Configurazione di SNA Manager per Microsoft Entra ID SSO

Sommario

Introduzione

In questo documento viene descritto come configurare Secure Network Analytics (SNA) per l'utilizzo di Microsoft Entra ID per Single Sign-On (SSO).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Microsoft Azure
- Secure Network Analytics

Componenti usati

- SNA Manager v7.5.2
- ID Entra Microsoft

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.

Procedura di configurazione

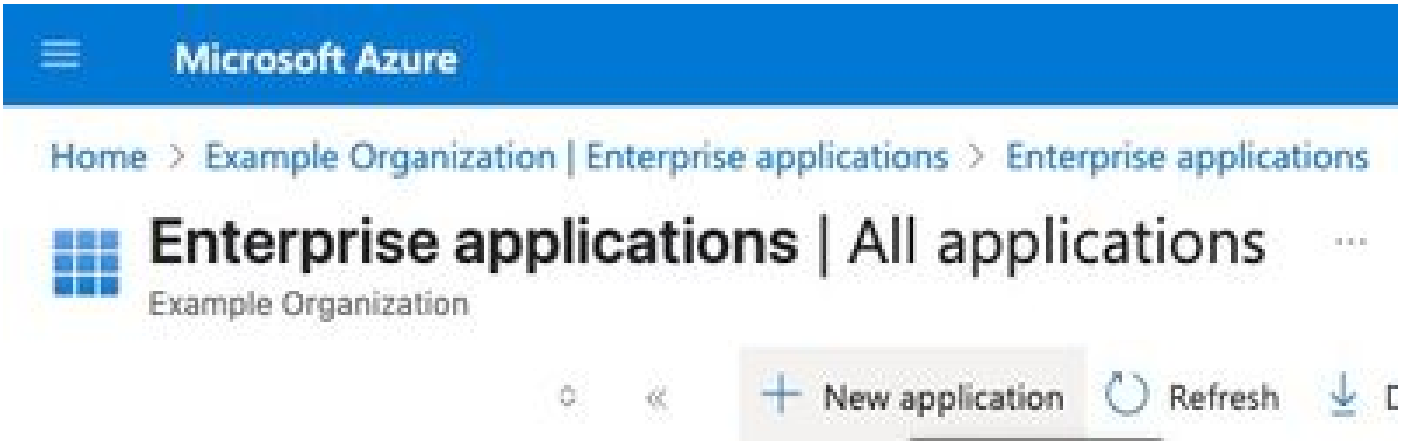
Configura applicazione enterprise in Azure

1. Accedere al portale cloud di Azure.

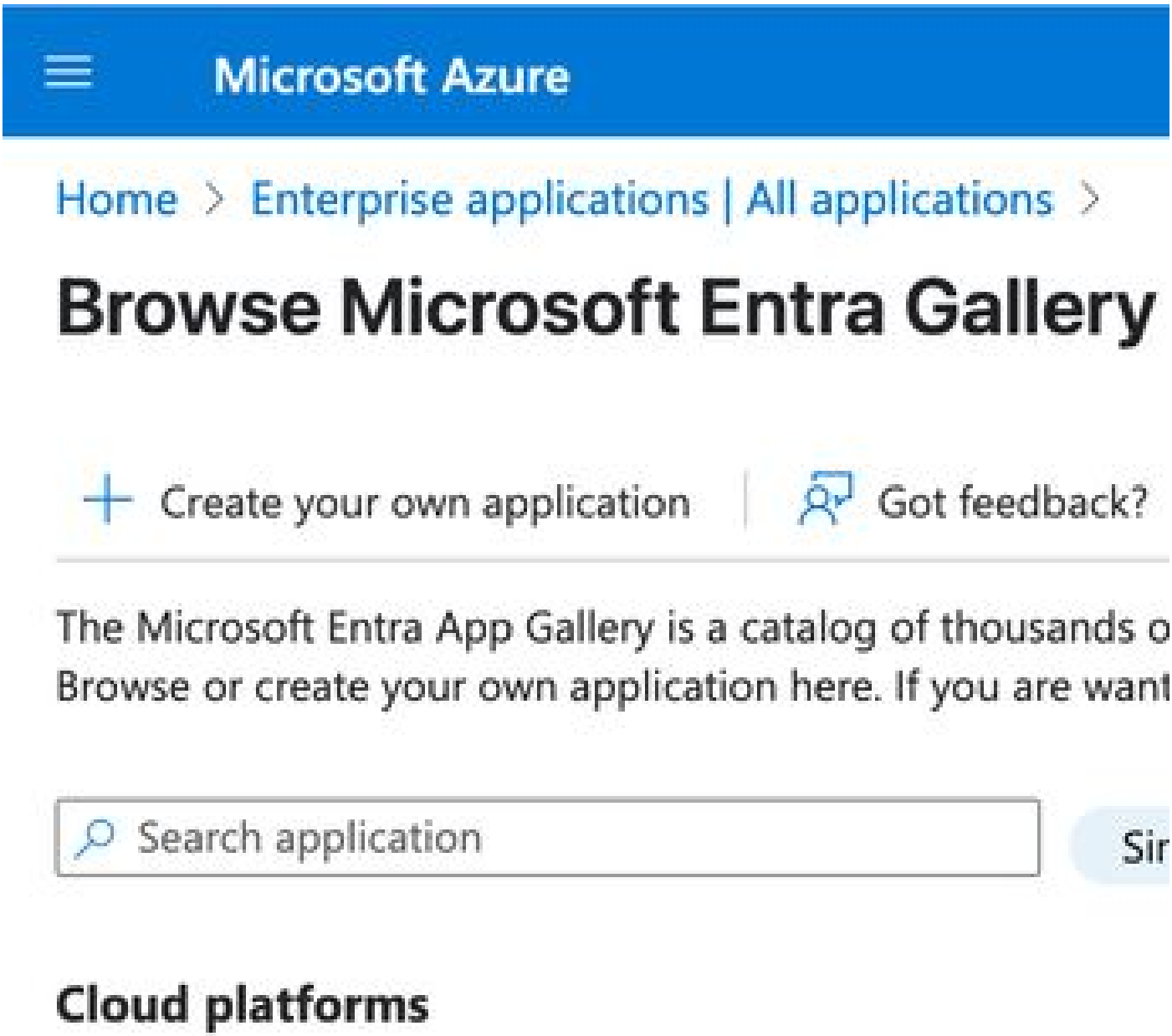
2. Cercare il servizio Entra ID nella casella di ricerca e selezionare Microsoft Entra ID.

3. Nel riquadro di sinistra espandere Gestisci e selezionare Applicazioni enterprise.

4. Fare clic su Nuova applicazione.



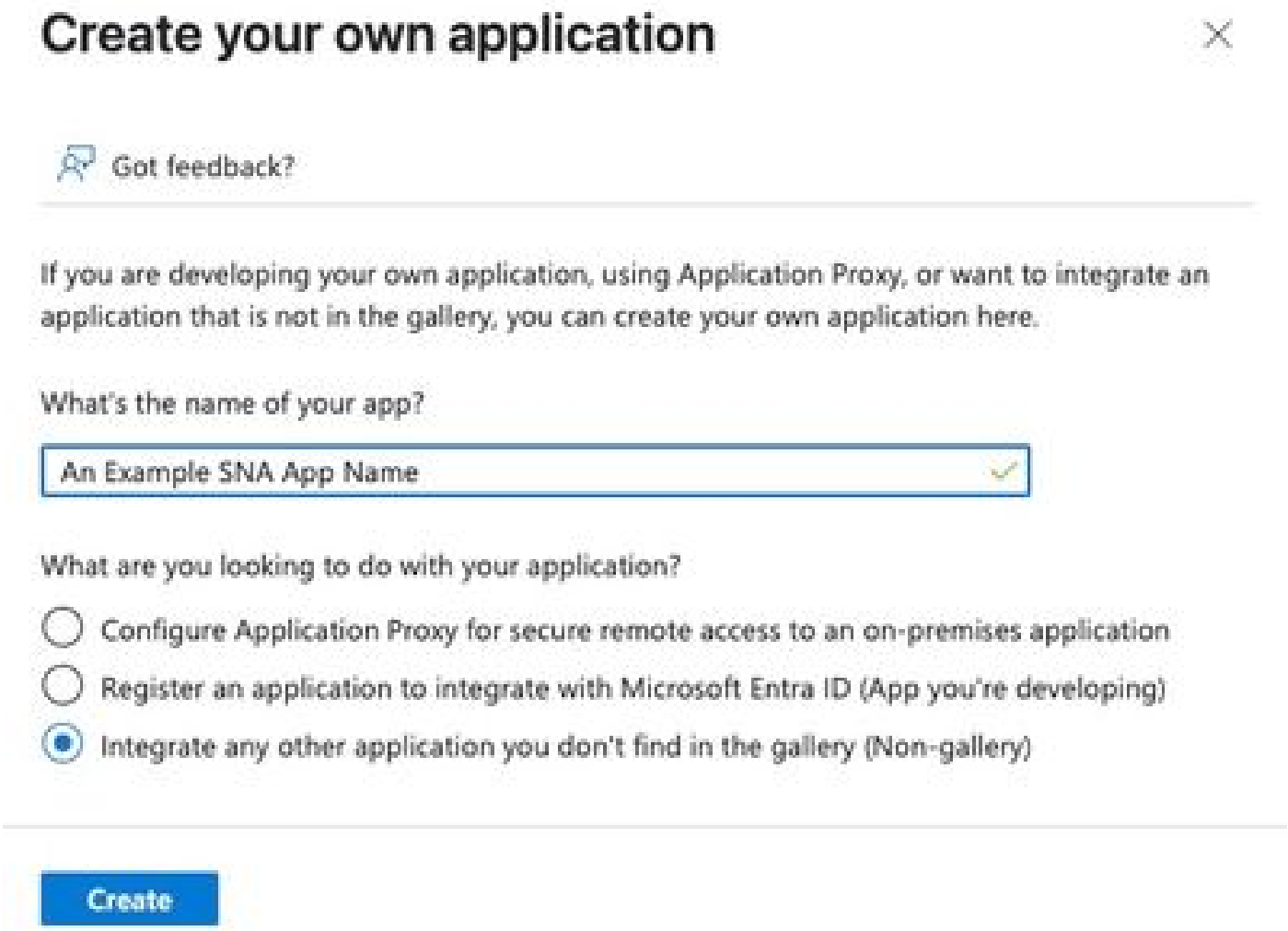
5. Selezionare Crea applicazione personalizzata nella nuova pagina che viene caricata.



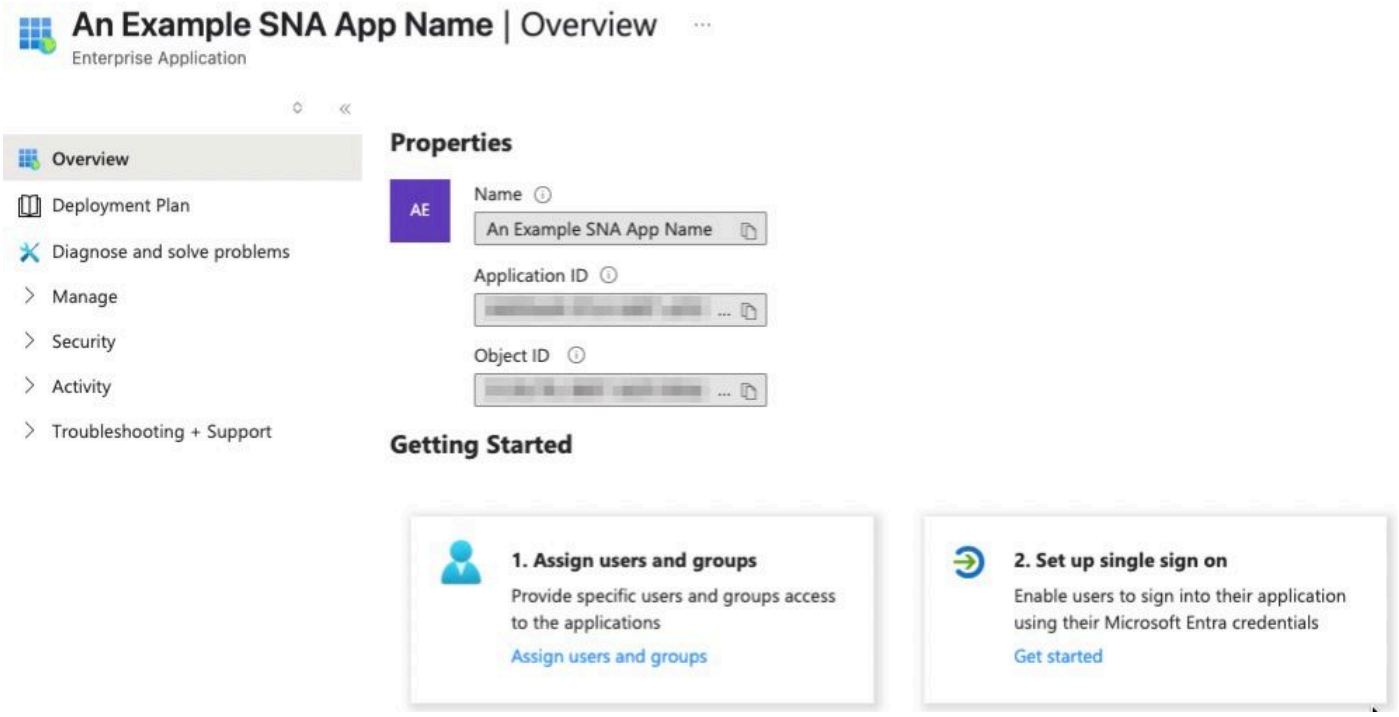
Azure-UI

6. Fornire un nome all'applicazione in Qual è il nome dell'applicazione? campo.

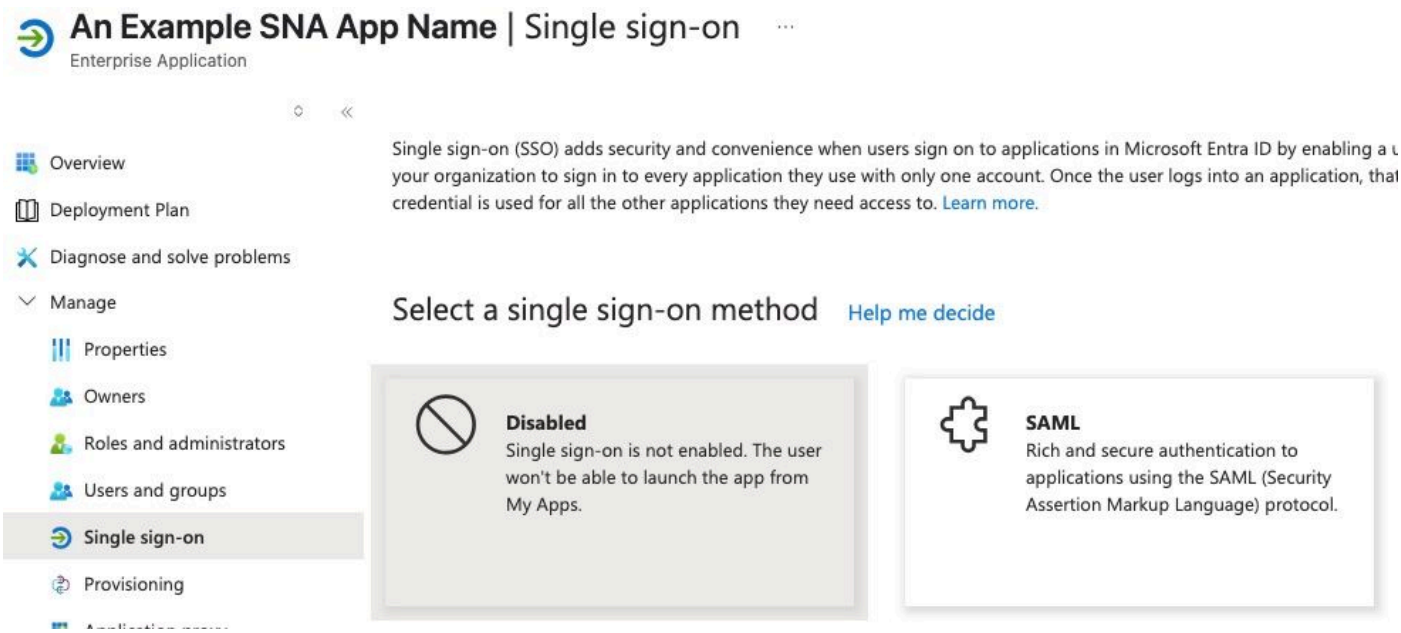
7. Selezionare il pulsante di opzione Integra qualsiasi altra applicazione non presente nella raccolta (Non-Gallery) e fare clic su Crea.



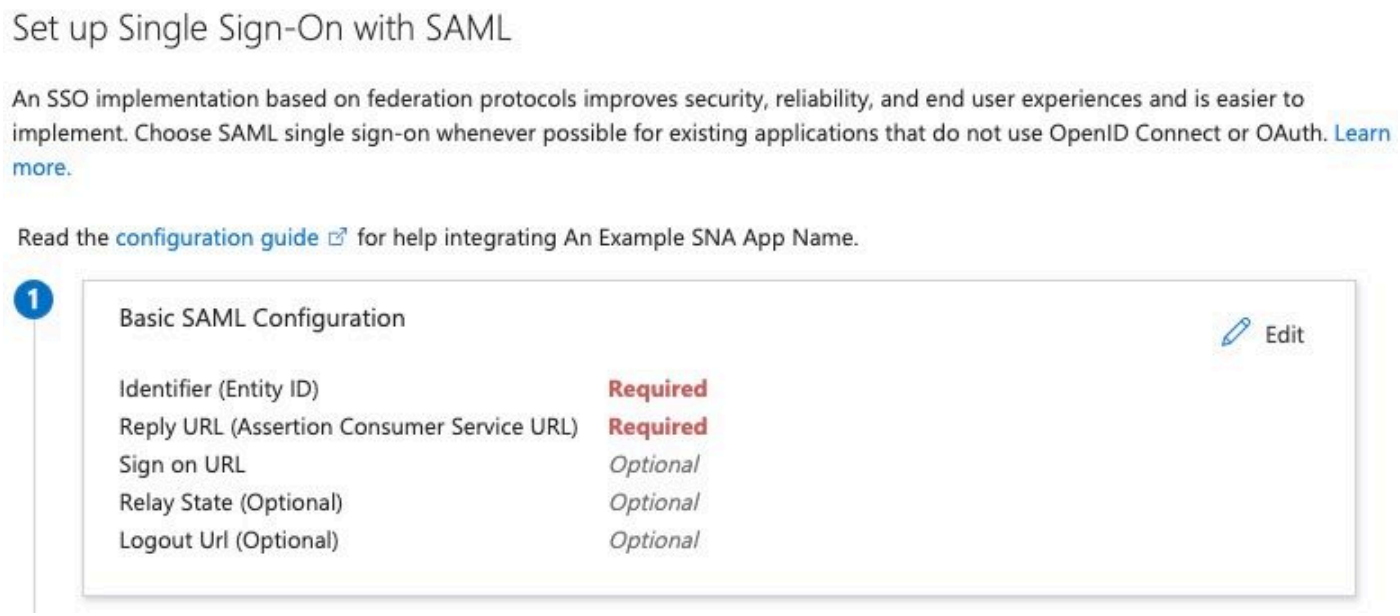
8. Nel dashboard dell'applicazione appena configurato, fare clic su Imposta Single Sign-On.



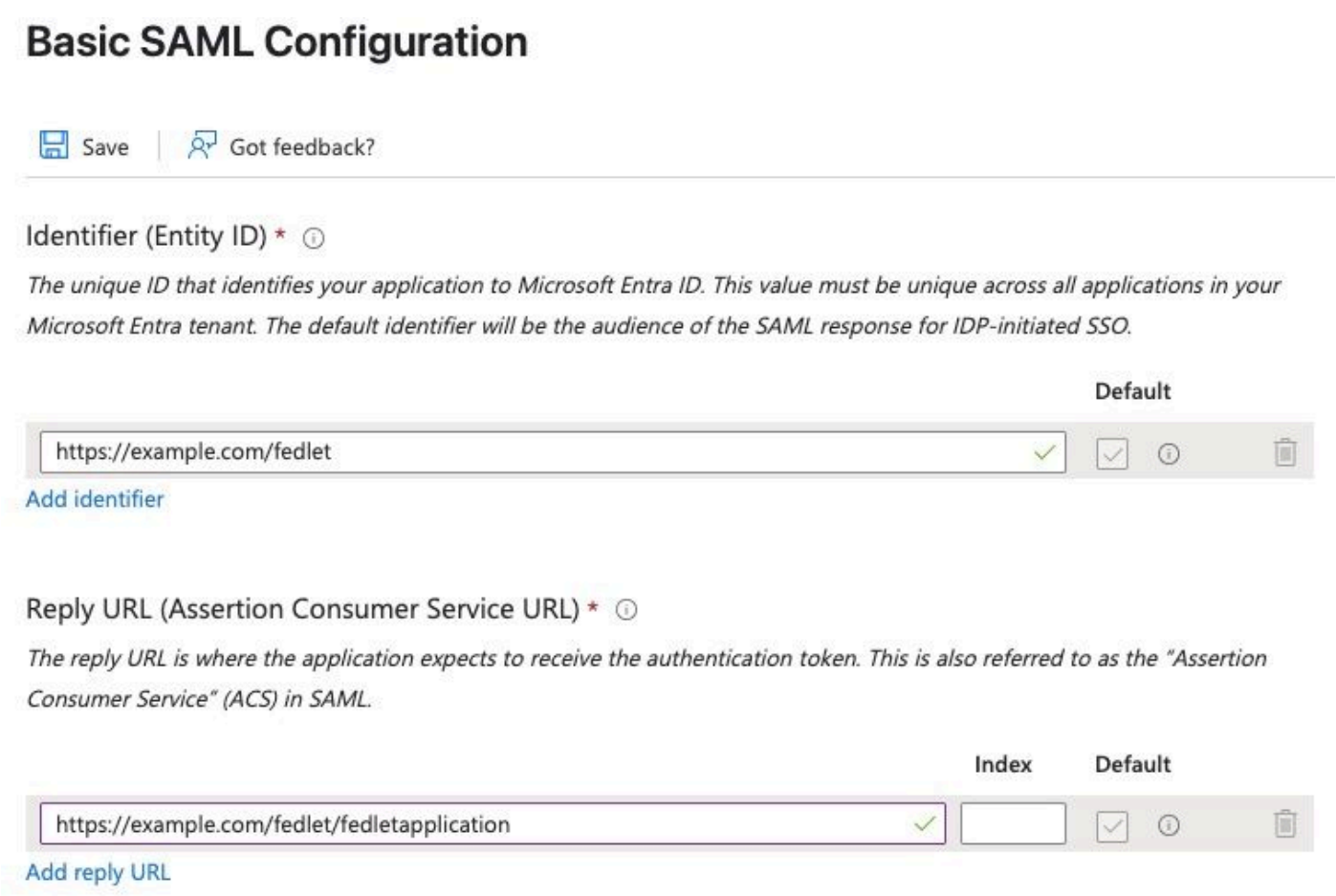
9. Selezionare SAML.



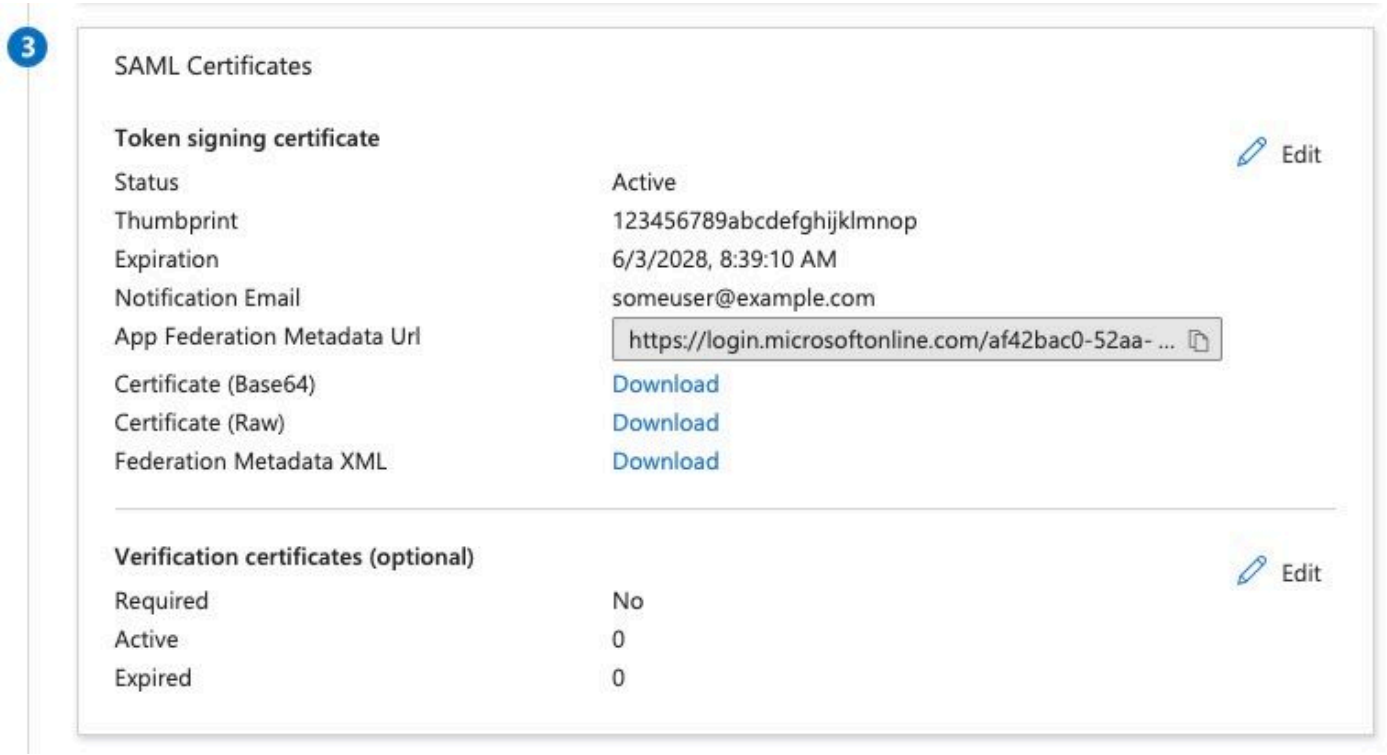
10. Nella pagina Configurazione Single Sign-On con SAML fare clic su Modifica in Configurazione SAML di base.



11. In Basic SAML Configuration pane configurare Add Reply URL in https://example.com/fedlet/fedletapplication sostituendo example.com con FQDN di SNA Manager e fare clic su save.

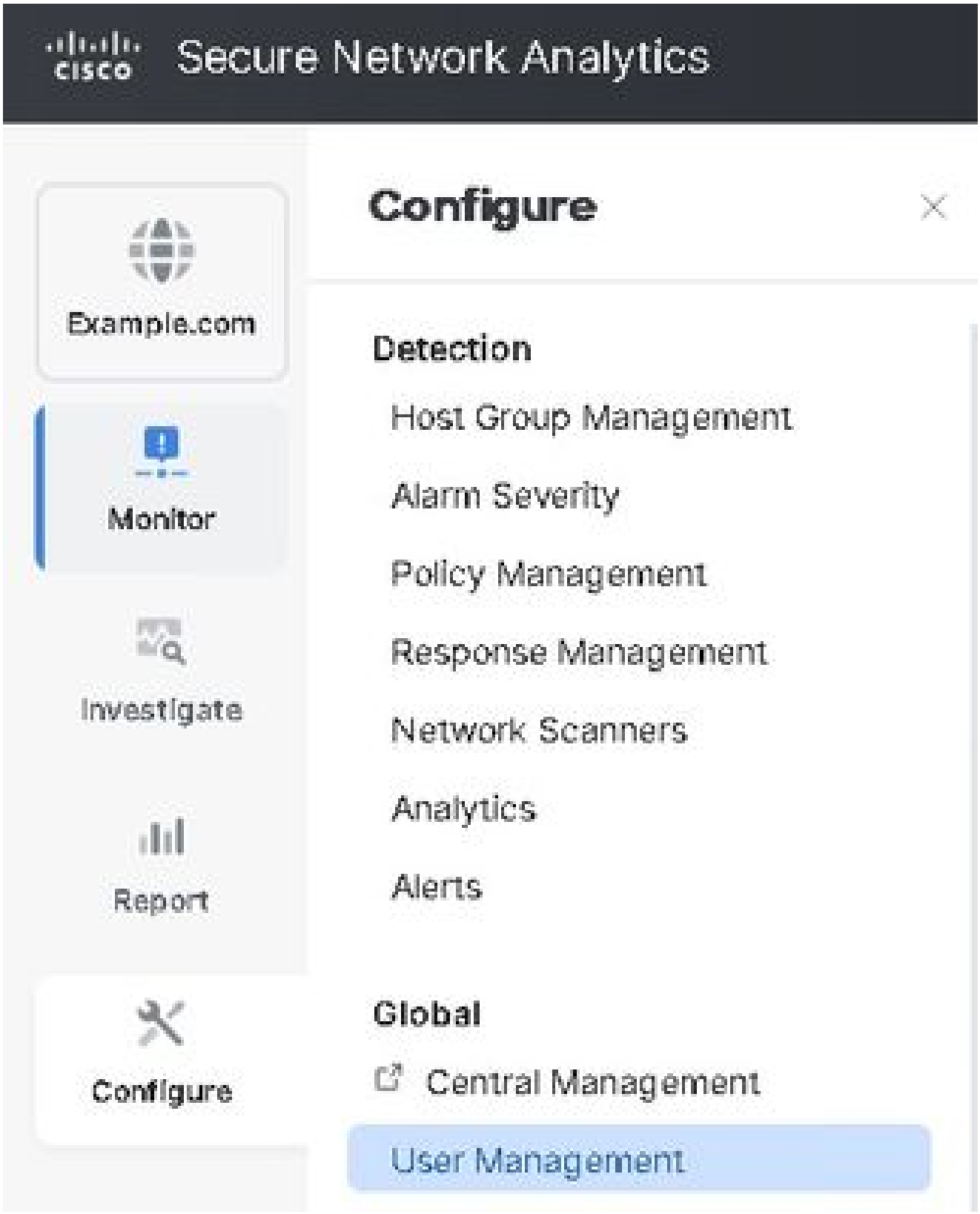


12. Individuare la scheda Certificati SAML e salvare il valore del campo URL metadati federazione app e scaricare il file XML metadati federazione.

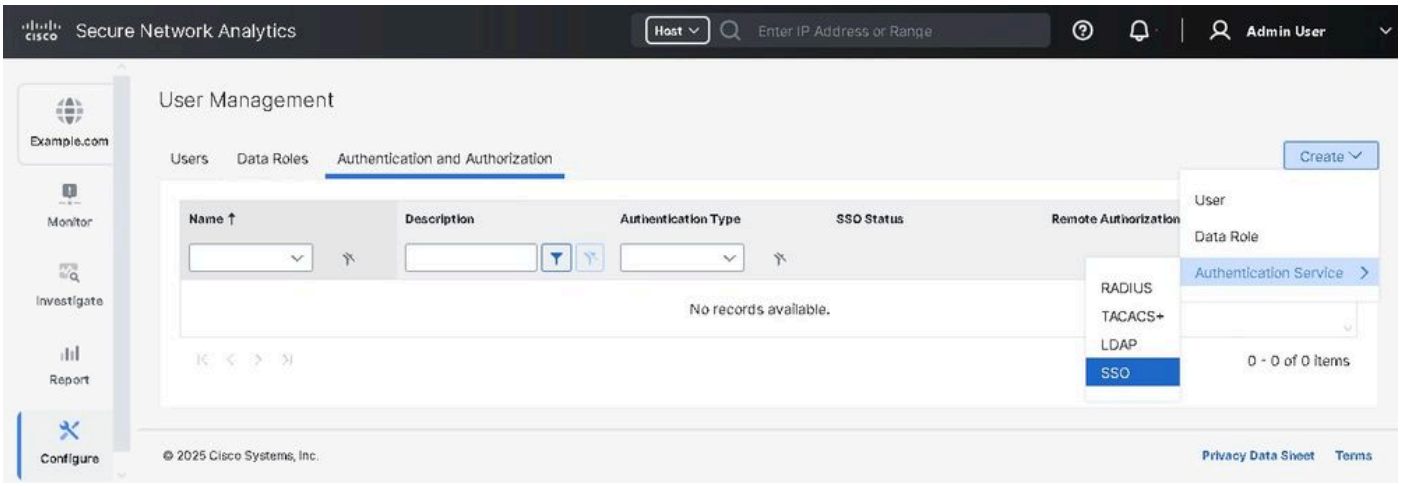


Configurazione e download del file XML del provider di servizi in SNA

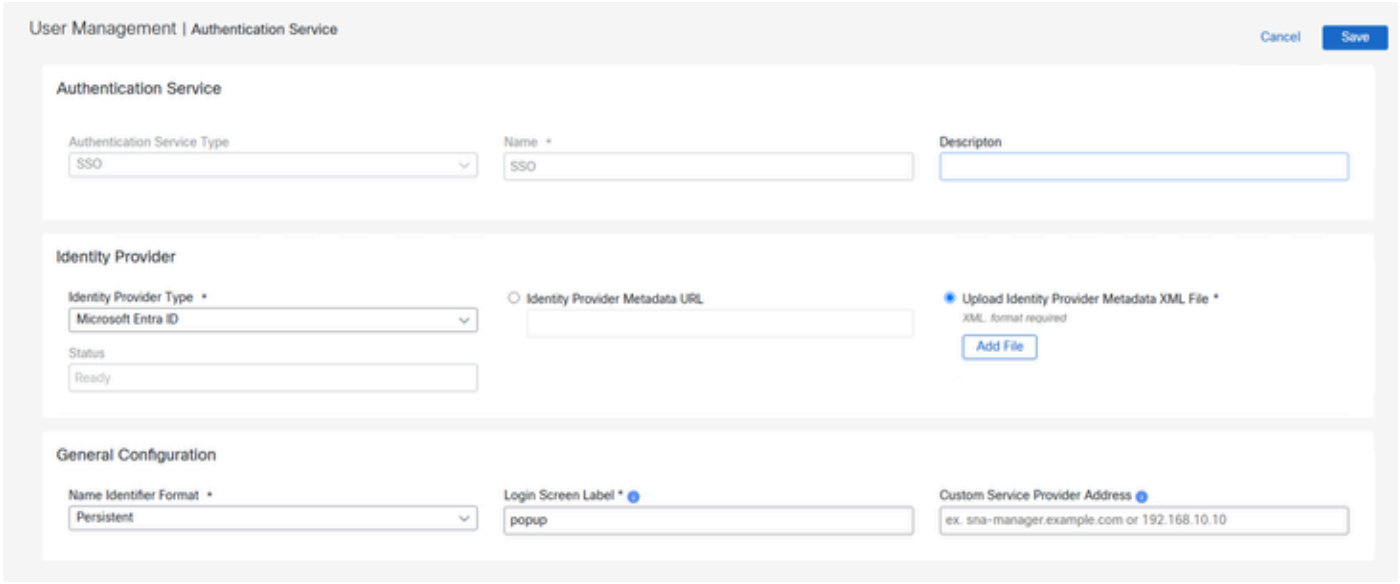
1. Accedere all'interfaccia utente di SNA Manager.
2. Passare a Configura > Globale > Gestione utente.

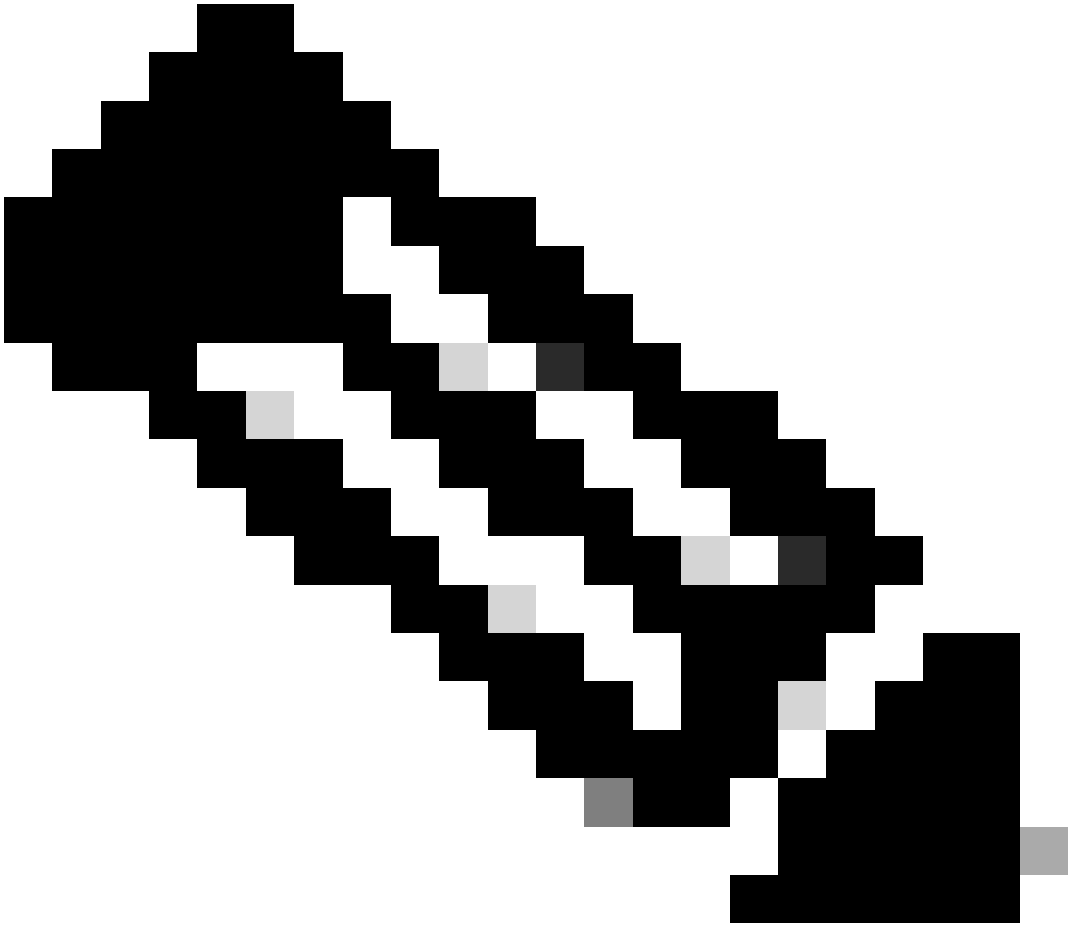


3. In scheda Autenticazione e autorizzazione fare clic su Crea > Servizio di autenticazione > SSO.



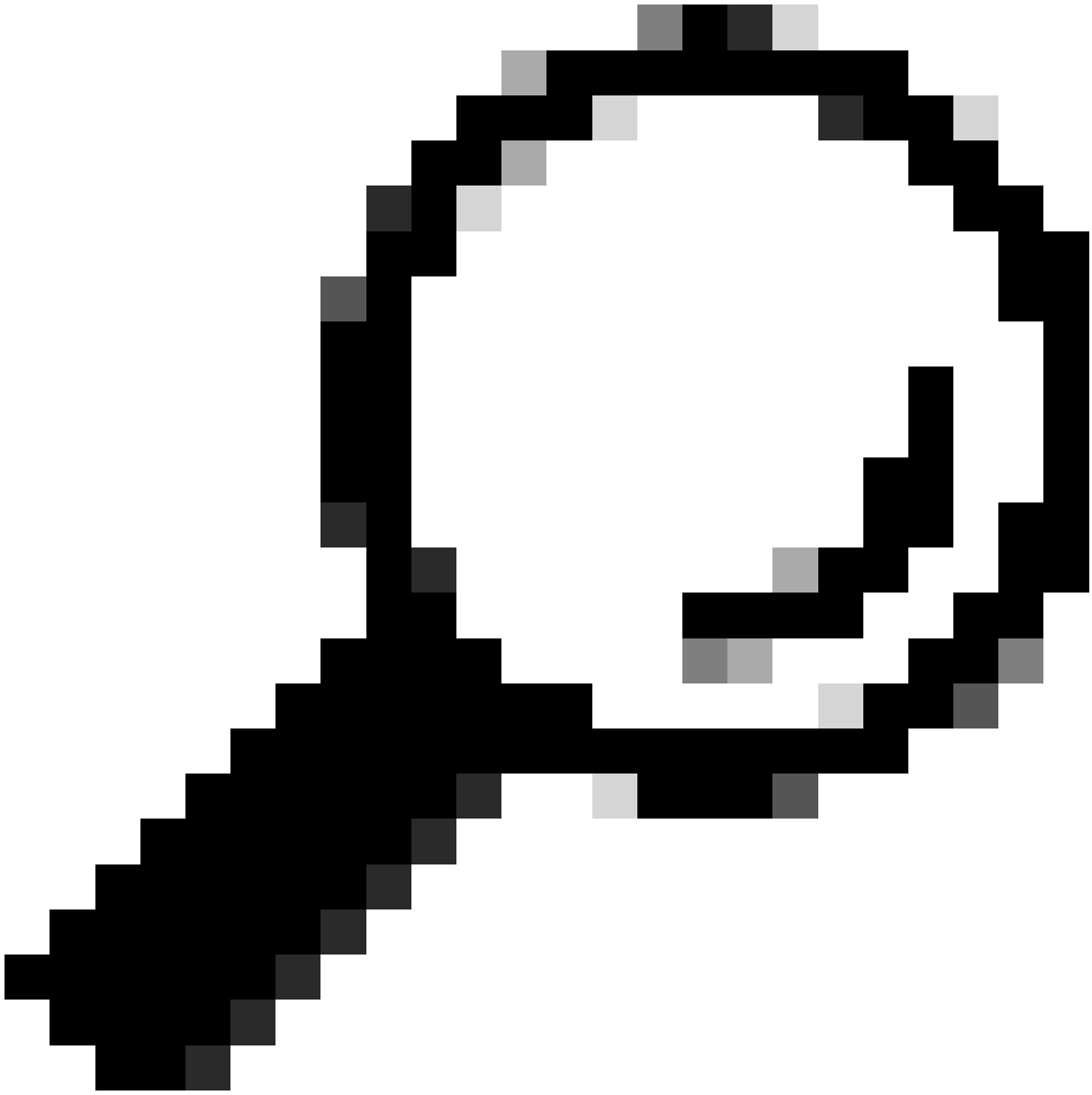
4. Selezionare il pulsante di opzione appropriato per URL metadati provider di identità o Carica file XML metadati provider di identità.





Nota: In questa demo è selezionata l'opzione Carica file XML metadati del provider di identità.

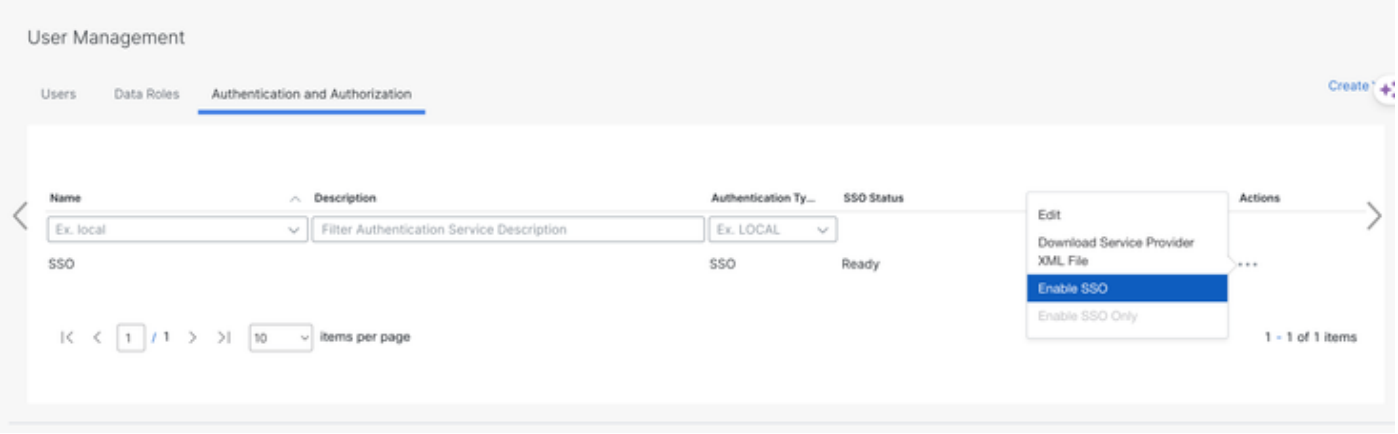
5. Configurare il campo Tipo di provider di identità su Microsoft Entra ID, Formato identificatore nome su Permanente, Digitare un'etichetta per la schermata di accesso.



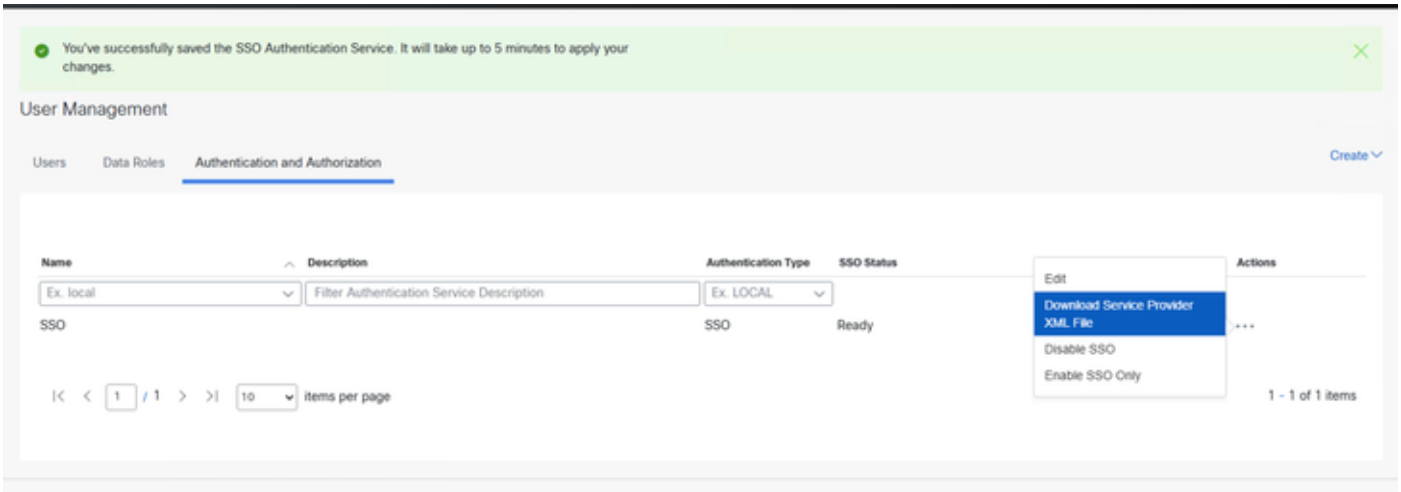
Suggerimento: L'etichetta della schermata di accesso configurata (nome/testo) viene visualizzata sopra il pulsante Accesso con SSO e non deve essere lasciata vuota.

6. Fare clic su Salva per tornare alla scheda Autenticazione e autorizzazione.

7. Attendere che lo stato sia READY e selezionare Abilita SSO dal menu Azione.



8. In Autenticazione e autorizzazione scheda fare clic sui tre punti nella colonna Azioni e fare clic su Scarica il file XML del provider di servizi.



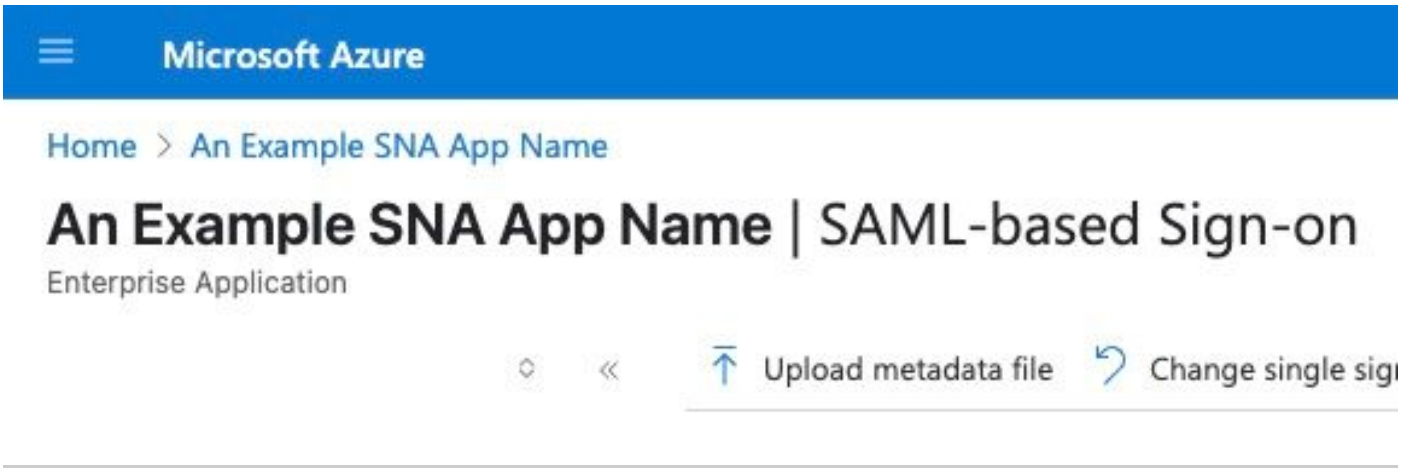
Configura SSO in Azure

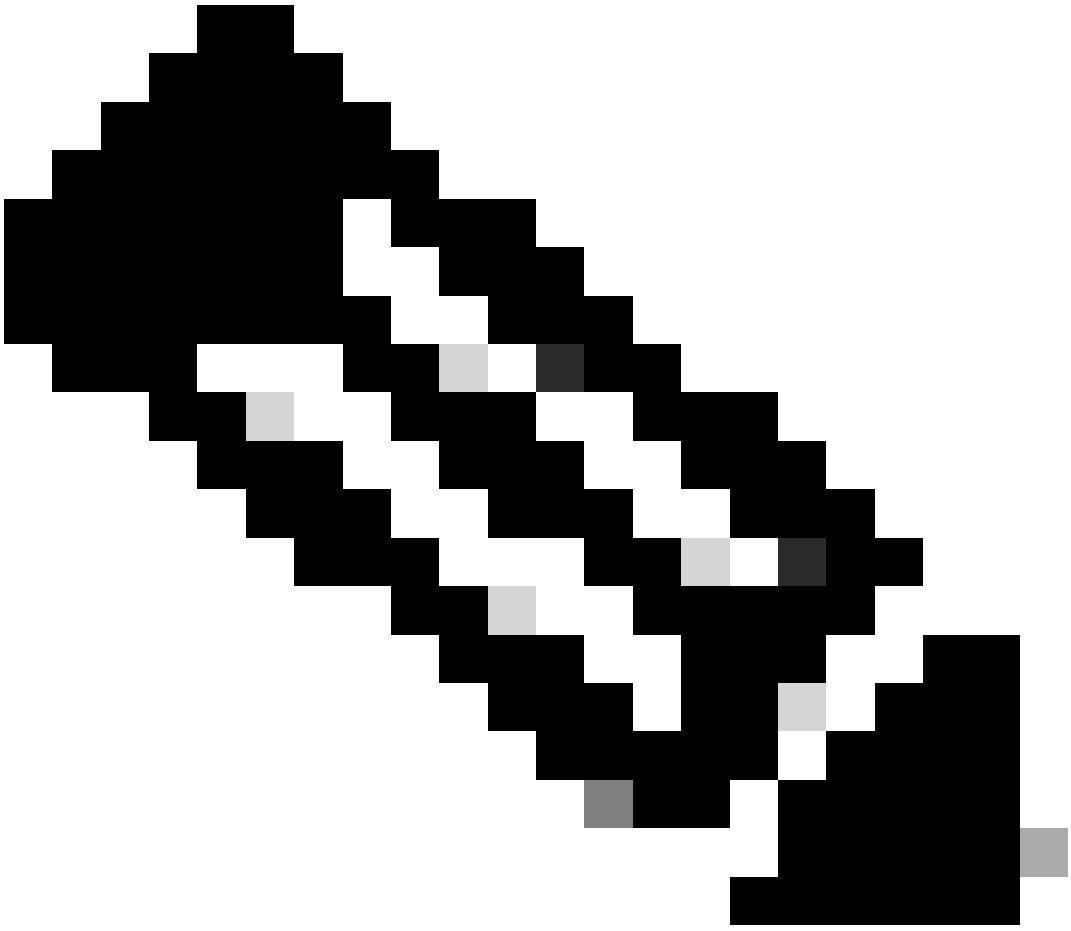
1. Accedere al portale di Azure.

2. Dalla barra di ricerca passare a Applicazione enterprise > Seleziona applicazione enterprise configurata > Fare clic su Imposta Single Sign-On.

3. Fare clic su Upload metadata file nella parte superiore della pagina e caricare il file sp.xml scaricato da SNA Manager.

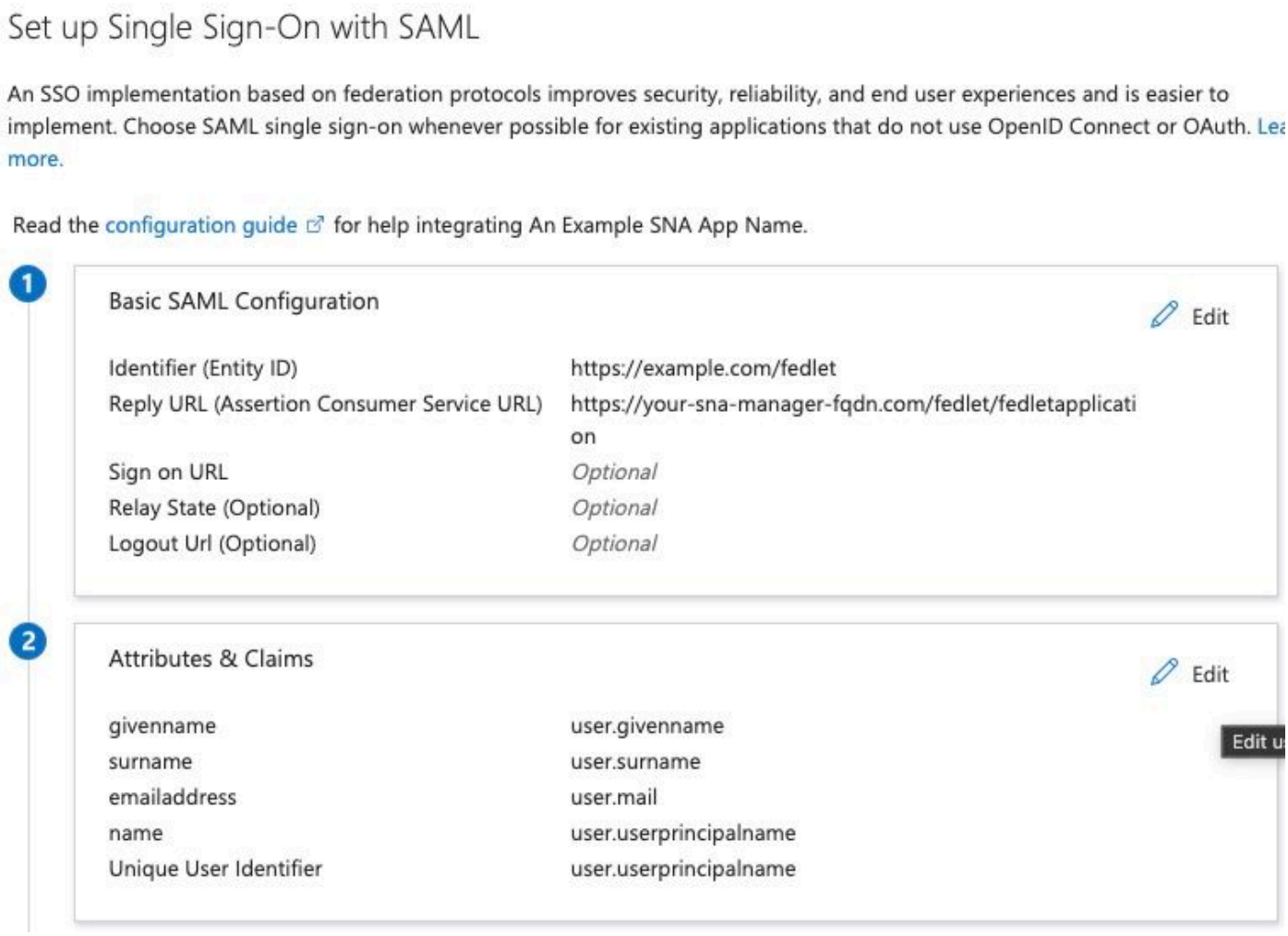
4. Viene visualizzata la schermata "Basic SAML Configuration" (Configurazione SAML di base) e si impostano varie impostazioni per correggere i valori. Fare clic su Save (Salva).



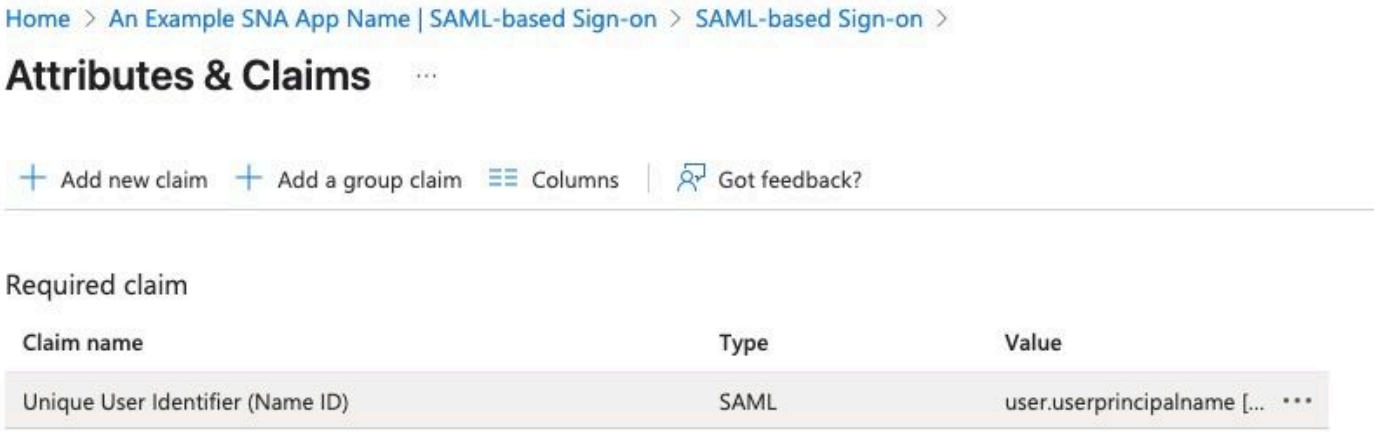


Nota: Assicurarsi che il formato ID del nome in Entra ID sia corretto.

5. Individuare la sezione Attributi e richieste di rimborso e fare clic su Modifica.



6. Fare clic sul valore user.userprincipalname nella sezione Nome attestazione.



7. In Gestisci risarcimento pagina Verifica Scegli formato identificativo nome.

Microsoft Azure

Search

Home > An Example SNA App Name | SAML-based Sign-on > SAML-based Sign-on > Attributes & Claims >

Manage claim ...

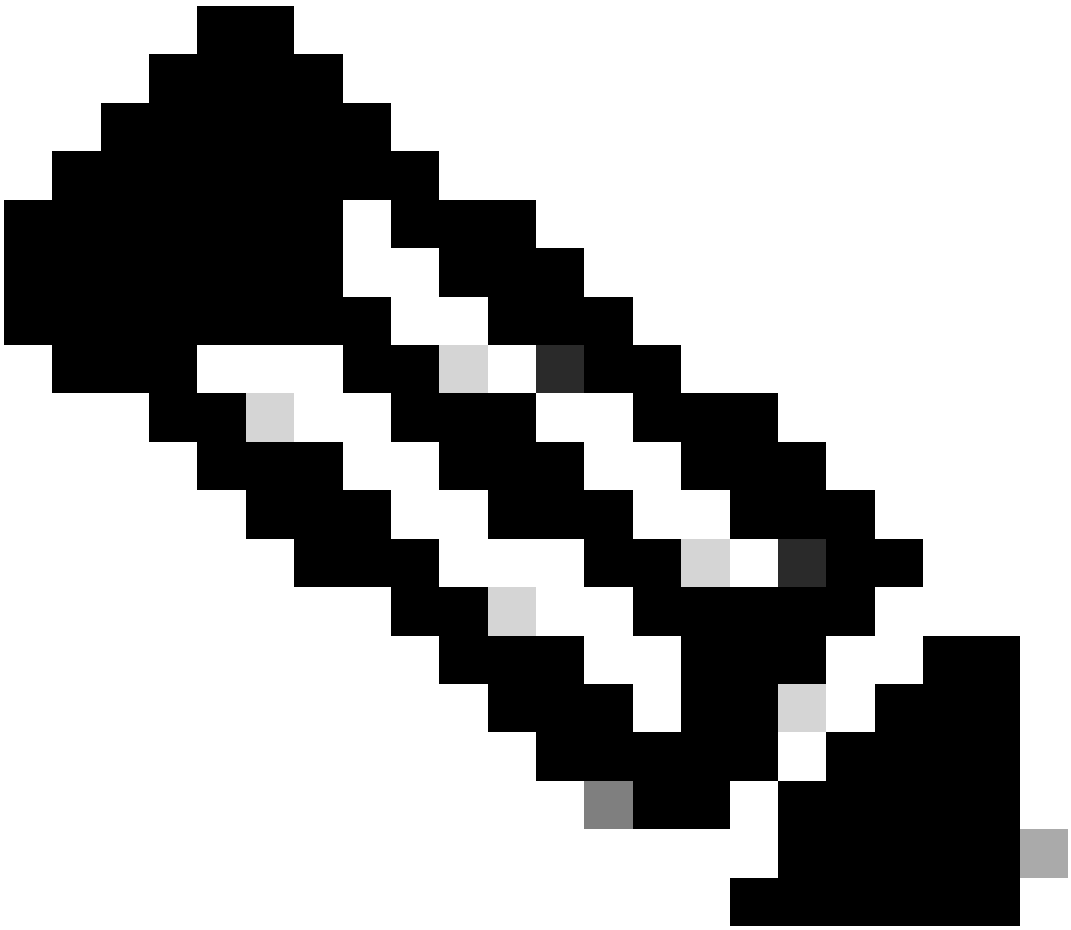
Save | Discard changes | Got feedback?

Name: nameidentifier

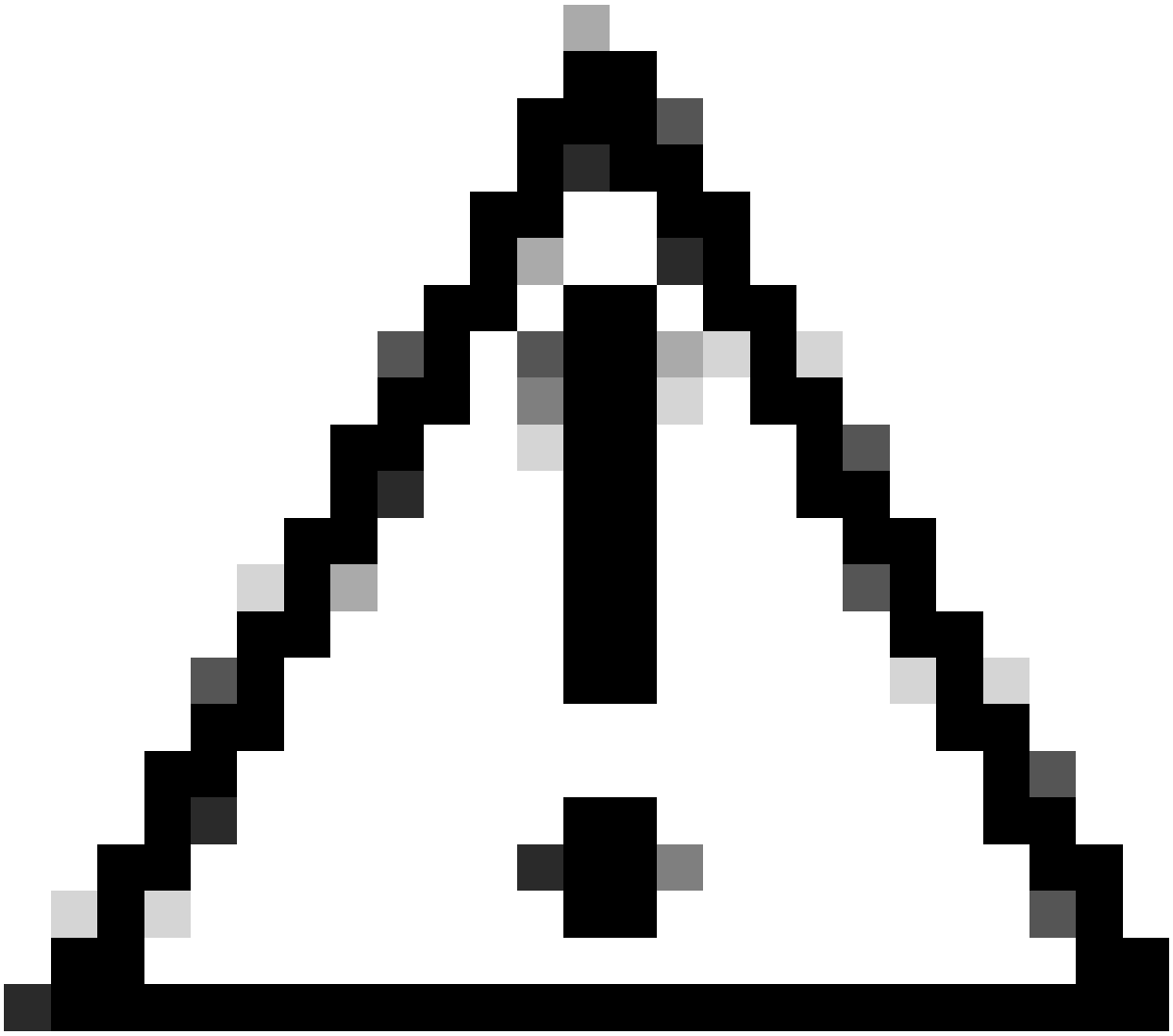
Namespace: http://schemas.xmlsoap.org/ws/2005/05/identity/claims

Choose name identifier format

Name identifier format *: Persistent



Nota: Il campo Formato identificatore nome è impostato su Persistente se non è selezionato dal menu a discesa. Fare clic su Salva se sono state apportate modifiche.

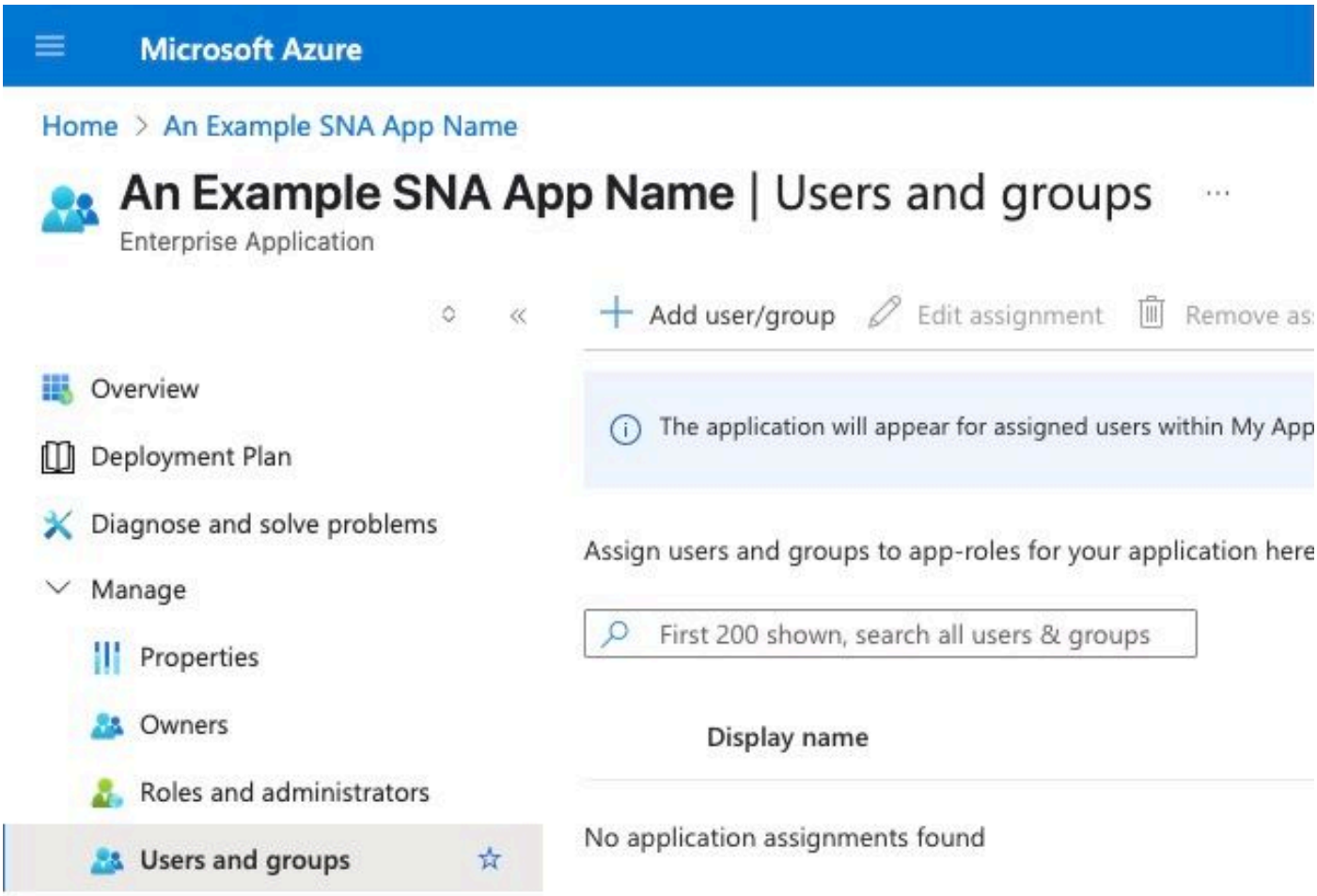


Attenzione: Si tratta del luogo più comune in cui si verificano problemi. Le impostazioni in Gestione SNA e Microsoft Azure devono corrispondere. se si è scelto di utilizzare il formato "indirizzo e-mail" in SNA, il formato deve essere "indirizzo e-mail".

Impostare gli utenti in Entra ID.

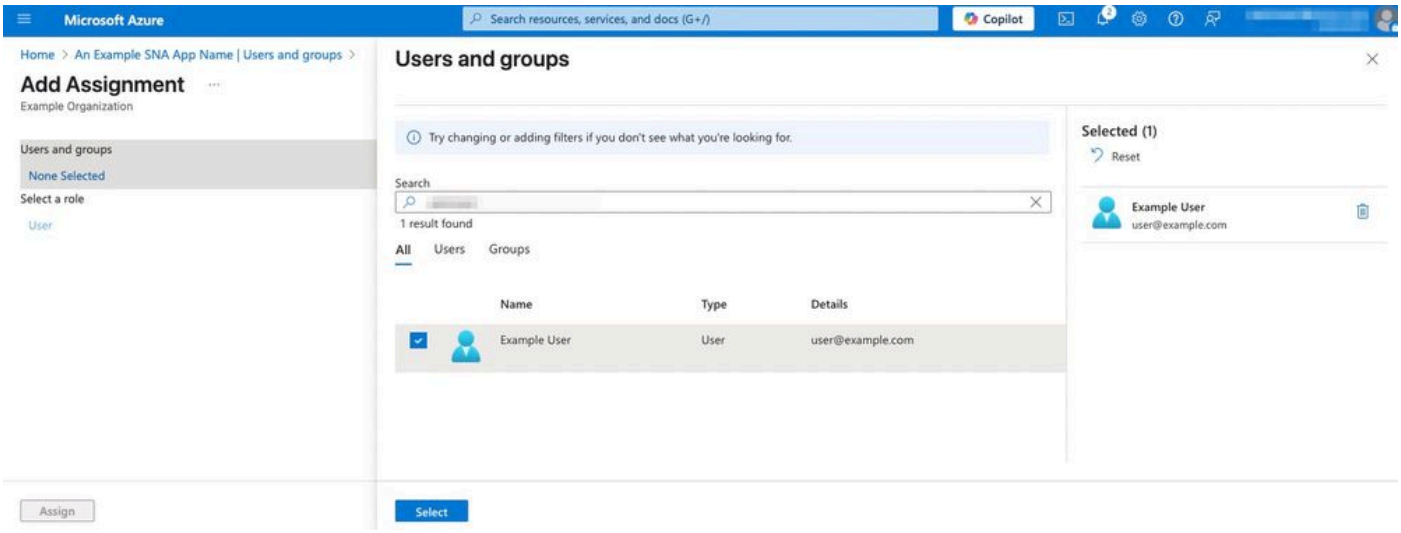
1. Accedere al portale di Azure.

2. Dalla barra di ricerca passare a Applicazione enterprise > Seleziona applicazione enterprise configurata > seleziona utenti e gruppi a sinistra > fare clic su Aggiungi utente/gruppo.



3. Nel riquadro sinistro fare clic su Nessuna selezione.

4. Cercare e aggiungere l'utente richiesto all'applicazione.

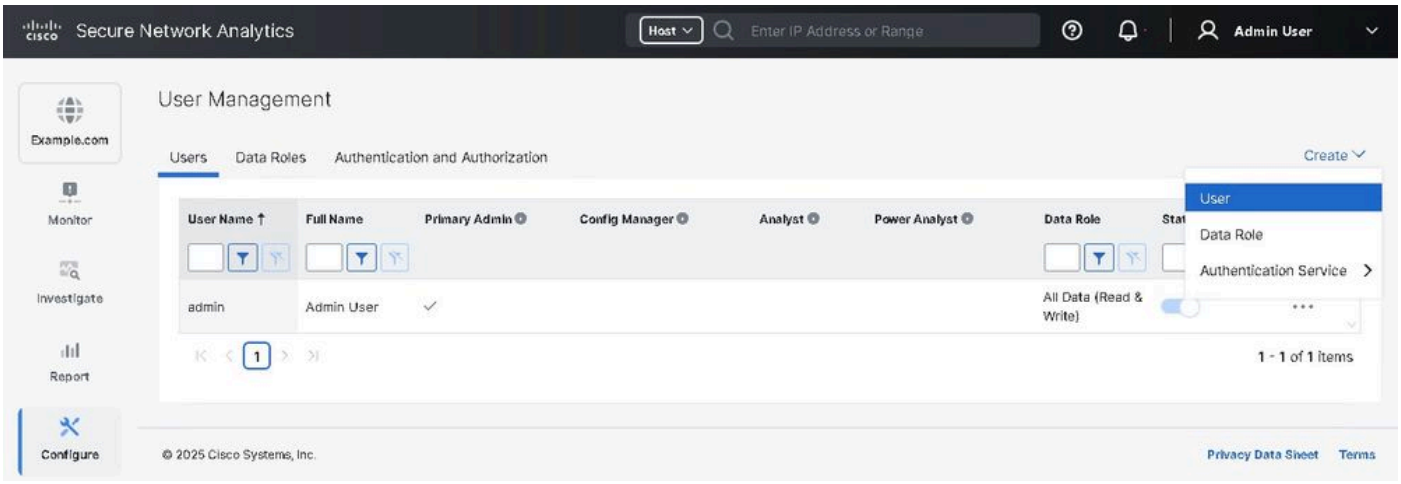


Configura SSO in SNA

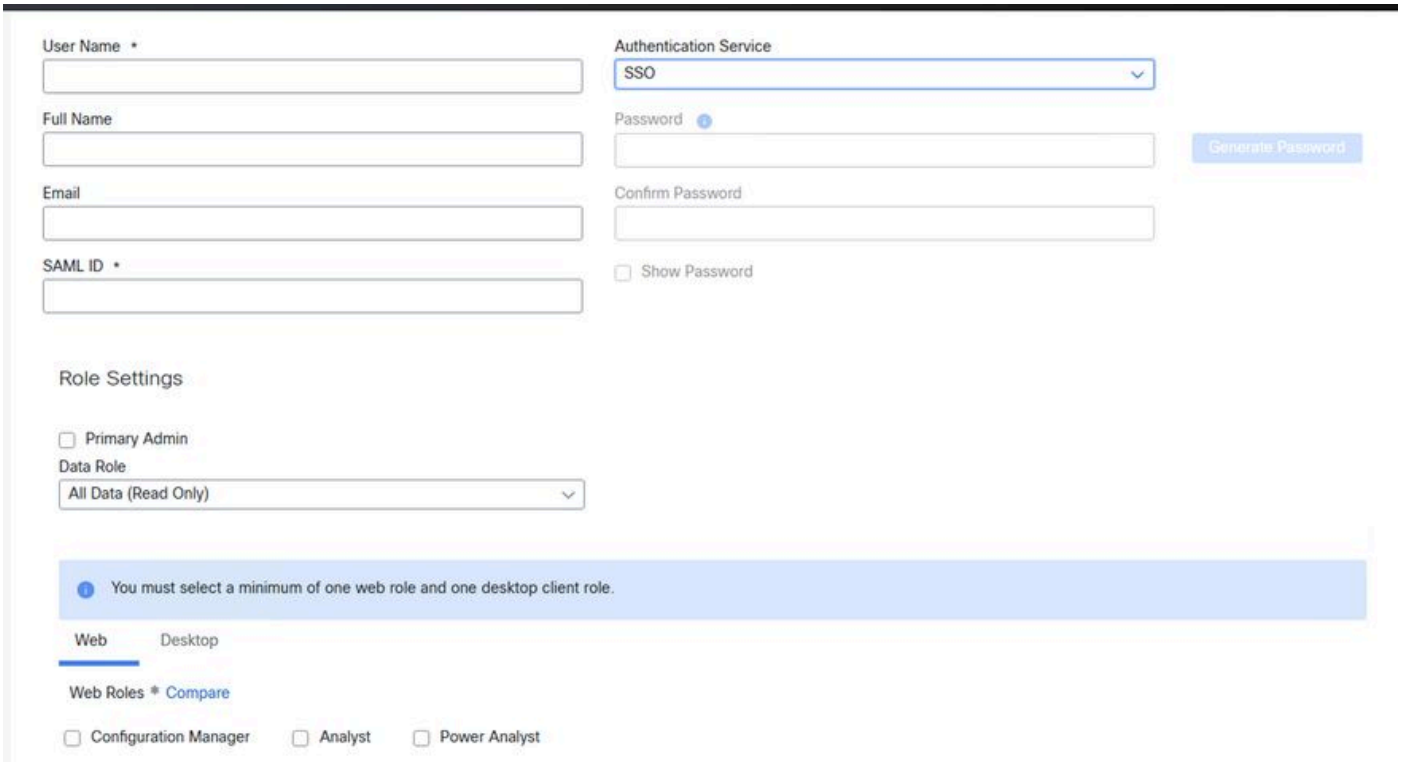
1. Accedere all'interfaccia utente di SNA Manager.

2. Passare a Configura > Globale > Gestione utente.

3. Fare clic su Crea > Utente.



4. Configurare l'utente fornendo i dettagli associati con il servizio di autenticazione selezionato come SSO e fare clic su Salva.



Creazione utente SAML in SNA-UI

Risoluzione dei problemi

Se gli utenti non sono in grado di accedere a SNA Manager, è possibile usare un tracer SAML per ulteriori informazioni.

Se è necessaria ulteriore assistenza nelle indagini sul gestore SNA, è possibile segnalare un caso TAC.

https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

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).