Windows 11 22H2 Security Baseline

Microsoft is pleased to announce the release of the security baseline package for Windows 11, version 22H2!

Please download the content from the Microsoft Security Compliance Toolkit, test the recommended configurations, and customize / implement as appropriate.

This release includes numerous changes to further assist in the security of enterprise customers. Changes have been made for additional protections around hardware and driver security, credential theft, printers, DNS, and account lockout.

Kernel Mode Hardware Enforced Stack Protection

A new feature has been added to the setting located in `System\Device Guard\Turn On Virtualization Based Security` called **Kernel Mode Hardware Enforced Stack Protection**. This new setting is applicable to Windows 11, version 22H2 and above, and provides additional security enhancement for kernel code.

Notes:

- This was first discussed in a blog post back in March of 2020 (Understanding Hardware-enforced Stack Protection - Microsoft Tech Community).
- There is a hardware dependency for this new feature that requires Intel Tiger Lake and beyond or AMD Zen3 and beyond.
- This setting has a dependency on HVCI (Virtualization Based Protection of Code Integrity). There shouldn't be any issues as long as enterprises are following the baselines but, if the organization deviates from HVCI, then Kernel Mode Hardware Enforced Stack Protection cannot be enabled.
- In enforcement mode, the security baseline configures this setting to **Enabled**.

  Important: If the hardware platform does not support it, then no enforcements are enabled.
- While compatibility concerns are unlikely, customers are encouraged to test compatibility to ensure an incompatible driver doesn't lead to instability.

Additional documentation on this feature is pending. For preliminary documentation, see the Developer Guidance for Hardware-enforced Stack Protection - Microsoft Tech Community blog post.

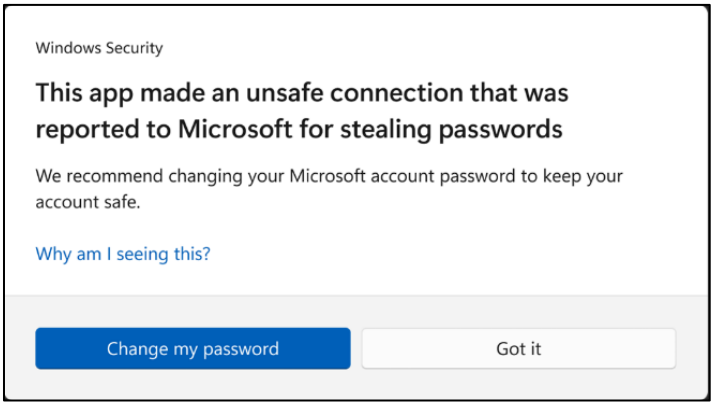
Enhanced Phishing Protection

New in Windows 11, version 22H2, are a set of features to better protect enterprise users who still rely on a username and password for Windows authentication.

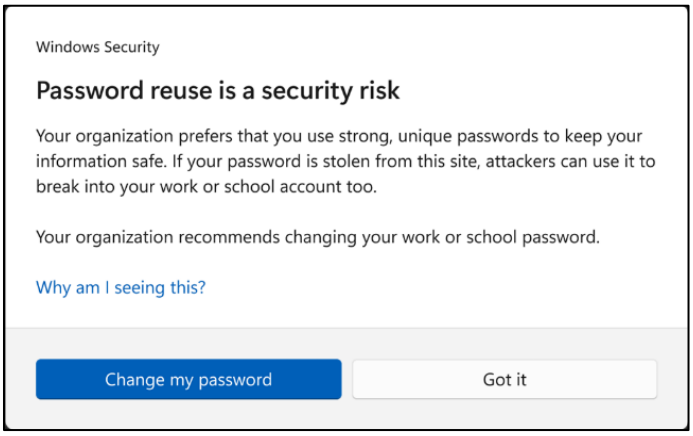
These new features, located in `Windows Components\Windows Defender SmartScreen\Enhanced Phishing Protection`, ensure that enterprise credentials cannot be used for malicious or unintended purposes. Related user activity is logged in the Microsoft Defender for Endpoint portal.

- Because this is an end-user option, the security baseline enforces enablement of the service (the **Service Enabled** setting) to ensure that the enterprise credentials used in the system are appropriately monitored and audited.

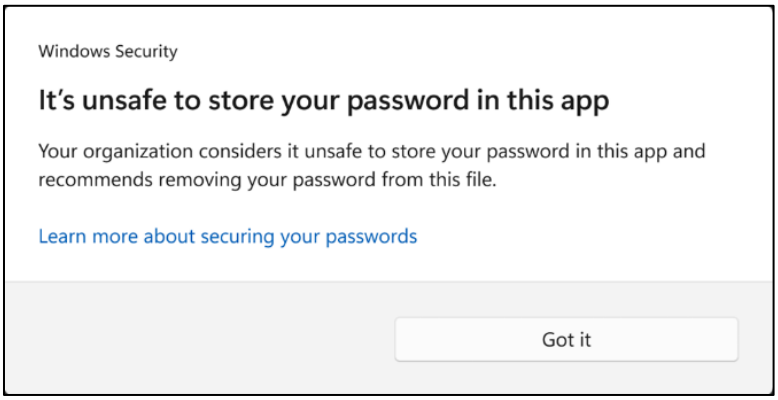
  Based on Microsoft Defender SmartScreen's robust security infrastructure, when a user enters their credentials into a known phishing or malicious site, the service alerts the user as illustrated below. In this scenario, the setting **Notify Malicious** is set to **Enabled**.



- Should an enterprise user re-use their corporate credentials in another application or website, a notification is displayed and logged, as illustrated below. In this scenario, the setting **Notify Password Reuse** is set to **Enabled.**



- Should the user decide to save their passwords in Notepad, WordPad, or other Office applications, this activity is logged with Microsoft Defender for Endpoint and the user is notified of the activity, as illustrated below. In this scenario, the setting **Notify Unsafe App** is set to **Enabled**.



Depending on your userbase, incoming support calls may question why the prompts are occurring. Microsoft advises that organizations inform security personnel and end users about the feature and how it helps keep credentials protected.

Printers

It is critical to continue to protect enterprise customers in print scenarios. With Windows 11, version 22H2, several new settings under `Administrative Templates\Printers` are enabled to further protect enterprises, including the following:

- Support for **RedirectionGuard** is added to the print service. RedirectionGuard is a security measure that prevents the use of non-administratively created redirection primitives from being followed within a given process. The setting **Configure Redirection Guard** is now **Enabled** as part of the baseline.
- Historically, Named Pipes were allowed with Print Spoolers. The use of TCP for the settings **Configure RPC connection** and **Configure RPC listener** is now enforced.
- **Configure RPC over TCP port** ensures that the incoming and outgoing connections default to a dynamic TCP port.

  Note: This setting typically requires a boundary (firewall) change to allow for a successful connection.
- **Manage processing of queue-specific files** (also called **CopyFilesPolicy**) was first introduced as a registry key in response to CVE-2021-36958 in September of 2021. This setting allows standard color profile processing using the inbox mscms.dll executable and nothing else. The security baseline is to configure this setting to **Enabled** with the option of **Limit queue-specific files to color profiles**.
- **Limit print driver installation to Administrators** was introduced to the security baselines as part of the SecGuide.ADMX before an inbox policy was available. This policy is now contained within the OS, and the MS Security Guide setting is deprecated. However, since both settings write to

the same location, the configured values still appear in both locations. The explanatory text in the MS Security Guide is updated to point users to the new location.

- **Configure RPC packet level privacy setting for incoming connections** has been added to SecGuide.ADMX as a result of CVE-2021-1678 and is set to **Enabled** as part of the baseline. The work of creating and deploying registry keys is now included in the security baseline until the setting becomes inbox to Windows.

DNS Hardening

The setting **Configure DNS over HTTPS (DoH) name resolution**, located under `Administrative Templates\Network\DNS Client`, was added as part of Windows 11 and Windows Server 2022. It is not yet part of the security baseline because it is too early to mandate encrypted DNS. Enterprises that wish to use encrypted DNS may take the following steps to implement it:

- Deploy their own Secure DNS over HTTPS (DoH) server infrastructure, whether self-managed or provided by a vendor.
- Configure Windows to use these DoH resolvers.
- When DoH servers cannot be reached, enterprises may require their endpoints to hard fail using encryption should the threat model requires this activity.

  Note: This requirement breaks scenarios such as captive portals, so it is not a recommended general practice.

The security baseline will adopt this setting in a future release. See Secure DNS Client over HTTPS (DoH) for additional information on DoH.

Configure NetBIOS settings

The setting **Configure NetBIOS settings**, located under `Administrative Templates\Network\DNS Client`, is configured to **Enabled** with a sub value of **Disable NetBIOS name resolution on public networks**. If applicable for your enterprise, optionally adjust this setting to **Disable NetBIOS name resolution**. In a future release of the security baseline, all name resolution over NetBIOS will be disabled.

Credential Theft Protection

Windows allows the use of custom security support providers and authentication providers to extend the authentication capabilities available during the login flow beyond those supported natively by Windows. These providers are loaded into Local Security Authority Subsystem Service (LSASS). Although they can provide a legitimate function, custom security packages can also be abused by attackers to gain persistence or to access and steal credentials stored in Windows. A new setting has been added to protect against this scenario:

- The setting **Allow Custom SSPs and APs to be loaded into LSASS,** located under `System\Local Security Authority`, restricts the loading of custom security packages.
- We recommend that you disable loading custom packages unless the custom package you are using is known.

Additional Local Security Authority (LSA) protection provides defense by running LSA as a protected process. LSA protection was first introduced in the Windows 8.1 security baseline, as part of the original Pass-the-Hash mitigations.

- A new setting **Configure LSASS to run as a protected process**, located under `System\Local Security Authority`, is now included inbox with Windows 11, version 22H2.
- The new setting is not backported. Therefore, all previous operating systems should continue to use the MS Security Guide setting **LSA Protection**, contained in SecGuide.ADMX. The security baseline continues to enforce the value of **Enabled with UEFI Lock** but does add a new configuration option that allows for LSA protection ***without*** UEFI lock. This brings it into parity with other features that support UEFI lock, like Credential Guard and Hypervisor-Protected Code Integrity, and allows more flexibility.

The legacy Multiple Provider Router (MPR) provides notifications to registered credential managers or network providers when there is a logon event or a password change event. MPR was created so that providers that need a user's password can collect and store credentials. This functionality is used by legitimate applications, but it can also be abused by attackers to harvest logon credentials.

- A new setting **Enable MPR notifications for the system**, located under `Windows Components\Windows Logon Options\` is used to disable MPR notifications.
- We recommend that you configure this setting to block password disclosure to providers.

Attack Surface Reduction

A new rule **Block abuse of exploited vulnerable signed drivers** is now included as part of the operating system baselines as part of the Microsoft Defender Antivirus GPO. This rule applies across both client and server and helps prevent an application from writing a vulnerable signed driver to disk.

For additional information, see the topic Attack surface reduction rules reference | Microsoft Docs.

Account Lockout Policies

A new policy **Allow Administrator account lockout**, located under `Security Settings\Account Policies\Account Lockout Policy` is added to mitigate brute-force authentication attacks. The recommended values for the policies **Account lockout duration** and **Reset account lockout counter after** are adjusted to be consistent with the defaults for out-of-the-box Windows installations.

Existing Windows installations, including upgrades to Windows 11, version 22H2, have not configured by default the **Allow Administrator account lockout** or other account lockout policies.

Other Changes

Corrected in this release was a mismatch between the security baseline documentation and the accompanying Group Policy for Microsoft Defender Antivirus settings. The documentation stated that **Windows Components\Microsoft Defender Antivirus\Real-time Protection\Turn on behavior monitoring** should be set to **Enabled**, but the actual GPO remained in a **Not Configured** state. This is corrected in this release.

Please let us know your thoughts by commenting on this post or through the Security Baseline Community.