# Integrazione di ISE e SecureX OnPremises attraverso l'orchestrazione

## Sommario

[Introduzione](#)
[Prerequisiti](#)
[Requisiti](#)
[Componenti usati](#)
[Configurazione](#)
[Esempio di rete](#)
[Configurazioni](#)
[ISE PAN configuration](#)
[Configurare e distribuire il server remoto](#)
[Configurazione della destinazione su SecureX](#)
[Importa il flusso di lavoro da Cisco Secure GitHub](#)
[Verifica](#)

## Introduzione

In questo documento viene descritto come integrare Identity Services Engine e SecureX tramite orchestrazione con un flusso di lavoro di Cisco Secure GitHub.

## Prerequisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Esperienza nella configurazione di Cisco ISE
- Conoscenza dell'API ISE
- Conoscenze sull'orchestrazione SecureX

### Requisiti

Ènecessario avere Cisco ISE implementato nella rete e avere un account SecureX attivo. I flussi di lavoro di orchestrazione vengono attivati tramite l'estensione del browser SecureX.

Nell'esempio il flusso di lavoro da utilizzare è stato importato dalla pagina Cisco Secure GitHub. Questa procedura è valida anche per un flusso di lavoro personalizzato.

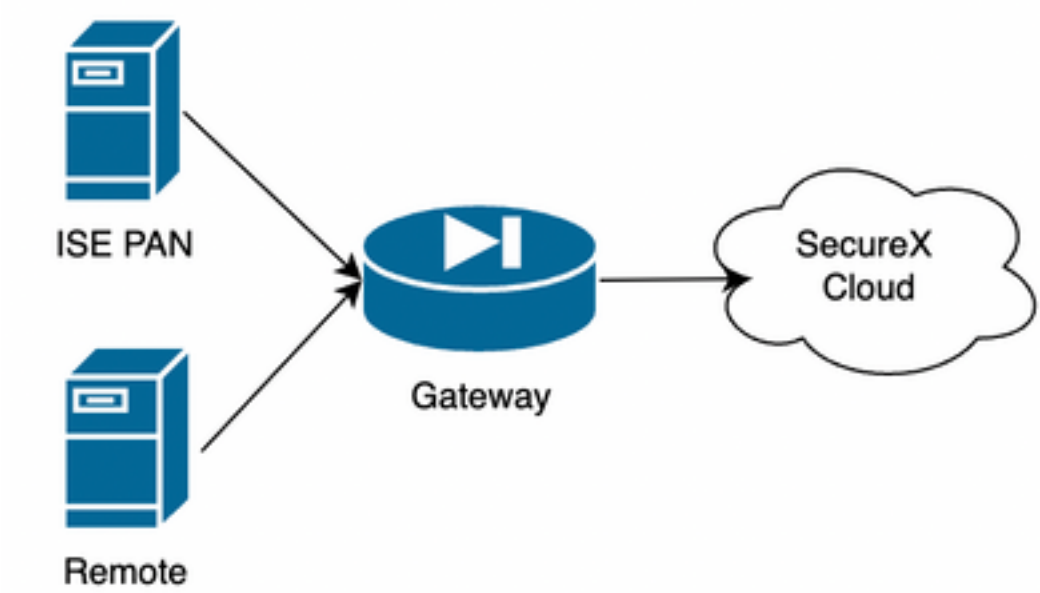
### Componenti usati

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

- Identity Services Engine ISE versione 3.1
- Account SecureX
- Dispositivo remoto SXO versione 1.7

# Configurazione

## Esempio di rete



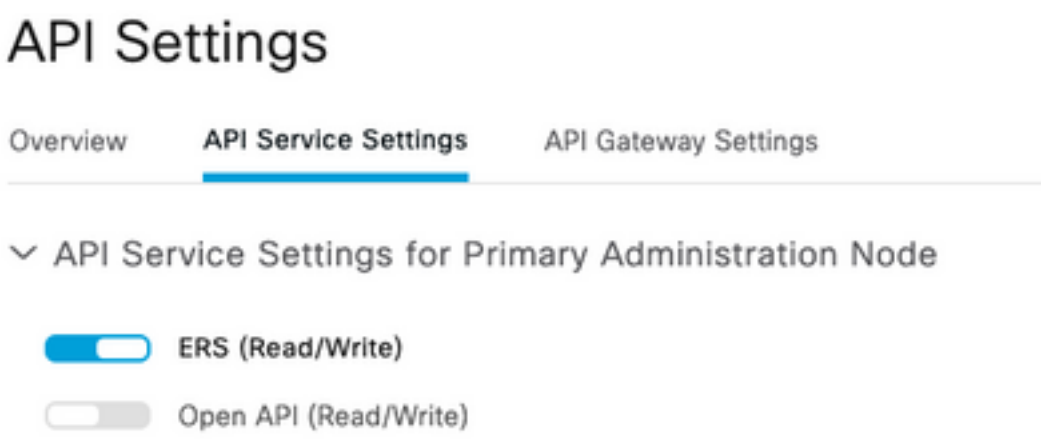

Nell'esempio riportato, ISE PAN e il server remoto si trovano nella stessa subnet per avere una connettività diretta.

Poiché ISE è un dispositivo locale, il server remoto deve connettersi al cloud Secure-X e inoltrare le informazioni alla PAN di ISE

## Configurazioni

### ISE PAN configuration

1. Passare a **Amministrazione > Sistema > Impostazioni > Impostazioni API > Impostazioni servizi API** e abilitare **ERS (Lettura/scrittura)**

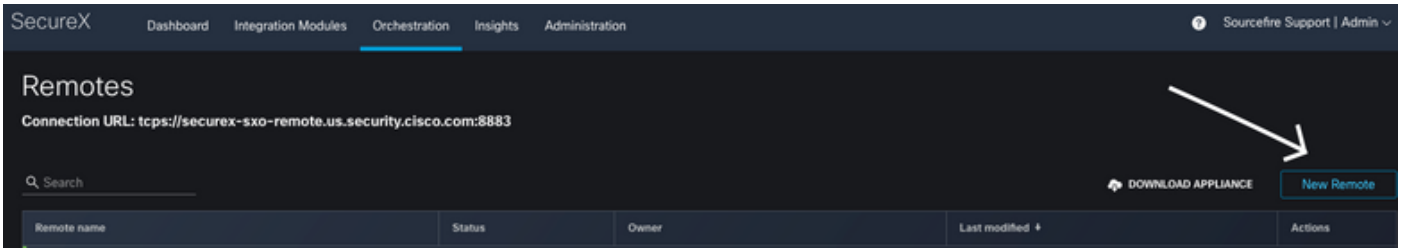


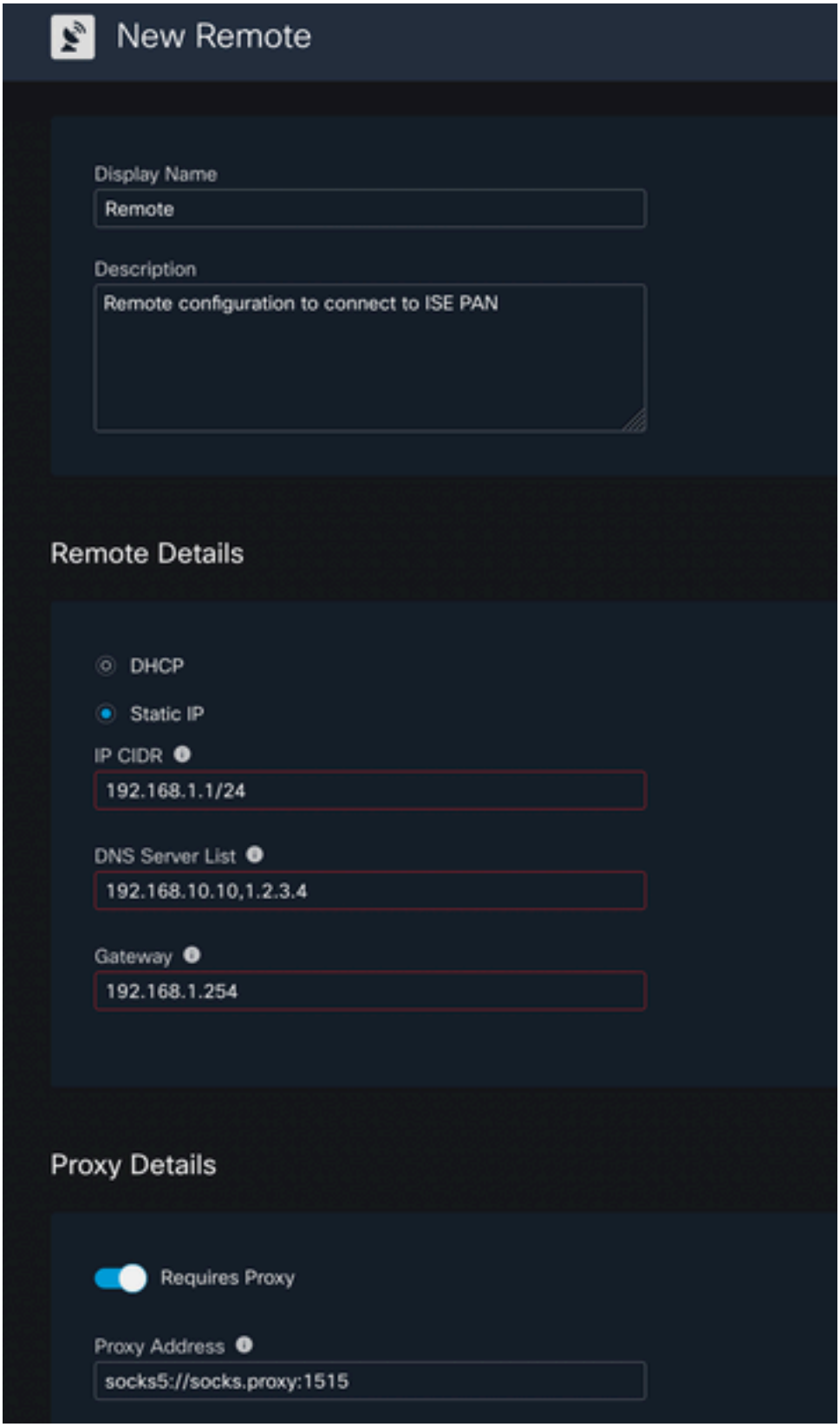

2. (Facoltativo) Creare un nuovo utente per la connessione Secure-X, selezionare **Amministrazione > Sistema > Accesso amministratore > Amministratore > Utenti amministratori** e creare un nuovo utente. Questo nuovo utente deve disporre delle autorizzazioni "Amministratore ERS" o può essere un utente con privilegi di amministratore privilegiato.

### Configurare e distribuire il server remoto

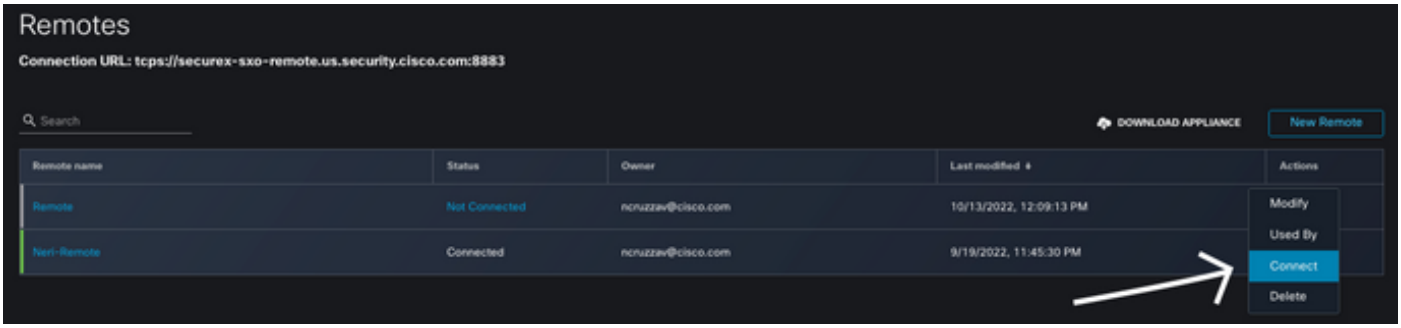
1. Configurare il server remoto. Nella console Secure-X passare a **Orchestrazione > Amministrazione > Configurazione remota** e selezionare l'opzione **Nuovo remoto. Le informazioni sull'indirizzo IP sono quelle da utilizzare al momento della creazione della VM e devono trovarsi nella stessa subnet in cui è distribuita la PAN ISE.**

> **Nota:** Se la connessione al cloud avviene tramite un proxy, attualmente solo un proxy SOCKS5 è supportato per questo scopo.

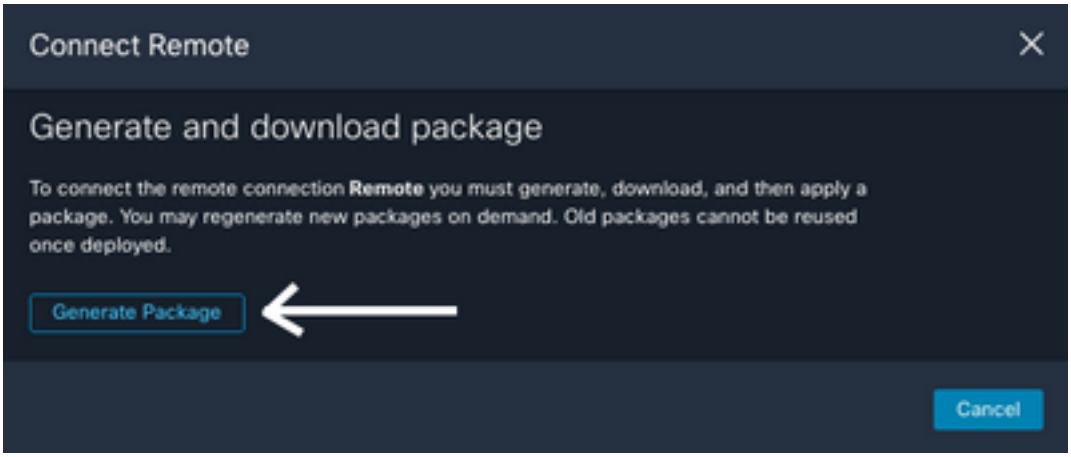





2. Scaricare le impostazioni configurate da utilizzare per la distribuzione della VM. Una volta salvate le informazioni, il telecomando viene visualizzato come "**Non connesso**", passare alla sezione Azioni e selezionare **Connetti**




Selezionare **Genera pacchetto,** questa azione consente di scaricare un file .zip contenente le informazioni appena configurate per l'utilizzo durante la distribuzione della macchina virtuale.




3. Scaricare e installare la VM, accanto a **Nuovo dispositivo remoto** selezionare **DOWNLOAD APPLIANCE** questa azione consente di scaricare un'immagine OAV che è necessario utilizzare per distribuire il server remoto.

Per le specifiche delle VM remote, fare riferimento alla guida SecureX Remote Setup (Impostazione remota SecureX)

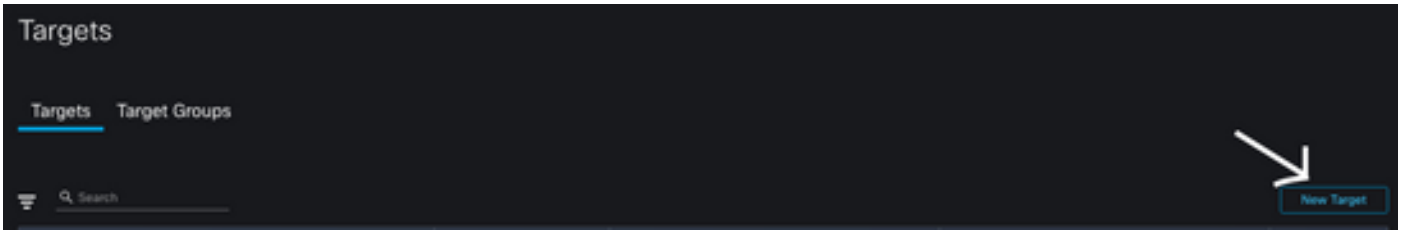
Le informazioni scaricate all'interno del file ZIP devono essere utilizzate nei **dati utente codificati** al momento della creazione della VM. Le informazioni remote configurate vengono inserite nel server una volta avviato.

4. Una volta attivata, la VM si connette automaticamente all'account SecureX per verificare che la connessione sia attiva. In Configurazione remota è necessario visualizzare un cambiamento dello stato in **"Connesso"**


## Configurazione della destinazione su SecureX

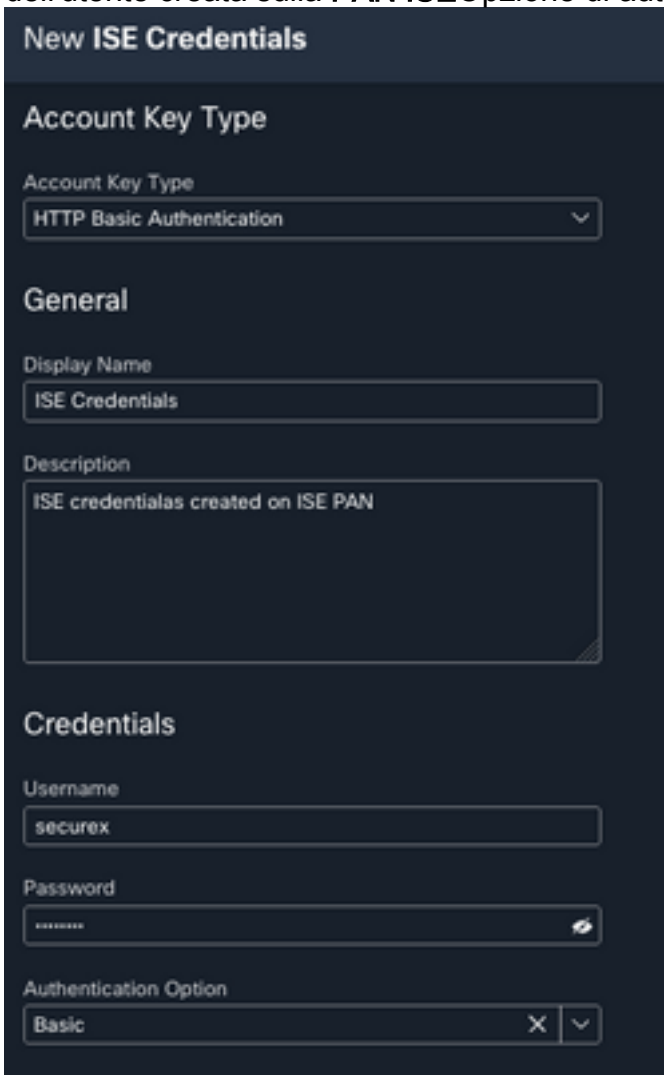
Affinché l'orchestrazione funzioni con un dispositivo è importante per configurare una **destinazione,** Secure X utilizza questa destinazione per inviare le chiamate API e interagire con il dispositivo tramite l'orchestrazione

1. Passare a **Orchestrazione > Oggetti > Nuovo oggetto**

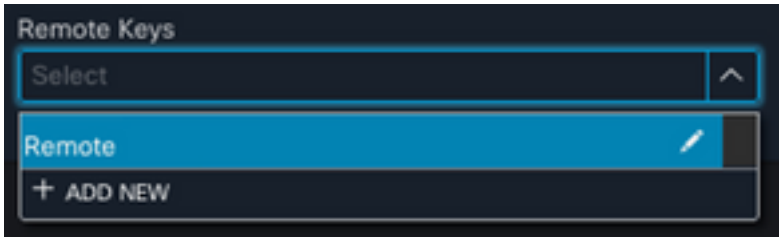



2. Inserire le informazioni sull'obiettivo nelle linee guida successive

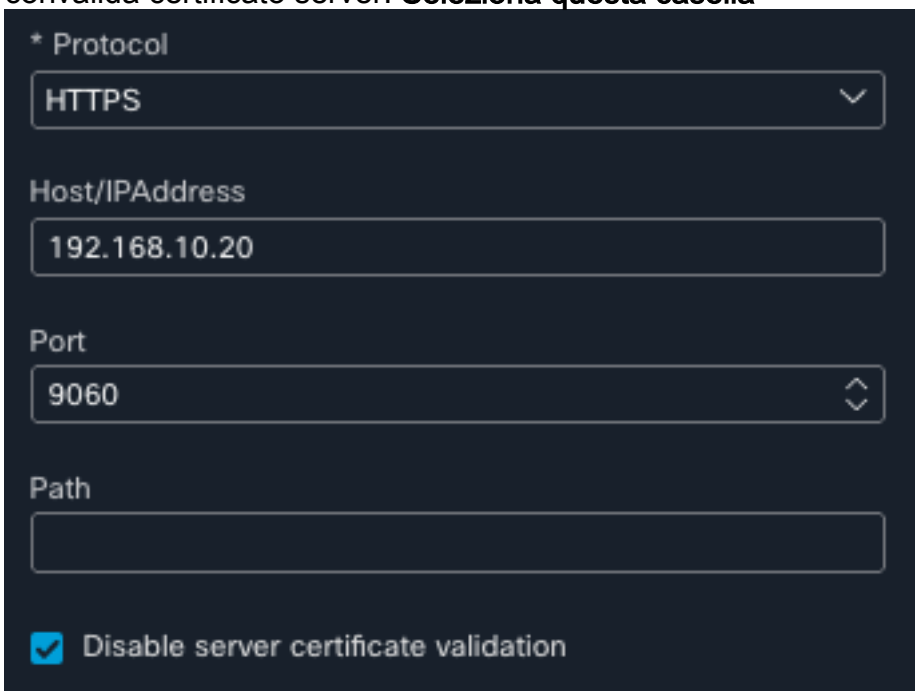
- Nome visualizzato: Identificatore destinazione
- Descrizione: Una breve descrizione per identificare lo scopo del target
- Chiavi account: Qui è necessario configurare l'utente/la password per accedere ad ISE tramite l'API Nessuna chiave account: **Falso**Chiavi account predefinite: Selezionare **Aggiungi nuovo** Tipo di chiave account: **Autenticazione di base HTTP**Nome visualizzato: Identificatore chiave accountUsername: Utente creato su **ISE PAN** come amministratore ERSPassword: Password dell'utente creata sulla **PAN ISE**Opzione di autenticazione: **Base**




- Remoto: Selezionare la connessione remota configurata in precedenza
  Tasti remoti: selezionare il telecomando dal menu a discesa




- HTTP: Qui è necessario configurare le informazioni API per la **PAN ISE** Protocollo: **HTTPS**Indirizzo host/IP: **ISE - PAN IP privato**Port: **9060**Percorso: Lasciare vuotoDisabilita convalida certificato server: **Seleziona questa casella**




- Proxy: Poiché la configurazione proxy è stata inclusa nella configurazione remota, è possibile lasciare vuota questa sezione
- Selezionare **Invia**

### Importa il flusso di lavoro da Cisco Secure GitHub

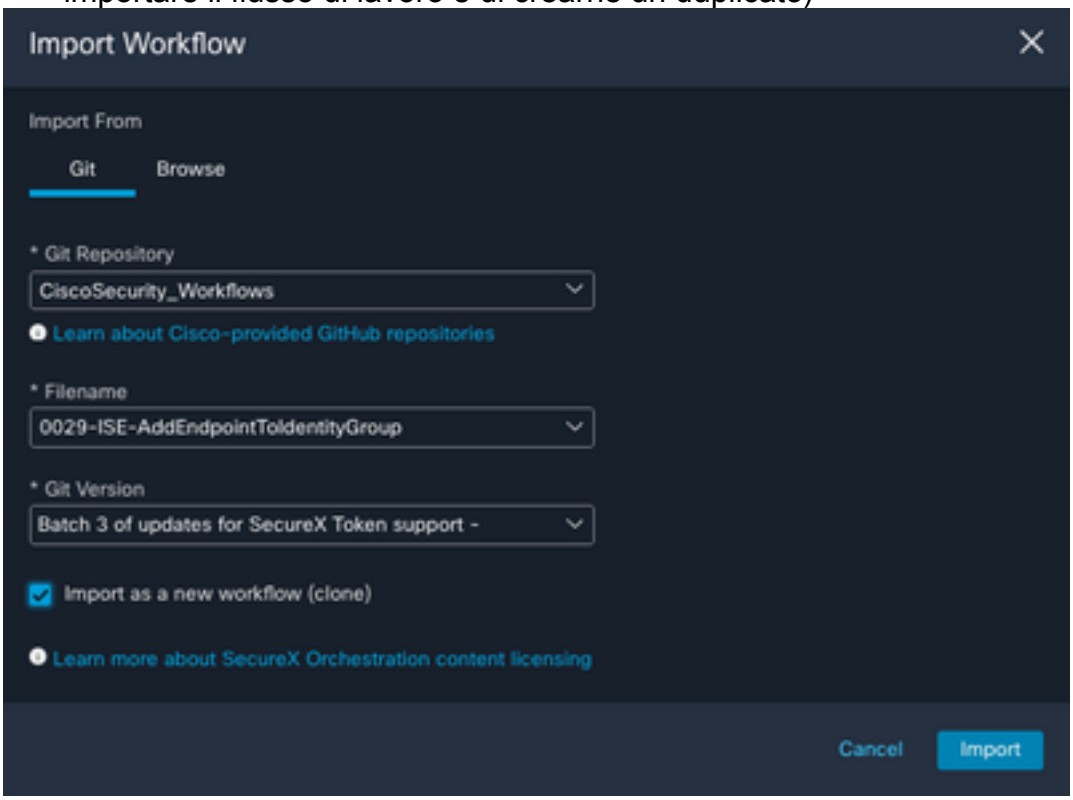
Per questo esempio il flusso di lavoro da utilizzare è "Aggiungi endpoint a gruppo di identità", è possibile utilizzare uno dei flussi di lavoro elencati nella pagina Cisco Secure GitHub oppure creare un flusso di lavoro personalizzato.

1. Passare a **Orchestrazione > Workflow utente > Importa flusso di lavoro**

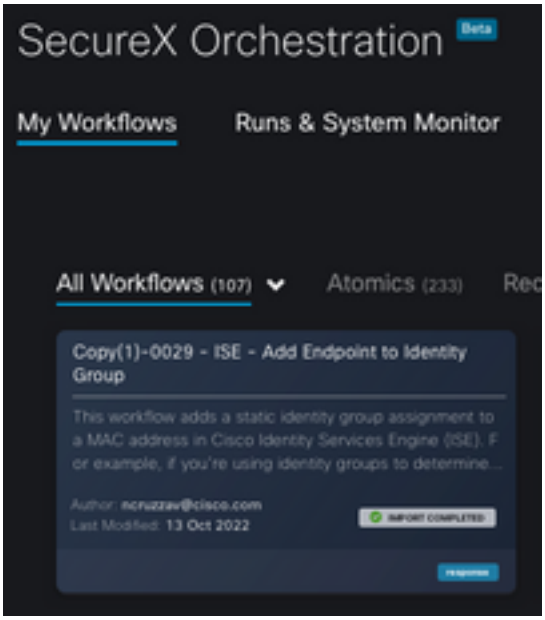

2. Per importare il flusso di lavoro, completare le informazioni come segue e selezionare **Importa;** per identificare il flusso di lavoro da importare, è possibile eseguire una ricerca in base al nome o al numero del flusso di lavoro

- Repository Git: **CiscoSecurity_Workflows** (posizione del flusso di lavoro)

- Nome file: **0029-ISE-AddEndpointToIdentityGroup** (selezionare il numero di flussi di lavoro che si desidera utilizzare)
- Versione Git: **Batch 3 degli aggiornamenti per il supporto di token SecureX** (versione più recente)
- Importa come nuovo flusso di lavoro (clone): **Selezionare** (questa opzione consente di importare il flusso di lavoro e di crearne un duplicato)

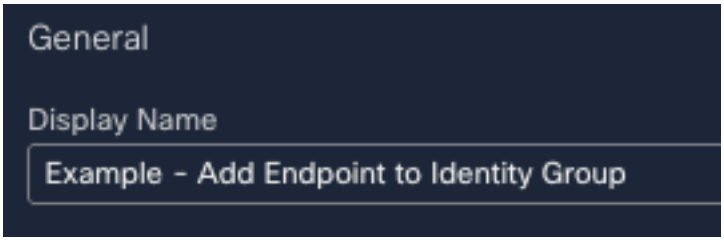



3. Una volta importato, il nuovo modello viene visualizzato in **Workflow utente,** Selezionare il nuovo workflow creato per modificare i parametri e utilizzarlo con **ISE**

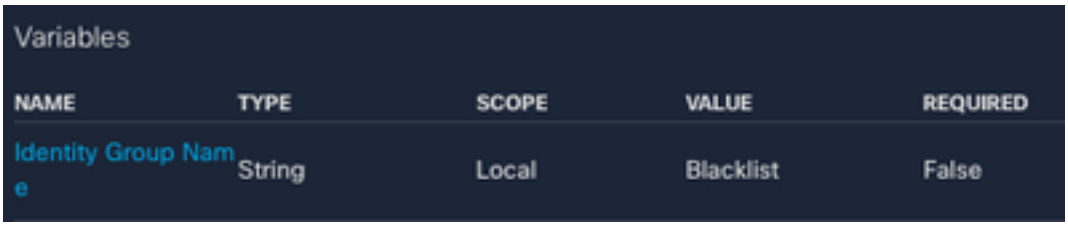



4. Poiché si tratta di un flusso di lavoro pre-generazione, è necessario modificare solo 3 sezioni:

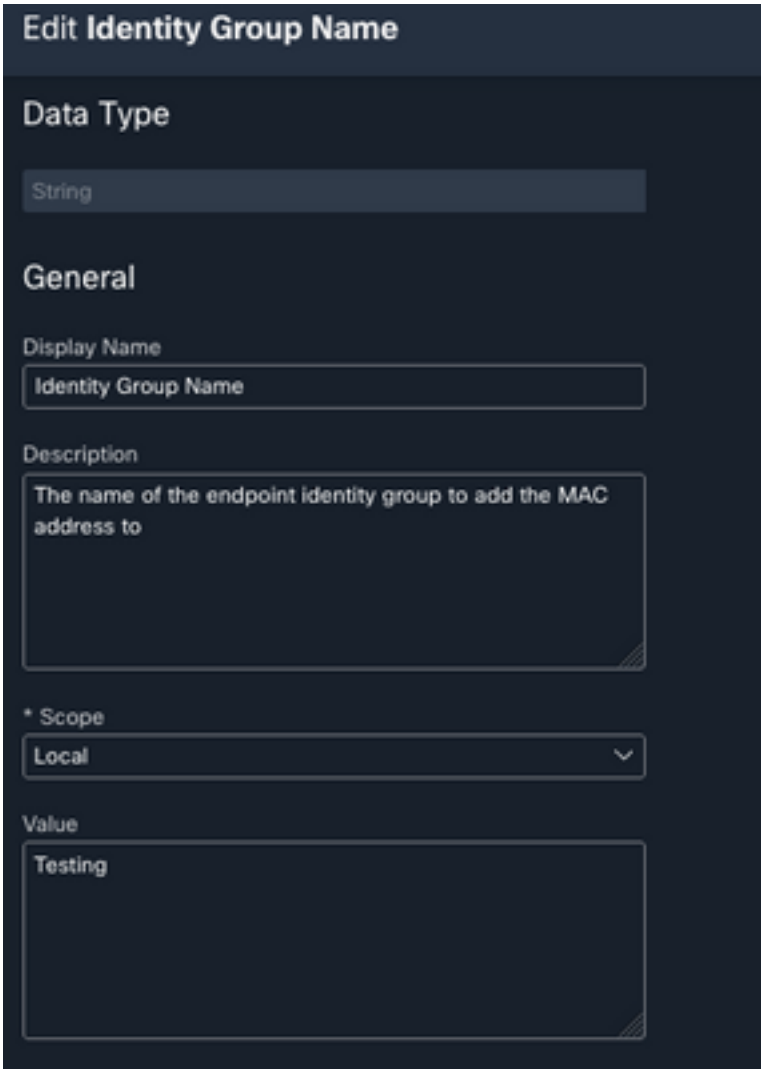
- Nome: modificare il nome visualizzato per un identificatore migliore




- Variabile gruppo di identità In Variabili, modificare la **variabile del gruppo di identità** per impostazione predefinita **Balcklist,** selezionare la variabile e configurare il nome del gruppo di identità da modificare tramite l'orchestrazione




- Selezionare **Salva**




- Destinazione: Configurare la **destinazione** configurata in precedenza Tipo di destinazione: **Endpoint HTTP**Destinazione: **Nome della destinazione configurata**


# Verifica

Una volta configurati tutti gli elementi, è possibile testare il flusso di lavoro

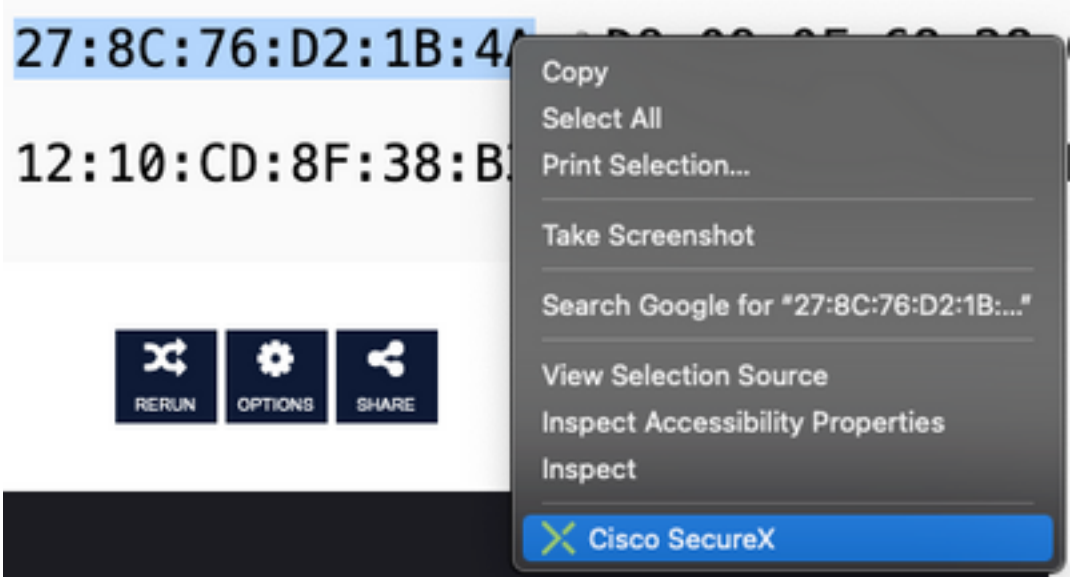
Il flusso di lavoro per il test esegue questa azione: se trovi un indirizzo MAC in una pagina Web, potrebbe trovarsi sulla stessa ISE o su un'altra pagina Web come Threat Response; tramite l'estensione del browser SecureX, il flusso di lavoro cerca l'indirizzo MAC nel database ISE tramite l'API; se l'indirizzo MAC non esiste, l'osservabile viene aggiunto all'Endpoint Identity Group senza dover copiare il valore e accedere all'ISE.

Per dimostrarlo, vedere l'esempio seguente:

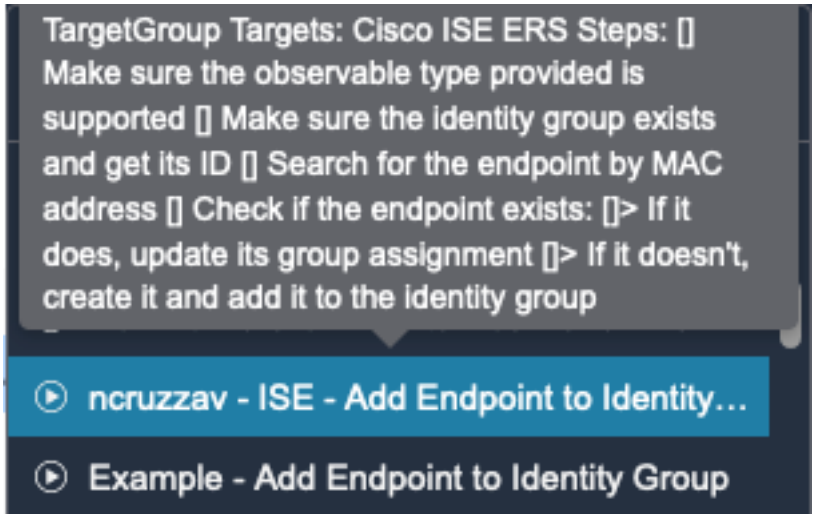
1. Il flusso di lavoro selezionato funziona con il tipo osservabile **"Indirizzo MAC"**

2. Trova un indirizzo MAC in una pagina Web ed esegui un clic con il pulsante destro del mouse.

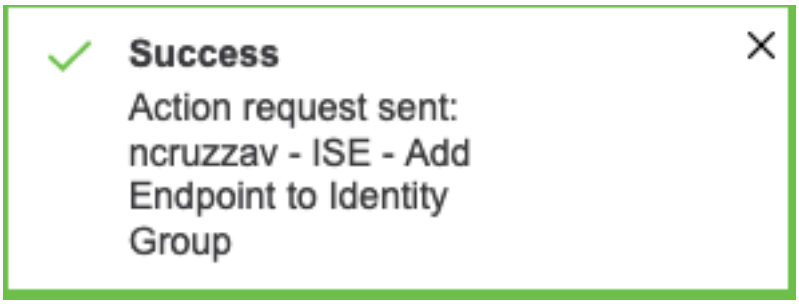
3. Selezionare l'opzione **SecureX**




4. Selezionare il **flusso di lavoro** creato prima

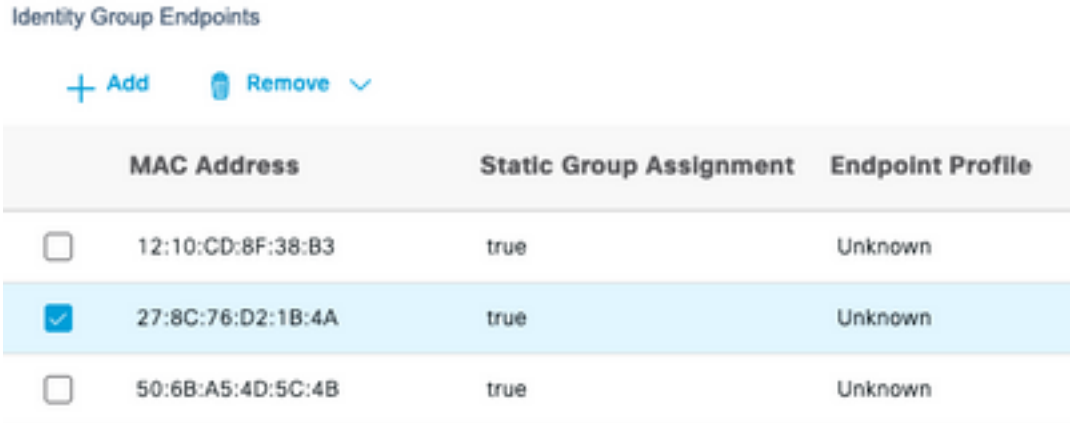



5. Confermare l'esecuzione del task




6. Nel piano **ISE** passare a **Amministrazione > Gestione delle identità > Gruppi > Gruppi di identità degli endpoint > (Il gruppo configurato nel flusso di lavoro)**

7. Aprire il **gruppo di identità degli endpoint** configurato nel flusso di lavoro e confermare che la selezione dell'indirizzo MAC sia stata aggiunta all'elenco indirizzi MAC



Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).