Security baseline (FINAL) for Windows 10 v1909 and Windows Server v1909

Microsoft is pleased to announce the *final* release of the security configuration baseline settings for Windows 10 version 1909 (a.k.a., “19H2”), and for Windows Server version 1909. Note that Windows Server version 1909 is Server Core only and does not offer a Desktop Experience (a.k.a., “full”) server installation option.

Download the content from the Microsoft Security Compliance Toolkit (click Download and select “Windows 10 Version 1909 and Windows Server Version 1909 Security Baseline.zip”).

This new Windows Feature Update brings very few new Group Policy settings, which we list in the accompanying documentation. None of them meet the criteria for inclusion in the baseline (which are reiterated below), but customers interested in controlling the use of USB drives and other devices should be interested in the new and very granular device installation restrictions. More about that later in this post.

The few changes we are making in the baseline since the September update to the version 1903 baselines are to remove a few settings that we have reevaluated: the restrictions on Thunderbolt devices in the BitLocker GPO, the enforcement of the default machine account password expiration for domain-joined systems, and the removal of the previously-recommended Exploit Protection settings.

In this baseline we have also removed the enforcement of the “Manage auditing and security log” privilege (SeSecurityPrivilege) on Domain Controllers because when Microsoft Exchange is installed it needs to grant this privilege to the Exchange Servers.

**Baseline criteria**

To reiterate, we follow a streamlined and efficient approach to baseline definition [when compared with the baselines we published before Windows 10](https://blogs.technet.microsoft.com/secguide/2015/11/18/changes-from-the-windows-8-1-baseline-to-the-windows-10-th11507-baseline/). The foundation of that approach is essentially this:

* The baselines are designed for well-managed, security-conscious organizations in which standard end users do not have administrative rights.
* A baseline enforces a setting only if it mitigates a contemporary security threat *and* does not cause operational issues that are worse than the risks they mitigate.
* A baseline enforces a default only if it is otherwise likely to be set to an insecure state by an authorized user:
  + If a non-administrator can set an insecure state, enforce the default.
  + If setting an insecure state requires administrative rights, enforce the default only if it is *likely* that a misinformed administrator will otherwise choose poorly.

For further illustration, see the “Why aren’t we enforcing more defaults?” section in [this blog post](https://blogs.technet.microsoft.com/secguide/2015/11/18/changes-from-the-windows-8-1-baseline-to-the-windows-10-th11507-baseline/).

**Thunderbolt devices**

First published in 2011, [Microsoft Knowledge Base article 2516445](https://support.microsoft.com/kb/2516445/) describes device installation restrictions for certain types of devices to mitigate DMA threats to BitLocker, including Thunderbolt devices. The BitLocker GPOs in our baselines have included these restrictions. Because Thunderbolt is popular, and newer computers can now mitigate that threat with kernel DMA protection – also in our baseline – we are removing the Thunderbolt restriction from our baseline. Customers on platforms that do not support kernel DMA protection can choose to continue blocking Thunderbolt, but we are no longer including it in our broad recommendations for all customers. For more information, see the KB article linked above and the articles to which it links.

**Machine account password expiration**

In Active Directory, each domain-joined computer has an Active Directory account with a strong, randomly-generated password. By default, these machine account passwords have a 30-day expiration, and computers automatically change their own passwords without any user involvement. Our baselines have always enforced these defaults. Note that reducing the expiration period will result in additional replication traffic. Also note that unlike with user account passwords, [AD doesn’t actually enforce password expiration for computer accounts](https://blogs.technet.microsoft.com/askds/2009/02/15/machine-account-password-process-2/). Password expiration and change is driven entirely by client systems. The password remains valid until it gets changed, irrespective of how “Domain member: Maximum machine account password age” is configured.

A problem that occasionally crops up is that when a domain-joined virtual machine is reverted to an earlier state that is prior to its most recent password change, the older password is no longer recognized by the domain controller, the computer has no way to authenticate to the domain, and it thus loses domain trust. Domain accounts cannot authenticate to it remotely, and interactive logon with a domain account works only if the computer has a cached credential verifier for the account and the person logging in remembers which password was used when its verifier was cached. Typically when this happens, a LAPS-managed local account cannot be used either, as the local account password will also have been reverted and not match the newer one stored in Active Directory.

Non-persistent VDI implementations and devices with write filters that disallow permanent changes to the OS volume are also examples of scenarios where machine account password expiration is problematic. When such systems change their passwords in Active Directory and then revert to their previous passwords, they can no longer authenticate.

In the absence of issues such as these, we recommend leaving the default 30-day expiration in place. But following the baseline criteria stated above, we are removing the explicit enforcement of those defaults from our baselines. Situations that necessitate disabling machine account password expiration can now be handled without being out of compliance with our baselines.

The risks of turning off machine account password expiration are relatively low. To steal a computer account password, you must first have already gained full administrative control of the computer. Having a computer account’s password gives you only the ability to act as that computer on the network from other systems. For example, if Mary gets administrative control of CONTOSO\COMPUTER\_ONE and extracts its domain account password (which is stored as an LSA secret), she can then connect to domain resources from CONTOSO\COMPUTER\_TEN but pretending to be CONTOSO\COMPUTER\_ONE. Default password expiration policy would limit her ability to do so to a maximum of 30 days. However, given that she had full control of COMPUTER\_ONE, she could presumably go back in and retrieve its new password, or have applied nefarious techniques to disable password change, keeping the password valid indefinitely.

**Exploit Protection**

Because of reported compatibility issues with the Exploit Protection settings that we began [incorporating with the Windows 10 v1709 baselines](https://blogs.technet.microsoft.com/secguide/2017/10/18/security-baseline-for-windows-10-fall-creators-update-v1709-final/), we have elected to remove the settings from the baseline and to provide a script for removing the settings from machines that have had those settings applied. (See Remove-EPBaselineSettings.ps1 in the download package’s Scripts folder.)

**New device installation restrictions available**

For many years, Windows has enabled administrators to allow or block devices such as external USB drives based on attributes such as vendor and product IDs. Windows now also enables control at a far more granular level: [device instance IDs](https://docs.microsoft.com/en-us/windows-hardware/drivers/install/device-instance-ids). For example, you could have ten identical thumb drives of the same brand, model, and capacity, pick two of them, and create a policy that allows just those to be mounted; the others would be blocked.

Because the way these settings would be configured are always specific to each customer’s situation, we don’t configure them in our baselines. But we wanted to highlight their availability as a major improvement in Windows’ device control.

You can configure the new “Allow installation of devices that match any of these device instance IDs” and “Prevent installation of devices that match any of these device instance IDs” Group Policy settings in Computer Configuration\Administrative Templates\System\Device Installation\Device Installation Restrictions. For more information, also see [How to control USB devices and other removable media using Microsoft Defender ATP](https://docs.microsoft.com/en-us/windows/security/threat-protection/device-control/control-usb-devices-using-intune).