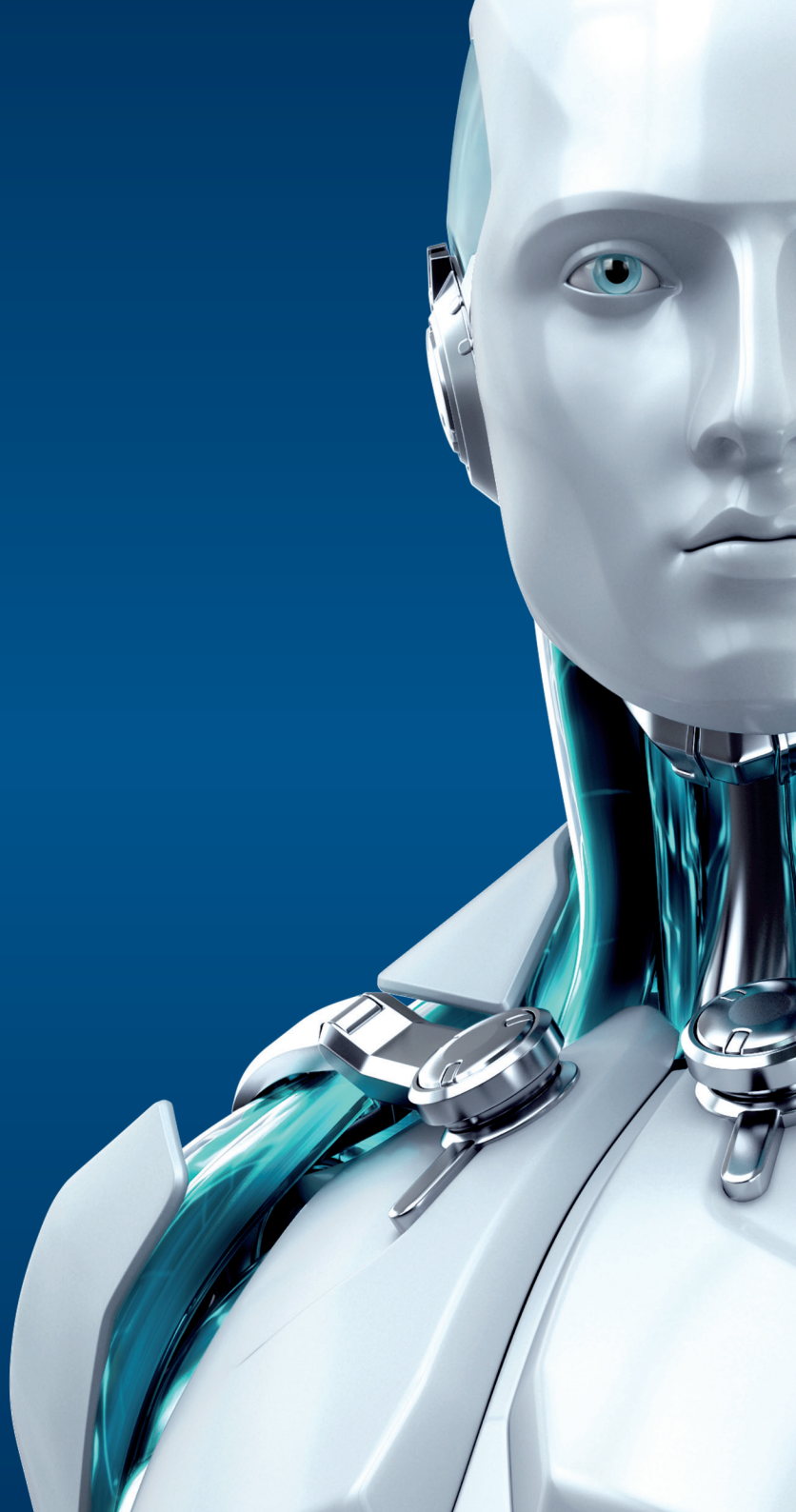
SECURE AUTHENTICATION

ENJOY SAFER TECHNOLOGY™



SECURE AUTHENTICATION

ESET Secure Authentication est une solution d'authentification à deux facteurs, basée sur mobile, qui offre une sécurité supplémentaire pour accéder au réseau de l'entreprise, ainsi qu'à ses données sensibles, et ce en toute simplicité.

La solution est constituée d'un produit déployé sur le server et d'une application mobile installée sur le smartphone. Adaptez la solution à vos besoins grâce aux options d'authentification : notification push, génération d'un mot de passe à usage unique via l'application, SMS, token.

Authentification ultra-puissante pour protéger les accès au réseau et aux données

Vous pouvez utiliser ESET Secure Authentication pour protéger :

- Vos accès VPN
- Remote Desktop Protocol
- L'authentification des postes de travail (ouverture des sessions)
- Services Web/Cloud via Microsoft ADFS 3.0, comme Office 365 et Google Apps
- Les applications Microsoft Web, telles que Outlook Web Access (OWA)
- Exchange Control Panel 2010 & Exchange Administrator Center 2013
- VMware Horizon View
- Services basés sur RADIUS

ESET Secure Authentication est également disponible en API pour s'intégrer avec votre authentification existante basée sur Active Directory, ainsi qu'en SDK pour une intégration simplifiée dans n'importe quel logiciel métier.

Avantages pour l'entreprise

- Aide à prévenir le risque de failles avec des mots de passe uniques pour chaque accès
- Protège contre les mots de passes faibles
- Flexibilité pour définir le mode de distribution du mot de passe à usage unique (ex : votre propre passerelle SMS)
- Economique – Aucun matériel supplémentaire nécessaire
- Facilité de migration et d'utilisation
- Compatible avec les tokens existants pour répondre aux exigences de conformité
- Authentification à deux facteurs pour vos applications Cloud, telles que Office 365 ou Google App

Avantages IT

- API / SDK pour une intégration simple avec des applications et systèmes personnalisés
- L'application fonctionne sans connexion internet (une fois téléchargée)
- Fonctionne avec une large gamme de VPN
- Compatible avec la plupart des systèmes d'exploitation mobiles
- Support technique en français
- Solution innovante
- Augmente la productivité et réduit les plaintes utilisateurs lors de l'accès à des sites de confiance, grâce à la liste blanche IP
- Outils de déploiement et configuration dans un vaste environnement utilisateur

Fiche technique

Authentification à deux facteurs	Basée sur mobile, authentification à deux facteurs avec mot de passe à usage unique pour un niveau de sécurité supérieur
	Compatible avec un large éventail de plateformes (voir les plateformes compatibles)
	Solution logicielle – pas besoin de transporter un appareil ou token supplémentaire
	Pratique pour les employés mobiles
	Compatible avec les tokens
Côté client (application mobile)	Installation directe, interface utilisateur simple et efficace
	Livraison du mot de passe à usage unique via l'application client, SMS ou token
	La génération du mot de passe à usage unique s'effectue indépendamment d'une connexion Internet
	Compatible avec tous les téléphones pouvant recevoir des SMS
	Compatible avec la majorité des systèmes d'exploitation
	Accès protégé par PIN pour prévenir la fraude en cas de vol ou perte de l'appareil
	Sert plusieurs zones de mots de passe à usage unique, ex : accès OWA, VPN et autres
	Application disponible en français
Méthodes d'authentification	Application mobile – génération de mots de passe à usage unique (OTP), aucune connexion Internet requise
	Notification push – authentification en un clic via son smartphone (nécessite l'utilisation de l'application mobile, compatibilité Android)
	SMS – réception de mots de passe à usage unique par SMS
	Tokens – la solution ne nécessite pas de token physique pour fonctionner mais est compatible avec les token OATH
	Méthodes personnalisées – Exemple : email
Côté serveur	Solution innovante
	Installation et configuration simple, en quelques clics seulement
	L'installeur reconnait automatiquement le système d'exploitation, et sélectionne tous les composants correspondants
	Installeur interactif, installation dans ADFS
Options d'intégration personnalisées	Dans l'environnement Active Directory, utilisez l'API ESET Secure Authentication ou l'API User Management pour une intégration facilitée dans les systèmes personnalisés
	Le SDK permet l'intégration pour les non-utilisateurs d'Active Directory
Administration à distance	Compatibilité Microsoft Management console (MMC)
	Intégration via l'Active Directory
	ESET Secure Authentication étend l'Active Directory (plugin ADUC) avec des fonctionnalités supplémentaires pour permettre la gestion des paramètres de l'authentification à deux facteurs des utilisateurs

Plateformes compatibles

Si vous souhaitez accéder aux prérequis techniques détaillés, veuillez consulter le manuel ESET Secure Authentication disponible sur : http://download.eset.com/manuals/eset_esa_product_manual_enu.pdf

Plateformes de connexion à distance	**Remote Desktop Protocol** **Protection VPN :** Barracuda, Cisco ASA, Citrix Access Gateway, Citrix NetScaler, Check Point Software, Cyberoam, F5 FirePass, Fortinet FortiGate, Juniper, Palo Alto, SonicWall	
Protection authentification locale (Windows)	Windows 7 et supérieur	Windows Server 2008 R2 et supérieur
Active Directory Federation Services	Microsoft ADFS 3.0 (Windows Server 2012 R2)	
Plateformes VDI compatibles	VMware Horizon View	Citrix XenApp
Microsoft Web Applications	Microsoft Web Applications Outlook Web Access Microsoft Exchange 2010 Outlook Web App Exchange Control Panel Microsoft Exchange 2013 Outlook Web App Exchange Admin Center	Microsoft Dynamics CRM 2011, 2013, 2015 Microsoft SharePoint 2010, 2013 Microsoft Remote Desktop Web Access Microsoft Terminal Services Web Access Microsoft Remote Web Access
Intégration personnalisée	ESET Secure Authentication s'intègre facilement avec vos services basés sur RADIUS, via l'API ESET Secure Authentication ou l'API User Management dans votre authentification basée sur Active Directory. Les non-clients d'Active Directory ayant des systèmes personnalisés peuvent utiliser le SDK simple à déployer.	
Systèmes d'exploitation (Côté serveur)	Windows Server 2003(32&64bit), 2003 R2 (32&64bit), 2008 (32&64bit), 2008 R2, 2012, 2012 R2 Windows Small Business Server 2008, 2011 Windows Server 2012 Essentials, 2012 R2 Essentials Les outils de gestion sont également compatibles avec les systèmes d'exploitation client à partir de Windows XP SP3 dans les versions 32-bit et 64-bit.	
Systèmes d'exploitation mobiles (Application côté client)	iOS 4.3 ou supérieur (iPhone) Android 2.1 ou supérieur Windows Phone 7 ou supérieur Windows Mobile 6	BlackBerry 4.3 à 7.1, 10 ou supérieur Symbian – compatible J2ME Tous les appareils compatibles J2ME