

System Hardening

Paul G. Gurke

University of Advancing Technology

System Hardening

This document shows steps taken to harden a Windows 10 Operating System.

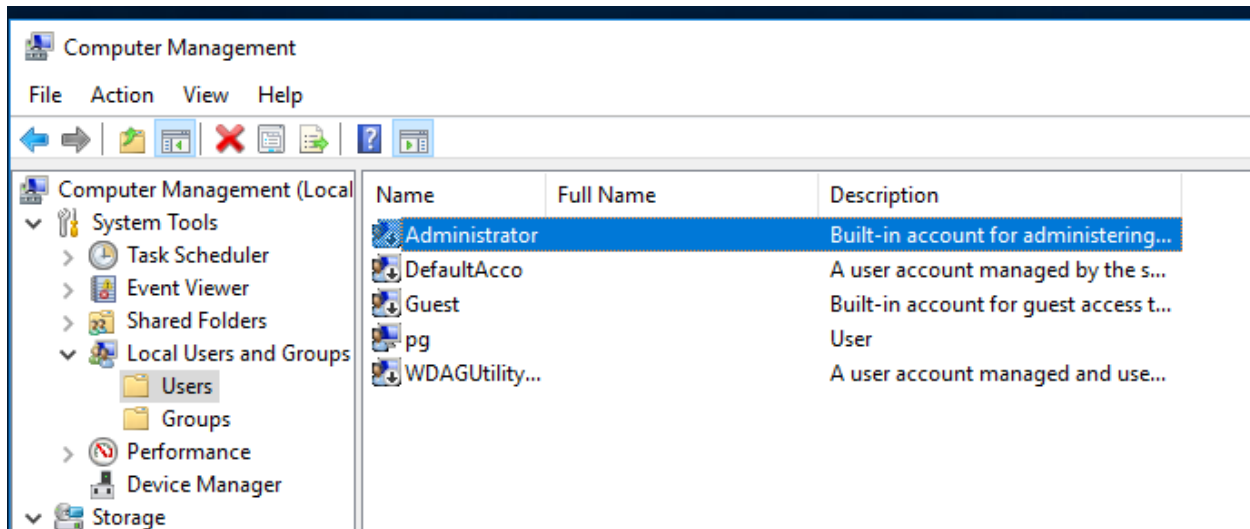
Disabling Remote Access

Surprisingly, Remote Assistance is enabled by default. Chose to uncheck “Allow Remote Assistance [...]” and select “Don’t allow [...]” in the remote tab of system properties.

The screenshot shows the Windows System Properties dialog box with the 'Remote' tab selected. The background is the Windows Control Panel 'System' page, which displays 'Windows 10 Education' and '© 2018 Microsoft Corporation. All rights reserved.' The left sidebar of the Control Panel includes links to 'Control Panel Home', 'Device Manager', 'Remote settings', 'System protection', and 'Advanced system settings'. At the bottom left, there is a 'See also Security and Maintenance' link. The 'System Properties' dialog box has tabs for 'Computer Name', 'Hardware', 'Advanced', 'System Protection', and 'Remote'. The 'Remote' tab contains two sections: 'Remote Assistance' and 'Remote Desktop'. In the 'Remote Assistance' section, the checkbox 'Allow Remote Assistance connections to this computer' is unchecked. Below it is a link 'What happens when I enable Remote Assistance?' and an 'Advanced...' button. In the 'Remote Desktop' section, the instruction 'Choose an option, and then specify who can connect.' is followed by three radio button options: 'Don't allow remote connections to this computer' (selected), 'Allow remote connections to this computer', and 'Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended)' (checked). There is also a 'Help me choose' link and a 'Select Users...' button. At the bottom of the dialog box are 'OK', 'Cancel', and 'Apply' buttons.

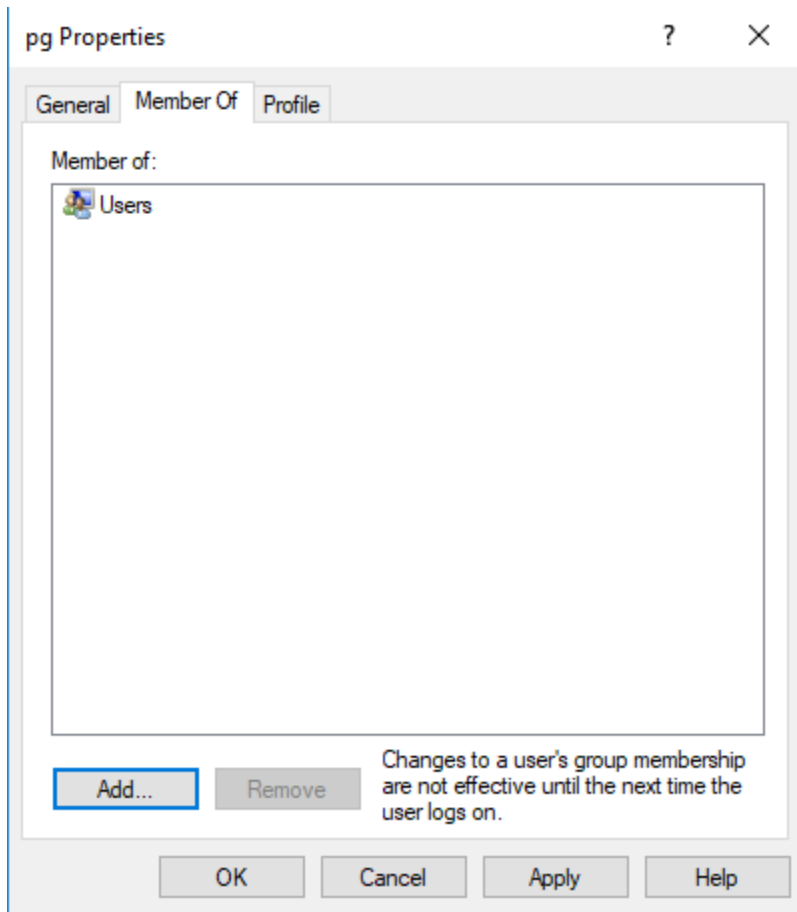
Deleting Unnecessary Accounts

Make sure there are no active unused local accounts. (This host is a member of a domain.)



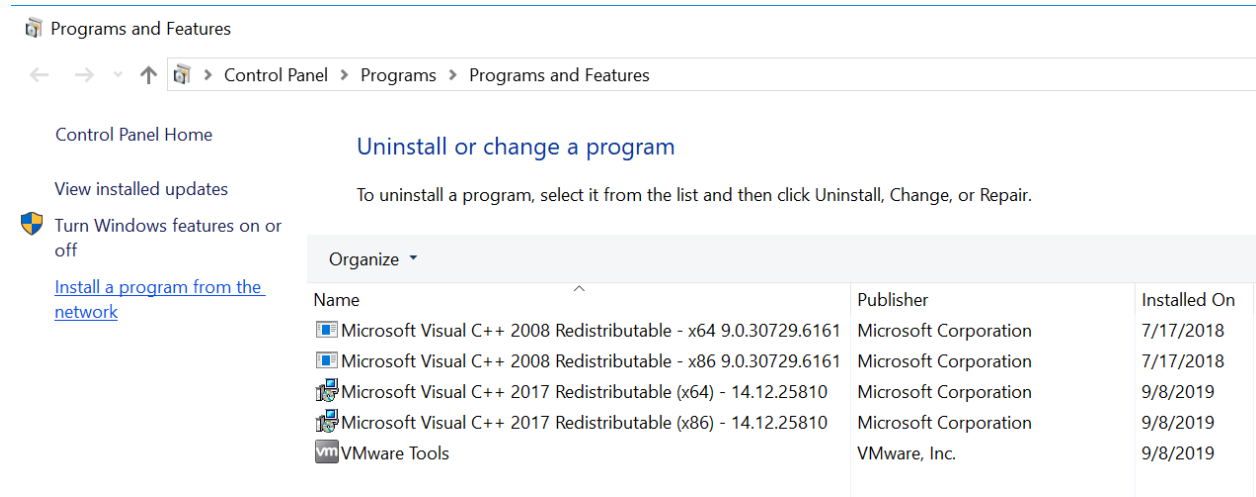
Create a Lower Than Admin Account

Ensure that the remaining user account is not an administrator.



Removal of Unnecessary Applications

This is what remained after I removed all but what I thought were necessary for core functionality.

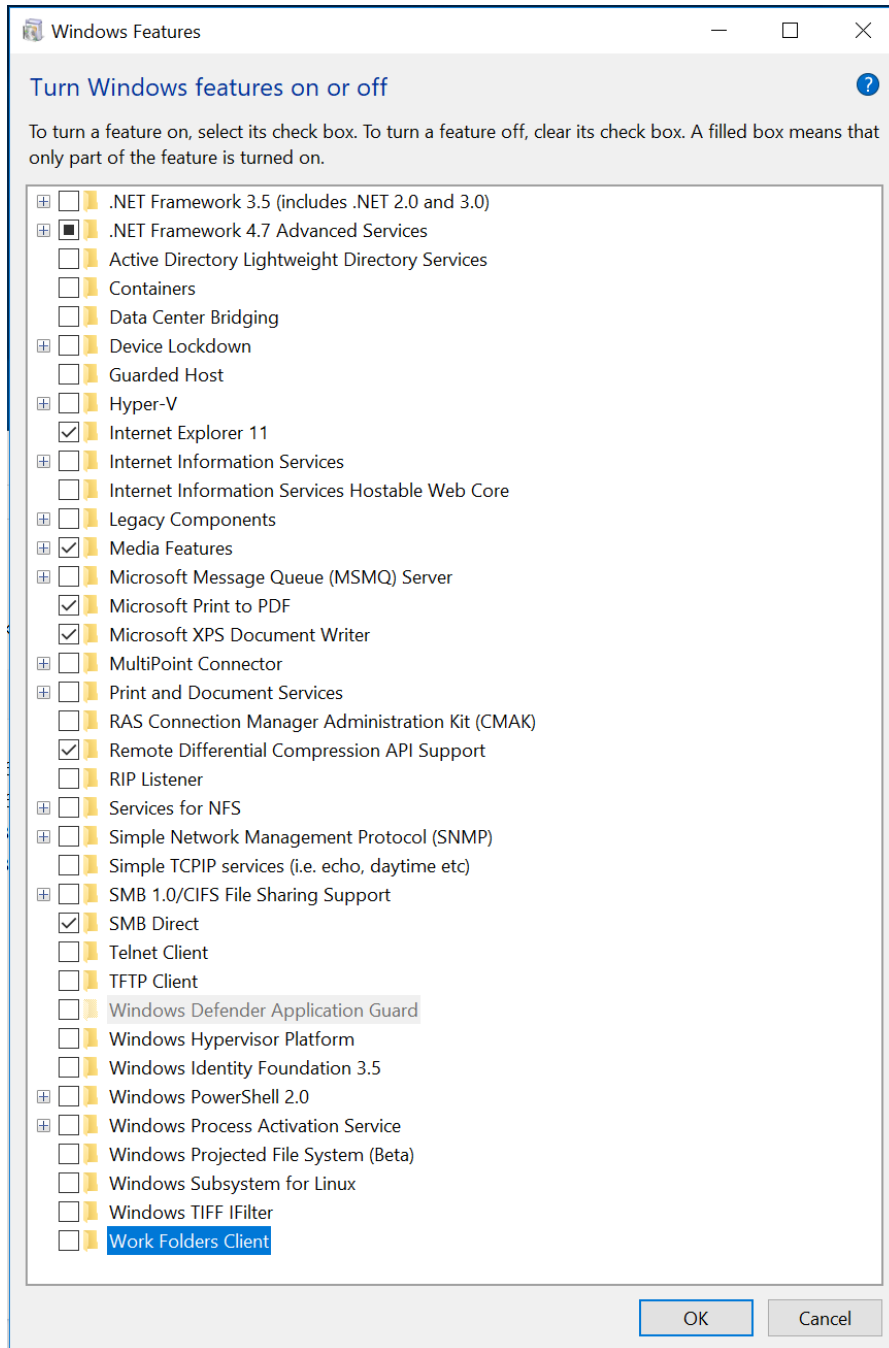


The screenshot shows the Windows Control Panel window for "Programs and Features". The title bar reads "Programs and Features". The breadcrumb navigation shows "Control Panel > Programs > Programs and Features". On the left sidebar, there are links for "Control Panel Home", "View installed updates", "Turn Windows features on or off", and "Install a program from the network". The main content area is titled "Uninstall or change a program" and includes the instruction: "To uninstall a program, select it from the list and then click Uninstall, Change, or Repair." Below this is a table of installed programs.

Name	Publisher	Installed On
Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.6161	Microsoft Corporation	7/17/2018
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161	Microsoft Corporation	7/17/2018
Microsoft Visual C++ 2017 Redistributable (x64) - 14.12.25810	Microsoft Corporation	9/8/2019
Microsoft Visual C++ 2017 Redistributable (x86) - 14.12.25810	Microsoft Corporation	9/8/2019
VMware Tools	VMware, Inc.	9/8/2019


Turn Off Unused Features

Navigate to “Turn Windows features on or off” and make sure that .net 3.5, SMB v1 and PowerShell 2 are unchecked.



BIOS Update

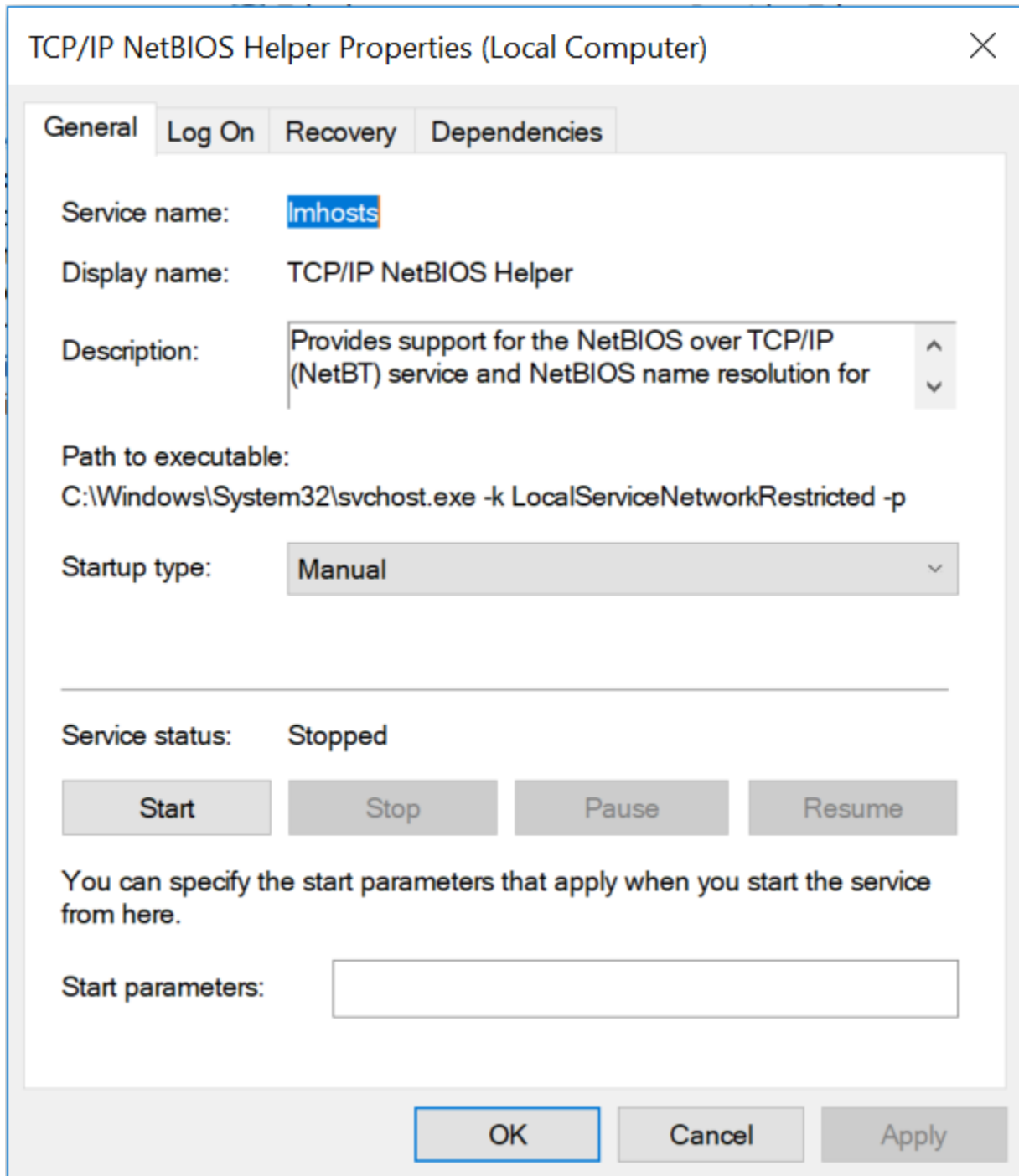
Update BIOS through computer or motherboard manufacturer. In this case, I went to Dell to get the latest BIOS update.

NAME	CATEGORY
<input type="checkbox"/> Alienware 15 R3 and Alienware 17 R4 System BIOS URGENT	BIOS
Version: 1.7.0 ,1.7.0 Older versions 	
Last Updated Date: 16 May 2019	

Item	Value
BIOS Version/Date	Alienware 1.5.0, 9/10/2018
SMBIOS Version	3.0

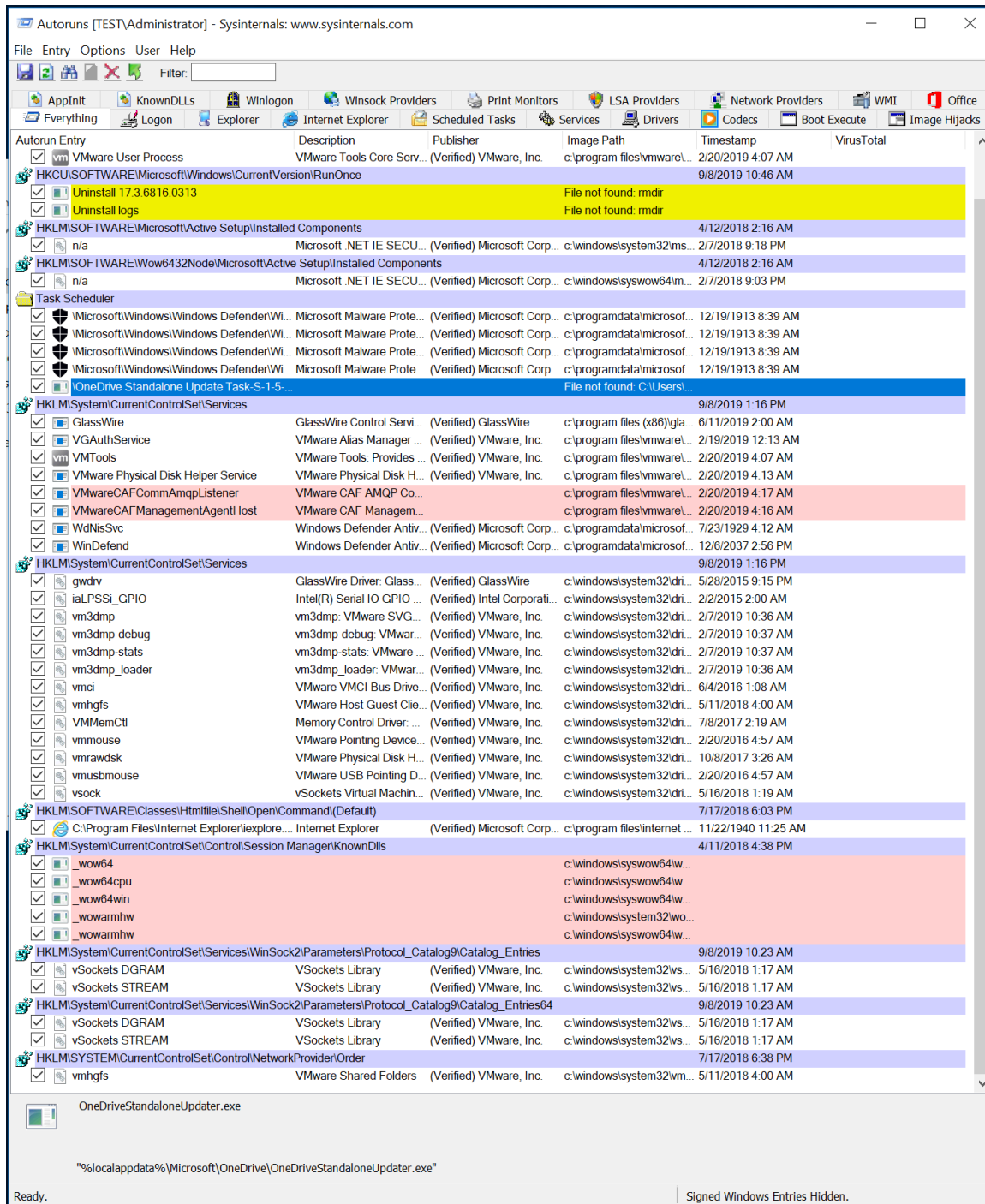
Stop TCP/IP NetBIOS Helper

Navigate to services via Run: services.msc and stop the TCP/IP NetBIOS Helper.



Autoruns (Sysinternals)

If the Sysinternals suite is available, run “Autoruns” to identify what is being ran automatically. On the machine I checked, I could see that even though OneDrive was uninstalled in a previous step (and restarted since), there was still a triggered task to run an update.



Remove Unused Shares

Check the shares with the Net Share command to ensure that there are no unutilized shares.

```
C:\Users\administrator>net share

Share name      Resource                Remark
-----
C$              C:\                    Default share
IPC$            C:\                    Remote IPC
ADMIN$          C:\Windows             Remote Admin
The command completed successfully.
```

Drive Encryption

To enable security control to your physical drives, BitLocker Drive Encryption can be turned on to encrypt your data. This even includes your running operating system.

