Control de Cuentas

Transcribed on August 3, 2025 at 1:51 PM by Minutes AI

Speaker 1 (00:08)

Bienvenidos a esta nueva sesión.

En esta sesión vamos a tratar el tema del Control de cuentas de usuario.

Vamos a hablar del control de cuentas de usuario, hablaremos del código de colores del control de cuentas de usuario, de la ventana emergente que nos aparece cuando salta el control de cuentas de usuario y otras maneras que tendremos para configurar el control de cuentas de usuario para que sea más eficiente y también las directivas que sirven para administrar el control de cuentas de usuario.

El control de cuentas de usuario está presente en Windows desde Windows Vista.

Lo que hace es que cuando un usuario administrador inicia sesión se le otorgan dos un token de usuario sin privilegios, que es el que va a utilizar habitualmente y cuando requiere utilizar el token de administrador porque una tarea necesita esos privilegios, va a aparecer la ventana emergente del control de cuentas de usuario que va a solicitar confirmación o en el caso de que utilicemos un usuario estándar, va a solicitar que pongamos usuario administrador y contraseña.

Una vez que ponemos las credenciales o damos la aprobación, automáticamente se continúa con la tarea, se realiza esa operación y después se vuelve a tener ese token sin privilegios.

El control de cuentas de usuario permite compartir permisos, perfiles y proteger al usuario manteniendo el mismo perfil y tenemos las configuraciones documentos en el mismo sitio, independientemente de utilizar un usuario con el token sin privilegios o con el token administrado.

El código de colores del control de cuentas de usuario cuando bloquea una ventana es rojo, cuando indica peligro, un firewall bloqueado, una aplicación desde Internet sin firma, verde, una aplicación firmada por Microsoft potencialmente segura, una aplicación con firma de terceros o amarillo que es una aplicación sin firma o con una firma que no es de confianza.

El diálogo del control de cuentas de usuario se ejecuta en otro contexto al que el fondo de escritorio normal no puede llegar.

Esto va a evitar que un malware pueda acceder a la pantalla de diálogo y aprobar la acción a ejecutar.

El mensaje del Control de cuentas de usuario aparece en un entorno de escritorio oscurecido.

En ese escritorio seguro, Windows solo permite procesos confiables de System.

Podemos utilizar el control de cuentas de usuario de una manera mucho más eficiente si nosotros elevamos el perfil de exigencia al nivel más alto.

De esta manera nosotros lo que vamos a hacer es que vamos a limitar todavía algún tipo de procesos que hay en el que tenemos por defecto, en el que elementos del sistema y algunas librerías tienen la capacidad de poder autoelevarse.

Si a esto le añadimos que utilizar un usuario que no tenga privilegios, cuando el control de cuentas de usuario salta, nos va a pedir no solo confirmación, sino que nos va a pedir ese usuario administrador con la contraseña correspondiente.

Esta configuración va a permitir que el control de cuentas de usuario no permita los ataques de autoelevación o limite mucho los ataques de autoelevación y otros ataques conocidos.

Bueno, estamos en la máquina virtual, nos vamos a la parte de configuración, nos vamos a la parte de usuarios y vamos a crear un usuario.

Vamos a añadir una cuenta de usuario, vamos a crear el usuario bajo.

Si nosotros estamos en un usuario que es administrador, vamos a la configuración del control de cuentas de usuario y vemos que la configuración por defecto que tenemos en el control de cuentas de usuario no está en el nivel más elevado.

Si nosotros lo situamos en el nivel más elevado nos pide confirmación.

Dentro de esta confirmación nosotros podemos ver más detalles y luego, aparte de ver más detalles, podemos ver información sobre el certificado digital del fabricante que ha lanzado esa petición, del software que ha lanzado esa petición.

Le decimos que sí y ya tendríamos la configuración del control de cuentas de usuario en el nivel más alto.

Si ahora nosotros nos vamos a un usuario que no tenga privilegios, vamos a cambiar el usuario, cerramos sesión, iniciamos sesión con nuevo usuario sin privilegios.

Si ahora nosotros vamos a la configuración del control de cuentas de usuario, la configuración del control de cuentas de usuario, el modificar esta configuración o el acceder a esta configuración ya de por sí nos va a solicitar privilegios.

Vemos que en este caso no sólo no nos pide confirmación, sino que además nos pide como usuario administrador una contraseña.

Introducimos el usuario y la contraseña y vemos que tenemos la configuración por defecto más estricta para un usuario estándar.

A partir de Windows 11 esta sería la configuración por defecto.

Esto va a evitar ataques de autoelevación de privilegios.

Había una serie de librerías, una serie de ejecutables del sistema que tenían la capacidad de autoelevar en la petición del control de cuentas de usuario.

En este nivel, que es el más exigente, se desactiva esa característica de tal manera que el entorno es mucho más seguro.

El control de cuentas de usuario puede configurarse para que sea todavía más seguro a través de directivas de grupo.

Para ello tenemos la opción de configuración mediante las directivas de seguridad utilizando el comando secund msc y configurar las opciones de seguridad.

También tenemos la posibilidad de hacer algunas configuraciones adicionales como requerir la ruta de acceso de confianza para la entrada de credenciales o enumerar las cuentas de administrador.

Estas dos opciones estarían dentro de la configuración de equipo de plantillas administrativas de componentes de Windows.

Abrimos la consola de directivas de seguridad, nos vamos a las directivas locales, nos vamos a las opciones de seguridad y vamos a ver que dentro de las opciones de seguridad vamos a tener una serie de configuraciones sobre el control de cuentas de usuario.

Vamos a la parte de abajo del todo y vemos Tenemos aquí las configuraciones del control de cuenta de usuario, vemos que la mayor parte de las configuraciones están deshabilitadas y nosotros tenemos algunas configuraciones que están habilitadas.

En este caso vemos que tenemos esta configuración habilitada y vemos que tendríamos aquí la explicación de lo que hace esa configuración.

Si nos vamos a una configuración que está deshabilitada tendríamos aquí la explicación de lo que hace.

Simplemente tendríamos que venir aquí y tendríamos que habilitar esto.

Si estamos en una organización, si estamos en una empresa, generalmente se hará de forma centralizada a través de directivas de grupo desde el controlador de dominio.

Si nosotros utilizamos el comando gpedit nos aparece el editor de directivas de grupo y dentro de lo que sería la parte de configuración de grupo y dentro de lo que sería la parte de configuración de grupo de equipo, dentro de lo que sería la parte de plantillas administrativas, dentro de lo que sería la parte de componentes de Windows, dentro de Interfaz de credenciales de usuario, pues vamos a tener la de enumerar las cuentas de administrador y vamos a tener la de requerir ruta de acceso de confianza para la entrada de credenciales.

De esta manera, habilitando estas características nosotros vamos a tener una configuración mucho más eficiente del funcionamiento del control de cuentas de usuario.

Microsoft dispone de una serie de tecnologías que nos ayudan a proteger el equipo, dificultando la ejecución de programas no autorizados o malware.

Estas opciones que funcionan por defecto pueden configurarse para ser más eficientes.

Un ejemplo es el control de cuentas de usuario.

Llegamos al final de la sesión.

Os esperamos en el siguiente vídeo.