Integration von ISE und SecureX OnPremises durch Orchestrierung

Inhalt

Einleitung

In diesem Dokument werden die Schritte zur Integration von Identity Services Engine und SecureX über die Orchestrierung in einen Workflow vom Cisco Secure GitHub beschrieben.

Voraussetzungen

Cisco empfiehlt, dass Sie über Kenntnisse zu folgenden Themen verfügen:

- Erfahrung mit der Konfiguration der Cisco ISE
- Kenntnisse der ISE-API
- Kenntnisse zu SecureX Orchestrierung

Anforderungen

Sie müssen die Cisco ISE in Ihrem Netzwerk implementiert haben und über ein aktives SecureX-Konto verfügen. Die Orchestrierungs-Workflows werden über die SecureX-Browsererweiterung ausgelöst.

In unserem Beispiel wurde der zu verwendende Workflow von der Seite Cisco Secure GitHub importiert. Dieses Verfahren gilt auch für einen benutzerdefinierten Workflow.

Verwendete Komponenten

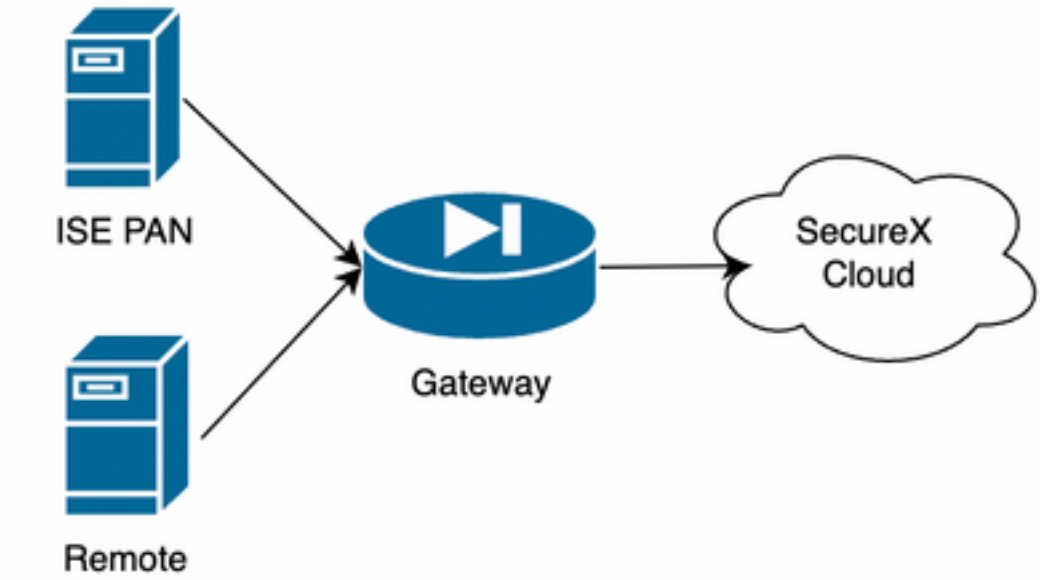
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher,

dass Sie die möglichen Auswirkungen aller Befehle verstehen.

- Identity Services Engine ISE Version 3.1
- SecureX-Konto
- SXO Remote-Gerät Version 1.7

Konfigurieren

Netzwerkdiagramm



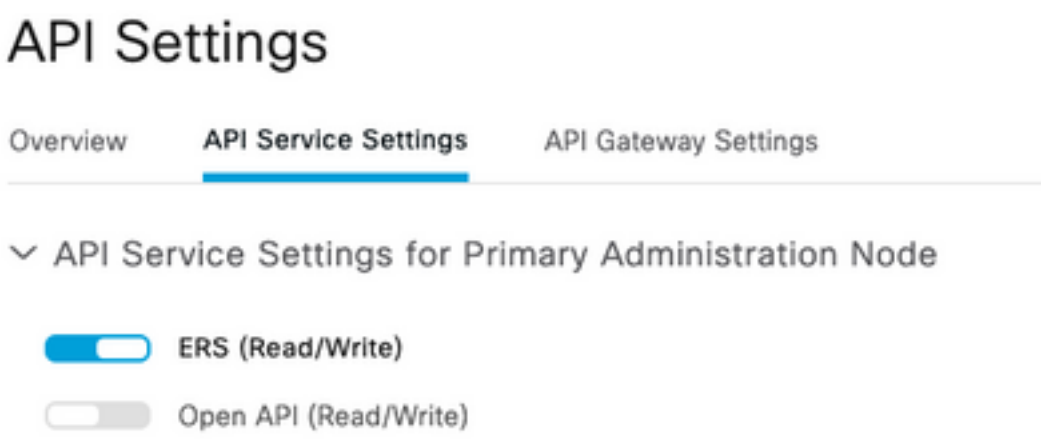
In unserem Beispiel werden ISE PAN und Remote-Server im gleichen Subnetz platziert, um eine direkte Verbindung zu haben.

Da es sich bei der ISE um Geräte vor Ort handelt, muss der Remote-Server mit der Secure-X Cloud in Verbindung stehen und die Informationen an das ISE-PAN weiterleiten.

Konfigurationen

ISE PAN-Konfiguration

1. Navigieren Sie zu **Administration > System > Settings > API Settings > API Service Settings,** und aktivieren Sie **ERS (Read/Write).**

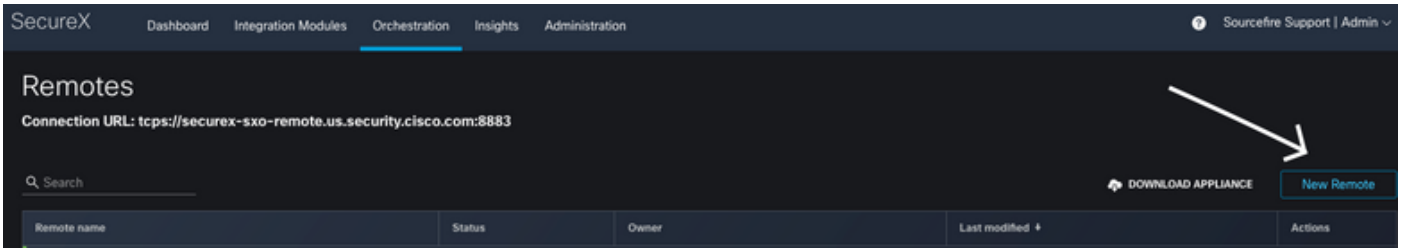


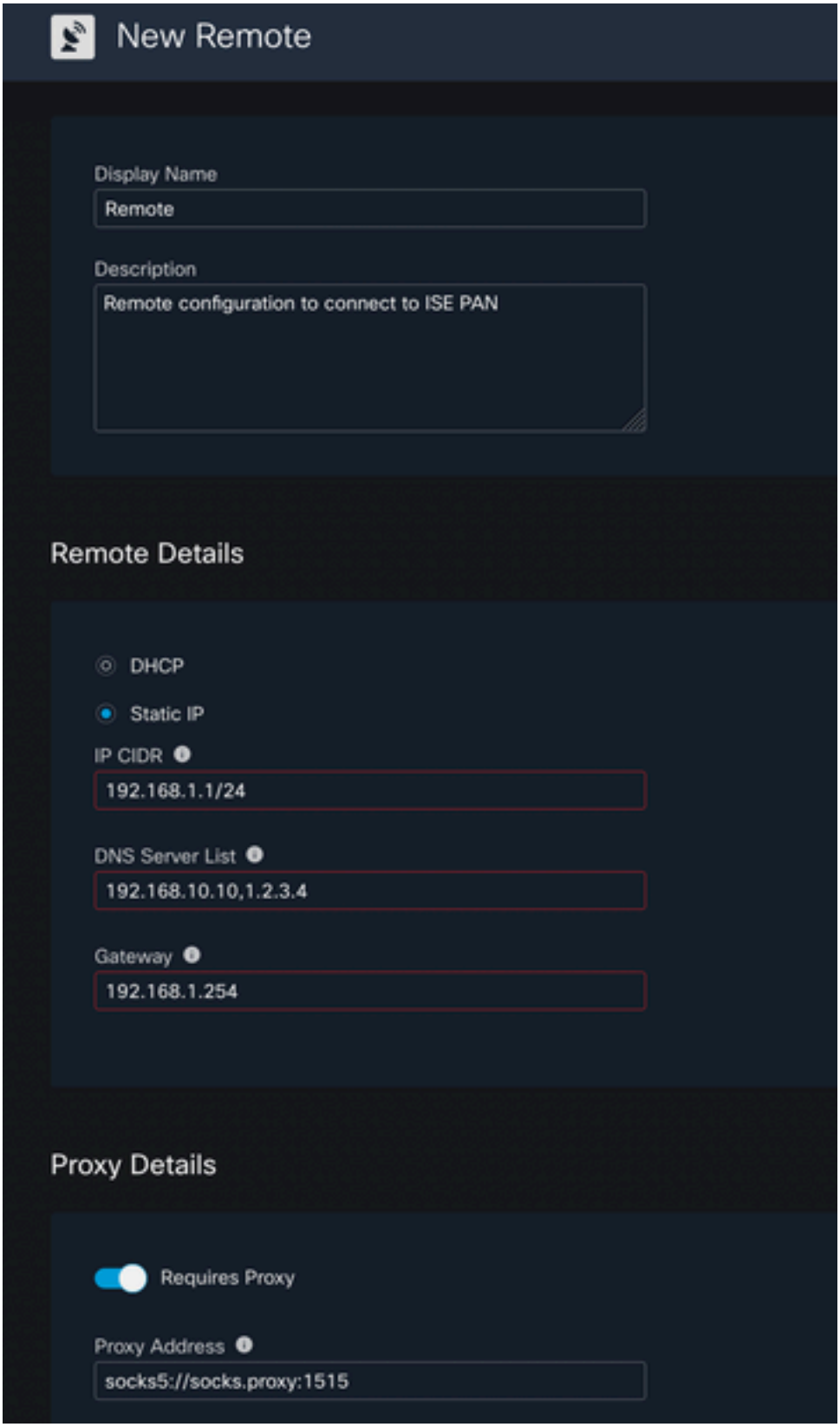
2. (Optional) Erstellen Sie einen neuen Benutzer für die Secure-X-Verbindung, navigieren Sie zu **Administration > System > Admin Access > Administrator > Admin Users,** und erstellen Sie einen neuen Benutzer. Dieser neue Benutzer muss über "ERS Admin"-Berechtigungen verfügen, oder es kann sich um einen Super-Admin-Benutzer handeln.

Remote-Server konfigurieren und bereitstellen

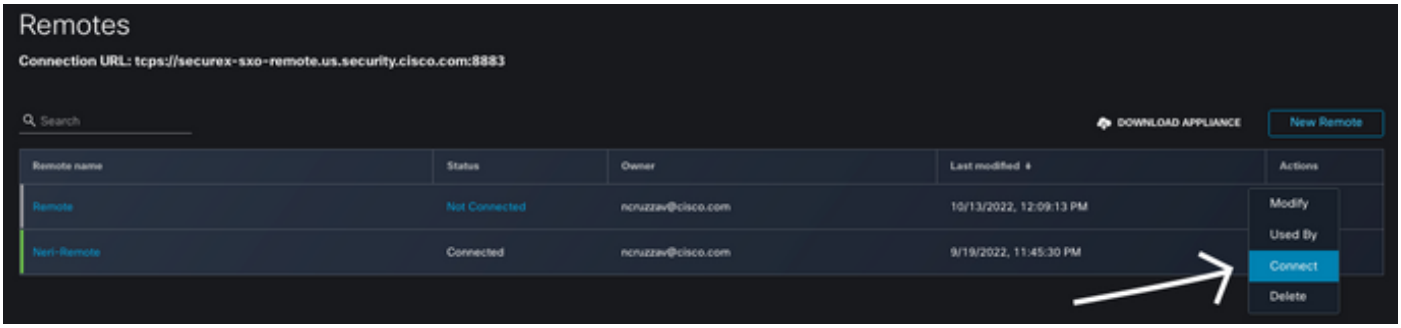
1. Konfigurieren Sie den Remote-Server. Navigieren Sie in der Secure-X-Konsole zu **Orchestrierung > Admin > Remote Configuration,** und wählen Sie die Option **New Remote.** Die IP-Adressinformationen werden beim Erstellen der VM verwendet. Sie müssen sich im gleichen Subnetz befinden, in dem das ISE PAN bereitgestellt wird.

> **Anmerkung:** Wenn die Verbindung zur Cloud über einen Proxy erfolgt, wird derzeit nur ein SOCKS5-Proxy für diesen Zweck unterstützt.

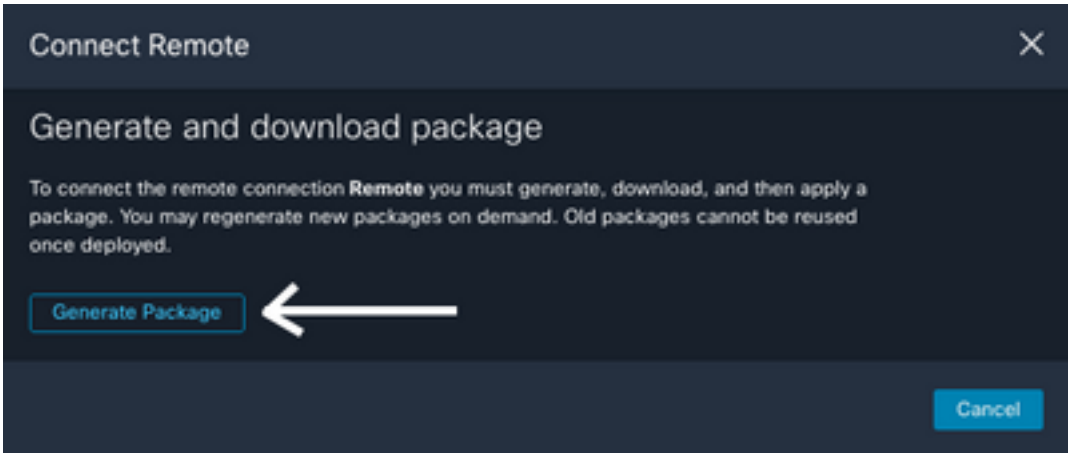




2. Laden Sie die konfigurierten Einstellungen herunter, die für die VM-Bereitstellung verwendet werden sollen. Sobald die Informationen gespeichert sind, wird die Remote-Verbindung als **"Not Connected" (Nicht verbunden) angezeigt,** navigieren Sie unter Aktionen, und wählen Sie **Verbinden** aus.



Wählen Sie **Paket generieren,** um mit dieser Aktion eine ZIP-Datei herunterzuladen, die die Informationen enthält, die gerade für die Verwendung bei der Bereitstellung der VM konfiguriert wurden.

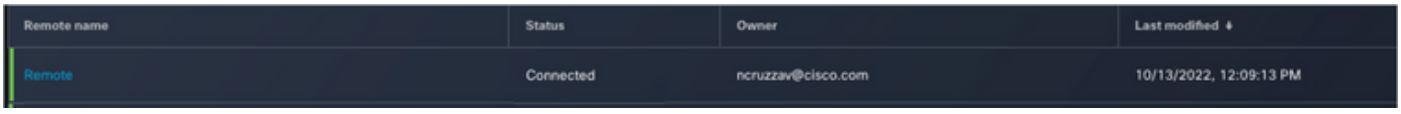


3. Laden Sie das virtuelle System herunter und installieren Sie es. Wählen Sie neben **"New Remote" die Option "APPLIANCE HERUNTERLADEN".** Mit dieser Aktion wird ein OVA-Image heruntergeladen, das Sie zum Bereitstellen des Remote-Servers verwenden müssen.

Informationen zu den VM-Spezifikationen für Remote-Standorte finden Sie im SecureX Remote Setup-Leitfaden.

Die heruntergeladenen Informationen in der ZIP-Datei müssen beim Erstellen der VM auf den **codierten Benutzerdaten** verwendet werden. Dadurch wurden die konfigurierten Remote-Informationen nach dem Start in den Server übernommen.

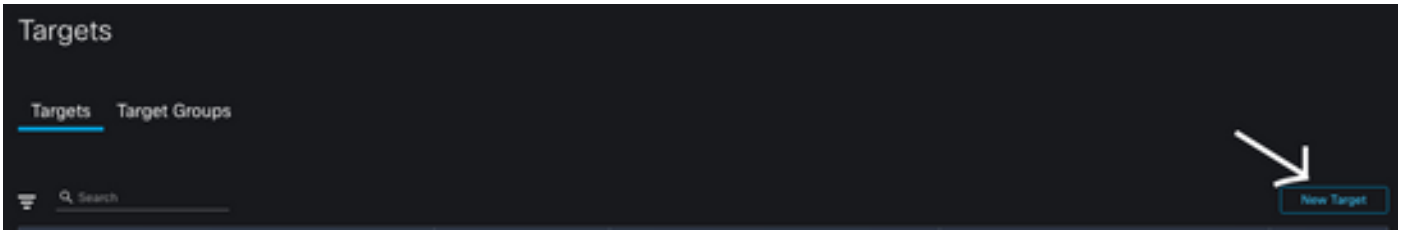
4. Sobald die VM aktiv ist, stellt sie automatisch eine Verbindung mit dem SecureX-Konto her, um zu überprüfen, ob die Verbindung aktiv ist. In der Remote-Konfiguration muss der Status auf **"Verbunden" geändert werden.**



Konfigurieren des Ziels auf SecureX

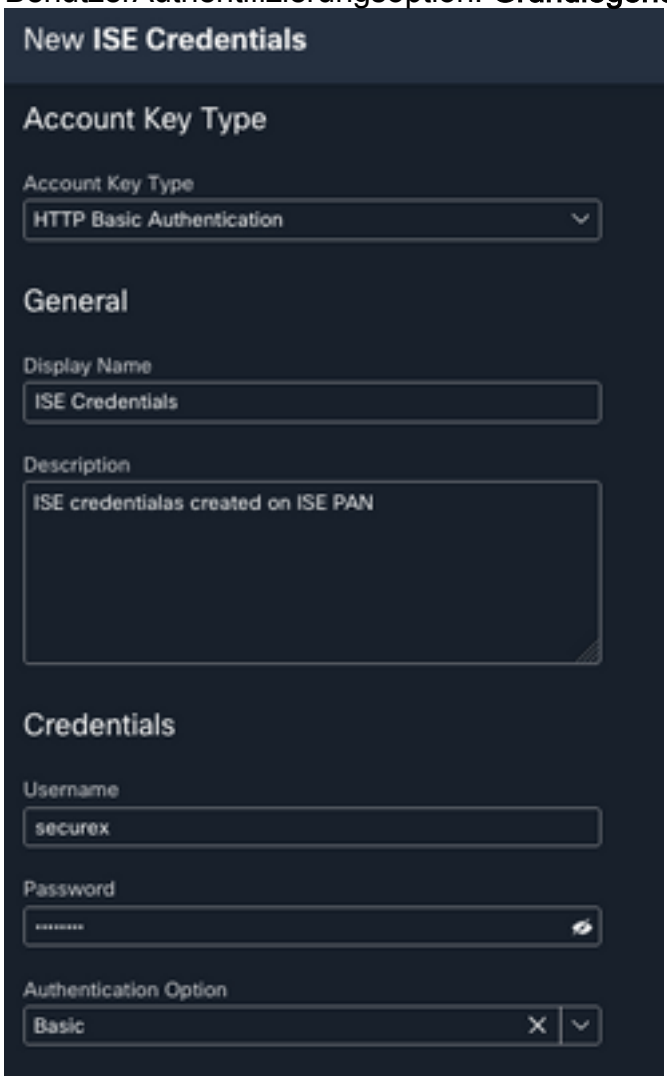
Damit die Orchestrierung mit einem Gerät funktioniert, ist es wichtig, ein **Ziel** zu konfigurieren. Secure X verwendet dieses Ziel, um die API-Anrufe zu senden und über die Orchestrierung mit dem Gerät zu interagieren.

1. Navigieren Sie zu **Orchestrierung > Ziele > Neues Ziel**

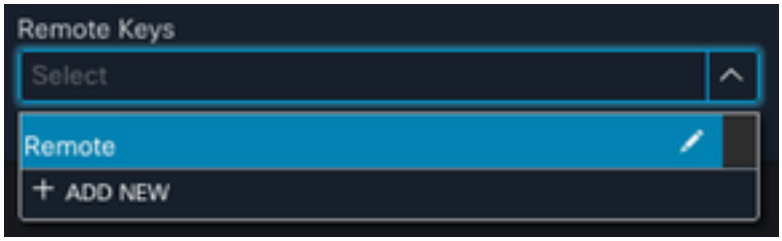


2. Tragen Sie die Zielinformationen in die nächsten Richtlinien ein

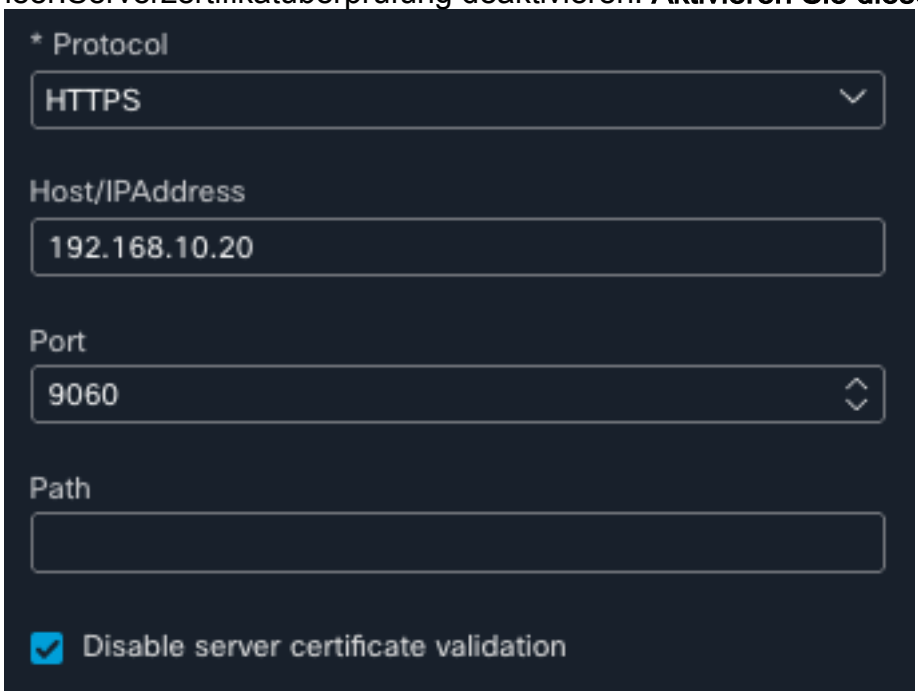
- Anzeigename: Zielkennung
- Beschreibung: Eine kurze Beschreibung zur Bestimmung des Ziels
- Kontoschlüssel: Hier müssen Sie den Benutzer/das Kennwort für den Zugriff auf die ISE über die API konfigurieren. Keine Kontoschlüssel: **Falsch**Standardkontenschlüssel: **Neu hinzufügen** auswählen Kontoschlüsseltyp: **Grundlegende HTTP-Authentifizierung**Anzeigename: Kontenschlüssel-IDBenutzername: Benutzer erstellt auf **ISE PAN** als ERS-AdministratorKennwort: Kennwort für den auf **ISE PAN** erstellten BenutzerAuthentifizierungsoption: **Grundlegend**



- Remote: Hier müssen Sie die zuvor konfigurierte Remote-Verbindung auswählen. Remote-Schlüssel: Wählen Sie Ihre Fernbedienung im Dropdown-Menü aus.



- HTTP: Hier müssen Sie die API-Informationen für den **ISE PAN** konfigurieren. Protokolle: **HTTPS**Host-/IP-Adresse: **ISE PAN, private IP**Anschluss: **9060**Pfad: Lassen Sie das Feld leer.Serverzertifikatüberprüfung deaktivieren: **Aktivieren Sie dieses Kontrollkästchen.**



- Proxy: Da die Proxy-Konfiguration in der Remote-Konfiguration enthalten war, können Sie diesen Abschnitt leer lassen.
- **Senden** auswählen

Workflow aus Cisco Secure GitHub importieren

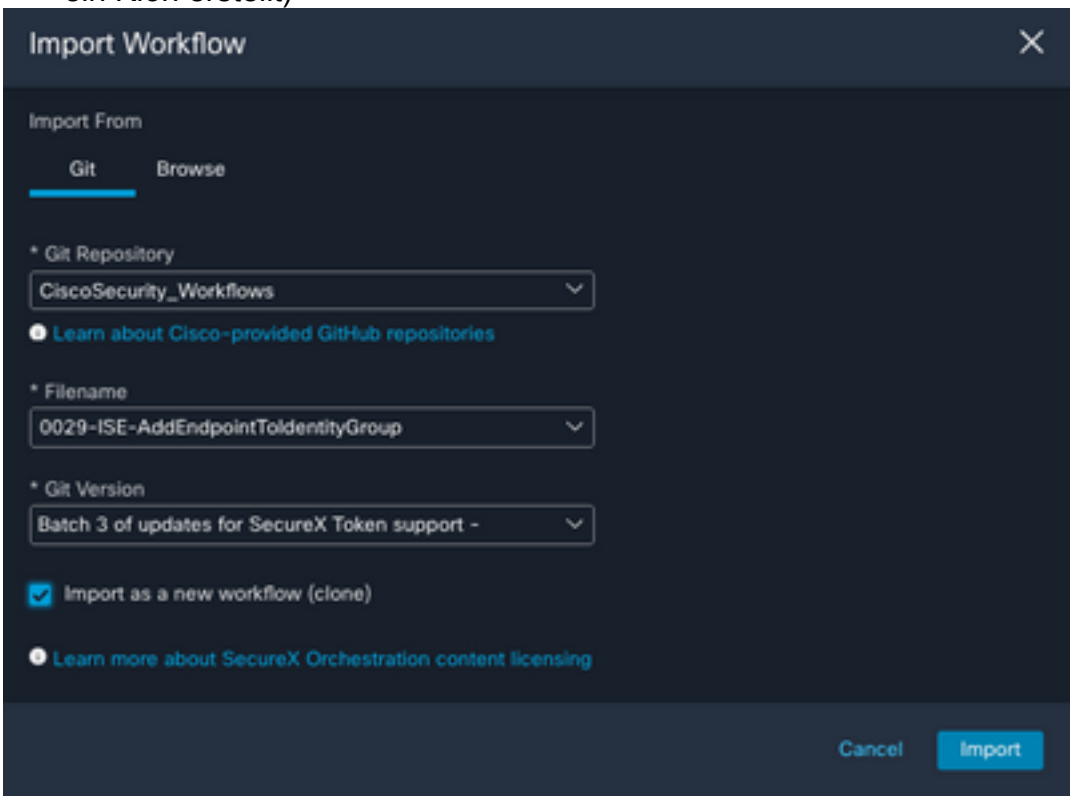
Für dieses Beispiel lautet der zu verwendende Workflow "Endpunkt zur Identitätsgruppe hinzufügen". Sie können alle aufgeführten Workflows auf der Seite "Cisco Secure GitHub" verwenden oder einen benutzerdefinierten Workflow erstellen.

1. Navigieren Sie zu **Orchestrierung > Meine Workflows > Workflow importieren**

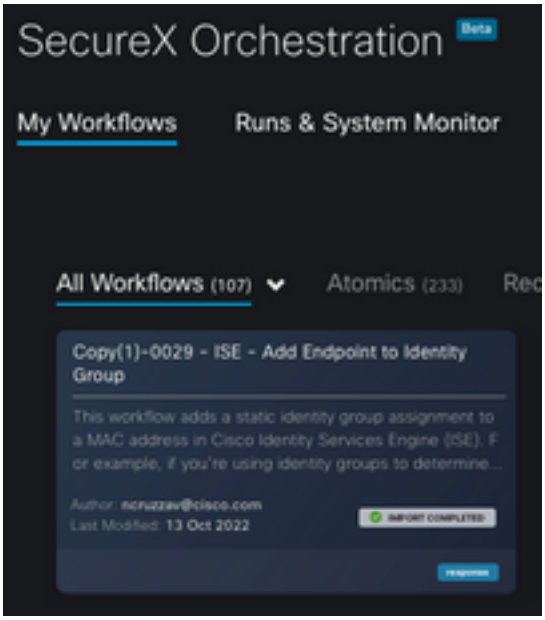
2. Um den Workflow zu importieren, füllen Sie die Informationen wie folgt aus, und wählen Sie **Importieren.** zum Identifizieren des zu importierenden Workflows können Sie nach Namen oder nach Workflownummer suchen.

- Git-Repository: **CiscoSecurity_Workflows** (Speicherort des Workflows)

- Dateiname: **0029-ISE-AddEndpointToIdentityGroup** (Wählen Sie die Anzahl der zu verwendenden Workflows aus.)
- Git-Version: **Batch 3 mit Updates für SecureX Token Support** (Neueste Version)
- Als neuen Workflow importieren (Klon): **Aktivieren** (Dadurch wird der Workflow importiert und ein Klon erstellt)

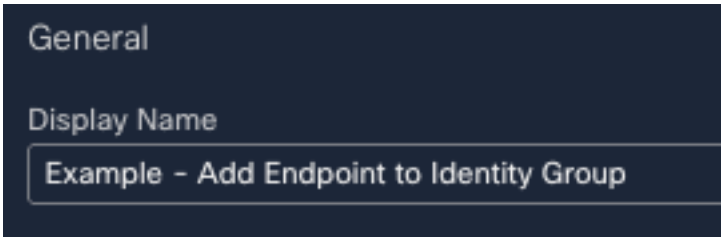


3. Nach dem Import wird die neue Vorlage unter **Meine Workflows** angezeigt. Wählen Sie den neu erstellten Workflow aus, um die Parameter zu bearbeiten, damit er mit **ISE** funktioniert.

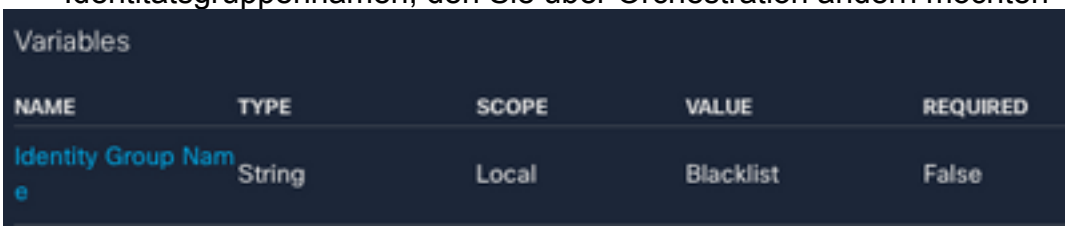


4. Da es sich um einen vorab erstellten Workflow handelt, müssen Sie nur drei Abschnitte des Workflows ändern:

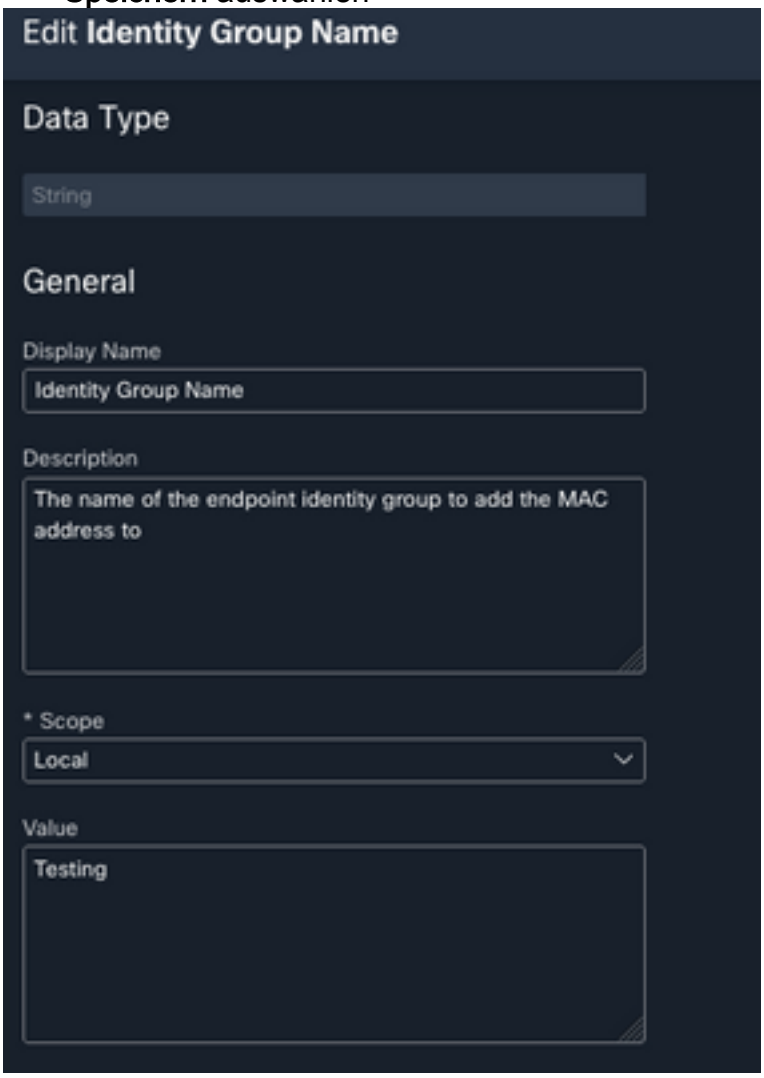
- Name: Ändern Sie den Anzeigenamen, um eine bessere Kennzeichnung zu erhalten.



- Identitätsgruppenvariable Bearbeiten Sie unter Variablen die **Identitätsgruppenvariable** standardmäßig **Balcklist,** wählen Sie die Variable aus, und konfigurieren Sie den Identitätsgruppennamen, den Sie über Orchestration ändern möchten



- **Speichern** auswählen



- Ziel: Konfigurieren Sie das zuvor konfigurierte **Ziel.** Zieltyp: **HTTP-Endpunkt**Ziel: **Name des konfigurierten Ziels**

Überprüfung

Ist alles konfiguriert, ist Zeit, den Workflow zu testen

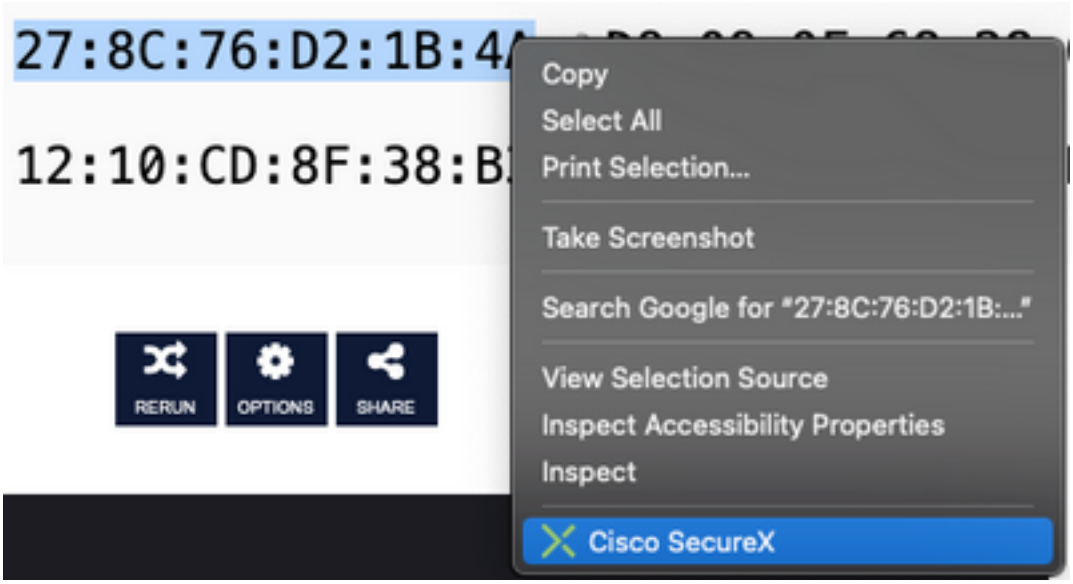
Der Workflow für den Test führt diese Aktion aus: Wenn Sie eine MAC-Adresse auf einer Webseite finden, kann diese sich auf der ISE selbst oder auf einer anderen Webseite wie Threat Response befinden. über die SecureX-Browsererweiterung sucht der Workflow über eine API in der ISE-Datenbank nach dieser MAC-Adresse. Wenn die MAC-Adresse nicht vorhanden ist, wird die beobachtbare Adresse der Endpoint Identity Group hinzugefügt, ohne dass der Wert und der Zugriff auf die ISE kopiert werden müssen.

Um dies zu veranschaulichen, sehen Sie sich das folgende Beispiel an:

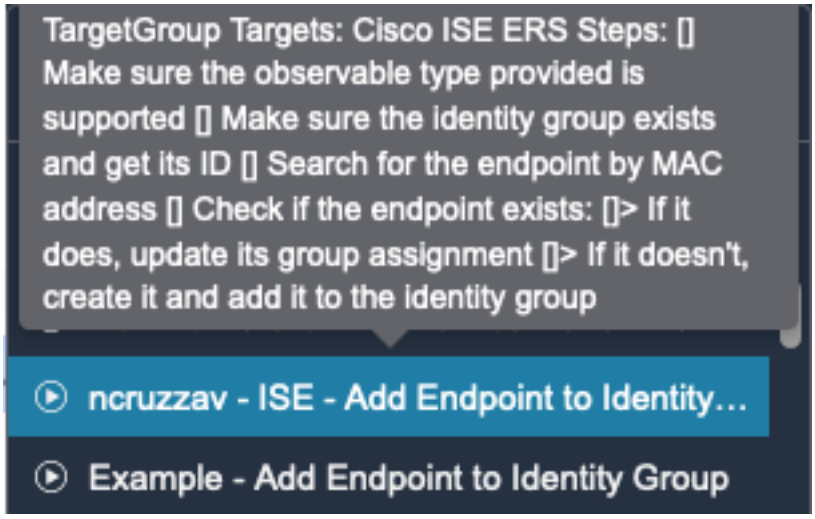
1. Der ausgewählte Workflow funktioniert mit dem beobachtbaren Typ "**MAC-Adresse**"

2. Suchen Sie eine MAC-Adresse auf einer Webseite, und klicken Sie mit der rechten Maustaste darauf.

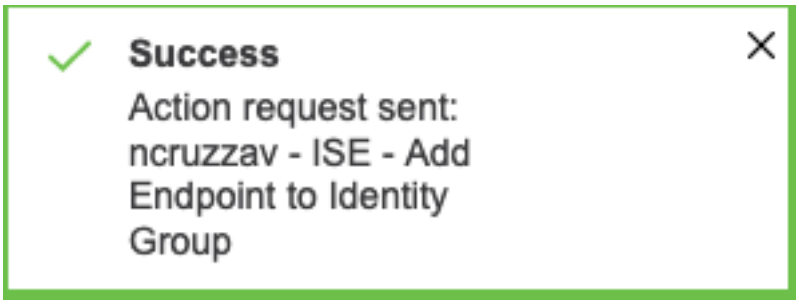
3. Wählen Sie die Option **SecureX**



4. Wählen Sie den zuvor erstellten **Workflow**

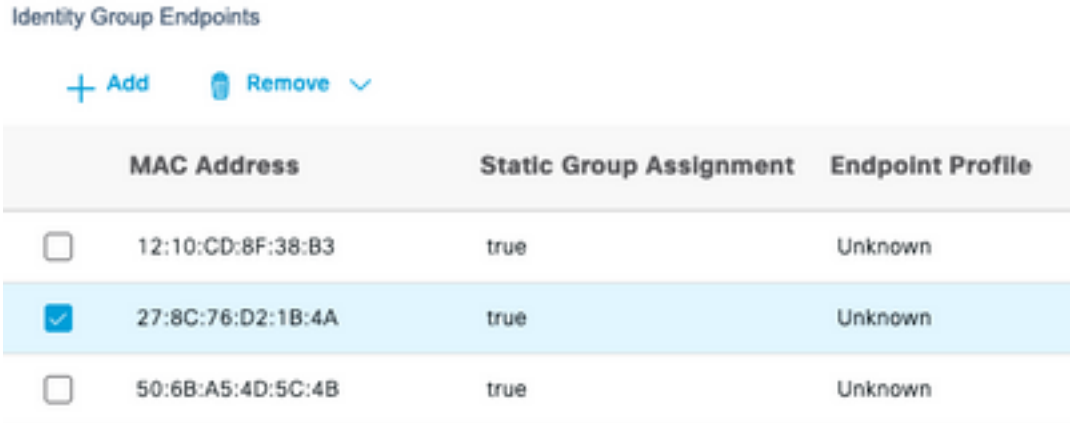


5. Bestätigen Sie, dass die Aufgabe erfolgreich ausgeführt wurde.



6. Navigieren Sie auf dem **ISE-PAN** zu **Administration > Identity Management > Groups > Endpoint Identity Groups > (Die im Workflow konfigurierte Gruppe).**

7. Öffnen Sie die im Workflow konfigurierte **Endpunkt-Identitätsgruppe,** und bestätigen Sie, dass die ausgewählte MAC-Adresse dieser MAC-Adressliste hinzugefügt wurde.



Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.