Installazione di Secure Client con Umbrella Protection su Android tramite MDM Zero-Touch

Sommario

Introduzione

Questo documento descrive come distribuire Cisco Secure Client con il modulo Umbrella su dispositivi Android usando la distribuzione zero-touch.

Premesse

È possibile distribuire Cisco Secure Client con il modulo Umbrella su dispositivi Android utilizzando la distribuzione zero-touch tramite soluzioni MDM come Workspace One, Cisco Meraki o Microsoft Intune. Questo processo consente una protezione completa a livello DNS per le applicazioni e il traffico del browser, garantisce l'abilitazione della VPN Always On ed elimina l'intervento dell'utente per l'accettazione della VPN e della SEULA.

Prerequisiti

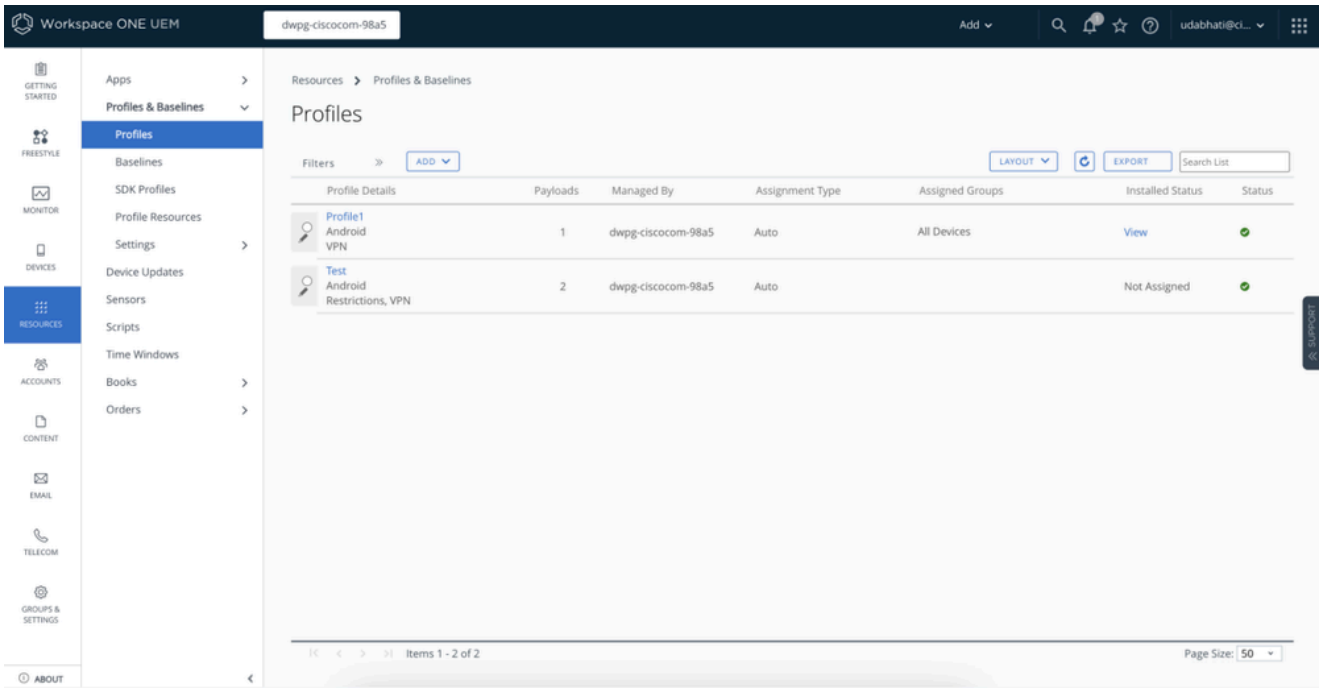
- Completamento della registrazione EMM (Android Enterprise Mobility Management) e della registrazione dei dispositivi con la creazione di profili di lavoro.
- L'app MDM (hub) deve essere visibile nel profilo di lavoro.
- Assegnare e installare Cisco Secure Client solo dopo la pubblicazione e l'installazione del profilo VPN Always On in Intelligent Hub.

Fasi di distribuzione

A. Creare il profilo VPN Always On

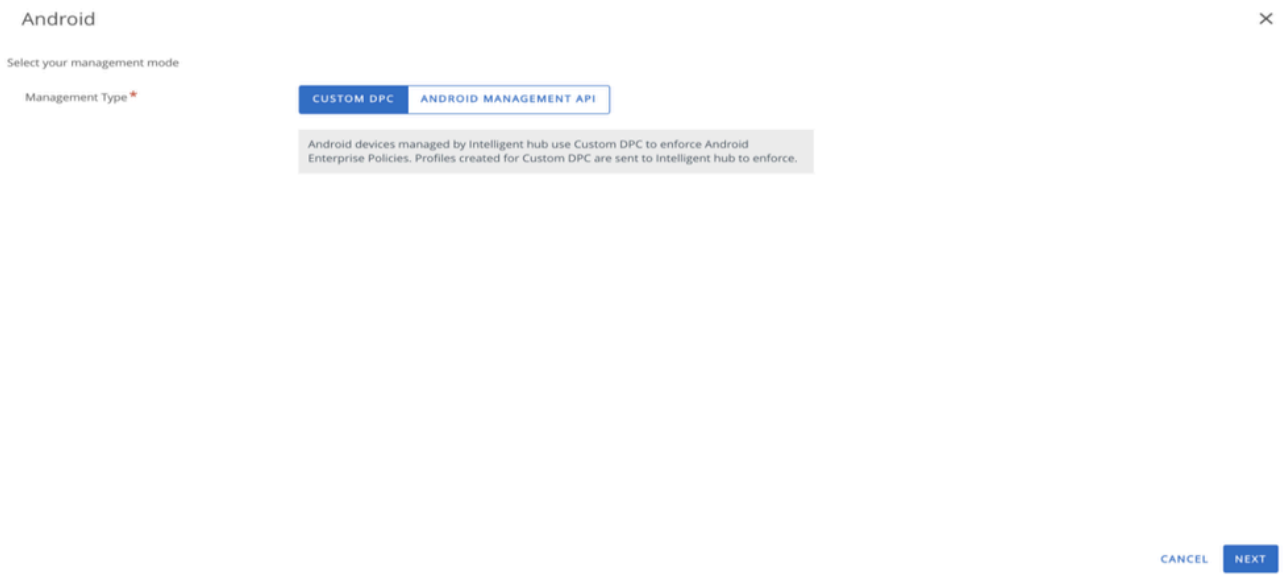
1. Passare a Profili:

    - Selezionare Risorse > Profili e baseline > Profili.
    - Fare clic su Aggiungi per creare un nuovo profilo.

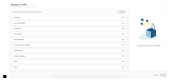


2. Impostazione profilo:

- Selezionate Androida come piattaforma.
- Scegliere il tipo di gestione richiesto.

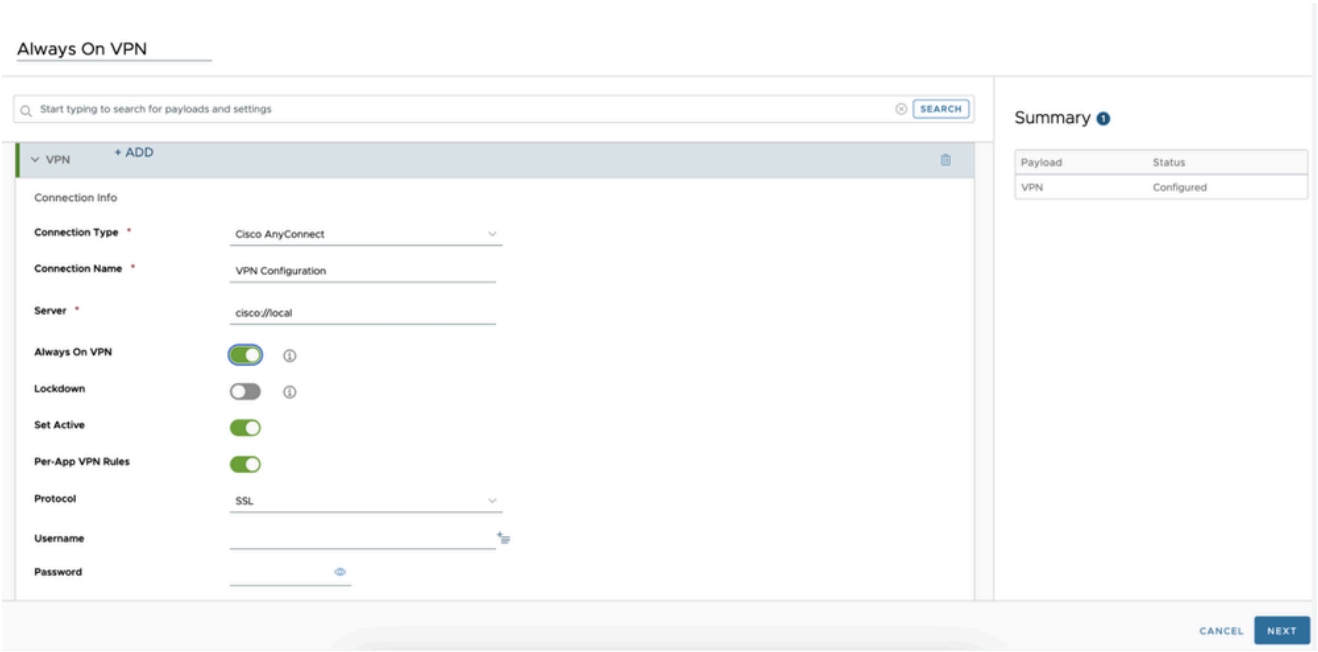


3. Configurare le impostazioni VPN:



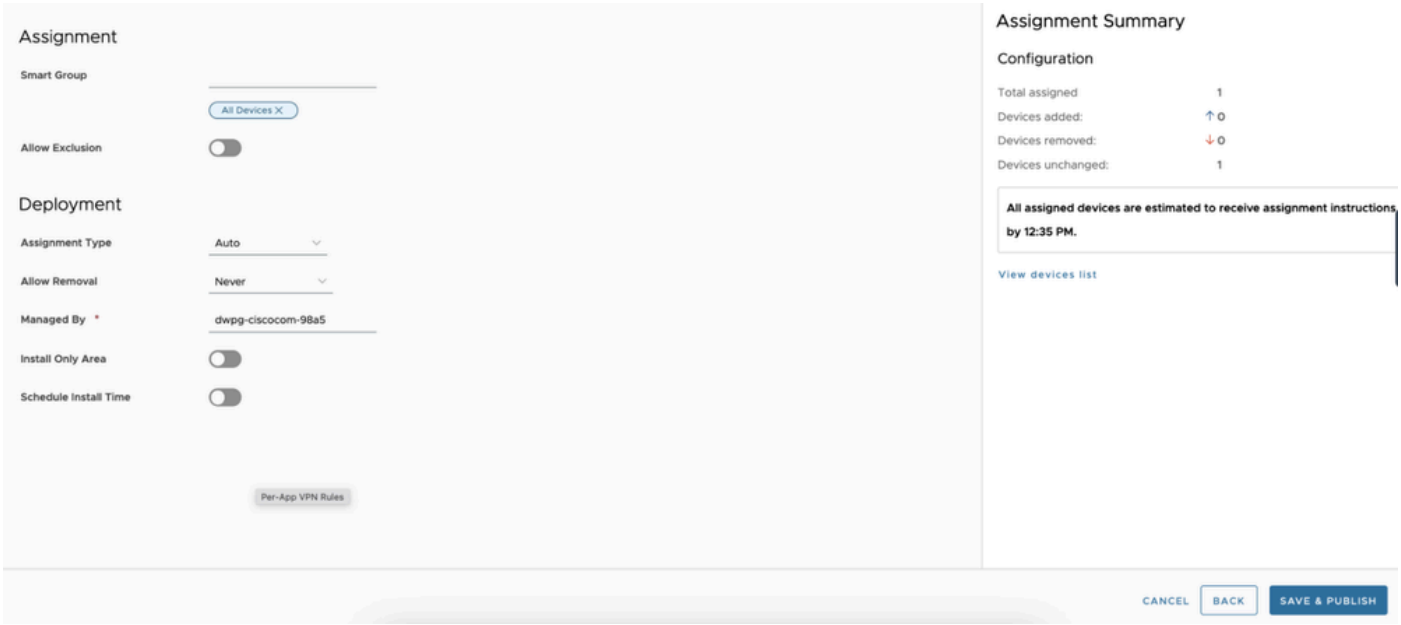
- Nella sezione del profilo, andare a Impostazioni VPN e fare clic su Aggiungi.
- Compilare i campi obbligatori:
  - Tipo di connessione:Cisco AnyConnect
  - Server:cisco://local
  - Abilitare la VPN Always On e configurare altre proprietà in base alle esigenze.
  - Abilita regole VPN per app.
  - EnableSet Attivo.

- Fare clic su Avanti.



4. Assegna profilo:

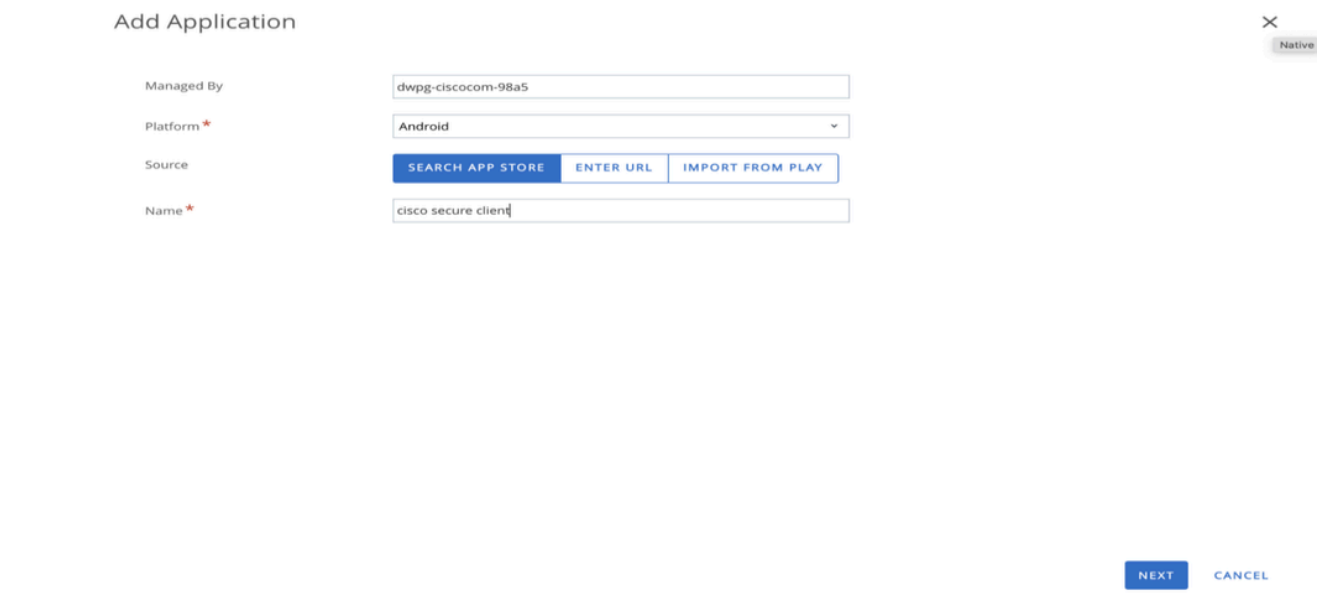
- Lasciare vuoto il gruppo smart.
- Assegnare il profilo ai dispositivi necessari.
- Selezionare i valori di distribuzione.
- Fare clic su Salva e pubblica.



B. Assegnazione dell'app Cisco Secure Client

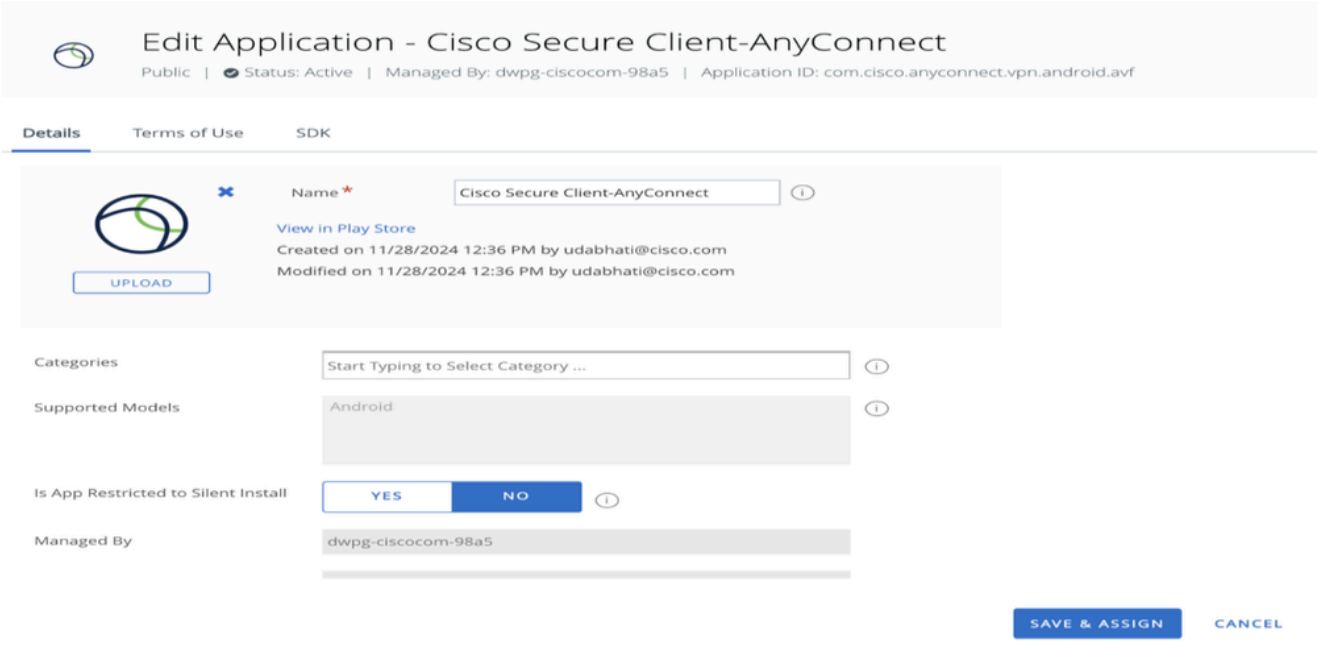
1. Aggiungi l'app:

- Andare a Risorse > Native > Pubbliche.
- Aggiungere Cisco Secure Client dal Play Store, se non è già disponibile.



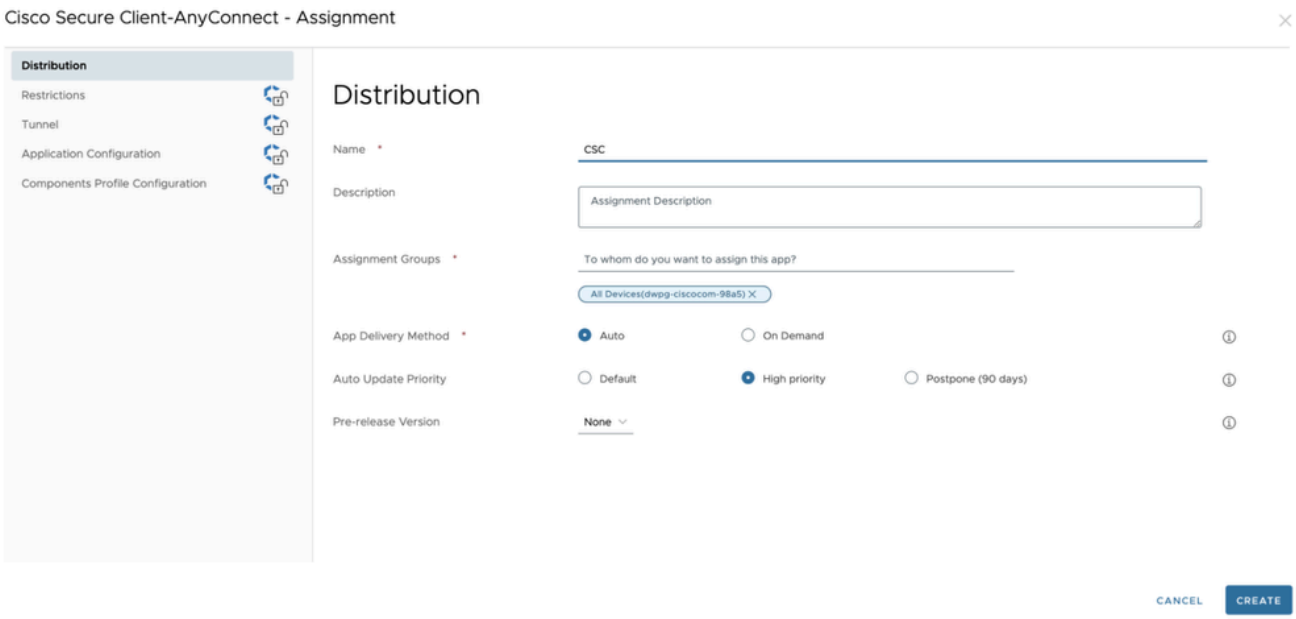
2. Assegnazione app:

- Selezionare l'app e immettere i valori richiesti.
- Nella sezione assegnazione creare una nuova assegnazione.



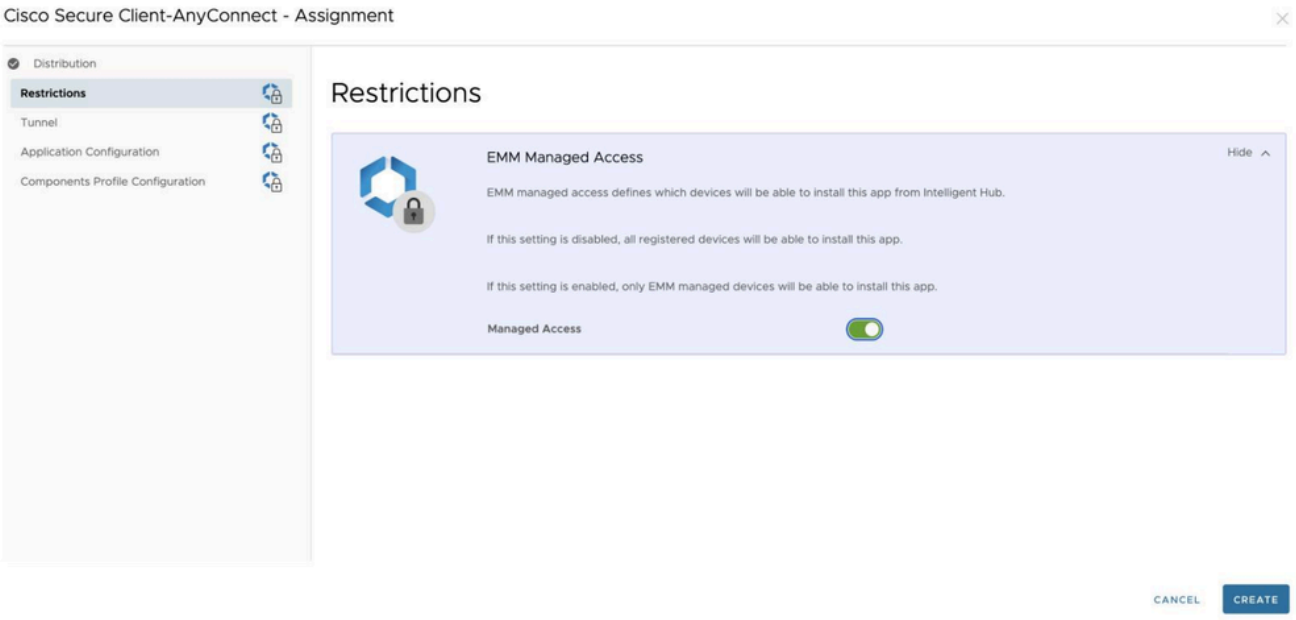
3. Configura distribuzione:

- Immettere i dettagli nella sezione Distribuzione.



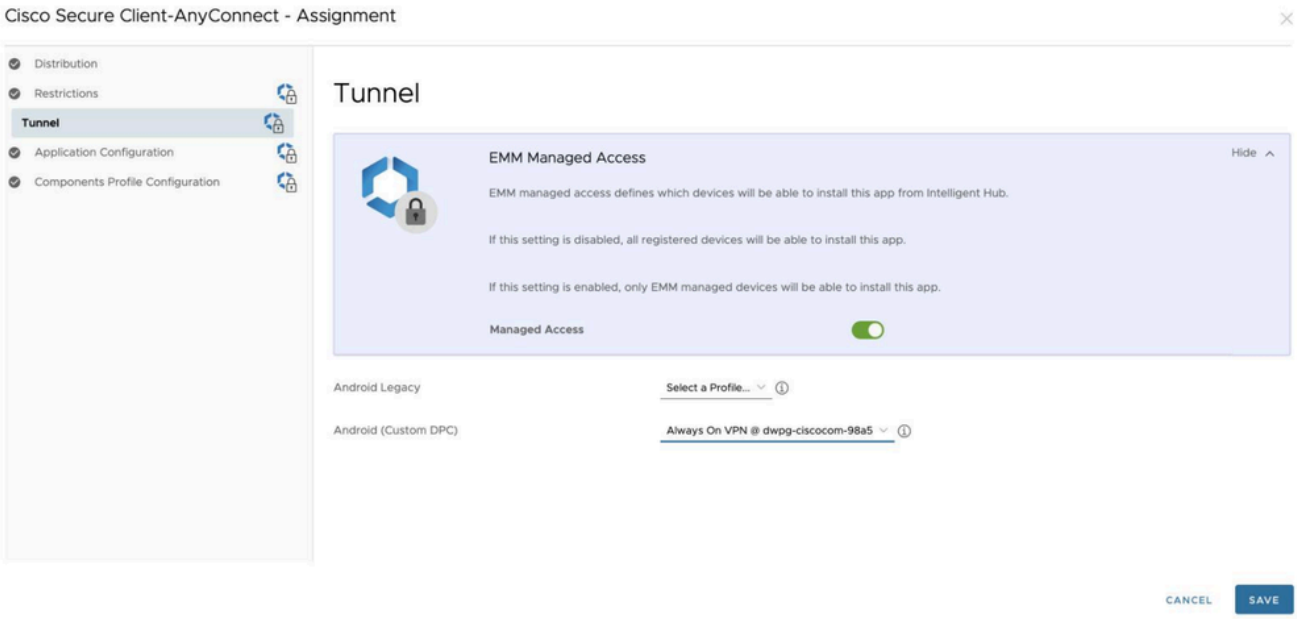
4. Abilita accesso gestito:

   - Nella scheda Restrictionstab, abilitare l'accesso gestito.



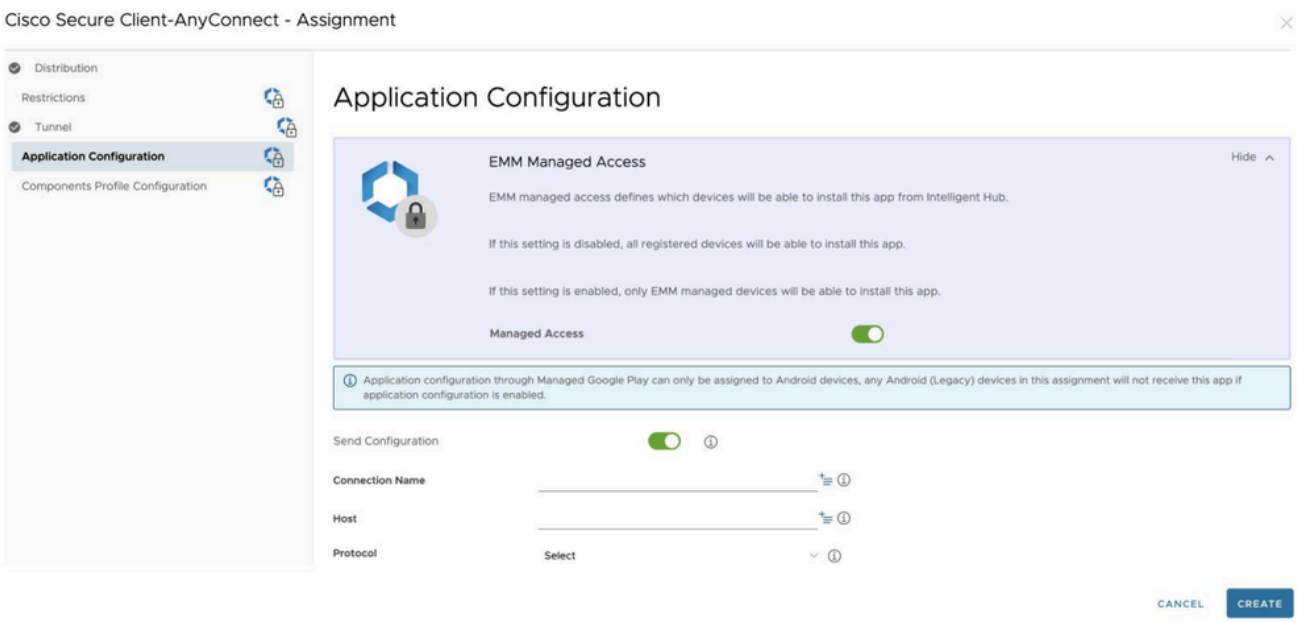
5. Seleziona profilo:

   - Nell'opzione Tunneling, selezionare il profilo creato in precedenza ('Always On VPN') in Android (Custom DPC).



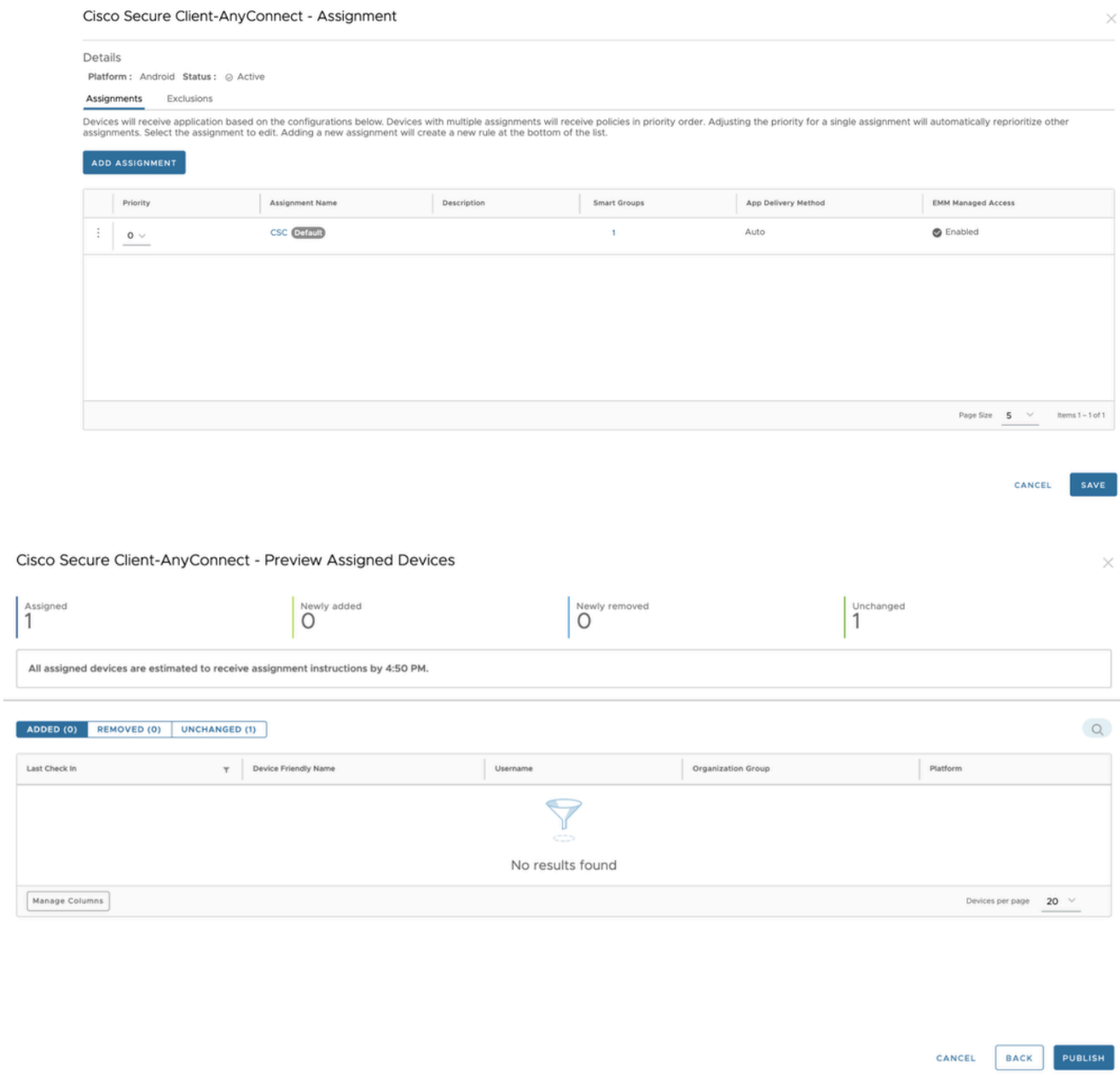
6. Configurazione applicazione:

- Immettere i dettagli di configurazione dell'applicazione, ad esempio ID organizzazione e Token reg, dal file di configurazione Android scaricato da Umbrella Dashboard.
- Abilitare Accetta SEULA per gli utenti in modo da ignorare l'accettazione manuale SEULA.
- Abilita la modalità VPN sempre attiva per la protezione degli ombrelli solo per una gestione VPN senza problemi da parte di Cisco Secure Client.
- Impedisce agli utenti di creare nuove connessioni VPN (lasciare vuoto il campo Host).



7. Salva e pubblica:

- Salva le modifiche e pubblica l'app Cisco Secure Client.



8. Eseguire il push del certificato Umbrella:

   - Per istruzioni, vedere: [Invia certificato ombrello ai dispositivi]

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).