

Hvordan konfigurerer du SSO med Active Directory ved hjelp av SAML?

Ester Andersson - 2024-02-19 - API, SAML, integrasjoner og generelle innstillinger

Trinn 1 - Kontakt Learnifier

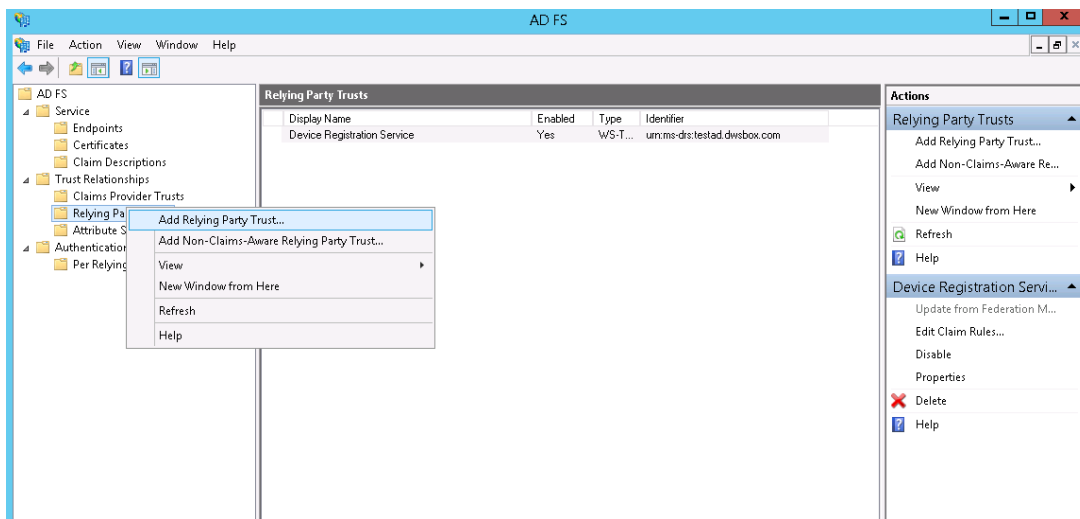
Kontakt support@learnifier.com og gi beskjed om at du ønsker å konfigurere SSO med Active Directory. Vi vil deretter gi deg en kundespesifikk metadata-URL å bruke.

OBS: Vi anbefaler at du bruker minst AD FS 3.0 (inkludert i Windows 2012R2) eller nyere.

Trinn 2 - Legg til Learnifier som en Relying Party Trust i ADFS

Start AD FS Management-verktøyet under Administrative Tools.

Velg mappen "Trust Relationships" og høyreklikk, og klikk deretter på "Add Relying Party Trusts".



På velkomstsiden i "Add Relying Party Trust Wizard" klikker du på Start.

Sørg for at alternativet "Import data about the relying party published online or on a local network" er valgt.

Angi den kundespesifikke metadata-URLen du mottok fra Learnifier. For eksempel, der du

skal angi "https://service.learnifier.com/auth_saml/saml/metadata" i feltet.

The screenshot shows a Windows-style dialog box titled "Add Relying Party Trust Wizard". On the left, a "Steps" pane lists: Welcome, Select Data Source (highlighted), Configure Multi-factor Authentication Now?, Choose Issuance Authorization Rules, Ready to Add Trust, and Finish. The main area is titled "Select Data Source" and contains the instruction: "Select an option that this wizard will use to obtain data about this relying party:". There are three radio button options: 1. "Import data about the relying party published online or on a local network" (selected). Below it is a text box containing "https://service.learnifier.com/auth_saml/saml/metadata" and an example: "Example: fs.contoso.com or https://www.contoso.com/app". 2. "Import data about the relying party from a file". Below it is a text box for "Federation metadata file location:" and a "Browse..." button. 3. "Enter data about the relying party manually". Below it is the text: "Use this option to manually input the necessary data about this relying party organization." At the bottom right are buttons for "< Previous", "Next >", and "Cancel".

Rediger "display name" og "note" om nødvendig. Når du er ferdig, klikker du på "Next".

Add Relying Party Trust Wizard

Specify Display Name

Enter the display name and any optional notes for this relying party.

Display name:

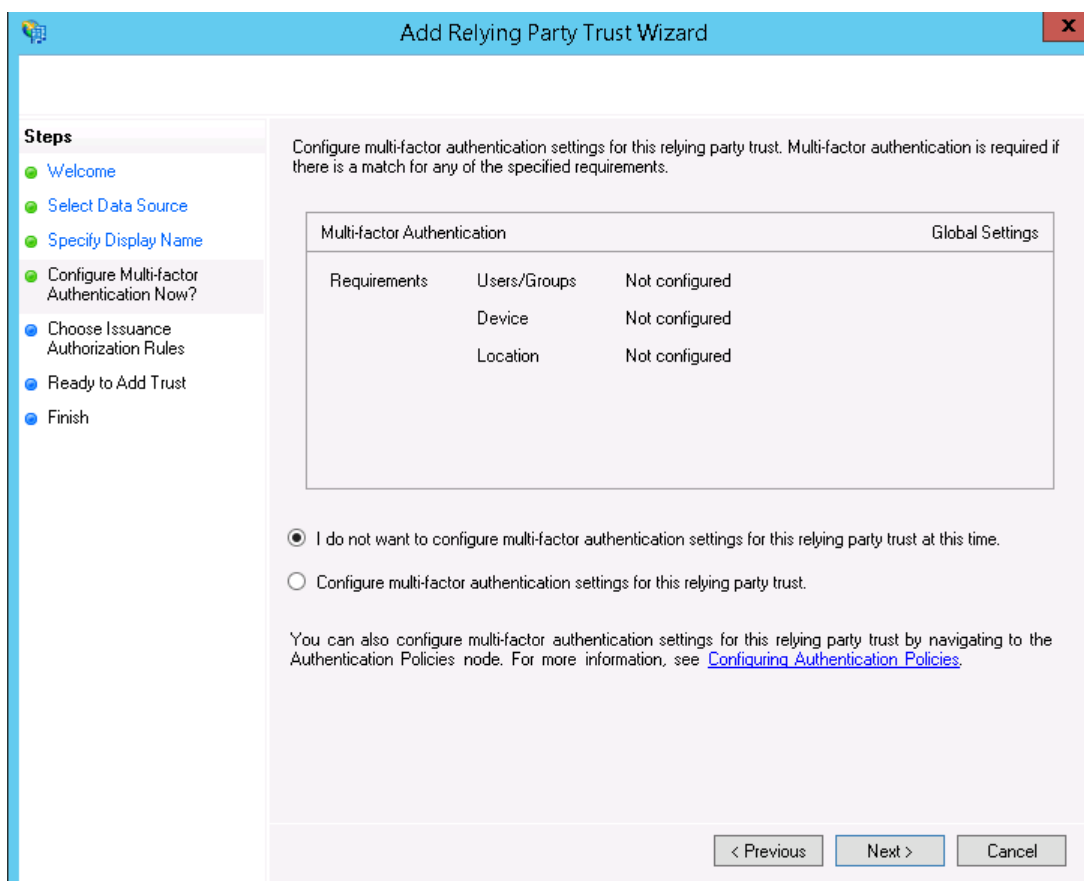
Notes:

< Previous Next > Cancel

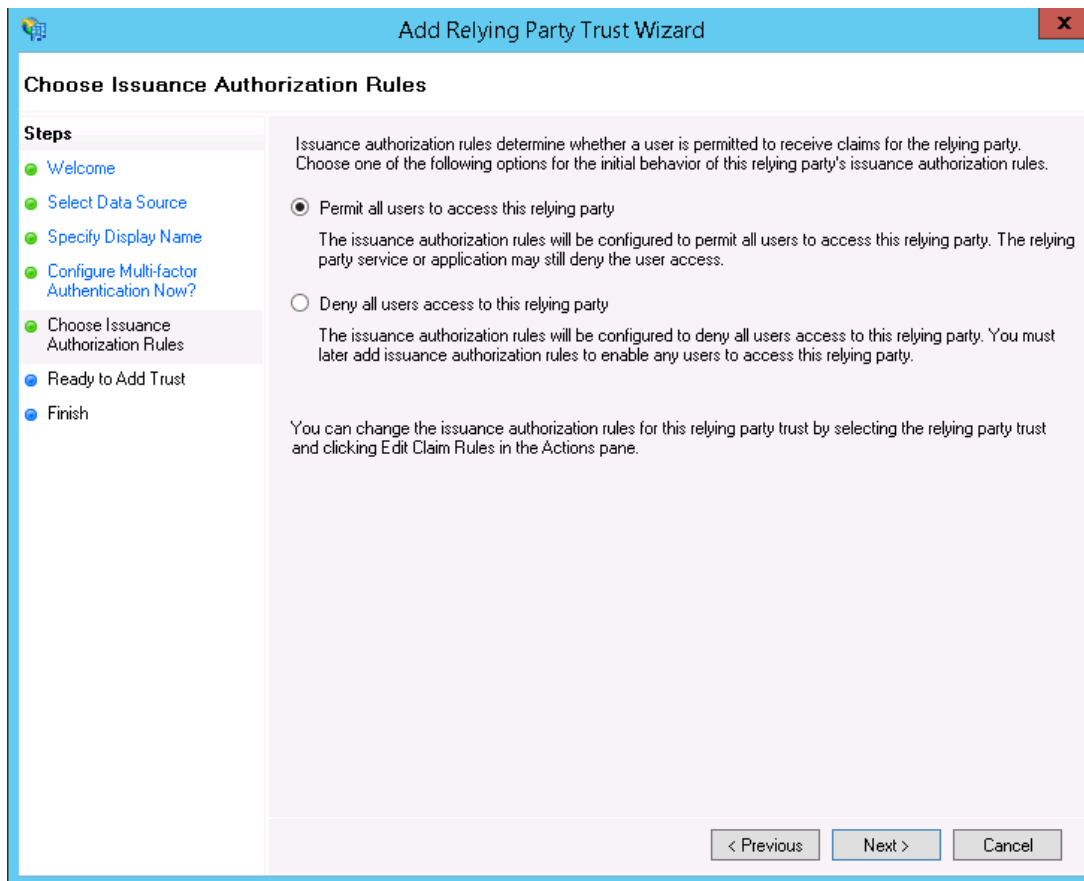
Steps

- Welcome
- Select Data Source
- Specify Display Name
- Configure Multi-factor Authentication Now?
- Choose Issuance Authorization Rules
- Ready to Add Trust
- Finish

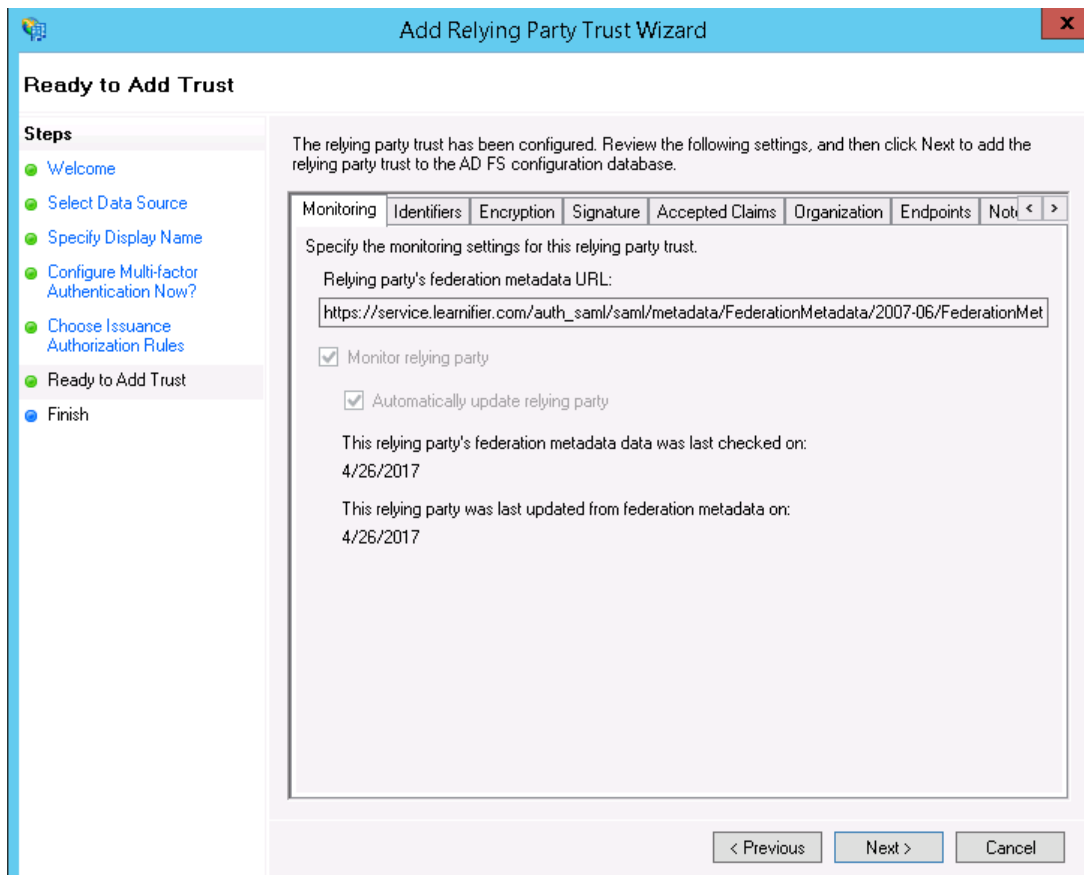
På denne siden velger du å ikke bruke MFA (Multi-Factor Authentication).



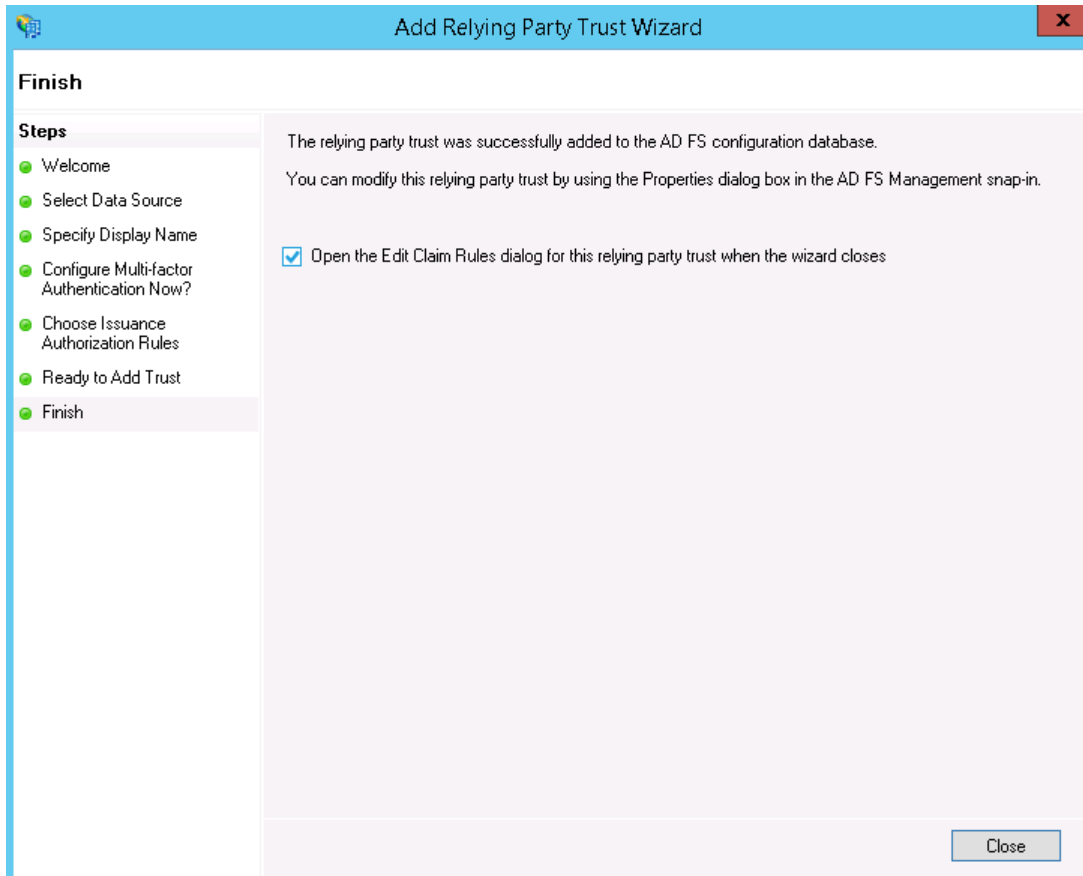
På denne siden tillater du alle brukere å få tilgang til Learnifier.



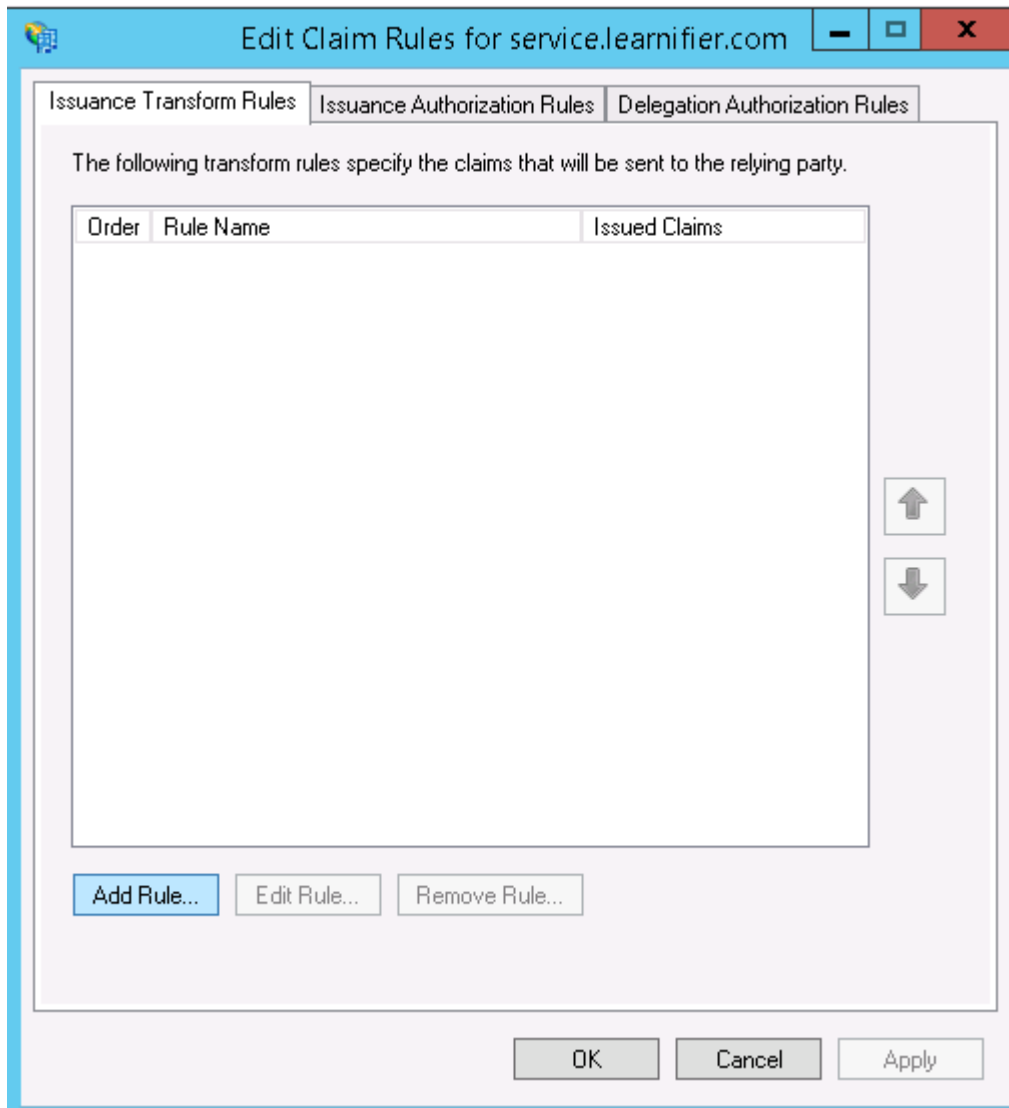
På denne siden klikker du bare på "Next".



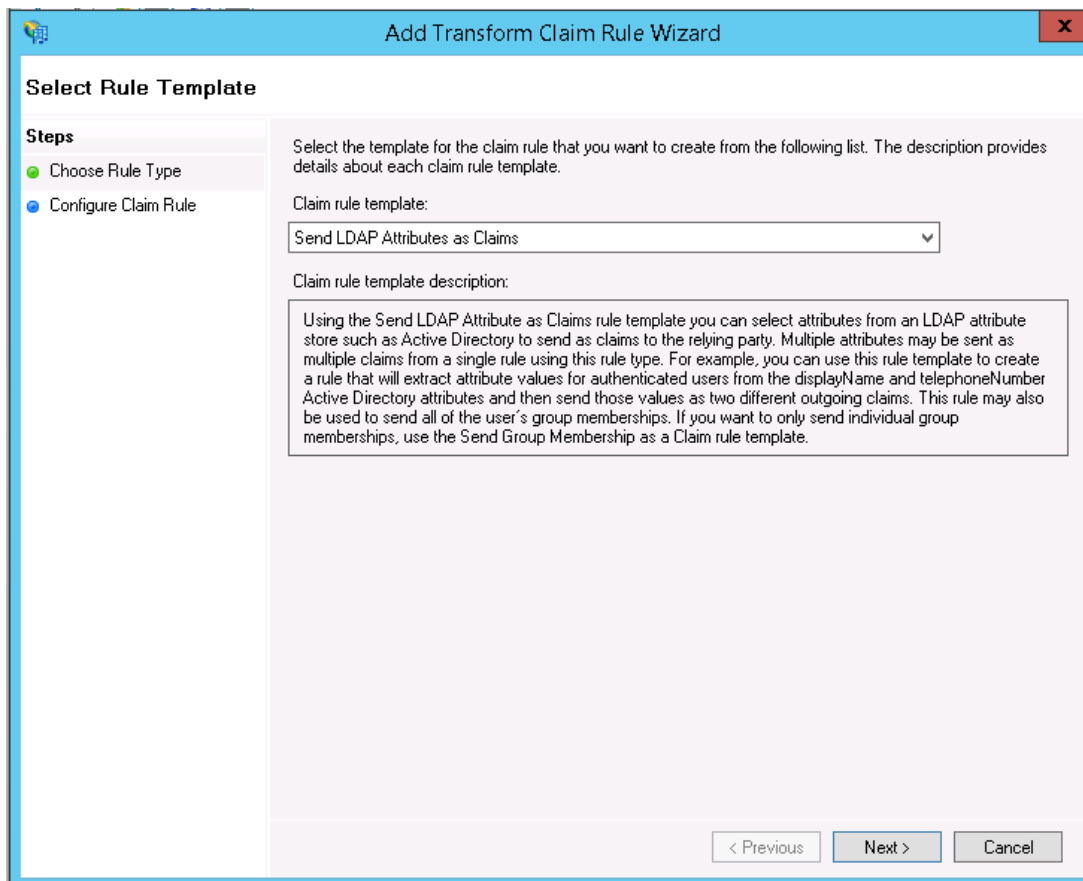
Sørg for at avmerkingsboksen er merket og klikk på "Close".



Klikk på "Add Rule".



Velg å sende "LDAP Attributes" som Claims.



Angi "Learnifier Claims" som Claim rule name. Sørg for at "Attribute Store" er "Active Director" og legg til verdiene som vist på skjermbildet.

Add Transform Claim Rule Wizard

Configure Rule

Steps

- Choose Rule Type
- Configure Claim Rule

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:

Rule template: Send LDAP Attributes as Claims

Attribute store:

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)		Outgoing Claim Type (Select or type to add more)
	SAM-Account-Name	▼	Name ID
	Display-Name	▼	Name
	E-Mail-Addresses	▼	E-Mail Address
	Given-Name	▼	Given Name
▶	Surname	▼	Surname

< Previous Finish Cancel

Trinn 3 - Kontakt Learnifier

Kontakt din representant og gi ham/henne URL-en for SAML-metadata for ditt Active Directory Federation Services. Hvis "login web server" / AD FS er tilgjengelig på <https://login.example.com>, er metadata vanligvis tilgjengelig på <https://login.example.com/FederationMetadata/2007-06/FederationMetadata.xml>. Lenken må være en HTTP-lenke, og serveren må være tilgjengelig fra det offentlige internettet.

Du bør få en "response" kort tid etter at tilkoblingen er etablert.

Feilsøking

Sørg for at Secure hash algorithm er satt til SHA-256 (tilgjengelig under fanen "Advanced") i den opprettede Relying Party Trust.