JOHNS HOPKINS

Institutional Computing Standards

Standards and Guidance for Windows Client Administration and Security

Created by IT @ JH

I. Table of Contents

II. Introduction

This document is written to support the operation of Windows-based clients at Johns Hopkins institutions. The objective of the document is to provide for effective and consistent management of Windows client systems. The goal of each standard is to enhance security of client systems that generally share the Hopkins backbone network resources. All systems must be administered securely as to not adversely affect other systems. This document is not meant to be a substitute for formal training of the Windows administrator. Windows client management is a complex system and should be administered by skilled personnel.

A. Background

This standard incorporates input from previous Windows standards and IT @ Johns Hopkins standards related to Windows server and workstation administration.

B. Policy

This standard applies to Windows clients and is required for systems that access, store, process or transmit Restricted information or serve or support another critical business purpose. Computing Device Security is addressed in JH IT Policies:

9. Computing Device Security

Administrators, managers and users share the responsibility of maintaining the security of servers, workstations and other computing devices.

Administrators and users managing their own devices are required to:

a. Protect any device under their management from compromise.

b. Modify default installation passwords and other configuration options to reduce vulnerabilities to a minimum.

c. Install updated anti-virus (see Anti-Virus Policy above) relevant security patches to fix security issues

d. Periodically verify audit and activity logs, examine performance data, and generally check for any evidence of unauthorized access, the presence of viruses or other malicious code.

e. Cooperate with IT@JH by providing support for and/or review of administrative activities as well as performing more sophisticated procedures such as penetration testing and real-time intrusion detection.

Administrators and managers who develop, maintain, or modify critical applications relating to Restricted information must deploy adequate procedures for change control, separation of test and production environments, and separation of responsibilities for staff involved in these functions. They must actively cooperate with IT@JH, the Office of Hopkins Internal Audits and other JH administrative entities working in application security.

Source: http://it.jhu.edu/policies/itpolicies.html

C. Audience

The target audience for this document is anyone who is responsible for deploying, building, and/or administering any Windows client systems on the Johns Hopkins Network. This document is intended for administrators who have some Windows administration experience.

D. Scope

This standard applies to all client systems running Windows Vista or later versions including Windows 7, Windows 8, Windows 8.1, and Windows 10.

Note: While the ICSC intends to keep this document updated frequently, issues related to Windows Client administration change rapidly with technology. It is therefore strongly recommended that administrators keep current with Microsoft documentation and updates. Discrepancies between these standards and Microsoft documentation should be directed to itpolicy@jhu.edu.

Microsoft online resources provide comprehensive, up-to-date technical guidance on all aspects of Windows server administration. This document provides high-level guidance for administrators supporting one or more Windows servers and links to Hopkins and Microsoft services.

E. Enforcement

Enforcement of IT Policies is intended to safeguard shared resources. It may be necessary to enforce specific standards in this document to ensure availability, performance or security of JH IT Resources.

III. Configuration Checklist

The configuration checklist below is required for IT@JH-managed clients and considered good practice for others..

- ☐ Name system according to a Client System Naming Convention
- ☐ Add client system to Windows Domain
- ☐ Implement Full Disk Encryption
- ☐ Local Account Management: Disable or delete any unnecessary user accounts. All passwords must be changed from vendor-supplied defaults
- ☐ Rename Administrator account and configure administrator password policies (15 characters minimum, both alpha and numeric characters)
- ☐ Rename and disable the guest account
- ☐ Remove all unnecessary file shares. Verify permissions on all shares that are necessary.
- ☐ Disable unnecessary services (or conversely, enable necessary services). It is the responsibility of the system administrator to determine what services should be disabled.
- ☐ Configure Audit Policy
- ☐ Configure event log settings
- ☐ Configure a logon message for user interfaces
- ☐ Disable SMB1 and configure SMB signing or disable SMB
- ☐ Apply all security updates. If patches cannot be applied due to software incompatibilities or other conflicts, it is the responsibility of the system

administrator to understand the vulnerability and implement appropriate measures to mitigate the vulnerability

- □ Apply all hardware management, driver and firmware updates
- □ Update Local Security Policy for “Pass the Hash” Mitigation
- □ Install KB and set registry for WDigest
- □ Configure Network settings
- □ Install Endpoint Protection software. Configure it to automatically update definitions. Apply an appropriate configuration for cleaning/quarantine/deletion of infected files, and configure notification of infections
- □ Configure Remote Desktop Security settings
- □ Configure Internet Explorer settings
- □ Configure browser settings to protect against WPAD vulnerability
- □ Configure Windows Telemetry
- □ Review Additional Local Security settings
- □ Ensure system is properly inventoried and monitored, critical data is backed up, and has proper Security Event Log Retention

IV. Physical Security

Users must provide physical security for their IT devices and storage media. Particular care must be paid to securing portable equipment and media -- such as notebook computers, PDAs, tapes, CDs and cellular phones -- especially when traveling in order to protect these devices. Confidential information may not be stored on portable devices or other media unless encrypted.

Device Encryption -- It is the responsibility of client system administrators to assess risk regarding physical loss or theft of mobile and stationary devices. Appropriate security controls to address these risks include physical security safeguards above, restrictions on access and encryption. See Section

- All laptops and mobile devices reasonably likely to be used to store Restricted information must have full disc encryption installed and activated. Laptop computers and mobile devices used by Johns Hopkins Medicine personnel for work purposes (including peronally owned devices) are presumed to be reasonably likely to store Restricted information unless designated otherwise by appropriate staff.

- All at-risk workstations (e.g. accessible to the public, open spaces, etc.) reasonably likely to store Restricted information must have full disc encryption installed and activated.

All servers storing Restricted information (e.g. file servers, email servers, databases) must be stored in a data center or otherwise secure area as described above. It is strongly recommended that such servers be placed in full service data centers.*Source:* http://it.jhu.edu/policies/itpolicies.html

V. Hardware Standards Committee

The Desktop Hardware Standards Committee consists of members of Purchasing and IT groups across JHU and JHM. This group defines desktop, laptop and tablet standards where Johns Hopkins receives the biggest discount on Dell and other products from our hardware Value-Added-Reseller, FutureTech.

Johns Hopkins Hardware Committee Roles & Responsibilities:

- Participate in quarterly review of current standards
- Participate in technology roadmap reviews two times per year
- Recommend updates to default options within the standards
- Review and recommend options and accessories for inclusion as options within the standards
- Review and recommend replacements and/or reduction of standard models
- Recommend actions that will promote adoption of standards
- Provide feedback on proposed changes to functionality on the purchasing web site
- Identify cost-saving opportunities
- Identify potential adverse impact of proposed changes to standards

This group is chaired by the Director of Client Technology Services (CTS) and the group email is listed below:

Desktop Hardware Standard Committee: desktopcommittee@lists.johnshopkins.edu

VI. System Installation and Configuration

A. Preparation

Required:
Before beginning an installation, the administrator should adhere to a naming convention and utilize a renamed administrator account, according to a sensible naming standard. Installation should proceed as though the client system will be under attack once it is installed on the network. It is therefore critical that the installation package include all recent security updates. In cases, where an older version must be installed, installation should take place completely off-line.

Microsoft security updates
http://windowsupdate.microsoft.com/

B. Client System Naming Conventions

Required for IT@JH:
A standard naming convention is important for identifying client system administrators for security and operational purposes. Typical workstation naming at Johns Hopkins is in the format of *OUNameorPrefix*-AssetTag. For example, computers managed by CTY would be CTY-AssetTag. Each group is free to choose their own naming convention. However, client systems should not contain any information about the user (e.g. JHED ID, Name, etc.) to protect the privacy of the customer.

It is best to ensure all computer names are 15 characters or less. While the 15-character limit is originally a NetBIOS computer name limitation, Windows and most Windows management systems will truncate a computer name to 15 characters.

Microsoft article on Naming Conventions: https://support.microsoft.com/en-us/kb/909264

VII. Security

A. Endpoint Protection

Required:
All Windows client systems on the Johns Hopkins network are required to run Endpoint Protection software. The current standard is System Center Endpoint Protection 2012 R2. A comprehensive guide may be found here.

IT@JH Antivirus Webpage: http://it.jhu.edu/antivirus/

Recommended:
It is recommended that LAN Admins review and create endpoint protection exclusion policies on their Windows client systems to ensure proper performance of their Windows client systems.

Microsoft Anti-Virus Exclusion List:
http://social.technet.microsoft.com/wiki/contents/articles/953.microsoft-anti-virus-exclusion-list.aspx

B. Auditing

Having the proper Windows Client auditing settings configured is critical to ensure proper monitoring and investigation when a system is compromised or has a critical issue.

Required:
The "legacy" Windows audit policy should only be used if you have Windows Vista systems. If you do not have Windows Vista systems in your environment, please see the Advanced Auditing section.

These include baseline recommendations below.

Audit Policy	**Security Setting**	
	Success	**Failure**
Audit account logon events	√	√
Audit account management	√	√
Audit logon events	√	√
Audit object access		√
Audit policy change		√

Audit Policy	**Security Setting**	
	Success	**Failure**
Audit privilege use		√
Audit process tracking	√	
Audit system events		√

Advanced Auditing
Introduced with Windows 7, Advanced Auditing provides a more granular ability to audit specific event types, rather than all events for a single category. This helps reduce the number of audited events. If you do not have Windows Vista systems to manage, it is recommended to only use the Advanced Auditing for your Windows clients. If you have Advanced Auditing enabled, Windows will ignore any "legacy" auditing settings defined.

Required for IT@JH and Recommended elsewhere:
Command Line Auditing
Introduced with a February 2015 Security Update, MS15-011, Command Line Auditing is available in Windows 7 and higher. This feature provides additional logging to help monitor and investigate activity when running cmd.exe or cscript.exe. To use this feature, Advanced Auditing (specifically Detailed Tracking-Process Creation) must be enabled. This can be set within Group Policy located at:

Computer Configuration\Policies\Administrative Templates\System\Audit Process Creation\Include command line in process creation events – Set this value to Enabled.

Advanced Auditing Recommendations for all domain member systems

Audit Category	**Policy**	**Setting**
Account Logon	Audit Credential Validation	Success
	Audit Other Account Logon Events	Success, Failure
Account Management	Audit Application Group Management	Success, Failure
	Audit Computer Account Management	Success, Failure
	Audit Security Group Management	Success, Failure
	Audit Other Account Management Events	Success, Failure
	Audit User Account Management	Success, Failure
Detailed Tracking	Audit Process Creation	Success, Failure

	Audit Process Termination	Success, Failure
Logon/Logoff	Audit Account Lockout	Success, Failure
	Audit Logoff	Success, Failure
	Audit Logon	Success, Failure
	Audit Other Logon/Logoff Events	Success, Failure
	Audit Special Logon	Success, Failure
Policy Change	Audit Audit Policy Change	Success, Failure
	Audit Authentication Policy Change	Success, Failure
Privilege Use	Audit Non Sensitive Privilege Use	Failure
	Audit Other Sensitive Privilege Use	Failure
	Audit Sensitive Privilege Use	Failure
System	Audit Security State Change	Success, Failure
	Audit System Integrity	Success, Failure

Recommended:
Folder File Auditing
In order to be aware of changes to critical files, auditing can be enabled on critical files or folders in Windows Clients. It is recommended to only selectively audit critical/sensitive/Restricted file access, as these events can create excessive events. Here is example of auditing recommended for any critical files or folders. It should be considered rare to have File Auditing on Windows Clients.

Access	**Successful**	**Failed**
Traverse Folder / Execute File		√
Read Attributes		√
Read Extended Attributes		√
Write Attributes	√	√
Write Extended Attributes		√
Delete Subfolders and Files	√	√
Delete	√	√
Read Permissions		√
Change Permissions	√	√
Take Ownership	√	√

PowerShell Auditing
At the present time, one of the most common techniques for malware is to use PowerShell to perform their malicious actions. By enabling PowerShell Logging, this can better identify actions that a malicious process has taken. It is highly recommended to also have Windows Management Framework 5.0 or higher installed on the Windows client system for maximum effect.

PowerShell Auditing can be set via Group Policy by enabling the settings listed here:

Computer Configuration\Policies\Administrative Templates\Windows Components\Windows PowerShell
Turn On Model Logging - Set to Enabled and Module Names Set to *
Turn on PowerShell Script Block Logging – Set to Enabled and Check Log script block invocation start/stop events

C. OS and Application Updates

Required:
All Windows client systems <u>must</u> run a Microsoft-supported OS version. (link)
Windows client systems should receive all Security Updates (MSXX-XX updates) in a timely manner. A timely manner is defined as systems having all Security Updates (MSXX-XX updates) applied within 30 days of release.

Recommended:
It is recommended Windows Software Updates can be automatically applied via the local 'Windows Software Update' , through the enterprise (WSUS) Windows Server Update Services or by using Software Updates in SCCM. Administrators should have documented procedures for testing, evaluating and deploying updates rapidly, preferably within the first two weeks for most updates. For out-of-band and critical updates, it may be necessary to expedite the update process. It is generally acceptable to leverage testing and update deployment schedules established by IT @ JH and follow its lead. There may be exceptions where the client in question runs a vulnerable system or service.

In addition to Microsoft Security Updates, Adobe and other common third-party application vendors frequently issue security updates. Just as with Microsoft updates, IT groups should test and evaluate each update. IT administrators should assess risk and consider following ICSC recommendations regarding individual 0-day updates or patches.

Download Critical Updates:
http://windowsupdate.microsoft.com/
Enterprise Update Server:
http://www.it.johnshopkins.edu/services/monitoring/sus.html

Contact for WUS/SCCM resources: monitoring@jhmi.edu

D. Encryption

Required:
All Johns Hopkins Medicine laptops and desktops are required to be encrypted using full disk encryption software. For all Microsoft Windows computers, this means using the Windows BitLocker technology.

Full disk encryption - BitLocker Drive Encryption is a data protection feature available in all supported Windows client Operating Systems. BitLocker provides enhanced protection against data theft, especially if a computer is lost or stolen. Full disk encryption tools other than Bitlocker are addressed in the *Encryption Standards* below. Non-Bitlocker tools are only acceptable for limited purposes where Bitlocker cannot be implemented.

Microsoft BitLocker Administration and Monitoring - For Johns Hopkins owned computers that are protected by BitLocker, the computer is required to be managed by Microsoft BitLocker Administration and Monitoring (MBAM). MBAM provides a web-based administrative interface for managing and monitoring BitLocker Drive Encryption on Windows systems. This includes reporting on encryption status across all JHM computers, the ability to recall a BitLocker recovery key to unlock a drive and audit data on for when a recovery key was recalled and who recalled it. All data that is stored in MBAM resides in an encrypted database and access is limited to authorized IT staff. Additional information about MBAM, its requirements, usage and how to deploy the MBAM client can be found in the MBAM 2.5 SP1 Overview and Usage guide in the MBAM SharePoint site.

MBAM SharePoint Site
https://collaborate.johnshopkins.edu/sites/EMMS/MBAM/.

Physical Security of IT Resources Policy addressing encryption
http://www.it.johnshopkins.edu/policies/itpolicies.html#Physical

Encryption Standards
http://www.it.johnshopkins.edu/policies/standards.html

E. Third Party Application Security Updates

Required:
Software that is installed on Windows client systems will eventually have vulnerabilities that need to be addressed. Many of these vulnerabilities are exploitable when browsing the internet or accessing email. Other software vulnerabilities are exploitable via remote methods and they must be addressed in a timely manner. Some typical vulnerabilities that need to be addressed in a timely manner are: Browser plug-ins such as Java, Flash, Adobe Reader, or Shockwave. Web browser plug-ins are often a target for 0-day exploits.

IT groups must have procedures in place to identify and quickly update their systems in the event of a third-party software security patch. IT groups should have dynamic inventory and software delivery solutions to update systems quickly, in the event of a 0-day exploit. IT groups are expected to provide reports to verify that their systems are updated to IT Security or IT Audit personnel when requested.

F. Microsoft Baseline Security Analyzer

Recommended:
The Microsoft Baseline Security Analyzer (MBSA) is a tool to scan Windows and Office security settings and updates. This includes missing security updates and a vulnerability assessment of registry and application configurations. MBSA can be run locally on a client system or remotely from a workstation where the user has Administrative rights. This tool can also be used to scan a large number of systems remotely.

Download MBSA
http://www.microsoft.com/en-us/download/details.aspx?id=7558

G. Local User Accounts

Use of Local Accounts on Windows Client systems should be limited. IT Staff should use JHED accounts when the Windows Client is on the network and only use the renamed Administrator account when there is limited or no network connectivity.

Required:
Rename Administrator account: Rename the built-in Administrator (do not delete) account and choose a strong administrator password (a minimum of 15 characters). In Windows Vista and above, passwords can be up to 127 characters long. Passwords should include UPPER and lower case letters, as well as non-alphanumeric characters. Administrator passwords should be changed via encrypted methods on a regular schedule and be randomized across groups of client systems.

Rename and Disable the Guest account: Rename the built-in Guest (do not delete) account and disable the account. Administrators may choose to set a strong password, but this is not necessary as long as the account is disabled and renamed.

Recommended:
Add and remove domain accounts: Remove any unneeded Domain accounts (e.g., Domain Admins) from Local Users and Administrators Groups. Add appropriate Domain Security Groups to their respective local groups.

Disable or remove any local accounts: Accounts that may be created by vendors, applications or other third-parties should be discouraged and strongly considered to be disabled or deleted. Domain Service Accounts are recommended to meet these needs.

Use of Microsoft's Local Administrator Password Solution (LAPS): In 2015, Microsoft released a tool called LAPS for randomizing, and securely changing the Local Administrator Password. This tool utilizes a client installation and group policy settings to define a randomized Administrator password. More information can be found in the detailed instructional document, located here:

https://collaborate.johnshopkins.edu/sites/EMMS/SCCM/Documents/Automated%20Local%20Administrator%20Password%20Change.docx?Web=1

H. Enterprise Authentication

The Enterprise Directory is utilized for authentication and access control. It allows for the creation and management of a single identity for Hopkins' faculty, staff and students.

Required:
All systems should reside in a Windows Domain where user accounts use an approved password complexity policy, accounts are monitored for inappropriate access, and both user and computer accounts are de-provisioned when staff or Windows computer systems are no longer employed by (users) or owned by (computers) Johns Hopkins. Local accounts on behalf of individuals and groups should not be used for day-to-day operational use.

Recommended:
The Enterprise Active Directory (WIN domain) provides the means to access and manage network resources on the Johns Hopkins' network. Windows clients should reside in a managed Organizational Unit (OU) within the WIN domain. Active Directory provides a number of benefits for client systems, primarily the use of Group Policy Objects (GPOs), to better manage and secure client systems.

Active Directory Services information:
http://www.it.johnshopkins.edu/services/directoryservices/ad/

Contact for Enterprise Directory resources: ad@jhmi.edu

I. Auto logon Workstations

For multi-user workstations, specifically for "Public" or "Clinical" workstations, it is desirable to use an account for automatic logons. In conjunction with ESSO (Imprivata OneSign), an auto logon can provide a number of benefits for clinical customers.

Required:

- Auto logon account must be a generic account (i.e., not a JHED ID)
- The account should not be a member of the Domain Users group, but a special group with only rights as a User on the Workstation
- The generic account password must be changed regularly; every 180 days at a minimum
- While auto logon practices store the password in plain text in the registry, steps should be made to ensure the password is not exposed elsewhere (e.g., Group Policy, local file system).
- With new regulatory requirements, Johns Hopkins may be required to identify the identity of people who have accessed a specific PC (or server). Therefore, if you use a generic account, you should be prepared to identify the JHED ID of anyone using the system. The most cost effective approach to meet these new regulatory requirements should be using ESSO.

Recommended:

- The generic account should be monitored for lockouts.

J. Internet Explorer Settings

There are a number of customizations that are available to better secure web browsing with Internet Explorer.

Internet Explorer Zones:
Internet Explorer has four different zones for security configuration: Internet, Local Intranet, Trusted sites, and Restricted sites. Each zone has a different default security level that determines what kind of content might be blocked for that site. Depending on the security level of a site, some content might be blocked until you choose to allow it, ActiveX controls might not run automatically, or you might see warning prompts on certain sites. You can customize the settings for each zone and decide which websites belong in which zone.

For systems that are locked down, such as Kiosk or "Public" Workstations, it is best to use a Site to Zone Assignment List GPO to assign sites to zones in IE.

> *User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page*

To apply sites to zones to "Private" workstations where customers should be able to edit their IE Zone Settings, it is best to assign Internet Zones through group policy using Registry key entries.
The Registry Key location is found here:

> *HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains*

To configure Internet Explorer settings, it is recommended to use the group policy preference found here:

> *User Configuration\Preferences\Control Panel Settings\Internet Settings*

Internet Explorer History:
Ensure that the "Do not set Delete Browsing History on Exit" setting is <u>not</u> set:

> *User Configuration\Administrative Templates\Windows Components\Internet Explorer\Delete Browsing History Value name: Configure Delete Browsing History on exit*

Ensure that PCs are able to keep the IE History for at least 30 -90 days:

> *Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Delete Browsing History with a Value name of Disable "Configuration History"*

Internet Explorer Enterprise Mode:
Enterprise Mode for Internet Explorer (EMIE) is a feature that Microsoft introduced with Internet Explorer 11 to enable enhanced compatibility with previous versions of Internet Explorer. Web sites are configured to use EMIE via centrally managed site lists.

Enterprise Mode site lists are centrally managed XML files that contain lists of web sites and the preferred compatibility settings for each web site. Test and production site lists are available. Web sites must be tested on the test site list before they can be added to the production site list.

The test site list can be downloaded in XML format from the following URL:
http://esgiisconfig.jh.edu/ECM-EnterpriseModeSiteList-Test.xml

The production site list can be downloaded in XML format from the following URL:
http://esgiisconfig.jh.edu/ECM-EnterpriseModeSiteList-Prod.xml

Contact for Internet Explorer Enterprise Mode: EDE@jhmi.edu

Chrome: Chrome has become a popular web browser and is often installed by customers. It is recommended that IT groups utilize the Google Chrome Enterprise version and look to manage Chrome settings. Details on management of Chrome can be found in the Chrome Enterprise Admin Guide.

Chrome Enterprise Admin Guide
https://collaborate.johnshopkins.edu/sites/EMMS/SCCM/Documents/IT%40JH-Google_Chrome_Enterprise-AdminGuide.docx?Web=1

K. Applocker

Recommended:
Applocker was introduced in Windows 7 and above and provides application whitelisting/blacklisting for Windows client systems. Applocker provides IT Administrators the ability to allow or deny applications from running based on unique identities of files and to specify which users or groups can run those applications. Applocker can be used to just allow/block specific file types/hashes, registry paths, or deny access for specific users.

Applocker has two modes: Audit Only and its regular implementation. Applocker writes audit only and blocking events to the Applocker log located in Event Viewer\Application and Services Logs\Microsoft\Windows\Applocker.

With Applocker, it is important to exclude IT Administrators and SYSTEM accounts from the Implicit Deny permission. This can prevent IT Administrators from servicing the Windows client or prevent the machine from working (SYSTEM).

How Applocker Works: https://technet.microsoft.com/en-us/library/ee460948(v=ws.11).aspx

L. EMET

Required:
The Enhanced Mitigation Experience Toolkit (EMET) is add-on software from Microsoft that provides an extra layer of defense against malware attacks and Windows client application exploits by preventing common attacks against system memory. EMET uses security mitigation technologies that function as additional protections and obstacles that makes exploitation much more difficult.

Recommended:
Windows 10 1607 has many of the same protections as EMET, but does not protect for some applications (i.e. Java, Adobe). EMET is not required for Windows 10 1607 and above, but recommended for systems that run Java and Adobe products.

EMET Download: https://www.microsoft.com/en-us/download/details.aspx?id=50766

M. SMB Protocol Security

Required:
Disable SMB1: SMB1 is a protocol that is nearly 30 years old and is enabled by default on nearly every Windows version. There are very few cases where SMB1 needs to be enabled, most revolve around Windows XP or Windows 2003 system requirements. This can be done through a registry change (SMB Server) or command line/PowerShell (SMB Client).

SMB Server
Registry
To enable or disable SMBv1 on the SMB server, configure the following registry key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters
Registry entry: SMB1
REG_DWORD: 0 = Disabled

Windows 7 and Windows Vista - PowerShell

```
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" SMB1 -Type DWORD -Value 0 –Force
```

Windows 8 –PowerShell

```
Set-SmbServerConfiguration -EnableSMB1Protocol $false
```

Windows 10 – PowerShell

```
Remove-WindowsFeature FS-SMB1
```

SMB Client
Windows 7, Windows Vista, Windows 8 Command Line

```
sc.exe config lanmanworkstation depend= bowser/mrxsmb20/nsi
sc.exe config mrxsmb10 start= disabled
```

Windows 10 – PowerShell

```
Disable-WindowsOptionalFeature -Online -FeatureName
smb1protocol
```

Recommended:
SMB Signing or Disable SMB: Ensuring that the SMB protocol has SMB signing set to enabled is an important security configuration for preventing “man in the middle” attacks. This should be set for client systems for both SMB Server and SMB client. If SMB1 and SMB2/3 are set to disabled, then SMB signing is not required.

Enabling signing via Group Policy determines whether SMB signing must be negotiated before further communication with an SMB client. This can be set within Group Policy located at:

SMB Server Signing
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network client: Digitally sign communications (always) Set to Enabled

SMB Client Signing
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Digitally sign communications (always) Set to Enabled

N. Pass the Hash Mitigation

The Windows “Pass the Hash” vulnerability allows an attacker to use credentials of accounts that have logged in to a Windows system and pass the credentials on to another Windows system. Details of this vulnerability are addressed in the SANS reading room article “Pass the hash attacks: Tools and Mitigation” and on various pass the hash toolkit sites.

Required:
Avoid LM and NTLM challenge response: These are older protocols used by Windows OSes prior to Windows XP and were primarily used for authentication in workgroups. LM and NTLM challenge-response are considered weak protocols and should no longer be used unless there is a significant requirement. It is best to only use Send NTLMv2 as response and configure settings to not store LAN Manager hash values. This can be set within Group Policy located at:

> *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network Security: Do not store LAN Manager hash value… &*
> *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\ Network Security: LAN Manager Authentication level Set to Send NTLMv2 response only. Refuse LM & NTLM*

Remove Admins from Debug Privilege: By default, Administrators have rights to Debug Programs. Malware writers can exploit this default setting to "pass the hash." Removing Administrators from this right can greatly reduce these exploits. This can be set via Local Security Policy or via Group Policy. It is recommended to use Local Security Policy or define an Active Directory Group only for this right (not Local Administrators), as some installations, such as Microsoft SQL Server, require this right to install the software or perform Service Pack installations. This can be set with the Local Security or Group Policy located at:

> *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Debug programs.*

Recommended:
Disable Cached Logons: This setting is used to define the number of previous logons to cache in the event that a Domain Controller is unavailable. While this setting is valuable for laptops and other mobile devices that may leave the JH Network, for systems that are always connected (i.e. VDI Systems, Desktops) it is recommended to set the cache value to zero. By default, Windows 7 caches 25 logons. This can be set with the Group Policy located at:

> *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Number of previous logons to cache*
> Set to 0

O. WDigest

Introduced with Windows XP and continued with all newer client Operating Systems, Microsoft added support for a protocol known as WDigest. The WDigest protocol is used for clients to send cleartext credentials to Hypertext Transfer Protocol (HTTP) and Simple Authentication Security Layer (SASL) applications based on RFC 2617 and 2831. Windows stores the password in memory for convenience when users log in to their local workstations. Windows 10 protects against this risk with the Credential Guard technology.

Required:
For systems below Windows 10, there are two requirements to mitigate against the WDigest attack technique:

- Installation of KB2871997 - https://support.microsoft.com/en-us/kb/2871997
- Set the Registry value *HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders\WDigest LogonCredential* value set to **0**

P. WPAD

Recommended:
An attack technique publicized in 2016 uses the proxy auto-config (WPAD) to convert HTTPS URL requests into plaintext. This technique can also be used by using malware to target the machine's network settings to use a malicious proxy server. This affects browsers on Windows, including Edge, IE, FireFox and Chrome. It is more important to disable this value on mobile devices than on desktop systems.

Chrome: https://www.expressvpn.com/support/troubleshooting/google-chrome-no-proxy/
FireFox: https://support.mozilla.org/en-US/questions/904019
Internet Explorer: Go to Internet Explorer-Internet Options-Connections-LAN Settings- and Uncheck Automatically detect settings

Chrome (Enterprise version) and Internet Explorer WPAD Disable settings are contained within the WIN Domain Group Policy called "Sample GPO for Windows Client Standard 2017" referenced at the end of this document.

Q. Services

Recommended:
Disable unnecessary services (e.g., file and print sharing and remote access should be disabled). These may waste system resources and create vulnerabilities. Other services that should be reviewed include:

- Help and Support Services
- Inter-site messaging
- Remote Access Connection Manager (if no VPN or Remote Access Service RAS are needed)
- Computer Browser
- Shell Hardware Detection
- Task Scheduler

NOTE – Do not disable the DHCP client service, as it is vital for Active Directory.

VIII. Networking

A. DNS / IP Configuration

Recommended:
The DNS request process for all JHU, JHMI, Johns Hopkins, and most organizationally owned domains has been consolidated into a centrally managed system. All Windows Client systems that receive DHCP provided IP Addresses are registered and updated dynamically in DNS.

IP addresses are provided via JHARS/Infoblox for all DHCP-assigned IP Addresses. For static IP Address requests, please contact the hostmaster.

DNS Requests:
Web: http://www.it.johnshopkins.edu/services/network/requests/dns.html

IP Configuration Info:
http://www.it.johnshopkins.edu/services/network/jhars/JHARS%20Step-By-Step.pdf

Contacts:
Email: hostmaster@jhmi.edu or hostmaster@jhu.edu

B. TCP & UDP Ports

Check the TCP and UDP ports to ensure no service or application is running that might compromise the client system. Consider these ports when configuring or updating firewall policy and security monitoring. Current active TCP and UDP ports can be viewed by starting a command prompt and running *netstat –a* command -- or from *TCPView*, a utility from Microsoft sysinternals. Active ports from PowerShell can be viewed by running the following command:

```
Get-NetTCPConnection | ? State -eq Established | FT -Autosize
```

TCPView download: https://technet.microsoft.com/en-us/library/bb897437.aspx

C. Network Security

Network security provides the community with information and tools to help provide additional security.

Links

More information: http://it.jhmi.edu/infosec
Johns Hopkins System Block List: http://it.jhmi.edu/restricted/infosec/blocklist.html
General questions**:** network.security@jhu.edu
Incidents: incident@jhu.edu

IX. Administrative & Performance Settings

A. Recovery Environment

Required:
Windows Recovery Environment (WinRE) is a recovery environment that can repair common causes of unbootable operating systems. WinRE is preloaded into Windows by default. There are different versions of WinRE for each Windows version. Accessing WinRE can also vary between different versions of Windows.

Recommended:
Microsoft Diagnostics and Recovery Toolset (DaRT) is a powerful set of tools that extend the Windows Recovery Environment (WinRE). It can be integrated into Windows as a replacement for the default WinRE or booted into from a CD or USB flash drive. DaRT should be customized with boot drivers for Dell hardware and

WinPE components for BitLocker encryption. Just like with WinRE, there are different versions of DaRT for each Windows version.

Links:
Windows 7 – How to Access Windows RE
http://social.technet.microsoft.com/wiki/contents/articles/11028.how-to-access-windows-recovery-environment-in-windows-7.aspx

Windows 7 – Windows RE Technical Reference https://technet.microsoft.com/en-us/library/dd744255.aspx

Windows 8/8.1 - Windows RE Overview https://technet.microsoft.com/en-us/library/hh825173.aspx

Windows 10 – Windows RE Technical Reference https://msdn.microsoft.com/en-us/windows/hardware/commercialize/manufacture/desktop/windows-recovery-environment--windows-re--technical-reference

DaRT - https://technet.microsoft.com/en-us/windows/hh826071.aspx

B. Windows Remote Desktop

Typically, IT Administrators and customers use Remote Desktop to provide access to their Windows Vista and above systems from anywhere on the Johns Hopkins network. This feature provides a number of benefits for customers and administrators alike.

Required:
If Remote Desktop for Administration is enabled, the Windows client system must be monitored and protected against "Man in the Middle" and User Dictionary Attacks.

Monitor for Remote Desktop Failures: In Windows 7 and above, there is a dedicated log file for Remote Desktop Session connections that is enabled by default called TerminalServicesLocalSessionManager. It is important to review and monitor this log file. In addition, in the Security Event Log Event ID there is Event ID 4624 with Logon Type 10 (when the recommended auditing is enabled). The TerminalServicesLocalSessionManager log file is located in the following location:

> *Event Viewer-Windows Logs-Applications and Services Logs-Microsoft-Windows-TerminalServicesLocalSessionManager in the Operational Log*

Network Level Authentication: This setting forces all Remote Desktop connections to use the Credential Security Support Provider (CredSSP) Protocol. This uses stronger authentication through TLS/SSL or Kerberos and protect against "Man in the Middle" attacks. This can be set within Group Policy located at:

> *Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host/Security\Require user authentication for remote connections by using Network Level Authentication Set to Enabled*

Recommended:
For most laptops, it is recommended to have Remote Desktop disabled if it is not required for the customer.

C. Telemetry

Windows Telemetry is a technology that Microsoft uses to analyze and fix software problems. Telemetry is enabled by default to send system data to Microsoft. Windows applications also use Telemetry through Customer Experience Improvement Programs (CEIP).

It is recommended to disable telemetry on Windows client systems and applications, unless the telemetry data is available for and accessed by Johns Hopkins IT staff for business purposes. If telemetry data is being accessed by JH IT staff, it is approved to be enabled.

To change Telemetry with Windows 10 Group Policy: *Computer Configuration-Policies-Administrative Templates>Windows Components>Data Collection and Preview Builds> Allow Telemetry*
Set Value to Basic

To disable Telemetry, the following services should be set to Disabled in Group Policy or set on the local machine (note these services may not exist on all Windows versions):

Diagnostics Tracking Service
Connected User Experiences and Telemetry

X. Systems Management and Monitoring

A. Tools

It is recommended that multiple tools or applications be used to monitor Windows client systems. These tools can be used to baseline system performance and health. In addition, host security monitoring is recommended for Windows client systems, and security logging should be part of a documented monitoring strategy. IT@JH Utilizes SCCM and SCOM for Systems Management and Monitoring.

B. Systems Management

Required:
It is critical to maintain an inventory for all online Johns Hopkins Windows client assets. This inventory should include some static information (e.g., location, customer information, etc.), along with dynamic information. For Windows clients, there are a number of key attributes that should be inventoried to collect information of WMI, Registry, or file attributes. This is valuable when trying to identify specific software versions, file versions or hardware vulnerabilities quickly and through dynamically generated reports.

It is required that all IT staff managing Windows clients utilize technology(s) which can deploy software, deploy security updates, and produce dynamic reports on the status of deployments/compliance/endpoint protection.

Recommended:
IT@JH provides access to an Enterprise instance of Microsoft's System Center Configuration Manager (SCCM) to all groups participating in the Enterprise Active Directory. All client systems do not need to participate in Enterprise Active Directory, but an OU must exist for delegation to the IT resources. SCCM provides static and dynamic inventory for Windows client systems, Software Deployments, Security Update Management, SCEP client management, dynamic reporting, and Operating System Deployment.

Items that should be dynamically inventoried include: Members of Local Administrators group, Security Update compliance, Windows Services, Installed Software, and file level inventory.

To participate in the Enterprise SCCM, contact: monitoring@jhmi.edu

SCCM SharePoint Site: https://collaborate.johnshopkins.edu/sites/EMMS/SCCM

C. Windows Operating System Deployment

Required:
Operating Systems must be deployed with up-to-date software, including security updates, endpoint protection, common applications, and drivers. Software must be kept up-to-date at least twice per year and IT groups must have documented procedures on updating and deploying the Windows OS.

Recommended:
Windows Operating Systems should be deployed using imaging technologies such as SCCM OSD or the Microsoft Deployment Toolkit (MDT). All Windows client imaging must use sysprep, which is required for a supported Windows Operating System.

Through a project called the Enterprise Client Image (ECI), IT groups can participate in a central Operating System build that can be customized by each group. The ECI is delivered to IT groups as templates that can be customized with the SCCM Admin Console. The ECI utilizes existing recommended solutions such as SCCM, MBAM, SCEP, and DaRT. The ECI templates are updated tri-annually and continually updated with the latest security and customer-centric customizations.

To participate in the Enterprise Client Image Committee, contact: monitoring@jhmi.edu

Links
Enterprise Client Image SharePoint:
https://collaborate.johnshopkins.edu/sites/EMMS/SCCM/ECI

Contact systems management resources: monitoring@jhmi.edu

D. Performance Monitor Tool

Recommended:
System administrators can use the Performance Monitor tool to send alerts over the network, record events to the event viewer application log, launch a program or batch file when high and low thresholds are reached. This utility can be useful to

administrators who need to be notified remotely when a resource has reached a threshold and action is required.

E. Task Manager

Recommended:
Task Manager is an integrated tool for monitoring applications and tasks. It reports key performance metrics of Windows-based systems and provides detailed information on each application and process running on the workstation in addition to memory and CPU usage. Task Manager also allows termination of applications and processes that are not responding.

F. Event Viewer

Required:
Event Viewer is the principal monitoring tool for discrete events in performance and security. Typically, a Windows client system stores application, security, and system logs. It could also contain other logs, depending on the computer's role and the applications installed. Microsoft continues to refine this tool, and it is especially useful for administrators troubleshooting a client system. The primary Event Logs, Application, Security, and System, should have their sizes set to a **minimum of 50MB** and set to 'Overwrite events as needed', to ensure that the logging does not fill up and need to be cleared. Systems with a high turnover of the Security Event log are highly encouraged to implement a larger Security Log size and the Security Event Log should be able to store a minimum of seven days' events.

G. Regular Reporting on Client Compliance

Required:
Windows client systems must be regularly monitored for security incidents or vulnerable systems. These include malware, viruses, vulnerable software versions, security events, etc. Monitoring software should provide event management, active monitoring and reporting. It is important for the security of a Windows client system to ensure it is monitored properly.

XI. Administration and Operations

A. Home Drives and Shared Drives

Recommended:
It is important that Johns Hopkins staff have alternatives to storing files locally on desktops or laptops. A department-provided Home or H:\ drive for individual use and/or a departmental share for collaboration is one approach that successfully minimizes data loss. It is critical that any file shares used by JH staff are in secure locations, have regular backups and restores are tested regularly.

Cloud Services provides home drives and departmental shares to departments and IT groups across Johns Hopkins institutions.

More details can be found on the IT website at http://www.it.johnshopkins.edu/services/sla/storage/.

Contact for storage resources: cloudrequests@jhmi.edu

B. Web/Cloud Personal and Shared Storage

Web-based storage, whether stored on-premises or in the Cloud, can add productivity for Johns Hopkins faculty and staff. Files on web-based storage can be accessed from any device and from inside and outside the network. Appropriate file sharing and management tools are discussed in greater detail in the Encryption Standards referenced below.

Required:
For Restricted Information, JHBox is the only authorized Cloud Storage solution. Sync tools, such as Box Sync, must not be used except on devices encrypted with Enterprise Full Disk Encryption (MBAM).

SharePoint
http://www.it.johnshopkins.edu/services/collaboration_tools/sharepoint/

JHBox
http://www.it.johnshopkins.edu/services/collaboration_tools/jhbox/

OneDrive – Not approved for Restricted Information
http://www.it.johnshopkins.edu/services/collaboration_tools/OneDrive/

Encryption Standards
http://www.it.johnshopkins.edu/policies/standards.html

C. SSL/TLS PKI

Recommended:
For the Johns Hopkins wireless SSID, JHACCESS, and for some applications, certificates are deployed to Windows client systems.

Certificates offered through the Johns Hopkins Enterprise PKI provides the ease of installing and renewing SSL/TLS certificates for systems participating in the Enterprise Active Directory. Certificates used for smartcards and other forms of certificate-based authentication and the need for other intended purposes for digital certificates are recommended for this certificate service. Digital certificate standards are discussed in the Encryption Standards.

Johns Hopkins SSL/TLS Certificate Services information:
http://www.it.johnshopkins.edu/services/directoryservices/sslcertificates

Encryption Standards
http://www.it.johnshopkins.edu/policies/standards.html

Contact PKI resources: PKIAdmins@jhmi.edu

XII. References

A. Books/Training

- *Windows 7: The Missing Manual* http://shop.oreilly.com/product/9780596806408.do
- *Windows 10 Guide for IT Pros*

https://technet.microsoft.com/en-us/windows/windows10.aspx

- *Microsoft Virtual Academy – Free Online Training from Microsoft* http://www.microsoftvirtualacademy.com/
- *eBooks – Microsoft Virtual Academy – Free Electronic Books from Microsoft* http://www.microsoftvirtualacademy.com/ebooks

B. Web Sites

- Deploy Windows 10
- https://technet.microsoft.com/en-us/library/mt158221(v=vs.85).aspx Windows 10 Enterprise Security Guide https://technet.microsoft.com/en-us/library/mt463092(v=vs.85).aspx
- Microsoft Services and Ports http://support.microsoft.com/kb/832017
- SANS "Pass the Hash Attacks: Tools and Mitigations" http://www.sans.org/reading_room/whitepapers/testing/pass-the-hash-attacks-tools-mitigation_33283

XIII. Appendix

A. Securing Service Accounts

Windows services typically run under the Local System account, but they can also run under a domain user or local account. A service runs under the security context of its service account, so if an attacker compromises a service on a member system, the service account can potentially be used to attack a domain controller. When determining which domain account to use as a service account, ensure that the assigned privileges are limited to what is required for the successful operation of the service and use the settings described below.

- The logon name could be an acronym but it is recommended to avoid making the logon name obvious or easy to guess in relationship to the service.
- For domain service accounts, the option "User cannot change password" should be set since this is a service account and there should be no need for the password to be updated interactively by a user logged in as the service account. Such a password change on the service account may affect service operations. Having this setting enabled also reduces the possibility of this account being used by an attacker.
- Consider limiting what workstations the user account can log on to though the user properties. This prevents compromised accounts from accessing other systems in the domain.
- Consider removing the Domain Users group from the Service Account.

B. Logon Banner

Recommended:
A Logon Banner is recommended to be used on all Windows client systems. A typical exception to having a logon banner is a Windows client serving as a "Public" workstation where a generic account is set to automatically logon.

BANNER Title: *Johns Hopkins IT Use Statement*

BANNER Message: *Use of this system is restricted to authorized personnel for clinical or other business purposes of Johns Hopkins in accordance with applicable law and Hopkins policies. Users are expected to exercise due care in protecting confidential information. Use of and activity on this system is monitored and logged. Use of this system constitutes consent to such monitoring.*

This can be set within Group Policy located at:

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive Logon\Interactive logon: Message title for users attempting to log on
&
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive Logon\ Interactive logon: Message text for users attempting to log on

C. Alertus Desktop Alerts

Required for JHM Clinical Applications Customers:
The Alertus Desktop Alert Management System is an application used to notify clinical staff when there are service disruptions with critical clinical applications. IT staff who support Johns Hopkins Medicine clinical application customers are required to have the Alertus application installed on the Windows client systems they support. The Alertus package is available in the Enterprise SCCM environment for deployment. The Alertus software is also available on the Software Catalog.

Software Catalog: https://itservices.johnshopkins.edu

D. Sample Group Policy Template

For Windows client systems that reside in the Enterprise Active Directory, a sample Group Policy Object (GPO) has been created that has applicable required and recommended settings defined for the Windows Client Standard. This GPO may be copied and linked to Organizational Units (OU) where JH IT group's client systems reside, typically the Computers OU. This GPO contains all of the recommended Group Policy Settings except for the elimination of Cached Credentials.

This GPO is called **Sample GPO for Windows Client Standard 2017**.
In addition to the Required and Recommended settings, the following settings would need to be changed by each IT group to make all the settings effective:

Accounts: Rename administrator account – Set to your group's unique value
LAPS – Define your group's unique Administrator account
Accounts: Rename guest account - Set to your group's unique value
Computer Services – Only Computer Browser is disabled in this GPO
Add and remove domain accounts – Listed in Computer Configuration-Policies-Windows Settings-Scripts-Startup called SampleAddingtoLocalGroups.cmd – you will find a sample command script for adding or removing domain accounts at Startup

These settings are Recommended but not defined in the Sample GPO for Windows Client Standard 2017.

Remove Admins from Debug Privilege – This setting is best defined locally on the PC or through a defined Win Domain Global group, rather than through a GPO, as there are some programs that require this right.
IE Settings listed in the Windows Client Standard are not defined in the GPO.
Wdigest – Requires an installation and registry value, best deployed as a package.
SMB – Not defined in the GPO. Best deployed as a package.

IMPORTANT NOTE – Do not link directly to this GPO, always make a copy before using.