**Acronis DeviceLock DLP**



Daniel Escaño Hernández CET Ciberseguridad

# **1. Índice:**

[**1. Índice:**](#_lmwzrhyaxgtw) **1**

[**2. Windows**](#_g59i8ewd3ed3) **2**

[**2.1 Acronis DeviceLock DLP:**](#_5d38uxjyswtl) **2**

# **2. Windows**

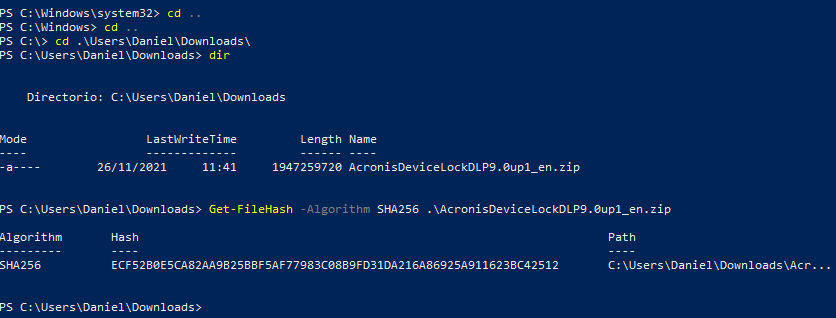
### **2.1 Acronis DeviceLock DLP:**

Desde la página oficial de Acronis DeviceLock descarga la versión de prueba

en la máquina virtual Windows. Con fecha de 21 Noviembre del 2021, el archivo

que propone a descargar es la build 91972 con un tamaño de 1,8GB, y

publicada el 1 de Julio del 2021.



Comprueba que el hash SHA256 coincide con el siguiente antes de instalarlo:

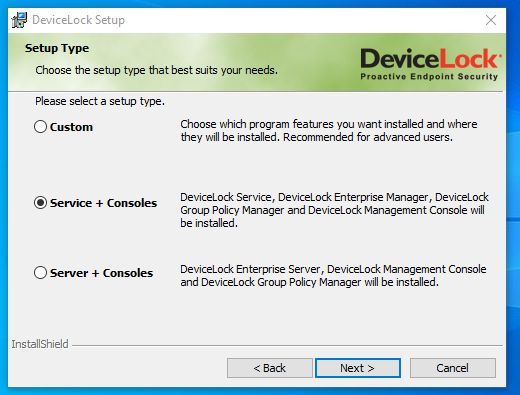
ecf52b0e5ca82aa9b25bbf5af77983c08b9fd31da216a86925a911623bc42512

2. Una vez que hemos comprobado la descarga y nos hemos asegurado de que

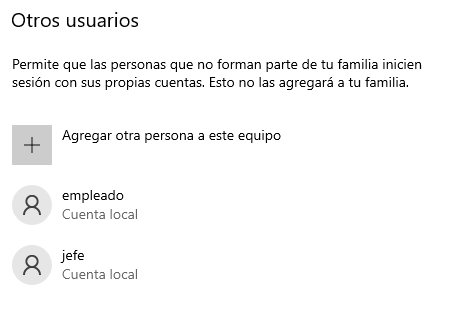
proviene de la fuente original, proceder a instalarlo en la máquina virtual

Windows 10. Hay que seleccionar el tipo de instalación Service + Consoles.

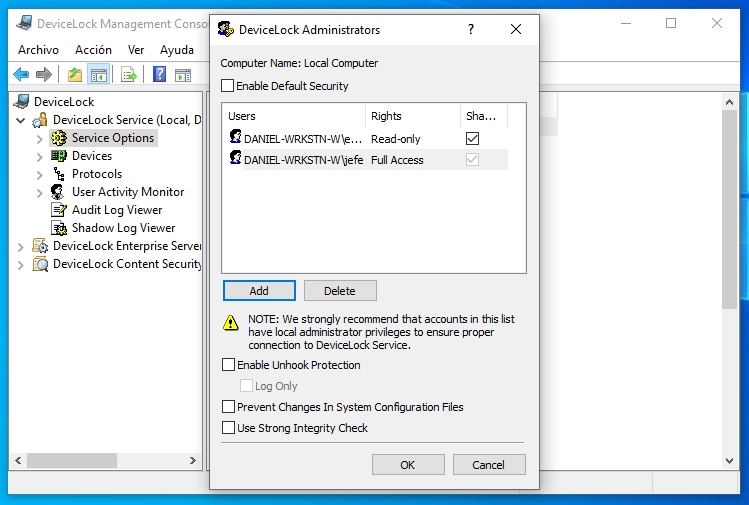
Este nos permite establecer los controles en un único ordenador.



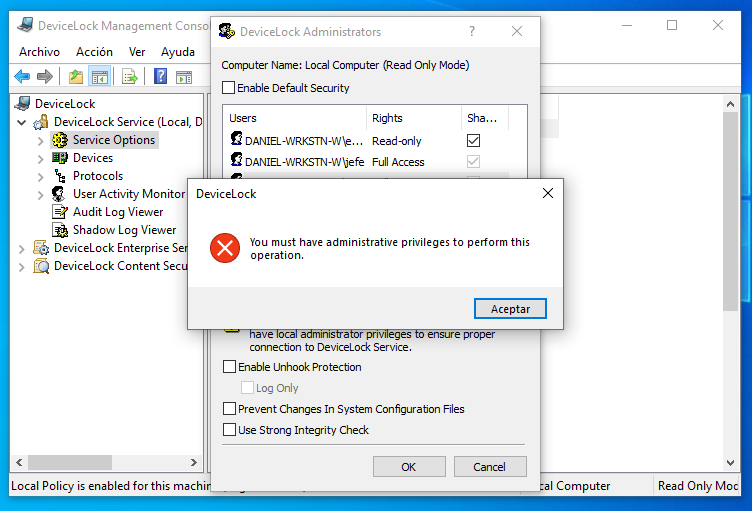
3. Crear un usuario en la máquina que se llame “empleado” y otro “jefe”.



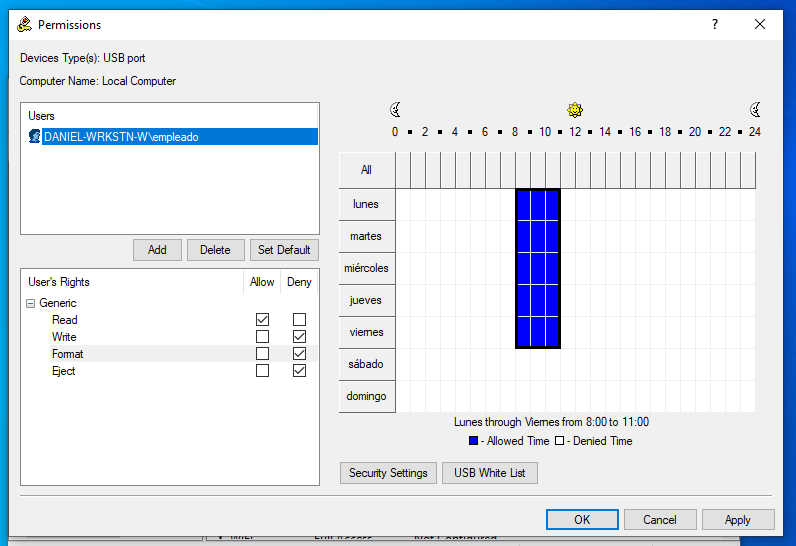
4. Abre DeviceLock Management Console. Configura en las opciones del servicio, la opción DeviceLockAdministrators a enabled. Añadir el usuario empleado en esta restricción con permiso de sólo-lectura y activar la casilla shadow data. Lo que hemos conseguido con esto, es impedir que el empleado pueda acceder a la Consola de Administración. Nota: te pedirá que al menos un usuario tenga permiso (añadiremos al jefe con acceso total).

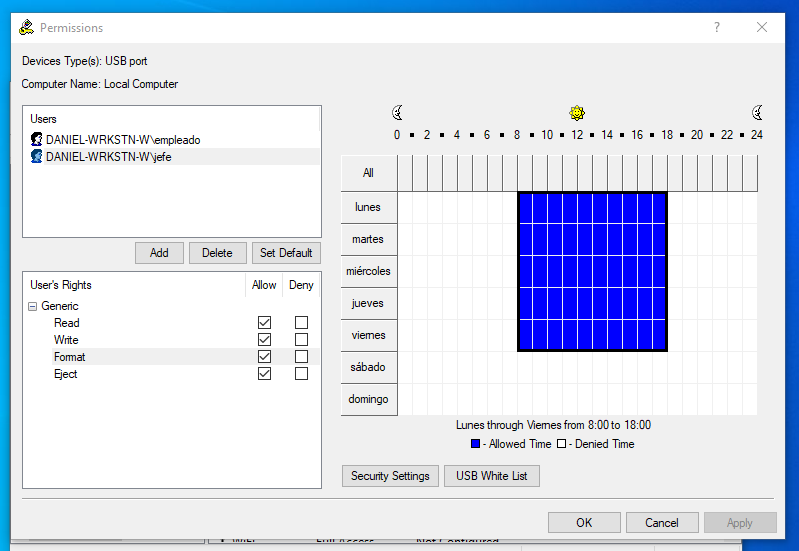


5. Haz login con el usuario empleado y comprueba que no puedes cambiar las opciones anteriores desde la Consola de Administración.

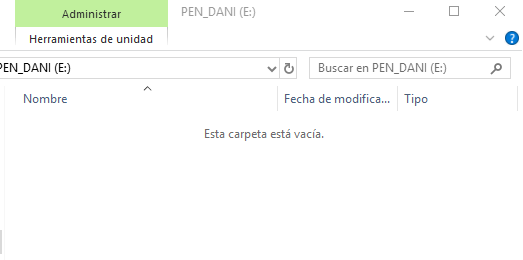


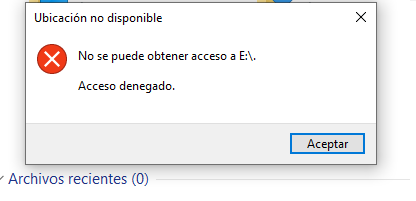
6. Vamos a establecer una opción para que todos los usuarios excepto los administradores puedan conectar un USB. DeviceLockService – Devices – Permissions. En la opción USB Port, hacer los cambios necesarios para el empleado de la siguiente forma: Podrá leer los dispositivos USB entre las 08:00 y las 10:00 de Lunes a Viernes. Denegar resto de opciones en cualquier horario (escritura, formateo y eject). Permitir al jefe, cualquier opción sobre los USB de 08:00 a 17:00 (coincide con el horario laboral de la empresa) Eliminar el grupo Todos.



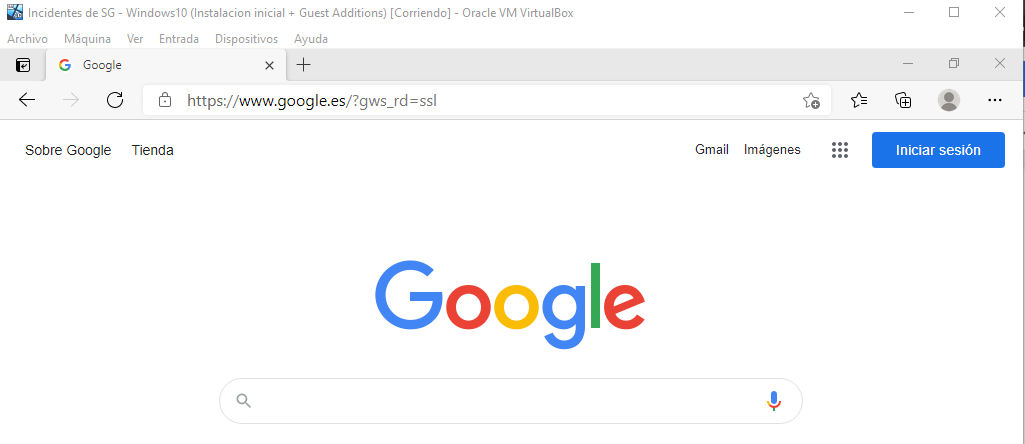


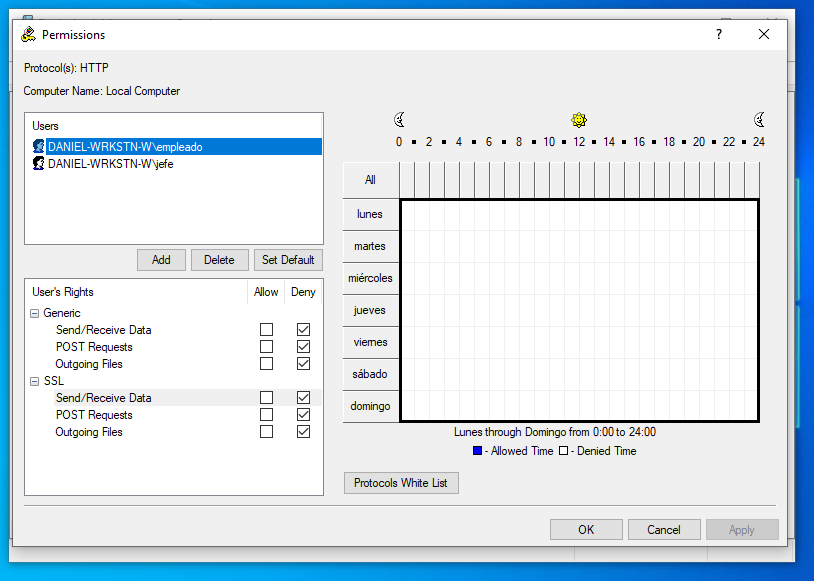
7. Logeate con el usuario jefe e introduce un pendrive. Comprueba que puedes acceder sin problemas. Haz la misma prueba con el usuario empleado y comprueba las restricciones aplicadas (dependiendo del horario).

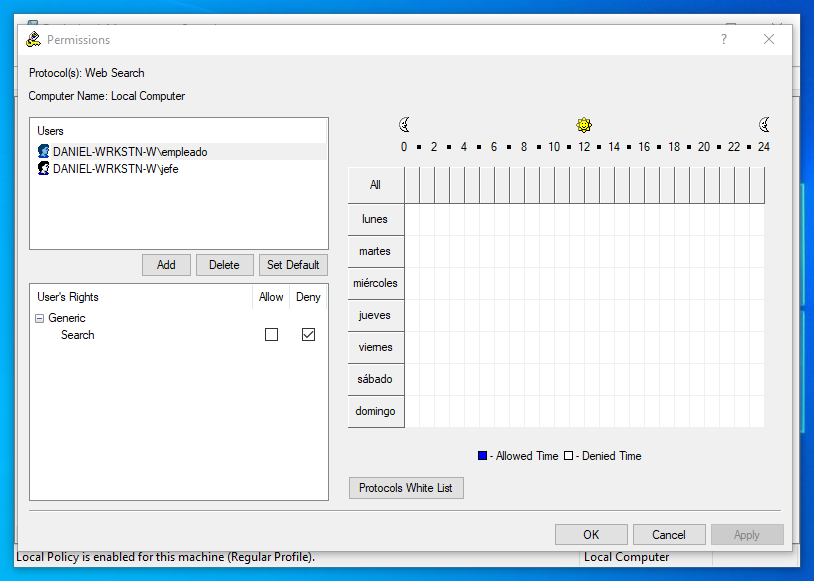


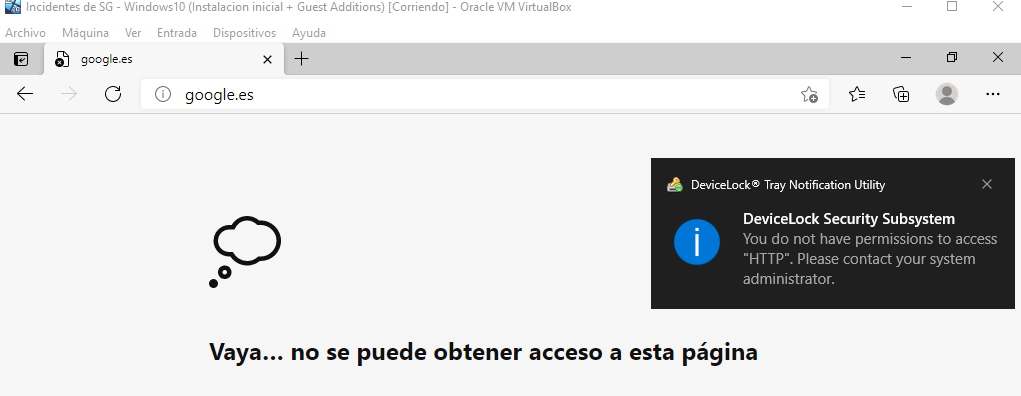


8. Desactiva la opción de navegación para el empleado y permítelo para el jefe. Haz las pruebas necesarias para comprobar que funciona.









9. De entre las múltiples opciones de configuración y bloqueo de este programa, elige a tu criterio alguna concreta y realiza las pruebas necesarias para comprobar que efectivamente funciona.

