Intégration d'ISE et de SecureX OnPremises par orchestration

Table des matières

Introduction

Ce document décrit les étapes pour intégrer Identity Services Engine et SecureX via l'orchestration avec un workflow de Cisco Secure GitHub.

Conditions préalables

Cisco vous recommande d'avoir des connaissances sur les sujets suivants :

- Expérience de la configuration Cisco ISE
- Connaissances sur l'API ISE
- Connaissances sur l'orchestration SecureX

Exigences

Cisco ISE doit être déployé sur votre réseau et disposer d'un compte SecureX actif. Les workflows d'orchestration sont déclenchés via l'extension du navigateur SecureX.

Dans notre exemple, le workflow à utiliser a été importé depuis la page Cisco Secure GitHub. Cette procédure s'applique également à un workflow personnalisé.

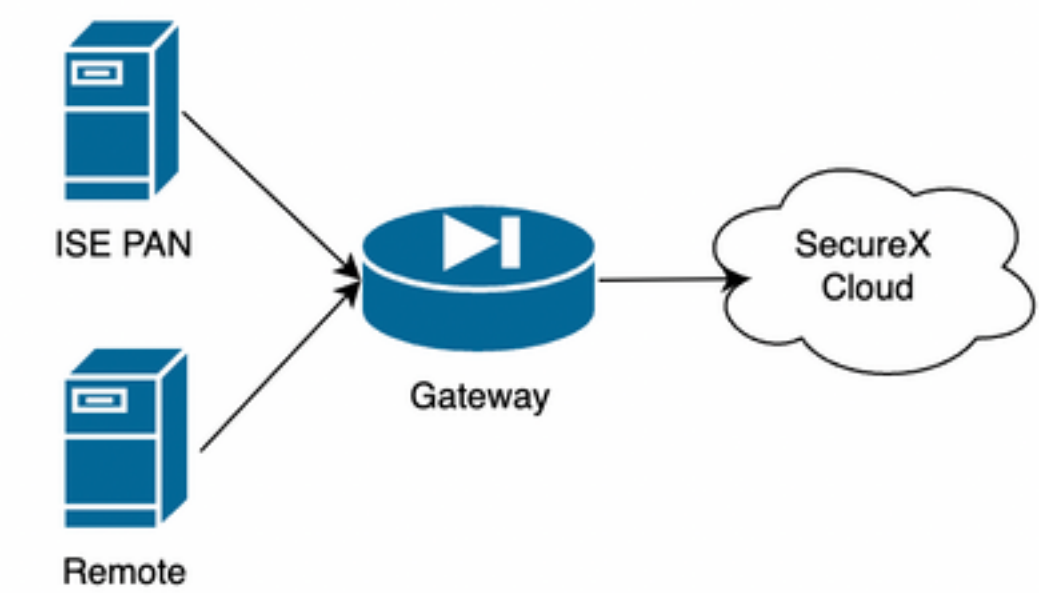
Composants utilisés

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

- Identity Services Engine ISE version 3.1
- compte SecureX
- Périphérique distant SXO version 1.7

Configurer

Diagramme du réseau



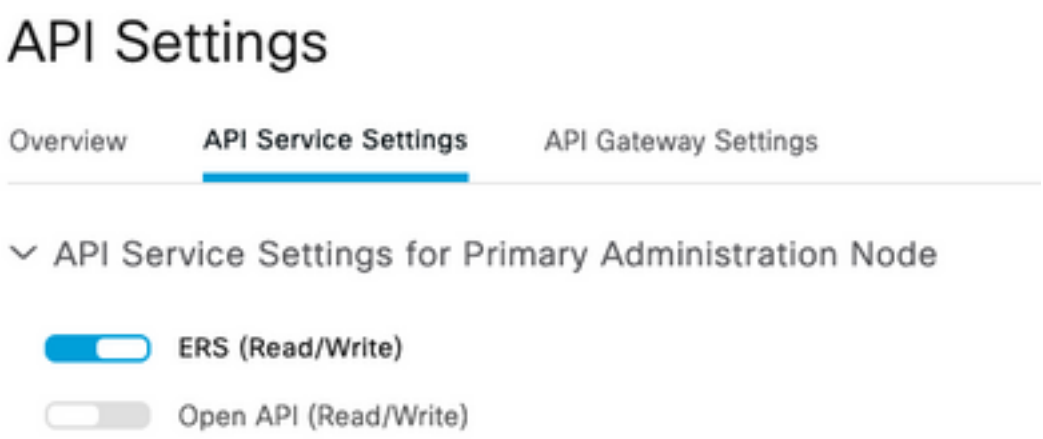
Dans notre exemple, le PAN ISE et le serveur distant sont placés dans le même sous-réseau pour avoir une connectivité directe.

ISE étant un périphérique sur site, le serveur distant doit être en contact avec le cloud Secure-X et transférer les informations au PAN ISE

Configurations

Configuration ISE PAN

1. Accédez à **Administration > System > Settings > API Settings > API Service Settings** et activez **ERS (Read/Write)**

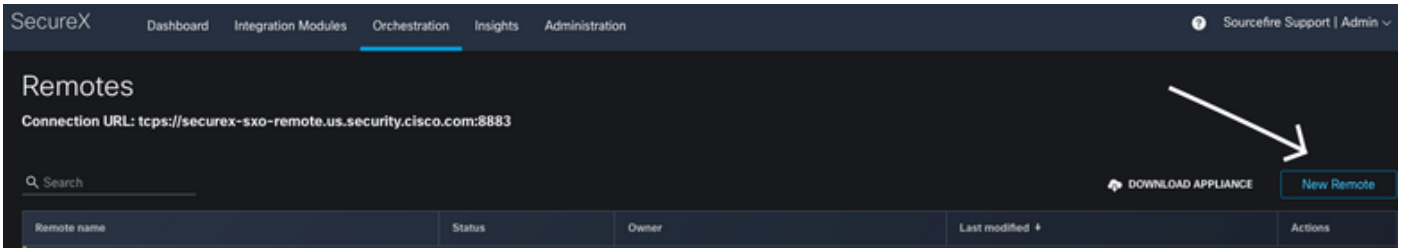


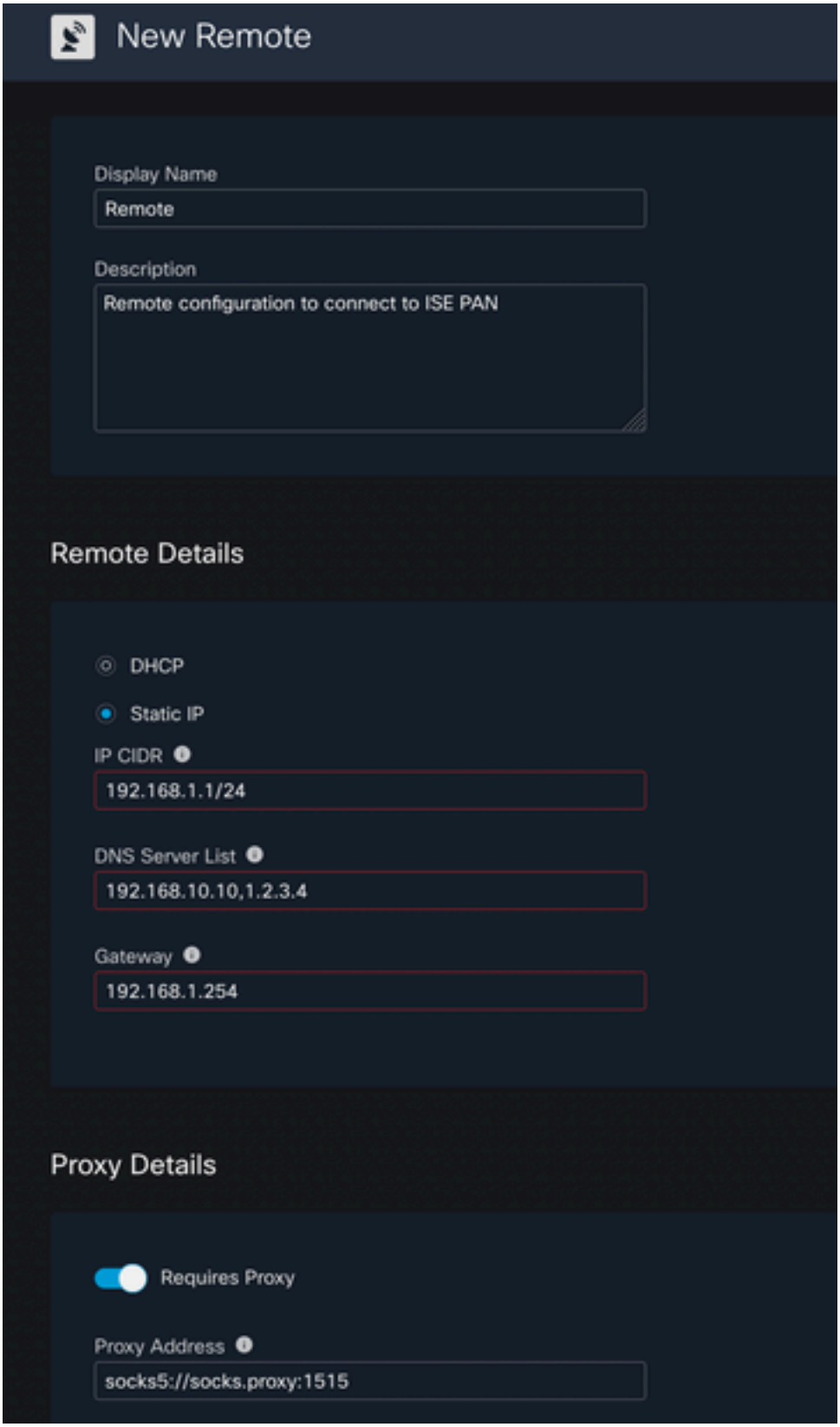
2. (Facultatif) Créez un nouvel utilisateur pour la connexion Secure-X, accédez à **Administration > System > Admin Access > Administrator > Admin Users** et créez un nouvel utilisateur. Ce nouvel utilisateur doit disposer des autorisations « ERS Admin » ou il peut s'agir d'un super administrateur.

Configurer et déployer un serveur distant

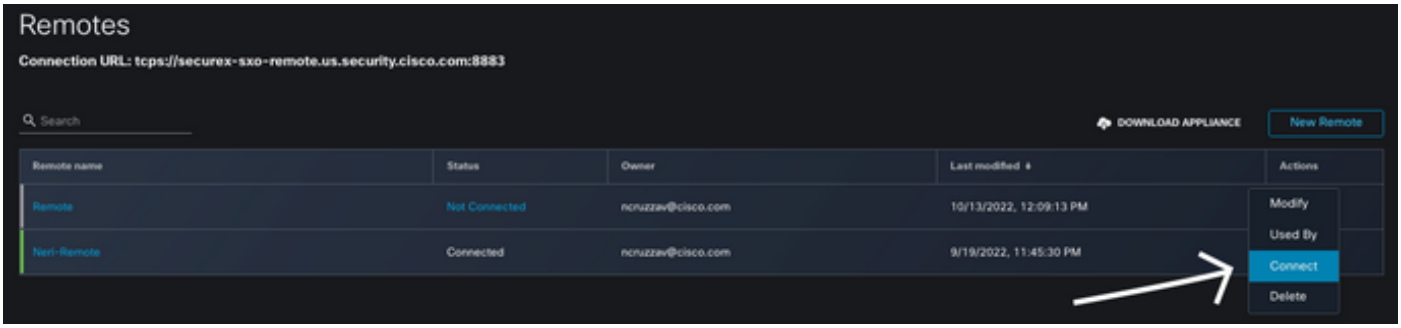
1. Configurez le serveur distant, sur la console Secure-X, accédez à **Orchestration > Admin > Remote Configuration** et sélectionnez l'option **New Remote,** les informations d'adresse IP sont celles à utiliser lors de la création de la VM, et elles doivent se trouver dans le même sous-réseau où le PAN ISE est déployé.

> **Note**: Si la connexion au cloud s'effectue via un proxy, actuellement, seul un proxy SOCKS5 est pris en charge à cette fin.

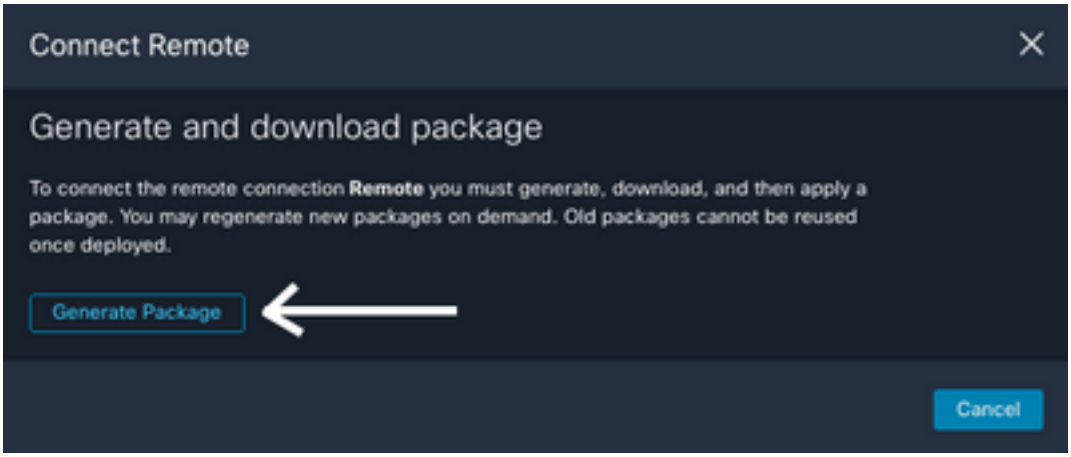




2. Téléchargez les paramètres configurés à utiliser pour le déploiement de la VM. Une fois les informations enregistrées, la télécommande apparaît comme « **Non connectée »**, naviguez sous Actions et sélectionnez **Connecter**



Sélectionnez **Générer un package.** Cette action télécharge un fichier .zip qui contient les informations configurées pour être utilisées lors du déploiement de la VM.



3. Téléchargez et installez la machine virtuelle, en regard de **New Remote** sélectionnez **DOWNLOAD APPLIANCE** cette action télécharge une image OVA que vous devez utiliser pour déployer le serveur distant.

Pour connaître les spécifications des machines virtuelles distantes, reportez-vous au guide [SecureX Remote Setup]

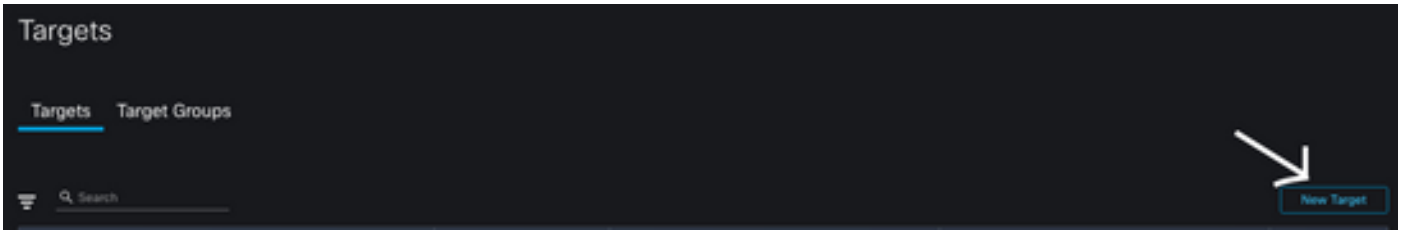
Les informations téléchargées dans le fichier ZIP doivent être utilisées sur les **données utilisateur codées** lors de la création de la machine virtuelle, ce qui remplit les informations distantes configurées dans le serveur une fois qu'il démarre.

4. Une fois que la machine virtuelle est activée, elle se connecte automatiquement au compte SecureX, pour vérifier que la connexion est activée, dans la configuration distante, vous devez voir un changement d'état à **"Connecté"**

Configurer la cible sur SecureX

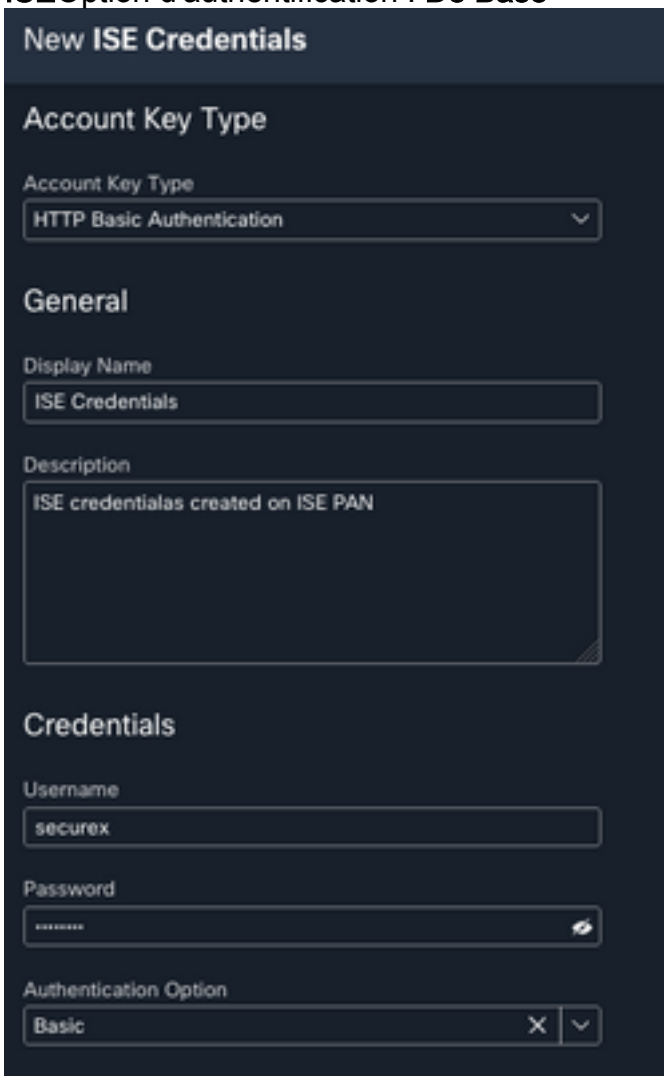
Pour que l'orchestration fonctionne avec un périphérique, il est important de configurer une **cible,** Secure X utilise cette cible pour envoyer les appels API et interagir avec le périphérique via l'orchestration

1. Accédez à **Orchestration > Cibles > Nouvelle cible**

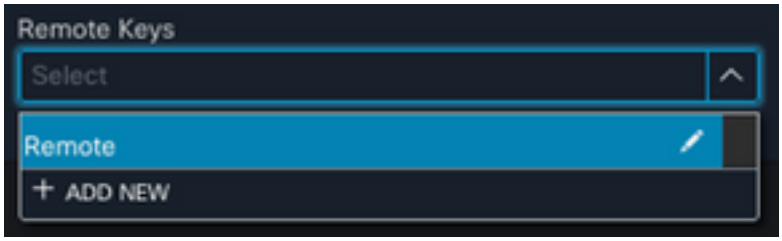


2. Complétez les informations cibles avec les instructions suivantes

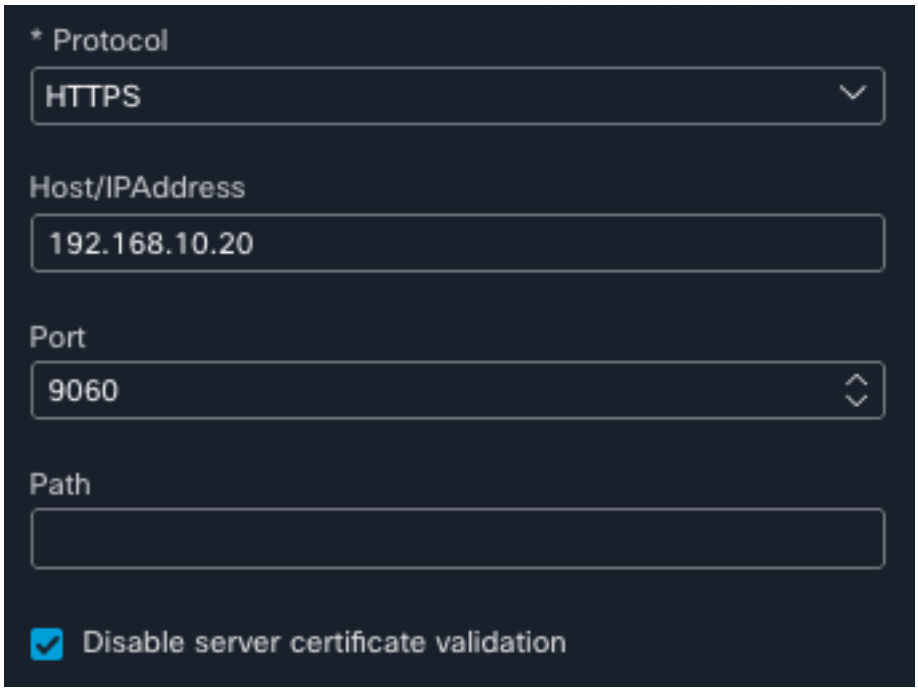
- Nom d'affichage : Identificateur de cible
- Description: Une petite description pour identifier le but de la cible
- Clés de compte : Ici, vous devez configurer l'utilisateur/le mot de passe pour accéder à ISE via l'API Aucune clé de compte : **Faux**Clés de compte par défaut : Sélectionnez **Add New (ajouter nouveau)** Type de clé de compte : **Authentification HTTP de base**Nom d'affichage : Identificateur de clé de compteusername (nom d'utilisateur) : Utilisateur créé sur le **PAN ISE** en tant qu'administrateur ERSMot de passe : Mot de passe de l'utilisateur créé sur le **PAN ISE**Option d'authentification : **De Base**



- Distant : Vous devez sélectionner ici la connexion à distance précédemment configurée Clés distantes : sélectionnez votre télécommande dans le menu déroulant



- HTTP : Ici, vous devez configurer les informations d'API pour le **PAN ISE** Protocole : **HTTPS**Adresse IP/hôte : **IP privé ISE PAN**Port : **9060**Chemin : Laissez-le en blancDésactiver la validation du certificat du serveur : **Cochez cette case**



- Proxy : La configuration du proxy étant incluse dans la configuration distante, vous pouvez laisser cette section vide
- Sélectionnez **Submit (soumettre)**

Importer le workflow depuis Cisco Secure GitHub

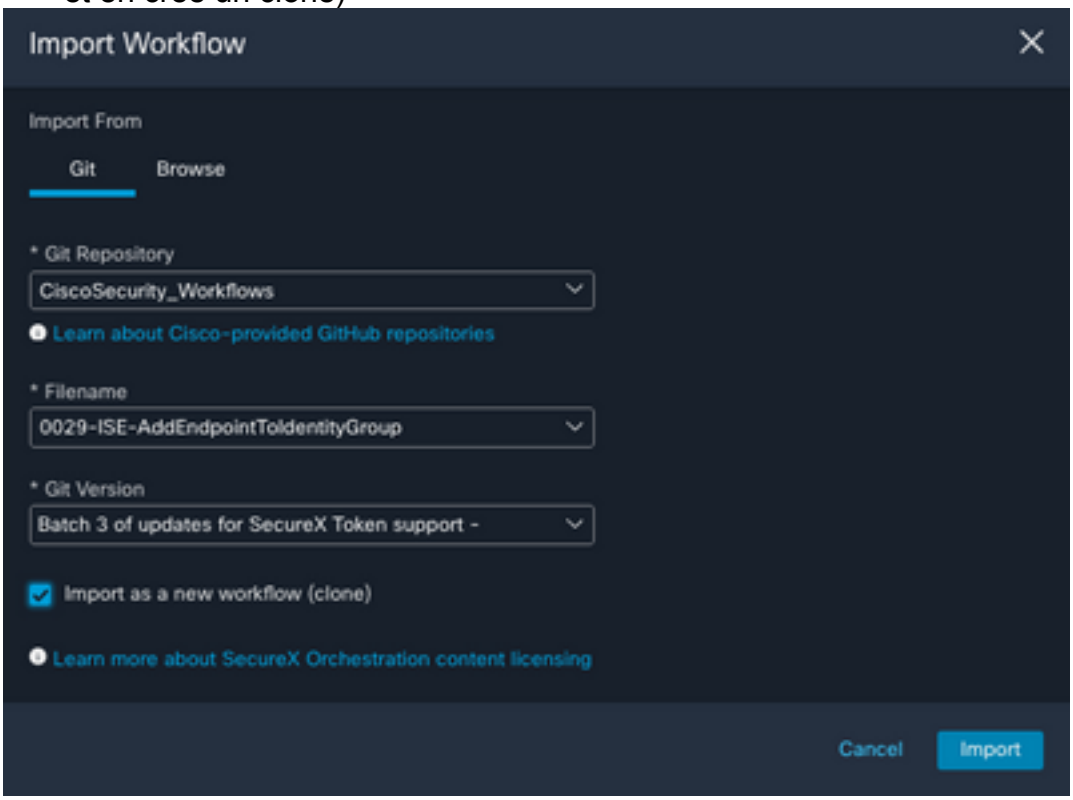
Dans cet exemple, le flux de travail à utiliser est « Add Endpoint to Identity Group », vous pouvez utiliser n'importe lequel des flux de travail listés sur la page Cisco Secure GitHub, ou vous pouvez créer un flux de travail personnalisé.

1. Accédez à **Orchestration > Mes Workflows > Importer un Workflow**

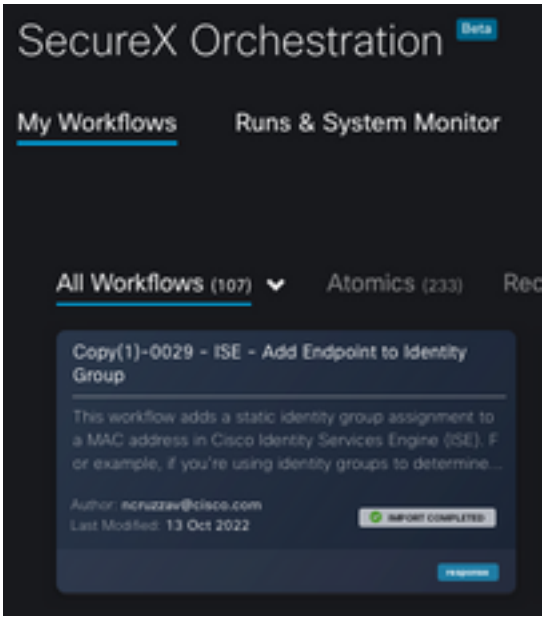
2. Pour importer le workflow, complétez les informations comme suit et sélectionnez **Importer ;** pour identifier le workflow à importer, vous pouvez effectuer une recherche par nom ou par numéro de workflow

- Référentiel Git : **CiscoSecurity_Workflows** (Emplacement du workflow)

- Nom du fichier : **0029-ISE-AddEndpointToIdentityGroup** (Sélectionnez le nombre de flux de travail à utiliser)
- Version Git : **Lot 3 de mises à jour pour la prise en charge des jetons SecureX** (dernière version)
- Importer en tant que nouveau workflow (clone) : **Vérifier** (cette opération importe le workflow et en crée un clone)

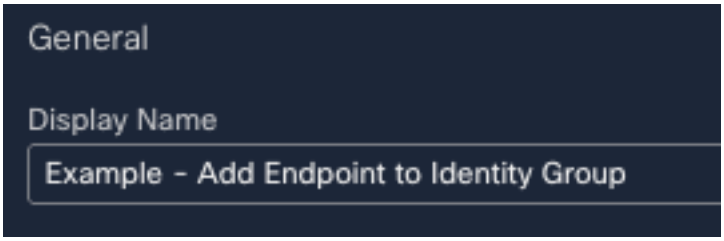


3. Une fois importé, le nouveau modèle apparaît sous **Mes Workflows,** Sélectionnez le nouveau workflow créé pour modifier les paramètres afin qu'il fonctionne avec **ISE**

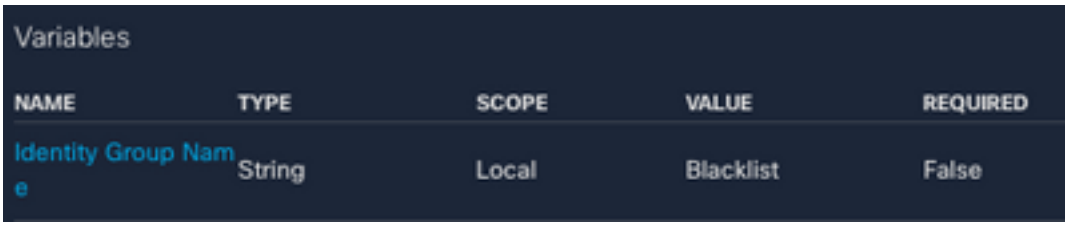


4. Puisqu'il s'agit d'un workflow prédéfini, il vous suffit de modifier 3 sections du workflow :

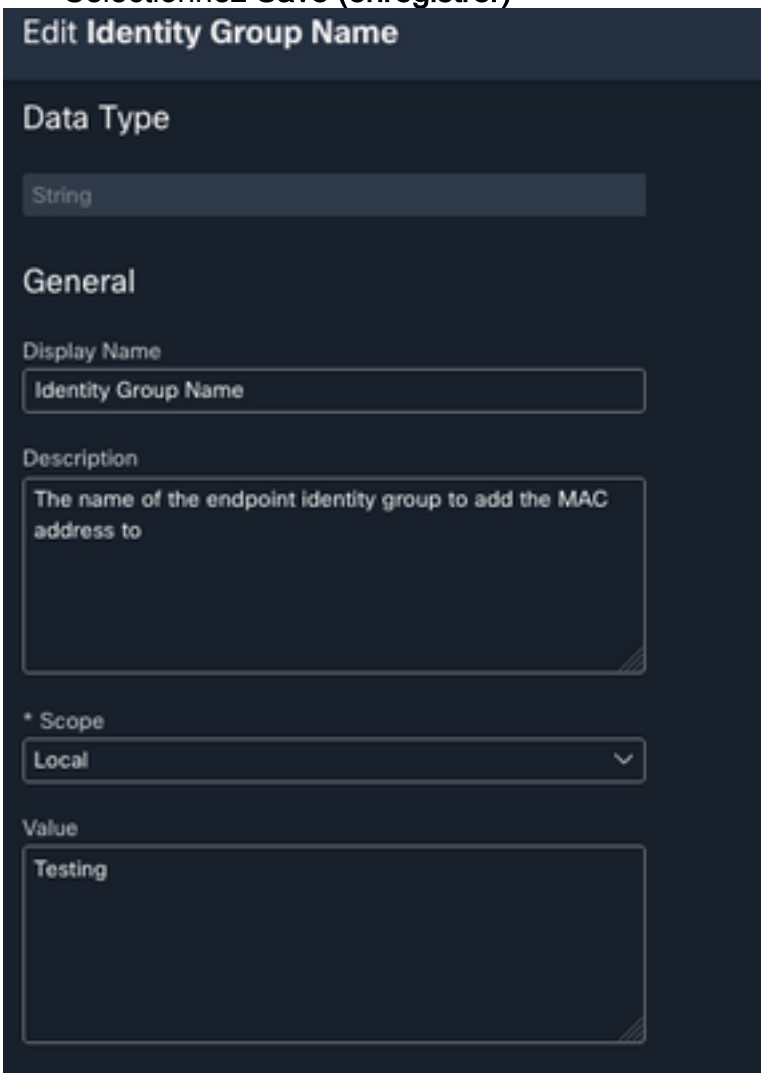
- Name : modifiez le nom d'affichage pour un meilleur identifiant



- Variable de groupe d'identités Sous Variables, modifiez la **variable du groupe d'identités** par défaut est **Liste noire,** sélectionnez la variable et configurez le nom du groupe d'identités que vous souhaitez modifier via l'orchestration



- Sélectionnez **Save (enregistrer)**



- Target (cible) : Configurer la **cible** configurée précédemment Type de cible : **Terminal HTTP**Target (cible) : **Nom de la cible configurée**

Vérifier

Une fois que tout est configuré, il est temps de tester le workflow

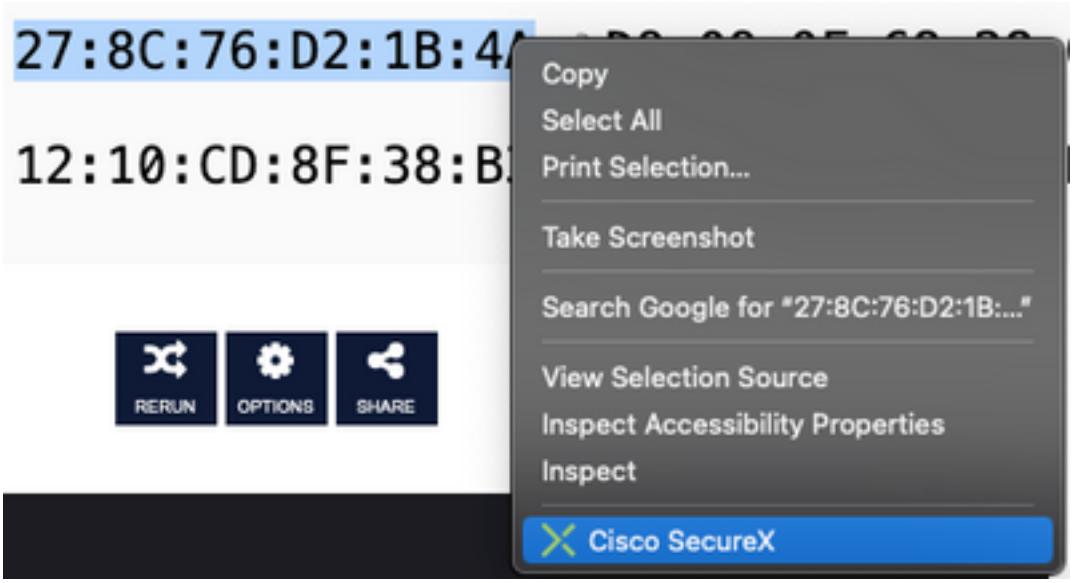
Le workflow pour le test effectue cette action : si vous trouvez une adresse MAC dans une page Web, elle peut se trouver sur ISE elle-même ou sur une autre page Web telle que Threat Response ; via l'extension de navigateur SecureX, le workflow recherche cette adresse MAC dans la base de données ISE via l'API. Si l'adresse MAC n'existe pas, l'élément observable est ajouté au groupe d'identités de point de terminaison sans avoir besoin de copier la valeur et l'accès à ISE.

Pour le démontrer, consultez l'exemple suivant :

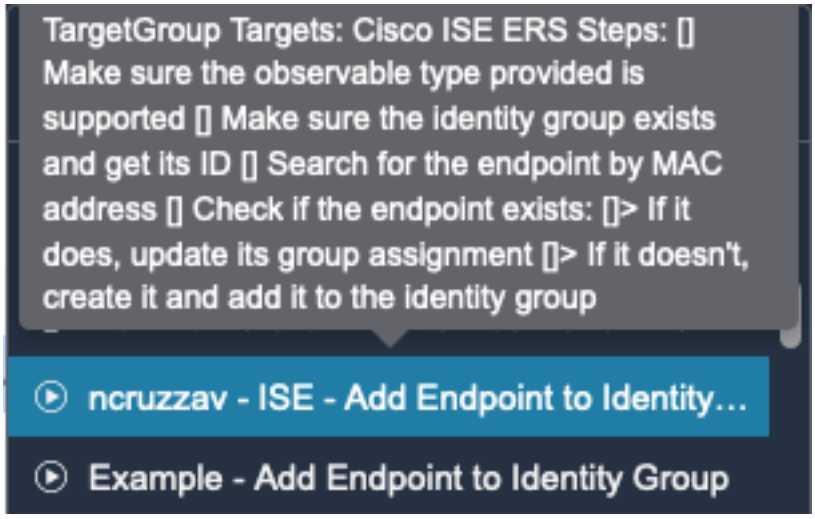
1. Le workflow sélectionné fonctionne avec le type observable **« Adresse MAC »**

2. Recherchez une adresse MAC sur une page Web et effectuez un clic droit.

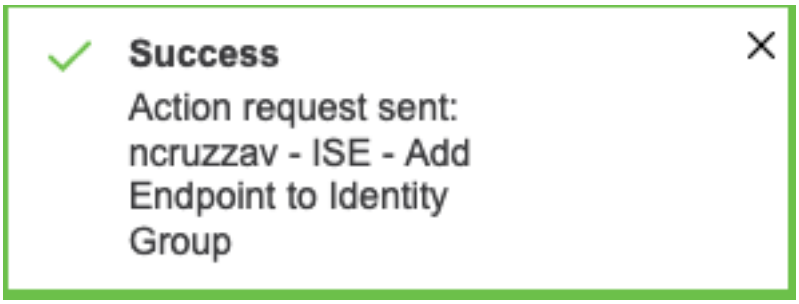
3. Sélectionnez l'option **SecureX**



4. Sélectionnez le **workflow** créé avant

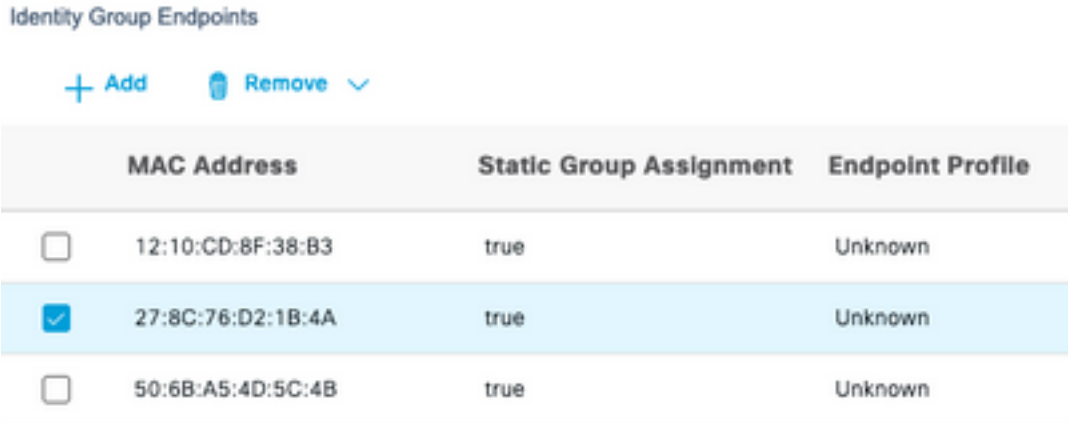


5. Confirmez que la tâche est exécutée avec succès



6. Sur le **PAN ISE**, naviguez jusqu'à **Administration > Gestion des identités > Groupes > Groupes d'identités de point de terminaison > (Le groupe configuré sur le workflow)**

7. Ouvrez le **groupe d'identités de point de terminaison** configuré sur le workflow et vérifiez que l'adresse MAC sélectionnée est ajoutée à cette liste d'adresses MAC



À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.