Recommended Security Baseline Settings

for Windows 8.1, Windows Server 2012 R2, and Internet Explorer 11

# Background and Summary

This document outlines recommended security configuration settings for Windows 8.1, Windows Server 2012 R2 and Internet Explorer 11, using the previously-published baselines for Windows 8, Windows Server 2012 and Internet Explorer 10 as the starting point. These guidelines are intended for well-managed enterprises.

Some of the more interesting changes from the Windows 8/2012/IE10 baselines:

* Use of new and existing settings to help block some Pass the Hash attack vectors
* Blocking the use of web browsers on domain controllers
* Incorporation of the Enhanced Mitigation Experience Toolkit (EMET) into the standard baselines
* Removal of almost all service startup settings, and all server role baselines that contain only service startup settings
* Removal of the recommendation to enable “FIPS mode”

Contents

[Background and Summary 1](#_Toc397455309)

[Settings New to Windows 8.1 and Windows Server 2012 R2 2](#_Toc397455310)

[Settings New to Internet Explorer 11 6](#_Toc397455311)

[Changes to Settings Inherited from Existing Baselines 8](#_Toc397455312)

[Changes to all Windows Server product baselines 8](#_Toc397455313)

[Pass the Hash 9](#_Toc397455314)

[Blocking the use of Web Browsers on Domain Controllers 11](#_Toc397455315)

[EMET 13](#_Toc397455316)

[Updated Guidance 14](#_Toc397455317)

[Advanced Auditing 16](#_Toc397455318)

[Removed Windows Recommendations 23](#_Toc397455319)

[Removed Internet Explorer Recommendations 26](#_Toc397455320)

[Bugs 27](#_Toc397455321)

# Settings New to Windows 8.1 and Windows Server 2012 R2

The following settings are new to Windows 8.1 and Windows Server 2012 R2, and have been identified for inclusion in both the Windows 8.1 and Server 2012 R2 security baselines.

For Windows Server 2012 R2, we recommend the creation of baselines only for “Domain Controller Security Compliance”, “Domain Security Compliance” and “Member Server Security Compliance”. We discuss this further in the “Changes to Both New and Existing Baselines” section under “Changes to all Windows Server product baselines”.

| ***Policy Path*** | ***Policy Name*** | ***Old Value*** | ***New Value*** | ***Rationale*** |
| --- | --- | --- | --- | --- |
| Computer Configuration\Administrative Templates\Control Panel\Personalization | Prevent enabling lock screen camera | N/A | Enabled | Unauthenticated user can create content in user’s Pictures folder (Tampering, Repudiation, Denial of Service) |
| Computer Configuration\Administrative Templates\Control Panel\Personalization | Prevent enabling lock screen slide show | N/A | Enabled | Potentially sensitive information from logged on user’s Pictures folder displayed on locked desktop (information disclosure) |
| Computer Configuration\Administrative Templates\System\Audit Process Creation | Include command line in process creation events | N/A | Not Configured | Enable only when needed; otherwise it provides an attacker with admin rights a lot of data, potentially including passwords (e.g., from a NET USE command line). |
| Computer Configuration\Administrative Templates\System\Logon | Do not display network selection UI | N/A | Enabled | Unauthenticated user should not be able to switch networks. (Tampering) |
| Computer Configuration\Administrative Templates\Windows Components\App runtime | Allow Microsoft accounts to be optional | N/A | Enabled | Enterprises have to be able to enable app use without tying to an MSA or automatically uploading data to SkyDrive. |
| Computer Configuration\Administrative Templates\Windows Components\Windows Logon Options | Sign-in last interactive user automatically after a system-initiated restart | N/A | Disabled | Requires Windows to retain plaintext-equivalent credentials during session |
| Computer Configuration\Windows Settings\Local Policies\User Rights Assignment | Deny access to this computer from the network | Guests | Guests, Local account  (for Member Server: Guests, Local account and member of Administrators group) | Win8.1/2012R2 introduces two new pseudo groups that a local-account logon can get in its token and that has been backported to Windows 7/2008R2 and newer with [KB 2871997](http://support.microsoft.com/kb/2871997). Guests and local accounts should be denied network logon on domain-joined systems. (For Member Server, replace “Local account” with “Local account and member of Administrators group” to avoid breaking failover clustering.) Also, Enterprise Admins and Domain Admins should also be denied all access on all clients and servers except for Domain Controllers and dedicated admin workstations. (Note that EA and DA are domain-specific and cannot be specified in generic baselines such as those in SCM.) |
| Computer Configuration\Windows Settings\Local Policies\User Rights Assignment | Deny log on through Remote Desktop Services | Guests | Guests, Local account | Win8.1/2012R2 introduces a new pseudo group called “Local account” that any local-account logon gets in its token and that has been backported to Windows 7/2008R2 and newer with [KB 2871997](http://support.microsoft.com/kb/2871997). Guests and Local Account should be denied remote desktop logon on domain-joined systems. Also, Enterprise Admins and Domain Admins should also be denied all access on all clients and servers except for Domain Controllers and dedicated admin workstations. (Note that EA and DA are domain-specific and cannot be specified in generic baselines such as those in SCM.) |
| Computer Configuration\Administrative Templates\SCM: Pass the Hash Mitigations | Lsass.exe audit mode (HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\LSASS.exe!AuditLevel | N/A | Not configured | For more information, see <http://technet.microsoft.com/en-us/library/dn408187.aspx>  A custom Administrative Template is provided so that this setting can be configured with the Group Policy editor. |
| Computer Configuration\Administrative Templates\SCM: Pass the Hash Mitigations | Enable LSA Protection (HKLM\SYSTEM\CurrentControlSet\Control\Lsa\RunAsPPL) | N/A | Not configured | For more information, see <http://technet.microsoft.com/en-us/library/dn408187.aspx>  A custom Administrative Template is provided so that this setting can be configured with the Group Policy editor. Note that on UEFI-capable machines, once the setting is enabled it cannot be disabled using Group Policy alone. |
| User Configuration\Administrative Templates\Start Menu and Taskbar\Notifications | Turn off toast notifications on the lock screen | N/A | Enabled | Information disclosure |

# Settings New to Internet Explorer 11

The following new settings have been identified for inclusion in the Internet Explorer 11 security baseline.

| ***Policy Path*** | ***Policy Name*** | ***Old Value*** | ***New Value*** | ***Rationale*** |
| --- | --- | --- | --- | --- |
| Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Advanced Page | Turn on 64-bit tab processes when running in Enhanced Protected Mode on 64-bit versions of Windows | N/A | Enabled | Increased protection; will break some sites, but applies only when EPM is enforced |
| Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Internet Zone | Don't run antimalware programs against ActiveX controls | N/A | Enabled: Disable | Enforce the default |
| Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Intranet Zone | Don't run antimalware programs against ActiveX controls | N/A | Enabled: Disable | (stronger than default; align with DoD STIG) |
| Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Local Machine Zone | Don't run antimalware programs against ActiveX controls | N/A | Enabled: Disable | (stronger than default; align with DoD STIG) |
| Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Restricted Sites Zone | Don't run antimalware programs against ActiveX controls | N/A | Enabled: Disable | Enforce the default |
| Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Trusted Sites Zone | Don't run antimalware programs against ActiveX controls | N/A | Enabled: Disable | (stronger than default; align with DoD STIG) |

# Changes to Settings Inherited from Existing Baselines

This section describes changes to settings that were inherited from older baselines. These changes will also be backported to those baselines: Windows 7, Windows 8, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012. The Baseline column describes which baselines are affected.

## Changes to all Windows Server product baselines

One change that we recommend for all Windows Server baselines is to create and maintain baselines only for “Domain Controller Security Compliance”, “Domain Security Compliance” and “Member Server Security Compliance”. We recommend not creating (and deleting where they now exist) server role baselines for AD Certificate Services, DHCP, DNS, File Server, Hyper-V, Network Policy and Access, Print Server, Remote Access Services, Remote Desktop Services or Web Server.

The reason for this change is because those baselines contain only configuration for service startup and simply try to enforce the defaults for their respective roles. The problems with these baselines are that 1) they are time-consuming to define and maintain, as service startup defaults may change between OS versions; 2) as one can safely assume that the built-in Server Manager or other configuration tools do their job correctly, the baselines provide almost no security benefit; and 3) they can create serious problems when they get it wrong. For example, in some scenarios, Windows temporarily configures the Windows Installer service (which is normally a Manual start service) to be an Automatic start service so that it can perform actions immediately following a reboot. The security baseline that forces it back to Manual-start thus causes updates not to be correctly installed.

For those reasons, we have also decided to remove all the service startup settings from the Server baselines that include them (e.g., Windows Server 2012 Domain Controller Security Compliance”). The one exception is the service startup configuration setting for the Application Identity service in Domain Controllers, which is required to support the use of AppLocker (described in the section below, “Blocking the use of Web Browsers on Domain Controllers”).

## Pass the Hash

The following settings changes are recommended to help mitigate against Pass the Hash and similar credential theft attacks.

| ***Baseline*** | ***Policy Path*** | ***Policy Name*** | ***Old Value*** | ***New Value*** | ***Rationale*** |
| --- | --- | --- | --- | --- | --- |
| All Client OS and Member Servers | Computer Configuration\Administrative Templates\SCM: Pass the Hash Mitigations | Apply UAC restrictions to local accounts on network logons  (HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System !LocalAccountTokenFilterPolicy) | N/A | Enable (REG\_DWORD 0) | Recommended in "Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft Techniques": <http://www.microsoft.com/en-us/download/details.aspx?id=36036>  A custom Administrative Template is provided so that this setting can be configured with the Group Policy editor. |
| All OS | Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment | Deny access to this computer from the network | Guests | Guests, Local account  (for Member Server: Guests, Local account and member of Administrators group) | Win8.1/2012R2 introduces two new pseudo groups that a local-account logon can get in its token and that has been backported to Windows 7/2008R2 and newer with [KB 2871997](http://support.microsoft.com/kb/2871997). Guests and local accounts should be denied network logon on domain-joined systems. (For Member Server, replace “Local account” with “Local account and member of Administrators group” to avoid breaking failover clustering.) Also, Enterprise Admins and Domain Admins should also be denied all access on all clients and servers except for Domain Controllers and dedicated admin workstations. (Note that EA and DA are domain-specific and cannot be specified in generic baselines such as those in SCM.) |
| All  OS | Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment | Deny log on through Remote Desktop Services | Guests | Guests, Local account | Win8.1/2012R2 introduces a new pseudo group called “Local account” that any local-account logon gets in its token and that has been backported to Windows 7/2008R2 and newer with [KB 2871997](http://support.microsoft.com/kb/2871997). Guests and Local Account should be denied remote desktop logon on domain-joined systems. Also, Enterprise Admins and Domain Admins should also be denied all access on all clients and servers except for Domain Controllers and dedicated admin workstations. (Note that EA and DA are domain-specific and cannot be specified in generic baselines such as those in SCM.) |
| All OS | Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment | Deny log on as a batch job | Guests | Guests | Also, Enterprise Admins and Domain Admins should also be denied all access on all clients and servers except for Domain Controllers and dedicated admin workstations. (Note that EA and DA are domain-specific and cannot be specified in generic baselines such as those in SCM.) |
| All OS | Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment | Deny log on as a service | Guests | Guests | Also, Enterprise Admins and Domain Admins should also be denied all access on all clients and servers except for Domain Controllers and dedicated admin workstations. (Note that EA and DA are domain-specific and cannot be specified in generic baselines such as those in SCM.) |
| All OS | Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment | Deny log on locally | Guests | Guests | Also, Enterprise Admins and Domain Admins should also be denied all access on all clients and servers except for Domain Controllers and dedicated admin workstations. (Note that EA and DA are domain-specific and cannot be specified in generic baselines such as those in SCM.) |
| All OS | Computer Configuration\Administrative Templates\SCM: Pass the Hash Mitigations | WDigest Authentication (disabling may require KB2871997) | N/A | Disabled | WDigest leaves users’ plaintext-equivalent passwords in Lsass.exe memory. Recommended in “Mitigating Pass-the-Hash and Other Credential Theft, version 2”, <http://www.microsoft.com/pth> |

## Blocking the use of Web Browsers on Domain Controllers

It is well-established within the security community that it is highly dangerous and unnecessary to browse the web from a high-value system such as a Domain Controller. The purpose of the new baseline recommendations in this section is to help prevent such behavior by using AppLocker to block the use of popular web browsers. Note that because it is impossible to prevent an administrator from bypassing these or any other rules, the real purpose of these rules is to prevent accidental use and to make it clear that web browser use on a DC is inadvisable.

While these rules will cover many cases, they should not be considered to be comprehensive. Not only are there other browsers that are not covered by this rule set, there are many other behaviors that are similarly dangerous when performed on a domain controller and that are not explicitly blocked. For such cases, these rules can be considered illustrative of an approach that can be extended to be more comprehensive.

These rules can also be applied to other high value systems, such as database servers and dedicated, single-purpose administrative workstations that are used solely to administer Active Directory.

| ***Baseline*** | ***Policy Path*** | ***Policy Name*** | ***New Value*** | ***Rationale*** |
| --- | --- | --- | --- | --- |
| All Windows Server “Domain Controller” baselines | Computer Configuration\Windows Settings\Security Settings\Application Control Policies\AppLocker | Enable enforcement of Executable Rules | Enable | Block web browsers on DCs |
| All Windows Server “Domain Controller” baselines | Computer Configuration\Windows Settings\Security Settings\Application Control Policies\AppLocker\Executable Rules | Block IE | FilePublisherRule: Deny Everyone  PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US"  ProductName="WINDOWS® INTERNET EXPLORER"  BinaryName="IEXPLORE.EXE" | Block web browsers on DCs |
| All Windows Server “Domain Controller” baselines | Computer Configuration\Windows Settings\Security Settings\Application Control Policies\AppLocker\Executable Rules | Block Chrome.exe | FilePublisherRule: Deny Everyone  PublisherName="O=GOOGLE INC, L=MOUNTAIN VIEW, S=CALIFORNIA, C=US"  ProductName="GOOGLE CHROME"  BinaryName="CHROME.EXE" | Block web browsers on DCs |
| All Windows Server “Domain Controller” baselines | Computer Configuration\Windows Settings\Security Settings\Application Control Policies\AppLocker\Executable Rules | Block Firefox | FilePublisherRule: Deny Everyone  PublisherName="O=MOZILLA CORPORATION, L=MOUNTAIN VIEW, S=CA, C=US"  ProductName="FIREFOX"  BinaryName="FIREFOX.EXE" | Block web browsers on DCs |
| All Windows Server “Domain Controller” baselines | Computer Configuration\Windows Settings\Security Settings\Application Control Policies\AppLocker\Executable Rules | Default rules | Allow non-admins to run executables in Program Files  Allow non-admins to run executables in Windir  Allow admins to run executables anywhere | Block web browsers on DCs |
| All Windows Server “Domain Controller” baselines | Computer Configuration\Windows Settings\Security Settings\System Services | Application Identity (AppIDSvc) | Service startup mode = Automatic | AppLocker requires AppIDSvc to be running to enforce rules |

## EMET

We recommend installing EMET on all workstations and servers, along with these Group Policy settings:

| ***Baseline*** | ***Policy Path*** | ***Policy Name*** | ***Old Value*** | ***New Value*** | ***Rationale*** |
| --- | --- | --- | --- | --- | --- |
| All  OS | Computer Configuration\Administrative Templates\Windows Components\EMET | Default Protections for Internet Explorer | N/A | Enabled | EMET protections |
| All  OS | Computer Configuration\Administrative Templates\Windows Components\EMET | Default Protections for Popular Software | N/A | Enabled | EMET protections |
| All  OS | Computer Configuration\Administrative Templates\Windows Components\EMET | Default Protections for Recommended Software | N/A | Enabled | EMET protections |
| All  OS | Computer Configuration\Administrative Templates\Windows Components\EMET | System ASLR | N/A | Enabled: Application Opt-In | EMET protections |
| All  OS | Computer Configuration\Administrative Templates\Windows Components\EMET | System DEP | N/A | Enabled: Application Opt-Out | EMET protections |
| All  OS | Computer Configuration\Administrative Templates\Windows Components\EMET | System SEHOP | N/A | Enabled: Application Opt-Out | EMET protections |

## Updated Guidance

This section defines settings in all baselines covered by this report that should be added or changed to be consistent with other baselines.

| ***Baseline*** | ***Policy Path*** | ***Policy Name*** | ***Old Value*** | ***New Value*** | ***Rationale*** |
| --- | --- | --- | --- | --- | --- |
| All Client OS | Computer Configuration\Windows Components\Event Log Service\Application | Specify the maximum log file size (KB) | 20480 | 32768 | Make consistent with Server OS recommendations and increase diagnostic and forensic abilities. |
| All Client OS | Computer Configuration\Windows Components\Event Log Service\Security | Specify the maximum log file size (KB) | 20480 | 196608 | Make consistent with Server OS recommendations and increase diagnostic and forensic abilities. |
| All Client OS | Computer Configuration\Windows Components\Event Log Service\System | Specify the maximum log file size (KB) | 20480 | 32768 | Make consistent with Server OS recommendations and increase diagnostic and forensic abilities. |
| All  OS | Computer Configuration\Administrative Templates\Windows Components\Search | Allow indexing of encrypted files | Not Configured | Disabled | Information disclosure; encrypted content potentially goes into unencrypted index |
| All  OS | Computer Configuration\ Windows Settings\Security Settings\Account Policies\Account Lockout Policy | Account lockout threshold | 50 invalid logon attempts | 10 invalid logon attempts | 50 gives attackers too many shots; the 50 most-used passwords will give attackers too many accounts. Too low a threshold causes accidental lockout from application-cached passwords. (Separate blog post describes issues in more detail.) |
| All  OS | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options | MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 Recommended) | 0 Seconds | 5 seconds | No real security benefit setting it to 0; align with DoD STIG. |
| All  OS | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options | Network security: Force logoff when logon hours expire | Not Configured | Enabled | Make logoff hours work over the network too. |
| All  OS | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options | User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode | Prompt for consent for non-Windows binaries | Prompt for consent on the secure desktop | Make consistent (note that the actual value for Server 2008 has to be “Prompt for consent”, as “secure desktop” is specified in another option on Server 2008). |
| All  OS | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options | User Account Control: Behavior of the elevation prompt for standard users | Prompt for credentials | Automatically deny elevation requests | UAC same-desktop elevation is not a security boundary; there are more secure ways to administer a system. |
| All Member Servers | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options | Network security: Allow Local System to use computer identity for NTLM | Not Defined | Enabled | Added to Member Server baseline to be consistent with client and domain controller baselines |
| All Member Servers | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options | Network security: Allow LocalSystem NULL session fallback | Not Defined | Disabled | Added to Member Server baseline to be consistent with client and domain controller baselines |
| All Client OS | Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment | Access this computer from the network | Users, Administrators | Authenticated Users, Administrators | Make consistent with Server guidance |

## Advanced Auditing

The guidance for Windows 8 and Windows Server 2012 recommends “No Auditing” for many settings where the intent was to specify “Not Defined” and to allow customer decisions. In some cases, “No Auditing” overrode a more secure default. We have tried to fix all those cases here.

| ***Baseline*** | ***Policy Path*** | ***Policy Name*** | ***Old Value*** | ***New Value*** | ***Rationale*** |
| --- | --- | --- | --- | --- | --- |
| All  OS | Computer Configuration\Windows Settings\Advanced Audit Policy Configuration\Audit Policies\Account Logon | Audit Kerberos Authentication Service | No Auditing | Not Defined | No security value; better to allow customers to decide |
| All  OS | Computer Configuration\Windows Settings\Advanced Audit Policy Configuration\Audit Policies\Account Logon | Audit Kerberos Service Ticket Operations | No Auditing | Not Defined | No security value; better to allow customers to decide |
| All  OS | Computer Configuration\Windows Settings\Advanced Audit Policy Configuration\Audit Policies\Account Logon | Audit Other Account Logon Events | No Auditing | Not Defined | No security value; better to allow customers to decide |
| All  OS | Computer Configuration\Windows Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management | Audit Application Group Management | No Auditing | Not Defined | No security value; better to allow customers to decide |
| All Client  OS | Computer Configuration\Windows Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management | Audit Computer Account Management | No Auditing | Not Defined | No security value; better to allow customers to decide |
| All  OS | Computer Configuration\Windows Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management | Audit Distributed Group Management | No Auditing | Not Defined | No security value; better to allow customers to decide |
| All  OS | Computer Configuration\Windows Settings\Advanced Audit Policy Configuration\Audit Policies\Detailed Tracking | Audit DPAPI Activity | No Auditing | Not Defined | No security value; better to allow customers to decide |
| All  OS | Computer Configuration\Windows Settings\Advanced Audit Policy\Configuration\Audit Policies\Detailed Tracking | Audit Process Termination | No Auditing | Not Defined | No security value; better to allow customers to decide |
| All  OS | Computer Configuration\Windows Settings\Advanced Audit Policy Configuration\Audit Policies\Detailed Tracking | Audit RPC Events | No Auditing | Not Defined | No security value; better to allow customers to decide |
| All  OS | Computer Configuration\Windows Settings\Advanced Audit Policy Configuration\Audit Policies\DS Access | Audit Detailed Directory Service Replication | No Auditing | Not Defined | No security value; better to allow customers to decide |
| All Client  OS | Computer Configuration\Windows Settings\Advanced Audit Policy Configuration\Audit Policies\DS Access | Audit directory service access | No Auditing | Not Defined | No security value; better to allow customers to decide |
| All Client  OS | Computer Configuration\Windows Settings\Advanced Audit Policy Configuration\Audit Policies\DS Access | Audit Directory Service Changes | No Auditing | Not Defined | No security value; better to allow customers to decide |
| All  OS | Computer Configuration\Windows Settings\Advanced Audit Policy Configuration\Audit Policies\DS Access | Audit Directory Service Replication | No Auditing | Not Defined | No security value; better to allow customers to decide |
| All  OS | Computer Configuration\Windows Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff | Audit Account Lockout | No Auditing | Success | “No Auditing” was probably a mistaken entry here. |
| All  OS | Computer Configuration\Windows Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff | Audit IPSec Extended Mode | No Auditing | Not Defined | No security value; better to allow customers to decide |
| All  OS | Computer Configuration\Windows Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff | Audit IPSec Main Mode | No Auditing | Not Defined | No security value; better to allow customers to decide |
| All  OS | Computer Configuration\Windows Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff | Audit IPSec Quick Mode | No Auditing | Not Defined | No security value; better to allow customers to decide |
| All  OS | Computer Configuration\Windows Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff | Audit Network Policy Server | No Auditing | Not Defined | No security value; better to allow customers to decide |
| All  OS | Computer Configuration\Windows Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff | Audit Other Logon/Logoff Events | No Auditing | Not Defined | No security value; better to allow customers to decide |
| All  OS | Computer Configuration\Windows Settings\Advanced Audit Policy Configuration\Audit Policies\Object Access | Audit Application Generated | No Auditing | Not Defined | No security value; better to allow customers to decide |
| All  OS | Computer Configuration\Windows Settings\Advanced Audit Policy Configuration\Audit Policies\Object Access | Audit Central Access Policy Staging | No Auditing | Not Defined | No security value; better to allow customers to decide |
| All  OS | Computer Configuration\Windows Settings\Advanced Audit Policy Configuration\Audit Policies\Object Access | Audit Certification Services | No Auditing | Not Defined | No security value; better to allow customers to decide |
| All  OS | Computer Configuration\Windows Settings\Advanced Audit Policy Configuration\Audit Policies\Object Access | Audit Detailed File Share | No Auditing | Not Defined | No security value; better to allow customers to decide |
| All  OS | Computer Configuration\Windows Settings\Advanced Audit Policy Configuration\Audit Policies\Object Access | Audit File Share | No Auditing | Not Defined | No security value; better to allow customers to decide |
| All  OS | Computer Configuration\Windows Settings\Advanced Audit Policy Configuration\Audit Policies\Object Access | Audit File System | No Auditing | Not Defined | No security value; better to allow customers to decide |
| All  OS | Computer Configuration\Windows Settings\Advanced Audit Policy Configuration\Audit Policies\Object Access | Audit Filtering Platform Connection | No Auditing | Not Defined | No security value; better to allow customers to decide |
| All  OS | Computer Configuration\Windows Settings\Advanced Audit Policy Configuration\Audit Policies\Object Access | Audit Filtering Platform Packet Drop | No Auditing | Not Defined | No security value; better to allow customers to decide |
| All  OS | Computer Configuration\Windows Settings\Advanced Audit Policy Configuration\Audit Policies\Object Access | Audit Handle Manipulation | No Auditing | Not Defined | No security value; better to allow customers to decide |
| All  OS | Computer Configuration\Windows Settings\Advanced Audit Policy Configuration\Audit Policies\Object Access | Audit Kernel Object | No Auditing | Not Defined | No security value; better to allow customers to decide |
| All  OS | Computer Configuration\Windows Settings\Advanced Audit Policy Configuration\Audit Policies\Object Access | Audit Other Object Access Events | No Auditing | Not Defined | No security value; better to allow customers to decide |
| All  OS | Computer Configuration\Windows Settings\Advanced Audit Policy Configuration\Audit Policies\Object Access | Audit Registry | No Auditing | Not Defined | No security value; better to allow customers to decide |
| All  OS | Computer Configuration\Windows Settings\Advanced Audit Policy Configuration\Audit Policies\Object Access | Audit Removable Storage | No Auditing | Not Defined | No security value; better to allow customers to decide |
| All  OS | Computer Configuration\Windows Settings\Advanced Audit Policy Configuration\Audit Policies\Object Access | Audit SAM | No Auditing | Not Defined | No security value; better to allow customers to decide |
| All  OS | Computer Configuration\Windows Settings\Advanced Audit Policy Configuration\Audit Policies\Policy Change | Audit Authorization Policy Change | No Auditing | Not Defined | No security value; better to allow customers to decide |
| All  OS | Computer Configuration\Windows Settings\Advanced Audit Policy Configuration\Audit Policies\Policy Change | Audit Filtering Platform Policy Change | No Auditing | Not Defined | No security value; better to allow customers to decide |
| All  OS | Computer Configuration\Windows Settings\Advanced Audit Policy Configuration\Audit Policies\Policy Change | Audit MPSSVC Rule-Level Policy Change | No Auditing | Not Defined | No security value; better to allow customers to decide |
| All  OS | Computer Configuration\Windows Settings\Advanced Audit Policy Configuration\Audit Policies\Policy Change | Audit Other Policy Change Events | No Auditing | Not Defined | No security value; better to allow customers to decide |
| All  OS | Computer Configuration\Windows Settings\Advanced Audit Policy Configuration\Audit Policies\Privilege Use | Audit Non Sensitive Privilege Use | No Auditing | Not Defined | No security value; better to allow customers to decide |
| All  OS | Computer Configuration\Windows Settings\Advanced Audit Policy Configuration\Audit Policies\Privilege Use | Audit Other Privilege Use Events | No Auditing | Not Defined | No security value; better to allow customers to decide |
| All  OS | Computer Configuration\Windows Settings\Advanced Audit Policy Configuration\Audit Policies\System | Audit Other System Events | No Auditing | Success and Failure | “No Auditing” was probably a mistaken entry here. |

## Removed Windows Recommendations

This section lists settings that we believe should be removed from the Windows recommendations. In many cases, they provide little or no security value. In other cases, the settings are no longer applicable.

| ***Baseline*** | ***Policy Path*** | ***Policy Name*** | ***Old Value*** | ***New Value*** | ***Rationale*** |
| --- | --- | --- | --- | --- | --- |
| All  OS | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options | System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing | Enabled | Not Defined | Limited security value; breaks many legitimate use cases; SSL 3.0 and earlier can be disabled through other means. Discussed in more detail here: http://blogs.technet.com/b/secguide/archive/2014/04/07/why-we-re-not-recommending-fips-mode-anymore.aspx |
| All  OS | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options | Interactive logon: Require Domain Controller authentication to unlock workstation | Enabled | Not Defined | No security value |
| All  OS | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options | User Account Control: Only elevate executables that are signed and validated | Disabled | Not Defined | No security value |
| All OS | Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment | Bypass traverse checking | Administrators, Users, Local Service, Network Service | Not Defined | No security value |
| All OS | Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment | Increase a process working set | Administrators, Local Service | Not Defined | No security value |
| All OS | Computer Configuration\Administrative Templates\System\Device Installation | Specify the search server for device driver updates | Enabled: Search Managed Server | Not configured | Setting is customer-specific |
| All  OS | Computer Configuration\Administrative Templates\System\Internet Communication Management\Internet Communication settings | Turn off Search Companion content file updates | Enabled | Not Defined | No longer applicable |
| All  OS | Computer Configuration\Administrative Templates\System\Internet Communication Management\Internet Communication settings | Turn off the "Publish to Web" task for files and folders | Enabled | Not Defined | No longer applicable |
| All  OS | Computer Configuration\Administrative Templates\System\Internet Communication Management\Internet Communication settings | Turn off the Windows Messenger Customer Experience Improvement Program | Enabled | Not Defined | No longer applicable |
| All  OS | Computer Configuration\Administrative Templates\System\Internet Communication Management\Internet Communication settings | Turn off Windows Update device driver searching | Enabled | Not Defined | No security value |
| All  OS | Computer Configuration\Administrative Templates\Windows Components\Event Log Service\Application | Control Event Log behavior when the log file reaches its maximum size | Disabled | Not Defined | No security value |
| All  OS | Computer Configuration\Administrative Templates\Windows Components\Event Log Service\Security | Control Event Log behavior when the log file reaches its maximum size | Disabled | Not Defined | No security value |
| All  OS | Computer Configuration\Administrative Templates\Windows Components\Event Log Service\System | Control Event Log behavior when the log file reaches its maximum size | Disabled | Not Defined | No security value |
| All  OS | Computer Configuration\Administrative Templates\Windows Components\Windows Remote Shell | Allow Remote Shell Access | Enabled | Not Defined | No security value (opposite!) |
| All DC | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options | Interactive logon: Number of previous logons to cache (in case domain controller is not available) | 4 logons | Not Defined | Not applicable since the role is a Domain Controller. |
| All DC | Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment | Log on as a batch job | Administrators | Not Defined | Previous guidance prevents some least-privilege scenarios. |

## Removed Internet Explorer Recommendations

This section lists settings that we believe should be removed from the Internet Explorer recommendations. In many cases, they provide little or no security value. In other cases, the settings are no longer applicable.

| ***Baseline*** | ***Policy Path*** | ***Policy Name*** | ***Old Value*** | ***New Value*** | ***Rationale*** |
| --- | --- | --- | --- | --- | --- |
| All  IE | User Configuration\Administrative Templates\Windows Components\Internet Explorer\Browser menus | Disable Save this program to disk option | Enabled | Not Configured | No security value |
| All  IE | Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel | Disable the Advanced page | Enabled | Not Configured | No security value |
| All  IE | Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel | Disable the Security page | Enabled | Not Configured | No security value |
| All  IE | Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Internet Zone | Software channel permissions | High Safety | Not Configured | No longer applicable |
| All  IE | Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Restricted Sites Zone | Software channel permissions | High Safety | Not Configured | No longer applicable |

# Bugs

This section lists defects in the existing guidance that need to be repaired.

| ***Baseline*** | ***Policy Path*** | ***Policy Name*** | ***Old Value*** | ***New Value*** | ***Rationale*** |
| --- | --- | --- | --- | --- | --- |
| Domain Controller | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options | Microsoft network server: Digitally sign communications (always) | Disabled | Enabled | Change value in “Default” column based on incorrect setting per <http://technet.microsoft.com/en-us/library/jj852239.aspx> |
| Domain Controller | Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options | Microsoft network server: Digitally sign communications (if client agrees) | Disabled | Enabled | Change value in “Default” column based on incorrect setting per <http://technet.microsoft.com/en-us/library/jj852242.aspx> |