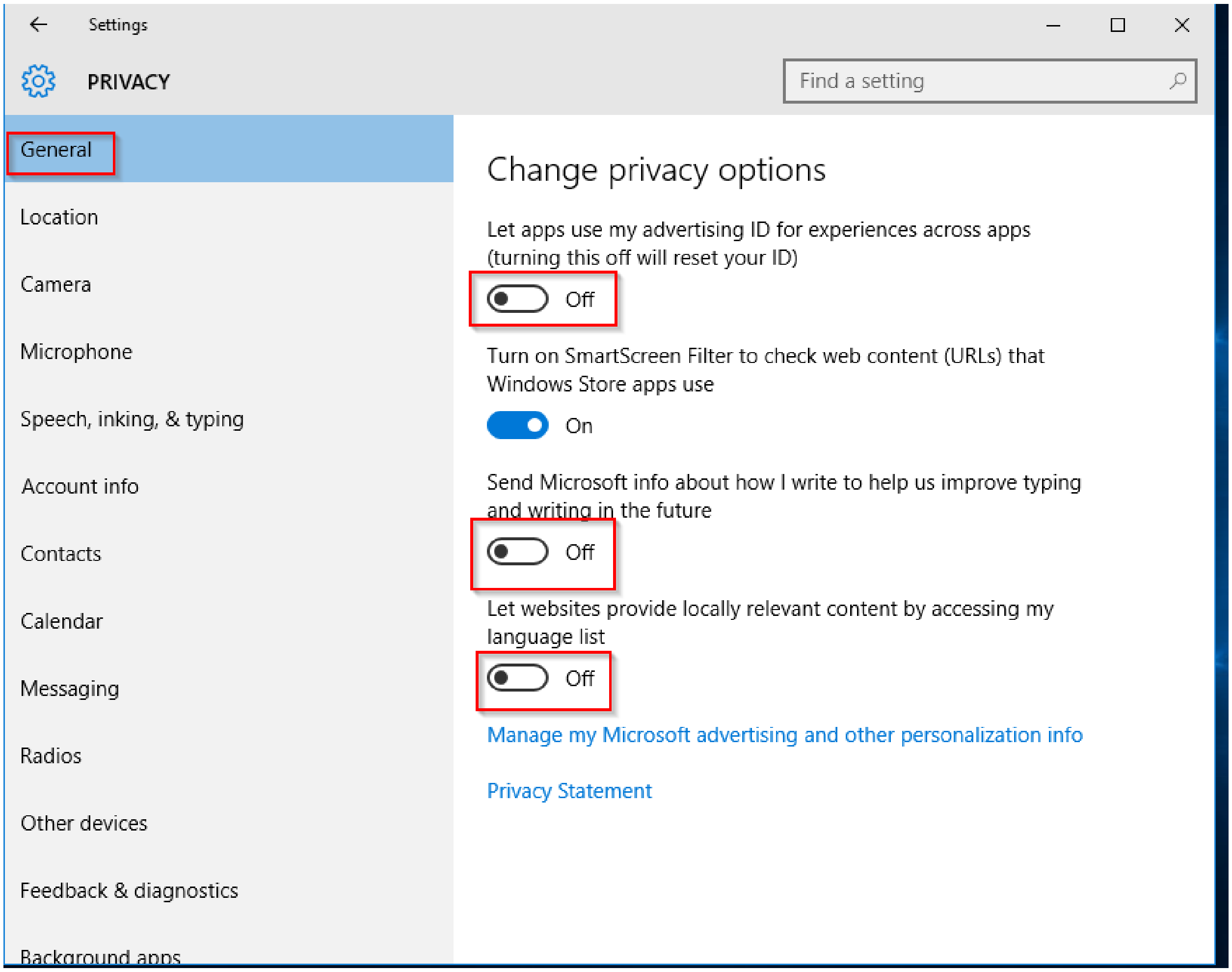
For personally-owned devices, below are the procedures for enacting most of UIT Security's recommendations via the graphical user interface.

From the Start menu, click on Settings, then choose Privacy:


Settings
SETTINGS
Find a setting
System
Display, notifications, apps, power
Devices
Bluetooth, printers, mouse
Network & Internet
Wi-Fi, airplane mode, VPN
Personalization
Background, lock screen, colors
Accounts
Your account, sync settings, work, other users
Time & language
Speech, region, date
Ease of Access
Narrator, magnifier, high contrast
Privacy
Location, camera
Update & security
Windows Update, recovery, backup

Select General. Turn Off:

- Let apps use my advertising ID for experiences across apps
- Send Microsoft info about how I write to help us improve typing and writing in the future
- Let websites provide locally relevant content by accessing my language list



Change privacy options

Let apps use my advertising ID for experiences across apps (turning this off will reset your ID)

Off

Turn on SmartScreen Filter to check web content (URLs) that Windows Store apps use

On

Send Microsoft info about how I write to help us improve typing and writing in the future

Off

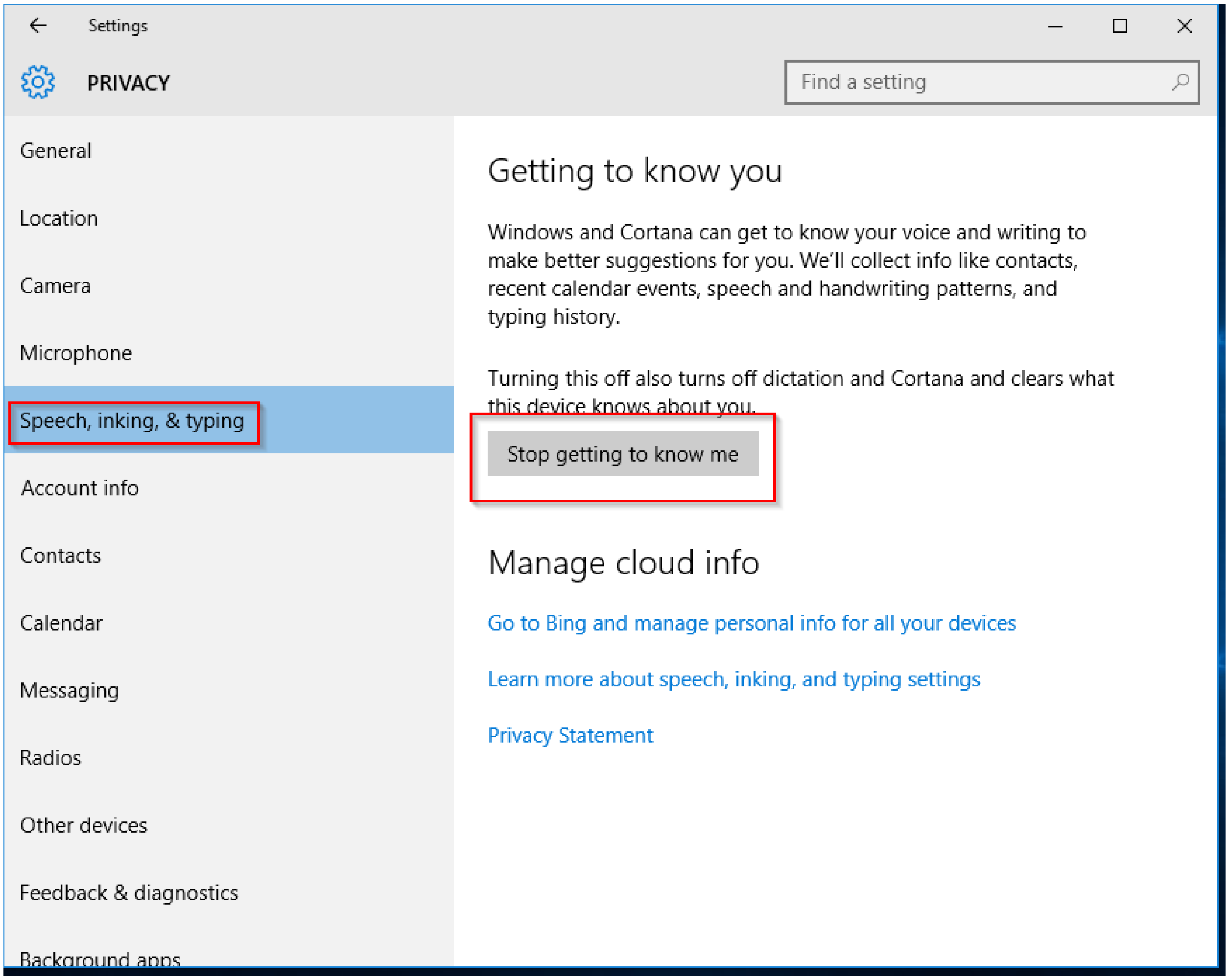
Let websites provide locally relevant content by accessing my language list

Off

Manage my Microsoft advertising and other personalization info

Privacy Statement

Select Speech, inking and, typing. If the Getting to Know You button reads Stop Getting to Know Me, select it to turn off Cortana and associated features:



Getting to know you

Windows and Cortana can get to know your voice and writing to make better suggestions for you. We'll collect info like contacts, recent calendar events, speech and handwriting patterns, and typing history.

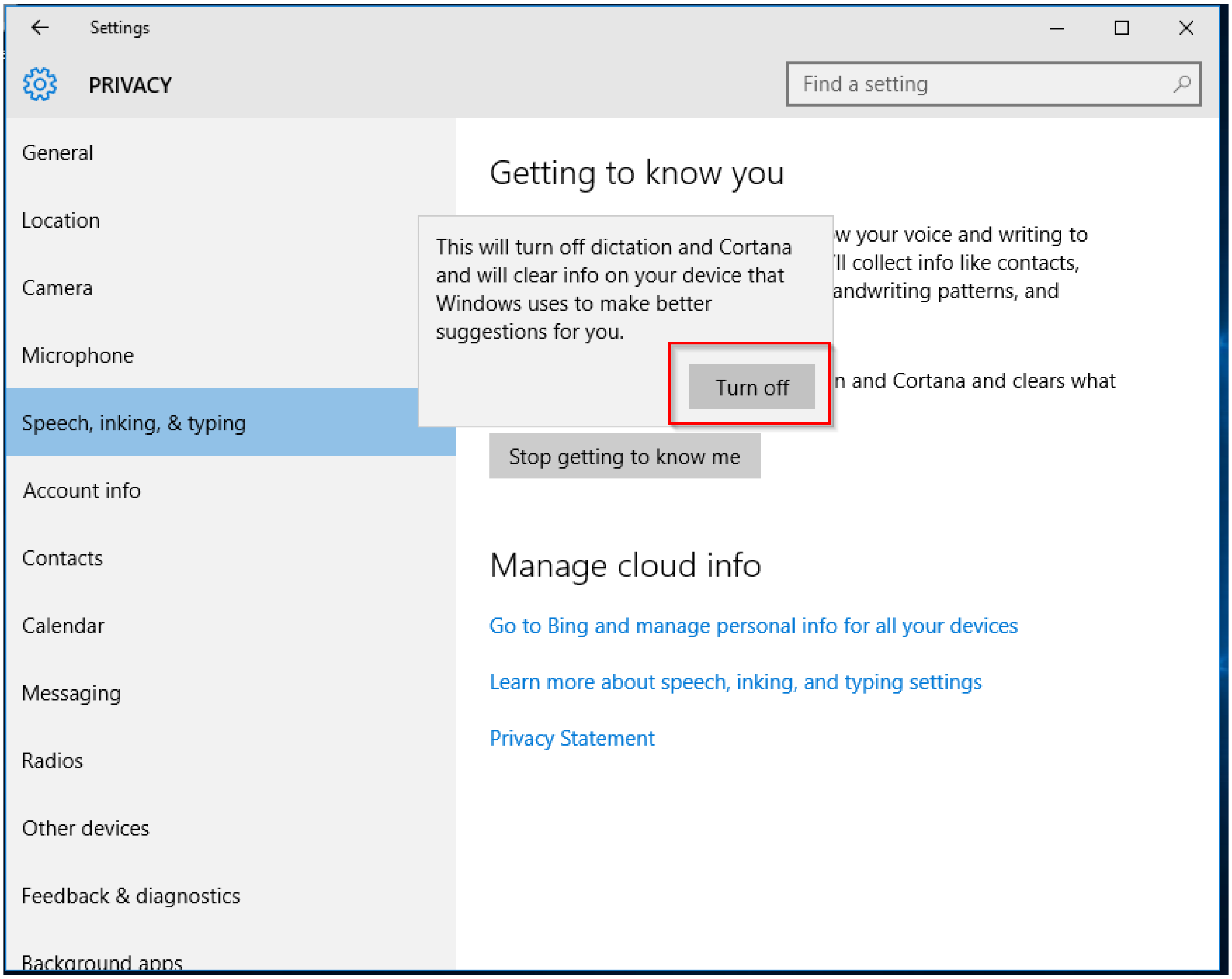
Turning this off also turns off dictation and Cortana and clears what this device knows about you.

Manage cloud info

Go to Bing and manage personal info for all your devices

Learn more about speech, inking, and typing settings

Privacy Statement



Getting to know you

This will turn off dictation and Cortana and will clear info on your device that Windows uses to make better suggestions for you.

Turn off

w your voice and writing to 'll collect info like contacts, andwriting patterns, and

n and Cortana and clears what

Stop getting to know me

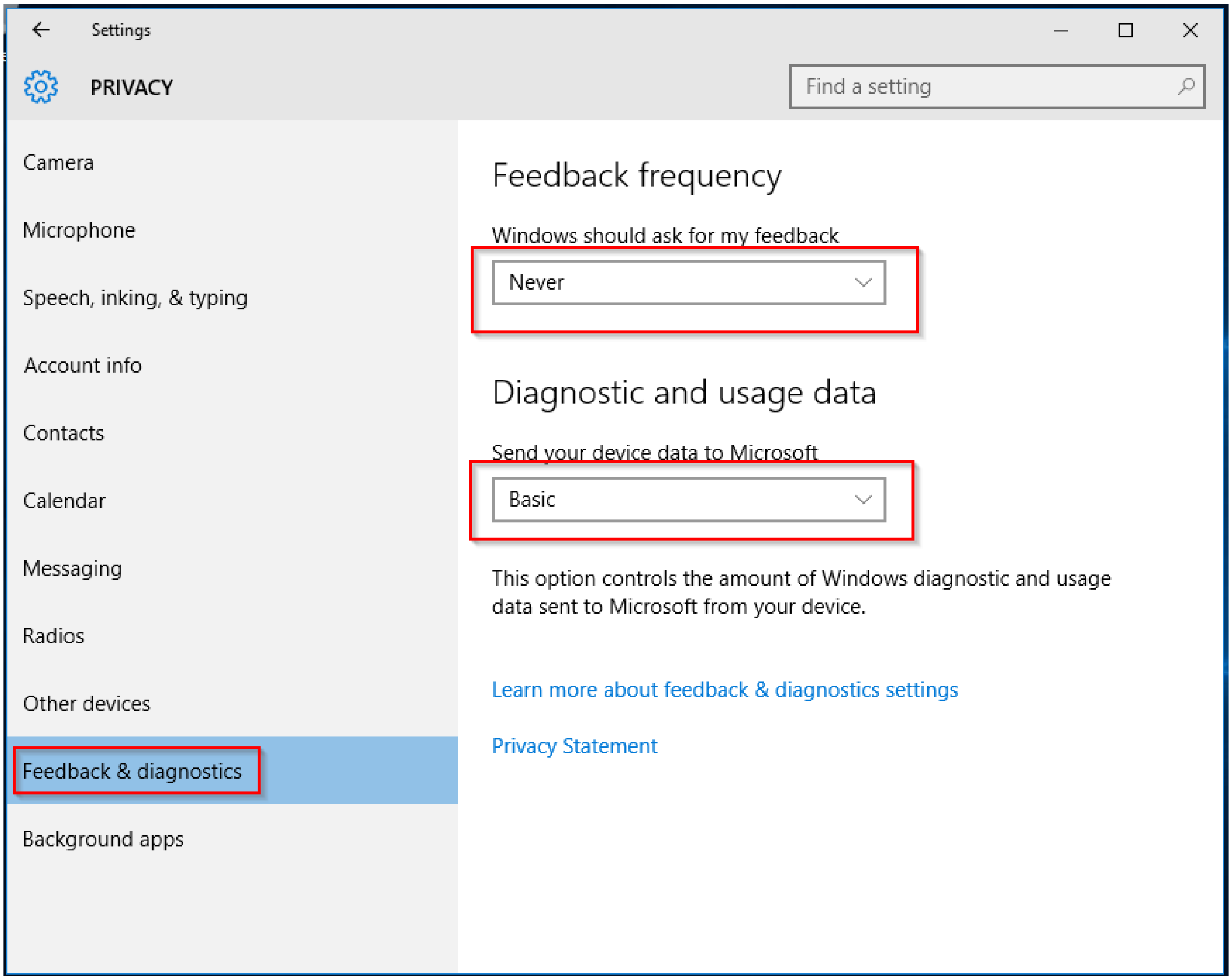
Manage cloud info

Go to Bing and manage personal info for all your devices

Learn more about speech, inking, and typing settings

Privacy Statement

Select Feedback & diagnostics and set Windows Should Ask for My Feedback to Never and Send Your Device Data to Microsoft to Basic:



Feedback frequency

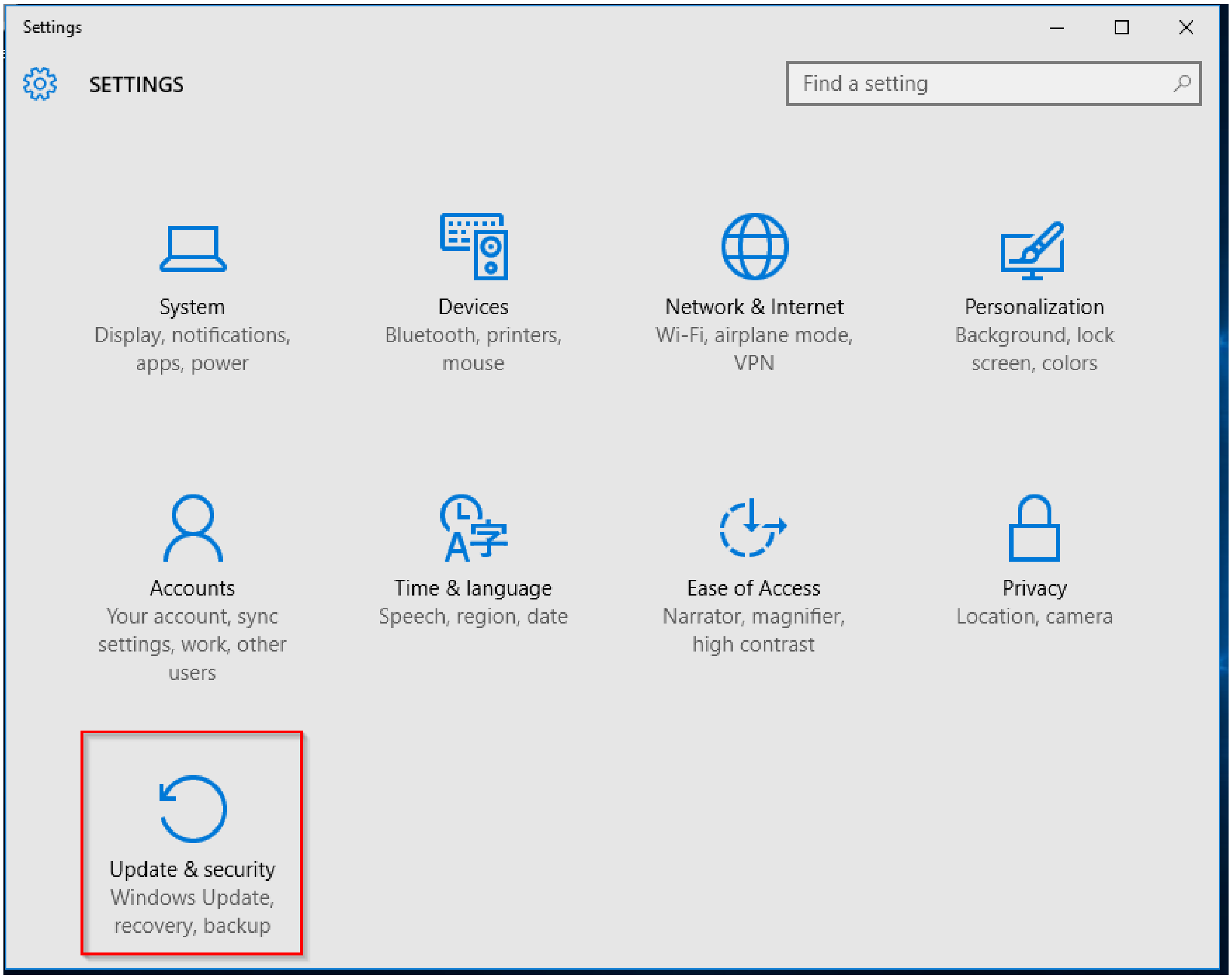
Windows should ask for my feedback: Never

Diagnostic and usage data

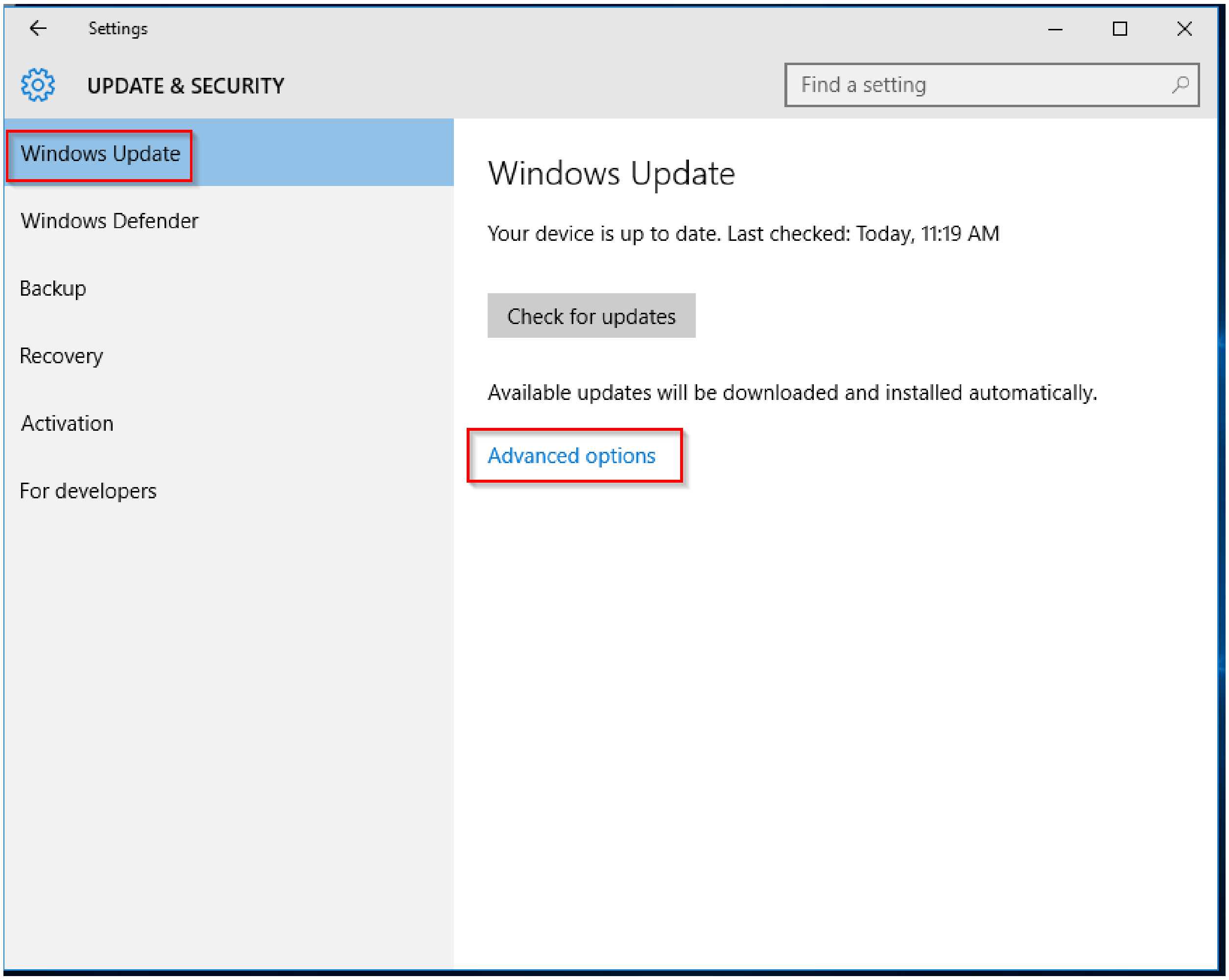
Send your device data to Microsoft: Basic

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

Return to the Control Panel by going to the Start Menu and choosing Settings. Select Update & Security:


Settings
SETTINGS
Find a setting
System
Display, notifications, apps, power
Devices
Bluetooth, printers, mouse
Network & Internet
Wi-Fi, airplane mode, VPN
Personalization
Background, lock screen, colors
Accounts
Your account, sync settings, work, other users
Time & language
Speech, region, date
Ease of Access
Narrator, magnifier, high contrast
Privacy
Location, camera
Update & security
Windows Update, recovery, backup

Choose Advanced Options:

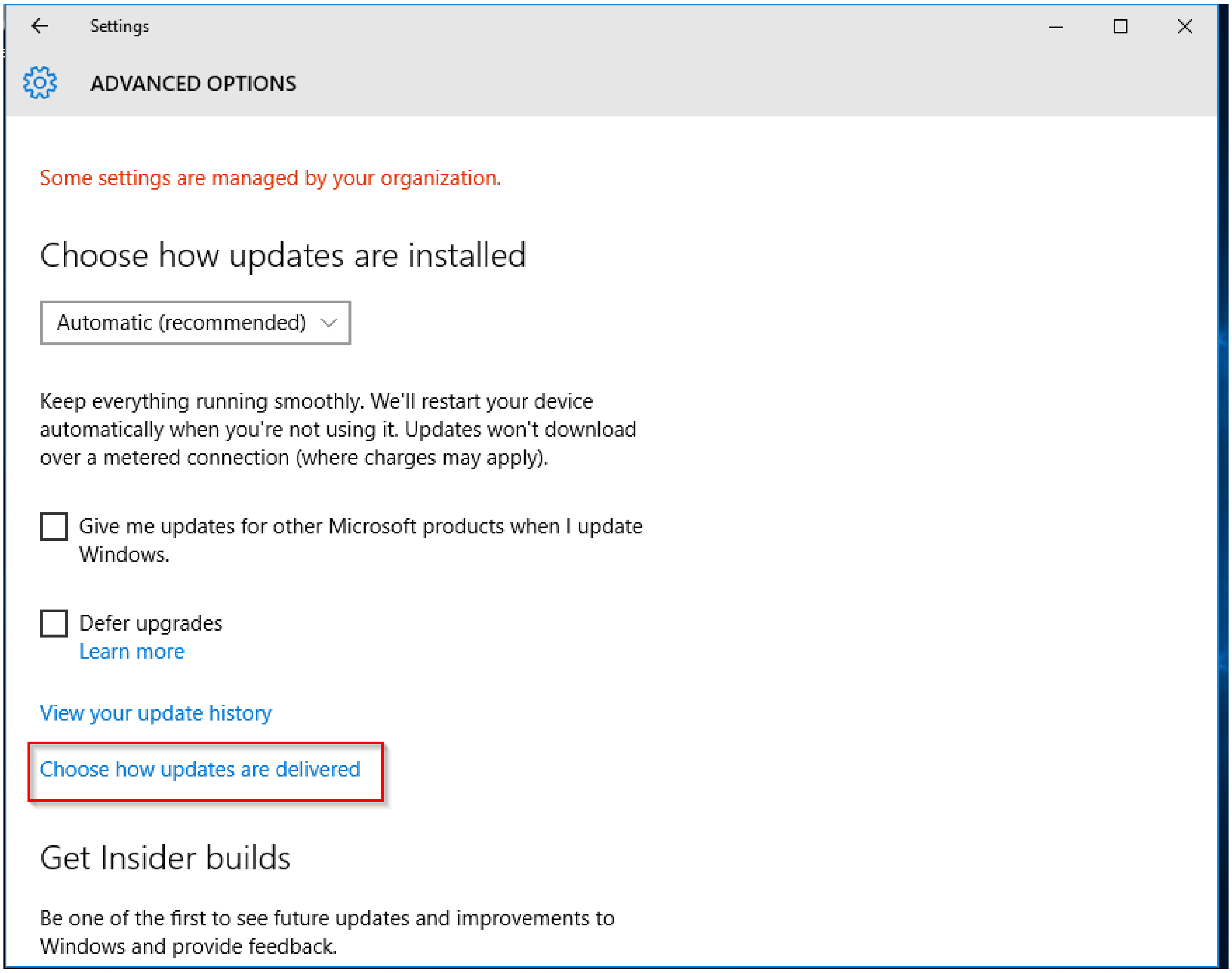


Windows Update

Your device is up to date. Last checked: Today, 11:19 AM

Available updates will be downloaded and installed automatically.

Select Choose How Updates Are Delivered:



ADVANCED OPTIONS

Some settings are managed by your organization.

Choose how updates are installed

Automatic (recommended)

Keep everything running smoothly. We'll restart your device automatically when you're not using it. Updates won't download over a metered connection (where charges may apply).

□ Give me updates for other Microsoft products when I update Windows.

□ Defer upgrades
Learn more

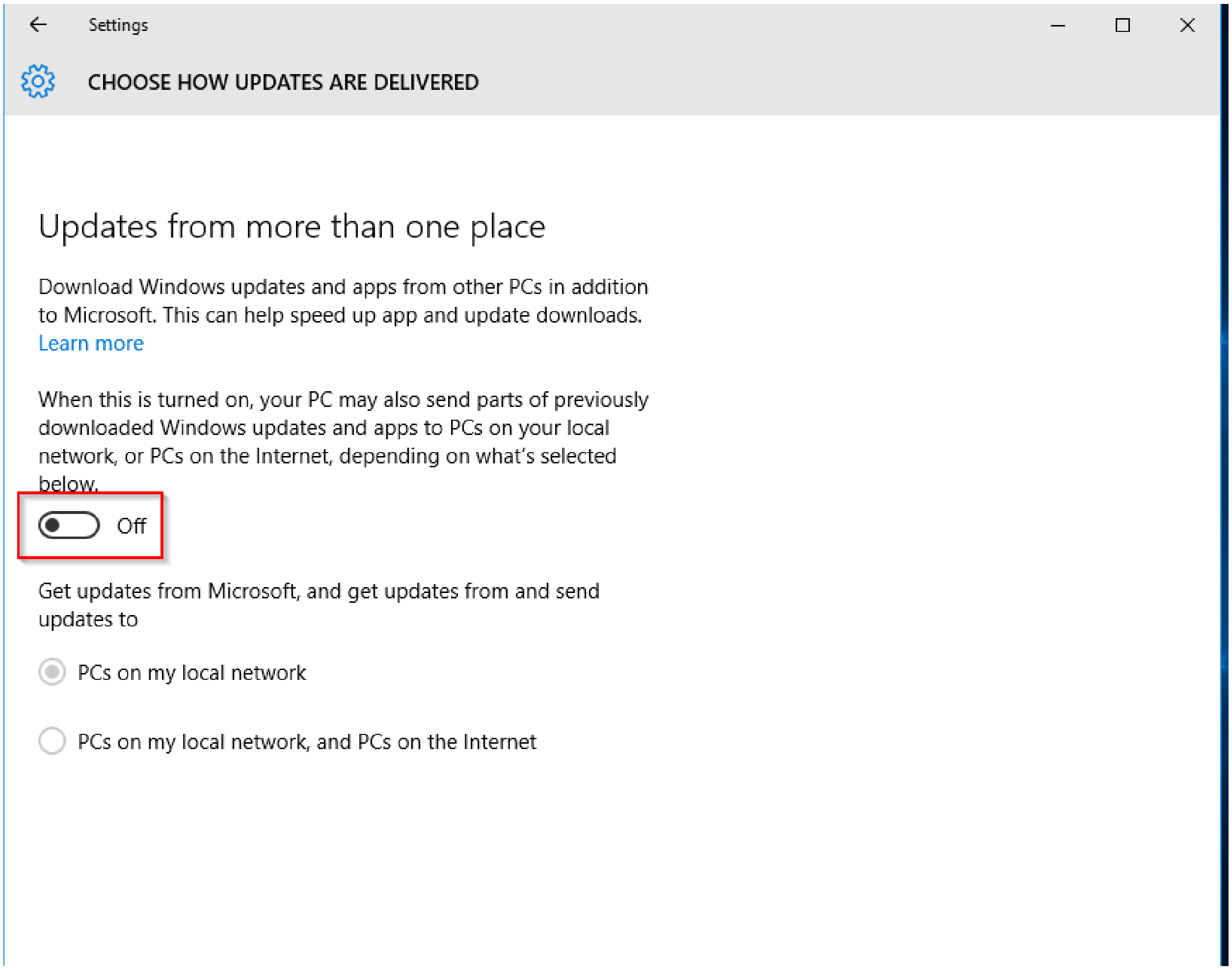
View your update history

Choose how updates are delivered

Get Insider builds

Be one of the first to see future updates and improvements to Windows and provide feedback.

Make sure that Updates From More Than One Place is turned off:



CHOOSE HOW UPDATES ARE DELIVERED

Updates from more than one place

Download Windows updates and apps from other PCs in addition to Microsoft. This can help speed up app and update downloads.

When this is turned on, your PC may also send parts of previously downloaded Windows updates and apps to PCs on your local network, or PCs on the Internet, depending on what's selected below.

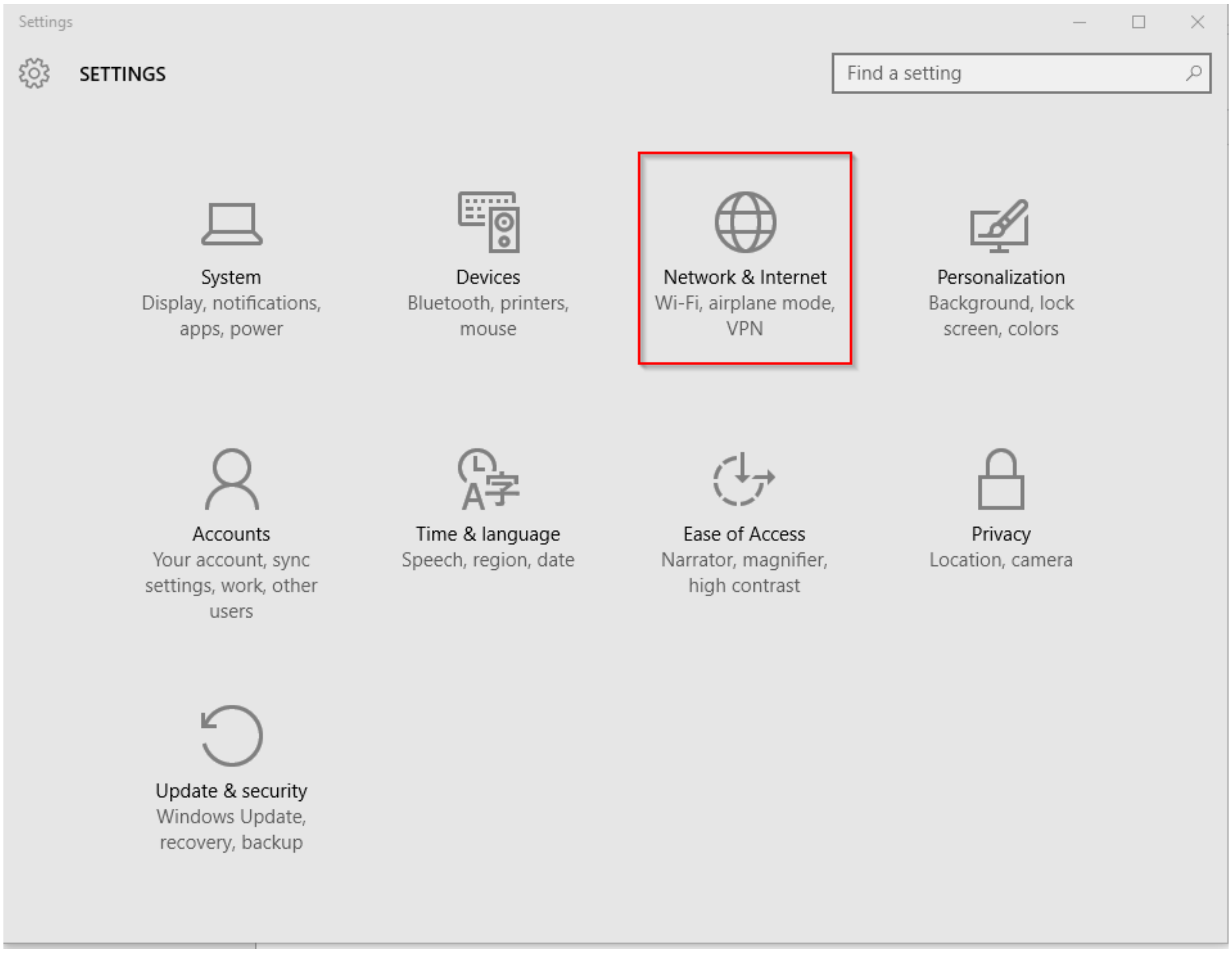
Off

Get updates from Microsoft, and get updates from and send updates to

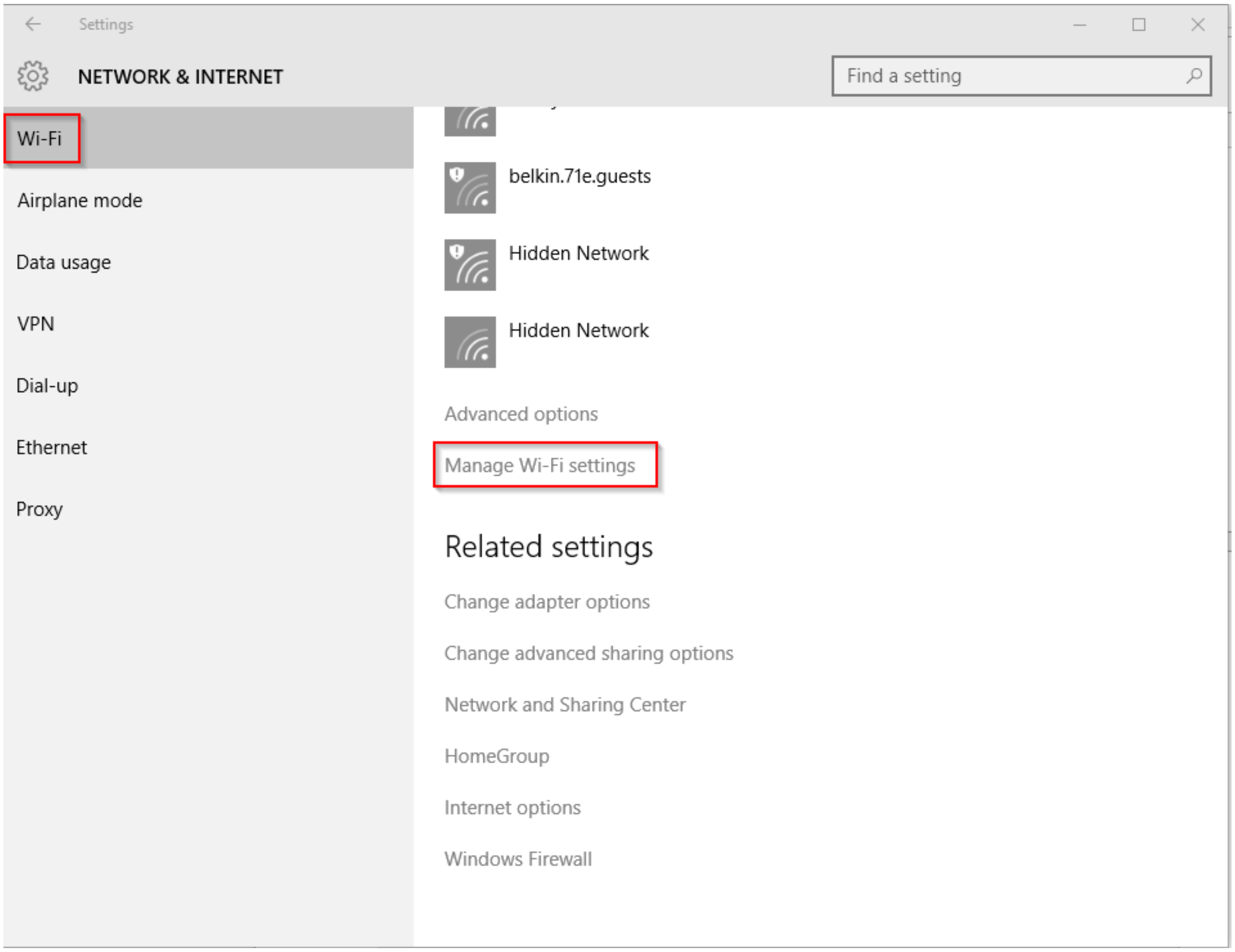
● PCs on my local network

○ PCs on my local network, and PCs on the Internet

From Settings, Choose Network & Internet:


Settings
SETTINGS
Find a setting
System
Display, notifications, apps, power
Devices
Bluetooth, printers, mouse
Network & Internet
Wi-Fi, airplane mode, VPN
Personalization
Background, lock screen, colors
Accounts
Your account, sync settings, work, other users
Time & language
Speech, region, date
Ease of Access
Narrator, magnifier, high contrast
Privacy
Location, camera
Update & security
Windows Update, recovery, backup

From the WiFi menu, choose Manage Wi-Fi Settings:



Settings

NETWORK & INTERNET

Find a setting

- Wi-Fi
- Airplane mode
- Data usage
- VPN
- Dial-up
- Ethernet
- Proxy

belkin.71e.guests

Hidden Network

Hidden Network

Advanced options

Manage Wi-Fi settings

Related settings

Change adapter options

Change advanced sharing options

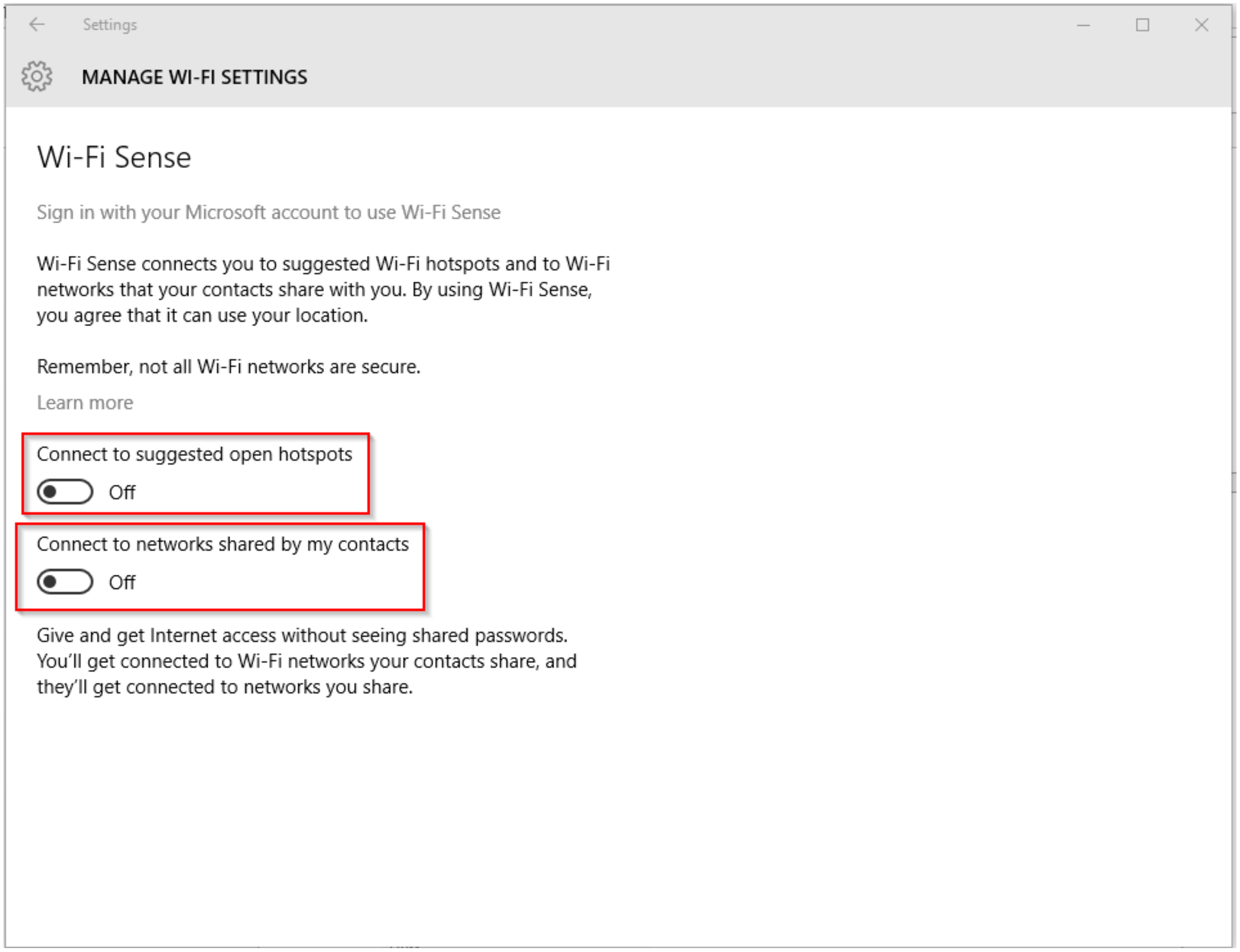
Network and Sharing Center

HomeGroup

Internet options

Windows Firewall

Make sure that Connect to suggest open hotspots and Connect to networks shared by my contacts are both off:



MANAGE WI-FI SETTINGS

Wi-Fi Sense

Sign in with your Microsoft account to use Wi-Fi Sense

Wi-Fi Sense connects you to suggested Wi-Fi hotspots and to Wi-Fi networks that your contacts share with you. By using Wi-Fi Sense, you agree that it can use your location.

Remember, not all Wi-Fi networks are secure.

Learn more

Connect to suggested open hotspots

Off

Connect to networks shared by my contacts

Off

Give and get Internet access without seeing shared passwords. You'll get connected to Wi-Fi networks your contacts share, and they'll get connected to networks you share.

Last updated: 12/17/2015