

Auditando Windows

Auditoría y Seguridad Informática

Alumno: Vietto Herrera, Santiago

Introducción

Documento: CIS Microsoft Windows 10 Enterprise (Release 20H2 or older) Benchmark
v1.10.0 - 01-27-2021

- Proporciona una guía prescriptiva para establecer una configuración segura para Microsoft Windows. Como el documento lo indica, este se probó específicamente con Microsoft Windows 10.
- En su contenido podemos ver cuestiones como los términos de uso, definiciones, estado de evaluación, convenciones tipográficas, agradecimientos (editores, contribuidores), recomendaciones.



Estado de evaluación

El estado de la evaluación indica si una recomendación dada se puede automatizar o requiere pasos manuales para implementarse:

Automatizado: son recomendaciones para las cuales la evaluación de un control técnico se puede automatizar completamente y validar a un estado de aprobado / reprobado. Las recomendaciones incluirán la información necesaria para implementar la automatización.

Manual: son recomendaciones para aquellas evaluaciones de controles técnicos que no se pueden automatizar por completo y requieren de todos o algunos pasos manuales para validar que el estado configurado es el esperado. En estas el estado esperado puede variar según el entorno.

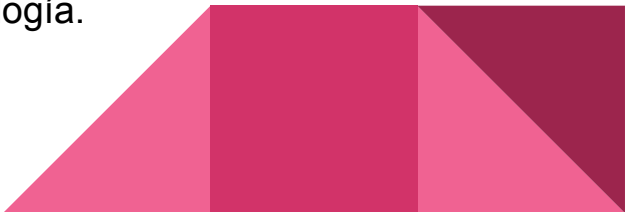


Definiciones de perfil

Este Benchmark define los siguientes perfiles de configuración:

Nivel 1 (L1) - Entorno corporativo/empresarial (uso general): los elementos de este perfil tienen la intención de ser la línea de base inicial para la mayoría de las organizaciones, para que sea práctico y prudente, proporcionar un beneficio de seguridad claro, y no inhibir la utilidad de la tecnología más allá de los medios aceptables.


Nivel 2 (L2) - Entorno de datos confidenciales/alta seguridad (funcionalidad limitada): este perfil amplía el perfil "Nivel 1 (L1)". Los elementos de este perfil exhiben uno o más de las siguientes características:

- Están destinados a entornos o casos de uso, en los que la seguridad es más crítica que la capacidad de gestión y la usabilidad.
 - Puede inhibir negativamente la utilidad o el rendimiento de la tecnología.
 - Limitar la capacidad de administración / acceso remoto.
- 

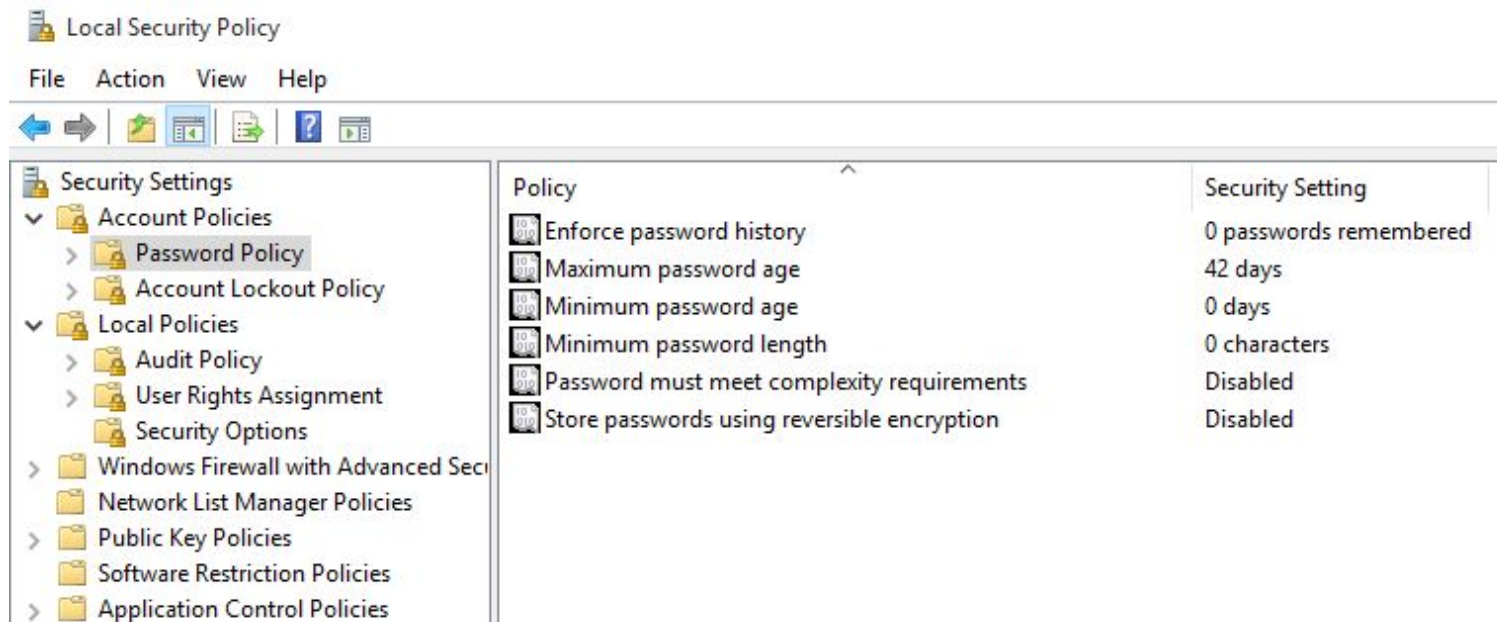
Recommendations

Account Policies

Password Policy

- 1) (L1 - automated) Ensure 'Enforce password history' is set to '24 or more password(s)'
 - 2) (L1 - automated) Ensure 'Maximum password age' is set to '60 or fewer days, but not 0'
 - 3) (L1 - automated) Ensure 'Minimum password age' is set to '1 or more day(s)'
 - 4) (L1 - automated) Ensure 'Minimum password length' is set to '14 or more character(s)'
 - 5) (L1 - automated) Ensure 'Password must meet complexity requirements' is set to 'Enabled'
 - 6) (L1 - automated) Ensure 'Store passwords using reversible encryption' is set to 'Disabled'
- 

Acceso: Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies>Password Policy\"..."



Recommendations

Account Policies

Account Lockout Policy

- 1) (L1 - automated) Ensure 'Account lockout duration' is set to '15 or more minute(s)'
- 2) (L1 - automated) Ensure 'Account lockout threshold' is set to '10 or fewer invalid logon attempt(s), but not 0'
- 3) (L1 - automated) Ensure 'Reset account lockout counter after' is set to '15 or more minute(s)'



Acceso: Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Account Lockout Policy\"..."

