



STORMSHIELD



GUIDE

**STORMSHIELD ENDPOINT SECURITY
EVOLUTION**

GUIDE DE DÉPLOIEMENT SAAS

Version 2.6.2

Dernière mise à jour du document : 11 septembre 2024

Référence : ses-fr-guide_de_déploiement_saas



Table des matières

1. Avant de commencer	3
2. Comprendre l'architecture	4
3. Configurer SES Evolution pour gérer plusieurs tenants	5
3.1 Prérequis	5
3.2 Créer les comptes locaux	5
3.3 Installer la console d'administration pour le premier tenant	6
3.4 Déclarer la console d'administration pour les tenants supplémentaires	7
3.5 Connaître les bonnes pratiques	7
3.6 Utiliser la console d'administration	7
3.7 Mettre à jour la console d'administration	8
3.8 Désinstaller la console d'administration	8
4. Pour aller plus loin	9

Dans la documentation, Stormshield Endpoint Security Evolution est désigné sous la forme abrégée : SES Evolution.



1. Avant de commencer

Bienvenue dans le guide de déploiement SaaS de Stormshield Endpoint Security Evolution.

Ce document contient des informations techniques propres à la version SaaS du produit et s'adresse aux fournisseurs de gestion de services de sécurité, aussi appelés MSSP (Managed Security Service Provider).

La solution de sécurité SES Evolution offre aux organisations de toutes tailles une protection complète des postes de travail des utilisateurs et des serveurs. Installé sur les postes de travail et les serveurs de vos clients, l'agent SES Evolution les protège des attaques connues et inconnues, ainsi que des intrusions, de façon transparente pour les utilisateurs.

En tant que MSSP, vous paramétrez les agents à partir d'une console d'administration et vous gérez le backoffice SES Evolution de chacun de vos clients.

La console d'administration vous permet de configurer les politiques de sécurité et également de consulter les logs des événements remontés par les postes de travail et serveurs afin d'en surveiller le fonctionnement.

SES Evolution dispose également d'une API REST publique. Par défaut, elle n'est pas activée. Pour plus d'informations sur l'API publique, reportez-vous à la section [Activer et gérer l'API publique de SES Evolution](#).

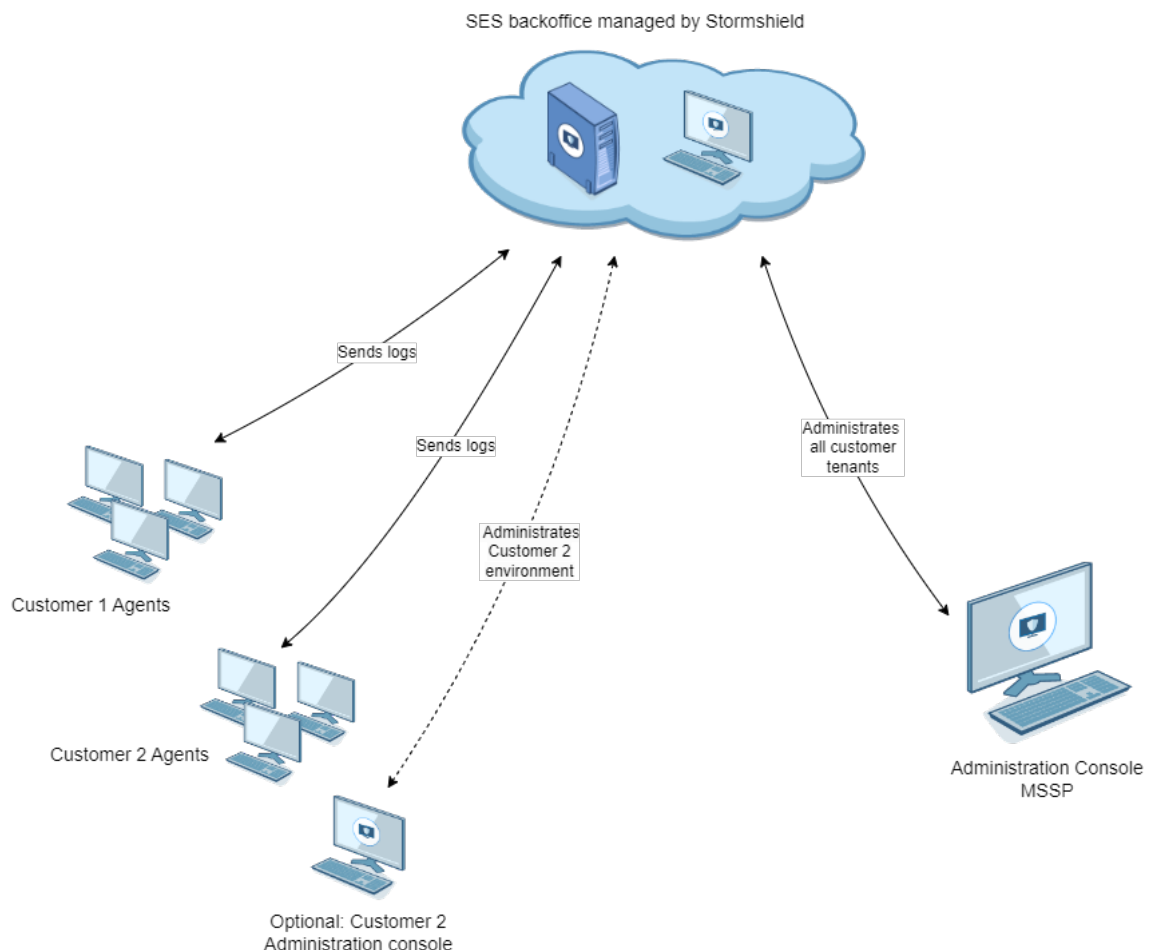


2. Comprendre l'architecture

Le schéma ci-dessous indique les principales connexions entre les différents composants de l'architecture de SES Evolution en mode SaaS :

- Stormshield gère et contrôle les backoffices de SES Evolution pour les clients finaux. L'ensemble des composants backoffice dédiés à un client est nommé un *tenant*. Notre service *Cloud Services* administre les machines grâce à des comptes spécifiques.
- Le MSSP dispose d'un poste de travail sur lequel la console d'administration SES Evolution est installée. Depuis ce poste, il se connecte au tenant de chacun de ses clients de manière distincte pour effectuer les tâches quotidiennes d'administration et de supervision de la solution SES Evolution.
- Chaque client récupère ses logs et sa politique de sécurité SES Evolution. Il peut optionnellement disposer d'une console d'administration pour se connecter à son propre tenant.

Tous les flux ci-dessous utilisent le port TCP 443.





3. Configurer SES Evolution pour gérer plusieurs tenants

En tant que MSSP, vous assurez l'administration et la surveillance du parc d'agents SES Evolution pour plusieurs clients. À partir d'un même poste de travail, vous pouvez vous connecter à l'un ou l'autre des tenants clients via la console d'administration SES Evolution. Pour cela, vous devez créer des comptes locaux sur votre poste, puis installer la console d'administration pour un premier tenant, et enfin déclarer la console pour les tenants supplémentaires.

3.1 Prérequis

Pour chacun des tenants que vous administrez, vous devez disposer des éléments suivants envoyés par e-mail par Stormshield :

- L'identifiant et le mot de passe du ou des comptes créés par Stormshield pour vos tenants,
- Le nom DNS public du backend SES Evolution pour vos tenants,
- L'URL du portail d'authentification Stormshield sur lequel se connecter pour accéder à vos tenants.

3.2 Créer les comptes locaux

1. Dans votre infrastructure, sur le poste de travail sur lequel vous souhaitez installer la console d'administration SES Evolution, créez les comptes locaux correspondant à ceux transmis par Stormshield. Utilisez le mot de passe et la politique de mot de passe transmis par Stormshield.

Il peut y avoir deux types de comptes. Les noms de comptes ci-dessous sont des exemples :

- *Admin* : Utilisé pour exécuter le Centre d'installation SES Evolution et déclarer les nouvelles instances de la console d'administration. Il existe un seul compte *Admin* pour tous vos tenants.
- *Prénom.Nom* (optionnel) : Utilisé pour exécuter la console d'administration afin d'effectuer les tâches quotidiennes d'administration du parc. Il existe autant de comptes *Prénom.Nom* que d'administrateurs de la console.

Si vous disposez d'un seul compte (*Admin*), celui-ci sera utilisé à la fois pour l'installation de la console et pour les tâches quotidiennes. Stormshield recommande toutefois d'utiliser un compte *Prénom.Nom* pour chaque administrateur de SES Evolution.



2. Ajoutez le compte *Admin* aux administrateurs locaux du système en utilisant la commande `lusrmgr.msc` ou la ligne de commande suivante :

```
$BuiltinUsersSid =  
[System.Security.Principal.SecurityIdentifier]::new  
([System.Security.Principal.WellKnownSidType]::BuiltinUsersSid,  
$null)  
  
$BuiltinAdminsSid =  
[System.Security.Principal.SecurityIdentifier]::new  
([System.Security.Principal.WellKnownSidType]::BuiltinAdministrato  
rsSid, $null)  
  
New-LocalUser -UserMayNotChangePassword -AccountNeverExpires -  
PasswordNeverExpires -Name "Admin" -Description "Console Admin" -  
FullName "Admin" -Password (Read-Host -AsSecureString)  
  
# (saisir le mot de passe d'Admin ici)  
  
Add-LocalGroupMember -Sid $BuiltinUsersSid -Member Admin  
Add-LocalGroupMember -Sid $BuiltinAdminsSid -Member Admin
```

3.3 Installer la console d'administration pour le premier tenant

1. Sur le même poste de travail, exécutez le fichier `SES_Evolution_Installation_Center_vxxx.exe` en tant qu'utilisateur *Admin*.
- ou -
Si le poste se trouve sur un domaine, exécutez la commande suivante :
`SES_Evolution_Installation_Center_vxxx.exe -NoDomainCheck.`
2. Sélectionnez **Ajouter un nouveau composant à une installation existante**, puis **Console**.
3. Renseignez le nom DNS du backend fourni par Stormshield.
La console s'installe et un raccourci est créé sur le Bureau public de Windows.
4. Ouvrez la console en tant qu'*Admin* pour vérifier la bonne connexion au backend.
5. Dans le panneau **Utilisateurs > Utilisateurs et groupes**, vérifiez que vos comptes *Prénom.Nom* pour ce tenant sont déclarés et disposent d'un rôle.
6. Renommez le raccourci sur le Bureau Windows pour identifier ce premier tenant.

Dans la suite de ce document, on appelle l'environnement du client 1 l'environnement primaire.



3.4 Déclarer la console d'administration pour les tenants supplémentaires

1. Sur le même poste de travail, lancez une invite de commande en tant qu'utilisateur *Admin* et exécutez la commande suivante :

```
EsInstaller.exe -NoDomainCheck -RegisterConsole -BackendAddress  
<Tenant2_Backend_DNS_Name> -ShortcutPath  
"C:\Users\Public\Desktop\SES Evolution Console - Tenant2.lnk".
```

où :

Paramètre	Description
-NoDomainCheck	À utiliser uniquement si la machine appartient à un domaine Active Directory.
-RegisterConsole	Permet d'enregistrer une nouvelle console liée à une autre backend SES Evolution.
-BackendAddress	Spécifie le nom DNS public du backend du tenant supplémentaire.
-ShortcutPath	Indique le chemin et le nom du raccourci sur le Bureau public de Windows.

Après une dizaine de secondes, un nouveau raccourci de la console s'affiche sur le Bureau public de Windows. Si ce n'est pas le cas, consultez les logs du centre d'installation dans *AppData/Local/Temp*, ou les logs du backend sur le deuxième tenant. Pour plus d'informations, reportez-vous [au Guide d'administration](#).

2. En utilisant le nouveau raccourci, ouvrez la console en tant qu'*Admin* pour vérifier la bonne connexion au backend.
3. Dans le panneau **Utilisateurs > Utilisateurs et groupes**, vérifiez que vos comptes *Prénom.Nom* pour ce tenant sont déclarés et disposent d'un rôle.
4. Répétez cette procédure pour tous les tenants supplémentaires que vous souhaitez administrer.
5. (Optionnel) Après cette procédure, Stormshield recommande de désactiver le compte *Admin* afin de ne pas laisser de compte privilégié non utilisé sur votre poste. Vous pourrez le réactiver si vous devez installer une console pour un nouveau tenant.

Dans la suite de ce document, on appelle l'environnement des clients supplémentaires les environnements secondaires.

3.5 Connaître les bonnes pratiques

- Si vous ajoutez ou supprimez des utilisateurs SES Evolution dans la console d'administration, informez-en l'équipe Cloud Services de Stormshield afin qu'ils soient ajoutés ou supprimés également sur le tenant.
- Ne changez pas le mot de passe des comptes Windows locaux utilisés pour se connecter à SES Evolution sans en informer l'équipe Cloud Services de Stormshield au préalable. En effet le mot de passe doit être modifié également sur le tenant.
- Avant de déployer des changements sur le parc d'un client, assurez-vous de bien le faire depuis la console d'administration liée au tenant de ce client.

3.6 Utiliser la console d'administration

L'utilisation de la console d'administration est détaillée dans le [Guide d'administration](#) .



3.7 Mettre à jour la console d'administration

Lorsque vous en recevez la notification, mettez à jour la console d'administration SES Evolution de la façon suivante afin de synchroniser sa version avec le backend :

- Démarrez la console **de l'environnement primaire**.
Elle sera mise à jour automatiquement et permettra également le bon fonctionnement des environnements secondaires.

3.8 Désinstaller la console d'administration

Pour désinstaller la console d'administration lorsqu'elle est configurée avec plusieurs tenants, ouvrez un ticket au support technique Stormshield qui vous accompagnera sur ce sujet.



4. Pour aller plus loin

Des informations complémentaires et réponses à vos éventuelles questions sur SES Evolution sont disponibles sur le site web [Documentation](#) et dans la [base de connaissances Stormshield](#) [authentification nécessaire].



STORMSHIELD

documentation@stormshield.eu

Les images de ce document ne sont pas contractuelles, l'aspect des produits présentés peut éventuellement varier.

Copyright © Stormshield 2024. Tous droits réservés. Tous les autres produits et sociétés cités dans ce document sont des marques ou des marques déposées de leur détenteur respectif.