Securing Your Windows 8 System

Written by:
Alex Smith
Junior Information Security Analyst
UCIT Office of Information Security
5/7/2013

Table of Contents
Configure Windows 8 Settings.................................................. 1-5
  Creating a Strong Password .................................................. 1
  Update Windows .................................................................. 2
  Privacy Settings .................................................................. 2
  Disable Dumpfile Creation .................................................. 2-3
  Set Bios Password (optional) .............................................. 3
  Configure Your Firewall ..................................................... 3
  Extra Security Settings ...................................................... 4
  New to Windows Login Features ........................................... 5
Installing Security Software ...................................................... 5-6
  3rd Party Security Suites .................................................... 5-6
  Anti-Malware Software ....................................................... 6
  Encryption Software .......................................................... 6
Securing Your Internet ............................................................ 7-8
  Secure with IE10 Settings ................................................... 7
  Which Browser(s) to use ..................................................... 8
Post-Configuration Clean-up .................................................... 8-10
  System Protection (Restore Points) ..................................... 8
  System Back-Ups .............................................................. 9
  How to Reset Settings ...................................................... 9-10
References .............................................................................. 11
Appendix A (Windows 8 Pro & Enterprise only) ....................... 12-15
**Intro:** Physical security of your system should be the number one priority. No system is safe if it is stolen or accessible by others. Do not leave your laptop unattended. Use locks for containers which your system may be in (cars, rooms, lockers). When a system is left unattended in a safe location, it is best practice to lock your computer to the logon screen so that others may not access your system without a password. Make sure to do this when friends and family are present too. Anyone may be curious, and events such as “Facebook status hacking” are preventable. 

A useful function in Windows 8 is the desktop tools function. Go to the Desktop or Start Menu page and right-click on the task bar at the very bottom left corner.

This will appear:

<table>
<thead>
<tr>
<th>Programs and Features</th>
<th>Power Options</th>
<th>Event Viewer</th>
<th>System</th>
<th>Device Manager</th>
<th>Disk Management</th>
<th>Computer Management</th>
<th>Command Prompt</th>
<th>Command Prompt (admin)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task Manager</td>
<td>Control Panel</td>
<td>File Explorer</td>
<td>Search</td>
<td>Run</td>
<td>Desktop</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Version differences:** Windows 8 Pro and Windows 8 Enterprise offer the following features which Windows 8 does not:

- Bitlocker Encryption
- Security Policy Customization (Appendix A)

**Last note:** Using the Windows key on the keyboard is a quick way to switch between the Desktop and Start Menu. This should greatly increase productivity.
Configure Windows 8 Settings

Creating a Strong Password
The first (and most important) step to securing Windows 8 is to make a strong password.

1. Begin by navigating to the sidebar and selecting Settings.
2. Select Change PC Settings, then click Users (left panel).
3. Select Change your password.
4. Create a new password using the following criteria:
   - Length of 8-16 characters
   - Use at least 3 of the 4 following character sets:
     - Uppercase Alphabetic Characters
     - Lowercase Alphabetic Characters
     - (2 +) Numeric Characters
     - Special Characters (!@#$%^&*)

(When adding a Password hint, make sure it is useful but not too revealing.)

Password Upon Wake-up Setting
This will ensure that when you leave your computer, it will require a password to wake-up after the screen saver is turned on.

1. Navigate to the sidebar and select Settings.
2. Select Change PC Settings, then click on Users (left panel).
3. Select Change to ensure the phrase, “Any user who has a password must enter it when waking this PC” is present. This is a toggle button, so the words “doesn’t need to” will alternate with the word “must.”

Update Windows
The second step to securing Windows 8 is to make sure the operating system is up to date. Windows updates provide patches for security holes and vulnerabilities. These are released on a regular basis.

1. To apply updates, begin at the Start Menu screen.
2. Right click on the background to select All apps.
3. Locate and select Control Panel.
4. Click **System and Security**, and then select **Windows Update**.
5. Select **Check for updates**.
6. Then go to **Change Settings**. Ensure that “Install updates automatically (recommended)” is on.
7. Select “Updates will be automatically installed during the maintenance window.” Ensure that the time which is selected is a time that your system will be powered on.

When this step is complete, the Windows Update screen should look like this:

![Windows Update Screen](image)

**Privacy Settings**

1. Navigate to the sidebar and select **Settings**, then click **Change PC Settings**.
2. Select **Privacy** on the left panel.
3. Set the following:
   - Let apps use my location – **OFF**
   - Let apps use my name and account picture – **OFF**
   - Help improve Windows Store by sending URLs for web content that apps use – **Choose Either**

**Disable Dumpfile Creation**

A dump file can be a useful troubleshooting tool when either the system or application crashes and causes the infamous "Blue Screen of Death". However, they also can provide a hacker with potentially sensitive information such as application passwords.

1. Go to Start Menu screen, then right click on the background and select **All apps**.
2. Right click **Computer**, select **Properties**.
3. Select **Advanced System Settings**, and then select the **Advanced** tab.
4. Select **Settings** under the **Startup and Recovery** section.
5. Under **Write debugging information**, change the drop down box setting to **(none)**.
6. Select **OK**.
Set Bios Password (optional)
For extra security, you can set the bios password so that the computer cannot boot without entering a password. This will require you to enter two passwords to start up your system (bios and Windows) and is normally not required.

Configure your Firewall
1. Begin at the Start Menu screen. Right click on the background to select All apps.
2. Select Control Panel, and click System and Security.
4. Select Turn Windows Firewall on or off.
5. Ensure that the Windows Firewall is turned on for Private and Public networks.

Extra Security Settings
1. Go to the Start Menu screen, right click on the background to select All apps.
2. Select Control Panel, and click System and Security.
3. Select Action Center.
4. On the left panel, select Change User Account Control settings.
5. Slide the bar all the way to the top. Click **OK**.
   (This will ensure that all apps making changes to your system are authorized to do so.)

![User Account Control Settings](image1.png)

6. Within the Action Center (under the **Security** section), select **Change Settings** next to **Turn on Windows SmartScreen**.

7. Select the top option for maximum security ("Get administrator approval before running an unrecognized app from the Internet").
   Having this setting selected will ensure that you approve anything trying to run on your computer from the internet.

![Windows SmartScreen](image2.png)

**New to Windows login features**
It is recommended using either one of these options for mobile devices with no sensitive information. These methods can be easily compromised given the right tools and amount of time, however, both are beneficial to the user by making a device easier to log into.
Picture Password  
1. Navigate to the sidebar and select **Settings**.  
2. Select **Change PC Settings**, and click **Users** on the left panel.  
3. Select **Create a picture password**.

PIN-login  
1. Navigate to the sidebar and select **Settings**.  
2. Select **Change PC Settings**, and click **Users** on the left panel.  
3. Then select **Create a PIN**. This will prompt you for your password and walk you through making a 4-digit PIN.  
4. Be sure to pick a smart PIN (nothing anyone else can figure out).  
   - A few bad PINS: 1234, 1212, 1111, (last 4 digits of phone), (4-digit address), (last 4 of social)

---

**Installing Security Software**  
**Third Party Security Suites**  
There are many choices for 3rd party security suites. There are many free and many paid ones, the one you choose is up to you. Well-known suites include Avira/Avast/ Comodo (Free), or Norton/McAfee (Paid). You may want to search the web for one that meets your needs (cost vs. security vs. performance). This guide will show you how to secure a computer with McAfee (free for UC students, faculty, and staff). If you choose to use a different security suite, use similar settings.  
1. Open up your browser, go to [http://www.uc.edu/ucit/ware/software/mcafee.html](http://www.uc.edu/ucit/ware/software/mcafee.html).  
2. From there select the **link under** “Then, download the software”.  
3. Update McAfee, then perform the initial scan, and then the rest should be good to go. For additional support consult the software website forum.
Anti-Malware Software
If you notice weird pop-ups or strange computer activities, possibly very annoying activity, you may have malware or spyware. Sometimes this is easy to get rid of by using free third-party software. Try one of these:

- AdwCleaner
- Malwarebytes
- HiJackThis

Encryption Software
Encryption software is very important for ensuring that physical access to hardware is difficult unless one knows the code to access it. Encryption is especially important for portable hardware such as external hard drives, laptops, and USB drives.

Windows 8 Pro and Enterprise come with Bitlocker encryption software pre-installed.

Attention: UC Faculty and Staff must use encryption software required by their department/college.

Here is how to activate it:

1. Go to the Start Menu screen, right click on the background to select All apps.
2. Locate and select Control Panel, then click on System and Security.
3. Select Bit Locker Drive Encryption, and click Turn On Bitlocker to encrypt your systems internal hard drive.
   (Below this option, you can also encrypt external devices).

Here are a few third-party encryption software programs:

- Kruptos 2 Professional
- Privacy Drive
- Truecrypt

Securing Your Internet

Secure with IE 10 settings

1. Go to the Start Menu screen, right click on the background, select All apps.
2. Select Control Panel, then click Network and Internet, and choose Internet Options.
3. Go to the Privacy tab and set cookie security to High.
4. Enable the Pop-up Blocker.
Once you have done this, you will need to explicitly add any site that you want to have cookies. This requires a little extra work on your part, but it will virtually eliminate the incredible proliferation of cookies that infect most computers and dramatically compromise your privacy. There are a relatively low number of sites that absolutely require cookies.

5. Go to the **Security** tab and set to **High** for the Internet zone.

**Browser(s) to use**

Choosing a web browser is almost entirely a matter of opinion. Some browsers are more secure than others and some are faster than others.

The three prominently used web browsers for the Windows Operating Systems are Internet Explorer, Mozilla Firefox, and Google Chrome. You can see a selection of the top ten browsers and how they are rated [here](#). Internet explorer is currently recommended for security purposes and Chrome for usability. Most browsers are available free online. Just open Internet Explorer and go to the appropriate website to download one.

**Setting up a share folder:**

If you want to share files with other computers on your home network you will need to set up a shared folder/folders.

1. Navigate in Windows Explorer to **C: Drive, Users, Public**.
2. Right click the folder you want select **Properties**, then **Share**, add Authenticated Users with Read permissions.

3. Select **Share**, go to the **Security** tab and ensure that there is **not** an Anonymous or Everyone group with Read or Write permission.

**Post-Configuration Clean-Up**

**System Protection (Restore Points)**

By turning on system protection, Windows 8 will allow you to create system restore points so you can restore your system to a point before unwanted changes were made to your system.

1. Go to the **Start menu screen**, right click on the background, select **All apps**.
2. Right click **Computer**, and select **Properties**.
3. Click **System protection** on the left panel.
4. Choose **Configure** (To the right of **Configure restore settings, manage disk space, and delete restore points**).
5. Select **Turn on system protection**.

![](image)

6. Select **OK**, then **Create a Restore Point** (i.e. “First Restore”).

**System Back-Ups**

It is highly recommended that you make a back-up of your system and update it on a regular basis. Doing so will limit the amount of data that is lost in the case that your hard drive crashes or is physically destroyed. To do so you will need an external device that is the same size as or larger than your internal hard drive.

**Attention:** UC Faculty and Staff must backup systems as specified by department/college.

**Frequency/location**

Here is how to use the Windows Back-Up tool:

1. Go to the Start menu screen, right click on the background, select **All apps**.
2. Select **Control Panel**, click **System and Security**, and choose **File History**.
3. Select **Windows 7 File Recovery** (bottom left of window), then **Set up Backup**.
4. Select the appropriate drive(s) and follow the instructions.

Another way to regularly backup data onto an external device is to manage the process with third-party software. (Sometimes external devices come with such software).

You can try one of these:

- Smartsync-Pro
- Recurva
- Acronis True Image Home

**How to reset settings**

1. Navigate to the sidebar and select **Settings**.
2. Click **Change PC Settings**, and select **General** on the left panel.
3. Scroll down to the bottom and you will have two options:
   - You can **Refresh your PC without affecting your files**
   - This will reset settings on the PC to default (used to fix errors)
   - You can **Remove everything and reinstall Windows**
   - This will delete everything on your computer including files and restore your PC to factory status.
     (Do NOT use unless ABSOLUTLY NECESSARY or you are getting rid of your computer).
4. To use either one of these with the current PC settings you must go to **User Accounts and Family Safety**.
5. Select **Change User Account Control Settings**, and slide the bar to the 3rd highest section.
6. Click **OK**.
7. After changing this, you can successfully **Refresh** or **Reinstall Windows 8**.

![Refresh and Reinstall Windows 8](image)

**Refresh your PC without affecting your files**

If your PC isn't running well, you can refresh it without losing your photos, music, videos, and other personal files.

**Get started**

**Remove everything and reinstall Windows**

If you want to recycle your PC or start over completely, you can reset it to its factory settings.

**Get started**
REFERENCES:

CNET Downloads
AdwCleaner - http://download.cnet.com/AdwCleaner/3000-7786_4-75851221.html
Kruptos 2 - http://download.cnet.com/Kruptos-2-Professional/3000-2092_4-10446164.html
Malwarebytes - http://download.cnet.com/Malwarebytes-Anti-Malware/3000-8022_4-10804572.html
Privacy Drive - http://download.cnet.com/Privacy-Drive/3000-2092_4-75752636.html
Recuva - http://download.cnet.com/Recuva/3000-2242_4-10753287.html
Smartsync Pro - http://download.cnet.com/SmartSync-Pro/3000-2242_4-10050564.html
TrueCrypt - http://download.cnet.com/TrueCrypt/3000-2092_4-10527243.html

Microsoft Support
http://support.microsoft.com/find-solutions/windows/windows-8/

Create Strong Passwords

PC World
Windows 8: Put its hidden security features to work! - Eric Geier

Setup Windows 7 Securely - UCIT Office of Information Security
http://www.uc.edu/content/dam/uc/infosec/docs/general/Setup_Windows_7.pdf

SourceForge
HiJackThis - http://sourceforge.net/projects/hjt/

Tech 90
Password Evaluator
https://www.tech90.com/tools/password-evaluator/

TopTenReviews.com
Encryption Software Review
http://encryption-software-review.toptenreviews.com/
Appendix A: (For systems with Windows 8 Pro or Enterprise)

Local Security Policies

Setting local security policies will ensure that all users on the system must use secure practices when on the machine. Having security policies set correctly on a machine will prevent the wrong people from making changes to settings and from making poor security choices.

Note: Local Security Policies are only configurable in Windows 8 Pro and Windows 8 Enterprise. Local Security Policies cannot be configured in the base version of Windows 8.

1. To apply security policies, begin at the Start Menu screen.
2. Right click on the background, select All apps.
3. Select Control Panel, and then click System and Security.
4. Select Administrative Tools, and then double click Local Security Policy.

In Account Policies:

1. After selecting Password Policy, make these changes:
   - Do Not Enforce Password History
   - Set Maximum Password Age – 42 days
   - Set Minimum Password Age – 0 days
   - Minimum password length – 10 characters
   - Password must meet complexity requirements – Enabled
   - Store password in reversible encryption – Disabled

2. Select Account Lockout Policy, and make these changes:
   - Duration - 60 minutes
   - Threshold - 5 attempts
   - Reset lockout counter - 60 min

In Local Policies:

1. Click Audit Policy, and make these selections:
   - Audit account logon events – Success, Failure
   - Audit account management – Success, Failure
   - Audit directory service access – Failure
   - Audit logon events – Success, Failure
- Audit object access – *Failure*
- Audit policy change – *Success, Failure*
- Audit privilege use – *Success, Failure*
- Audit process tracking – *No auditing*
- Audit system events – *Success, Failure*

2. Select *User Rights Assignment*, and make these changes:
   
   **Note:** You will be removing groups (i.e. Everyone) and adding others (i.e. SYSTEM).
   
   - Access this computer from the network – *Administrators* (remove *Everyone* and any other groups)
   - Deny access to this computer from the network – *ANONYMOUS LOGON*
   - Deny logon locally – DoNotUse (*Guest*)

   ![User Rights Assignment](image)

   - Log on as a batch job – (Remove entries)
   - Log on as a service – (Remove entries)

3. Click *Security Options*, and make the changes in the following sections:

   **Accounts**
   - Guest account status – *Disabled*
   - Rename administrator account (i.e. “HighLevel”) 
   - Rename guest account (i.e. “DoNotUse”)
• Domain member
• Require strong (Windows 2000 or later) session key – **Enabled**

**Interactive logon**
• Do not display last user name – **Enabled**
• Do not require CTRL+ALT+DEL – **Disabled**
• Message text for users attempting to log on – **Set a logon message if desired** (i.e. “This computer is the property of company X. Authorized use only.”)
• Message title for users attempting to log on – **Set a logon message if desired**

**Microsoft network client**
• Send unencrypted password to third-party SMB servers – **Disabled**

**Network access**
• Allow anonymous SID/Name translation – **Disabled**
• Do not allow anonymous enumeration of SAM accounts – **Enabled**
• Do not allow anonymous enumeration of SAM accounts and shares – **Enabled**
• Do not allow storage of credentials or .NET Passports for network authentication – **Enabled**
• Let **Everyone** permissions apply to anonymous users – **Enabled**
• Shares that can be accessed anonymously – **Do Not Enter Anything** (By default, there are no values in this setting)
• Sharing and security model for local accounts – **Classic**

**Prevention of “Null Session” attacks:**
• Named Pipes that can be accessed anonymously (Remove Entries)
• Remotely accessible registry path (Remove Entries)
• Remotely accessible registry paths and sub-paths (Remove Entries)
• Shares that can be accessed anonymously (Remove Entries)
These are the default values for the above keys:

- **Named Pipes:**
  - Do Not Enter Anything: by default there are no values in this setting

- **Remotely accessible registry path**
  - System\CurrentControlSet\Control\ProductOptions
  - System\CurrentControlSet\Control\Server Applications
  - Software\Microsoft\Windows NT\CurrentVersion

- **Remotely accessible registry paths and sub-paths**
  - System\CurrentControlSet\Control\Print\Printers
  - System\CurrentControlSet\Services\Eventlog
  - Software\Microsoft\OLAP Server\Software\Microsoft\Windows NT\CurrentVersion\Print
  - Software\Microsoft\Windows NT\CurrentVersion\Windows
  - System\CurrentControlSet\Control\ContentIndex
  - System\CurrentControlSet\Control\Terminal Server
  - System\CurrentControlSet\Control\Terminal Server\UserConfig
  - System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration
  - Software\Microsoft\Windows NT\CurrentVersion\Perflib
  - System\CurrentControlSet\Services\SysmonLog

**Network security**

- Do not store LAN Manager hash value on next password change – **Enabled**
- LAN Manager authentication level
  - **Send NTLMv2 response only. Refuse LM & NTLM**
- Minimum session security for NTLM SSP based (including secure RPC) client
  - Check **Require NTLMv2** and **Require 128-bit encryption**
- Minimum session security for NTLM SSP based (including secure RPC) server
  - Check **Require NTLMv2** and **Require 128-bit encryption**

**Recovery console**

- Allow automatic administrative logon – **Disabled**