

PROCÉDURE DE MIGRATION

Migrer ESET PROTECT On-Premise
vers ESET PROTECT Cloud

PUBLIC

Document Version 1.0
13 Septembre 2024
Auteur: Romain Ravon

Table des matières

1 - Introduction	3
2 - Recommandations.....	3
3 - Liens utiles	3
4 - Procédure de migration en 10 étapes détaillées	4
4.1 - Créer une nouvelle instance ESET PROTECT.....	4
4.1.1 - Dans le cas où vous utilisez ESET Business Account	4
4.1.2 - Dans le cas où vous utilisez ESET MSP Administrator.....	5
4.2 - Migrer les politiques de ESET PROTECT On-Prem vers ESET PROTECT	6
4.3 - Migrer des modèles de groupe dynamique de ESET PROTECT On-Prem vers ESET PROTECT	8
4.4 - Migrer les modèles de rapport de ESET PROTECT On-Prem vers ESET PROTECT	9
4.5 - Migrer la structure des groupes statiques vers ESET PROTECT.....	11
4.5.1 - Exporter la structure des groupes statiques depuis ESET PROTECT On-Prem	11
4.5.2 - Importer la structure des groupes statiques dans ESET PROTECT	12
4.6 - Migrer les ordinateurs gérés (Management Agents) à l'aide de la politique de migration	12
4.7 - Migration des périphériques mobiles.....	16
4.8 - Configurer les utilisateurs ESET PROTECT	17
4.8.1 – Dans le cas où vous utilisez ESET Business Account.....	17
4.8.2 – Dans le cas où vous utilisez ESET MSP Administrator	20
4.9 - Ajouter les utilisateurs à la console web ESET PROTECT Web Console	22
4.9.1 – Dans le cas où vous utilisez ESET Business Account.....	22
4.9.2 – Dans le cas où vous utilisez ESET MSP Administrator	25
4.10 - Mettre hors service le serveur ESET PROTECT sur site.....	27
4.10.1 - Conserver le système d'exploitation de l'ordinateur serveur et le réutiliser	27
4.10.2 - Conserver l'ordinateur serveur	27

1 - Introduction

Ce document explique succinctement et simplement comment migrer un ou plusieurs postes de votre console ESET PROTECT On-Premise vers votre console ESET PROTECT Cloud. Vous trouverez dans ce document les variantes entre le processus via ESET Business Account et ESET MSP Administrator.

2 - Recommandations

- Les machines que vous souhaitez migrer doivent communiquer avec la console ESET PROTECT On- Premise.
- Nous conseillons de déchiffrer les appareils administrés chiffrés par ESET Full Disk Encryption (EFDE) avant la migration. Après la migration, vous pourrez chiffrer à nouveau les appareils nouvellement administrés à partir de la nouvelle console Cloud.
- Nous conseillons d'effectuer la migration sur un échantillon de postes dans un premier temps. Une fois cet échantillon remonté sur la nouvelle console, vous pouvez effectuer la procédure sur le reste des postes.

3 - Liens utiles

- La procédure de migration vers ESET PROTECT Cloud est détaillée sur notre site d'aide **help.eset.com** : https://help.eset.com/protect_cloud/fr-FR/cloud_migration.html
- Nous vous invitons à regarder la **vidéo-démo** ci-dessous sur laquelle nous effectuons la migration d'un poste d'une console On-Premise vers ESET PROTECT Cloud : https://www.youtube.com/watch?v=4Yu5J1TpV6k&list=PLTsLW998ww7ShNST07DPsIE1QFTFLXA_nx&index=3

4 - Procédure de migration en 10 étapes détaillées

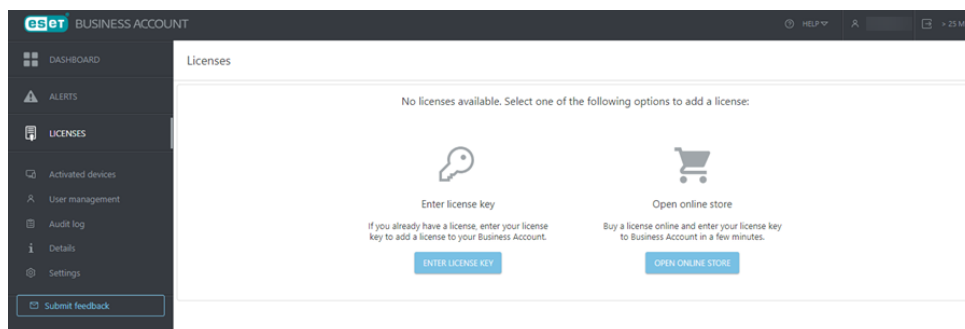
Ce document explique succinctement et simplement comment migrer un ou plusieurs postes de votre console ESET PROTECT On-Premise vers votre console ESET PROTECT Cloud.

4.1 - Créer une nouvelle instance ESET PROTECT

Vous devez dans un premier temps créer une nouvelle instance via ESET Business Account ou ESET MSP Administrator. Vous devez avoir un compte superutilisateur dans ESET Business Account ou ESET MSP Administrator ainsi qu'avoir une licence admissible pour ESET PROTECT.

4.1.1 - Dans le cas où vous utilisez ESET Business Account

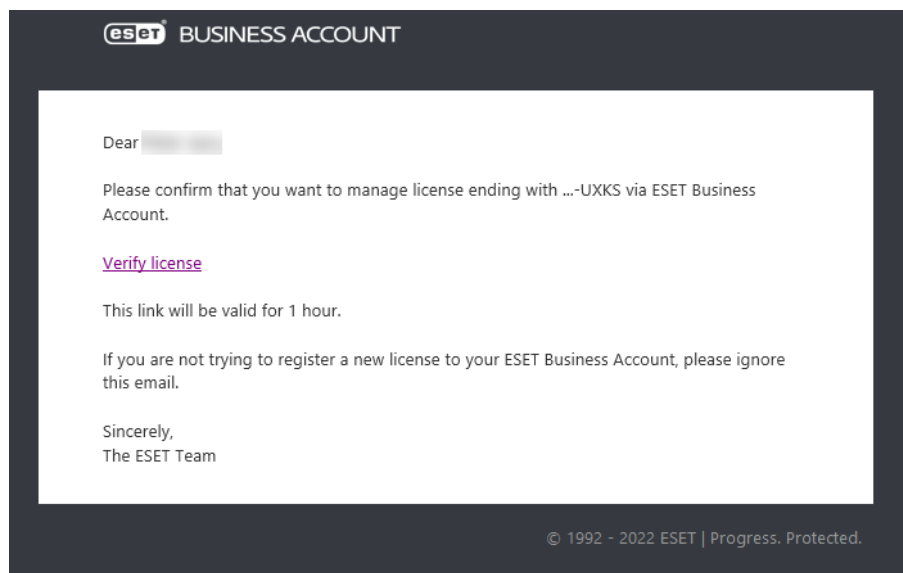
1. Ouvrez [EBA](#) et connectez-vous.
2. Cliquez sur Licences > Entrer la clé de licence



3. Dans la fenêtre **Ajouter une licence**, entrez votre **clé de licence** ESET PROTECT et cliquez sur **Ajouter une licence**.

The screenshot shows a modal dialog box titled 'Add License' with a close button (X) in the top right corner. The dialog contains the text: 'The License Key is in the confirmation email you received after buying it online. If you bought it in a store you can find the key on the license card.' Below this text is the label 'License key' followed by an information icon (i). Underneath is a text input field. At the bottom right of the dialog is a blue button labeled 'ADD LICENSE'.

4. Vous recevrez un courriel de vérification. Cliquez sur **Vérifier Licence**.



5. Dans le tableau de bord, cliquez sur Activer sous ESET PROTECT.
6. Une fenêtre Activer ESET PROTECT s'affiche. Lisez les conditions d'utilisation et cochez la case si vous les acceptez.
7. Sélectionnez un emplacement de centre de données pour votre instance ESET PROTECT la plus proche de l'emplacement de votre réseau géré et cliquez sur Continuer.
8. L'instance de votre ESET PROTECT sera créée. Vous pouvez attendre quelques minutes pour que la création se termine ou vous pouvez vous déconnecter et être averti par courriel lorsque l'instance de ESET PROTECT est disponible.
9. Cliquez sur Continuer. Vous pouvez également cliquer sur Tableau de bord, puis sur ouvrir dans la mosaïque ESET PROTECT pour ouvrir un nouvel onglet avec la Web Console de ESET PROTECT. ESET PROTECT synchronise la structure de votre ESET Business Account avec l'arborescence du groupe statique dans Ordinateurs dans la console Web.

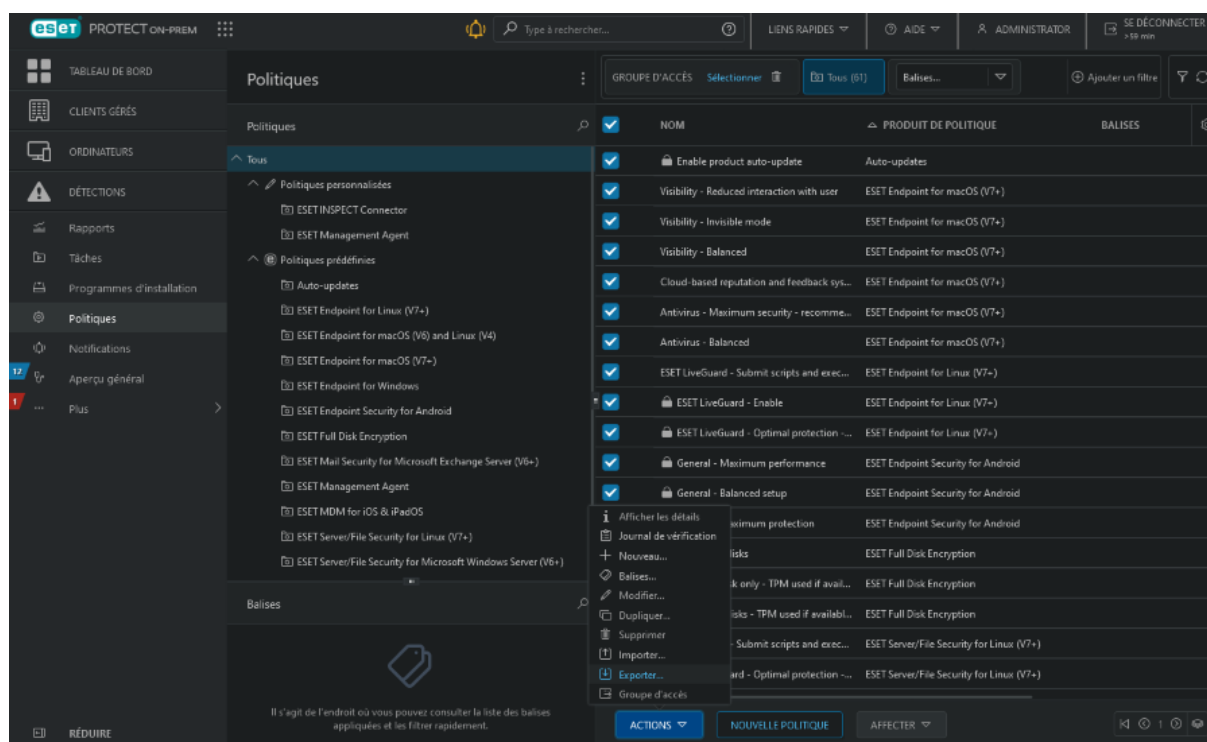
4.1.2 - Dans le cas où vous utilisez ESET MSP Administrator

1. Ouvrez [EMA](#) et connectez-vous.
2. Cliquez sur My company > Details
3. Dans les Produits disponibles, vérifiez que l'une des bundles éligibles est disponible. Si l'offre applicable ne figure pas dans la liste, demandez à votre responsable MSP de l'ajouter pour vous.
4. Cliquez ensuite sur Companies.
5. Sélectionnez un client
6. Cliquez sur Licences et sélectionnez Ajouter une licence
7. Sélectionnez l'un des ensembles de licences éligibles, saisissez le nombre d'unités et cliquez sur Ajouter.

8. Après avoir acheté une licence éligible, accédez au tableau de bord EMA 2. Recherchez l'encart ESET PROTECT et cliquez sur Activer.
9. Si plusieurs centres de données sont disponibles, sélectionnez-en un. Cochez la case J'accepte l'accord et cliquez sur Activer.
10. Lorsque l'instance ESET PROTECT est prête, ouvrez la console Web.

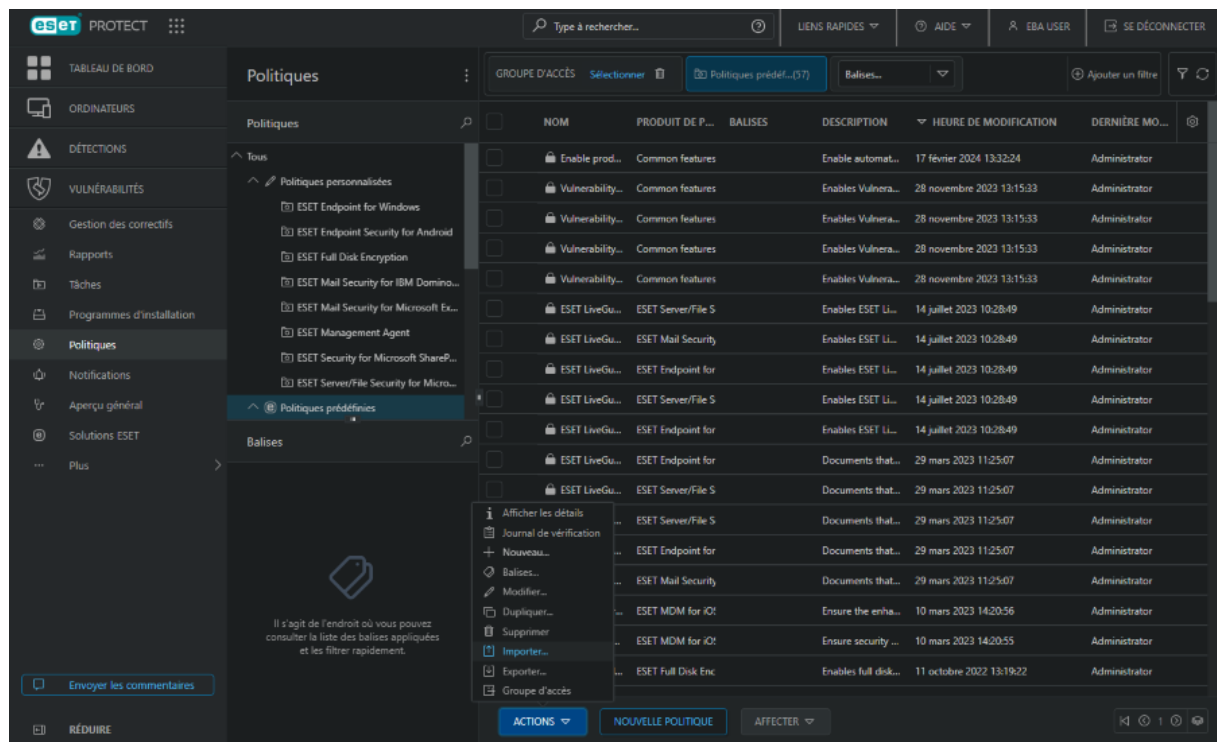
4.2 - Migrer les politiques de ESET PROTECT On-Prem vers ESET PROTECT

1. Connectez-vous à votre ESET PROTECT On-Prem.
2. Dans votre ESET PROTECT On-Prem, sélectionnez Politiques > Tous > cochez la case dans l'en-tête du tableau (ou cochez les cases en regard des politiques que vous souhaitez exporter) et cliquez sur Actions > Exporter.



3. Enregistrez le fichier .dat avec la liste des politiques.

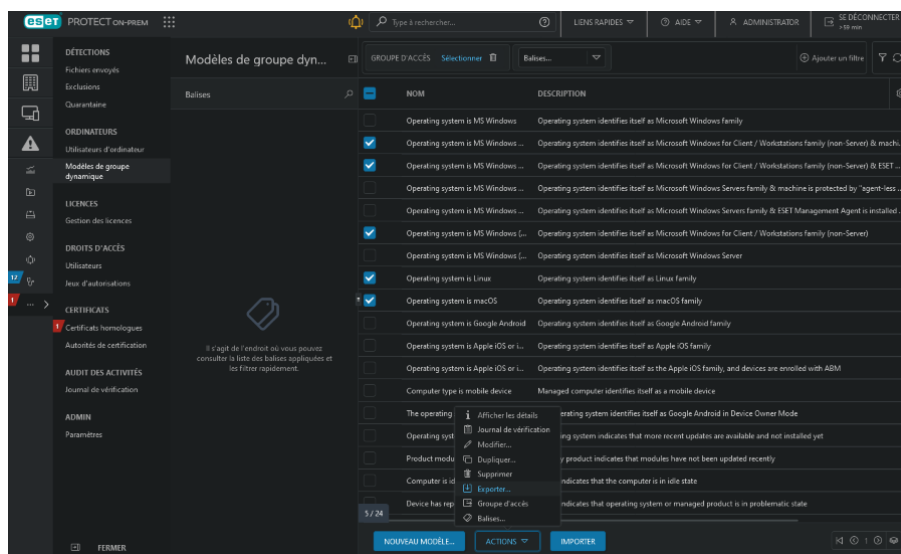
4. Dans ESET PROTECT, cliquez sur Politiques > Actions > Importer et sélectionnez le fichier .dat contenant la liste des politiques exportée à partir de ESET PROTECT On-Prem à l'étape 2, puis cliquez sur Importer pour les importer dans ESET PROTECT.



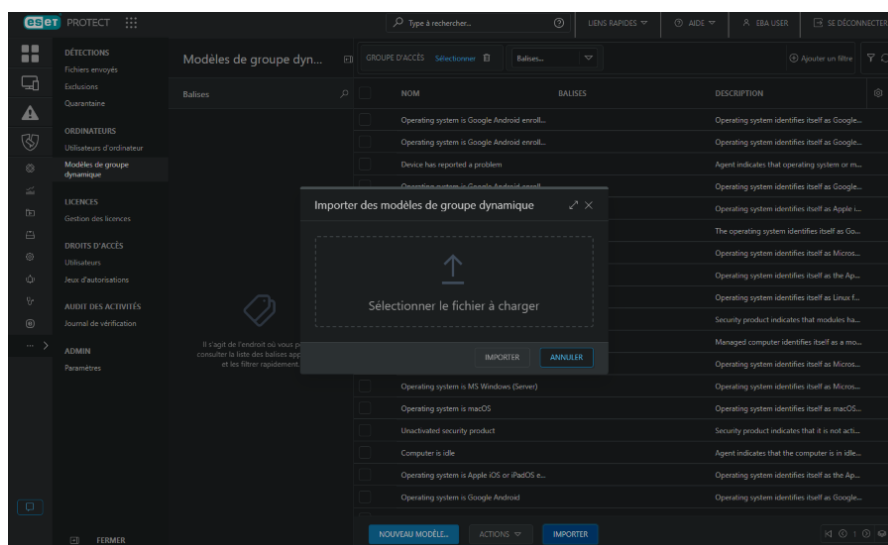
5. Les politiques importées seront affichées sous **Politiques personnalisées**. Après la migration des ordinateurs de ESET PROTECT On-Prem vers ESET PROTECT, les politiques qui ont été attribuées aux ordinateurs dans ESET PROTECT On-Prem ne seront pas conservées. Après avoir importé des politiques dans ESET PROTECT, vous pouvez les attribuer aux ordinateurs importés dans ESET PROTECT.

4.3 - Migrer des modèles de groupe dynamique de ESET PROTECT On-Prem vers ESET PROTECT

1. Dans votre ESET PROTECT On-Prem, sélectionnez Plus > Modèles de groupe dynamique.
2. Cochez les cases en regard des modèles de groupe dynamique que vous souhaitez exporter et cliquez sur Actions > Exporter



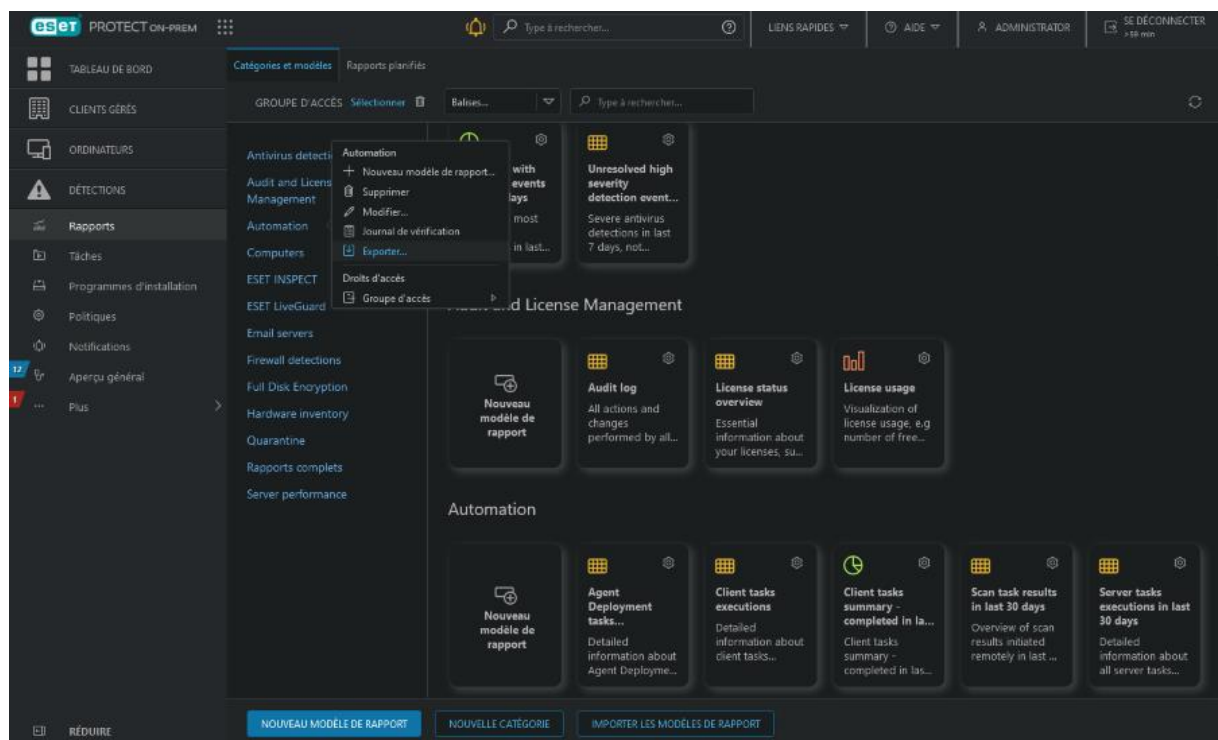
3. Enregistrez le fichier .dg avec les modèles de groupe dynamique exportés.
4. Dans ESET PROTECT, cliquez sur Plus > Modèles de groupe dynamique > Importer et sélectionnez le fichier .dg avec les modèles de groupe dynamique exportés à partir de ESET PROTECT On-Prem et cliquez sur Importer pour les importer dans ESET PROTECT



5. Les modèles de groupe dynamique importés apparaîtront dans la liste de tous les modèles de groupe dynamique et vous pouvez les utiliser pour créer des groupes dynamiques (vous ne pouvez pas migrer des groupes dynamiques).

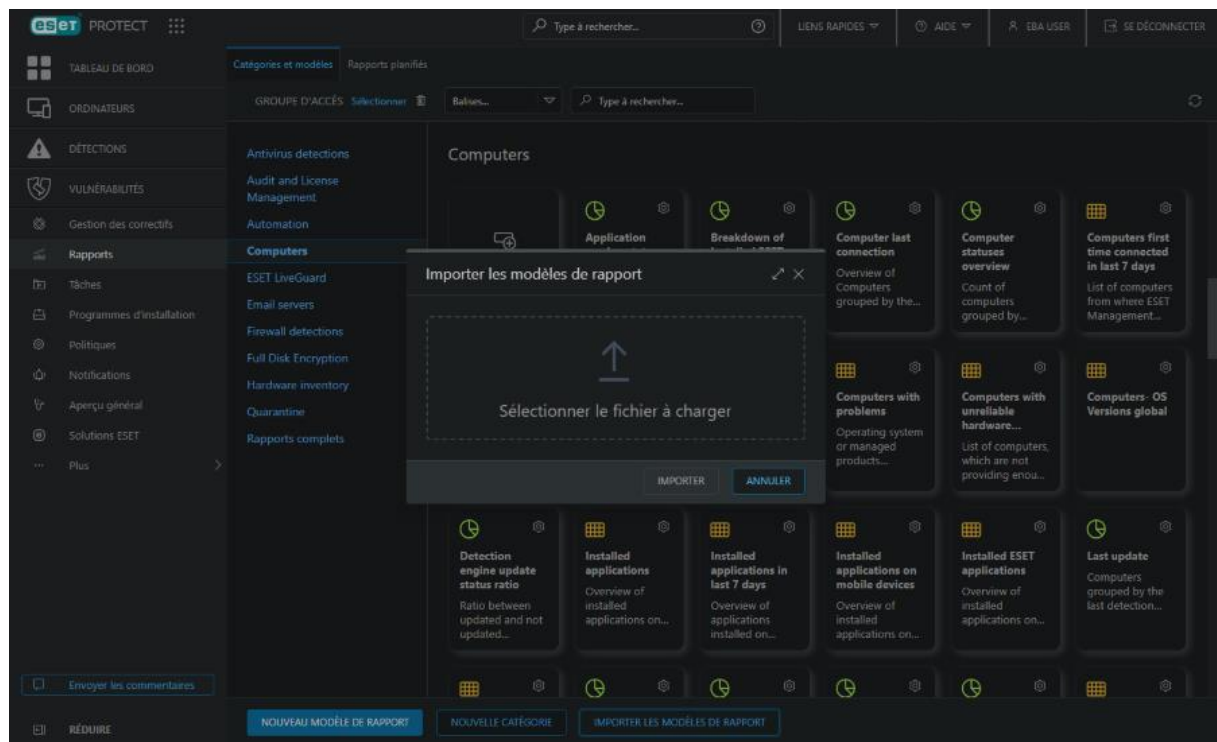
4.4 - Migrer les modèles de rapport de ESET PROTECT On-Prem vers ESET PROTECT

1. Dans votre ESET PROTECT On-Prem, sélectionnez Rapports.
2. Cliquez sur l'icône de l'engrenage en regard d'une catégorie de rapport ou d'un modèle de rapport individuel, puis cliquez sur **Exporter**.



3. Enregistrez le fichier .dat avec les modèles de rapport exportés.

4. Dans ESET PROTECT, cliquez sur **Rapports** > **Importer des modèles de rapport** et sélectionnez le fichier *.dat* avec les modèles de rapport exportés à partir de ESET PROTECT On-Prem et cliquez sur **Importer** pour les importer dans ESET PROTECT.



5. Les modèles de rapport importés apparaîtront dans **Rapports**. Vous pouvez utiliser les modèles de rapport pour planifier et générer des rapports.

4.5 - Migrer la structure des groupes statiques vers ESET PROTECT

Vous pouvez exporter la structure des groupes statiques (non-MSP ou MSP) depuis ESET PROTECT On-Prem. Vous pouvez ensuite importer la structure des groupes statiques dans ESET PROTECT.

4.5.1 - Exporter la structure des groupes statiques depuis ESET PROTECT On-Prem

4.5.1.1 - ESET PROTECT sur site 11.1 et versions ultérieures

6. Dans la ESET PROTECT On-Prem, cliquez sur Ordinateurs.
7. Cliquez sur l'icône d'engrenage en regard du groupe statique Tous, sélectionnez  Exporter vers le cloud, cliquez sur Oui pour exporter les ordinateurs à partir de sous-groupes.
8. Téléchargez et enregistrez le fichier .txt généré avec la structure des groupes statiques.
9. Vous pouvez également utiliser l'outil d'exportation d'ordinateurs décrit ci-dessous, dans la section pour les versions antérieures d'ESET PROTECT On-Prem.

4.5.1.2 - ESET PROTECT sur site 11.0 et versions antérieures

10. Téléchargez l'outil d'exportation d'ordinateurs sur l'ordinateur.
11. Décompressez le fichier computers_export_tool.zip téléchargé.
12. Ouvrez le dossier computers_export_tool dans la fenêtre d'invite de commandes Windows ou de terminal Linux.
13. Exécutez la commande suivante :
14. Windows : pythoncomputers_export_tool.py
Linux : python3 computers_export_tool.py
15. Dans Hostname, saisissez le nom d'hôte d'ESET PROTECT On-Prem et appuyez sur Enter. Si vous exécutez l'outil d'exportation d'ordinateurs sur ESET PROTECT Server, appuyez sur Enter pour utiliser la valeur par défaut localhost.
16. Dans Port, appuyez sur Enter si ESET PROTECT On-Prem utilise le port de console web par défaut (2223) ou saisissez le port de console web personnalisé et appuyez sur Enter.
17. Dans Username, saisissez le nom d'utilisateur de la console web et appuyez sur Enter.
18. Dans Password, saisissez le mot de passe de l'utilisateur de la console web (vous ne verrez pas les caractères saisis) et appuyez sur Enter.
19. L'outil génère un fichier computers.csv (situé dans le même dossier : computers_export_tool). Le fichier computers.csv contient la structure des groupes statiques ESET PROTECT On-Prem avec les noms d'ordinateur. Remarque : Si vous réexécutez l'outil, il remplace le fichier computers.csv.

4.5.2 - Importer la structure des groupes statiques dans ESET PROTECT

1. Dans la console web d'ESET PROTECT cloud, cliquez sur Ordinateurs > cliquez sur l'icône de l'engrenage en regard du groupe statique Tous > sélectionnez Importer.
2. Cliquez sur Sélectionner un fichier, sélectionnez le fichier exporté depuis ESET PROTECT On-Prem, puis cliquez sur Ouvrir.
3. Cliquez sur Importer. ESET PROTECT importera la structure des groupes statiques ESET PROTECT On-Prem. Vous pouvez fermer la fenêtre d'importation et continuer à utiliser ESET PROTECT.
4. Une fois l'importation terminée, la structure des groupes statiques avec les noms d'ordinateurs d'ESET PROTECT On-Prem apparaît dans la section Ordinateurs de la console web ESET PROTECT cloud. Passez aux étapes suivantes : utilisez la politique de migration pour migrer les ordinateurs gérés (ESET Management Agents).

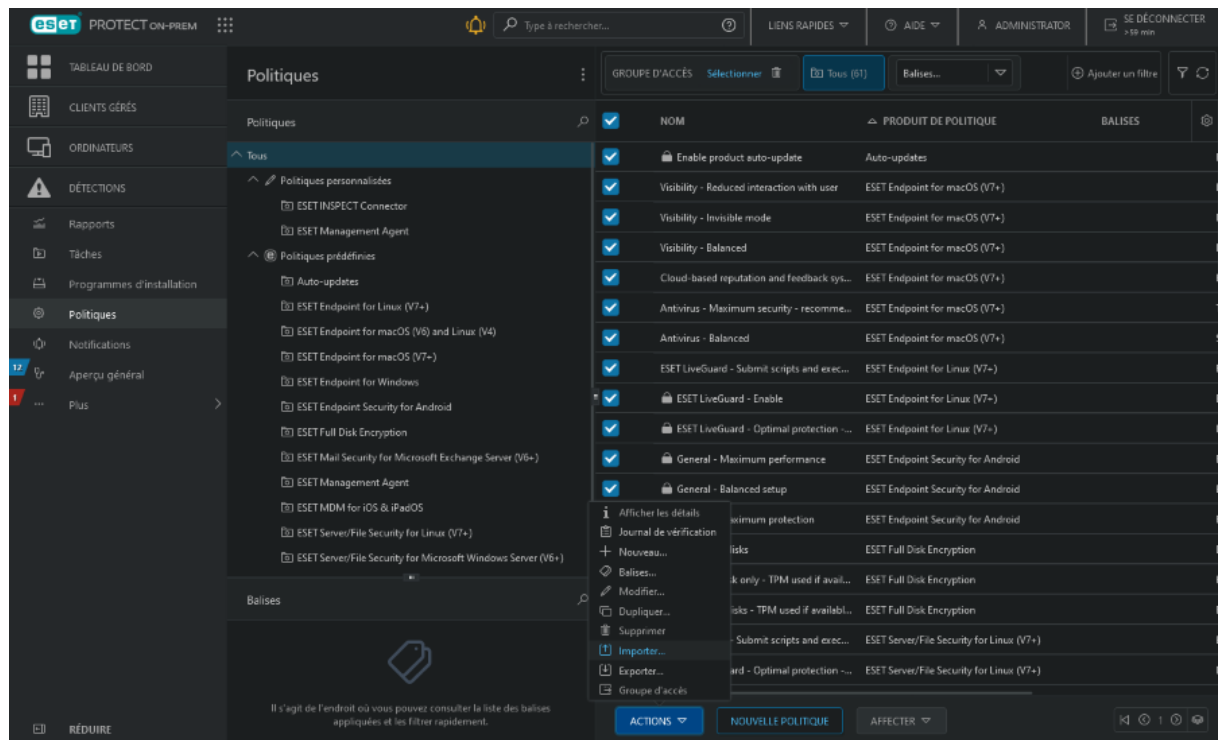
4.6 - Migrer les ordinateurs gérés (Management Agents) à l'aide de la politique de migration

1. Dans ESET PROTECT Web Console, cliquez sur Liens rapides > Télécharger la politique de migration et enregistrez le fichier .dat.

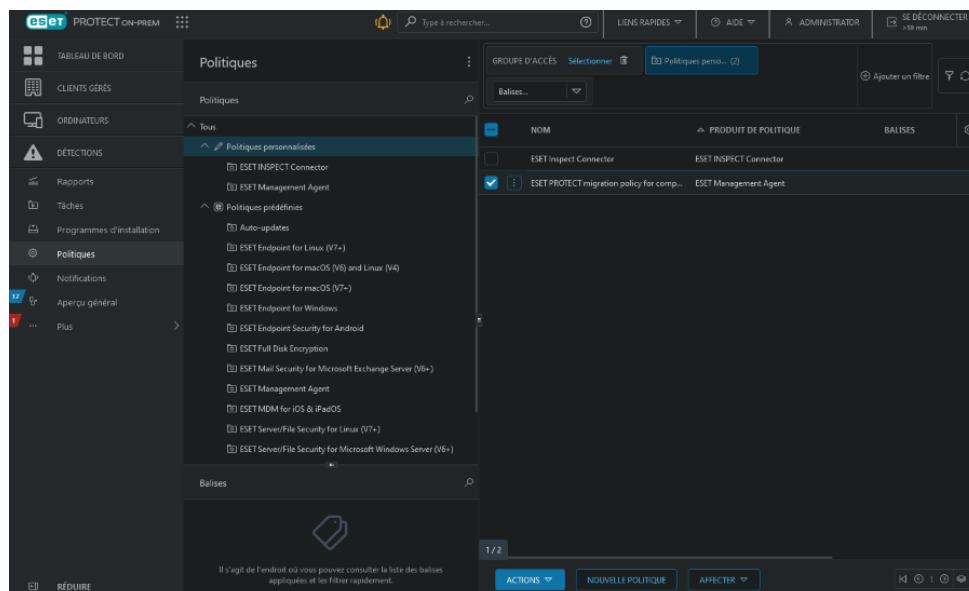
The screenshot displays the ESET PROTECT Web Console interface. The left sidebar contains navigation options: TABLEAU DE BORD, ORDINATEURS, DÉTECTIONS, and VULNÉRABILITÉS. The main area shows the 'Tableau de bord' with several charts: 'Computer statuses overview' (a donut chart showing 12 OK and 1 Risky), 'Operating systems' (a donut chart showing various OS types), 'Rogue computers ratio' (a donut chart showing 100% Known), and 'Computers with problems' (a table listing issues). A dropdown menu for 'LIENS RAPIDES' is open, showing options like 'CONFIGURER VOS APPAREILS', 'GÉRER LES APPAREILS', 'GÉRER LE COMPTE', and 'Télécharger la politique de migration...' (highlighted).

Nom de l'ordinateur	Heure de l'occurrence	Gravité	Source	Fonctionnalité	État	Problème
...	14 février 2024...	Critique	Produit de séc...	Mise à jour	Risque relatif à...	Le moteur de ...
...	4 février 2024...	Critique	ESET INSPECT ...		Risque relatif à...	Produit non ac...
...	25 janvier 202...	Critique	Produit de séc...	Autre	Risque relatif à...	Produit non ac...
...	18 décembre 2...	Critique	Produit de séc...		Risque relatif à...	La gestion des ...
...	18 décembre 2...	Critique	Produit de séc...		Risque relatif à...	La gestion des ...
...	24 août 2023 1...	Critique	Produit de séc...		Risque relatif à...	La gestion des ...

2. Dans votre ESET PROTECT On-Prem, sélectionnez **Politiques** > **Importer**. Sélectionnez le fichier **.dat** téléchargé aux étapes précédentes, puis cliquez sur **Importer**.

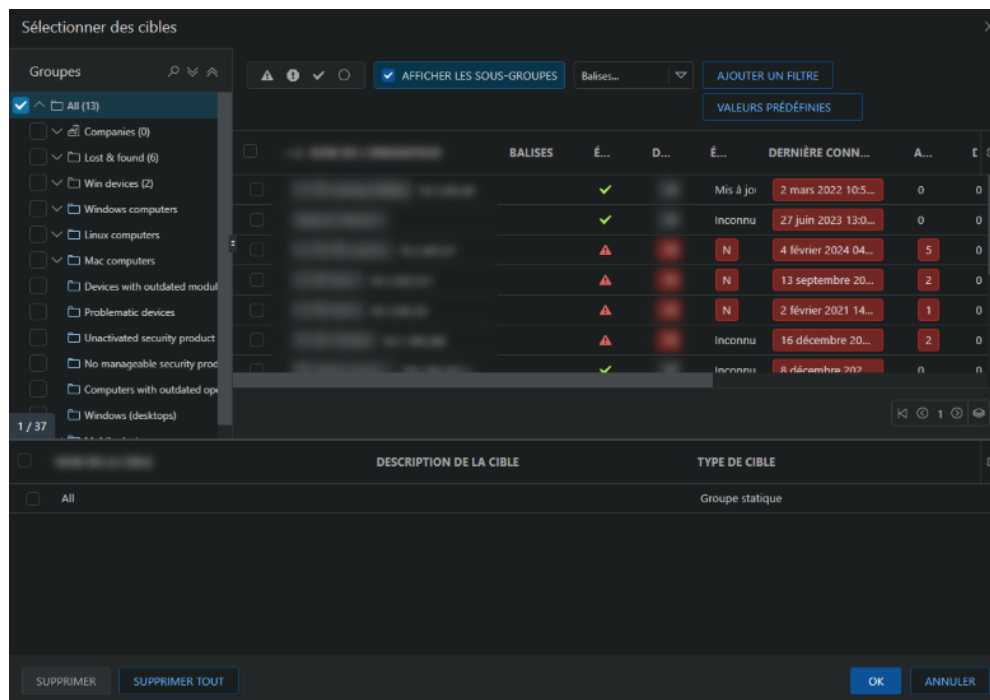


3. Accédez à **Politiques personnalisées** et sélectionnez votre politique de migration importée.



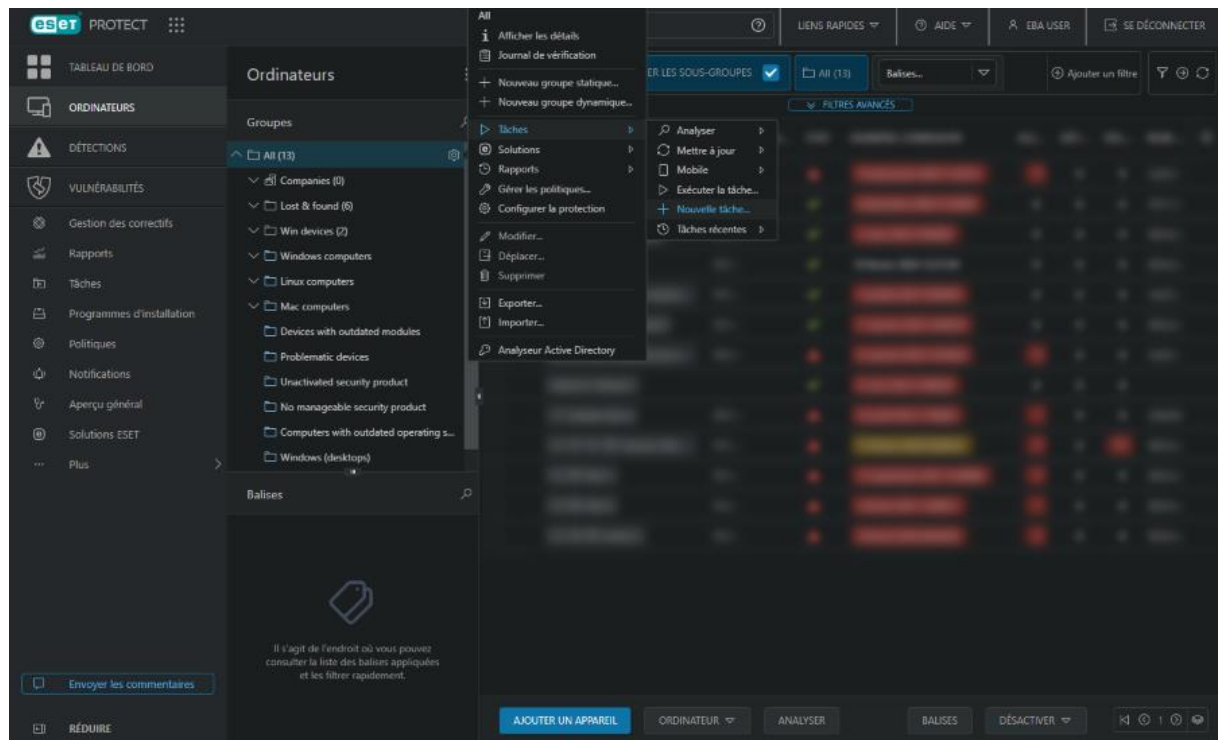
4. Cliquez sur la politique de migration, puis sur **Modifier**.
5. Dans **Paramètres** > **Connexion**, définissez l'indicateur ⚡ **Forcer** pour les options **Serveurs auxquels il faut se connecter** et **Certificat**.
6. Cliquez sur **Terminer**.

7. Cliquez sur Attribuer > Attribuer des groupes.
8. Sélectionnez le groupe statique Tout, puis cliquez sur OK.



9. Cliquez sur Terminer pour appliquer la politique.
10. Connectez-vous à la console Web de ESET PROTECT. Dans Ordinateurs, vous verrez les ordinateurs migrés à partir d' ESET PROTECT On-Prem. Vous devrez peut-être patienter quelques minutes jusqu'à ce que tous les ordinateurs de ESET PROTECT On-Prem commencent à se connecter à ESET PROTECT.
11. Après avoir migré des ordinateurs de ESET PROTECT On-Prem vers ESET PROTECT, vous devez réactiver les produits de sécurité ESET sur les ordinateurs gérés avec des licences du nuage gérées par ESET PROTECT :

12. Dans la console Web de ESET PROTECT, cliquez sur Ordinateurs > cliquez sur l'icône de l'engrenage en regard du groupe statique Tout > sélectionnez Tâches > Nouvelle tâche.



13. Sélectionnez **Activation du produit** dans le menu déroulant **Tâche**.
14. Sélectionnez la licence du produit de sécurité ESET dans **Paramètres**, passez en revue les ordinateurs cibles dans **Cibles** et cliquez sur **Terminer**.
15. Veuillez patienter quelques minutes jusqu'à ce que les produits de sécurité ESET soient activés.

4.7 - Migration des périphériques mobiles

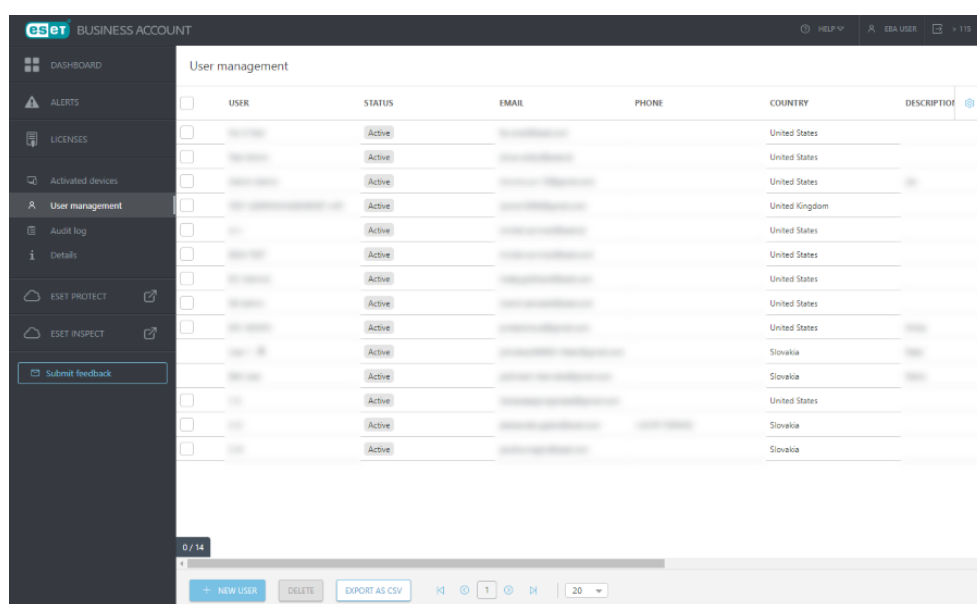
1. Ouvrez la Web Console de ESET PROTECT.
2. Cliquez sur Plus > Paramètres > Migration des périphériques mobiles depuis ESET PROTECT On-Prem.
3. Sélectionnez la licence à utiliser pour l'activation des périphériques mobiles gérés une fois la migration terminée.
4. Sélectionnez le groupe parent pour le placement initial des périphériques après la migration.
5. Limite d'utilisation du jeton : vous pouvez limiter le nombre de périphériques pour la migration à l'aide du jeton de migration.
6. Sélectionnez Générer un jeton pour générer un jeton de migration avec les paramètres définis pour le processus de migration.
7. Le jeton de migration se présente sous la forme d'une chaîne de caractères dans le champ ci-dessous. Copiez-le dans un éditeur de texte.
8. Ouvrez la Web Console de ESET PROTECT On-Prem.
9. Cliquez sur > Politiques > Nouvelle politique.
10. Dans la section L'essentiel, remplissez le nom et la description de la politique. Cette politique migre les périphériques mobiles actuellement gérés de l'environnement local vers l'environnement en nuage.
11. Dans la section Paramètres, sélectionnez Agent ESET Mobile Device Connector.
12. Sous Général > Migration de ESET PROTECT, collez le jeton de migration dans le champ de texte Jeton de migration.
13. Dans la section Affecter, sélectionnez le périphérique exécutant Mobile Device Connector.
14. Une fois la politique appliquée, le processus de migration commence.
15. Vous pouvez surveiller la migration dans la console Web ESET PROTECT. Une fois le périphérique mobile migré, il se connectera à ESET PROTECT et il sera visible dans la section Ordinateurs de la console Web ESET PROTECT.
16. Une fois que la migration du périphérique vers l'environnement ESET PROTECT a réussi, vous pouvez le supprimer de la console Web ESET PROTECT On-Prem.
17. Une fois tous les périphériques mobiles ESET PROTECT migrés vers l'environnement, vous pouvez mettre hors service le composant Mobile Device Management en toute sécurité.

4.8 - Configurer les utilisateurs ESET PROTECT

4.8.1 – Dans le cas où vous utilisez ESET Business Account

Suivez les étapes ci-dessous pour créer un nouvel utilisateur de ESET PROTECT dans ESET Business Account et mapper le compte d'utilisateur dans ESET PROTECT :

1. Connectez-vous à votre compte ESET Business Account.
2. Sélectionnez Gestion des utilisateurs > Nouvel utilisateur.



3. Remplissez les champs requis (pour en savoir plus, consultez l'aide en ligne de ESET Business Account) :
4. Général : Fournit des informations de base sur l'utilisateur
5. Droits d'accès :
6. Accès entreprise - Sélectionnez le niveau d'accès de l'utilisateur à l'entreprise : Écrire, Lire, Accès uniquement à des sites sélectionnés.
7. Accès à la gestion des utilisateurs - Cochez la case pour permettre à l'utilisateur de gérer d'autres utilisateurs dans ESET Business Account.
8. ESET PROTECT et accès ESET Inspect :
9. Écriture - L'utilisateur a un accès complet à ESET PROTECT et ESET Inspect.
10. Lire - L'utilisateur ne peut consulter les données que dans ESET PROTECT et ESET Inspect.
11. Personnalisée - Vous pouvez définir l'accès des utilisateurs plus tard dans ESET PROTECT dans Jeux d'autorisations.
12. Aucun accès - L'utilisateur n'a aucun accès à ESET PROTECT et ESET Inspect.

13. Préférences - permet de définir la langue de l'utilisateur pour ESET Business Account et ESET PROTECT et de définir le fuseau horaire.
14. Sécurité - Ajuster les paramètres de sécurité pour l'utilisateur (expiration du mot de passe, délai d'inactivité de la session, vérification à deux facteurs).

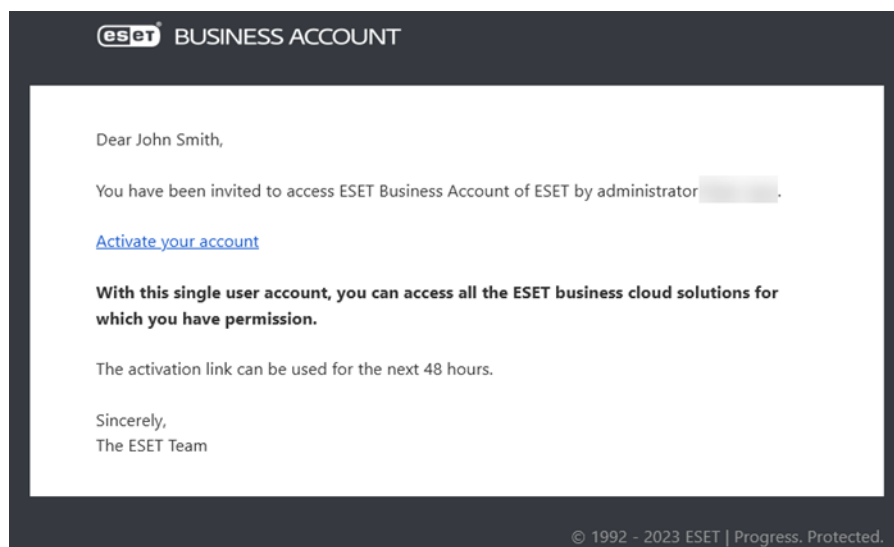
Cliquer sur Créer pour créer l'utilisateur.

The screenshot shows the 'New user' form in the ESET Business Account interface. The form is divided into two main sections: 'GENERAL' and 'ACCESS RIGHTS'. The 'GENERAL' section contains the following fields: First name (John), Last name (Smith), Description (Optional), Email address (email@address.com), Phone number (Optional), and Country (United States). The 'ACCESS RIGHTS' section contains three radio button options: 'Write' (User has full access), 'Read' (User can only view collected data), and 'Write' (User has full access and can create and execute actions). The 'Read' option is selected. At the bottom of the form, there are 'CREATE' and 'CANCEL' buttons.

15. Le nouvel utilisateur apparaît dans la fenêtre Gestion des utilisateurs avec l'étiquette **En attente d'activation**.

User management		
	USER	STATUS
☐		Active
☐		Active
☐	John Smith	Waiting for activation

16. L'utilisateur recevra un courriel d'activation (à l'adresse de courriel que vous avez indiquée lors de la création de l'utilisateur). L'utilisateur doit cliquer sur **Activer votre compte**.



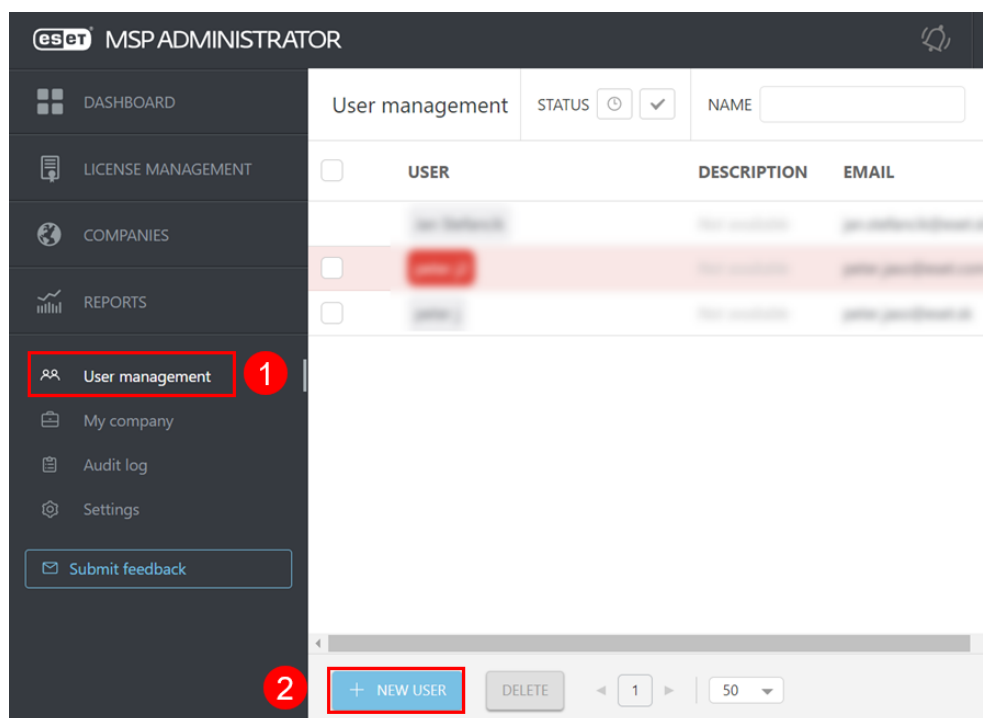
17. L'utilisateur doit ajuster les paramètres utilisateur et saisir le mot de passe deux fois (**créer un mot de passe et confirmer le mot de passe**); ensuite, il doit cocher la case **J'accepte les conditions d'utilisation d'ESET** et cliquer sur **Activer le compte**.

A screenshot of the ESET Business Account activation form. The form is titled 'ESET BUSINESS ACCOUNT' and includes a list of benefits: 'Create a fully functional free trial (no commitment)', 'Get an overview of all your security licenses', 'Check the real-time status on used up seats', and 'Deactivate and recoup immediately'. The form fields include: Name (John Smith), E-mail, Phone number, Language (English), EPC Language (English), Create password (masked with dots), and Confirm password (masked with dots). Below the password fields, there are checkboxes for password requirements: 'Minimum number of characters: 10', 'One lowercase character', 'One uppercase character', 'One number', and 'One special character'. A checkbox labeled 'I agree to the ESET Terms of Use' is checked. At the bottom, there is a blue button labeled 'ACTIVATE THE ACCOUNT'.

18. Mappez l'utilisateur dans ESET PROTECT Web Console.

4.8.2 – Dans le cas où vous utilisez ESET MSP Administrator

1. Accédez à la gestion des utilisateurs dans l'administrateur ESET MSP 2.
2. Cliquez sur Nouvel utilisateur.



3. Tapez le nom et le prénom dans les champs correspondants.
4. Saisissez une adresse électronique active. L'utilisateur peut modifier cette adresse ultérieurement.
5. Sélectionnez le pays applicable.
6. À côté de Droits d'accès, sélectionnez l'option de permission de l'utilisateur applicable. Consultez la rubrique Permissions pour plus d'informations.
7. Cliquez sur Créer un utilisateur.

8. Le nouvel utilisateur reçoit un courriel d'invitation et doit terminer la procédure de création de compte.

The screenshot shows the 'New user' form in the ESET MSPADMINISTRATOR interface. The form is divided into two main sections: 'GENERAL' and 'PERMISSIONS'. The 'GENERAL' section contains fields for 'First and last name', 'Description', 'Email address', 'Phone number', and 'Country'. The 'PERMISSIONS' section contains 'ACCESS RIGHTS' with three radio button options. Red boxes and numbers highlight specific elements: 3 points to the 'First and last name' field (containing 'John' and 'Doe'); 4 points to the 'Email address' field (containing 'email_of_john@doe.no'); 5 points to the 'Country' dropdown menu (set to 'United States'); 6 points to the 'Write access to MSP' radio button; and 7 points to the 'CREATE USER' button at the bottom.

GENERAL

First and last name **3** John Doe

Description - Optional Ordinary MSP user

Email address **4** email_of_john@doe.no
Address will be used for sending an email invitation.
Each user can set up his own email address afterward.

Phone number - Optional +123456789

Country **5** United States

PERMISSIONS

ACCESS RIGHTS

6 ☒ Write access to MSP and all customers
User can manage company, it's users and customers. Write access allows user to order licenses, update license seats quantity, activate, deactivate and rename customers' seats.

☐ Read access to MSP and all customers
User can see details of MSP and all customers. Read access allows user to activate, deactivate and rename customers' seats.
His rights for defined customers can be elevated in the table below.

☐ No access to MSP and custom access on customers
User can manage or view customers defined in the table below.

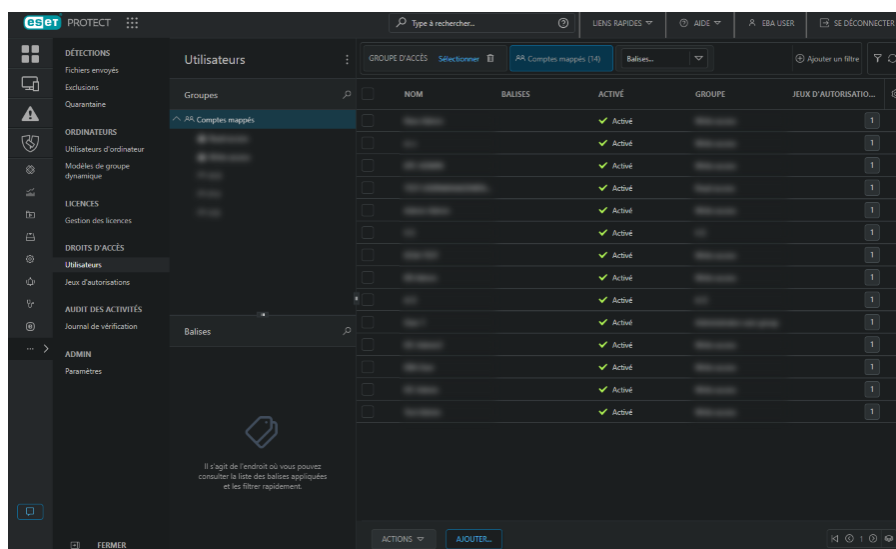
7 CREATE USER CANCEL

4.9 - Ajouter les utilisateurs à la console web ESET PROTECT Web Console

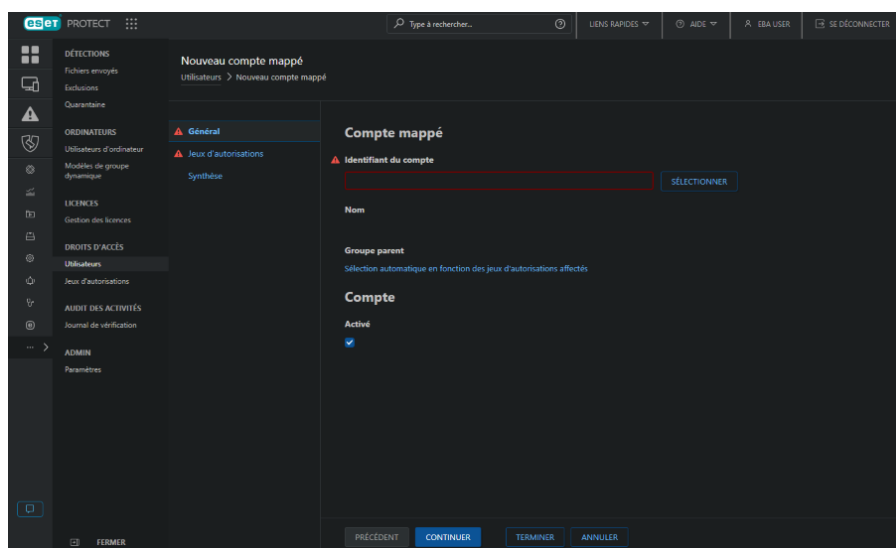
4.9.1 – Dans le cas où vous utilisez ESET Business Account

Suivez les étapes ci-dessous pour mapper un utilisateur de ESET Business Account dans ESET PROTECT :

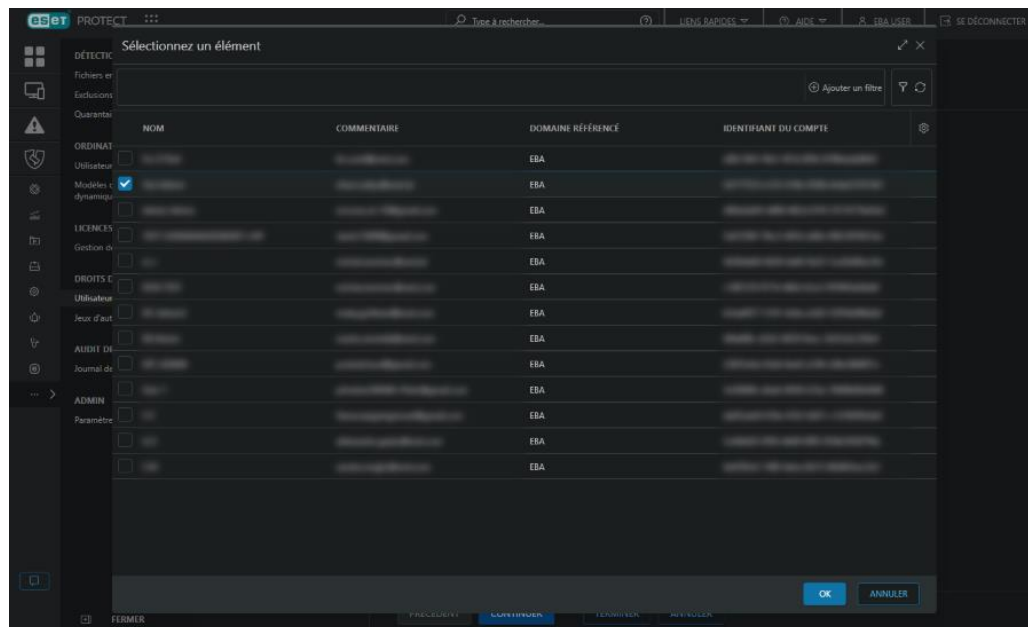
1. Connectez-vous à ESET Business Account à l'aide du compte utilisateur que vous avez indiqué lors [de la création d'un nouvel utilisateur dans ESET Business Account](#); n'utilisez pas encore le compte d'utilisateur nouvellement créé.
2. Ouvrez la Web Console de ESET PROTECT. Cliquez sur **Plus > Utilisateurs**, puis sélectionnez **Comptes mappés**; ensuite cliquez sur le bouton **Ajouter un nouveau**.



3. Cliquez sur Sélectionner sous Identificateur de compte.



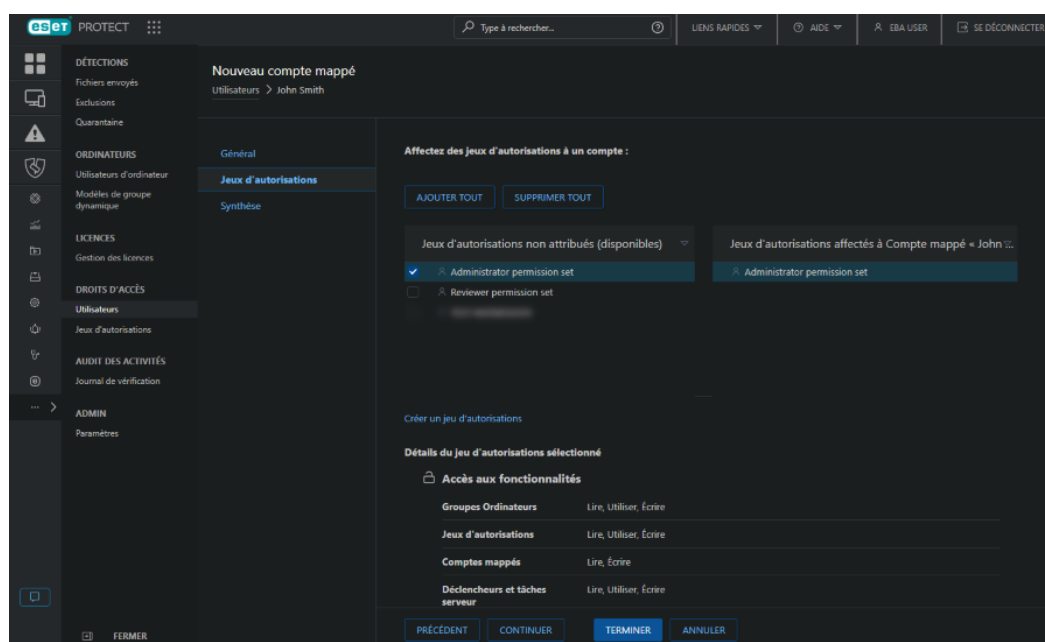
4. Sélectionnez l'utilisateur que vous avez [créé dans ESET Business Account](#) et cliquez sur **OK**.



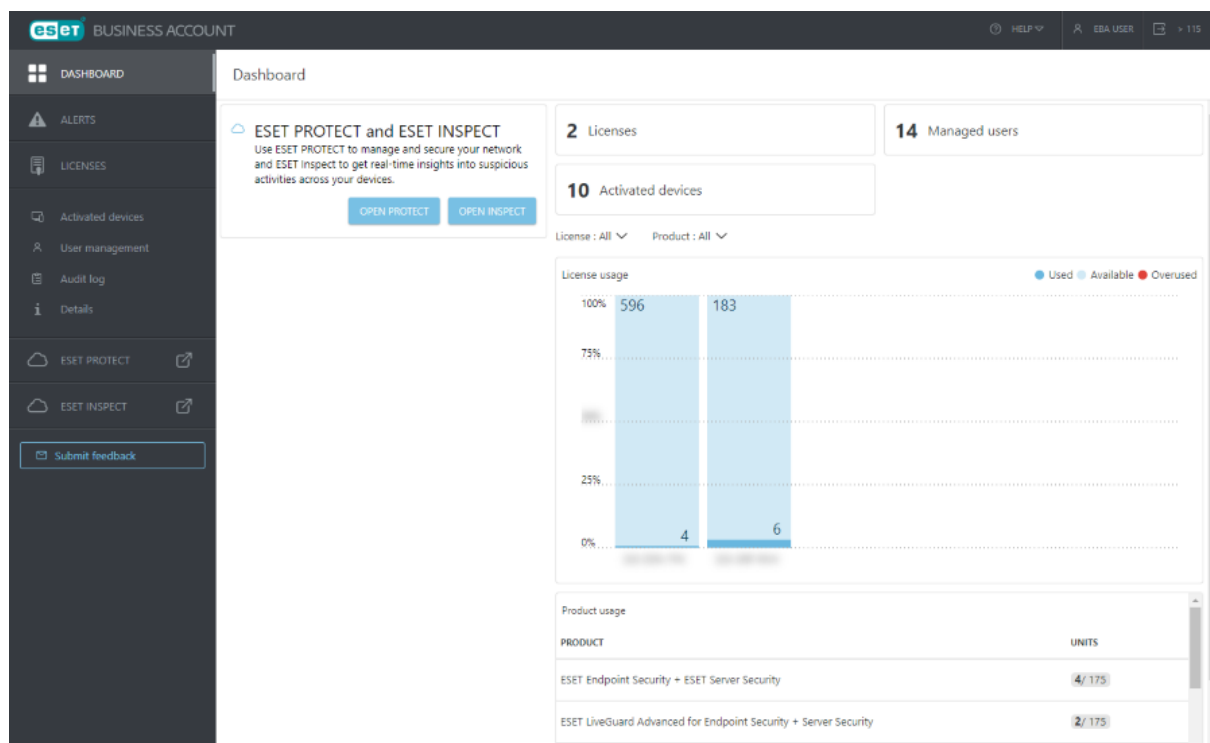
5. **Groupe d'accueil** : Le groupe d'accueil est automatiquement détecté en fonction de l'ensemble d'autorisations attribué à l'utilisateur actuellement actif.

Si le groupe d'accueil présélectionné ne répond pas à vos attentes, vous pouvez sélectionner le groupe d'accueil manuellement.

6. Dans **Jeux d'autorisations**, vous pouvez voir le niveau d'autorisation que vous avez attribué à l'utilisateur lors de sa [création dans ESET Business Account](#). Si vous avez sélectionné **Accès ESET PROTECT personnalisé**, vous devez attribuer un jeu d'autorisations à l'utilisateur (un jeu existant ou vous pouvez [créer un nouveau jeu d'autorisations](#)). Cliquez sur **Terminer**.



7. Les utilisateurs qui ont accès à ESET PROTECT auront la possibilité d'ouvrir ESET PROTECT dans leur ESET Business Account.

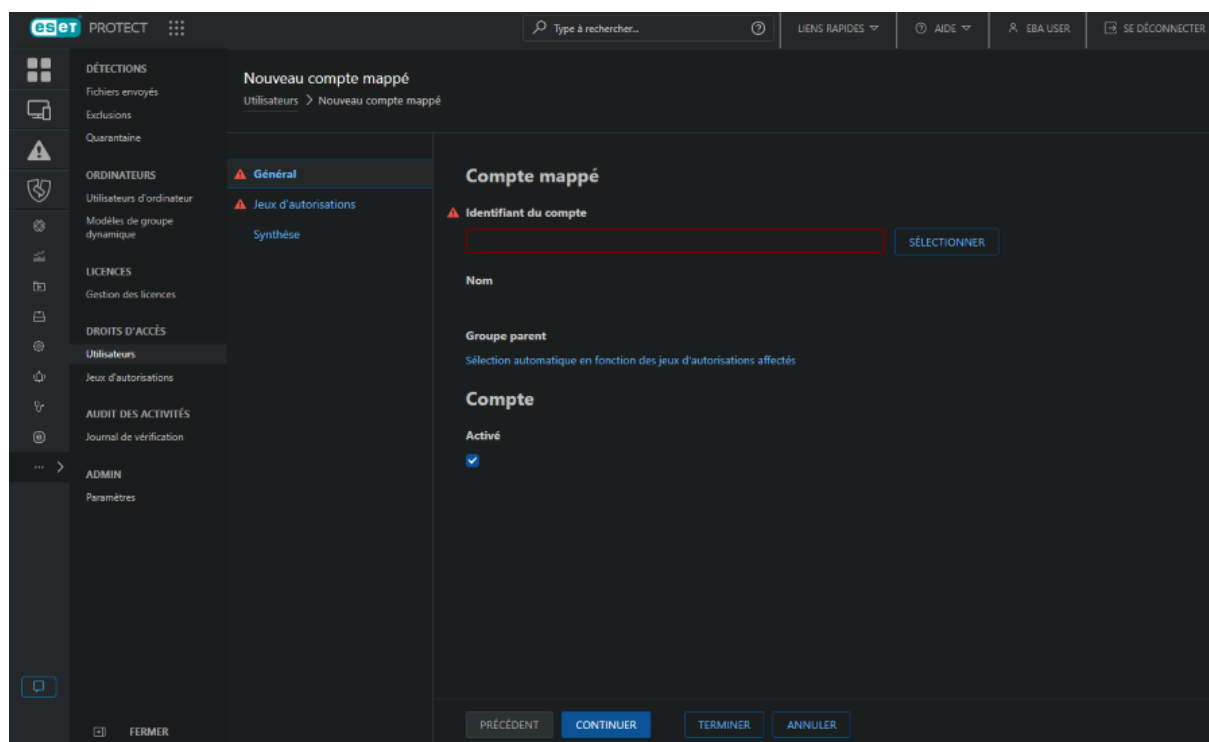


4.9.2 – Dans le cas où vous utilisez ESET MSP Administrator

Pour créer un nouvel utilisateur pour la console web ESET PROTECT, vous devez d'abord créer cet utilisateur dans ESET MSP Administrator (EMA 2). Consultez la rubrique [Aide en ligne EMA 2](#) pour un guide étape par étape sur l'ajout d'un utilisateur. Vous pouvez ajouter le nouvel utilisateur au cours de la [Configuration de client MSP](#) ou en suivant les étapes ci-dessous.

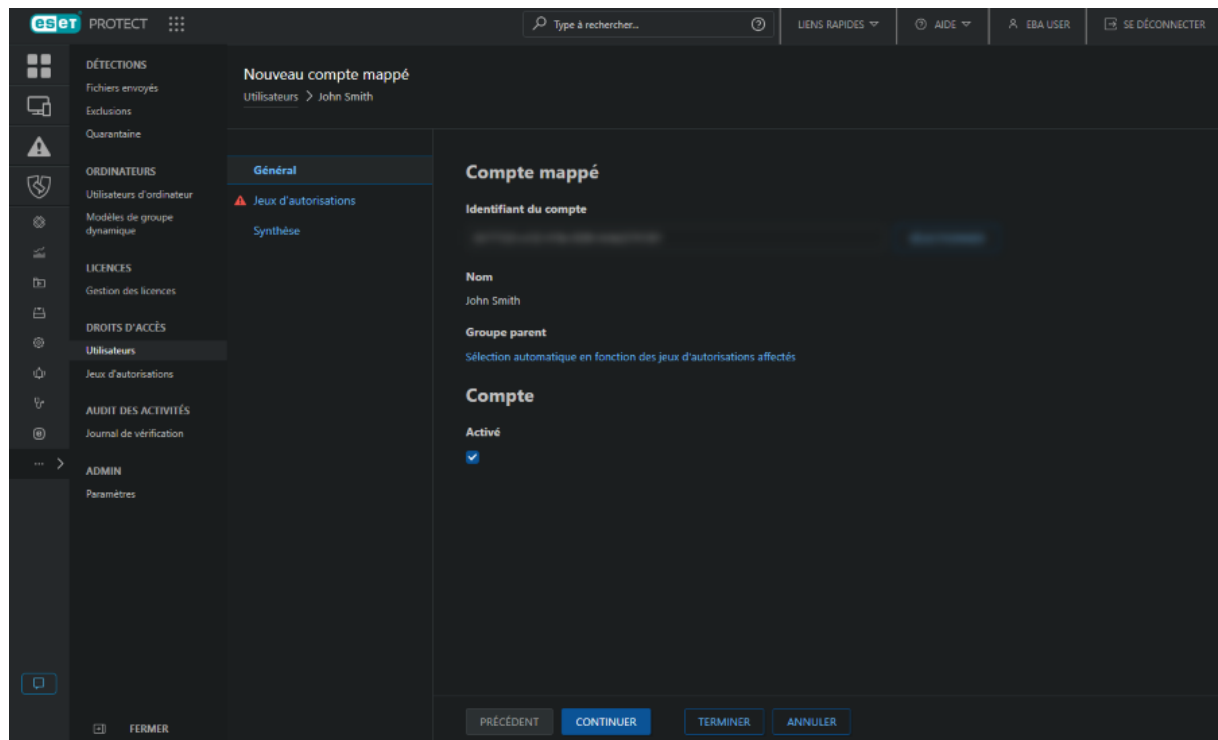
- [Voyez comment fonctionnent les autorisations d'utilisateur dans EMA 2 et ESET PROTECT dans l'aide en ligne EMA 2.](#)
- [Voyez le guide étape par étape sur la création de l'instance ESET PROTECT.](#)

1. Ouvrez la Web Console.
2. Accédez à Utilisateurs.



3. Cliquez sur **Sélectionner** à côté du champ **Identificateur de compte** et sélectionnez l'utilisateur que vous souhaitez activer dans ESET PROTECT.
4. Vous pouvez ajouter des balises, nouvelles ou existantes, à l'utilisateur.
5. Cliquez sur Sélectionner à côté du champ Groupe d'accueil. Le groupe d'accueil est le groupe statique dans lequel les objets créés par l'utilisateur sont enregistrés par défaut.

6. Cliquez sur Jeux d'autorisations.



7. Sélectionnez un jeu d'autorisations pour le nouvel utilisateur. Un jeu d'autorisations détermine les [droits d'accès](#) de l'utilisateur. Chaque jeu d'autorisations donne à l'utilisateur des droits sur certains groupes statiques. Les groupes sont définis dans chaque jeu d'autorisations. Un ou plusieurs jeux d'autorisations peuvent être attribués à un utilisateur. Vous pouvez sélectionner un des jeux d'autorisations proposés ou en [créer un nouveau](#).
8. Cliquez sur **Terminer** pour enregistrer les modifications. Le nouvel utilisateur peut maintenant se connecter à la console web ESET PROTECT en utilisant ses authentifiants EMA 2.

4.10 - Mettre hors service le serveur ESET PROTECT sur site

Après avoir réussi à migrer vers ESET PROTECT, mettez hors service le serveur ESET PROTECT.

Vérifiez que le nouveau serveur ESET PROTECT Server est en cours d'exécution et que les ordinateurs clients se connectent correctement au nouveau ESET PROTECT On-Prem.

Plusieurs méthodes permettent de désactiver l'ancien ESET PROTECT Server après la migration vers un autre serveur :

4.10.1 - Conserver le système d'exploitation de l'ordinateur serveur et le réutiliser

1. [Arrêtez le service de l'ancien ESET PROTECT Server.](#)
2. Supprimez (DROP DATABASE) l'ancienne instance de la base de données ESET PROTECT Server (Microsoft SQL ou MySQL). Si vous avez effectué une migration de la base de données vers le nouveau serveur ESET PROTECT Server, veillez à supprimer la base de données de l'ancien serveur ESET PROTECT Server avant la désinstallation afin d'empêcher la dissociation (suppression) des licences de la nouvelle base de données ESET PROTECT Server.
3. Désinstallez l'ancien ESET PROTECT On-Prem Server et tous ses composants (y compris ESET Management Agent, Rogue Detection Sensor, etc.) :
 - a. [Désinstaller ESET PROTECT On-Prem - Windows](#)
 - b. [Désinstaller ESET PROTECT On-Prem - Linux](#)
4. Planifiez le redémarrage du système d'exploitation de votre serveur après la désinstallation

4.10.2 - Conserver l'ordinateur serveur

La méthode la plus simple pour supprimer ESET PROTECT On-Prem consiste à formater le disque sur lequel le produit est installé. Ce formatage efface tout ce qui se trouve sur le disque, notamment le système d'exploitation.