Configurazione di Cisco Secure Access per RA VPNaaS con Entra ID

Sommario

Introduzione

In questo documento viene descritto passo a passo come configurare una VPN RSA su Cisco Secure Access per l'autenticazione con Entra ID.

Prerequisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenza tramite Azure/Entra ID.
- Conoscenza di Cisco Secure Access.

Requisiti

Prima di procedere, è necessario soddisfare i seguenti requisiti:

- Accedere a Cisco Secure Access Dashboard come amministratore completo.
- Accesso ad Azure come amministratore.
- Provisioning utente già completato per Cisco Secure Access.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Secure Access Dashboard.

- Portale di Microsoft Azure.
- Cisco Secure Client AnyConnect VPN versione 5.1.8.105

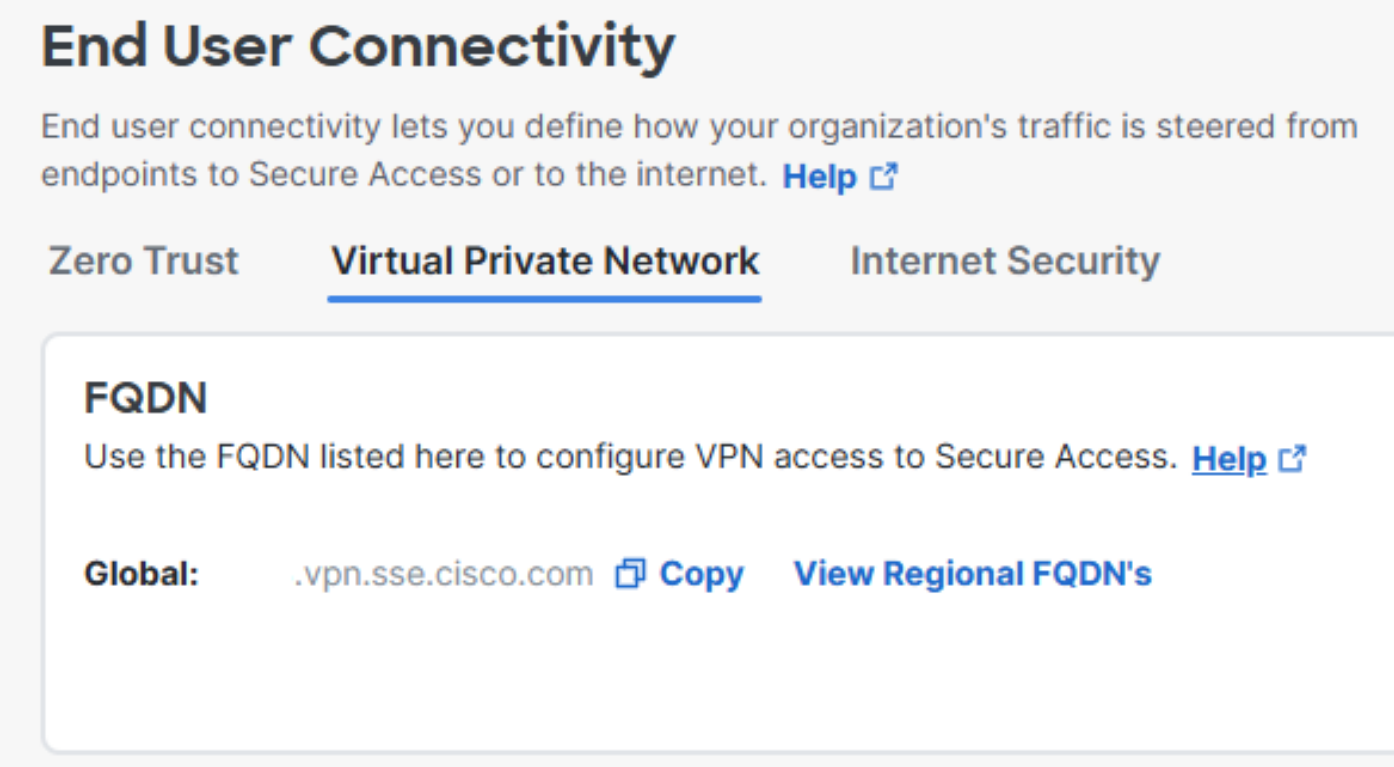
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze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

Configurazione

Configurazione di Azure

1. Accedi al dashboard di Cisco Secure Access e copia il nome di dominio completo (FQDN) globale della VPN. Questo FQDN è in uso nella configurazione dell'applicazione aziendale di Azure.

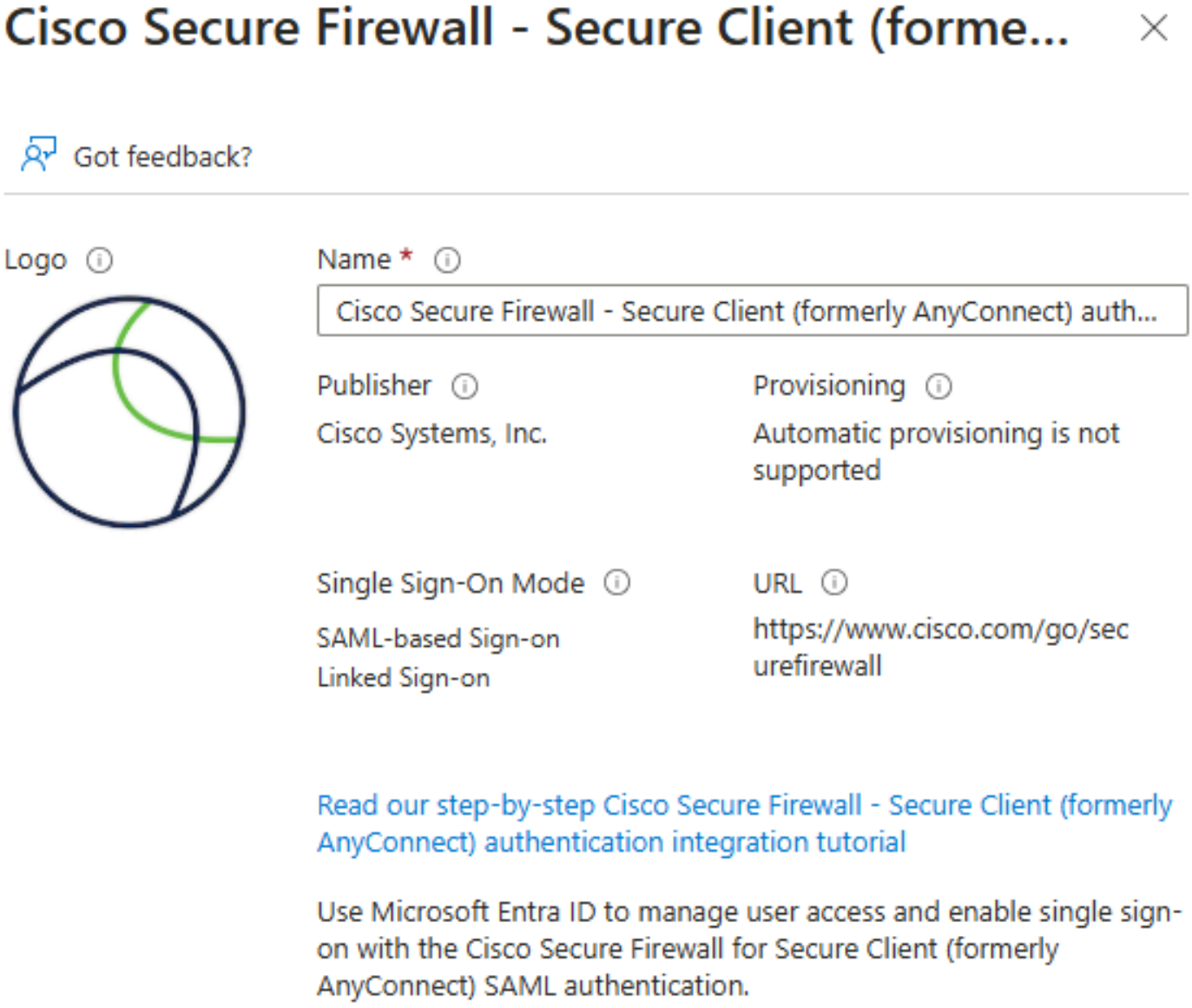
Connetti > Connettività utente finale > Rete privata virtuale > FQDN > Globale



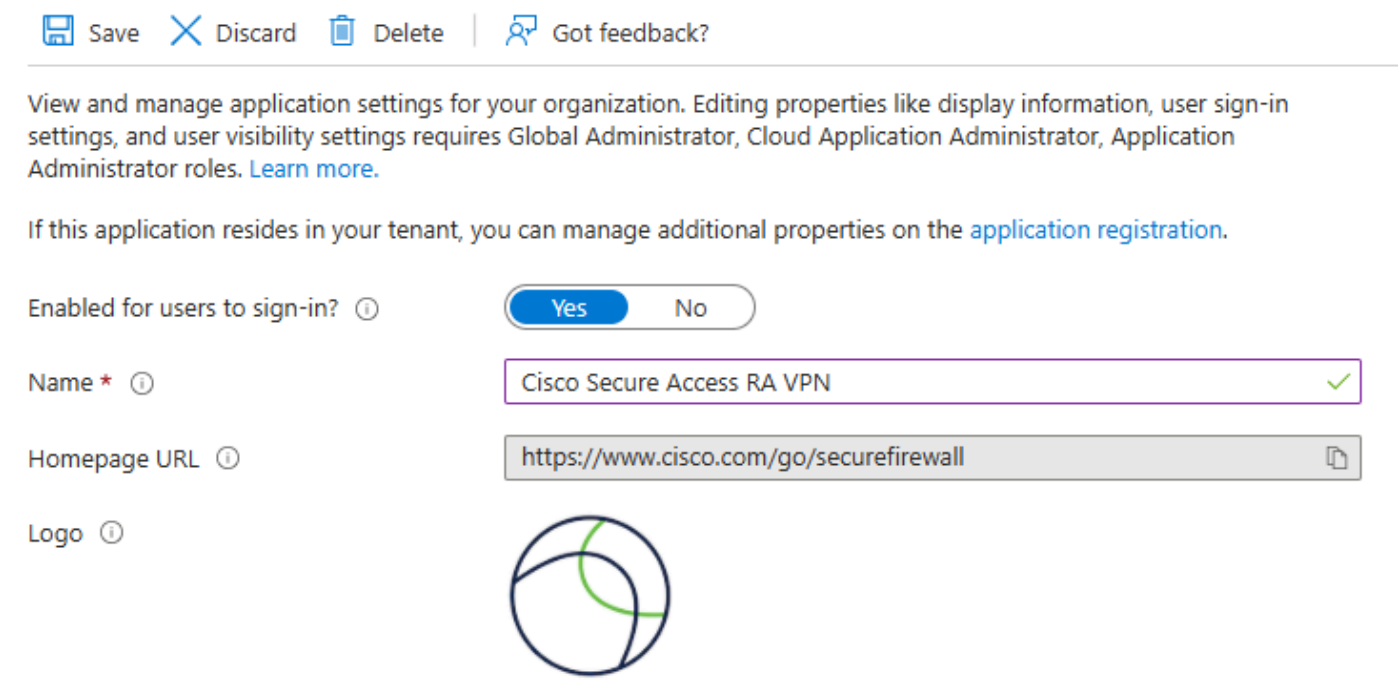
FQDN globale VPN

2. Accedere ad Azure e creare un'applicazione enterprise per l'autenticazione VPN per l'Autorità registrazione integrità. È possibile usare l'applicazione predefinita "Cisco Secure Firewall - Autenticazione client sicura (in precedenza AnyConnect)".

Home > Applicazioni enterprise > Nuova applicazione > Cisco Secure Firewall - Autenticazione client sicura (in precedenza AnyConnect) > Crea



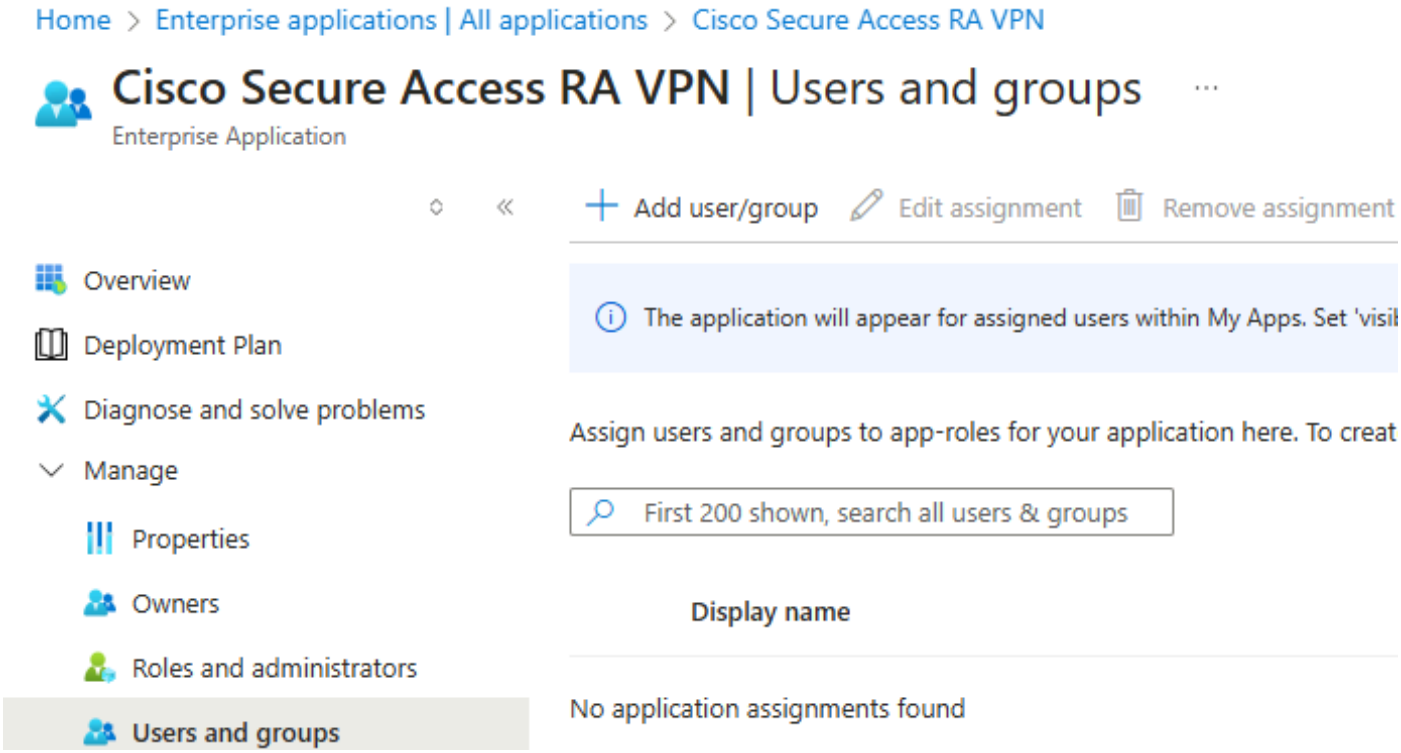
3. Rinominare l'applicazione.
   Proprietà > Nome



Rinomina l'applicazione

4. Nell'applicazione enterprise, assegnare gli utenti autorizzati all'autenticazione tramite la VPN AnyConnect.

Assegna utenti e gruppi > + Aggiungi utente/gruppo > Assegna

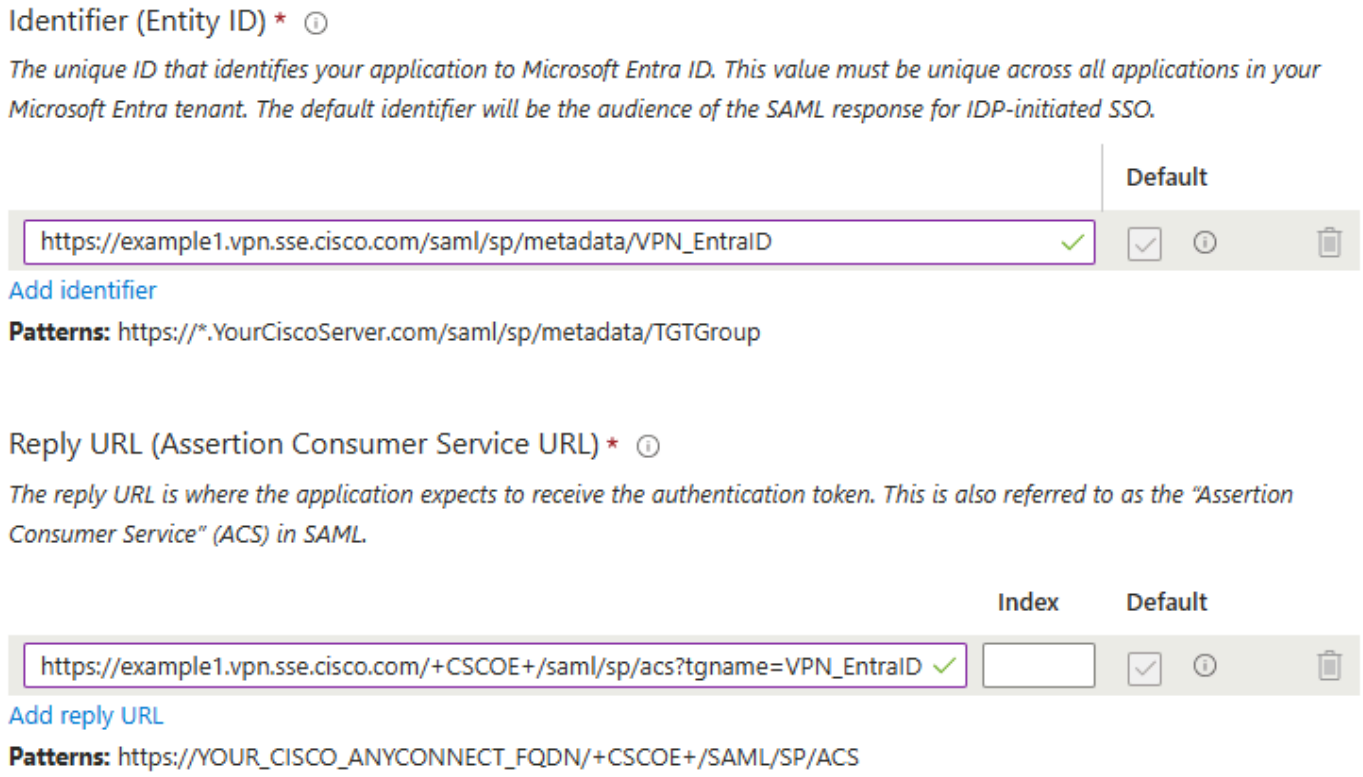


Utenti/gruppi assegnati

5. Fare clic su Single Sign-On e configurare i parametri SAML. In questa sezione viene usato l'FQDN copiato nel passaggio 1 e il nome del profilo VPN che si sta configurando in "Configuration Cisco Secure Access" più avanti nel passaggio 2.

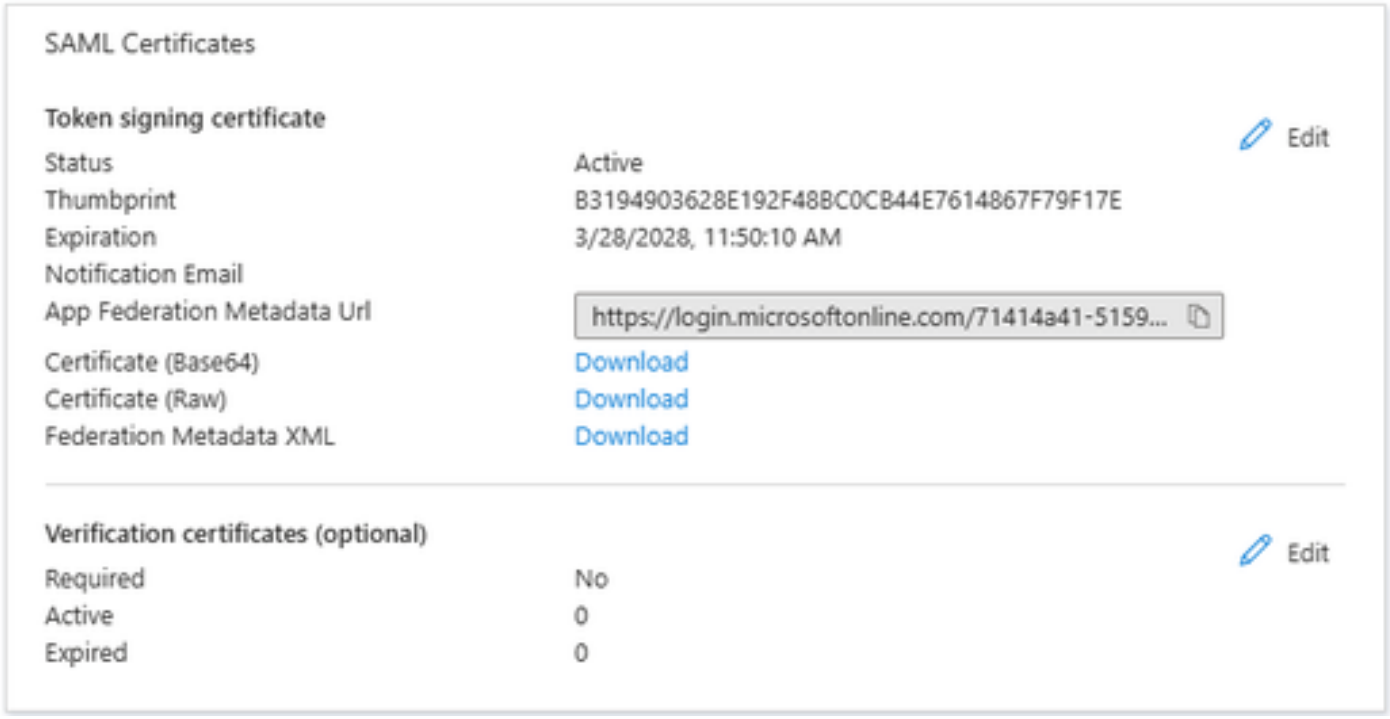
Ad esempio, se il nome di dominio completo (FQDN) globale della VPN è example1.vpn.sse.cisco.com e il nome del profilo VPN ad accesso sicuro di Cisco è VPN_EntraID, i valori per (ID entità) e URL di risposta (URL servizio consumer asserzione) sono:

Identificatore (ID entità): https://example1.vpn.sse.cisco.com/saml/sp/metadata/VPN_EntraID
URL risposta (URL servizio consumer asserzione): https://example1.vpn.sse.cisco.com/+CSCOE+/saml/sp/acs?tgname=VPN_EntraID



Parametri SAML in Azure

6. Scaricare il file XML dei metadati federativi.



Configurazione Cisco Secure Access

1. Accedi al dashboard di Cisco Secure Access e aggiungi un pool IP.

   Connetti > Connettività utente finale > Rete privata virtuale > Aggiungi pool IP

Regione: Selezionare l'area in cui verrà distribuita la VPN dell'Autorità registrazione.
Nome visualizzato: Nome del pool IP della VPN.
Server DNS: Creare o assegnare gli utenti del server DNS utilizzati per la risoluzione DNS una volta connessi.
Pool IP di sistema: Utilizzata da Secure Access per funzionalità quali l'autenticazione Radius, la richiesta di autenticazione ha origine da un indirizzo IP compreso in questo intervallo.
Pool IP: Aggiungere un nuovo pool IP e specificare gli IP che gli utenti ottengono una volta connessi alla VPN dell'Autorità registrazione.

Setup VPN profiles

No VPN profiles added. To configure VPN profiles, you must first setup IP pools and then add profiles that map to users. Help

Add IP Pool

Aggiungi profilo VPN

Parameters

Edit this IP pool's parameters including its mapped region, DNS servers, and IP addresses

Region

Canada (Central)

Display name

RA VPN

DNS Server

DNS (208.67.222.222)

+ Add

DDNS Servers updates

System IP Pool

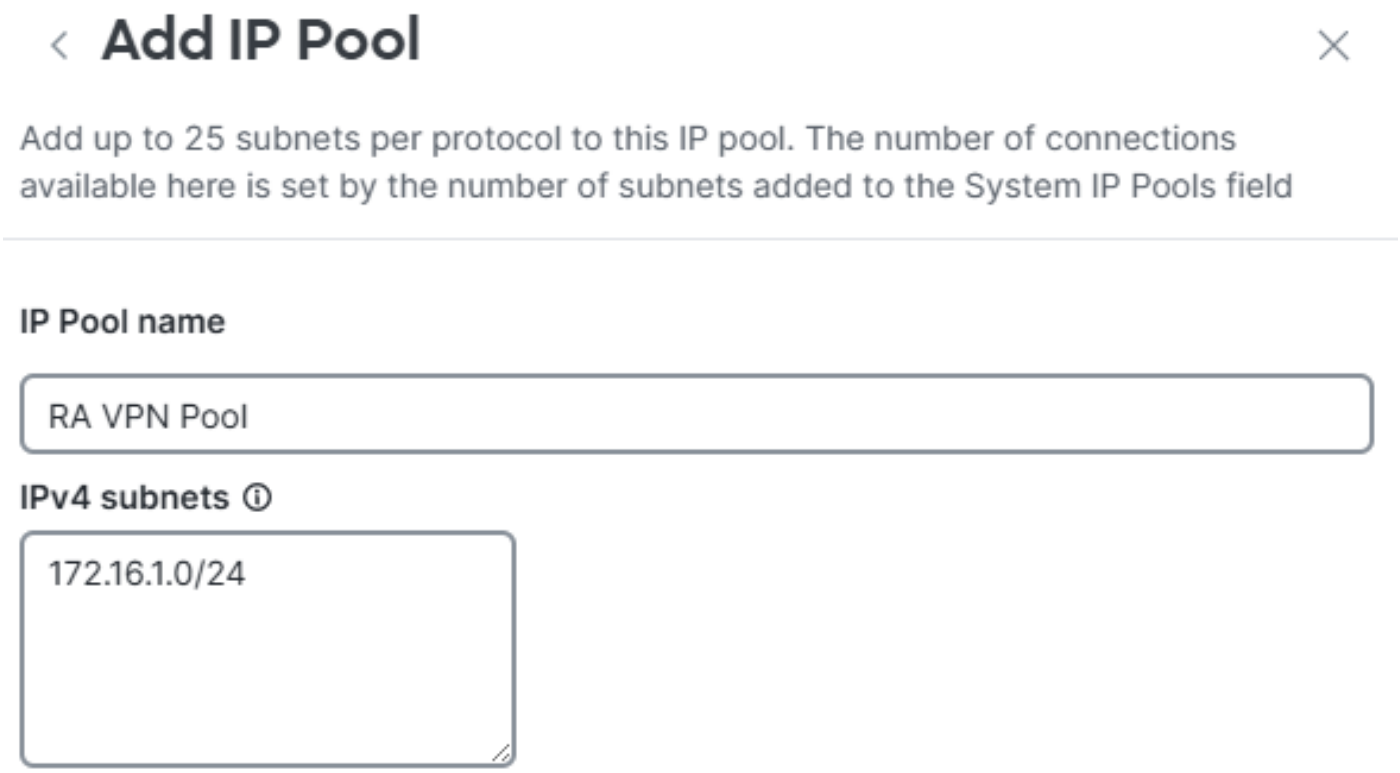
172.16.2.0/24

IP Pools

Add the IP pools this region will use. You can add a maximum of 25 IPV4 and 25 IPV6 subnets per IP pool. Help

+ Add

Configurazione del pool IP - Parte 1

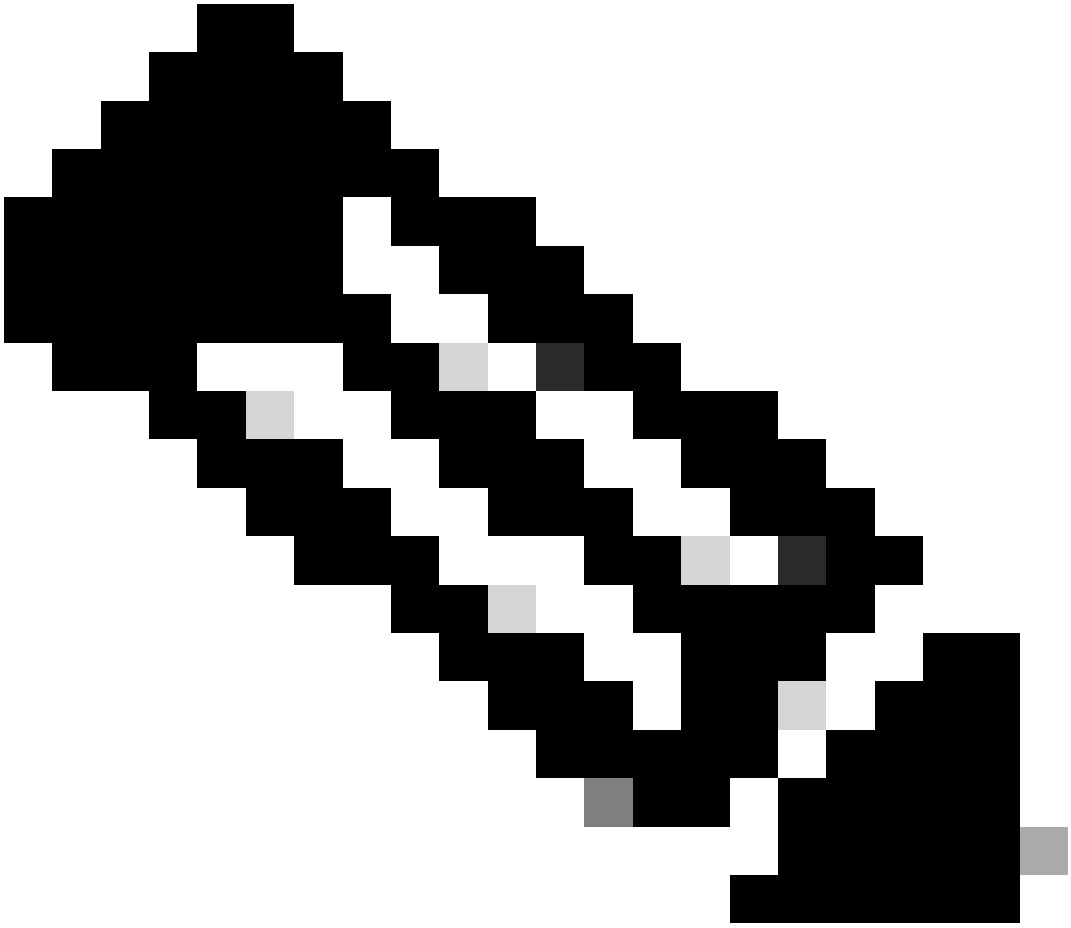


Configurazione del pool IP - Parte 2

2. Aggiungere un profilo VPN.

Connetti > Connettività utente finale > Rete privata virtuale > + Profilo VPN

Impostazioni generali



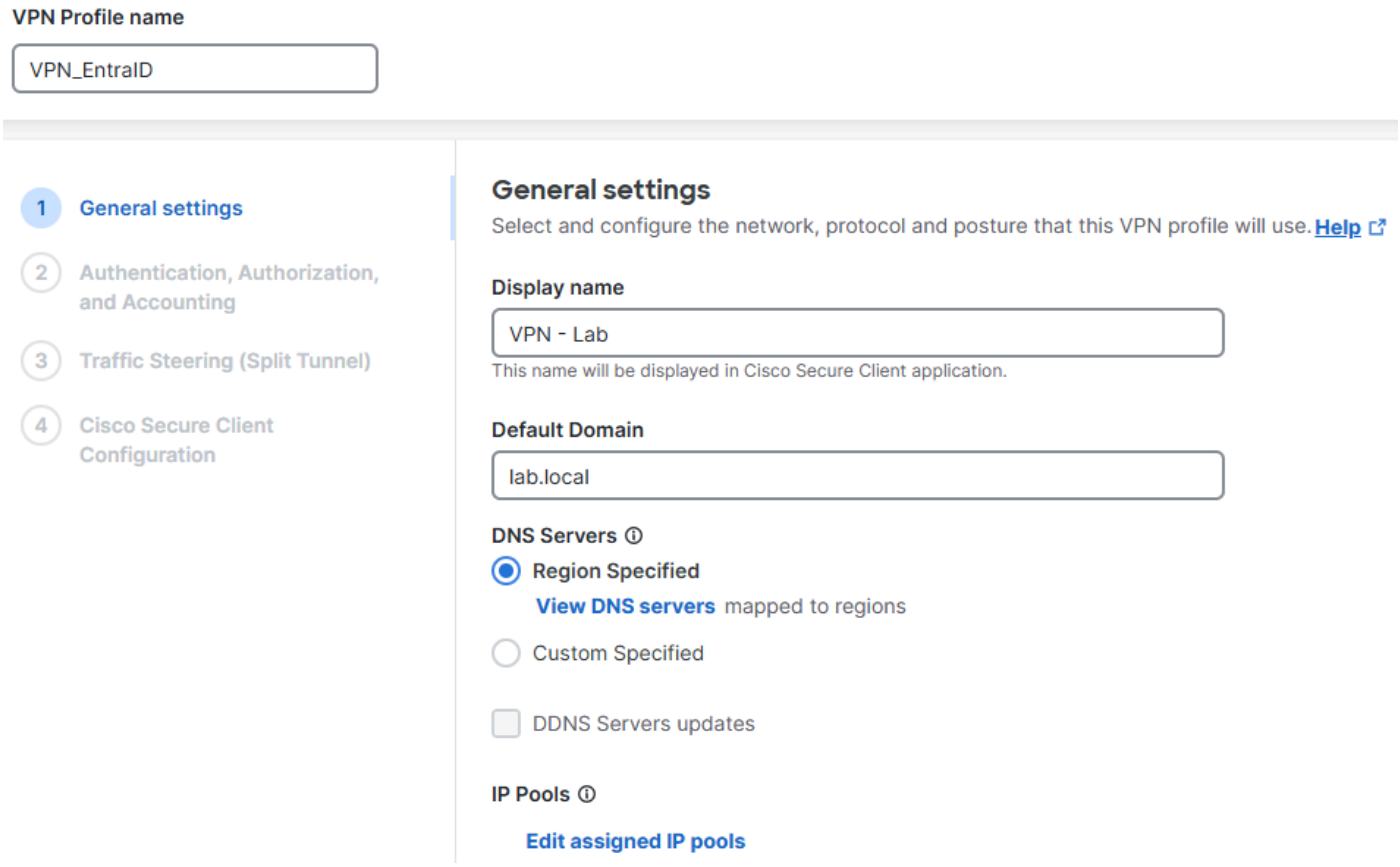
> Nota: Nota: Il nome del profilo VPN deve corrispondere al nome configurato in "Azure di configurazione" nel passaggio 5. In questa guida alla configurazione è stato utilizzato VPN_EntraID, quindi in Cisco Secure Access viene configurato lo stesso nome del profilo VPN.

Nome profilo VPN: Nome per questo profilo VPN, visibile solo nel dashboard.

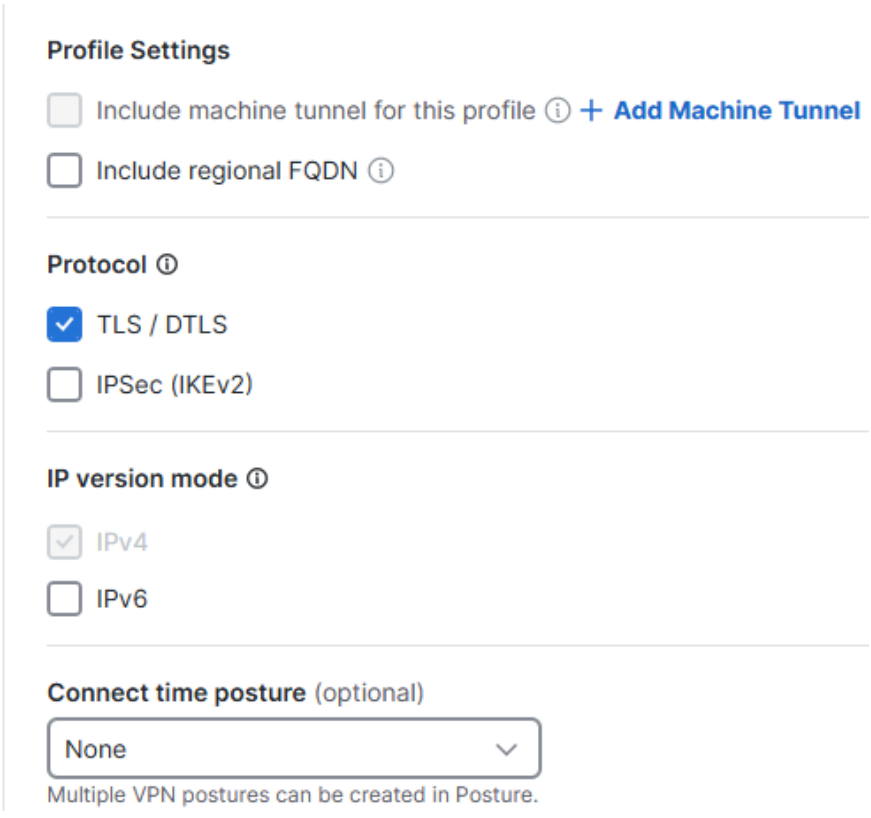
Nome visualizzato: Il nome che gli utenti finali visualizzano nel menu a discesa 'Secure Client - Anyconnect' mostra quando si connettono a questo profilo VPN per l'Autorità registrazione.
Dominio predefinito: Una volta connessi alla VPN, gli utenti del dominio.
Server DNS: Server DNS utilizzato dagli utenti VPN una volta connessi alla VPN.
- Area specificata: Utilizza il server DNS associato al pool IP della VPN.
- Personalizzato specificato: È possibile assegnare manualmente il DNS desiderato.

Pool IP: IP assegnati agli utenti una volta connessi alla VPN.
Impostazioni profilo: Per includere questo profilo VPN per il tunnel macchina o per includere il nome di dominio completo (FQDN) regionale in modo che l'utente finale selezioni la regione a cui desidera connettersi (soggetta ai pool IP distribuiti).

Protocolli: Selezionare il protocollo che gli utenti VPN devono utilizzare per il tunneling del traffico.
Postura tempo di connessione (facoltativa): Se necessario, eseguire VPN Posture al momento della connessione. Ulteriori informazioni



Configurazione profilo VPN - Parte 1

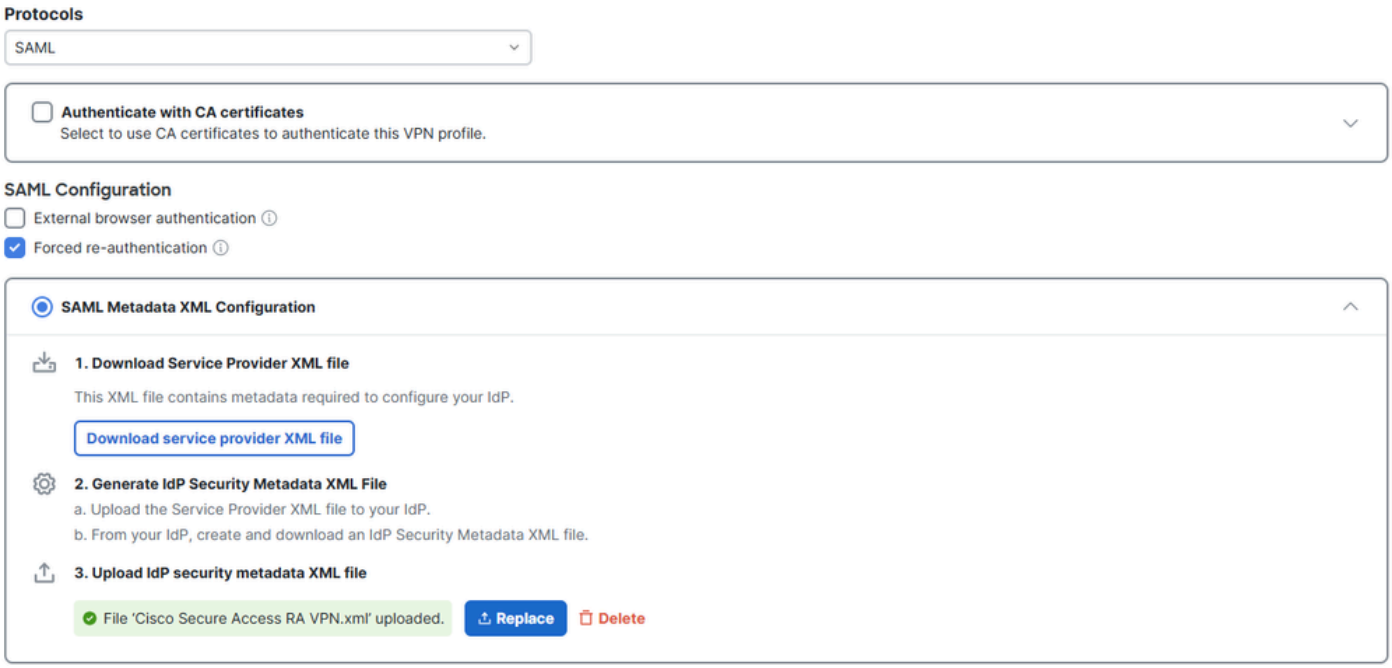


Autenticazione, autorizzazione e accounting

Protocolli: Selezionare SAML.

Autenticazione con certificati CA: Se si desidera eseguire l'autenticazione utilizzando un certificato SSL e l'autorizzazione per un provider SAML IdP.
Forza riautenticazione: Forza una riautenticazione ogni volta che viene stabilita una connessione VPN. La riautenticazione forzata è basata sul timeout della sessione. Potrebbe essere soggetto alle impostazioni del provider di identità SAML (Azure in questo caso).

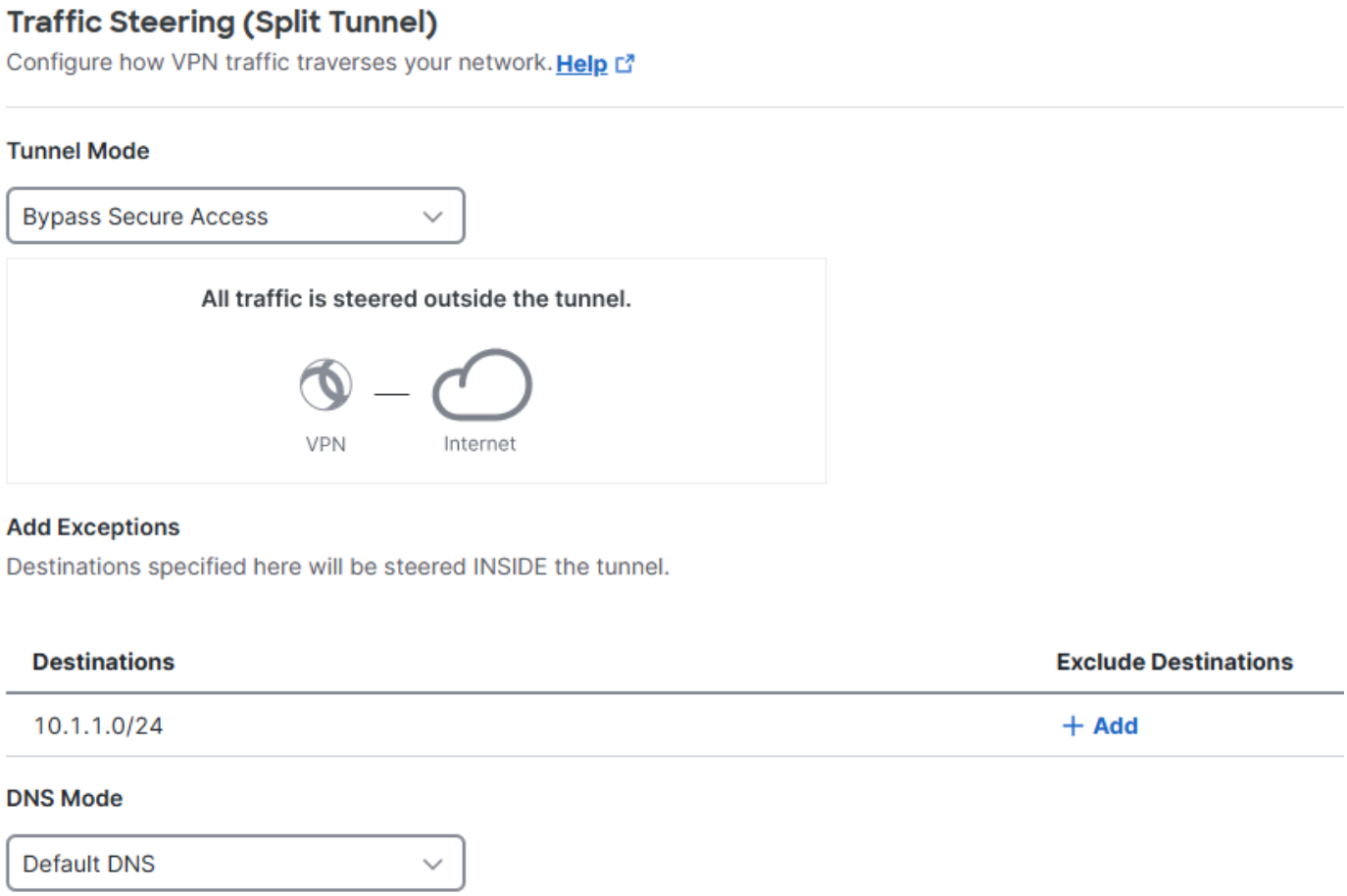
Caricare il file XML metadati federazione file XML scaricato in "Configura Azure" nel passaggio 6.



Configurazione SAML

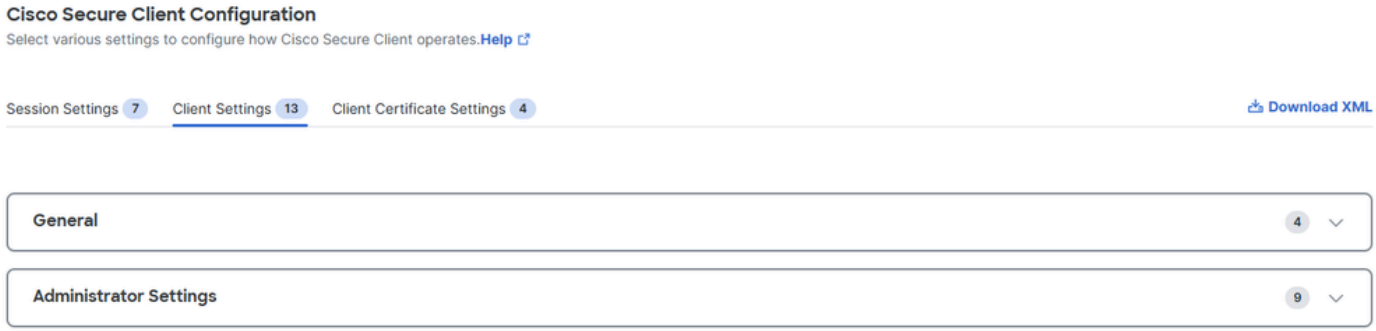
Traffic Steering (split tunnel)

Modalità tunnel:
Connetti ad accesso sicuro: Tutto il traffico viene inviato attraverso il tunnel (Tunnel All).
Ignora accesso sicuro: Solo il traffico specifico definito nella sezione Exceptions è tunneling (Split Tunnel).
Modalità DNS:
DNS predefinito: Tutte le query DNS vengono spostate nei server DNS definiti dal profilo VPN. In caso di risposta negativa, le query DNS possono anche passare ai server DNS configurati sulla scheda fisica.
Tunnel per tutti i DNS: Esegue il tunnel di tutte le query DNS tramite VPN.
Dividi DNS: Solo le query DNS specifiche vengono spostate nel profilo VPN, a seconda dei domini specificati di seguito.



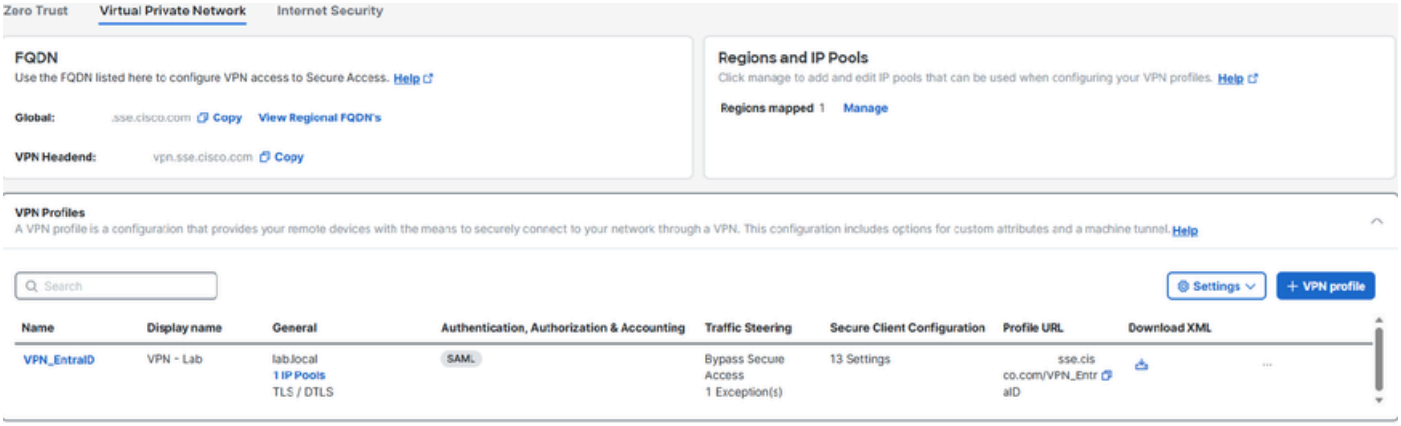
Configurazione Traffic Steering

Cisco Secure Client Configuration
Ai fini di questa guida, non stiamo configurando nessuna di queste impostazioni avanzate. Le funzioni avanzate possono essere configurate qui, ad esempio: TND, Always-On, Corrispondenza certificati, Accesso LAN locale e così via. Salvare le impostazioni qui.



Impostazioni avanzate

3. Il tuo profilo VPN deve avere questo aspetto. È possibile scaricare e pre-distribuire il profilo xml agli utenti finali (in "C:\ProgramData\Cisco\Cisco Secure Client\VPN\Profile") per iniziare a utilizzare la VPN o fornire loro l'URL del profilo da immettere nell'interfaccia utente di Cisco Secure Client - AnyConnect VPN.



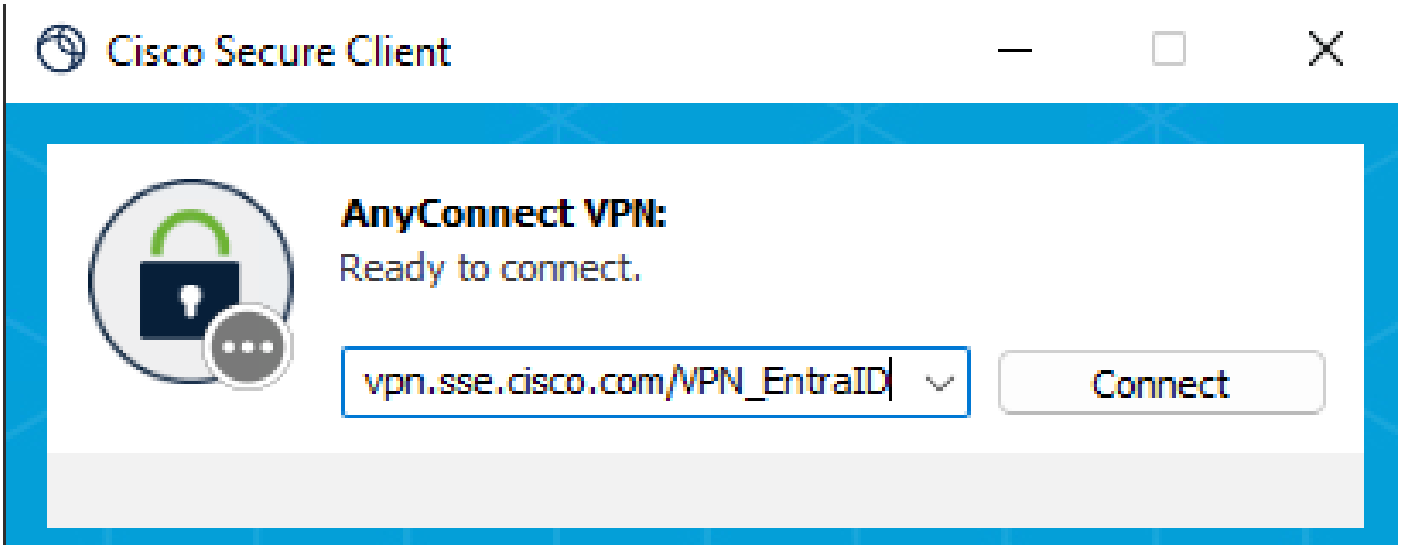
FQDN globale e URL profilo

Verifica

A questo punto, la configurazione della VPN dell'Autorità registrazione deve essere pronta per il test.
Notare che la prima volta che gli utenti si connettono, devono ricevere l'indirizzo URL del profilo o pre-distribuire il profilo xml nei loro PC in "C:\ProgramData\Cisco\Cisco Secure Client\VPN\Profile", riavviare il servizio VPN e devono vedere nel menu a discesa l'opzione per connettersi a questo profilo VPN.

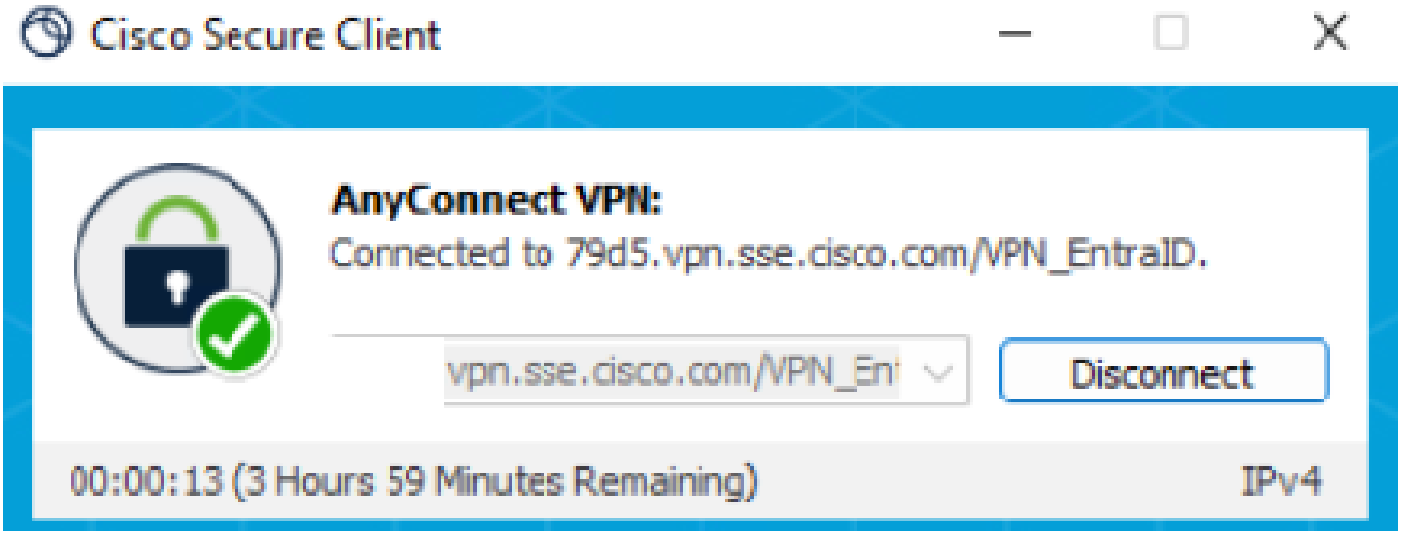
In questo esempio, viene fornito all'utente l'indirizzo URL del profilo per il primo tentativo di connessione.

Prima della prima connessione:



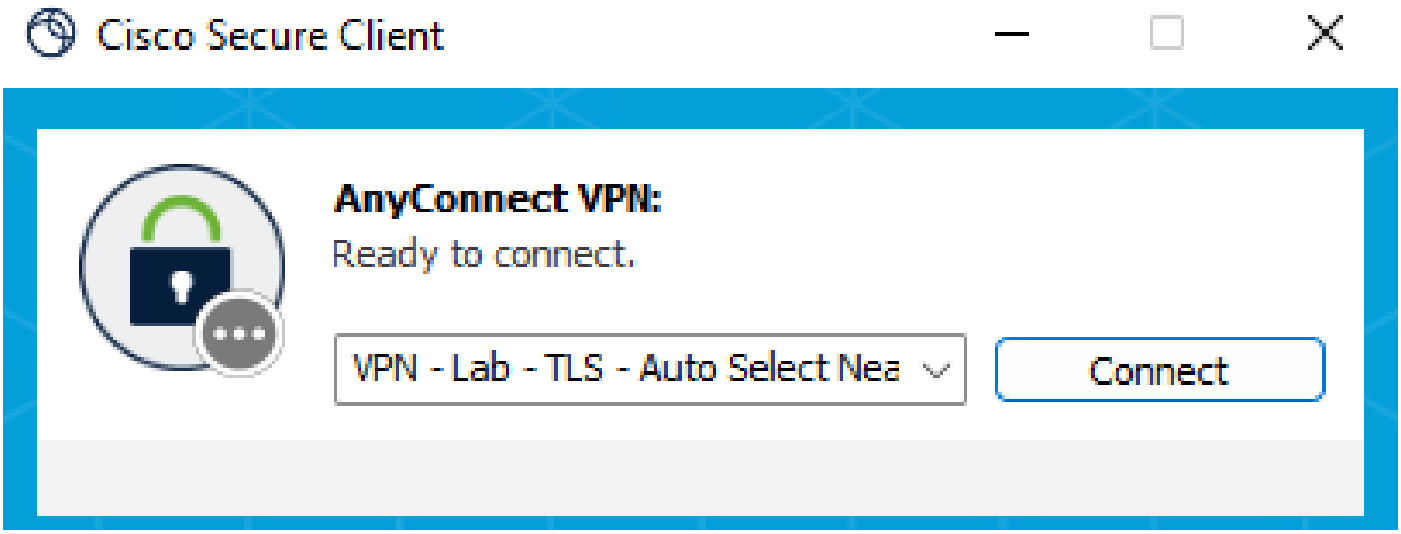
Connessione VPN precedente

Immettere le credenziali e connettersi alla VPN:



Connesso a VPN

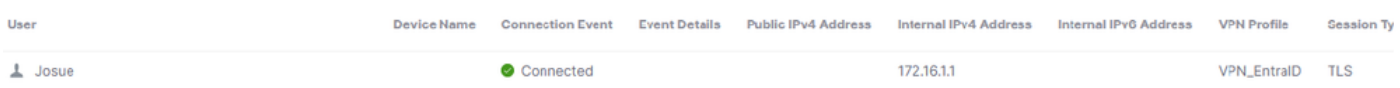
Dopo aver effettuato la connessione per la prima volta, dal menu a discesa, è necessario poter visualizzare ora l'opzione per connettersi al profilo VPN "VPN - Lab":



Dopo la prima connessione VPN

Archiviare i registri di Accesso remoto a cui l'utente è riuscito a connettersi:

Monitor > Registro di accesso remoto



Log in Cisco Secure Access

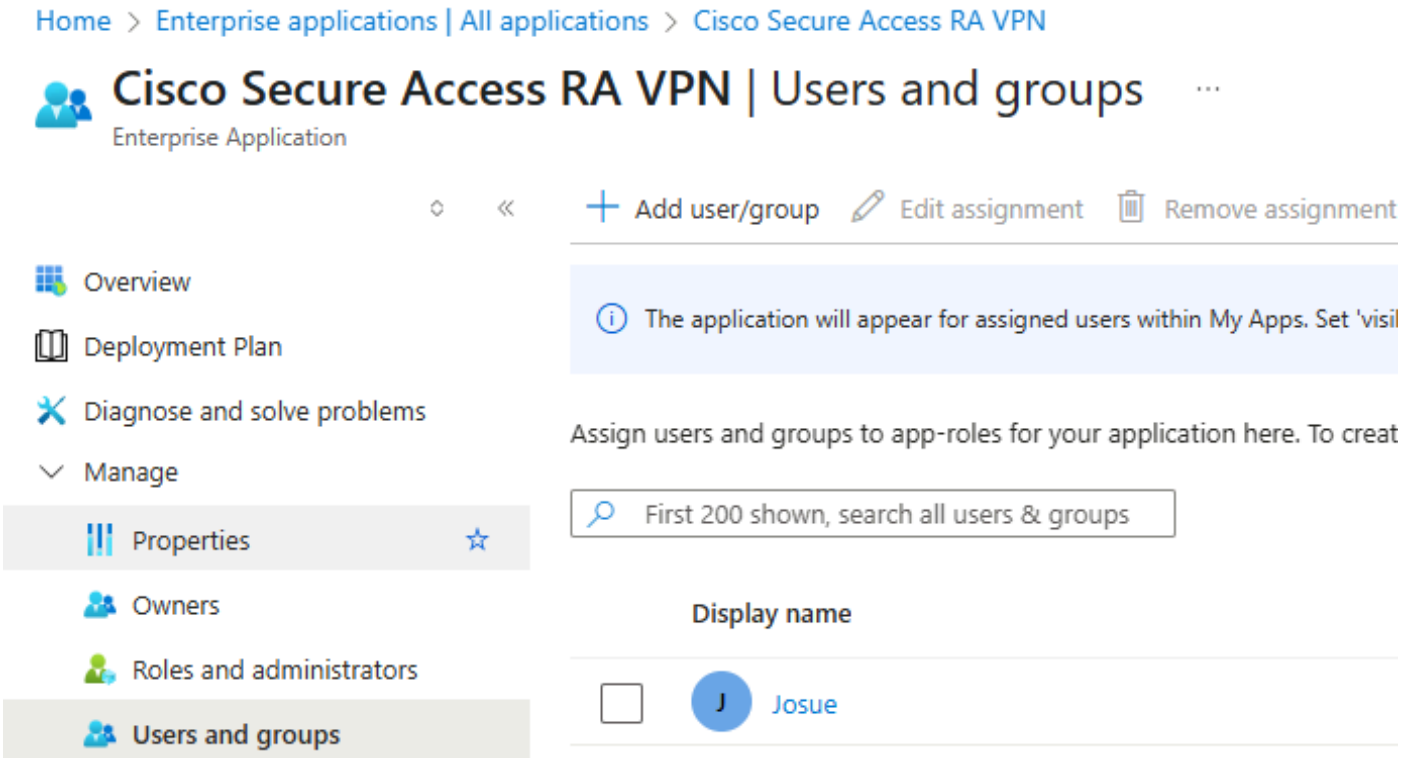
Risoluzione dei problemi

Di seguito viene descritta la risoluzione dei problemi di base che è possibile eseguire per alcuni problemi comuni:

Azzurro

In Azure verificare che gli utenti siano stati assegnati all'applicazione enterprise creata per l'autenticazione con Cisco Secure Access:

Home > Applicazioni enterprise > Cisco Secure Access RSA VPN > Gestisci > Utenti e gruppi

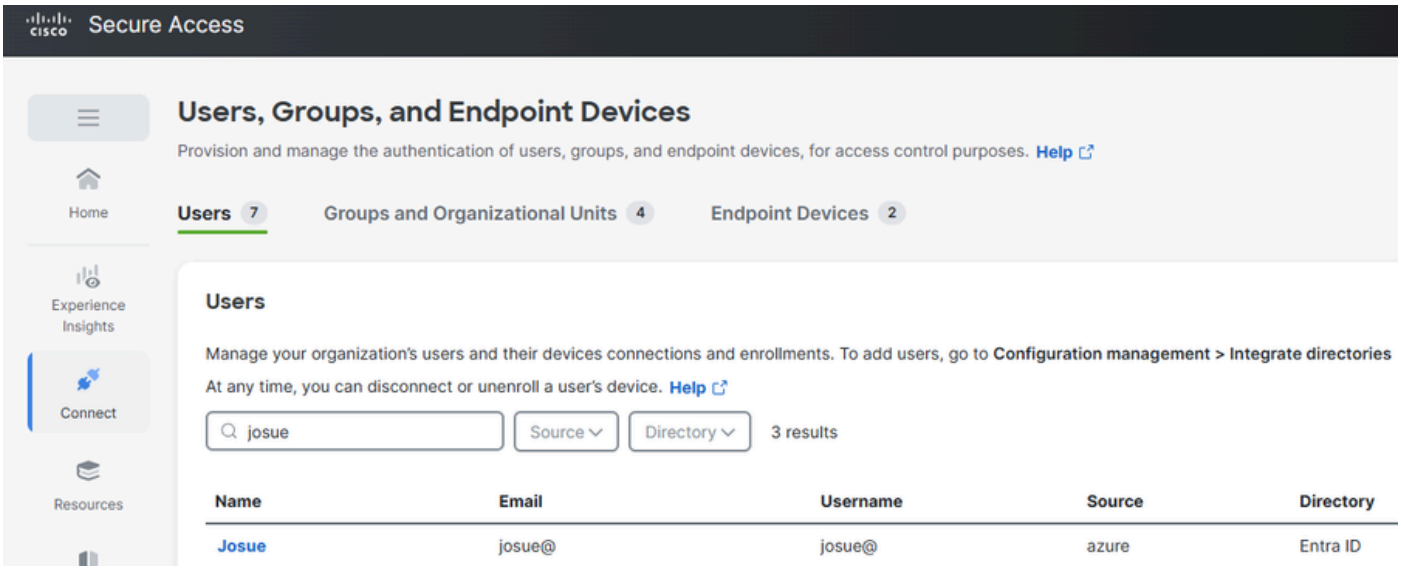


Verifica assegnazione utenti

Cisco Secure Access

In Cisco Secure Access verificare di aver eseguito il provisioning degli utenti a cui è consentito connettersi tramite la VPN RSA e che anche gli utenti a cui è stato eseguito il provisioning in Cisco Secure Access (in utenti, gruppi e dispositivi endpoint) corrispondano agli utenti in Azure (gli utenti assegnati nell'applicazione enterprise).

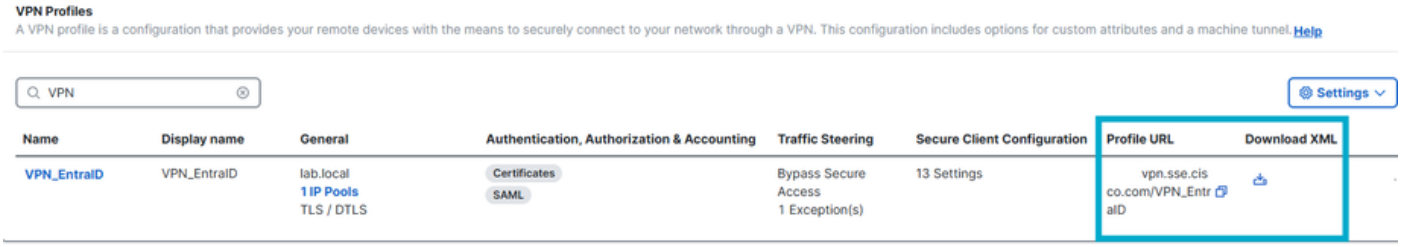
Connetti > Utenti, gruppi e dispositivi endpoint



Utenti in Cisco Secure Access

Verificare che all'utente sia stato assegnato il file XML corretto sul PC o che all'utente sia stato assegnato l'URL del profilo, come indicato nel passaggio "Verifica".

Connetti > Connettività utente finale > Rete privata virtuale



URL del profilo e profilo XML

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).