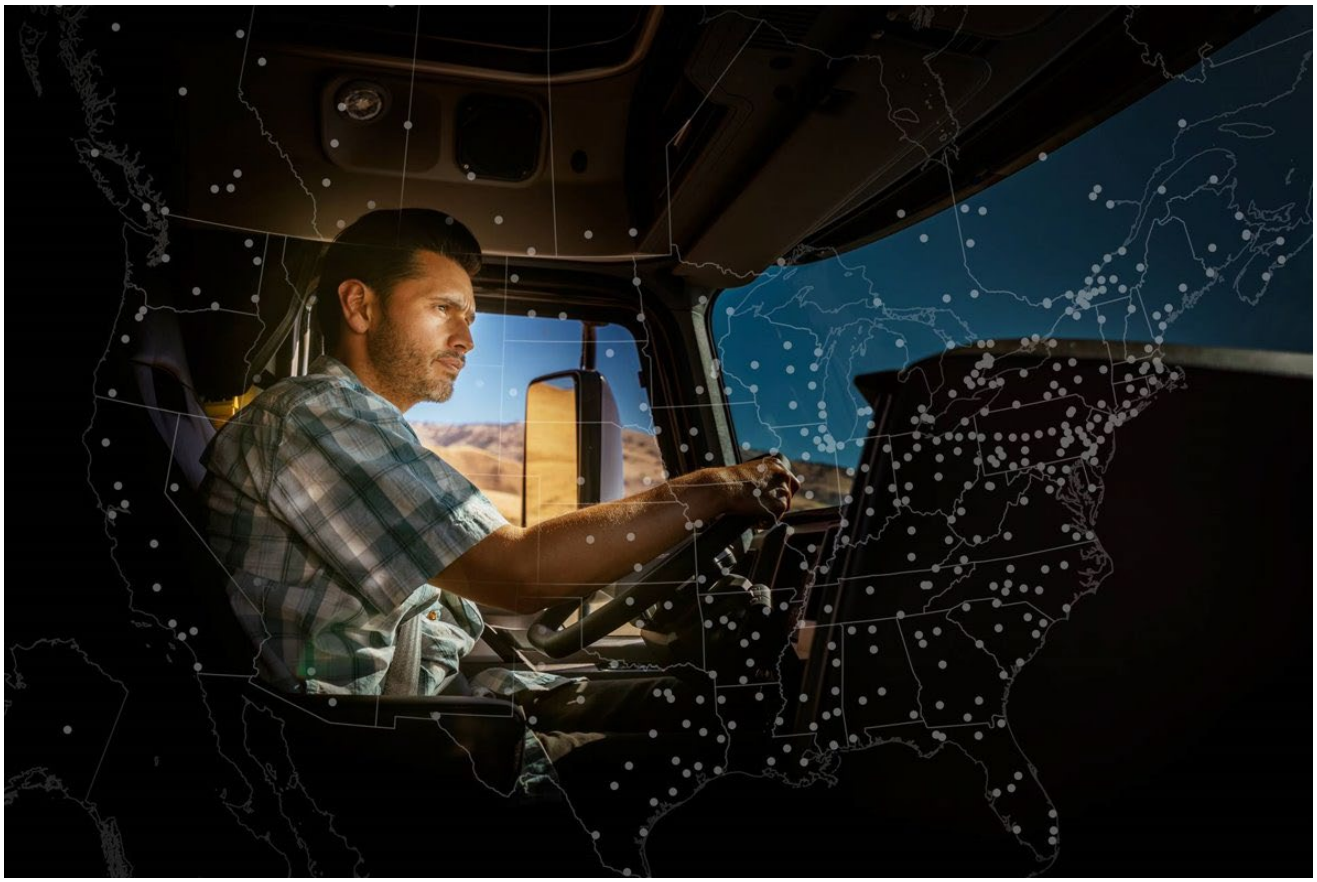

Améliorer la cybersécurité avec AMF(Authentification multifacteur)

Questions fréquentes (FAQ)

Authentification multifacteur

Étape 1: Activation AMF (adresse e-mail unique)	
Question	Répondre
Comment achetons-nous les clés de sécurité ?	https://www.yubico.com/products/yubikey-5-overview/ https://support.yubico.com/hc/en-us/articles/5036367557148-Where-can-I-buy-YubiKeys-
Comment Volvo pourrait-il intégrer les numéros de série dans la nouvelle solution AMF pour Tech Tool (TT) ?	Nous détaillons les étapes de l'intégration AMF. L'approche consisterait pour les utilisateurs à s'inscrire à l'AMF. Sur la base de l'option, les utilisateurs seront guidés à travers les étapes d'enregistrement de la clé de sécurité (c'est-à-dire que YubiKey est une marque d'appareil). Note: - Une clé de sécurité par ordinateur portable (pas par personne). - Le nombre d'utilisateurs par clé de sécurité est limité à 25 utilisateurs (si vous utilisez des clés biométriques, la limite est de 5 utilisateurs) - Les clés de sécurité ne sont pas liées à un emplacement ou à un appareil spécifique. Les utilisateurs individuels et les ID de boutique peuvent être ajoutés et supprimés aux clés selon les besoins.
L'enregistrement de l'appareil est-il effectué comme première étape de l'activation pour pouvoir utiliser la clé ou lorsque les techniciens tenteraient pour la première fois de l'utiliser pour Tech Tool ?	La première étape du processus est l'intégration de l'AMF. La deuxième étape consiste à publier le logiciel TT prêt pour l'authentification multifacteur en août. Indiquez que les utilisateurs pourront utiliser AMF pour TT.

Une adresse e-mail d'entreprise unique est-elle obligatoire ?	Une adresse e-mail unique est fortement préférée selon les normes d'AMF.
Qu'en est-il des petits concessionnaires qui n'ont pas leur propre domaine?	Une adresse e-mail d'entreprise est fortement préférée mais pas obligatoire.
Pourquoi deux méthodes d'AMF sont-elles nécessaires ?	Deux méthodes d'AMF sont requises pour que chaque utilisateur puisse accéder aux applications Volvo. Disposer d'une méthode d'AMF de sauvegarde dans le cas où une réinitialisation du mot de passe est requise pour une récupération plus rapide en cas de perte de la clé de sécurité.
Sera-t-il possible pour 1 utilisateur de se connecter à 2 Tech Tools en même temps ?	Oui.
Quels sont les délais que nous devons avoir sur notre radar concernant le déploiement de l'AMF?	Le 23 novembre, 2023.
Où puis-je trouver plus d'informations sur l'application Microsoft Authenticator ?	https://support.microsoft.com/en-us/account-billing/download-and-install-the-microsoft-authenticator-app-351498fc-850a-45da-b7b6-27e523b8702a
Qui signaler les problèmes d'autorisation lors de la connexion d'AMF?	Contactez votre bureau d'assistance de première ligne respectif et ils auront des processus en place pour vous obtenir le soutien nécessaire pour remédier à l'issue.
Quelles sont les spécifications requises pour la clé ?	https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-passwordless#fido2-security-keys
Qu'en est-il des applications locales (concessionnaires) susceptibles d'être connectées aux systèmes du groupe Volvo ?	À terme, toutes les applications du groupe Volvo utiliseront l'authentification multifacteur.
Les revendeurs à double marque (MACK/VCE), dans deux domaines d'activité différents, auront 2 identifiants de connexion (UserID) mais seulement 1 e-mail. L'authentification multifacteur fonctionne-t-elle pour chaque connexion ?	L'authentification multifacteur est configurée pour chaque compte. L'approche multifactorielle pour les concessionnaires à double marque est toujours en cours d'examen et le cas d'utilisation n'a pas été approuvé.

Étape 2 : Inscription AMF (méthode d'installation d'AMF)	
Question	**Answer**
Quand puis-je commencer à configurer mes méthodes d'AMF ?	Dès que possible! Visitez https://myaccount.microsoft.com et connectez-vous à votre compte Microsoft Azure à l'aide de votre UPN (12345@ext.volvogroup.com) pour configurer vos méthodes d'AMF.
Quelles sont les applications d'authentification prises en charge ?	Application Microsoft Authenticator. Configuration requise pour le système d'exploitation de l'application Authenticator : Android - v8.0 ou version ultérieure IOS - v14.0 ou version ultérieure IPad OS – 14.0 ou version ultérieure
Prenez-vous en charge une autre application d'authentification ?	Volvo Group recommande l'application Microsoft Authenticator pour vérifier que Multi-Factor Authentication est configuré. Si vous préférez utiliser d'autres applications fournisseur, veuillez suivre les instructions fournies par le fournisseur.
Peut-on utiliser le même numéro de téléphone pour plusieurs utilisateurs ?	Le groupe Volvo recommande d'utiliser un téléphone dédié à chaque utilisateur afin d'éviter les problèmes de sécurité potentiels.
Comment l'appel téléphonique fonctionnera-t-il avec un système téléphonique automatisé? Un numéro de composition directe sera-t-il nécessaire?	Volvo utilise un système automisé.
Quelle est la solution de repli si un appel téléphonique devait échouer? (c.-à-d. que l'utilisateur change de numéro de téléphone)	Volvo recommande de sélectionner la méthode d'AMF principale et de secours pendant le processus de configuration de l'authentification multifacteur.
Où allions-nous pour mettre à jour le numéro de téléphone d'un utilisateur?	Options de connexion MFA Mes connexions | Informations sur la sécurité | Microsoft.com permet à une personne de modifier les options et le numéro de téléphone.
Combien de temps faut-il pour qu'un numéro de téléphone soit mis à jour s'il a été modifié?	Les mises à jour se font en temps réel.

L’e-mail est-il une option de méthode d’AMF ?	Non, le courrier électronique n’est pas une option d’AMF disponible car ce n’est pas un moyen sécurisé de fournir une authentification multifacteur. L’adresse e-mail est requise pour AMF et MS prend en charge la réinitialisation du mot de passe en utilisant l’e-mail comme identifiant, mais l’e-mail n’est pas un moyen sécurisé de fournir une validation d'AMF.

Étape 3 : Application de l'authentification multifacteur (connexion Microsoft Azure)	
Question	**Answer**
Que se passe-t-il lorsqu'un utilisateur se connecte à l'aide d'Azure AD ?	**Scénario 1 - L'utilisateur se connecte pour la première fois avec un mot de passe qui n'est pas conforme à la stratégie de mot de passe:** Si un nouvel utilisateur est créé, le mot de passe doit toujours être conforme à la stratégie de mot de passe. Le seul cas où un utilisateur peut se connecter avec un format de mot de passe « non valide » est s'il a été créé avant l'application de la stratégie de mot de passe. **Scénario 2 – Pour les mots de passe utilisateur non expirés:** Lorsqu'un mot de passe n'arrive pas à expiration, la stratégie de mot de passe n'est pas déclenchée. L'utilisateur ne recevra aucune notification pour changer le mot de passe. **Scénario 3 – Connexions Azure identifiées comme « à haut risque »:** La réinitialisation du mot de passe peut être demandée pour les utilisateurs à haut risque conformément à la stratégie d'accès conditionnel Azure AD. Un exemple : si un ID utilisateur / login est actif dans l'Amérique du Nord et qu'une connexion est tentée en France une heure plus tard, cette activité est signalée comme présentant un risque élevé par Azure et une erreur sera envoyée lors de la connexion.