

Konfigurieren von SNA Manager für Microsoft Entra ID SSO

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurationsschritte](#)

[Enterprise-Anwendung in Azure konfigurieren](#)

[Konfigurieren und Herunterladen der Service Provider-XML-Datei in SNA](#)

[Konfigurieren von SSO in Azure](#)

[Setup-Benutzer in Entra-ID](#)

[Konfigurieren von SSO in SNA](#)

[Fehlerbehebung](#)

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

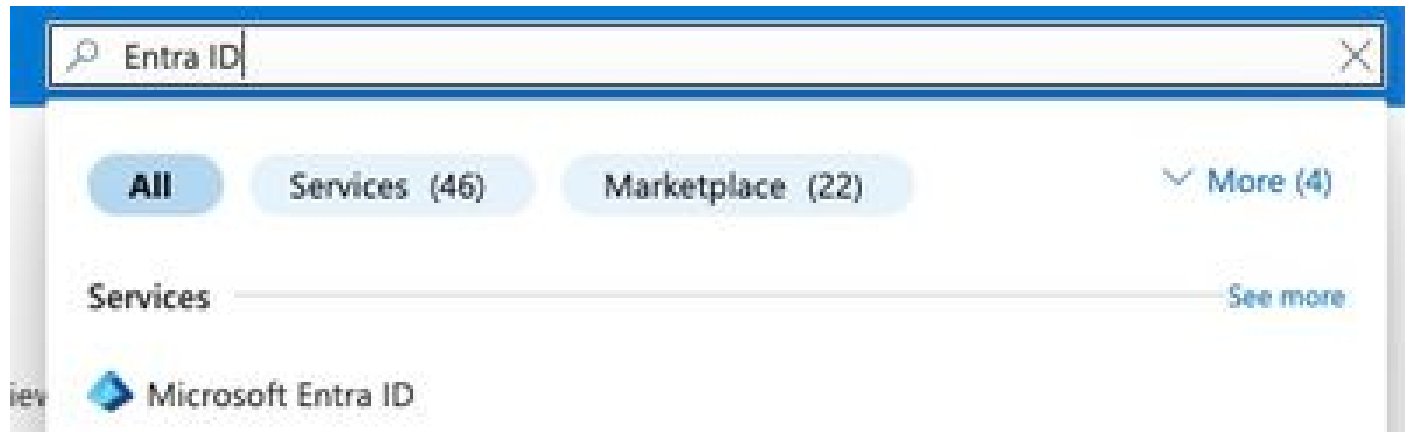
- SNA Manager v7.5.2
- Microsoft Entra-ID

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.

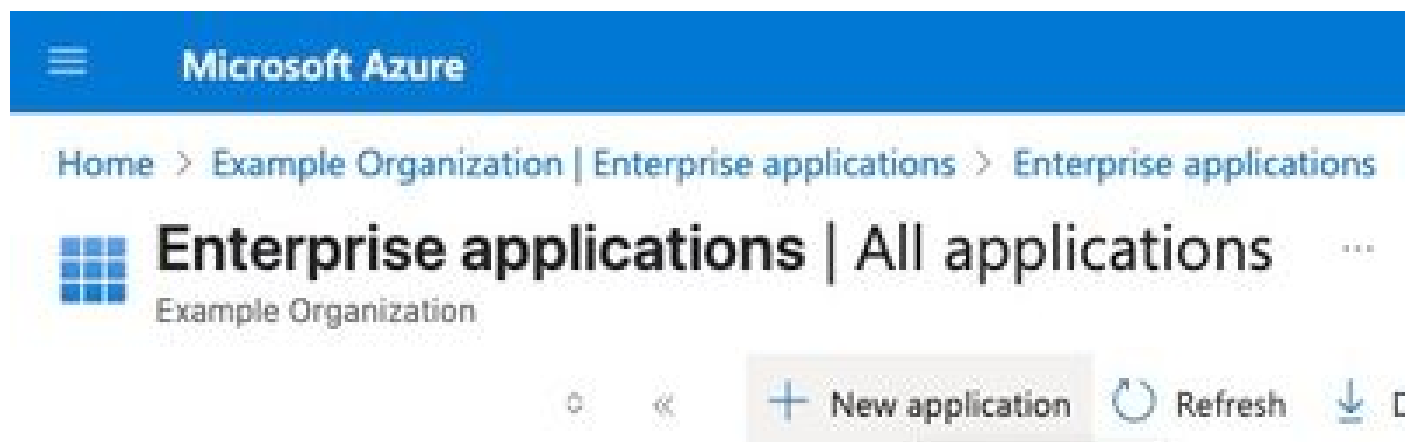
Konfigurationsschritte

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.



[Home](#) > [Enterprise applications](#) | [All applications](#) >

Browse Microsoft Entra Gallery



Create your own application



Got feedback?

The Microsoft Entra App Gallery is a catalog of thousands of applications. Browse or create your own application here. If you are want



Sir

Cloud platforms

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.

Create your own application



Got feedback?

If you are developing your own application, using Application Proxy, or want to integrate an application that is not in the gallery, you can create your own application here.

What's the name of your app?

An Example SNA App Name



What are you looking to do with your application?

- ☐ Configure Application Proxy for secure remote access to an on-premises application
- ☐ Register an application to integrate with Microsoft Entra ID (App you're developing)
- ☒ Integrate any other application you don't find in the gallery (Non-gallery)

Create

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



An Example SNA App Name | Overview

Enterprise Application



Overview



Deployment Plan



Diagnose and solve problems



Manage



Security



Activity



Troubleshooting + Support

Properties

AE

Name ⓘ

An Example SNA App Name

Application ID ⓘ

...

Object ID ⓘ

...

Getting Started



1. Assign users and groups

Provide specific users and groups access to the applications

[Assign users and groups](#)



2. Set up single sign on

Enable users to sign into their application using their Microsoft Entra credentials

[Get started](#)

9. Wählen Sie SAML.

**An Example SNA App Name | Single sign-on**
Enterprise Application

- Overview
- Deployment Plan
- Diagnose and solve problems
- Manage
 - Properties
 - Owners
 - Roles and administrators
 - Users and groups
 - Single sign-on**
 - Provisioning

Single sign-on (SSO) adds security and convenience when users sign on to applications in Microsoft Entra ID by enabling a user's organization to sign in to every application they use with only one account. Once the user logs into an application, that credential is used for all the other applications they need access to. [Learn more.](#)

Select a single sign-on method [Help me decide](#)

**Disabled**
Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

**SAML**
Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

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

Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. [Learn more.](#)

Read the [configuration guide](#) for help integrating An Example SNA App Name.

1

Basic SAML Configuration [Edit](#)

Identifier (Entity ID)	Required
Reply URL (Assertion Consumer Service URL)	Required
Sign on URL	<i>Optional</i>
Relay State (Optional)	<i>Optional</i>
Logout Url (Optional)	<i>Optional</i>

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.

Basic SAML Configuration

 Save |  Got feedback?

Identifier (Entity ID) * ⓘ

The unique ID that identifies your application to Microsoft Entra ID. This value must be unique across all applications in your Microsoft Entra tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.

Default



[Add identifier](#)

Reply URL (Assertion Consumer Service URL) * ⓘ

The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.

Index

Default



[Add reply URL](#)

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

3

SAML Certificates

Token signing certificate

Status

Active

Thumbprint

123456789abcdefghijklmnopqrstuvwxyz

Expiration

6/3/2028, 8:39:10 AM

Notification Email

someuser@example.com

App Federation Metadata Url

Certificate (Base64)

[Download](#)

Certificate (Raw)

[Download](#)

Federation Metadata XML

[Download](#)

Verification certificates (optional)

Required

No

Active

0

Expired

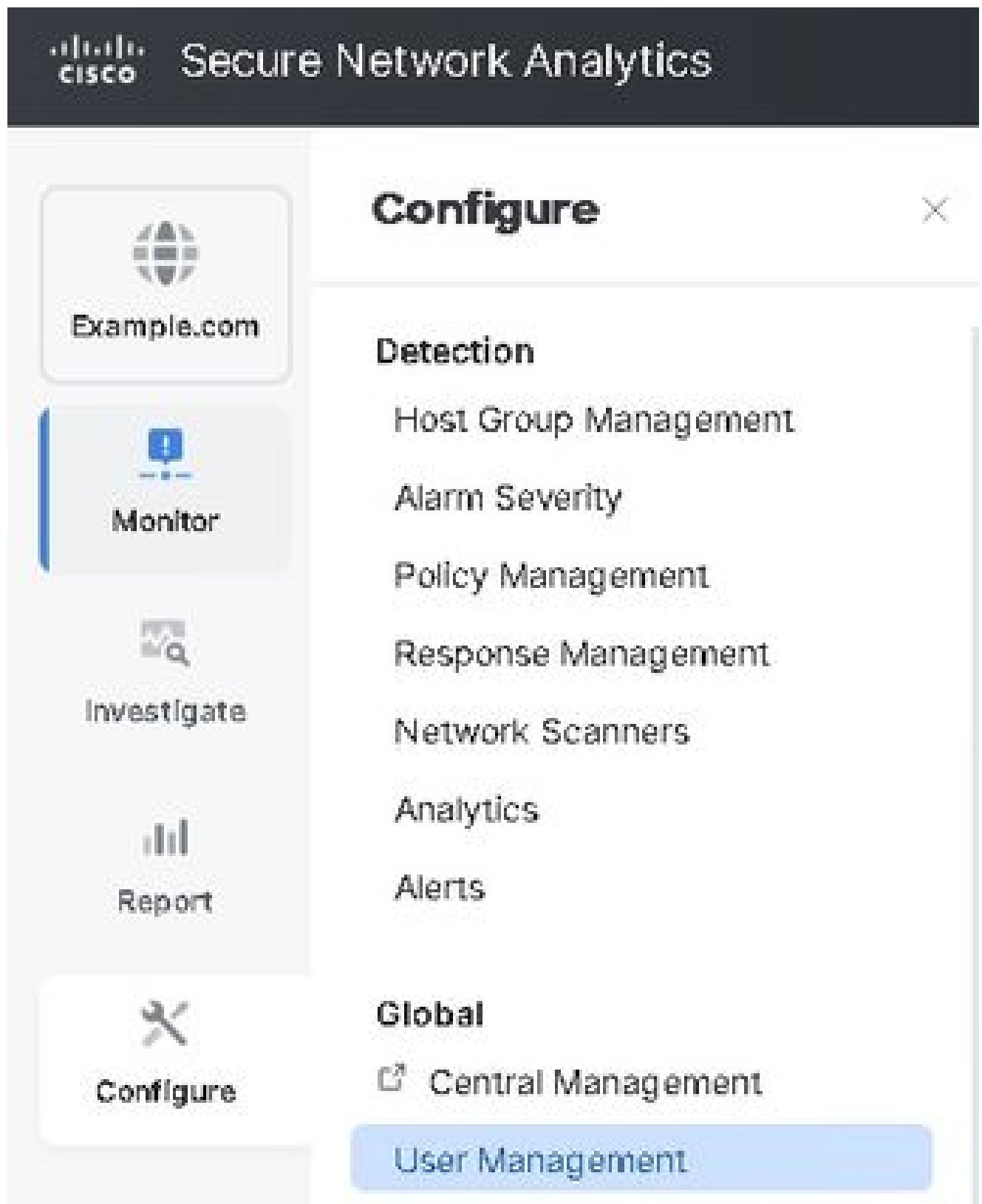
0

Edit

Edit

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.

Secure Network Analytics

Host Enter IP Address or Range

Admin User

User Management

Users Data Roles Authentication and Authorization

Create

Name ↑	Description	Authentication Type	SSO Status	Remote Authorization
No records available.				

0 - 0 of 0 Items

© 2025 Cisco Systems, Inc. Privacy Data Sheet Terms

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

User Management | Authentication Service

Cancel Save

Authentication Service

Authentication Service Type: SSO

Name: SSO

Description:

Identity Provider

Identity Provider Type: Microsoft Entra ID

Status: Ready

☐ Identity Provider Metadata URL

☒ Upload Identity Provider Metadata XML File *

XML format required

Add File

General Configuration

Name Identifier Format: Persistent

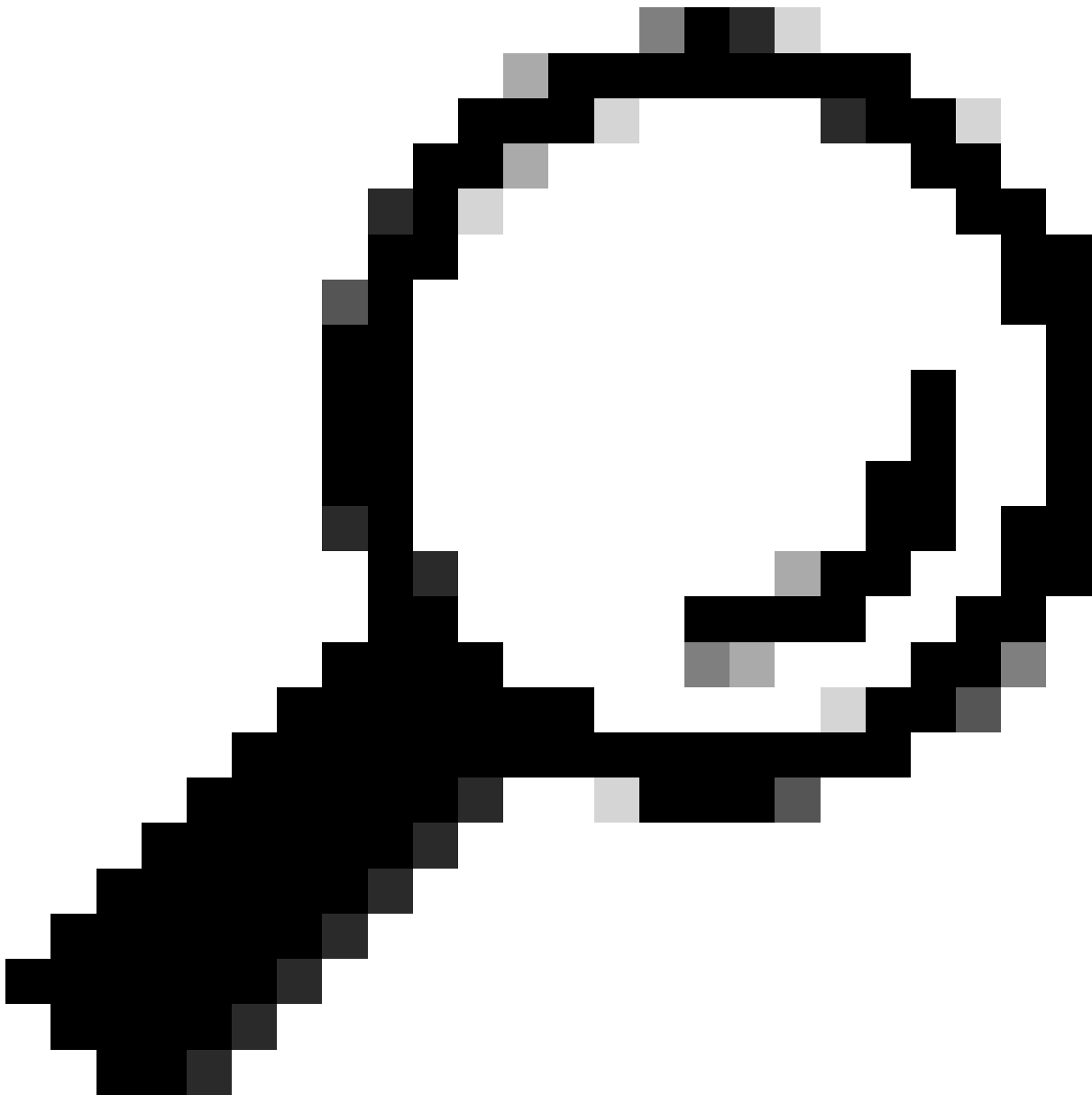
Login Screen Label: popup

Custom Service Provider Address: ex. sna-manager.example.com or 192.168.10.10



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

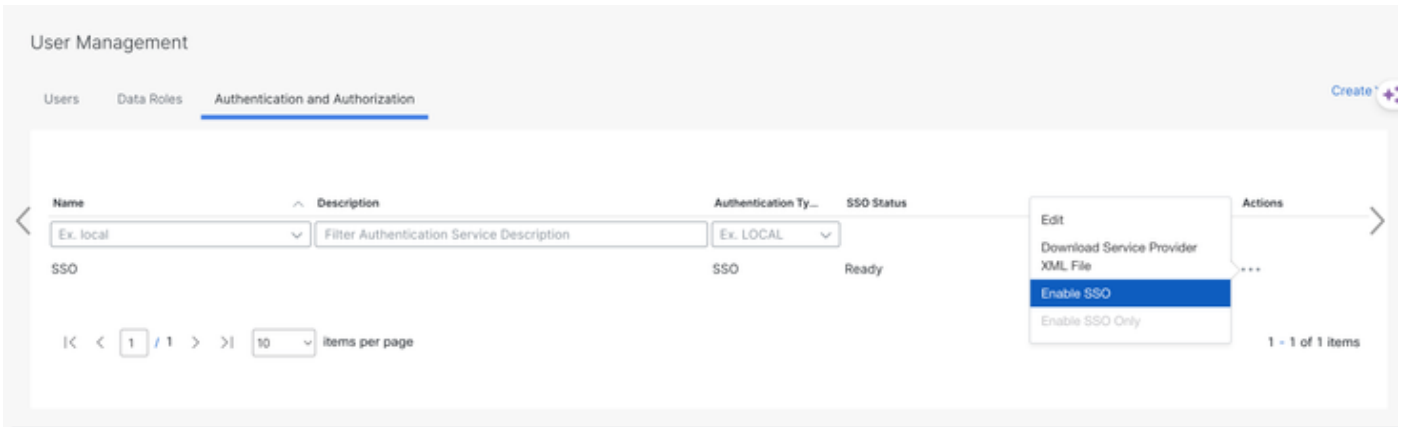
5. Konfigurieren Sie das Feld für den Identitätsanbietertyp für Microsoft Entra ID, das Namensidentifizierungsformat für Beständig, und geben Sie ein Anmeldefenster-Label ein.



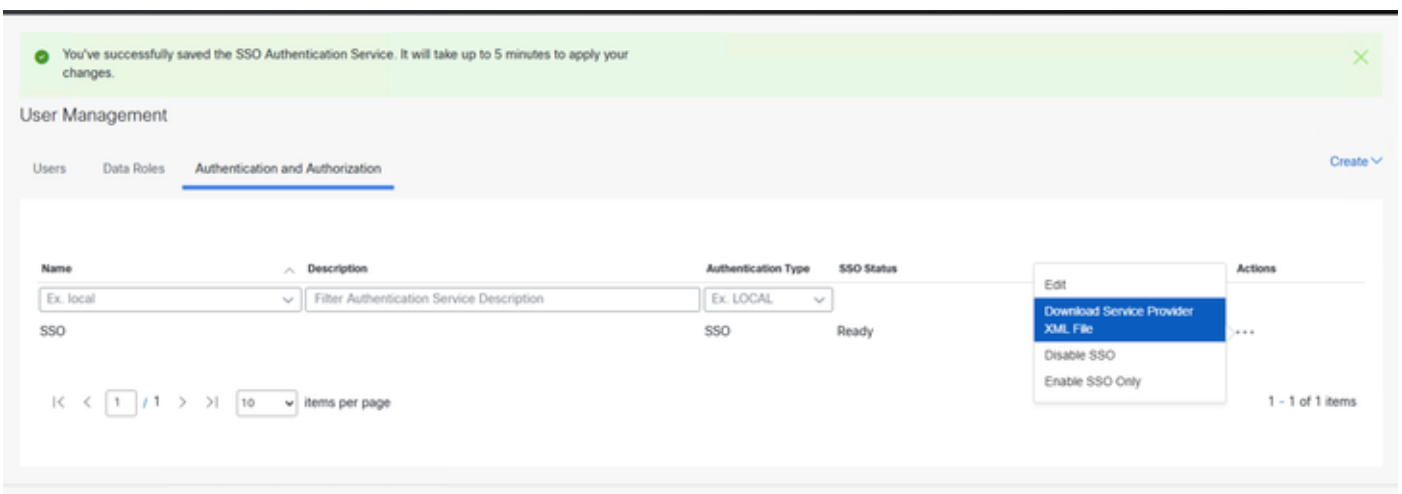
Tipp: Die Beschriftung des konfigurierten Anmeldebildschirms (Name/Text) wird über der Schaltfläche Anmelden mit SSO angezeigt und darf nicht leer gelassen werden.

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 Metadatenfile 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.



[Home](#) > [An Example SNA App Name](#)

An Example SNA App Name | SAML-based Sign-on

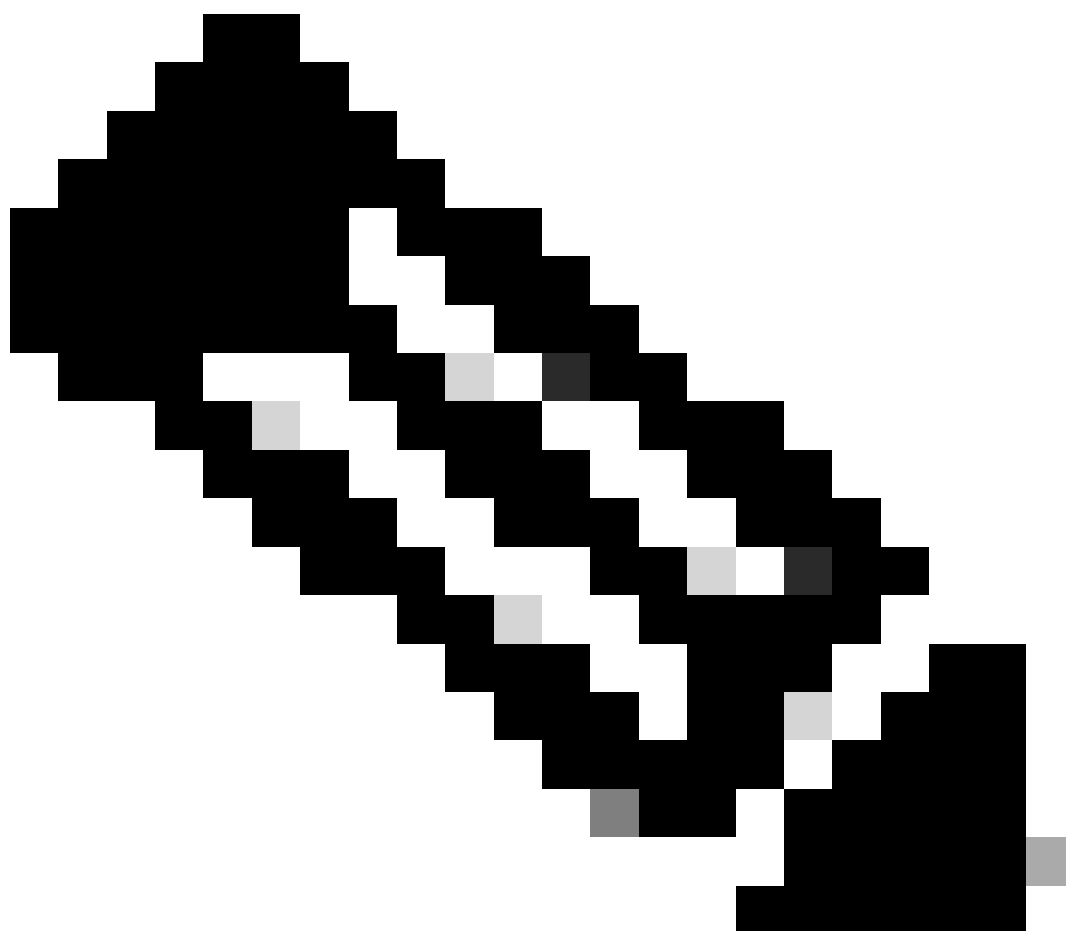
Enterprise Application



Upload metadata file



Change single sign-on



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.

Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. [Learn more.](#)

Read the [configuration guide](#) for help integrating An Example SNA App Name.

1

Basic SAML Configuration

Edit

Identifier (Entity ID)	https://example.com/fedlet
Reply URL (Assertion Consumer Service URL)	https://your-sna-manager-fqdn.com/fedlet/fedletapplication
Sign on URL	Optional
Relay State (Optional)	Optional
Logout Url (Optional)	Optional

2

Attributes & Claims

Edit

Edit u

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

6. Klicken Sie unter Forderungsname auf user.userprincipalname.

[Home](#) > [An Example SNA App Name | SAML-based Sign-on](#) > [SAML-based Sign-on](#) >

Attributes & Claims ...

[+ Add new claim](#) [+ Add a group claim](#) [≡ Columns](#) | [🗨 Got feedback?](#)

Required claim

Claim name	Type	Value
Unique User Identifier (Name ID)	SAML	user.userprincipalname [...] ***

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



Manage claim ...



Save



Discard changes



Got feedback?

Name

nameidentifier

Namespace

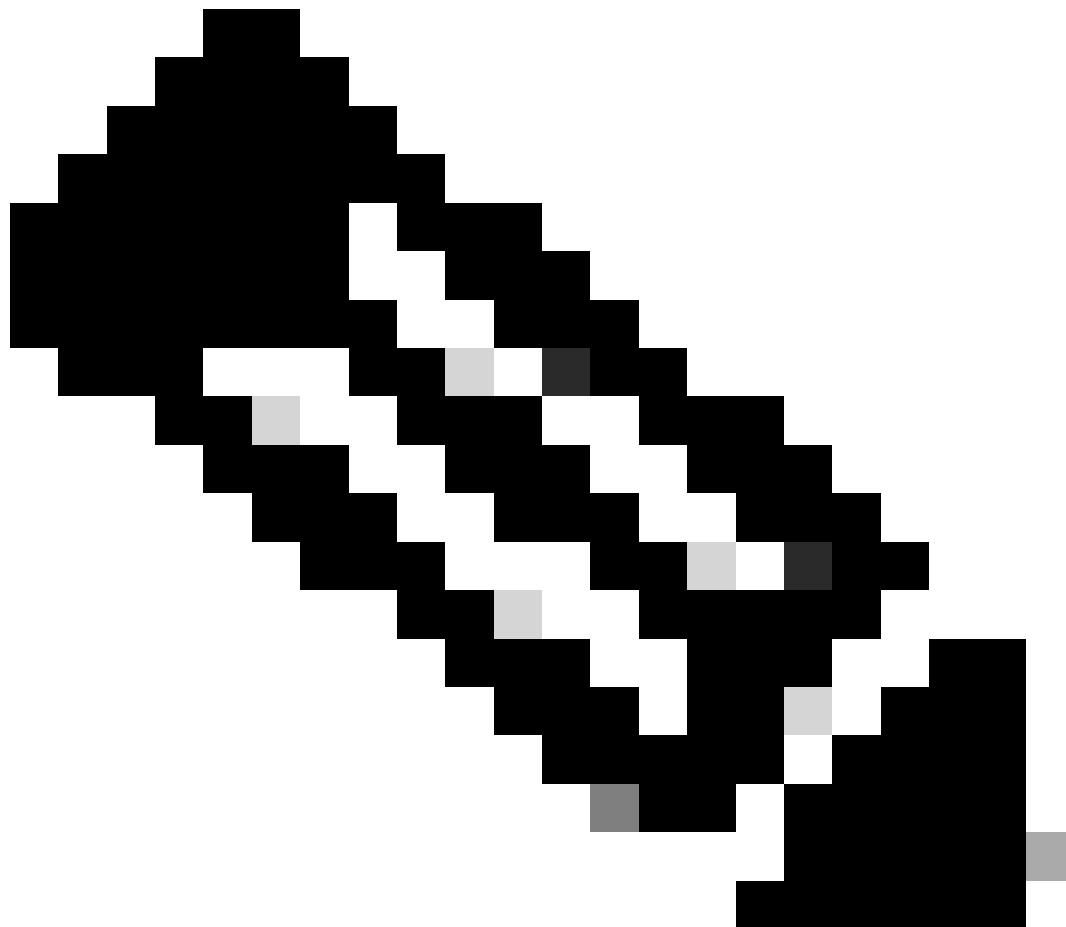
http://schemas.xmlsoap.org/ws/2005/05/identity/claims



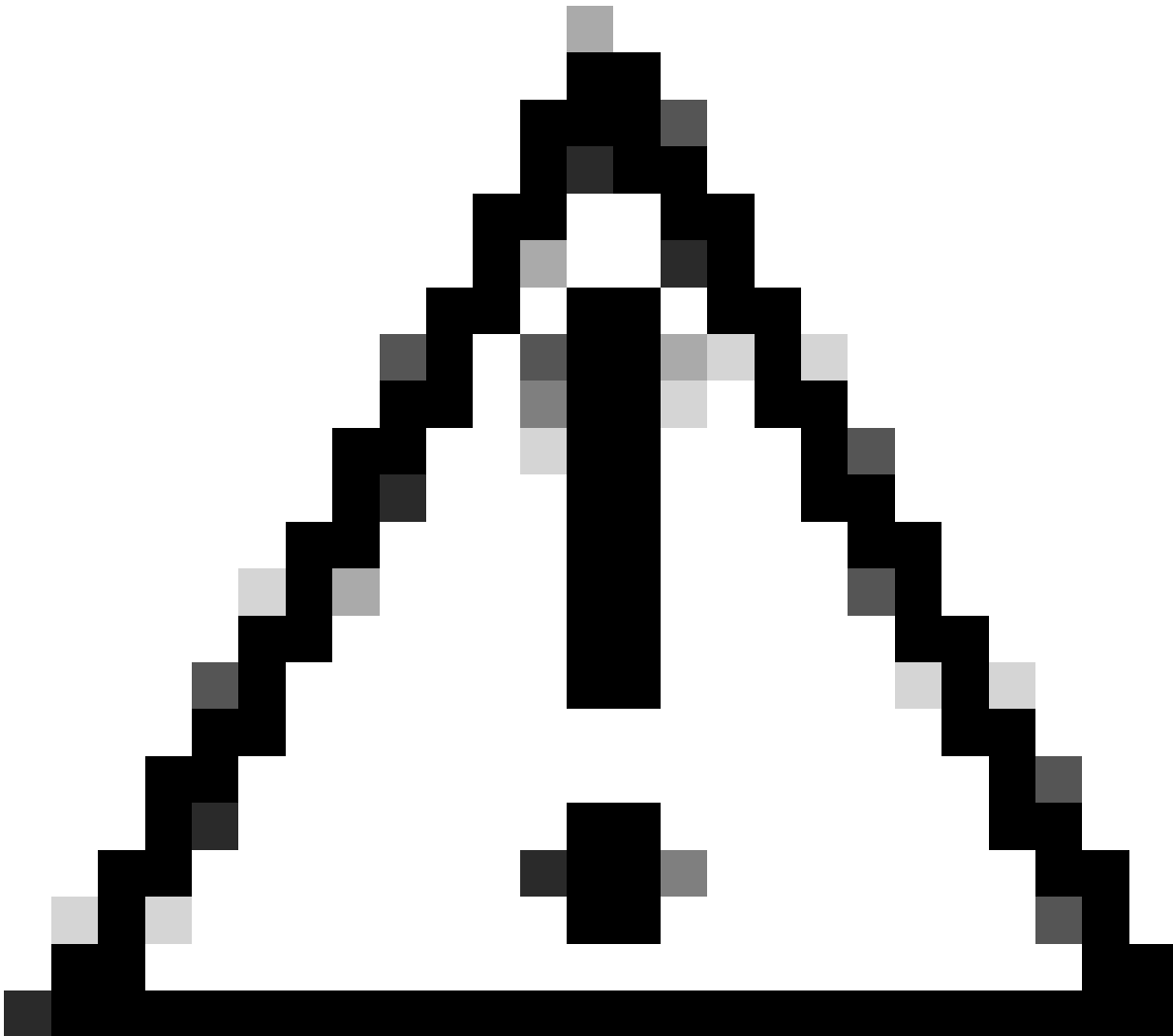
Choose name identifier format

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.

The screenshot shows the 'Users and groups' management page in the Microsoft Azure portal. The left-hand navigation pane includes links for Overview, Deployment Plan, Diagnose and solve problems, Manage (expanded), Properties, Owners, Roles and administrators, and Users and groups (which is highlighted with a star). The main content area has a top bar with '+ Add user/group', 'Edit assignment', and 'Remove as...'. Below this is an information box stating: 'The application will appear for assigned users within My App'. A message reads: 'Assign users and groups to app-roles for your application here'. A search bar contains the text 'First 200 shown, search all users & groups'. The 'Display name' section is empty, showing 'No application assignments found'.

3. Klicken Sie im linken Bereich auf Keine ausgewählt.

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

This screenshot shows the 'Add Assignment' dialog box. On the left, the 'Users and groups' section is active, showing 'None Selected' and a 'Select a role' dropdown. The main area is titled 'Users and groups' and contains a search bar with the text 'Try changing or adding filters if you don't see what you're looking for.' Below the search bar, it says '1 result found'. There are tabs for 'All', 'Users', and 'Groups'. A table lists the search results:

	Name	Type	Details
☒	Example User	User	user@example.com

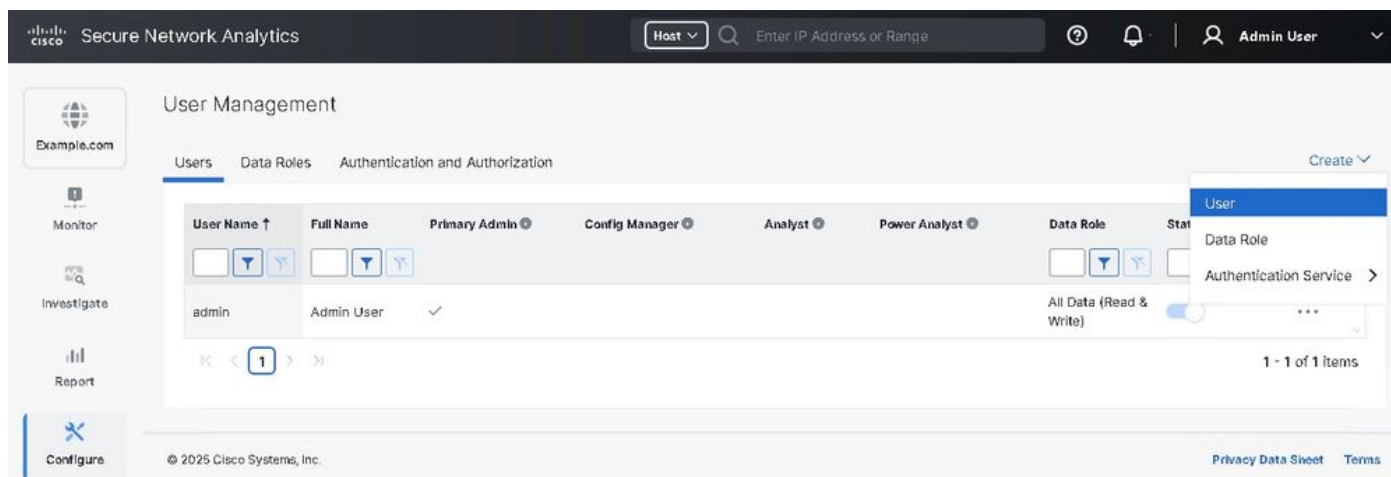
On the right side of the dialog, the 'Selected (1)' section shows a 'Reset' link and the selected user: 'Example User' with email 'user@example.com'. At the bottom, there are 'Assign' and 'Select' buttons.

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.

The screenshot shows the configuration form for a new user in the Cisco Secure Network Analytics (SNA) User Management interface. The form is divided into several sections. The top section contains input fields for 'User Name', 'Full Name', 'Email', and 'SAML ID'. To the right of these fields is a dropdown menu for 'Authentication Service' set to 'SSO'. Below this are fields for 'Password' and 'Confirm Password', with a 'Generate Password' button next to the password field. There is also a checkbox for 'Show Password'. The 'Role Settings' section includes a checkbox for 'Primary Admin' and a dropdown menu for 'Data Role' set to 'All Data (Read Only)'. A blue message box with an information icon states: 'You must select a minimum of one web role and one desktop client role.' At the bottom, there are tabs for 'Web' and 'Desktop'. Under the 'Web' tab, there is a section for 'Web Roles' with a 'Compare' link and checkboxes for 'Configuration Manager', 'Analyst', and 'Power Analyst'.

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.