Windows 10 Deployment Guide

Windows 10 is approved for use on campus with university owned devices or personally owned devices storing confidential (Category I) university data as long as the steps outlined in this deployment guide are followed.

Contents

- Purpose
- Scope
- Deployment Requirements
  - Professionally-managed devices
  - Self-managed devices
- Non-Compliance and Exceptions
- Related UT Austin Policies, Procedures, Best Practices
- External References
  - Optional privacy and security settings for all Windows 10 devices

Purpose

With Windows 10, Microsoft introduced some new features that 1) mine user data for the purpose of making the operating system more social and personalized, 2) collect data about user's habits and usage patterns for the purposes of diagnostics and troubleshooting, and 3) allow users to share Windows updates with local networks and the Internet in order to crowd-source distribution of updates. These features are enabled by default in all Windows 10 editions. The use of these new features pose a significant risk for exfiltration of confidential university data to Microsoft (and then to undisclosed third parties at Microsoft's whim), and, in the case of distributed updates, may violate state law governing the use of government property.

In order to comply with university policy, these features of Windows 10 must be disabled. This is best done through GPO for all domain joined machines, but instructions are also provided for stand-alone devices.

Scope

- All university-owned tablets, laptops, and desktops running Windows 10.
- All personally-owned tablets, laptops, and desktops running Windows 10 that are used to store confidential (Category I) university data.

Deployment Requirements

Professionally-managed devices

Use Group Policy or Local Policy as needed to make the following changes:

<table>
<thead>
<tr>
<th>Enforced</th>
<th>Policy Name</th>
<th>Policy Location</th>
<th>Applies To</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Turn off Application Telemetry</td>
<td>Administrative Templates</td>
<td>Windows Components</td>
<td>Application Compatibility</td>
</tr>
</tbody>
</table>
| Yes      | Allow Telemetry               | Administrative Templates | Windows Components | Data Collection and Preview Builds | At least Windows 10 Server, Windows 10 or Windows 10 RT | Set policy to Enabled and set Options to "0 - Off [Enterprise Only]"

Windows 10 is approved for use on campus with university owned devices or personally owned devices storing confidential (Category I) university data as long as the steps outlined in this deployment guide are followed.
<table>
<thead>
<tr>
<th>Yes</th>
<th>Allow input personalization</th>
<th>Administrative Templates</th>
<th>Control Panel</th>
<th>Regional and Language Options</th>
<th>At least Windows Server Technical Preview 2, Windows 10 or Windows RT 8.1</th>
<th>Set to Disabled. This disables the use of Cortana, collection of speech and handwriting patterns, typing history, contacts, and calendar information.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Allow Cortana</td>
<td>Administrative Templates</td>
<td>Windows Components Search</td>
<td>At least Windows Server Technical Preview 2, Windows 10 or Windows RT 8.1</td>
<td>Set to Disabled</td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td>Turn off picture password sign-in</td>
<td>Administrative Templates</td>
<td>System Logon</td>
<td>At least Windows Server 2012, Windows 8 or Windows RT</td>
<td>Set to Enabled</td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td>Accounts: Block Microsoft Accounts</td>
<td>Windows Settings Security Settings Local Policies Security Options</td>
<td>At least Windows Server 2012, Windows 8 or Windows RT</td>
<td>Check &quot;Define this policy setting&quot; and choose &quot;Users can't add or log on with Microsoft Accounts&quot;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>Turn off the Advertising ID</td>
<td>Administrative Templates</td>
<td>System User Profiles</td>
<td>At least Windows Server 2012 R2, Windows 8.1 or Windows RT 8.1</td>
<td>Set to Enabled. This is not required, but is recommended to protect user privacy.</td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>Use Microsoft Passport for Work</td>
<td>Administrative Templates</td>
<td>Windows Components Microsoft Passport for Work</td>
<td>At least Windows 10 Server or Windows 10</td>
<td>Set as desired. This functionality is used with biometrics and PINs</td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>Turn on PIN sign-in</td>
<td>Administrative Templates</td>
<td>System Logon</td>
<td>At least Windows 10 Server 2012, Windows 8 or Windows RT</td>
<td>Set as desired. If PINs are allowed, they must comply with section 15.2 of the Information Resources Use and Security Policy.</td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td>Use digits</td>
<td>Administrative Templates</td>
<td>Windows Components Microsoft Passport for Work PIN complexity</td>
<td>At least Windows 10 Server or Windows 10</td>
<td>All passwords, including device PINs, must comply with section 15.2 of the Information Resources Use and Security Policy. Another option is to disable PIN sign-in entirely.</td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td>DownloadMode</td>
<td>Preferences Windows Settings Registry</td>
<td>All versions of Windows will accept the registry change, but will only be effective on Windows 10</td>
<td>This registry policy preference will disable peer-to-peer update sharing and should be created with the name &quot;DownloadMode&quot; as a &quot;Replace&quot; action, in the HKEY_LOCAL_MACHINE hive, at the &quot;SOFTWARE\Microsoft\Windows\CurrentVersion\DeliveryOptimization\Config&quot; key. The value type is &quot;REG_DWORD&quot;, and the value data is &quot;0&quot;. On the Common tab, the setting &quot;Remove this item when it is no longer applied&quot; should be checked.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*These requirements will be enforced by GPO for all members of the Austin Active Directory domain.*

**Self-managed devices**

This guide assumes that the operating system is already installed. All of these settings may also be configured during installation if "Customise settings" is chosen during the "Get going fast" stage of installation.

Follow the instructions to make the following changes:
<table>
<thead>
<tr>
<th>Requirement</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable &quot;Getting to know you&quot;</td>
<td>From the Start menu, click on &quot;Settings&quot;&lt;br&gt;Click on &quot;Privacy&quot;&lt;br&gt;Click on &quot;Speech, inking, &amp; typing&quot;&lt;br&gt;Click on the button &quot;Stop getting to know me&quot;&lt;br&gt;Click on &quot;Turn off&quot; in the confirmation dialog</td>
</tr>
<tr>
<td>Disable sending diagnostic and usage data to Microsoft (i.e. telemetry)</td>
<td>From the Start menu, click on &quot;Settings&quot;&lt;br&gt;Click on &quot;Privacy&quot;&lt;br&gt;Click on &quot;Feedback &amp; diagnostics&quot;&lt;br&gt;Select &quot;Basic&quot; under &quot;Diagnostic and usage data&quot;&lt;br&gt;NOTE: With this setting, Windows 10 will still send some telemetry data to Microsoft. In Enterprise editions of Windows, telemetry can be completely disabled, but only via (local or group) policy. Contact your IT support staff for assistance with this if desired.</td>
</tr>
</tbody>
</table>
| Disable receiving/sharing Windows updates with the Internet (desktops) or both the Internet and local networks (mobile devices) | From the Start menu, click on "Settings"
| |   Click on "Update & security"
| |   Under "Windows Update" click on "Advanced options"
| |   Click on "Choose how updates are delivered"
| |   For mobile devices, click the toggle to turn distributed updates off entirely.
| |   For desktops, ensure that "PCs on my local network" is selected (or turn off distributed updates entirely via the toggle). |
Do not use a Microsoft account to sign-in

If you have already setup a Microsoft Account for authenticating to a local account by doing the following:

From the Start menu, click on "Settings"
Click on "Accounts"

Click on "Sign in with a local account instead"

Enter your Microsoft Account password when prompted

Choose a username, password, and password hint

Click on "Sign out and finish"

Do not use a picture password to sign-in. PINs must meet password policy complexity requirements.

Section 15.2 of the Information Resources Use and Security Policy (IRUSP) mandates the use of strong passwords for user authentication.

Non-Compliance and Exceptions

If any of the configuration requirements contained within this document cannot be met, an Exception Process must be initiated that includes reporting the non-compliance to the Information Security Office, along with a plan for risk assessment and management. (See Security Exception Report.) Non-compliance with these standards may result in revocation of system or network access, notification of supervisors, and reporting to the Office of Internal Audit.

University of Texas at Austin employees are required to comply with both institutional rules and regulations and applicable UT System rules and regulations. In addition to university and System rules and regulations, University of Texas at Austin employees are required to comply with state laws and regulations.

Related UT Austin Policies, Procedures, Best Practices

The policies and practices listed here inform the system hardening procedures described in this document and with which you should be familiar. (This is not an all-inclusive list of policies and procedures that affect information technology resources.)

Information Resources Use and Security Policy (IRUSP)

UT Austin Acceptable Use Policy (AUP)
Optional privacy and security settings for all Windows 10 devices

Privacy-conscious users may find the guides below useful for addressing other features of Windows 10 that pose a privacy/security risk: