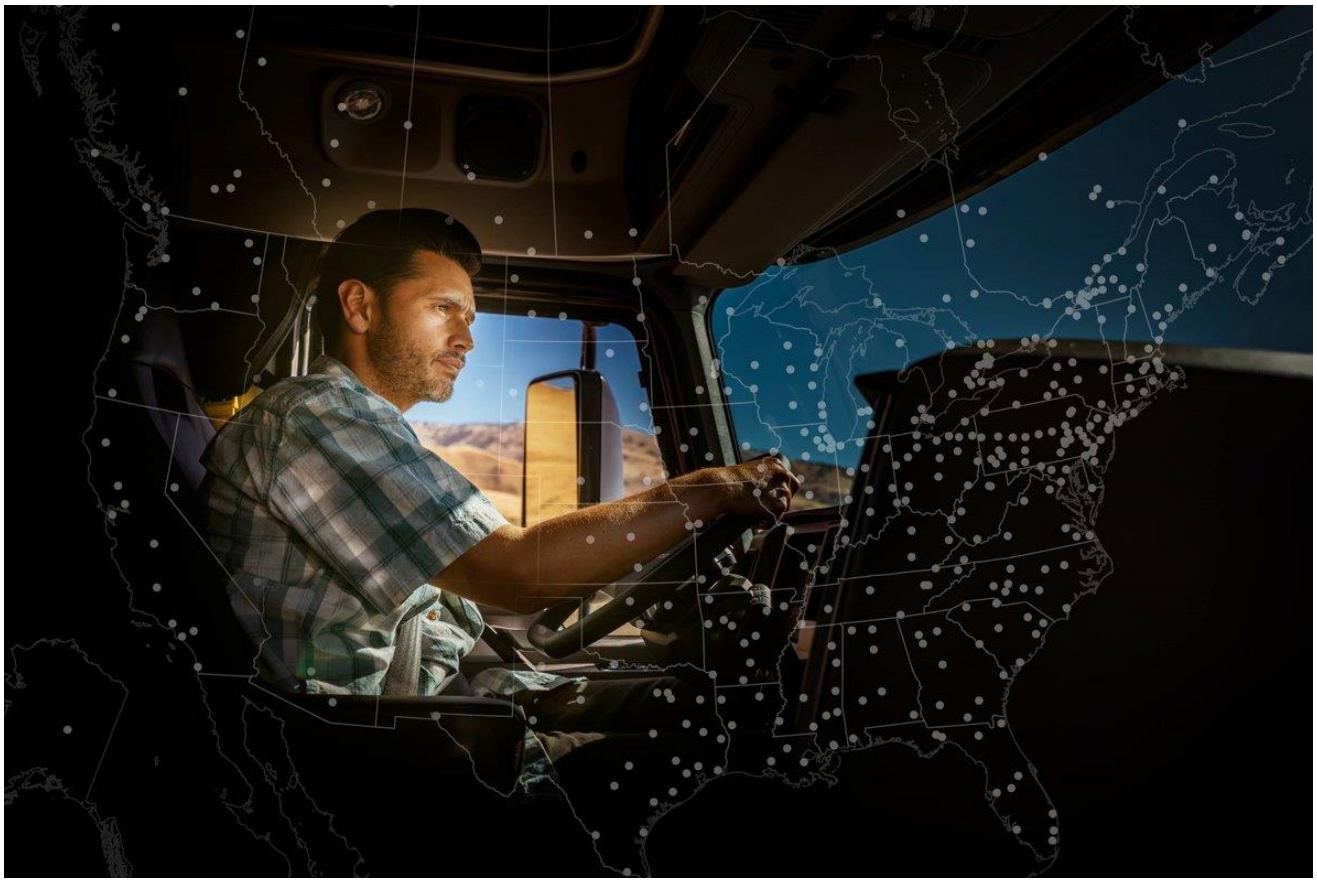

Mejora de la ciberseguridad con **AMF** (Autenticación multifactorial)

Preguntas frecuentes (FAQ)

Autenticación multifactor

Paso 1: Activación de AMF (dirección de correo electrónico única)	
Pregunta	Respuesta
¿Cómo compramos las llaves de seguridad?	https://www.yubico.com/products/yubikey-5-overview/ https://support.yubico.com/hc/en-us/articles/5036367557148-Where-can-I-buy-YubiKeys-
¿Cómo obtendría Volvo los números de serie integrados en la nueva solución AMF para Tech Tool (TT)?	Estamos detallando los pasos para la incorporación de AMF. El enfoque consistiría en que los usuarios se registraran en AMF. Según la opción, los usuarios serán guiados a través de los pasos para registrar la clave de seguridad (es decir, YubiKey es una marca de dispositivo). Nota: - Una llave de seguridad por computadora portátil (no por persona). - El número de usuarios por clave de seguridad está limitado a 25 usuarios (si se utilizan claves biométricas, el límite es de 5 usuarios) - Las llaves de seguridad no están vinculadas a ubicaciones o dispositivos específicos. Los usuarios individuales y los ID de tienda se pueden agregar y eliminar a las claves según sea necesario.
¿El registro del dispositivo se realiza como el primer paso de activación para poder usar la clave o se realiza cuando los técnicos intentarían usarla por primera vez para Tech Tool??	El primer paso del proceso es la incorporación de AMF. El segundo paso es lanzar el software TT que está listo para AMF en agosto. Publicar que los usuarios podrán usar AMF para TT.

Es obligatoria una dirección de correo electrónico única de la empresa.?	Se prefiere encarecidamente una dirección de correo electrónico única según los estándares de AMF.
¿Qué pasa con los pequeños distribuidores que no tienen su propio dominio??	Se prefiere encarecidamente una dirección de correo electrónico de la empresa, pero no es obligatoria.
¿Por qué se requieren dos métodos AMF?	Se requieren dos métodos AMF para que cada usuario acceda a las aplicaciones Volvo. Tener un método AMF de copia de seguridad en caso de que se requiera un restablecimiento de contraseña para una recuperación más rápida si se pierde la clave de seguridad.
¿Será posible que 1 usuario se conecte a 2 herramientas técnicas al mismo tiempo??	Sí.
¿Cuáles son los plazos que debemos tener en nuestro radar con respecto al despliegue de AMF??	Noviembre 23rd 2023.
¿Dónde puedo encontrar más información sobre la aplicación Microsoft Authenticator?	https://support.microsoft.com/en-us/account-billing/download-and-install-the-microsoft-authenticator-app-351498fc-850a-45da-b7b6-27e523b8702a
¿Quién informar de problemas de autorización durante el inicio de sesión de AMF?	Póngase en contacto con su respectivo servicio de soporte de primera línea y ellos tendrán procesos establecidos para obtener el soporte necesario para solucionar el problema.
¿Qué especificaciones se requieren para la llave?	https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-passwordless#fido2-security-keys
¿Qué pasa con las aplicaciones locales (concesionarios) que podrían estar conectadas a los sistemas de Volvo Group?	Eventualmente, todas las aplicaciones de Volvo Group utilizarán AMF.
Los distribuidores de doble marca (MACK / VCE), en dos áreas comerciales diferentes, tendrán 2 inicios de sesión de ID de usuario, pero solo 1 correo electrónico. ¿Funciona AMF para cada inicio de sesión?	AMF se configura para cada cuenta. El enfoque multifactorial para los distribuidores de doble marca todavía está en revisión y el caso de uso no ha sido aprobado.

Paso 2: Inscripción de AMF (Método AMF de configuración)	
Question	**Answer**
¿Cuándo puedo empezar a configurar mis métodos AMF??	¡Lo antes posible! Visite https://myaccount.microsoft.com e inicie sesión en su cuenta de Microsoft Azure con su UPN (12345@ext.volvogroup.com) para configurar sus métodos de AMF.
¿Cuáles son las aplicaciones de autenticación compatibles??	Aplicación Microsoft Authenticator. Requisitos del sistema operativo de la aplicación Authenticator: Android - v8.0 o posterior IOS - v14.0 o posterior iPad OS – 14.0 o más tarde
¿Es compatible con alguna otra aplicación de autenticación??	Volvo Group recomienda la aplicación Microsoft Authenticator para verificar que Multi-Factor Autenticación esté configurado. Si prefiere utilizar aplicaciones de otros proveedores, siga las instrucciones proporcionadas por el proveedor.
¿Podemos usar el mismo número de teléfono para varios usuarios?	Volvo Group recomienda usar un teléfono dedicado para cada usuario para evitar posibles problemas de seguridad.
¿Cómo funcionará la llamada telefónica con un sistema telefónico automatizado? ¿Se requerirá un número de marcación directa??	Volvo utiliza un sistema de perfeccionamiento.
¿Cuál es la alternativa si una llamada telefónica fallara? (es decir, el usuario cambia el número de teléfono)	Volvo recomienda seleccionar el método AMF primario y de respaldo durante el proceso de configuración del AMF.
¿Dónde iríamos para actualizar el número de teléfono de un usuario??	Las opciones de inicio de sesión de AMF Mis inicios de sesión | Información de seguridad | Microsoft.com permite a una persona cambiar las opciones y el número de teléfono.
¿Cuánto tiempo tarda un número de teléfono en actualizarse si se cambiara??	Las actualizaciones se realizan en tiempo real.
¿Es el correo electrónico una opción de método AMF??	No, el correo electrónico no es una opción AMF disponible, ya que no es una forma segura de proporcionar autenticación multifactorial.

	La dirección de correo electrónico es necesaria para AMF y MS admite el restablecimiento de contraseña utilizando el correo electrónico como identificador, pero el correo electrónico no es una forma segura de proporcionar validación AMF.

Paso 3: Aplicación de AMF (inicio de sesión de Microsoft Azure)	
Pregunta	Respuesta
¿Qué sucede cuando un usuario inicia sesión con Azure AD?	**Escenario 1: el usuario inicia sesión por primera vez con una contraseña que no cumple con la directiva de contraseñas:** Si se crea un nuevo usuario, la contraseña siempre debe cumplir con la directiva de contraseñas. El único caso en el que un usuario puede iniciar sesión con un formato de contraseña "no válido" es si se creó antes de que se aplicara la directiva de contraseñas. **Escenario 2: para contraseñas de usuario que no caducan:** cuando una contraseña no caduca, no se activará la política de contraseñas. El usuario no recibirá ninguna notificación para cambiar la contraseña. **Escenario 3: inicios de sesión de Azure identificados como de "alto riesgo":** se puede solicitar un restablecimiento de contraseña para usuarios de alto riesgo de acuerdo con la directiva de acceso condicional de Azure AD. Un ejemplo: si un ID de usuario / inicio de sesión está activo en North America y se intenta iniciar sesión en Francia una hora más tarde, Azure marca esta actividad como de riesgo elevado y se enviará un error al iniciar sesión.