

ADMINISTRATOR
KONSOLE

> MELDEN SIE SICH MIT
SSO AN

> IMPLEMENTIERUNGSLEITFÄDEN

ADFS SAML Implementierung

ADFS SAML Implementierung

Dieser Artikel enthält **Active Directory Federation Services (AD FS)-spezifische** Hilfe zur Konfiguration der Zugangsdaten mit SSO über SAML 2.0. Für Hilfe bei der Konfiguration der Zugangsdaten mit SSO für einen anderen IdP, verweisen Sie auf [SAML 2.0 Konfiguration](#).

Die Konfiguration beinhaltet das gleichzeitige Arbeiten innerhalb der Bitwarden-Web-App und dem AD FS Server-Verwalter. Während Sie fortfahren, empfehlen wir, beides griffbereit zu haben und die Schritte in der Reihenfolge durchzuführen, in der sie dokumentiert sind.



Tip

Bereits ein SSO-Experte? Überspringen Sie die Anweisungen in diesem Artikel und laden Sie Screenshots von Beispielkonfigurationen herunter, um sie mit Ihren eigenen zu vergleichen.

⬇ Typ: Asset-Hyperlink ID: 5892IOGrU7B9lvBmN0P0xl

Öffnen Sie SSO in der Web-App

Melden Sie sich bei der Bitwarden-Web-App an und öffnen Sie die Administrator-Konsole mit dem Produktschalter :



My Organization

Collections

Members

Groups

Reporting

Billing

Settings

Organization info

Policies

Two-step login

Import data

Export vault

Domain verification

Single sign-on

Device approvals

SCIM provisioning

Single sign-on

Use the [require single sign-on authentication policy](#) to require all members to log in with SSO.

☒ Allow SSO authentication

Once set up, your configuration will be saved and members will be able to authenticate using their Identity Provider credentials.

SSO identifier (required)

unique-organization-identifier

Provide this ID to your members to login with SSO. To bypass this step, set up [Domain verification](#)

Member decryption options

☒ Master password

☐ Trusted devices

Once authenticated, members will decrypt vault data using a key stored on their device. The [single organization](#) policy, [SSO required](#) policy, and [account recovery administration](#) policy with automatic enrollment will turn on when this option is used.

Type

SAML 2.0

SAML service provider configuration

☒ Set a unique SP entity ID

Generate an identifier that is unique to your organization

SP entity ID

SAML 2.0 metadata URL

SAML 2.0 Konfiguration

Wenn Sie es noch nicht getan haben, erstellen Sie einen einzigartigen **SSO-Identifikator** für Ihre Organisation und wählen Sie **SAML** aus dem **Typ**-Dropdown aus. Lassen Sie diesen Bildschirm geöffnet für eine einfache Referenz.

Sie können die Option **Einen einzigartigen SP-Entity-ID festlegen** in diesem Stadium ausschalten, wenn Sie möchten. Wenn Sie dies tun, wird Ihre Organisations-ID aus Ihrem SP-Entity-ID-Wert entfernt. In fast allen Fällen wird jedoch empfohlen, diese Option aktiviert zu lassen.



Tip

Es gibt alternative **Mitglied Entschlüsselungsoptionen**. Erfahren Sie, wie Sie mit [SSO auf vertrauenswürdigen Geräten](#) oder mit [Key Connector](#) beginnen können.

Erstellen Sie eine Vertrauensstellung für die vertrauende Partei

Im AD FS Server Manager wählen Sie **Tools → AD FS Verwaltung → Aktion → Vertrauensstellung hinzufügen**. Im Assistenten treffen Sie die folgenden Auswahlmöglichkeiten:

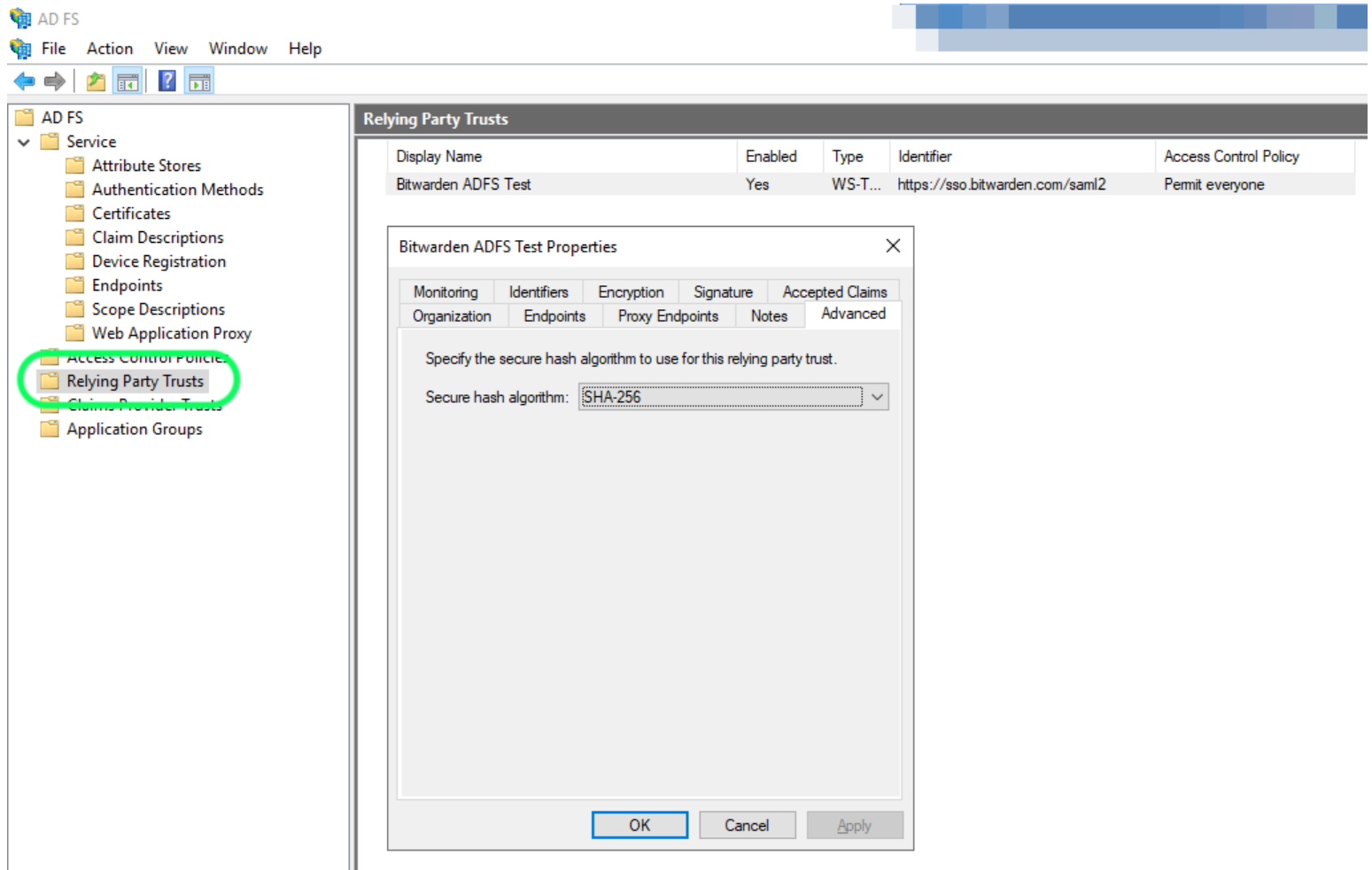
1. Auf dem Willkommensbildschirm wählen Sie **Claims Aware**.
2. Auf dem Bildschirm Datenquelle auswählen, wählen Sie **Geben Sie Daten über die vertrauende Partei manuell ein**.
3. Auf dem Bildschirm "Anzeigenamen festlegen" geben Sie einen spezifischen Anzeigenamen für Bitwarden ein.
4. Auf dem Bildschirm "URL konfigurieren" wählen Sie **Unterstützung für SAML 2.0 WebSSO-Protokoll aktivieren**.
 - Geben Sie in das Eingabefeld **Vertrauensstellende Partei SAML 2.0 SSO Service URL** die Assertion Consumer Service (ACS) URL ein. Dieser automatisch generierte Wert kann von der **Einstellungen → Single Sign-On** Seite der Organisation kopiert werden und variiert je nach Ihrer Konfiguration.
5. Auf dem Bildschirm **Zugriffskontrollrichtlinie auswählen**, wählen Sie die Richtlinie aus, die Ihren Sicherheitsstandards entspricht.
6. Auf dem Bildschirm **Kennungen konfigurieren**, fügen Sie die SP-Entity-ID als Vertrauenskennung der vertrauenden Partei hinzu. Dieser automatisch generierte Wert kann von der **Einstellungen → Single Sign-On** Seite der Organisation kopiert werden und variiert je nach Ihrer Konfiguration.
7. Auf dem Bildschirm **Zugriffskontrollrichtlinie auswählen**, wählen Sie die gewünschte Richtlinie aus (standardmäßig ist **Jedem erlauben** ausgewählt).
8. Auf dem Bildschirm **Bereit zum Hinzufügen von Vertrauen**, überprüfen Sie Ihre Auswahl.

Erweiterte Optionen

Sobald das Vertrauen der vertrauenden Partei erstellt wurde, können Sie dessen Einstellungen weiter konfigurieren, indem Sie **Vertrauende Parteien** aus dem linken Dateinavigators auswählen und den korrekten Anzeigenamen auswählen.

Hash-Algorithmus

Um den **Secure Hash Algorithmus** (standardmäßig SHA-256) zu ändern, navigieren Sie zum **Erweitert** Tab:



AD FS

File Action View Window Help

AD FS

- Service
 - Attribute Stores
 - Authentication Methods
 - Certificates
 - Claim Descriptions
 - Device Registration
 - Endpoints
 - Scope Descriptions
 - Web Application Proxy
 - Access Control Policies
 - Relying Party Trusts**
 - Claims Provider Trusts
 - Application Groups

Relying Party Trusts

Display Name	Enabled	Type	Identifier	Access Control Policy
Bitwarden ADFS Test	Yes	WS-T...	https://sso.bitwarden.com/saml2	Permit everyone

Bitwarden ADFS Test Properties

Monitoring Identifiers Encryption Signature Accepted Claims

Organization Endpoints Proxy Endpoints Notes Advanced

Specify the secure hash algorithm to use for this relying party trust.

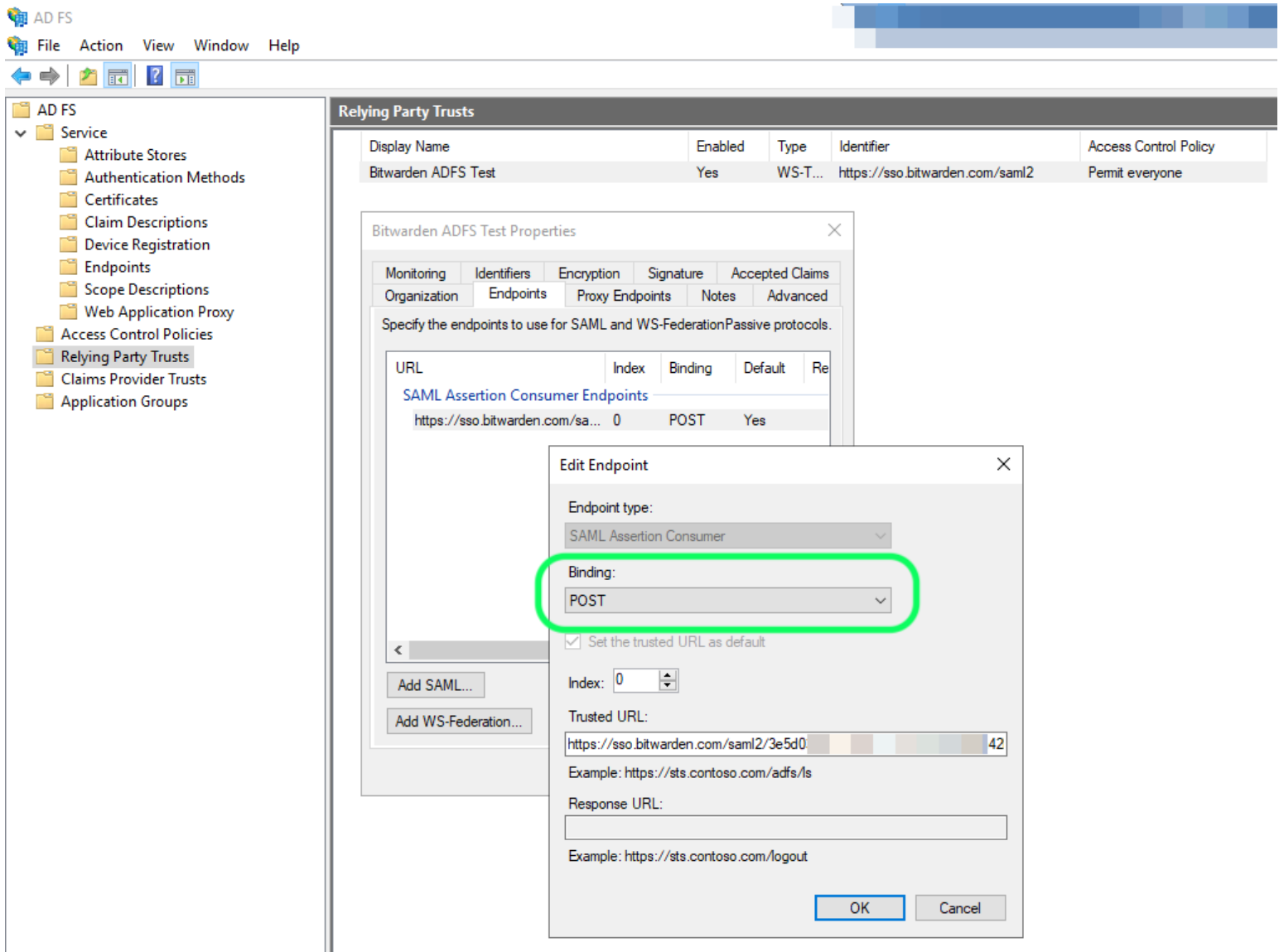
Secure hash algorithm: SHA-256

OK Cancel Apply

Stellen Sie einen sicheren Hash-Algorithmus ein

Endpunktbindung

Um den Endpunkt **Binding** zu ändern (standardmäßig POST), navigieren Sie zum **Endpoints** Tab und wählen Sie die konfigurierte ACS-URL aus:



AD FS

File Action View Window Help

AD FS

- Service
 - Attribute Stores
 - Authentication Methods
 - Certificates
 - Claim Descriptions
 - Device Registration
 - Endpoints
 - Scope Descriptions
 - Web Application Proxy
 - Access Control Policies
 - Relying Party Trusts
 - Claims Provider Trusts
 - Application Groups

Relying Party Trusts

Display Name	Enabled	Type	Identifier	Access Control Policy
Bitwarden ADFS Test	Yes	WS-T...	https://sso.bitwarden.com/saml2	Permit everyone

Bitwarden ADFS Test Properties

Monitoring Identifiers Encryption Signature Accepted Claims

Organization Endpoints Proxy Endpoints Notes Advanced

Specify the endpoints to use for SAML and WS-FederationPassive protocols.

URL	Index	Binding	Default	Re
SAML Assertion Consumer Endpoints				
https://sso.bitwarden.com/sa...	0	POST	Yes	

Add SAML...

Add WS-Federation...

Edit Endpoint

Endpoint type: SAML Assertion Consumer

Binding: POST

☒ Set the trusted URL as default

Index: 0

Trusted URL: https://sso.bitwarden.com/saml2/3e5d0

Example: https://sts.contoso.com/adfs/ls

Response URL:

Example: https://sts.contoso.com/logout

OK Cancel

Endpunkt bearbeiten

Bearbeiten Sie die Ausstellungsregeln für Ansprüche

Erstellen Sie Ausstellungsregeln für Ansprüche, um sicherzustellen, dass die entsprechenden Ansprüche, einschließlich **Name ID**, an Bitwarden weitergegeben werden. Die folgenden Tabs veranschaulichen ein Beispiel für eine Regelmenge:

⇒Regel 1

AD FS

Service

Attribute Stores

Authentication Methods

Certificates

Claim Descriptions

Device Registration

Endpoints

Scope Descriptions

Web Application Proxy

Access Control Policies

Relying Party Trusts

Claims Provider Trusts

Application Groups

File Action View Window Help

← →

📁

🔍

❓

🔧

Relying Party Trusts

Display Name	Enabled	Type	Identifier	Access Control Policy
Bitwarden ADFS Test	Yes	WS-T...	https://sso.bitwarden.com/saml2	Permit everyone

Edit Claim Issuance Policy for Bitwarden ADFS Test

Issuance Transform Rules

The following transform rules specify the claims that will be sent to the relying party.

Order	Rule Name	Issued Claims
1	Bitwarden	E-Mail Address, Name, Giv...
2	UPN	UPN
3	Transform Name ID	Name ID

Edit Rule - Bitwarden

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:

Bitwarden

Rule template: Send LDAP Attributes as Claims

Attribute store:

Active Directory

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)
▶	E-Mail-Addresses	E-Mail Address
	Display-Name	Name
	Given-Name	Given Name
	Surname	Surname
*		

View Rule Language...

OK

Cancel

ADFS Regel 1

© 2025 Bitwarden Inc | Page 8 of 16

⇒Regel 2

AD FS

File Action View Window Help

AD FS

Service

- Attribute Stores
- Authentication Methods
- Certificates
- Claim Descriptions
- Device Registration
- Endpoints
- Scope Descriptions
- Web Application Proxy

Access Control Policies

Relying Party Trusts

Claims Provider Trusts

Application Groups

Relying Party Trusts

Display Name	Enabled	Type	Identifier	Access Control Policy
Bitwarden ADFS Test	Yes	WS-T...	https://sso.bitwarden.com/saml2	Permit everyone

Edit Claim Issuance Policy for Bitwarden ADFS Test

Issuance Transform Rules

The following transform rules specify the claims that will be sent to the relying party.

Order	Rule Name	Issued Claims
1	Bitwarden	E-Mail Address, Name, Giv ...
2	UPN	UPN
3	Transform Name ID	Name ID

Edit Rule - UPN

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:
UPN

Rule template: Send LDAP Attributes as Claims

Attribute store:
Active Directory

Mapping of LDAP attributes to outgoing claim types:

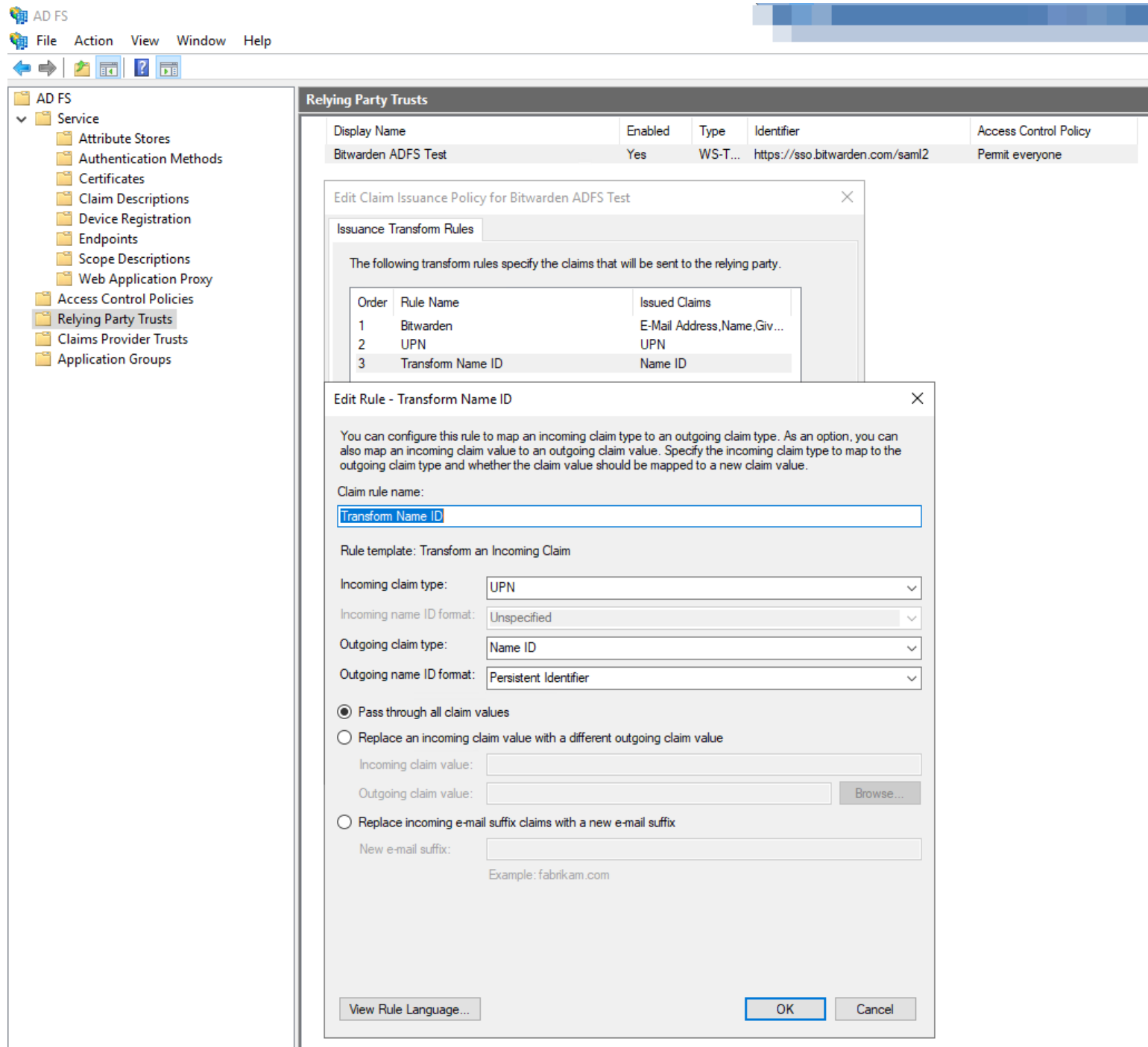
	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
▶	User-Principal-Name	UPN
*		

View Rule Language...

OK Cancel

ADFS-Regel 2

⇒Regel 3



AD FS

File Action View Window Help

AD FS

- Service
 - Attribute Stores
 - Authentication Methods
 - Certificates
 - Claim Descriptions
 - Device Registration
 - Endpoints
 - Scope Descriptions
 - Web Application Proxy
- Access Control Policies
- Relying Party Trusts**
- Claims Provider Trusts
- Application Groups

Relying Party Trusts

Display Name	Enabled	Type	Identifier	Access Control Policy
Bitwarden ADFS Test	Yes	WS-T...	https://sso.bitwarden.com/saml2	Permit everyone

Edit Claim Issuance Policy for Bitwarden ADFS Test

Issuance Transform Rules

The following transform rules specify the claims that will be sent to the relying party.

Order	Rule Name	Issued Claims
1	Bitwarden	E-Mail Address, Name, Giv...
2	UPN	UPN
3	Transform Name ID	Name ID

Edit Rule - Transform Name ID

You can configure this rule to map an incoming claim type to an outgoing claim type. As an option, you can also map an incoming claim value to an outgoing claim value. Specify the incoming claim type to map to the outgoing claim type and whether the claim value should be mapped to a new claim value.

Claim rule name:
Transform Name ID

Rule template: Transform an Incoming Claim

Incoming claim type: UPN

Incoming name ID format: Unspecified

Outgoing claim type: Name ID

Outgoing name ID format: Persistent Identifier

☒ Pass through all claim values

☐ Replace an incoming claim value with a different outgoing claim value

Incoming claim value:

Outgoing claim value: Browse...

☐ Replace incoming e-mail suffix claims with a new e-mail suffix

New e-mail suffix:

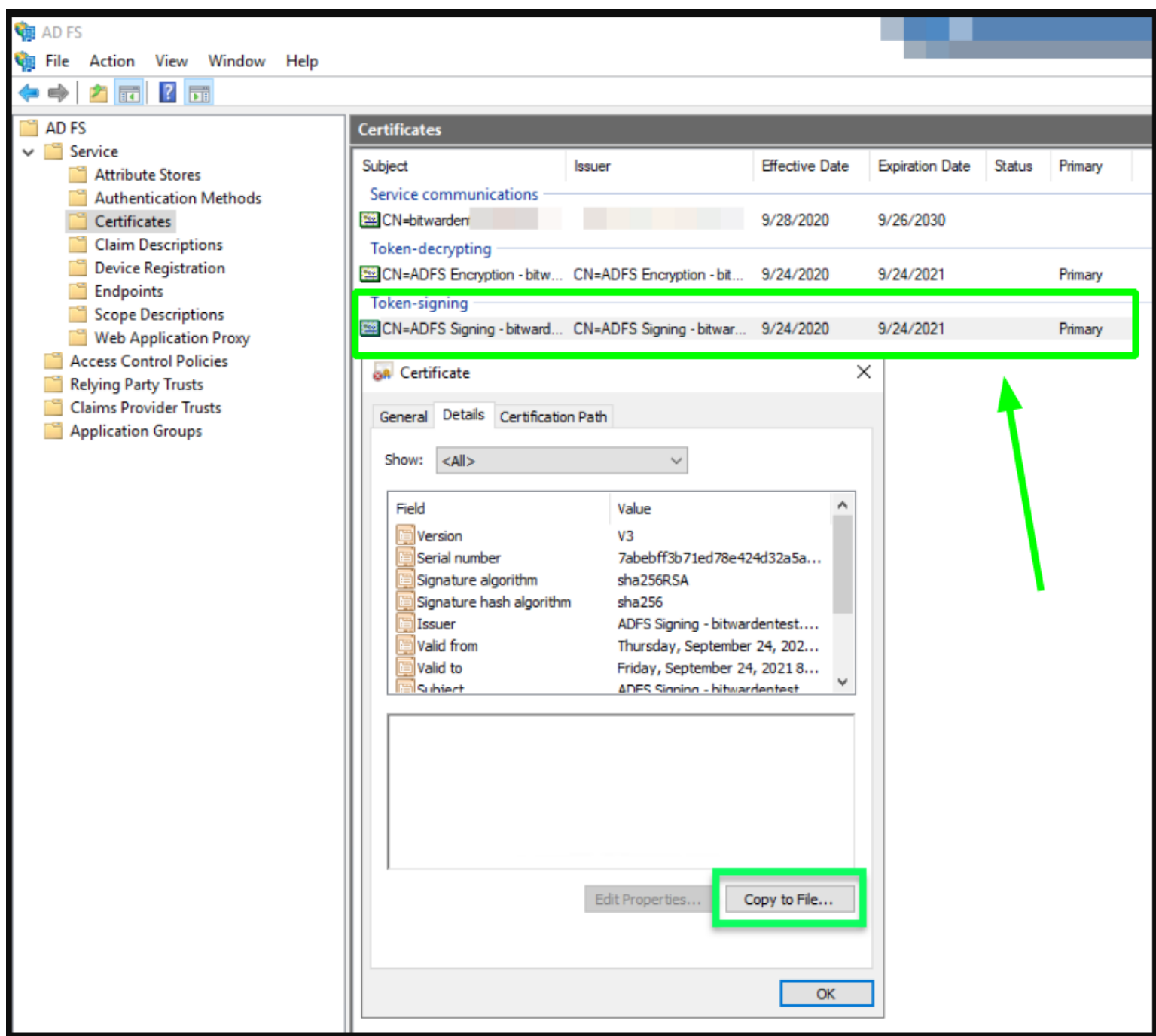
Example: fabrikam.com

View Rule Language... OK Cancel

ADFS Regel 3

Zertifikat erhalten

Im linken Datei-Navigator wählen Sie **AD FS** → **Service** → **Zertifikate**, um die Liste der Zertifikate zu öffnen. Wählen Sie das **Token-Signatur** Zertifikat aus, navigieren Sie zu seinem **Details** Tab und wählen Sie die **Kopieren in Datei...** Schaltfläche, um das Base-64 codierte Token-Signatur-Zertifikat zu exportieren:

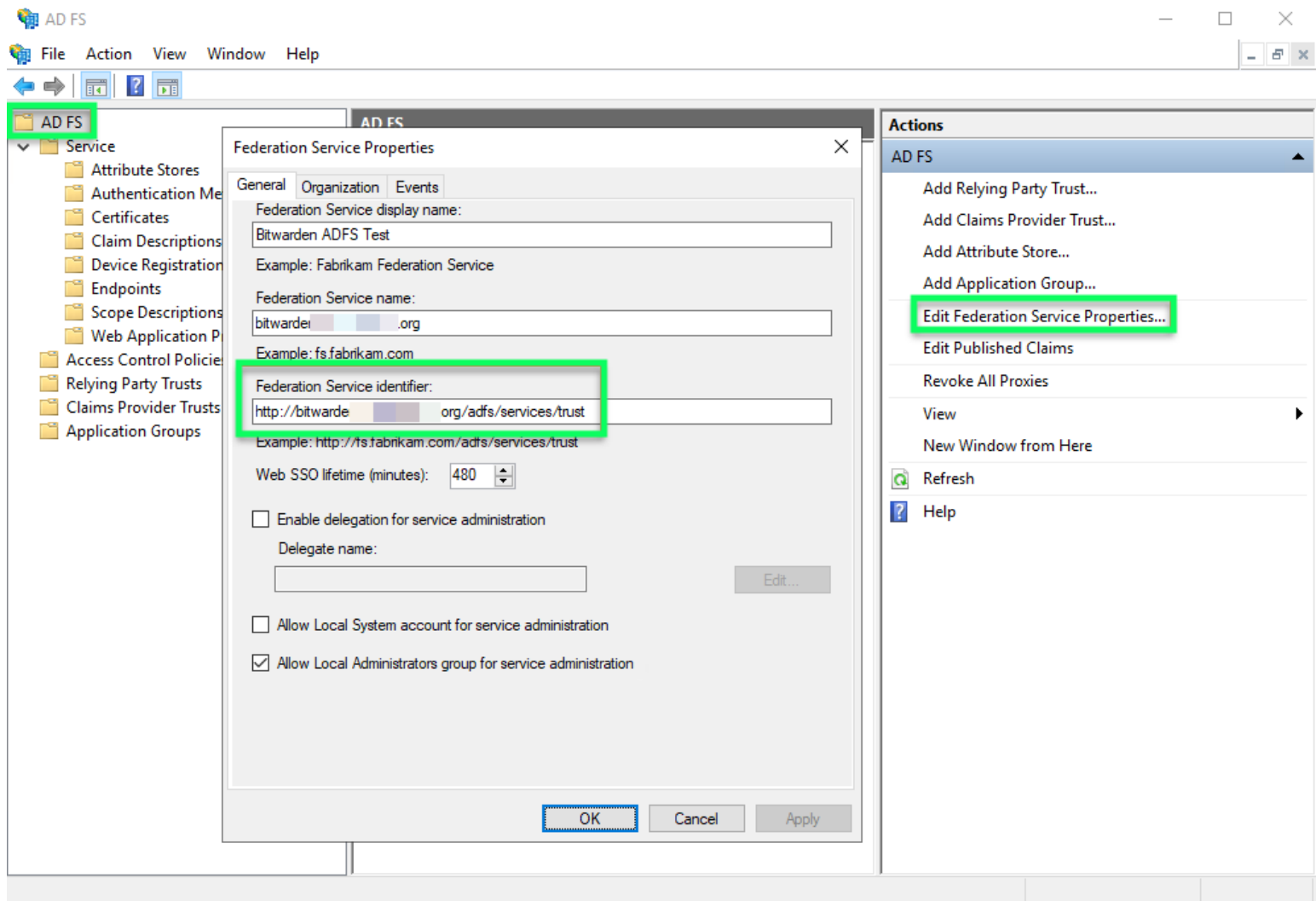


Token-Signatur Zertifikat erhalten

Sie werden dieses Zertifikat [in einem späteren Schritt](#) benötigen.

Holen Sie sich den Verbunddienst-Identifikator

Im linken Dateinavigator wählen Sie **AD FS** aus und im rechten Optionsmenü wählen Sie **Federation Service Eigenschaften bearbeiten**. Im Fenster für die Federation Service Eigenschaften, kopieren Sie den **Federation Service Identifier**:



Erhalten Sie den Federation Service Identifier

Sie werden diesen Identifikator [in einem späteren Schritt](#) benötigen.

Zurück zur Web-App

Bis zu diesem Zeitpunkt haben Sie alles, was Sie im Kontext des AD FS Server Managers benötigen, konfiguriert. Kehren Sie zur Bitwarden-Webanwendung zurück, um die Konfiguration abzuschließen.

Der Single-Sign-On-Bildschirm teilt die Konfiguration in zwei Abschnitte auf:

- Die Konfiguration des **SAML-Dienstanbieters** bestimmt das Format der SAML-Anfragen.
- **Durch die Konfiguration des SAML-Identitätsanbieters** wird das zu erwartende Format für SAML-Antworten bestimmt.

Konfiguration des Dienstanbieters

Im Abschnitt zur Konfiguration des Dienstanbieters konfigurieren Sie die folgenden Felder:

Feld	Beschreibung
Namens-ID-Format	Wählen Sie das Format der ausgehenden Namens-ID aus, das bei der Erstellung von Regeln für die Ausstellung von Ansprüchen ausgewählt wurde (siehe Regel 3).
Ausgehendes Signatur-Algorithmus	Der Algorithmus, den Bitwarden zur Signierung von SAML-Anfragen verwenden wird.
Unterzeichnungsverhalten	Ob/wann SAML-Anfragen signiert werden.
Mindesteingehendes Signaturalgorithmus	Standardmäßig wird AD FS mit SHA-256 signieren. Wählen Sie SHA-256 aus dem Dropdown-Menü, es sei denn, Sie haben AD FS so konfiguriert, dass ein anderer Algorithmus verwendet wird .
Möchte Behauptungen unterschrieben haben	Ob Bitwarden erwartet, dass SAML-Behauptungen signiert werden.
Zertifikate validieren	Markieren Sie dieses Kästchen, wenn Sie vertrauenswürdige und gültige Zertifikate von Ihrem IdP über eine vertrauenswürdige CA verwenden. Selbstsignierte Zertifikate können fehlschlagen, es sei denn, die richtigen Vertrauensketten sind innerhalb des Bitwarden Zugangsdaten mit SSO Docker-Image konfiguriert.

Wenn Sie mit der Konfiguration des Dienstanbieters fertig sind, **speichern** Sie Ihre Arbeit.

Konfiguration des Identitätsanbieters

Die Konfiguration des Identitätsanbieters erfordert oft, dass Sie auf den AD FS Server Manager zurückgreifen, um Werte abzurufen:

Feld	Beschreibung
Entitäts-ID	Geben Sie den abgerufenen Federation Service Identifier ein. Bitte beachten Sie, dass dies möglicherweise kein HTTPS verwendet . Dieses Feld ist Groß- und Kleinschreibungssensitiv.

Feld	Beschreibung
Bindungsart	Standardmäßig verwendet AD FS die HTTP POST Endpunktbindung. Wählen Sie HTTP POST , es sei denn, Sie haben AD FS so konfiguriert, dass eine andere Methode verwendet wird .
Einmaliges Anmelden Service URL	Geben Sie den SSO-Service-Endpunkt ein. Dieser Wert kann im Service → Endpoints Tab im AD FS Manager erstellt werden. Die Endpunkt-URL ist als URL-Pfad für SAML2.0/WS-Federation aufgeführt und ist normalerweise so etwas wie <code>https://ihre-Domain/adfs/ls</code> . Sie können den genauen Wert aus dem Konfigurationsschlüssel für SingleSignOnService im <code>FederationMetadata.xml</code> Dokument erhalten.
X509 Öffentliches Zertifikat	Fügen Sie das heruntergeladene Zertifikat ein und entfernen Sie es. -----BEGIN ZERTIFIKAT----- und -----ENDE ZERTIFIKAT----- Der Zertifikatswert ist Groß- und Kleinschreibungssensitiv, zusätzliche Leerzeichen, Zeilenumbrüche und andere überflüssige Zeichen werden dazu führen, dass die Zertifizierung fehlschlägt.
Ausgehendes Signatur-Algorithmus	Standardmäßig wird AD FS mit SHA-256 signieren. Wählen Sie SHA-256 aus dem Dropdown-Menü, es sei denn, Sie haben AD FS so konfiguriert, dass ein anderer Algorithmus verwendet wird .
Deaktivieren Sie ausgehende Abmeldeanfragen	Die Anmeldung mit SSO unterstützt derzeit nicht SLO. Diese Option ist für zukünftige Entwicklungen geplant.
Möchte Authentifizierungsanfragen signiert haben	Ob AD FS erwartet, dass SAML-Anfragen signiert werden.

Note

Bei der Ausstellung des X509-Zertifikats, machen Sie eine Notiz vom Ablaufdatum. Zertifikate müssen erneuert werden, um jegliche Unterbrechungen im Dienst für SSO-Endbenutzer zu verhindern. Wenn ein Zertifikat abgelaufen ist, können sich Administrator- und Eigentümer-Konten immer mit E-Mail-Adresse und Master-Passwort anmelden.

Wenn Sie mit der Konfiguration des Identitätsanbieters fertig sind, **speichern** Sie Ihre Arbeit.

 Tip

Sie können Benutzer dazu auffordern, sich mit SSO anzumelden, indem Sie die Richtlinie für die Authentifizierung mit Single Sign-On aktivieren. Bitte beachten Sie, dass dies auch die Aktivierung der Einzelorganisation-Richtlinie erfordern wird. [Erfahren Sie mehr.](#)

Testen Sie die Konfiguration

Sobald Ihre Konfiguration abgeschlossen ist, testen Sie diese, indem Sie zu <https://vault.bitwarden.com> navigieren, Ihre E-Mail-Adresse eingeben, **Weiter** auswählen und den **Enterprise Single-On** Knopf auswählen:



Log in to Bitwarden

Email address (required)

☒ Remember email

Continue

or

 Log in with passkey

 Use single sign-on

New to Bitwarden? [Create account](#)

Unternehmens Single Sign On und Master-Passwort

Geben Sie die [konfigurierte Organisationskennung](#) ein und wählen Sie **Anmelden**. Wenn Ihre Implementierung erfolgreich konfiguriert ist, werden Sie zum AD FS SSO Zugangsdaten-Bildschirm weitergeleitet. Nachdem Sie sich mit Ihren AD FS-Anmeldeinformationen authentifiziert haben, geben Sie Ihr Bitwarden Master-Passwort ein, um Ihren Tresor zu entschlüsseln!

Note

Bitwarden unterstützt keine unaufgeforderten Antworten, daher führt das Initiieren von Zugangsdaten von Ihrem IdP zu einem Fehler. Der SSO-Zugangsdaten-Fluss muss von Bitwarden aus initiiert werden.