オーケストレーションによるISEとSecureX OnPremisesの統合

内容

概要

このドキュメントでは、オーケストレーションを介してIdentity Services Engine(ISE)とSecureXをCisco Secure GitHubのワークフローと統合する手順について説明します。

前提条件

次の項目に関する知識が推奨されます。

- Cisco ISE設定の経験
- ISE APIに関する知識
- SecureXオーケストレーションに関する知識

要件

ネットワークにCisco ISEを導入し、アクティブなSecureXアカウントを持っている必要があります。オーケストレーションワークフローは、SecureXブラウザ拡張機能を介してトリガーされます。

この例では、使用するワークフローがCisco Secure GitHubページからインポートされています。この手順は、カスタムワークフローにも適用されます。

使用するコンポーネント

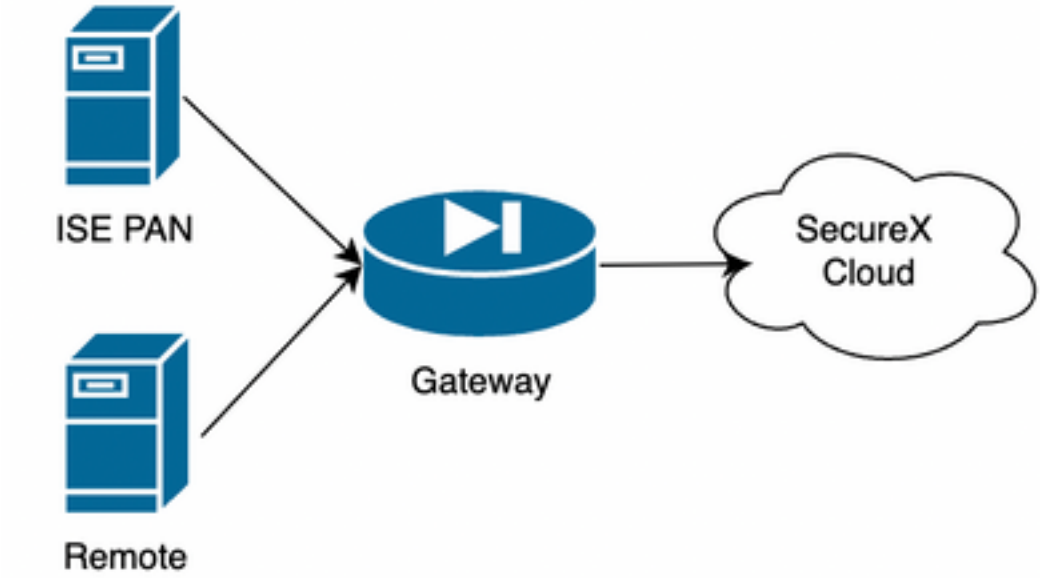
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してく

ださい。

- Identity Services Engine(ISE)バージョン3.1
- SecureXアカウント
- SXO Remoteデバイスバージョン1.7

設定

ネットワーク図



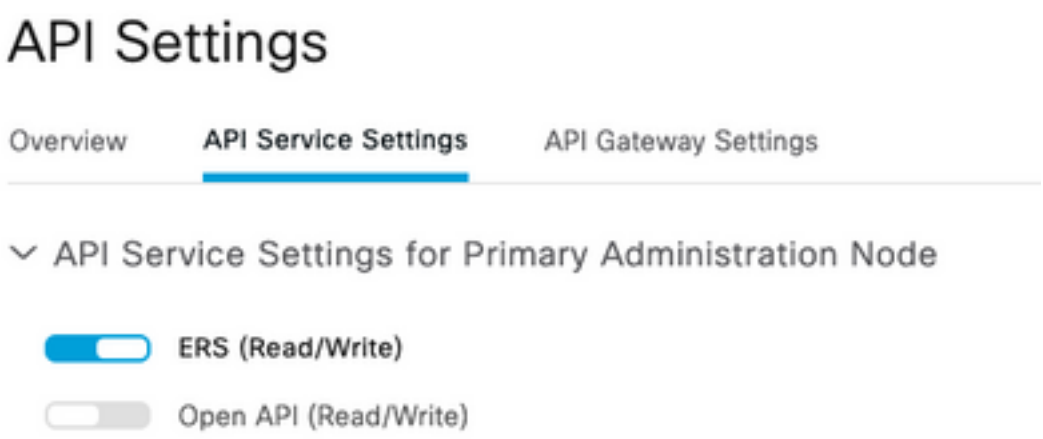
この例では、ISE PANとリモートサーバは直接接続できるように同じサブネットに配置されています。

ISEはオンプレミスデバイスであるため、リモートサーバはSecure-Xクラウドに接続し、情報をISE PANに転送します

設定

ISE PANの設定

1. [Administration] > [System] > [Settings] > [API Settings] > [API Service Settings] に移動し、ERS（読み取り/書き込み）を有効にします。

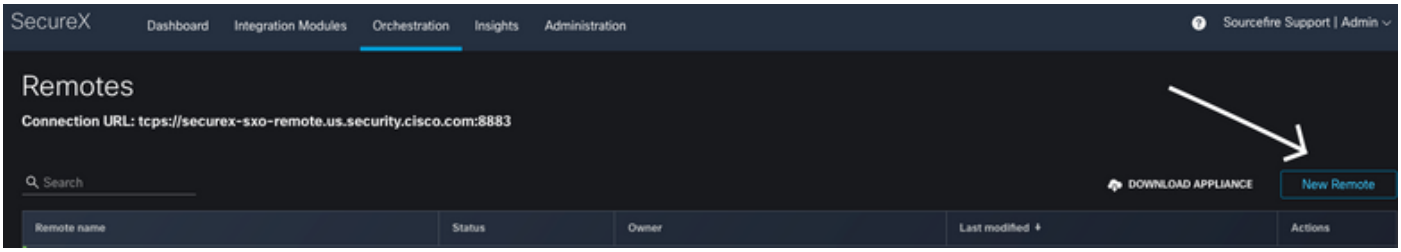


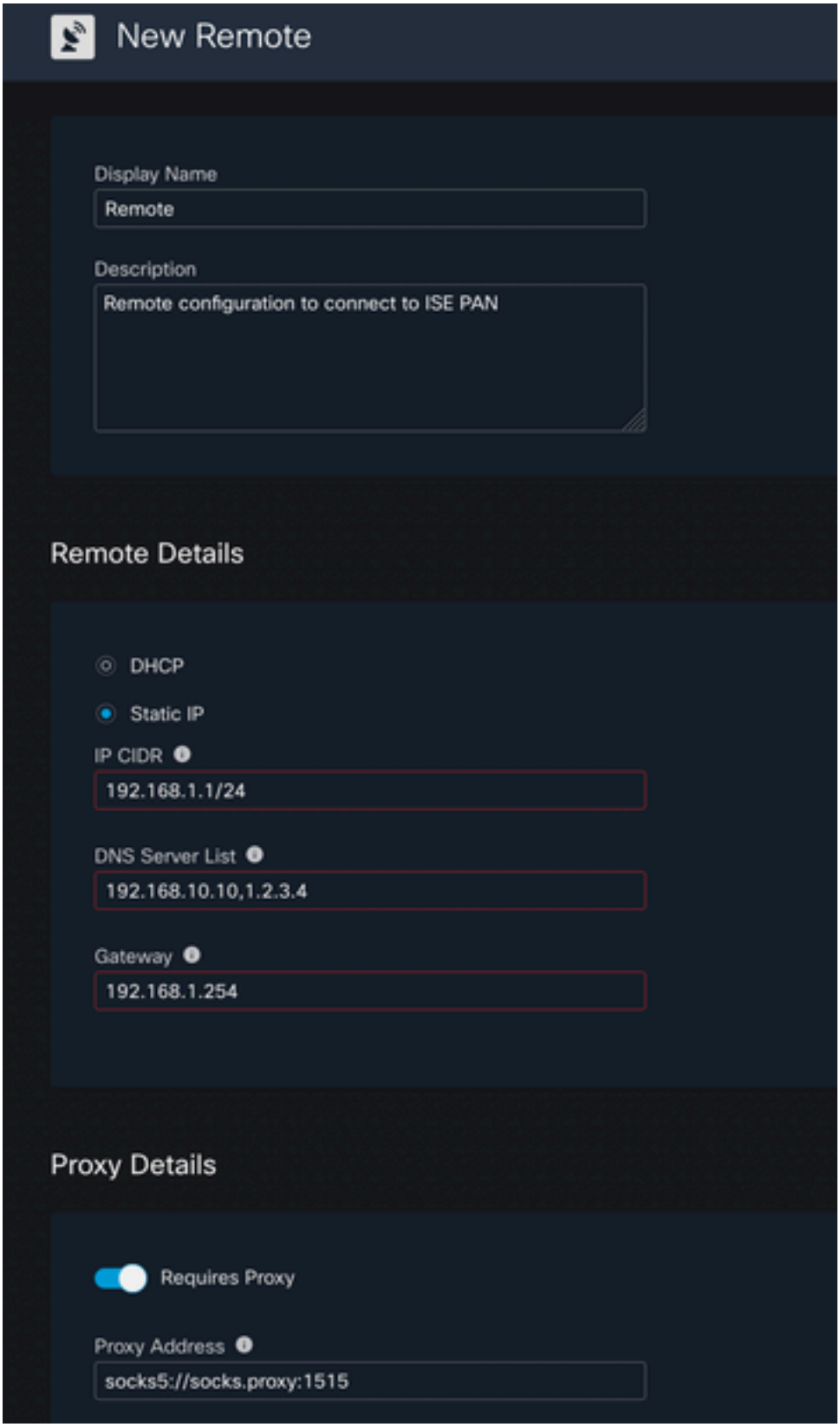
2.（オプション）Secure-X接続用の新しいユーザを作成し、[Administration] > [System] > [Admin Access] > [Administrator] > [Admin Users] に移動して新しいユーザを作成します。この新しいユーザは「ERS Admin」権限を持っている必要があります。あるいは、スーパー管理者ユーザでもかまいません。

リモートサーバーの構成と展開

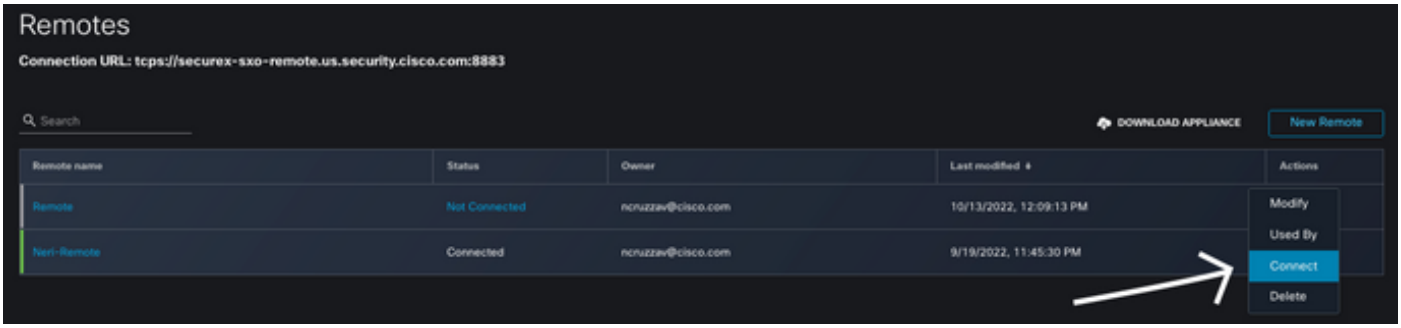
1.リモートサーバを設定し、Secure-Xコンソールで[Orchestration] > [Admin] > [Remote Configuration] に移動し、オプション[New Remote] を選択します。VMの作成時にIPアドレス情報が使用されます。IPアドレス情報は、ISE PANが展開されているサブネットと同じである必要があります。

> **注**：クラウドへの接続がプロキシ経由で行われる場合、現時点では、この目的でサポートされているのはSOCKS5プロキシだけです。

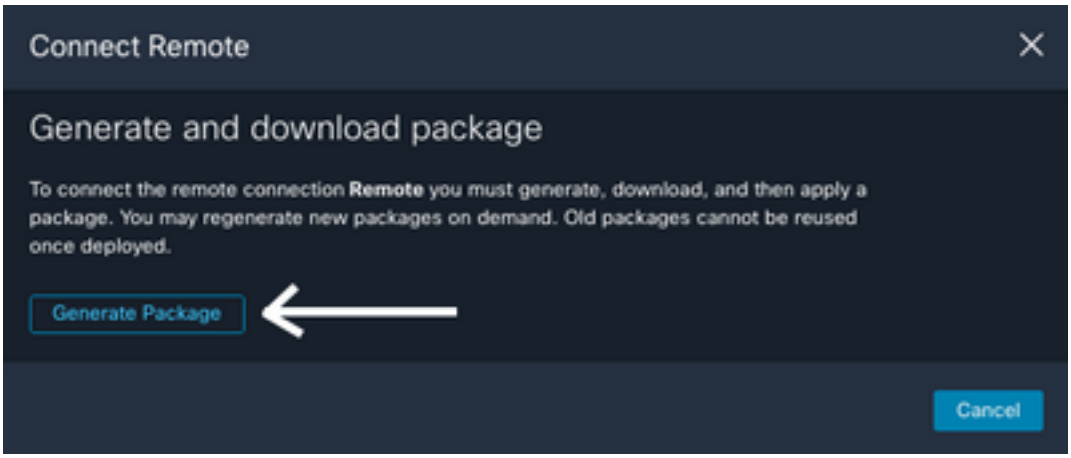




2. VM展開に使用する設定済み設定をダウンロードします。情報が保存されると、リモートは「Not Connected」と表示され、アクションの下に移動して[Connect] を選択します



[Generate Package] を選択すると、VMの導入時に使用するように設定した情報を含む.zipファイルがダウンロードされます。

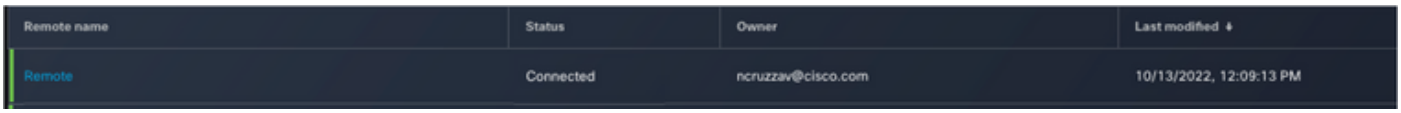


3. VMをダウンロードしてインストールし、[New Remote] の横にある[DOWNLOAD APPLIANCE] を選択します。この操作により、リモートサーバの展開に使用する必要があるOVAイメージがダウンロードされます。

リモートVMの仕様については、『SecureXリモートセットアップ』ガイドを参照してください

VMの作成時には、ZIPファイル内のダウンロードされた情報を**エンコードされたユーザデータ**で使用する必要があります。これにより、サーバの起動時に、設定済みのリモート情報がサーバに入力されます。

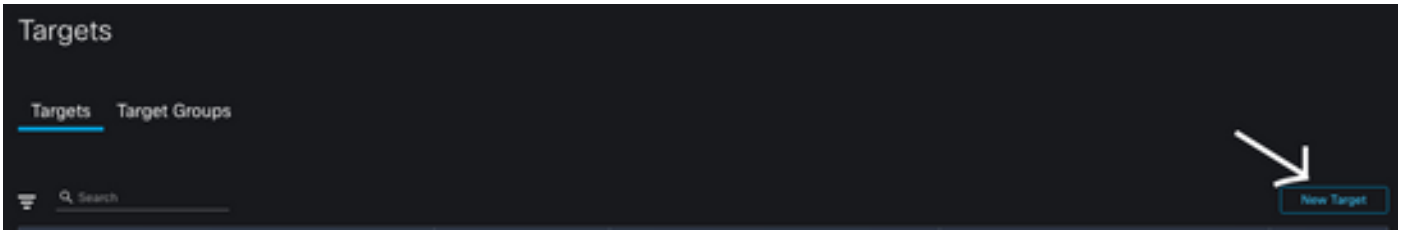
4. VMが起動すると、自動的にSecureXアカウントに接続され、接続が起動していることを確認するため、[Remote]設定で状態が[Connected] に変更されていることを確認する必要があります



SecureXでのターゲットの設定

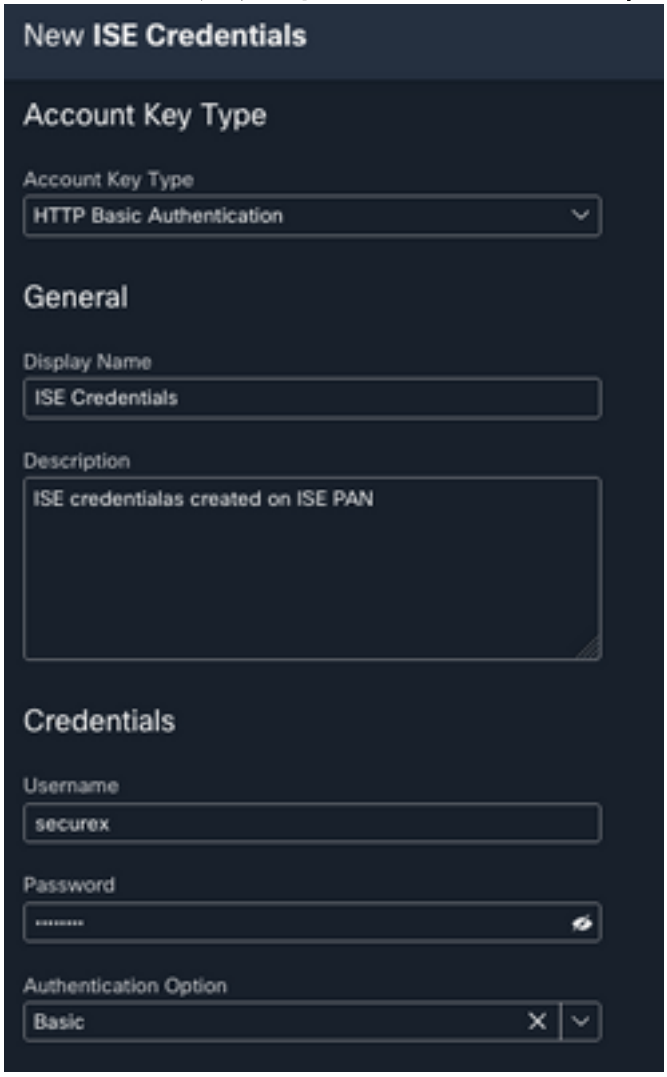
オーケストレーションがデバイスと連携して動作するためには、**ターゲットを設定することが重要です。**Secure Xは、このターゲットを使用してAPIコールを送信し、オーケストレーションを介してデバイスと対話します

1. [Orchestration] > [Targets] > [New Target] に移動します。

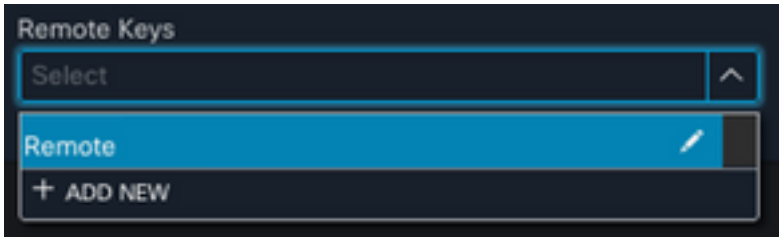


2.ターゲット情報に次のガイドラインを入力します

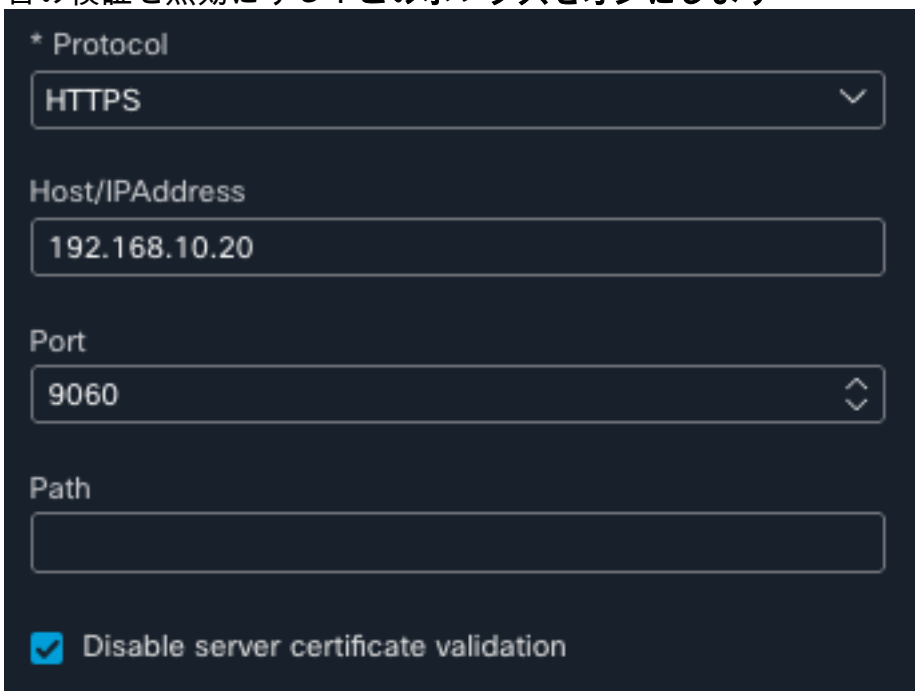
- 表示名:ターゲットID
- 説明:ターゲットの目的を特定するための簡単な説明
- アカウントキー：ここでは、APIを介してISEにアクセスするためのユーザ/パスワードを設定する必要があります アカウントキーなし：**False**既定のアカウントキー：[新規追加（Add New）] を選択します。 アカウントキータイプ：**HTTP基本認証**表示名:アカウントキー識別子ユーザ名:**ISE** PANでERS管理者として作成されたユーザパスワード：**ISE** PANで作成されたユーザのパ**スワード**認証オプション：**基本**



- Remote：ここで、以前に設定したリモート接続を選択する必要があります
  リモートキー：ドロップダウンメニューからリモートを選択します



- HTTP:ここでは、**ISE** PANのAPI情報を設定する必要があります プロトコル:**HTTPS**ホスト/IPアドレス：**ISE PANプライベートIP**[Port]：**9060**Path: 空欄にしておきなさいサーバー証明書の検証を無効にする：**このボックスをオンにします**



- [Proxy]：プロキシ設定はリモート設定に含まれているので、このセクションは空白にしておくことができます
- [送信（Submit）] を選択します。

Cisco Secure GitHubからワークフローをインポートする

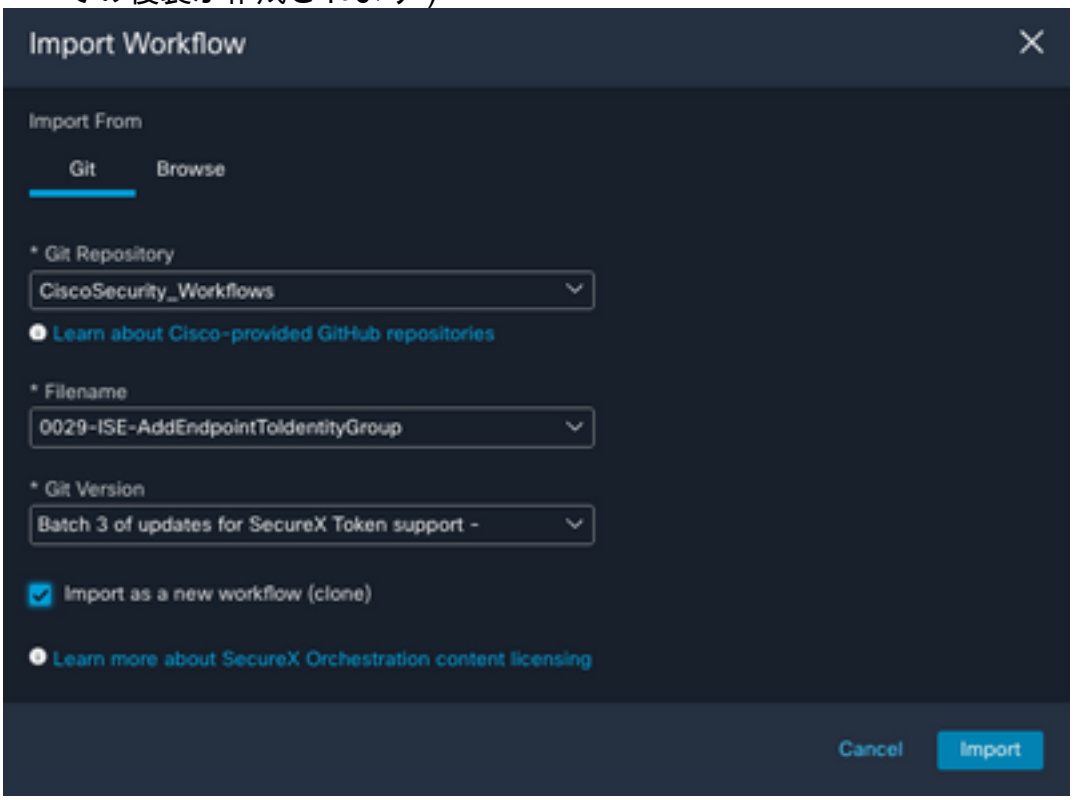
この例では、使用するワークフローは「Add Endpoint to Identity Group」です。Cisco Secure GitHubページにリストされている任意のワークフローを使用するか、カスタムワークフローを作成できます。

1. [Orchestration] > [My Workflows] > [Import Workflow] に移動します。

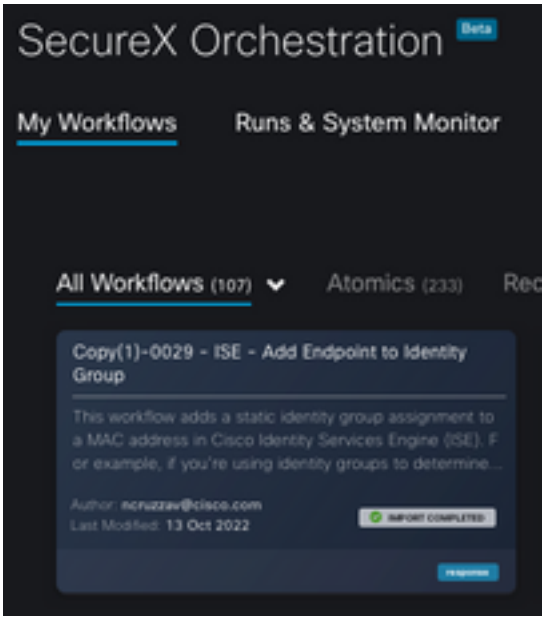
2.ワークフローをインポートするには、次の情報を入力し、[インポート]を選**択します。**インポートするワークフローを特定するには、名前またはワークフロー番号で検索します

- Gitリポジトリ：**CiscoSecurity_Workflows**（ワークフローの場所）
- Filename :**0029-ISE-AddEndpointToIdentityGroup**（使用するワークフローの数を選択）

- Gitバージョン：**SecureXトークンサポートの更新のバッチ3**（最新バージョン）
- 新しいワークフローとしてインポート（複製）:**チェック**（ワークフローがインポートされ、その複製が作成されます）

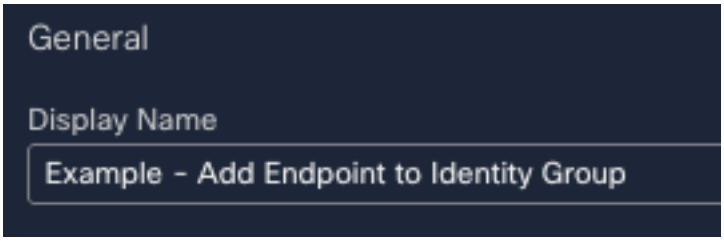


3.インポートすると、新しいテンプレートが[My Workflows] の下に表示されます。作成した新しいワークフローを選択してパラメータを編集し、ISEと連携するように**します**

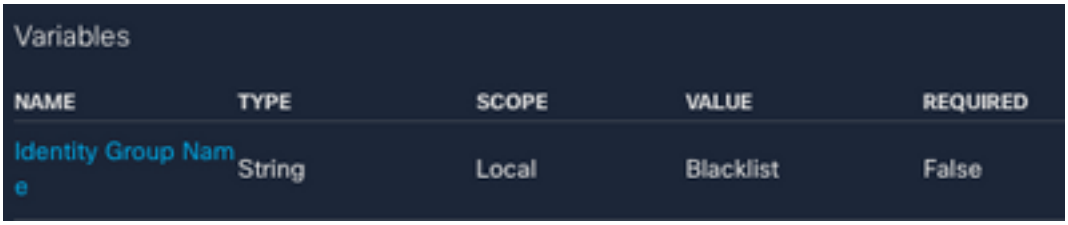


4.これはビルド前のワークフローであるため、ワークフローの3つのセクションを変更するだけで済みます。

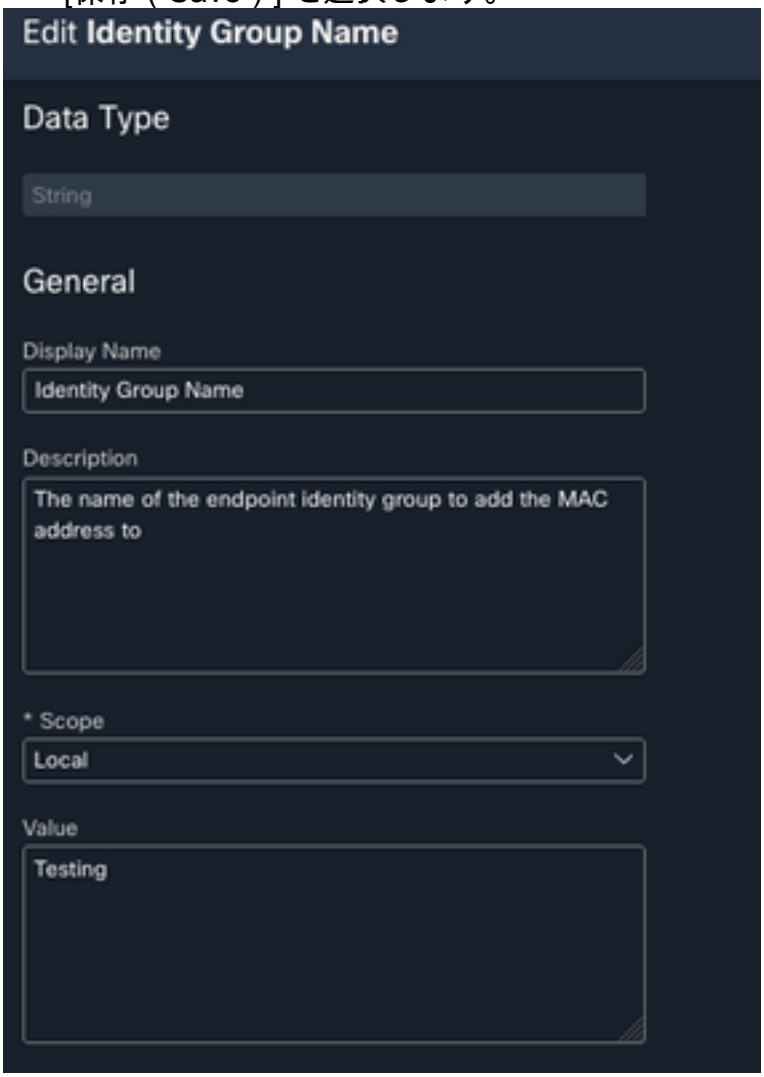
- [名前(Name)]：表示名を変更して、より適切な識別子にします



- IDグループ変数 [Variables]の下で、[Identity Group Variable] をデフォルトで**Balcklist**に編集し、変数を選択して、オーケストレーションで変更するIDグループ名を設定します



- [保存（Save）] を選択します。



- Target:以前に設定した**Target**を設定します ターゲットの種類：**HTTPエンドポイント**
  Target:**構成されたターゲットの名前**

確認

すべてが設定されたら、次にワークフローをテストします

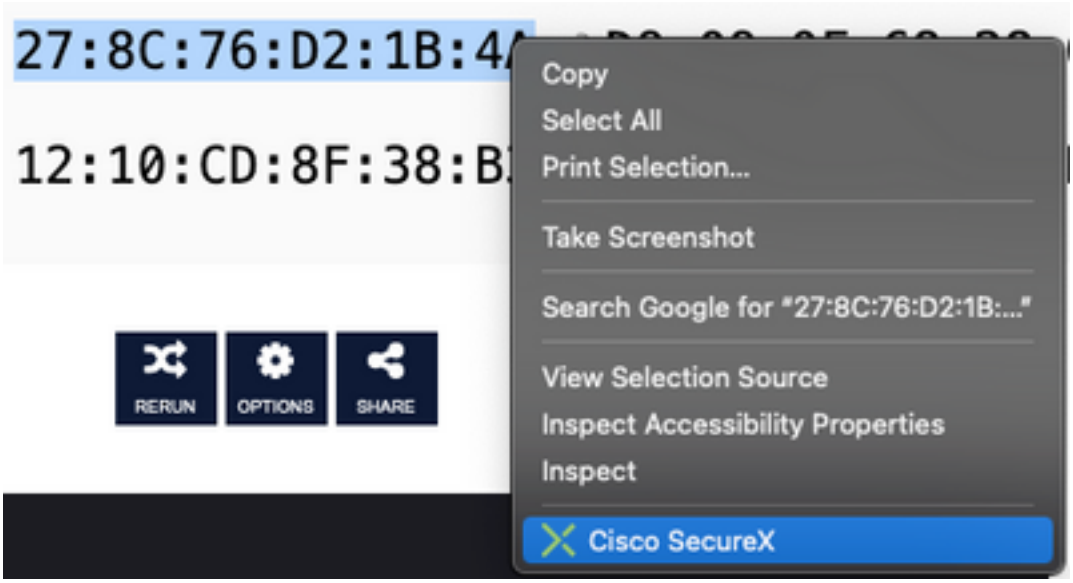
テストのワークフローでは、次のアクションが実行されます。webページにMACアドレスが見つかった場合は、ISE自体か、Threat Responseなどの別のWebページにMACアドレスが存在する可能性があります。secureXブラウザ拡張機能を使用して、ワークフローはAPIを介してISEデータベース内でそのMACアドレスを検索します。MACが存在しない場合は、値をコピーしてISEにアクセスする必要なく、監視可能なMACアドレスがエンドポイントアイデンティティグループに追加されます。

これを実証するために、次の例を見てみましょう。

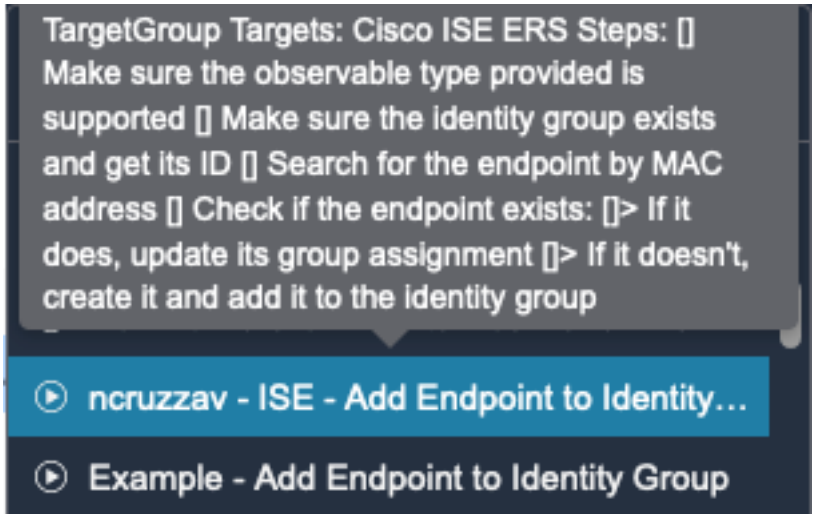
1.選択したワークフローは、監視可能なタイプ「**MACアドレス」で動作します**

2. WebページでMACアドレスを検索し、右クリックを実行します。

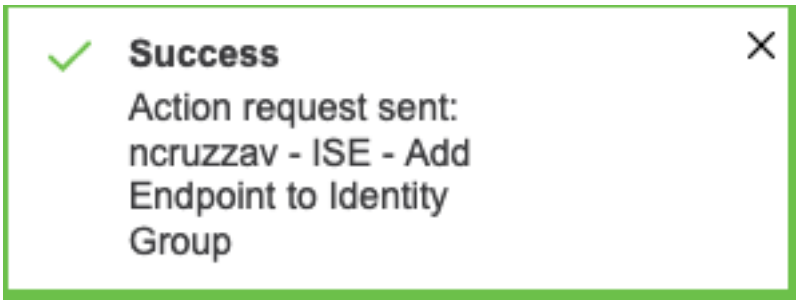
3. [SecureX] オプションを選択します



4.前に作成した**ワークフロー**を選択します

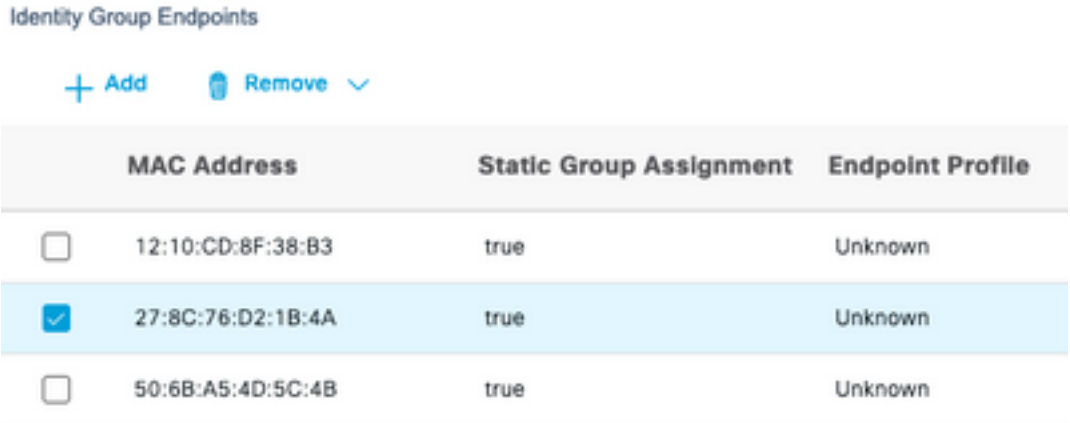


5.タスクが正常に実行されたことを確認します



6. **ISE PAN**で、[Administration] > [Identity Management] > [Groups] > [Endpoint Identity Groups] > （ワークフローで設定されたグループ）に移動します。

7.ワークフローで設定されている**エンドポイントIDグループ**を開き、選択したMACアドレスがそのMACアドレスリストに追加されていることを確認します



翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。