

Guía para proteger la instalación de su M365 Security Plus



Descripción

El directorio de instalación de M365 Security Plus contiene archivos importantes requeridos para que funcione adecuadamente, incluyendo archivos que se usan para iniciar y detener el producto y el archivo de licencia. El acceso no autorizado al directorio de instalación podría indicar que un usuario está alterando su contenido, lo que a su vez podría resultar en posibles amenazas de seguridad, tales como la divulgación de información confidencial o que el producto no funcione. En este documento se analizan las medidas para evitar que usuarios no autorizados accedan al directorio de instalación de M365 Security Plus y modifiquen su contenido.

Para nuevas instalaciones de M365 Security Plus

Para nuevas instalaciones de las compilaciones 4538 y posteriores, solo se suministra acceso automáticamente a los siguientes tipos de cuentas para el directorio de instalación con el fin de garantizar la seguridad e integridad de los archivos:

- Cuenta de sistema local
- Cuenta de usuario utilizada durante la instalación del producto
- Grupo de administradores de dominios
- Grupo de administradores

Importante:

- Si el producto se instala como un servicio, asegúrese de que a la cuenta configurada en la **pestaña Inicio de sesión** de las propiedades del servicio se le asigne el permiso de **Control completo** para el directorio de instalación.
- Para permitir que otros usuarios accedan al directorio de instalación, se les debe asignar el permiso de **Control completo** para tal fin. Consulte el [Apéndice](#) para instrucciones paso a paso.

Para instancias existentes de M365 Security Plus

Se puede evitar que usuarios no autorizados accedan al directorio de instalación de M365 Security Plus para compilaciones previas a 4539 de dos formas:

- i. Ejecute el archivo [SetPermission.bat](#)
- ii. Elimine permisos innecesarios manualmente

I. Ejecute el archivo SetPermission.bat

Con este método, el acceso al directorio de instalación se restringe automáticamente solo a las cuentas necesarias.

Actualice a la compilación 4539 o posterior usando [service packs](#).

Abra el **símbolo de sistema** como administrador y vaya a la carpeta **<installation directory>/bin** (predeterminadamente **C:\Program Files\ManageEngine\M365 Security Plus\bin**.) Ejecute el archivo **SetPermission.bat**.

```

Microsoft Windows [Version 10.0.22631.3593]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>cd C:\Program Files\ManageEngine\M365 Security Plus\bin

C:\Program Files\ManageEngine\M365 Security Plus\bin>SetPermission.bat

C:\Program Files\ManageEngine\M365 Security Plus\bin>set SERVER_HOME=C:\Program Files\ManageEngine\M365 Security Plus\bin\..\

C:\Program Files\ManageEngine\M365 Security Plus\bin>set SERVER_HOME=C:\Program Files\ManageEngine\M365 Security Plus\bin\..\

C:\Program Files\ManageEngine\M365 Security Plus\bin>icacls.exe /grant *S-1-5-18:(OI)(CI)F /T /Q /grant *S-1-5-32-544:(OI)(CI)F /T /Q
Successfully processed 11433 files; Failed processing 0 files

C:\Program Files\ManageEngine\M365 Security Plus\bin>icacls.exe "C:\Windows\system32\icacls.exe" "C:\Program Files\ManageEngine\M365 Security Plus\bin\.." /grant:(OI)(CI)RM /T /Q
Successfully processed 11433 files; Failed processing 0 files

C:\Program Files\ManageEngine\M365 Security Plus\bin>icacls.exe "C:\Program Files\ManageEngine\M365 Security Plus\bin\.." /grant:(OI)(CI)RM /T /Q
Successfully processed 11433 files; Failed processing 0 files

C:\Program Files\ManageEngine\M365 Security Plus\bin>icacls.exe "C:\Windows\system32\icacls.exe" "C:\Program Files\ManageEngine\M365 Security Plus\bin\.." /inheritance:r /Q
Successfully processed 1 files; Failed processing 0 files

C:\Program Files\ManageEngine\M365 Security Plus\bin>icacls.exe "C:\Windows\system32\icacls.exe" "C:\Program Files\ManageEngine\M365 Security Plus\bin\.." /remove:g "CREATOR OWNER" /T /Q /remove:g "BUILTIN\Users" /T /Q /remove:g "S-1-15-2-1" /T /Q
Successfully processed 11433 files; Failed processing 0 files

C:\Program Files\ManageEngine\M365 Security Plus\bin>icacls.exe "C:\Windows\system32\icacls.exe" "C:\Program Files\ManageEngine\M365 Security Plus\bin\.." /remove:g *S-1-5-11 /T /Q /remove:g *S-1-15-2-2 /T /Q
Successfully processed 11433 files; Failed processing 0 files

C:\Program Files\ManageEngine\M365 Security Plus\bin>GOTO End

C:\Program Files\ManageEngine\M365 Security Plus\bin>endlocal

C:\Program Files\ManageEngine\M365 Security Plus\bin>

```

II. Modifique los permisos requeridos manualmente

Para eliminar permisos de acceso para grupos innecesarios, como Usuarios autenticados y Usuarios de dominios, siga los pasos detallados abajo.

- Deshabilite la Herencia para el directorio de instalación (predeterminadamente **C:\Program Files\ManageEngine\M365 Security Plus**). Consulte el apéndice para instrucciones paso a paso.
- Elimine los permisos de acceso para todos los grupos innecesarios. Consulte el [Apéndice](#) para instrucciones paso a paso.
- Suministre permisos de **Control completo** a las siguientes cuentas y grupos para el directorio de instalación del producto:

- Cuenta de sistema local
- Grupo de administradores de dominios
- Grupo de administradores
- Para usuarios que pueden abrir el producto

Consulte el [Apéndice](#) para instrucciones paso a paso.

- Asigne el permiso de **Control completo** para la carpeta del directorio de instalación a usuarios que puedan abrir el producto. Consulte el [Apéndice](#) para instrucciones paso a paso.
- Si el producto se instala como un servicio, asegúrese de que a la cuenta configurada en la pestaña **Inicio de sesión** de las propiedades del servicio se le asigne el permiso de **Control completo** para la carpeta.

Nota:

- Microsoft recomienda que el software se instale en el directorio de **Archivos de programa**. Con base en sus necesidades específicas o políticas organizacionales, puede escoger una ubicación distinta.

Apéndice

Pasos para deshabilitar la herencia

1. Haga clic derecho en el directorio de instalación y escoja **Propiedades**.
2. Vaya a la pestaña **Seguridad** y haga clic en **Avanzado**.
3. Haga clic en **Deshabilitar herencia**.
4. Haga clic en **Aplicar** y luego en **OK**.

Pasos para eliminar cuentas innecesarias de la ACL

1. Haga clic derecho en el directorio de instalación y escoja **Propiedades**.
2. Vaya a la pestaña **Seguridad** y haga clic en **Editar**.
3. Seleccione los grupos innecesarios y haga clic en **Eliminar**.
4. Haga clic en **Aplicar** y luego en **OK**.

Para asignar permisos de control completo a usuarios

1. Haga clic derecho en el directorio de instalación y escoja **Propiedades**.
2. Vaya a la pestaña **Seguridad** y haga clic en **Editar**.
3. Haga clic en **Añadir**.
4. Ingrese el nombre del usuario o grupo y haga clic en **OK**.
5. En la sección **Permisos para usuarios**, en la columna **Permitir**, marque la casilla para permitir el permiso de **Control completo**.
6. Haga clic en **Aplicar** y luego en **OK**.

Nuestros productos

AD360 | Log360 | ADAudit Plus | EventLog Analyzer | DataSecurity Plus | Exchange Reporter Plus

M365 Security Plus es una herramienta de seguridad exclusiva para Microsoft 365 que ayuda a detectar ataques de seguridad y analiza riesgos en su entorno de M365 Security Plus. Con esta interfaz intuitiva puede proteger y reforzar Exchange Online, Azure Active Directory, Skype for Business, OneDrive for Business, SharePoint Online, Microsoft Teams y otros servicios de Microsoft 365 desde una misma consola.