Konfigurieren von SNA Manager für Microsoft Entra ID SSO

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie Secure Network Analytics (SNA) für die Verwendung von Microsoft Entra ID für Single Sign On (SSO) konfigurieren.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Microsoft Azure
- Sichere Netzwerkanalysen

Verwendete Komponenten

- SNA Manager v7.5.2
- Microsoft Entra-ID

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 kennen.

Konfigurationsschritte

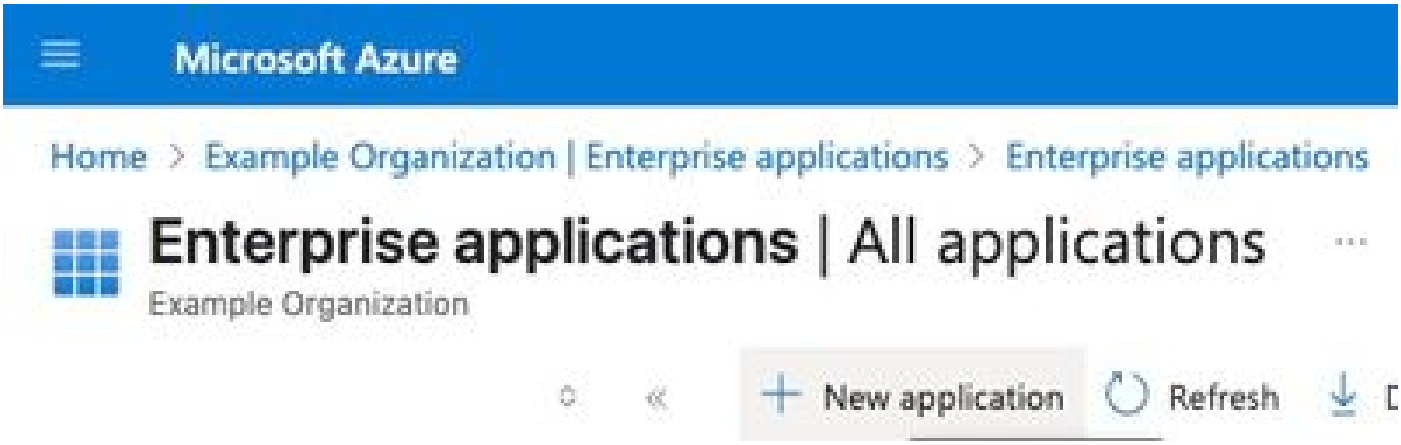
Enterprise-Anwendung in Azure konfigurieren

1. Melden Sie sich beim Azure Cloud Portal an.

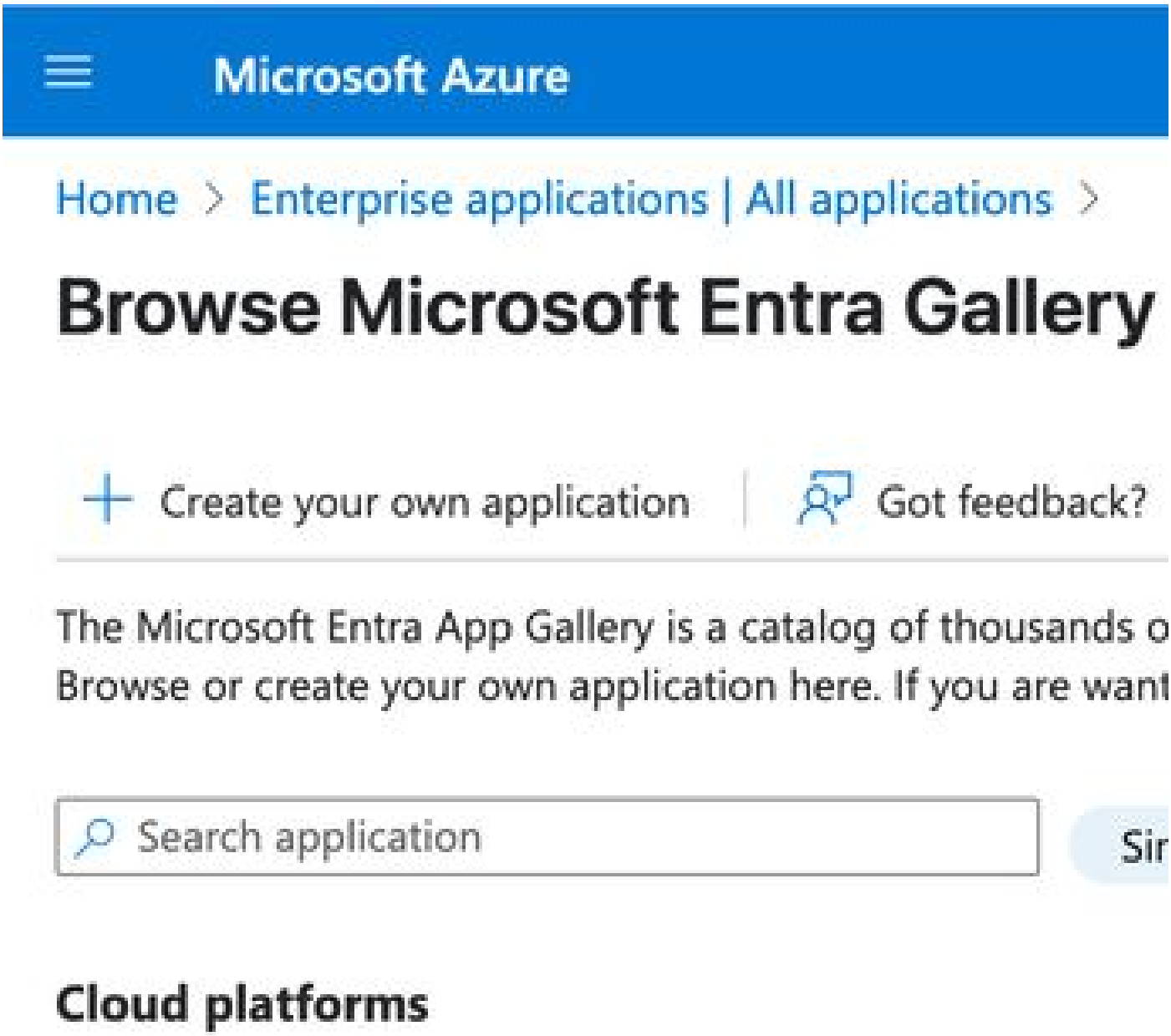
2. Suchen Sie im Suchfeld nach Entra ID-Dienst, und wählen Sie Microsoft Entra ID aus.

3. Erweitern Sie im linken Bereich die Option Verwalten, und wählen Sie Enterprise Applications aus.

4. Klicken Sie auf Neue Anwendung.



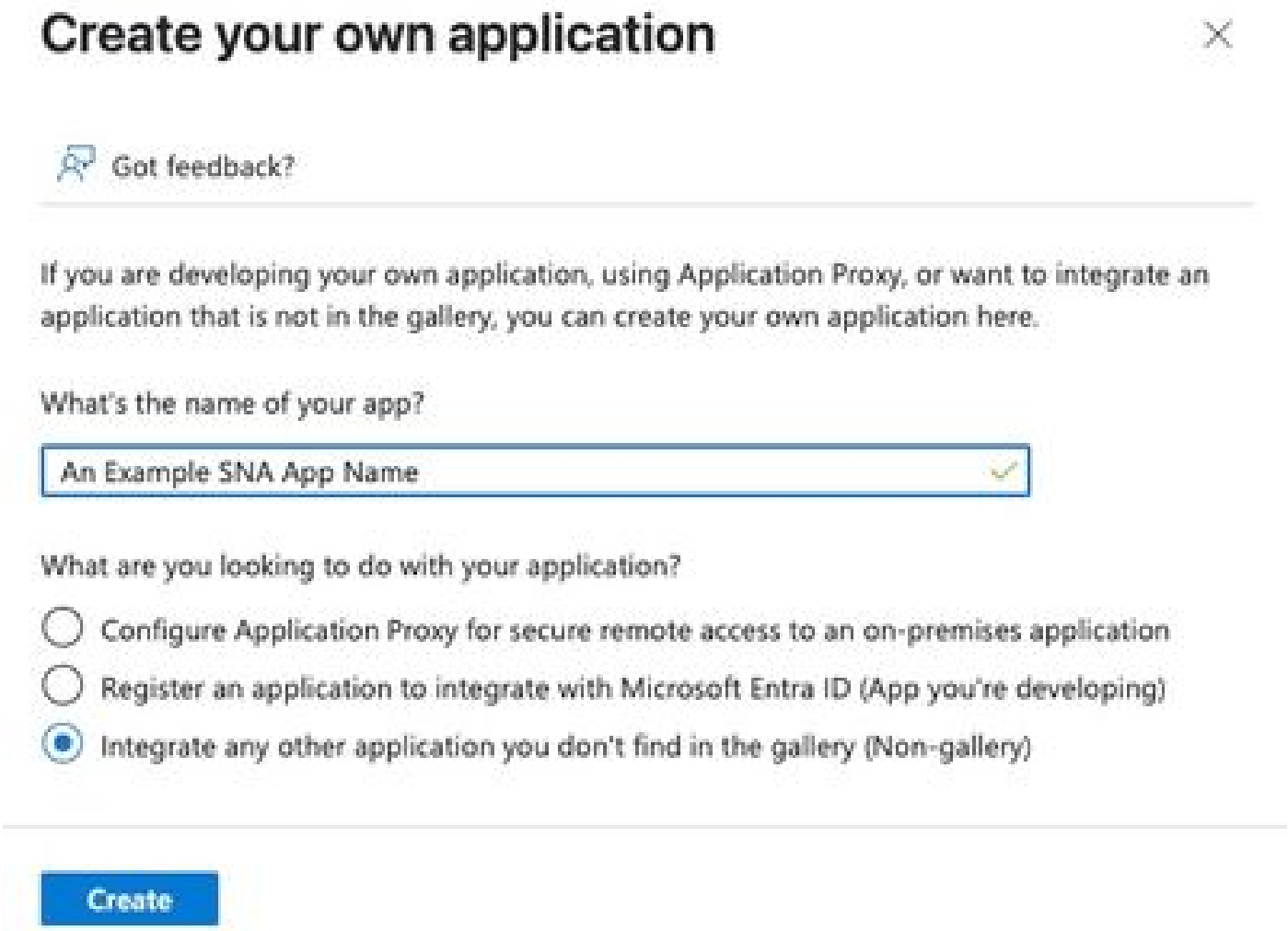
5. Wählen Sie Eigene Anwendung erstellen auf der neuen Seite, die geladen wird.



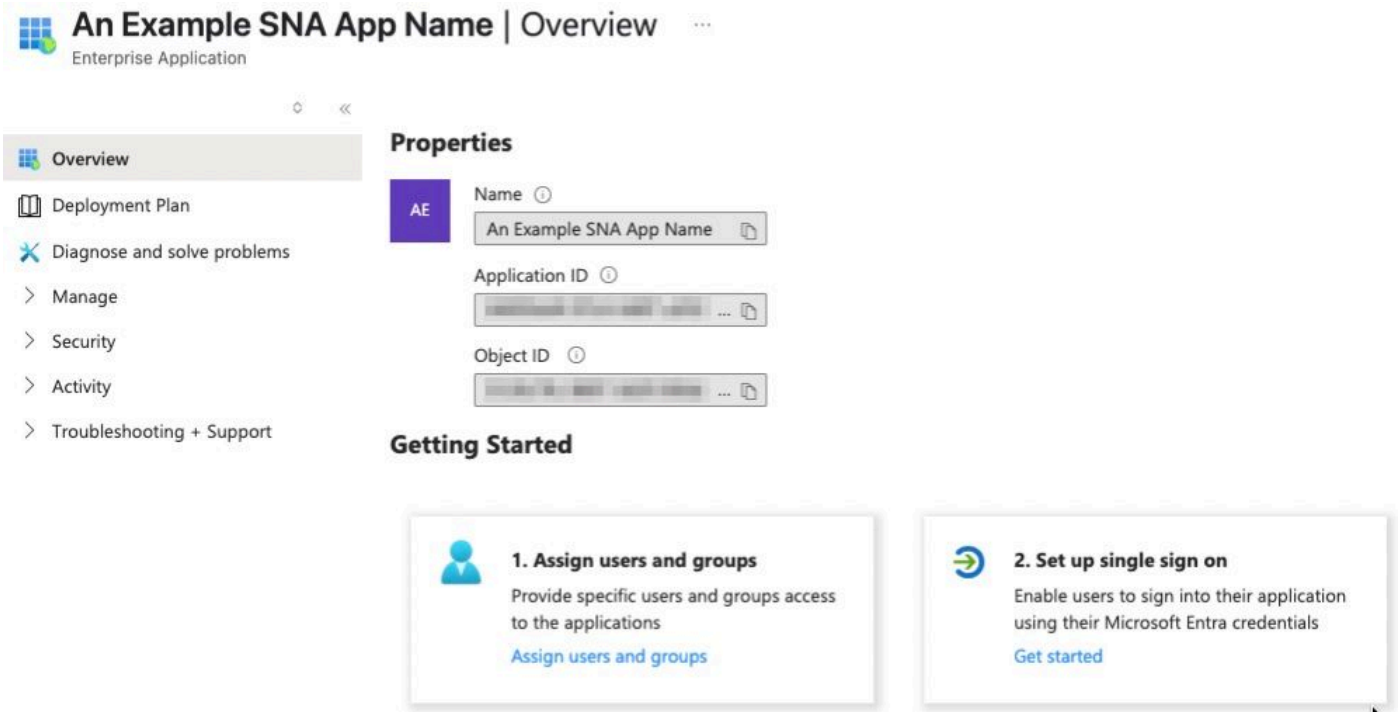
Azure-Benutzeroberfläche

6. Geben Sie einen Namen für die Anwendung in Wie lautet der Name Ihrer Anwendung? feld.

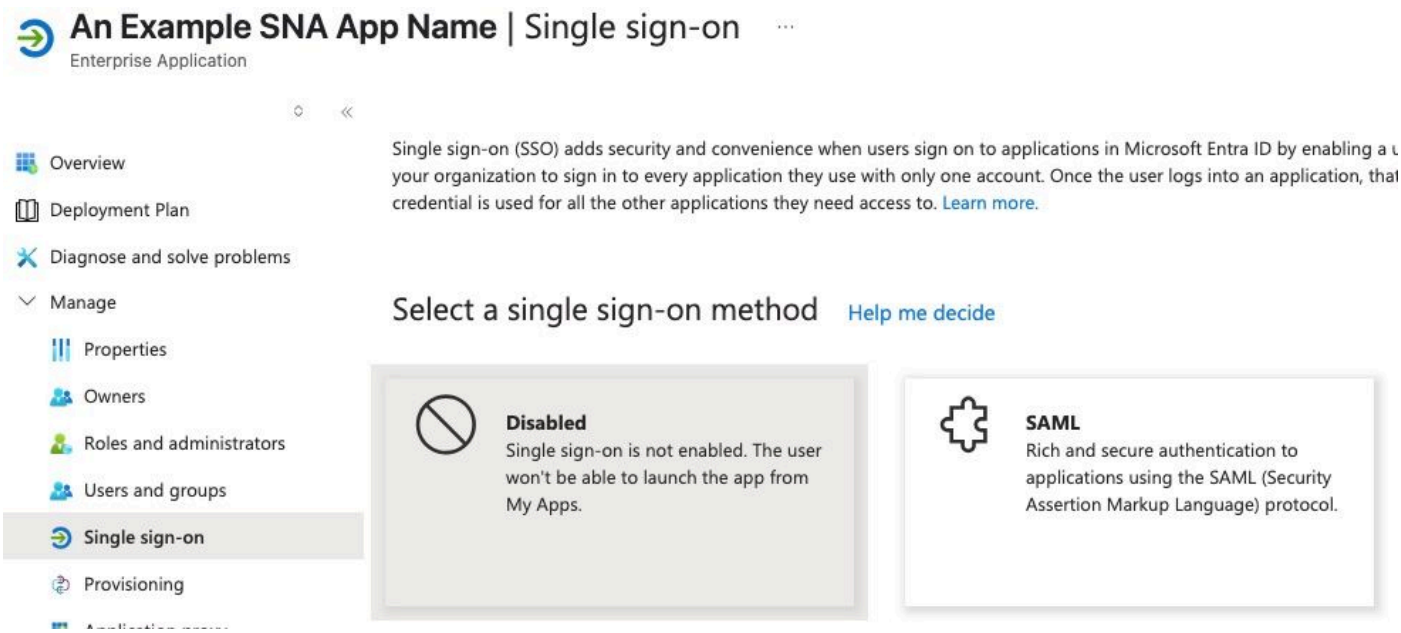
7. Wählen Sie das Optionsfeld Andere Anwendung integrieren, die Sie nicht in der Galerie finden (Nicht-Galerie) und klicken Sie auf Erstellen.



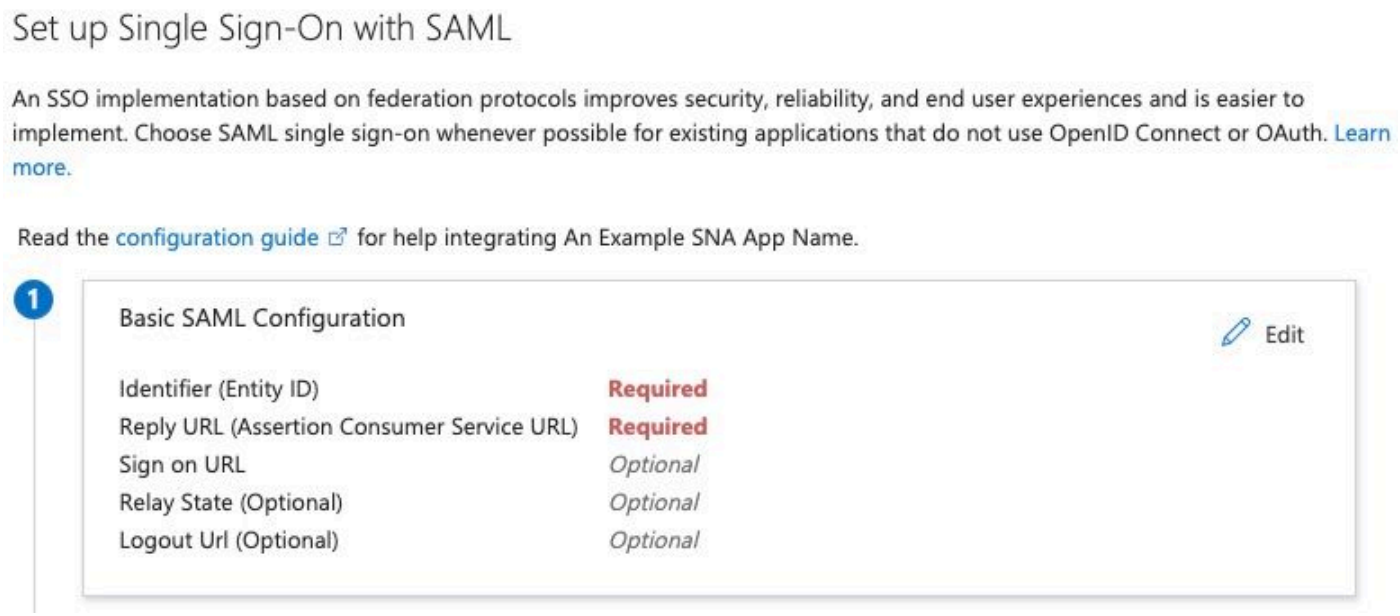
8. Klicken Sie im neu konfigurierten Anwendungs-Dashboard auf einmalige Anmeldung einrichten.



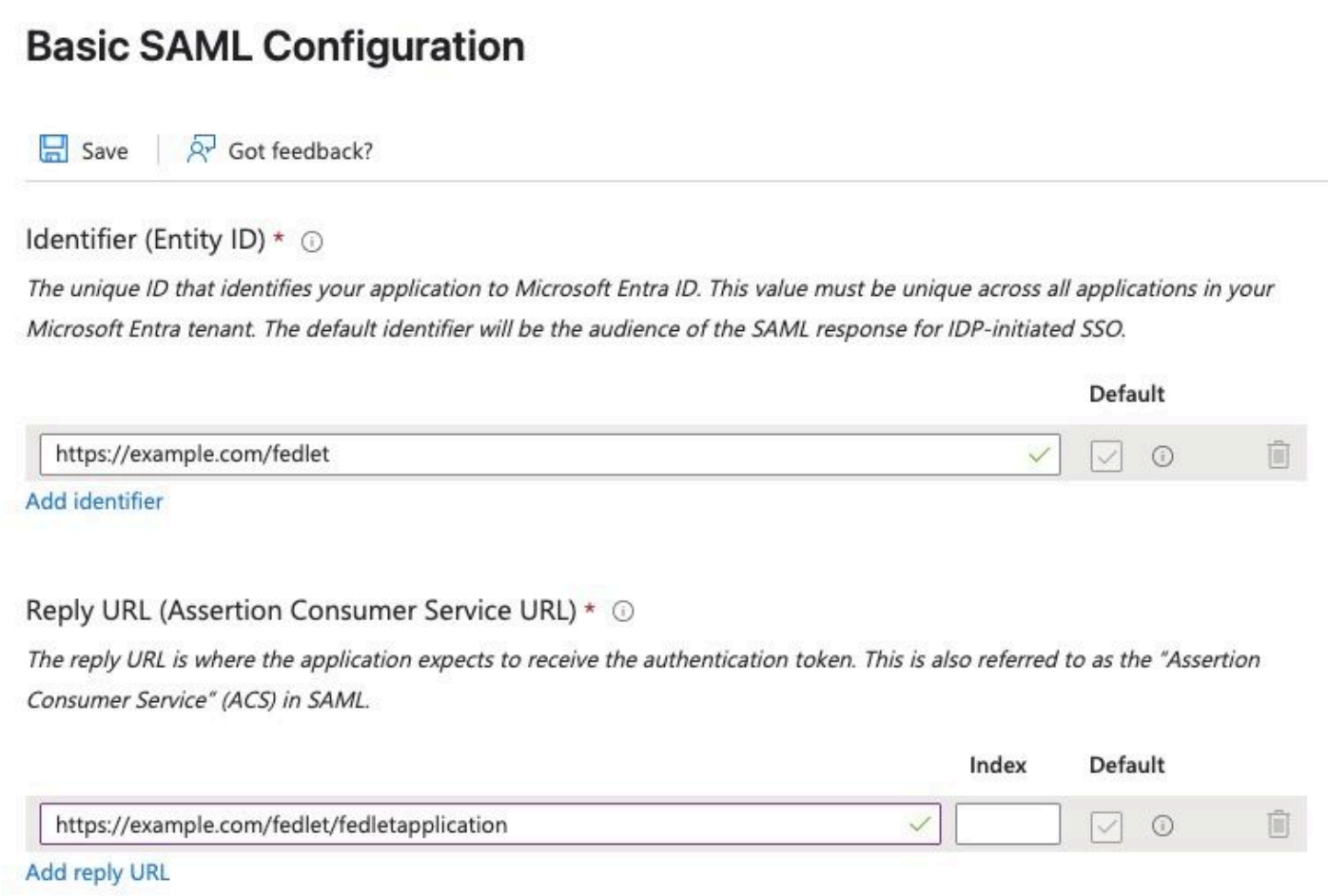
9. Wählen Sie SAML.



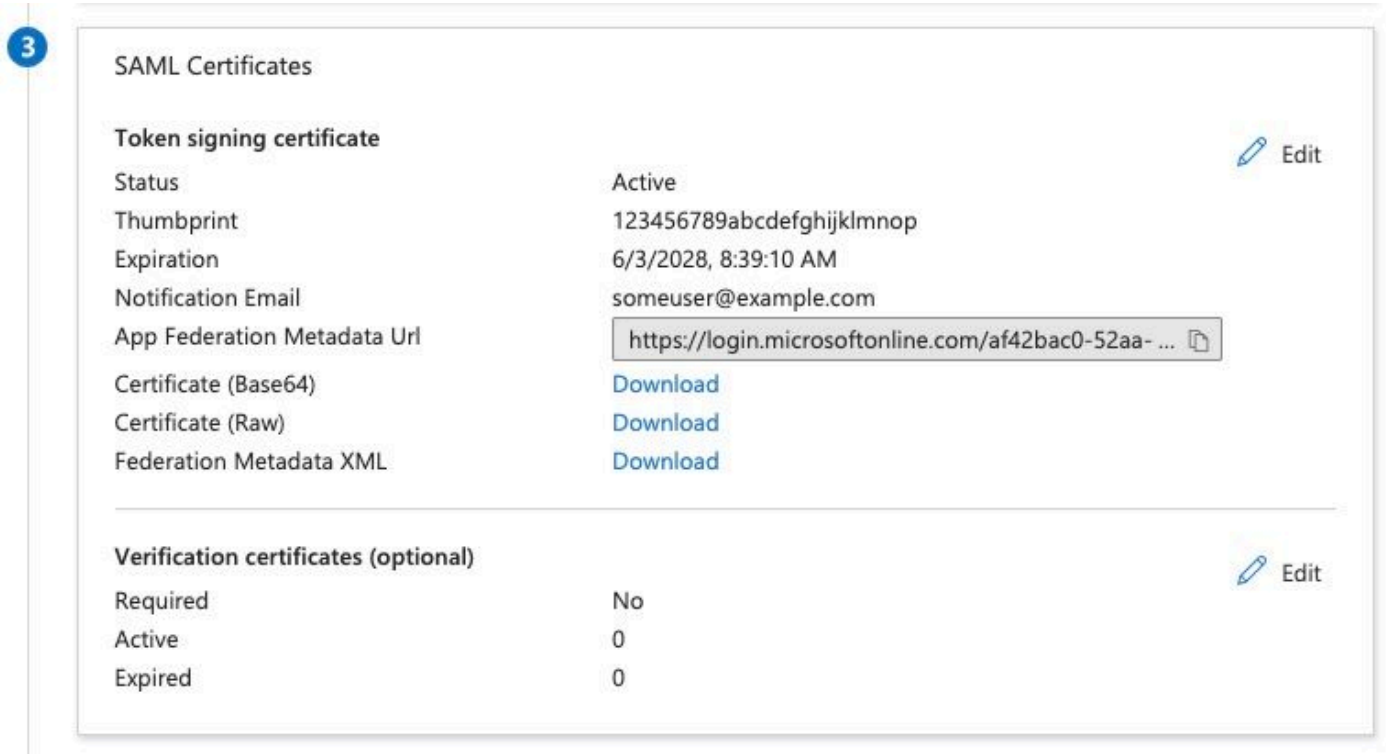
10. Klicken Sie auf der Seite "Einmaliges Anmelden mit SAML einrichten" unter "Grundlegende SAML-Konfiguration" auf Bearbeiten.



11. Konfigurieren Sie im Bereich SAML-Basiskonfiguration die Option Antwort-URL zu https://example.com/fedlet/fedletapplication hinzufügen, und ersetzen Sie example.com durch den FQDN des SNA Managers. Klicken Sie dann auf Speichern.

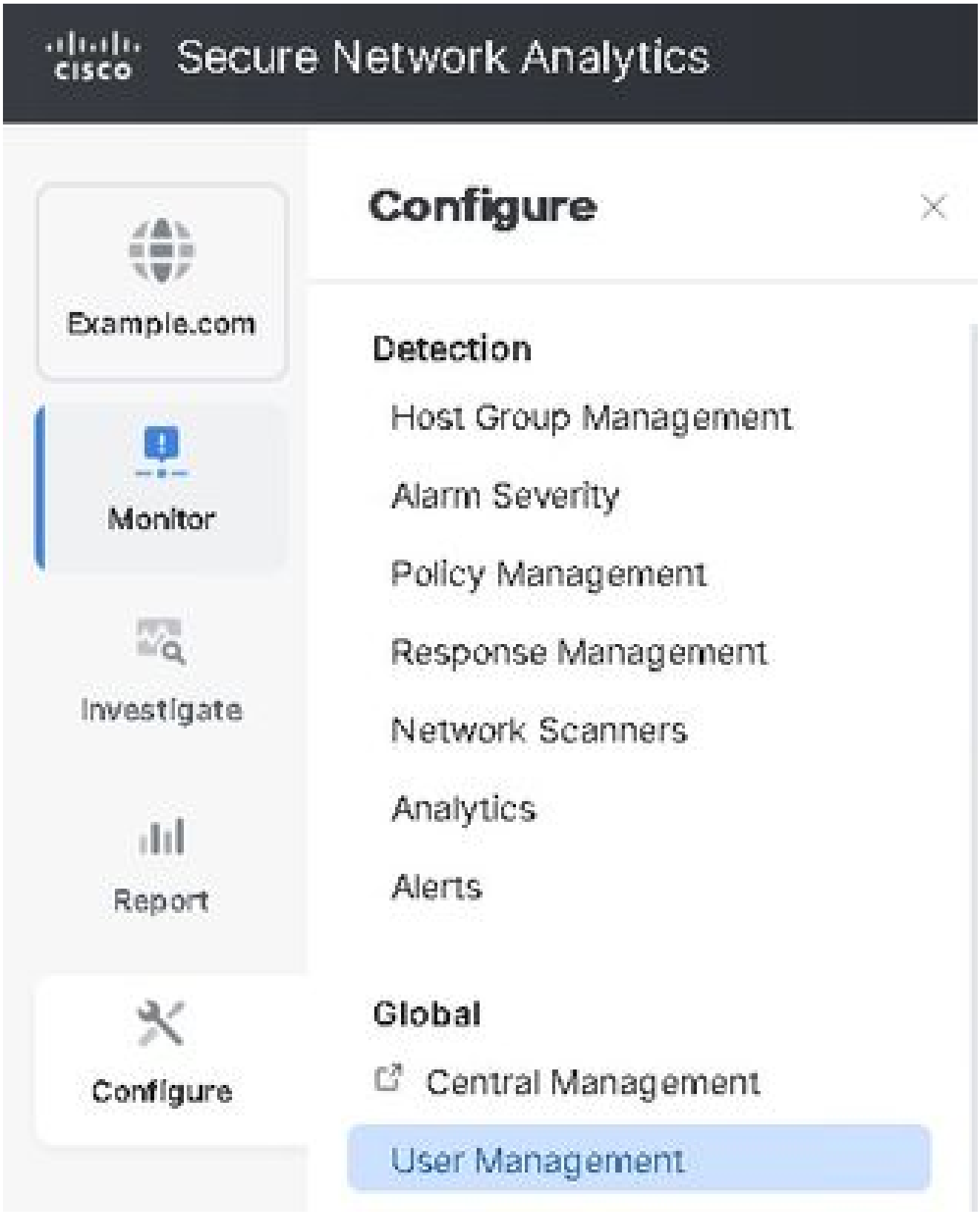


12. Suchen Sie die SAML-Zertifikatskarte, speichern Sie den URL-Feldwert für App-Verbund-Metadaten, und laden Sie die Verbandmetadaten-XML herunter.

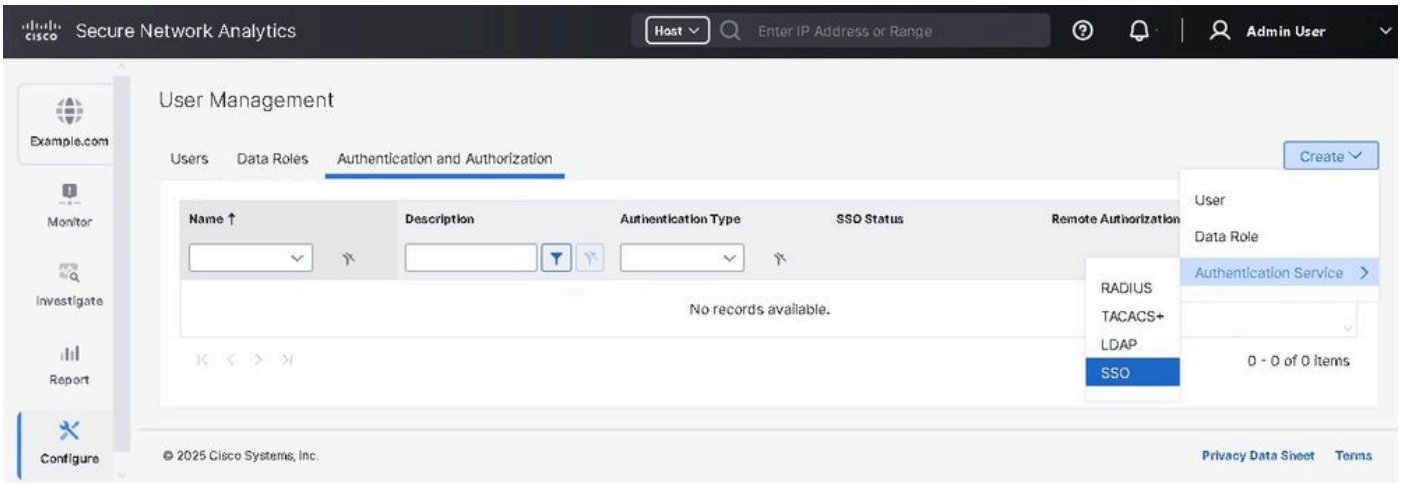


Konfigurieren und Herunterladen der Service Provider-XML-Datei in SNA

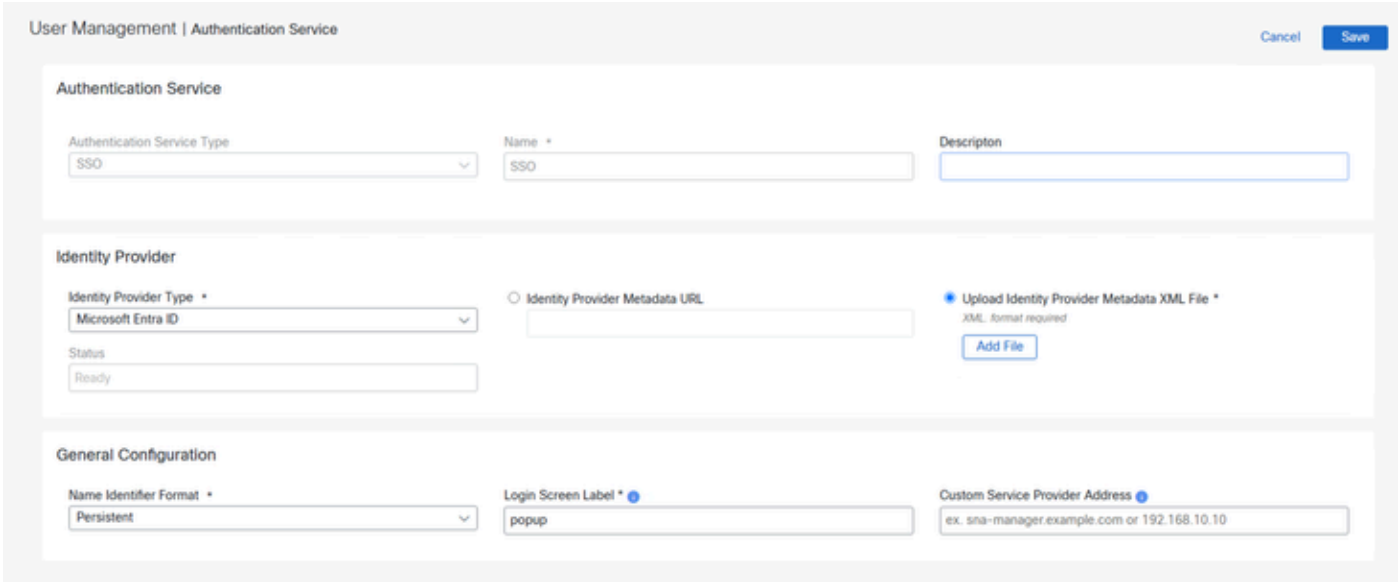
1. Melden Sie sich bei der SNA Manager-Benutzeroberfläche an.
2. Navigieren Sie zu Konfigurieren > Global > Benutzerverwaltung.

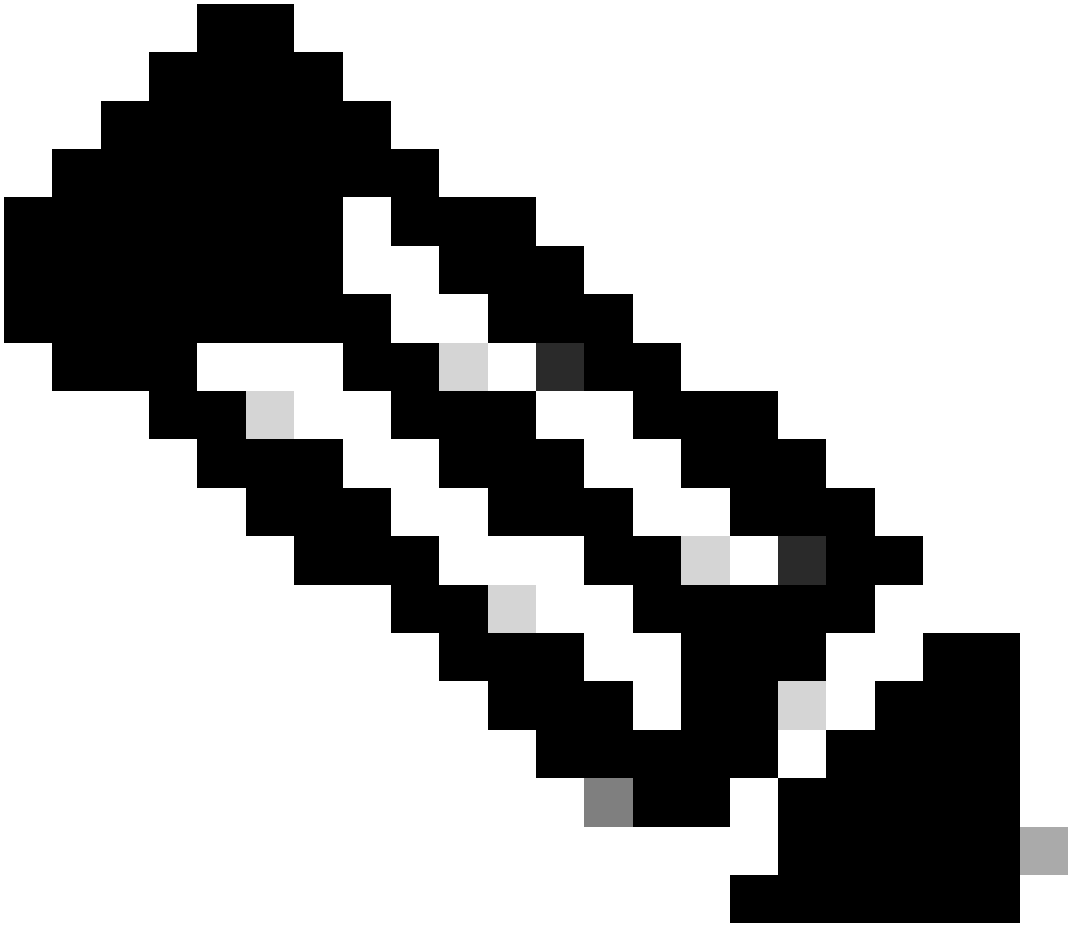


3. Klicken Sie auf der Registerkarte Authentifizierung und Autorisierung auf Erstellen > Authentifizierungsdienst > SSO.



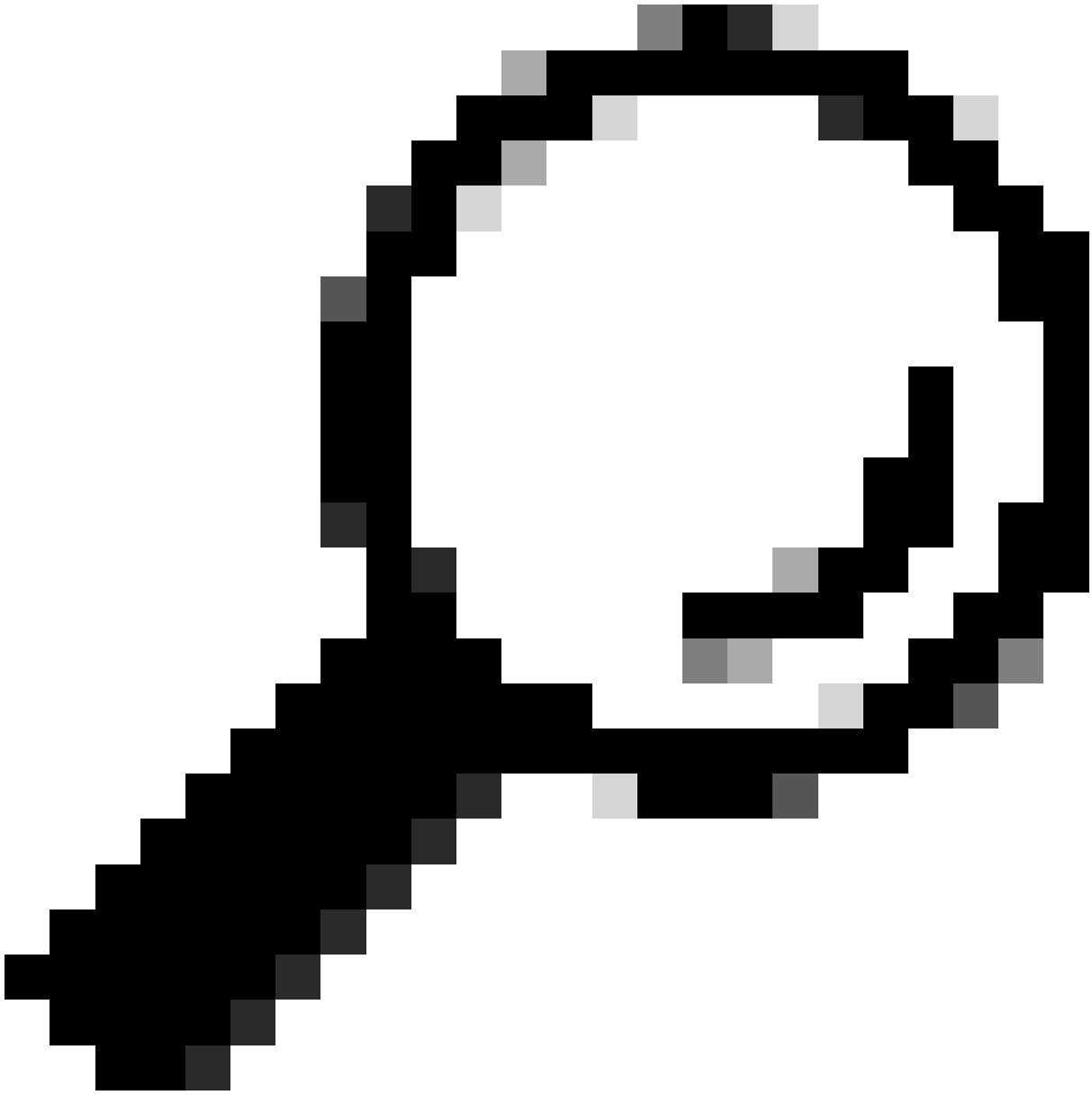
4. Wählen Sie das entsprechende Optionsfeld für die Metadaten-URL des Identitätsanbieters oder das Hochladen der XML-Metadatendatei des Identitätsanbieters aus.





Anmerkung: In dieser Demo wird "Identitätsanbieter-Metadaten-XML-Datei hochladen" ausgewählt.

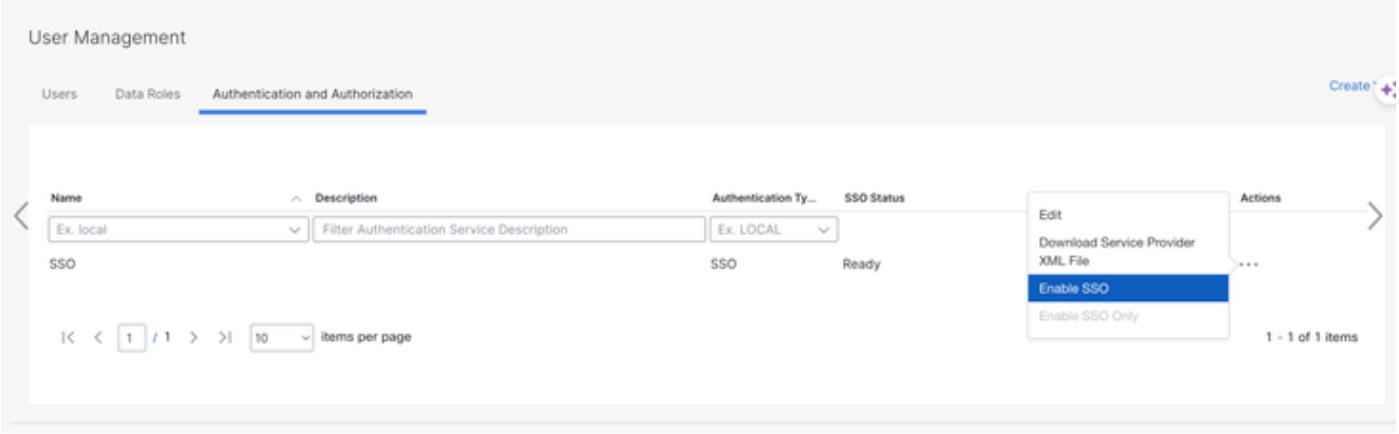
5. Konfigurieren Sie das Feld für den Identitätsanbietertyp für Microsoft Entra ID, das Namensidentifizierungsformat für Beständig, und geben Sie ein Anmeldefenster-Label ein.



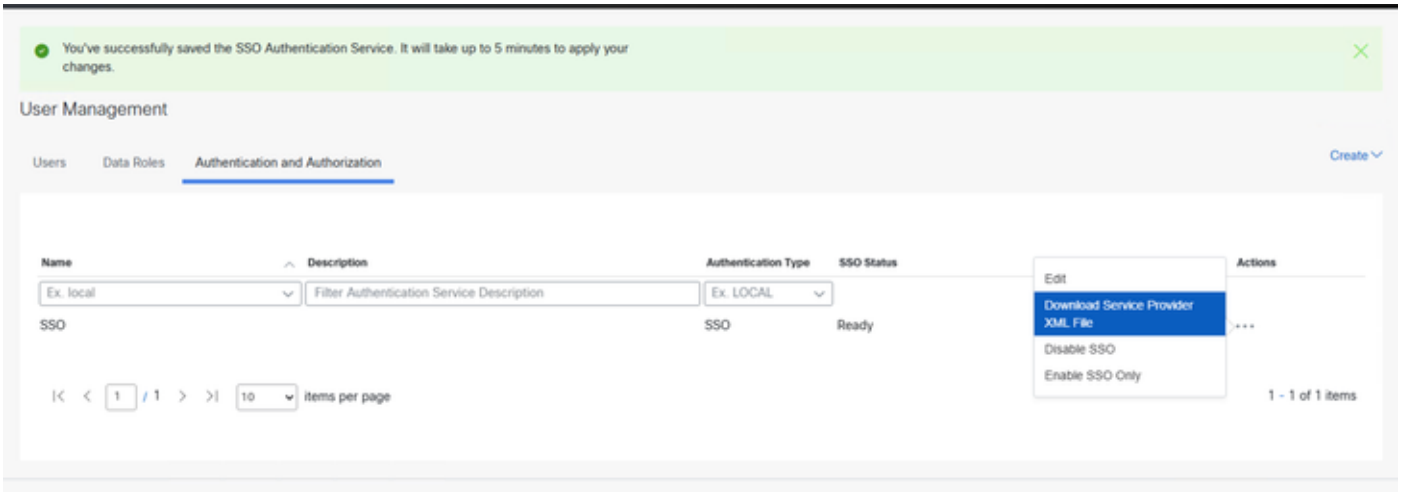
Tipp: Die Beschriftung des konfigurierten Anmeldebildschirms (Name/Text) wird über der Schaltfläche Anmelden mit SSO angezeigt und darf nicht leer gelassen werden.

6. Klicken Sie auf Speichern, um zur Registerkarte "Authentifizierung und Autorisierung" zurückzukehren.

7. Warten Sie, bis der Status BEREIT ist, und wählen Sie im Aktionsmenü die Option SSO aktivieren.



8. Klicken Sie auf der Registerkarte Authentifizierung und Autorisierung auf die drei Punkte in der Spalte Aktionen und dann auf Dienstanbieter-XML-Datei herunterladen.



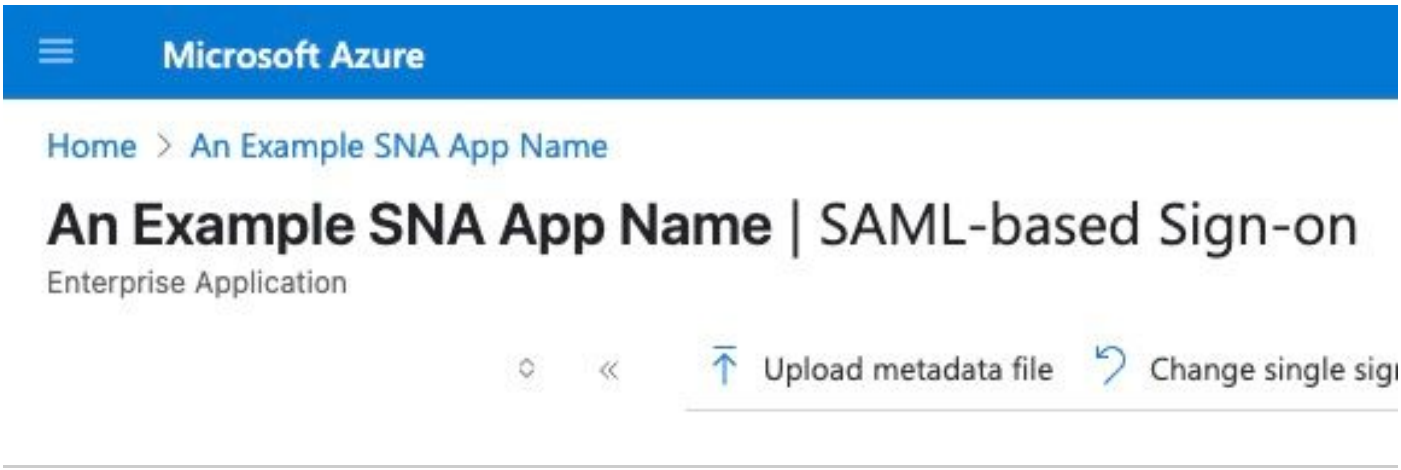
Konfigurieren von SSO in Azure

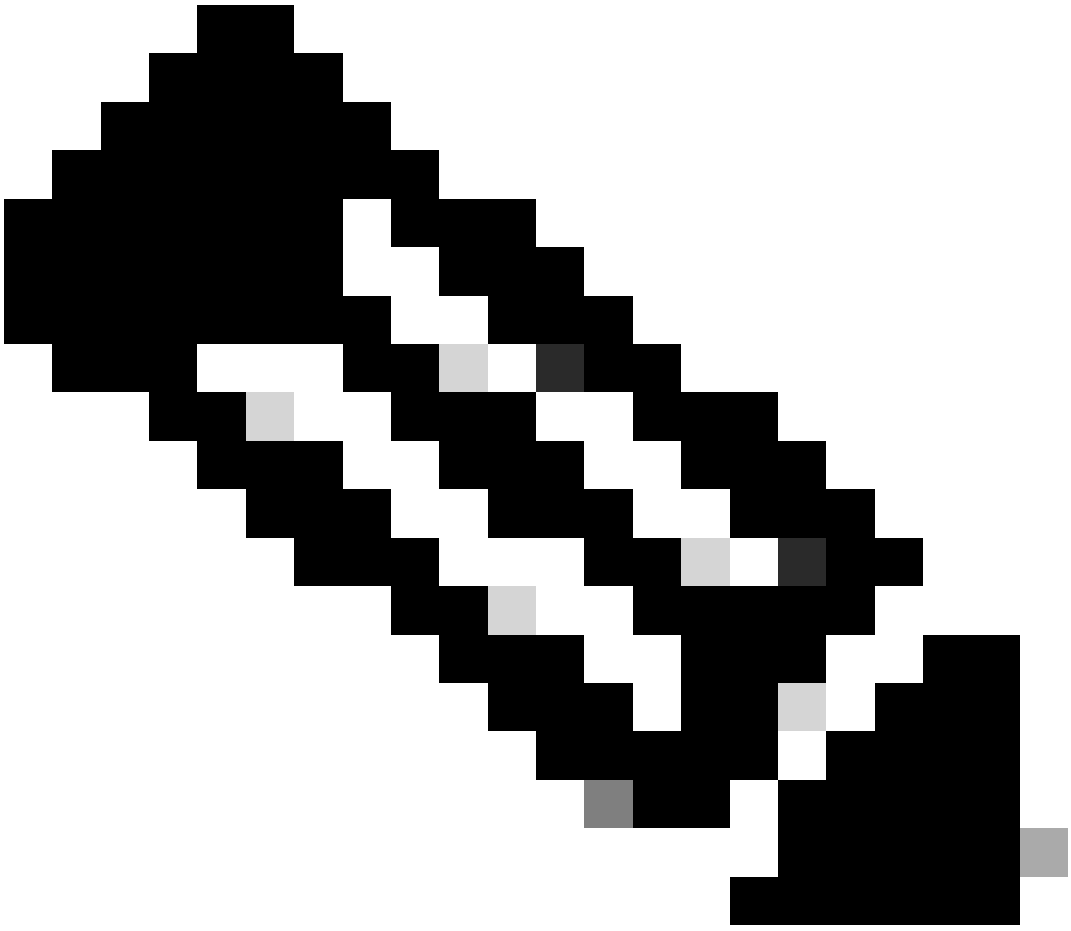
1. Melden Sie sich beim Azure-Portal an.

2. Navigieren Sie von der Suchleiste zu Enterprise Application > Select configured Enterprise Application > Click setup single sign on.

3. Klicken Sie oben auf der Seite auf Metadatendatei hochladen, und laden Sie die vom SNA Manager heruntergeladene Datei sp.xml hoch.

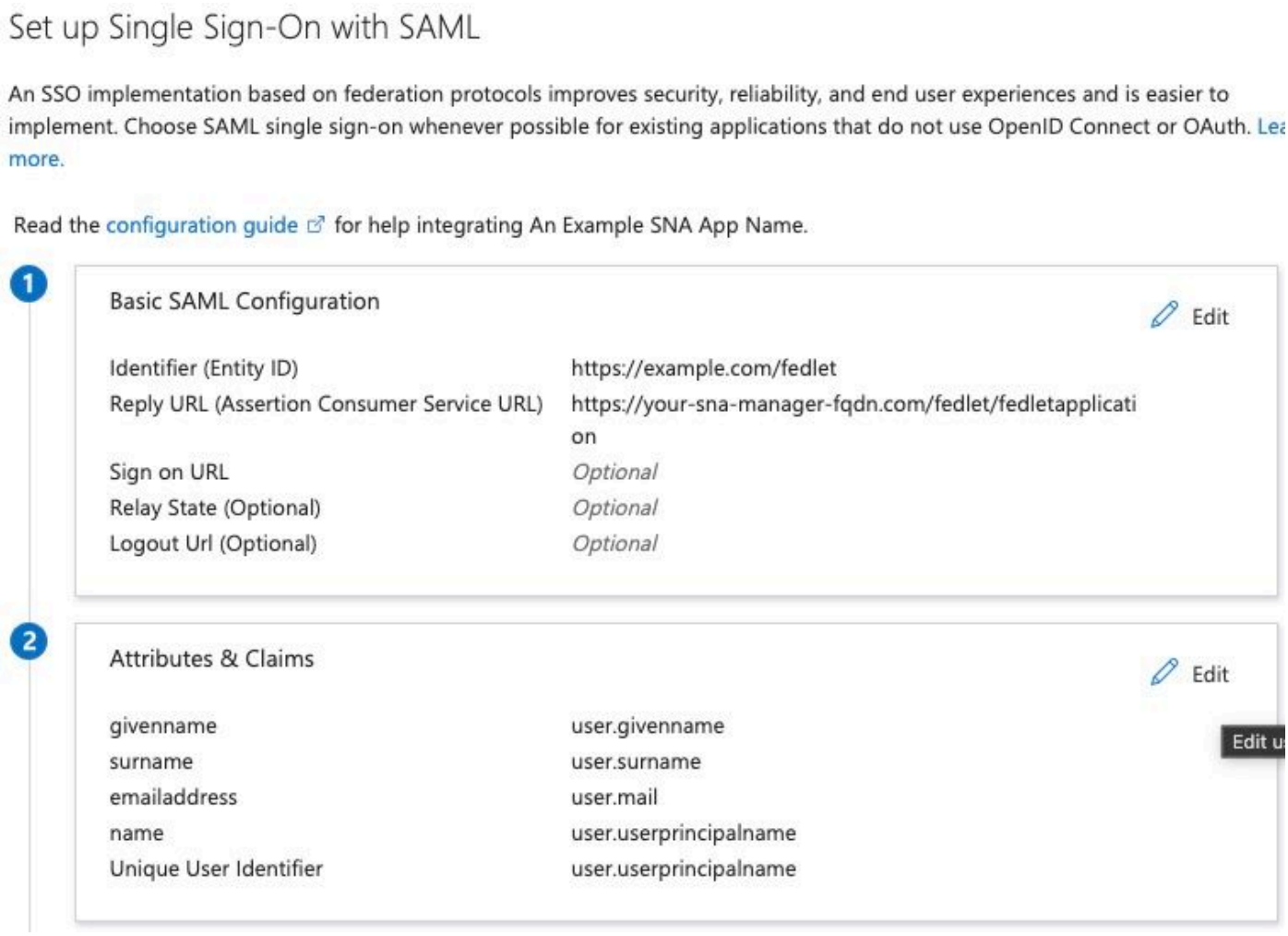
4. Es öffnet den Bildschirm "Basic SAML Configuration" und setzt verschiedene Einstellungen, um die Werte zu korrigieren, klicken Sie auf Speichern.





Anmerkung: Stellen Sie sicher, dass das Namens-ID-Format in der Entra-ID korrekt ist.

5. Suchen Sie den Abschnitt Attribute & Ansprüche, und klicken Sie auf Bearbeiten.



6. Klicken Sie unter Forderungsname auf user.userprincipalname.

7. Überprüfen Sie auf der Seite "Forderungen verwalten" das Format für die Namenskennzeichnung auswählen.

Microsoft Azure

Search

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

Manage claim ...

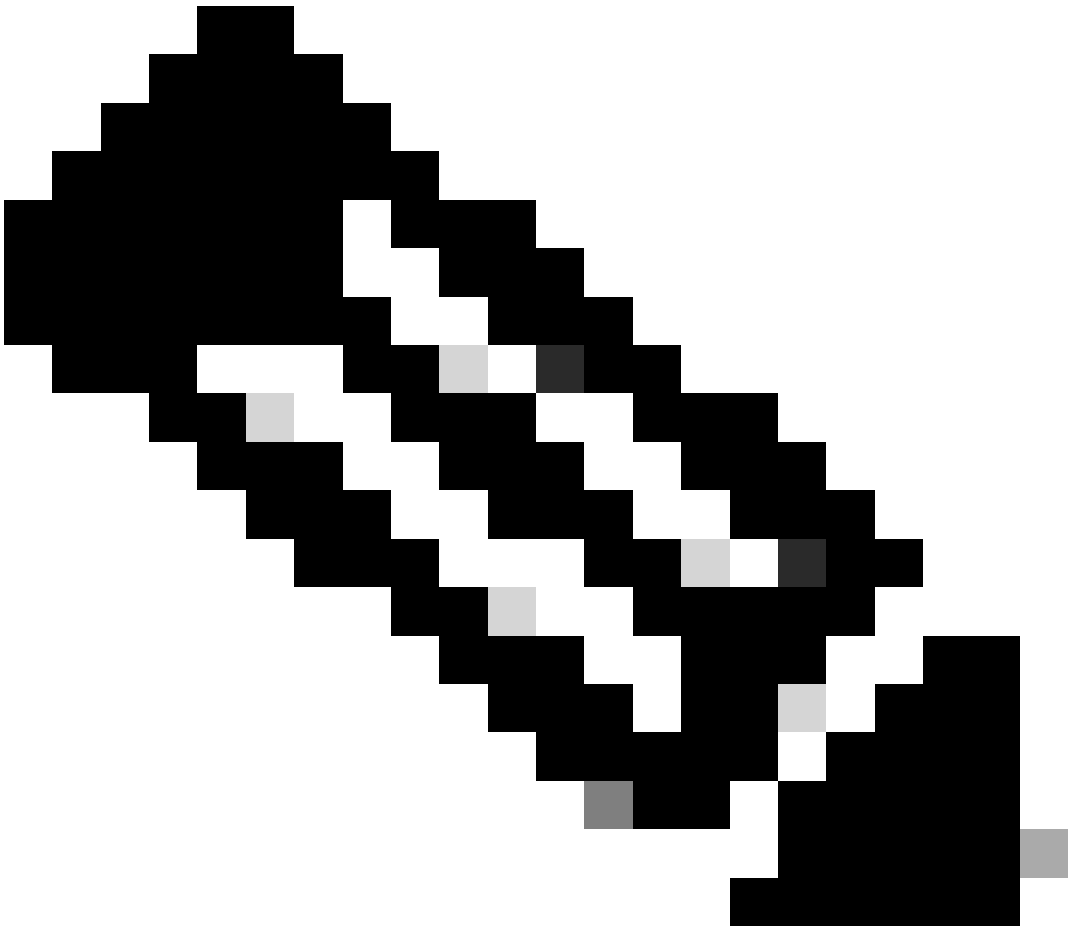
Save | Discard changes | Got feedback?

Name: nameidentifier

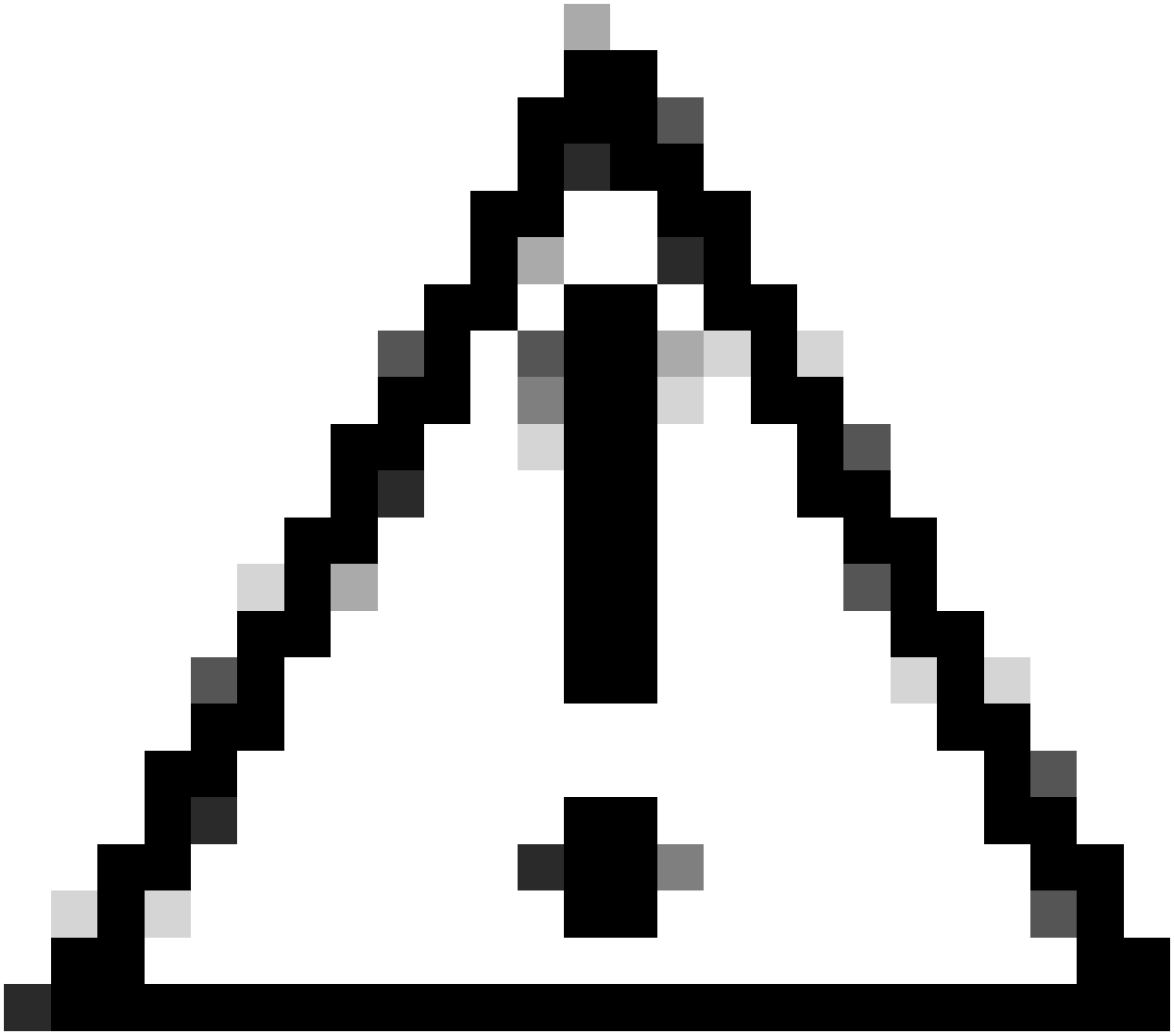
Namespace: http://schemas.xmlsoap.org/ws/2005/05/identity/claims

Choose name identifier format

Name identifier format *: Persistent



Anmerkung: Das Formatfeld für die Namens-ID ist auf "Persistent" gesetzt, wenn nicht, und wählen Sie es dann aus dem Dropdown-Menü aus. Klicken Sie auf Speichern, wenn Änderungen vorgenommen wurden.

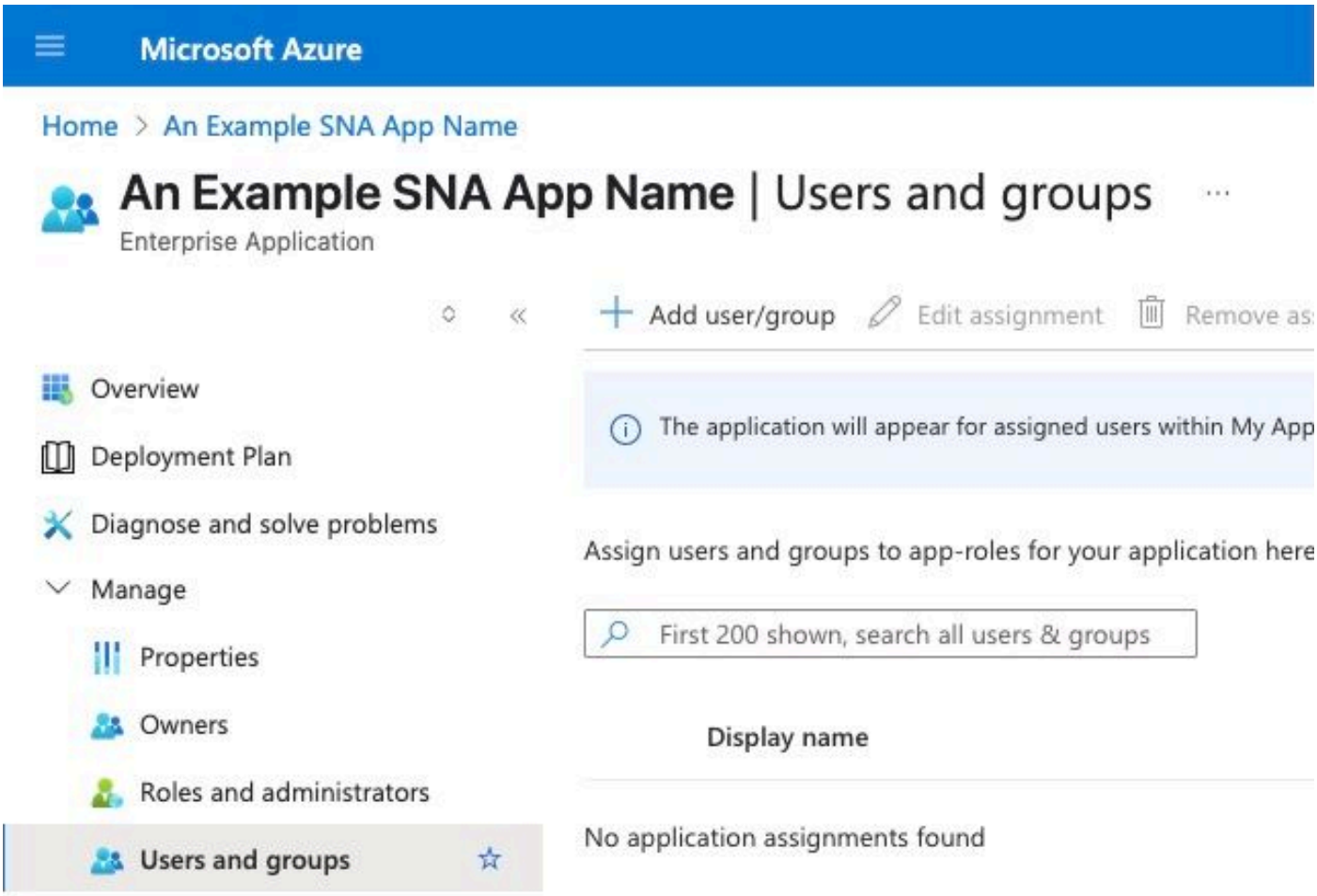


Vorsicht: Dies ist der häufigste Ort, um auf Probleme zu stoßen. Die Einstellungen für SNA Manager und Microsoft Azure müssen übereinstimmen. Wenn Sie sich für die Verwendung des Formats "emailAddress" in SNA entschieden haben, muss das Format hier ebenfalls "Email Address" lauten.

Setup-Benutzer in Entra-ID.

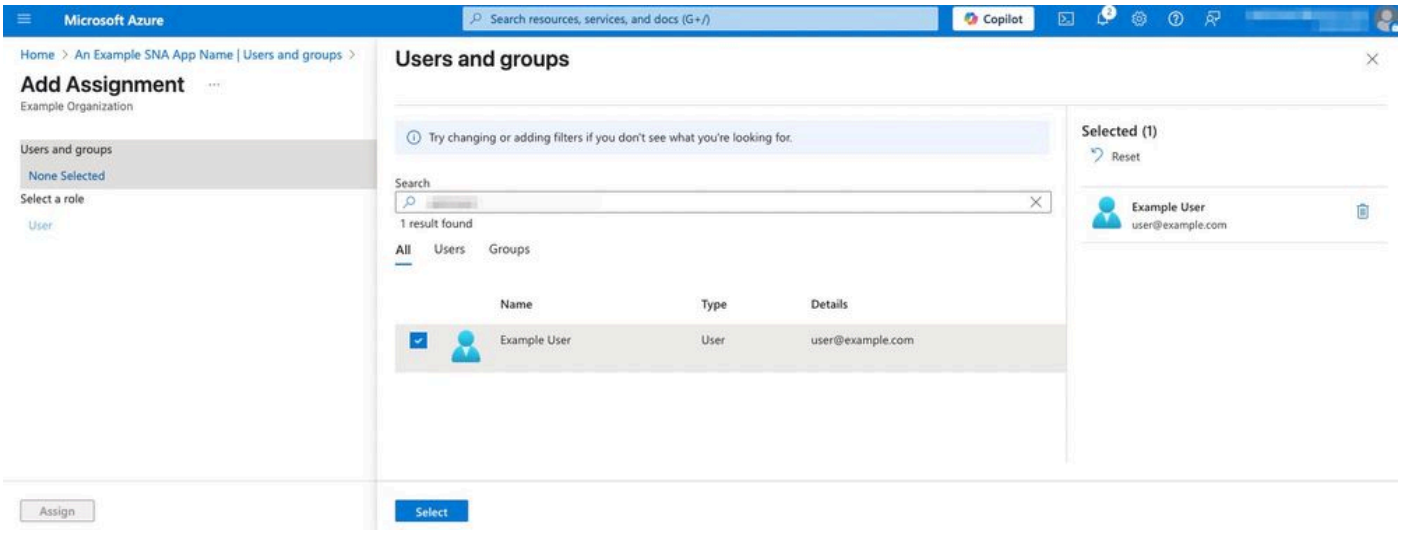
1. Melden Sie sich beim Azure-Portal an.

2. Navigieren Sie in der Suchleiste zu Enterprise Application > Select configured Enterprise Application > wählen Sie links Benutzer und Gruppen aus > klicken Sie auf Benutzer/Gruppe hinzufügen.



3. Klicken Sie im linken Bereich auf Keine ausgewählt.

4. Suchen Sie nach dem gewünschten Benutzer, und fügen Sie ihn der Anwendung hinzu.

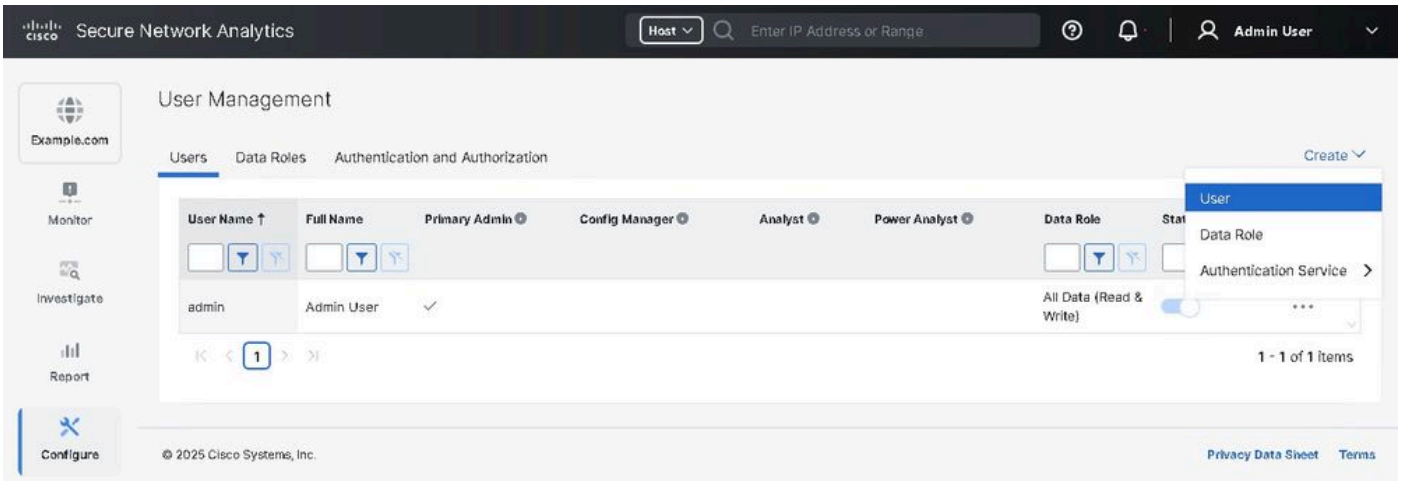


Konfigurieren von SSO in SNA

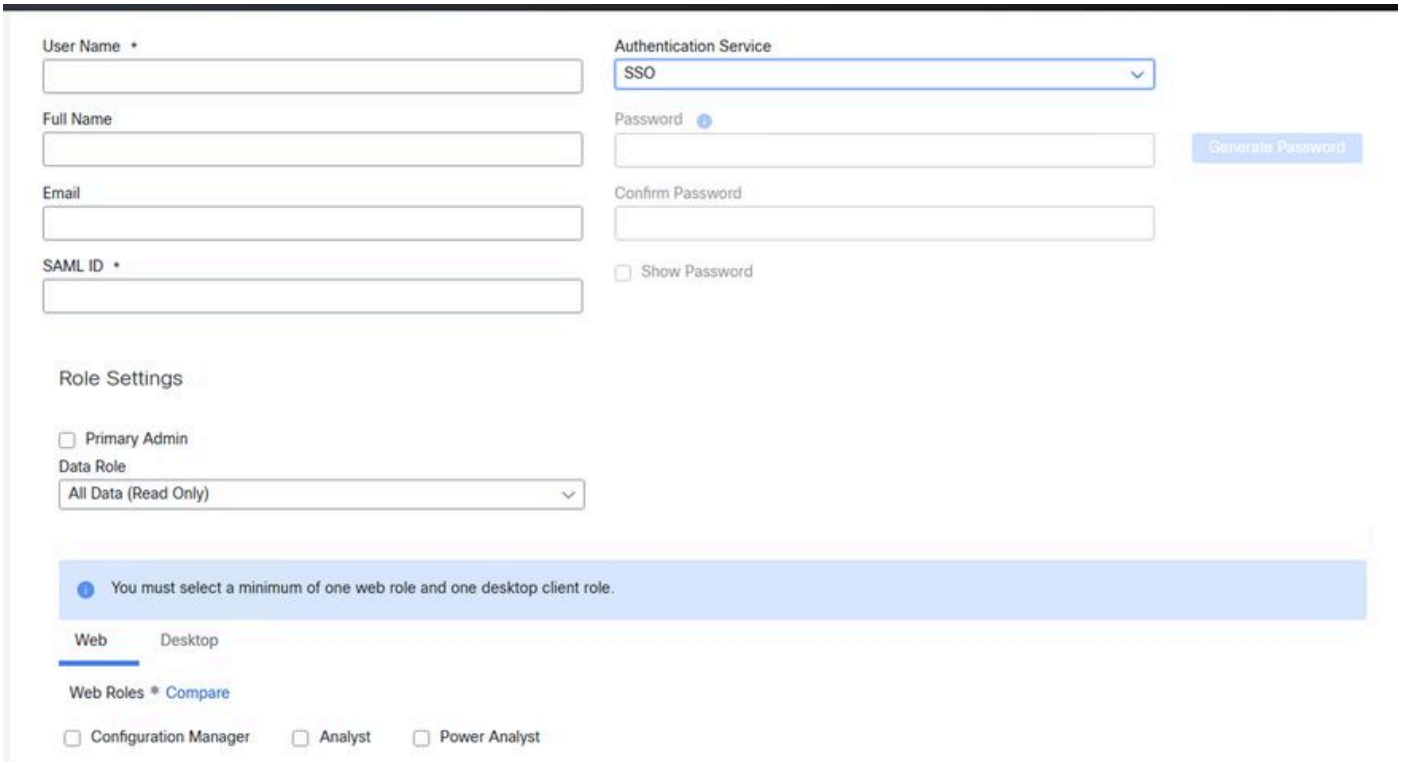
1. Melden Sie sich bei der SNA Manager-Benutzeroberfläche an.

2. Navigieren Sie zu Konfigurieren > Global > Benutzerverwaltung.

3. Klicken Sie auf Erstellen > Benutzer.



4. Konfigurieren Sie den Benutzer, indem Sie die zugehörigen Details für den als SSO ausgewählten Authentifizierungsdienst bereitstellen, und klicken Sie auf Speichern.



SAML-Benutzererstellung in der SNA-Benutzeroberfläche

Fehlerbehebung

Wenn sich Benutzer nicht beim SNA Manager anmelden können, kann ein SAML-Tracer verwendet werden, um weitere Informationen zu erhalten.

Wenn weitere Unterstützung bei der Untersuchung des SNA-Managers erforderlich ist, kann ein TAC-Fall erstellt werden.

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

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.