Security Configuration Guide for Microsoft Windows 7 Enterprise Workstation

Security Configuration Guide for Microsoft Windows 7 Enterprise Workstation
Document Author: Catherine J. Ullman
Last Revision: August 2011

Table of Contents

1. Abstract

This document provides a baseline guide to securing the Microsoft Windows 7 Enterprise Workstation operating system as a member workstation in an Active Directory domain in the University at Buffalo computing environment. The intended audience of this internal document is IT administrators and support staff at the State University of New York at Buffalo.

2. How to Use this Guide

The security guideline section 5 below involves implementing group policies. Each setting must be carefully examined before implementing the recommended changes. Do not attempt to implement any of the settings in this guide without first testing in a non-production environment. The entire process for each workstation may take several minutes to even hours (especially if you are doing this for the first time), depending on the level of security enhancement you choose to implement.
Consider the following important issues before deciding to apply system changes:

•Much of the security enhancement changes are implemented in the Registry. Before you edit the registry, make sure that you understand how to restore a registry key(s) with Registry Editor if a problem occurs.

•In order for the majority of the changes to take effect, you must reboot the workstation.

•As you take each action or simply audit applicable areas throughout the steps, document each change you implement. You may print this document, put checkmarks next to the items you implement, and use the hardcopy for record-keeping purposes.

Although below recommendations will lead to significantly a more secure workstation, keep in mind that no computer on the wire (or wireless) is completely immune from well-seasoned hackers whose tools and techniques are becoming more sophisticated and detrimental everyday.

3. Preliminary Requirements

---

1. Read University at Buffalo's IT Use Policies at:
http://www.itpolicies.buffalo.edu/
2. Make sure the NETBIOS name of the workstation and DHCP/DNS name of the workstation match.
3. Activate/Install and Configure Firewall - Activate the built in Windows firewall or install another firewall package and configure it to block all unnecessary incoming connections at a minimum. The current University licensed package is Symantec Endpoint Protection software. If using SEP be sure both Proactive Threat Protection and Network Threat Protection (firewall) is enabled.
4. Install anti-virus software and make sure the definitions are up to date. Configure the definitions to update daily if possible or as often as possible if not daily.
5. Disable or remove unnecessary services and applications.
6. Apply the latest Windows 7 operating system Service Pack.
7. Apply security hotfixes, or patches, to date for both the operating system and all third party applications using HFNetChkPro.
8. Assign the built in Administrator account a secure passphrase, but do NOT enable it.
9. Create a new local Administrator account with a secure passphrase.
10. Download and install the Security Compliance Manager from here:
http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=16776 **NOTE: This step is REQUIRED to obtain baseline policies listed below.

4. File/Disk System

4.1. It is generally recommended that all partitions be NTFS.* Partitions should be set to NTFS upon install of the operating system or the correct permissions will not be applied. *Note: It is understood that the typical Windows 7 install creates a hidden OEM partition, which is fine.

4.2 Note: By default, the "Last Accessed Time" file property is not enabled in Windows 7. Any machines handling Regulated Private Data or Protected Data (see section below for classifications) should enable this property. Enabling this property is required for potential forensic investigations to determine if the data on the machine was exposed as required by NYS law.
This property can be changed in the registry manually or via Group Policy.
Set the HKLM\SYSTEM\CurrentControlSet\Control\FileSystem\NtfsDisableLastAccessUpdate key to 0.

5. Recommendations via Data Category Breakdown

NOTE: Apply the appropriate Microsoft baseline policy via group policy. (See Prerequisite Step #10) There are two categories of policies: EC (Enterprise Computing), and SSLF (Specialized Security Limited Functionality). Within these categories there is baselines for desktop machines and separate one for laptop machines. Two baseline policies also exist for using Bitlocker with either a laptop or a desktop.
NOTE - The following policy recommendations are based on the University at Buffalo's data classification standards which can be found here:
http://itpolicies.buffalo.edu/data-sec/Data%20Classification%20Standard-...

5.1 **Category I: Regulated Private Data** - Machines used by employees whose job duties require handling Category I: Regulated Private Data (e.g. SSN, Driver's License #, Credit/Debit Card #, etc. - see data classification standard for additional examples and more detail)

5.1.1 Machines used by employees that process Regulated Private Data should have the Win7-SSLF-Desktop or Win7-SSLF-Laptop baselines applied to them at a minimum. If the hardware supports it, they should be running some form of full disk encryption as well. If Bitlocker is being used for encryption, the Win7-Bitlocker-SSLF policy should also be applied.

5.1.2 No user who handles Regulated Private Data should be a member of the local Administrators group on the machine. All users should be members of the local Users group on the machine only.

5.1.3 Additional policy to remove modify rights to the %SystemDrive% must also be created and applied. Additional group policy should be set to remove modify rights (write or delete) to the root of the System Drive for the built in Users group. This policy can be found under Computer Configuration-Policies-Windows Setting-Security Setting-File System

5.1.4 Deploy and apply an AppLocker Policy
An AppLocker Policy should be applied to all machines used by employees whose job duties require handling Regulated Private Data. All Default Rules, Windows Installer Rules and Script Rules should be enabled and then exceptions added only for necessary legitimate applications. *NOTE*: Exception rules for AD scripts such as startup, shutdown, login and logout scripts will be required for EACH domain controller (i.e. \\itorg-cc1.itorg.ad.buffalo.edu\netlogon\ubda*)
For additional details see Microsoft's documentation which can be found here:
http://technet.microsoft.com/en-us/library/dd723678(WS.10).aspx

5.2 **Category II: Protected Data** - Machines used by employees whose job duties require handling Category II: Protected Data (e.g. FERPA, HR employment data, IT Infrastructure data, etc - see data classification standard for additional examples and more detail)

5.2.1 Machines used by employees that process Protected Data should have the Win7-EC-Desktop or Win7-EC-Laptop baseline applied to them at a minimum.

5.2.2 No user who handles Protected Data should be a member of the local Administrators group on the machine. All users should be members of the local Users group on the machine only.

5.2.3 Additional policy to remove modify rights to the %SystemDrive% must also be created and applied. Additional group policy should be set to remove modify rights (write or delete) to the root of the System Drive for the built in Users group. This policy can be found under Computer Configuration-Policies-Windows Setting-Security Setting-File System

5.2.4 An AppLocker Policy should be applied to all machines used by employees whose job duties require handling Protected Data. All Default Rules, Windows Installer Rules and Script Rules should be enabled and then exceptions added only for necessary legitimate applications. *NOTE*: Exception rules for AD scripts such as startup, shutdown, login and logout scripts will be required for EACH domain controller
(i.e. \\itorg-cc1.itorg.ad.buffalo.edu\netlogon\ubda*)
For additional details see Microsoft's documentation which can be found here:
http://technet.microsoft.com/en-us/library/dd723678(WS.10).aspx

5.3 **Category III - Internal Use Data** - Machines used by employees whose job duties require handling Category III: Internal Use Data (e.g. University Financial Data, University Person Number, Licensed Software, etc. - see data classification standard for additional examples and more detail)

5.3.1 Machines used by employees that process Internal Use Data should have the Win7-EC-Desktop or Win7-EC-Laptop baseline applied to them at a minimum.

5.3.2 No user who handles Internal Use Data should be a member of the local Administrators group on the machine. All users should be members of the local Users group on the machine only.

5.3.3 Additional policy to remove modify rights to the %SystemDrive% must also be created and applied. Additional group policy should be set to remove modify rights (write or delete) to the root of the System Drive for the built in Users group. This policy can be found under Computer Configuration-Policies-Windows Setting-Security Setting-File System

5.3.4 An AppLocker Policy should be applied to all machines used by employees whose job duties require handling Internal Use Data. All Default Rules, Windows Installer Rules and Script Rules should be enabled and then exceptions added only for necessary legitimate applications. *NOTE*: Exception rules for AD scripts such as startup, shutdown, login and logout scripts will be required for EACH domain

controller
(i.e. \\itorg-cc1.itorg.ad.buffalo.edu\netlogon\ubda*)
For additional details see Microsoft's documentation which can be found here:
http://technet.microsoft.com/en-us/library/dd723678(WS.10).aspx

6. Possible Baseline Issues

6.1 There are a number of possible conflicts between standard UB practices and the baseline policies set above. Below are a few of the known potential issues and suggestions for mitigation.

6.1.1 Any setting that Requires NTLM v2 only might cause communication issues with older servers or clients (pre-Windows 2000) or systems not configured to use NTLMv2. Older clients that do not support these security settings will be unable to communicate with the computer. As there is a significant security risk in using older versions of NTLM, the best mitigation is to upgrade the older clients or to change the settings on the other machines as needed.

6.1.2 Microsoft Network Client: Digitally sign communications (always) and Microsoft Network Server: Digitally sign communications (always) can cause communication problems with storage in UBFS space. These must be set to Disabled to resolve the problem. For more information
see: http://support.microsoft.com/kb/887429/en-us

6.1.3 Devices: Allowed to format and eject removable media - be aware that the default in all security policies is to only allow Administrators this permission. Although using external media presents a security risk, you may find that it is necessary for business practices.

6.1.4 Interactive Logon: Prompt user to change password before expiration - the default for this setting is 14 days, which could become problematic since at UB our AD accounts are synchronized with our UBIT passwords.

6.1.5 User Account Control: Behavior of the elevation prompt for standard users - the default for this setting is Automatically deny elevation requests. While this setting is ideal, support staff may find it frustrating. If this setting impedes support, it can be changed to 'Prompt for credentials'.

6.1.6 Windows Firewall settings - by default, the Windows Firewall settings are all ON. If using the Symantec Firewall or other third party product instead, you may want to alter this setting.

6.1.7 Windows Update settings - be aware that WSUS settings are configured here so if you already have a GPO for these settings already, the two might conflict unless prioritized in the proper order.