OneSpan Sign

SAML Administrator's Guide

Date: February 15, 2019

Version: OneSpan Sign 7

Copyright Notices

Trademarks

Intellectual Property

Disclaimer

OneSpan accepts no liability for the accuracy, completeness, or timeliness of content, or for the reliability of links to and content of external or third party websites or materials.

OneSpan shall have no liability under any circumstances for any loss, damage, or expense incurred by you, your company, or any third party arising from the use or inability to use OneSpan Software or Materials, or any third party material made available or downloadable. OneSpan will not be liable in relation to any loss/damage caused by modification of these Legal Notices or content.

Reservation

OneSpan reserves the right to modify these Notices and the content at any time. OneSpan likewise reserves the right to withdraw or revoke consent or otherwise prohibit use of the OneSpan Software or Materials if such use does not conform to the terms of any written agreement between OneSpan and you, or other applicable terms that OneSpan publishes from time to time.

Contact us

Phone: 1-855-MYESIGN
e-Mail: sign.support@onespan.com
Customer Support: https://www.esignlive.com/customer-support
Resource center: https://www.esignlive.com/resource-center
Company Website: https://www.onespan.com

Date: February 15, 2019

CONTENTS

1 Introduction

The product called OneSpan Sign provides a complete e-signature platform for the Web, including preparing, distributing, reviewing, signing, and downloading documents.

SAML (*Security Assertion Markup Language*) is a format for exchanging authentication and authorization data between an Identity Provider and a Service Provider.

To facilitate integration with third-party applications that provide Web SSO (*Single Sign-On*), OneSpan Sign supports the SAML 2.0 protocol. By performing the procedures listed below, you can:

- Enable "senders" (members of an OneSpan Sign account) to log in to OneSpan Sign using SSO via SAML 2.0 tokens.
- Enable "recipients" (not members of an OneSpan Sign account) to access the Signing Ceremony using SSO via SAML 2.0 tokens.

SAML logins to OneSpan Sign enable:

- A better User Experience, since users are logged in to OneSpan Sign transparently
- No need for the user to remember a password to log in
- Less time spent re-entering a password
- The option of automatically creating a new sender for the OneSpan Sign account upon a user's very first login to OneSpan Sign

- Reduced IT costs (via centrally-managed accounts and credentials)
- "Recipients" to access the Signing Ceremony in a more secure manner

Enabling a SAML login to OneSpan Sign generally entails successively performing the following procedures:

1. Getting Started
2. Configuring Your Identity Provider
3. Configuring SAML on Your eSignLive Account
4. Testing Your SSO Functionality

> **NOTE:** The protocol binding for SAML 2.0 is `HTTP-Redirect` and `HTTP-POST`.

2 Getting Started

The following sections contain information that is relevant to getting started with SAML on OneSpan Sign:

2.1 Configuring One or More Accounts for Senders

> **NOTE:** This section is relevant only if you want to configure SSO for "senders" (members of an OneSpan Sign account).

One of the following topics applies to your situation:

- Configuring a Single Account on page 4
- Configuring Multiple Accounts on page 4

2.1.1 Configuring a Single Account

OneSpan Sign has a setting for single accounts, called *Sender Auto Provisioning* . This feature is enabled by default.

If this feature is enabled, the first time a sender tries to log in via SSO, OneSpan Sign will create an account for them, and will give them access to OneSpan Sign's User Interface for senders.

If this feature is disabled, an organization must manually add a sender to a OneSpan Sign account before they can log in via SSO.

2.1.2 Configuring Multiple Accounts

Optionally, multiple OneSpan Sign accounts can be configured to use the same Identity Provider for SSO.

> **CAUTION:** This approach does not support the *Sender Auto Provisioning* feature described above. Thus senders must be *manually* added to accounts.

> **TIP:** Senders can be provisioned programmatically via OneSpan Sign's REST API or SDK, without the senders receiving notifications to sign up for an account. For help with this, please contact Technical Support (sign.support@onespan.com; 1-855-MYESIGN).

2.2 Optional Account Settings for Senders

> **NOTE:** This section is relevant only if you want to configure SSO for "senders" (members of an OneSpan Sign account).

The following optional SSO-related settings can be configured at the account level:

- Force SSO Login on page 5
- Custom Redirection URLs on page 5
- Sender Email Templates on page 6

2.2.1 Force SSO Login

To force the senders on an account to log in to OneSpan Sign via SSO, use *OneSpan Sign BackOffice* to enable **SSO login** at the account level.

This setting will block users from accessing OneSpan Sign via its *Login* page.

2.2.2 Custom Redirection URLs

In response to certain events, OneSpan Sign by default redirects users back to OneSpan Sign's main *Login* page.

This may be undesirable when using SSO, since a typical user will not have a *username* or *password* for that page (instead they use an SSO login URL).

The best practice is to override these redirection URLs. Thus you should provide URLs of your choice for the following:

URL	Definition
Handover URL	For more information, see Handover URLs.
Session timeout for sender	Senders will be redirected to this URL when their session times out.
Sender logout	Senders will be redirected to this URL when they log out of the OneSpan Sign application.
Session timeout for signer	Signers will be redirected to this URL when their session times out.

2.2.3 Sender Email Templates

OneSpan Sign's SAML feature has email templates that can be used to send email notifications to senders under the following conditions:.

- Forgot your password
- Opt out
- Decline
- Account invitation
- Expire
- Bounced
- Complaint
- Out of the office
- Reassign sender
- Ready to complete
- Lock signer
- Login lockout
- KBA failure

CAUTION: The above email templates contain the variable `$LINK_URL;`, which redirects senders to OneSpan Sign's *Login* page. Instead, you will want to redirect senders to the SSO URL. To arrange this, please contact Technical Support (sign.support@onespan.com; 1-855-MYESIGN). Note: Switching to the SSO URL prevents senders from using the *Forgot Password* link on OneSpan Sign's main page.

NOTE: The *Account invitation* email will not be sent to senders if they are auto-provisioned upon SSO login (see Configuring a Single Account on page 4), or if they are provisioned via the REST API or SDK.

2.3 Configuring SSO for Recipients

> **NOTE:** This section is relevant only if you want to configure SSO for "recipients" (not members of an OneSpan Sign account).

For a given transaction, SSO authentication can be assigned to one or more "recipients" in either of the following ways:

- Configuring SSO via the New User Experience
- Configuring SSO via the SDK and REST API

3 Configuring Your Identity Provider

Many organizations can serve as your Identity Provider for SAML.

The following sections describe how to configure two such providers:

- Configuring ADFS for SAML
- Configuring OKTA for SAML

No matter which Identity Provider you use, you should do the following:.

1. Set the **Signature algorithm name for SAML** to **SHA1withRSA**.
2. On your Identity Provider, configure the following Attribute Mappings (OneSpan Sign will use them to identify the user who is logging in):

User	Attributes
email	One of the following: • email • emailaddress • mail
first name	One of the following: • firstname • givenname • cn

User	Attributes
last name	One of the following: • lastname • surname • sn

NOTE: If you want to configure an Identity Provider only for "recipients" (not members of an OneSpan Sign account), specify only the parameter *email*. You don't need to specify a *first name* or *last name* .

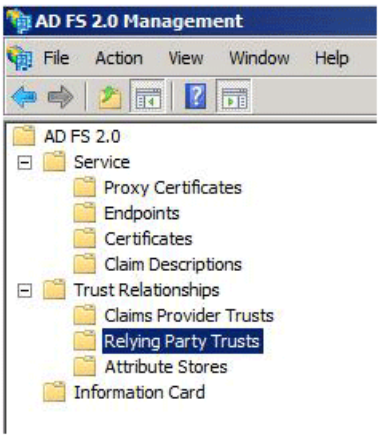
TIP: If you need to import the required metadata into your keystore, see SAML Metadata on page 17

3.1 Configuring ADFS for SAML

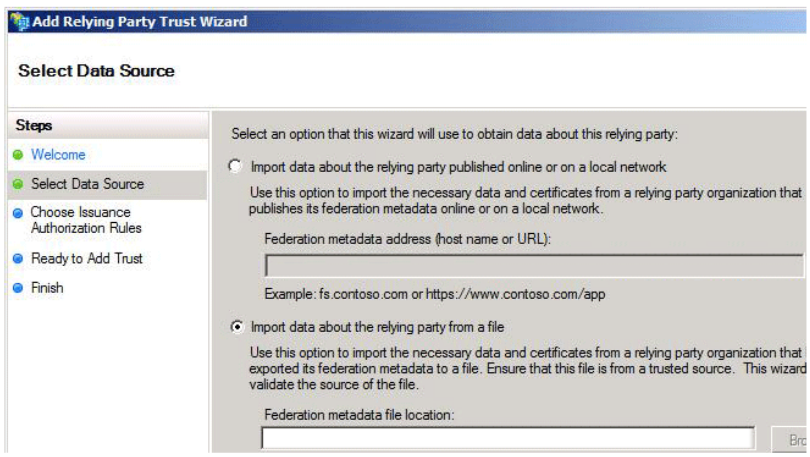
Microsoft's *Active Directory Federation Services* **(ADFS) can serve as a SAML 2.0 Identity Provider for OneSpan Sign.**

To configure ADFS to serve as a SAML Identity Provider for OneSpan Sign:

1. Start the ADFS 2.0 *Management Console*.
2. Open the **Trust Relationships** folder, and right-click **Relying Party Trusts**.



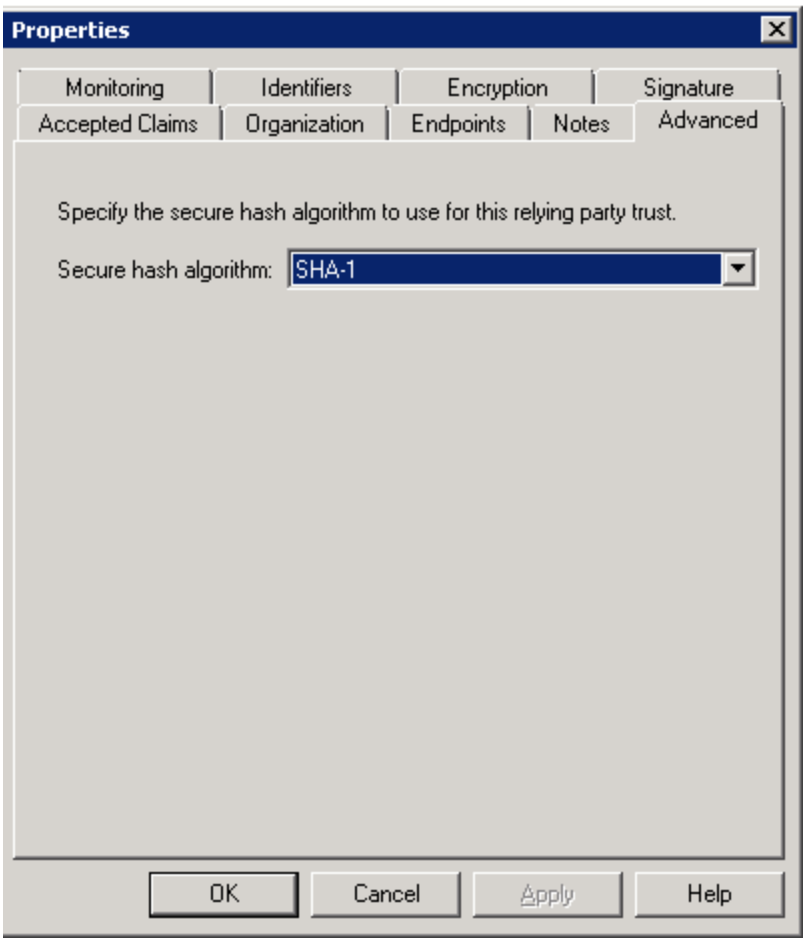
3. Select **Add Relying Party Trust**, and then **Start**.
4. In the *Add Relying Party Trust* wizard, select **Import data about the relying party from a file**.



5. Import the required metadata into your keystore. To download it, see SAML Metadata on page 17.

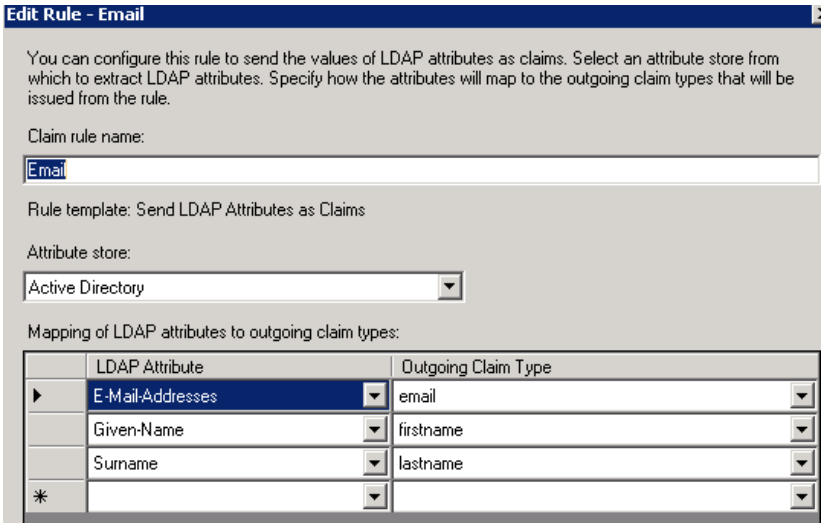
6. Complete the wizard as necessary, entering your **Display Name**, and the **Authorization Rules** you want to use.

7. On the *Advanced* tab, change the *Secure hash algorithm* to **SHA-1**.

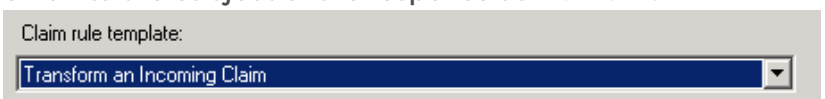


8. Create new **Claims Rule for LDAP Attributes** using the following template:

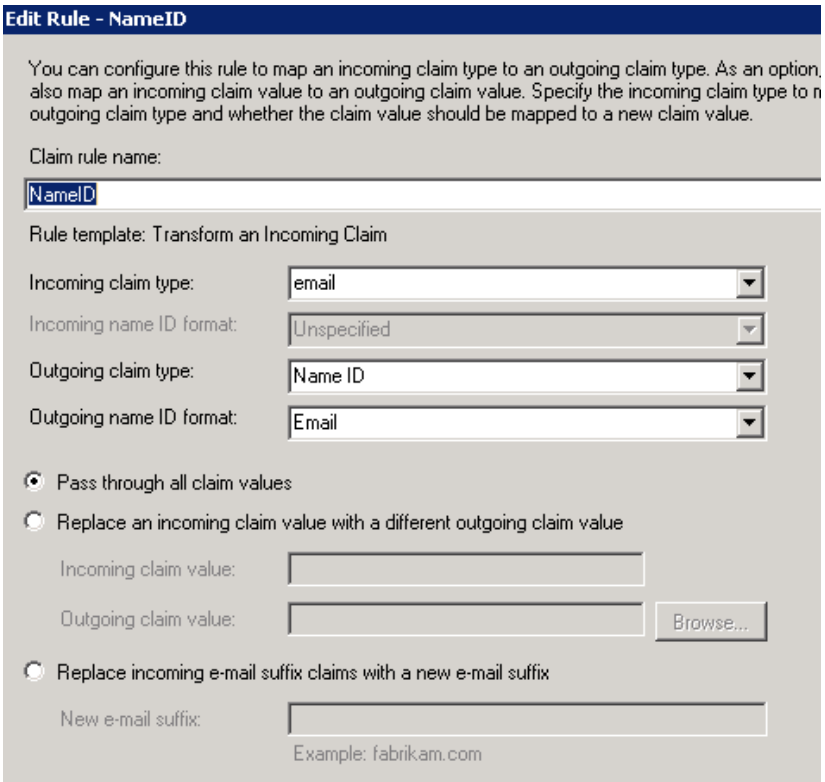
9. Edit the rule so your screen looks as follows:



10. Create another Claims Rule to **Transform an Incoming Claim**. This will add email to the Subject of the response as *NameID*.



11. This Claim Rule will reference the first Claim Rule. For this reason, the latter must remain *Rule 1*.


Edit Rule - NameID
You can configure this rule to map an incoming claim type to an outgoing claim type. As an option
also map an incoming claim value to an outgoing claim value. Specify the incoming claim type to m
outgoing claim type and whether the claim value should be mapped to a new claim value.
Claim rule name:
NameID
Rule template: Transform an Incoming Claim
Incoming claim type:
email
Incoming name ID format:
Unspecified
Outgoing claim type:
Name ID
Outgoing name ID format:
Email
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

3.2 Configuring OKTA for SAML

OKTA (https://www.okta.com) can serve as a SAML Identity Provider for OneSpan Sign.

> **NOTE:** The following example configures OKTA as the Identity Provider for an eSignLive *US Sandbox* instance.

To configure OKTA to serve as a SAML Identity Provider for eSignLive:

1. Navigate to https://www.okta.com/developer/signup/, and create a free OKTA *Developer Edition* organization.
2. Log in to the Admin Console, and click **Add Applications**.
3. Click **Create New App**, and select **SAML 2.0** as the *Sign On Method*.
4. In the *General Settings* section, enter an **App** name. Then click **Next**.
5. In the *Configure SAML* section, paste the following URL into the **Single sign on URL** fields:

   `https://sandbox.e-signlive.com/sso/saml/SSO/alias/e-signlive`

> **NOTE:** Keep the recipient URL and destination URL the same.

6. In the **Audience Restriction** field, enter the **SP entity ID**. For example: `urn:saml:sso:sandbox:e-signlive:com`.
7. For the default **relay state value**, enter `https://sandbox.e-signlive.com/packages/inbox`
8. Click **Show Advanced Settings**, and configure the settings in the following table:

SETTING	VALUE
Name ID format	EmailAddress
Response	Signed
Assertion Signature	Unsigned
Signature Algorithm	RSA_SHA1
Digest Algorithm	SHA1
Assertion Encryption	Unencrypted
SAML Single Logout	Disabled
authContextClassRef	Unspecified
Honor Force Authentic-ation	No
SAML Issuer ID	http://www.okta.com/${org.externalKey}

9. In the *Attribute Statements* section, add the following three attribute statements, and then click **Next**:

Name	Name Format	Value
email	URI Reference	user.email
firstname	URI Reference	user.FirstName
lastname	URI Reference	user.lastName

10. In the *Feedback* section, select **This is an internal application that we created**. Then click **Finish**.

    You will now see the *Sign On* section of your newly created *Example SAML Application*. Keep this page open in a separate browser tab or window. You will need its *Identity Provider* metadata link when you perform the procedure Configuring SAML on Your eSignLive Account.

    > **TIP:** To copy the Identity Provider metadata link, right-click it and select **Copy**.

11. Right-click the **People** section of the **Name** of your application, and select **Open Link In New Tab** (so you can come back to the *Sign On* section later).

12. In the new tab that opens, click the **Assign Application** button.

13. A dialog box called *Assign name of Application to up to 500 people* **appears.** Type your **username** in the search box, and select the check box next to your username. Then click **Next**.

14. You will be prompted to enter user-specific attributes. Click **Confirm Assignments** to keep the defaults.

> **TIP:** You are now ready to perform the procedure Configuring SAML on Your eSignLive Account. You will need the *Identity Provider* metadata link from Step 10.

3.3 SAML Metadata

One of the following links to OneSpan Sign metadata may be required when you configure your Identity Provider:

- apps.e-signlive.ca
- apps.esignlive.com.au
- apps.esignlive.com
- apps.e-signlive.com
- apps.esignlive.eu
- sandbox.e-signlive.ca
- sandbox.esignlive.com
- sandbox.e-signlive.com

4 Configuring SAML on Your OneSpan Sign Account

To configure SAML on your OneSpan Sign account:

1. For a "sender" (a member of an OneSpan Sign account), complete the configuration of your Identity Provider, and gather the following information:
   - The email address of the OneSpan Sign account on which SSO will be configured
   - The Identity Provider's metadata – This will be a *SAML metadata URL*, or a *metadata XML file*.
   - The Identity Provider's *Entity ID*
   - The Identity Provider's Public Certificate

> **NOTE:** OneSpan Sign supports importing metadata from an XML file to accommodate organizations whose Identity Provider's SAML metadata is not exposed on the web due to security concerns.

2. For a "recipient" (not a member of an OneSpan Sign account), complete the configuration of your Identity Provider, and gather the following information:
   - The email address of the OneSpan Sign account on which SSO will be configured
   - The Identity Provider's metadata – This will be a *SAML metadata URL*, or a *metadata XML file*.

- The Identity Provider's *Entity ID*
- The Identity Provider's Public Certificate
- The Identity Provider's URL

3. Contact Technical Support (sign.support@onespan.com; 1-855-MYESIGN), and give them the Identity Provider information gathered in the previous step.
4. Technical Support will give you up-to-date configuration information that includes:
   - OneSpan Sign metadata (to download that data, see SAML Metadata on page 17)
   - An *Entity ID*
   - An SP consumer end-point URL (e.g,, https://sandbox.e-signlive.ca/s-so/saml/SSO/alias/e-signlive)
5. Use the information from the previous step to reconfigure your Identity Provider.

5 Testing Your SSO Functionality

NOTE: This section describes only how to test SSO functionality for "senders" (members of an OneSpan Sign account). Testing SSO functionality for "recipients" (not members of an OneSpan Sign account) is more complex, since it requires creating an OneSpan Sign transaction.

Once your configurations are complete, you can use either your *SP URL* (obtained from OneSpan Sign) or the *Identity Provider URL* (obtained from your Identity Provider) to start a session and test your SSO functionality.

To test your SSO functionality:

1. Navigate to the *SSO URL* (either the *SP URL*, or the *Identity Provider URL*). You should be redirected to the Identity Provider server's *Login* page.

   Your *SP URL* should look something like this:

   ```
   https://
   {
   server:por
   t}/sso/saml/login/alias/eSignLive?idp=
   {Entity ID of the Identity Provider}
   ```

   The following example *SP URL* is from our U.S. Production environment:

   ```
   https://apps.eSignLive.com/sso/saml/log
   in/alias/eSignLive?idp={Entity ID of the
   Identity Provider}
   ```

2. Log in with your Identity Provider server credentials (SSO credentials). You should be redirected to OneSpan Sign's *Inbox*. Once that happens, you have successfully logged into OneSpan Sign using SSO via SAML 2.0 tokens.