DocuSign Single Sign On Implementation Guide

Published: June 8, 2016

Copyright

Table of Contents

DocuSign Single Sign On Overview

Single Sign On, also known as Federation, provides a secure way to exchange authentication information between two parties, a Service Provider and an organization's Identity Provider, allowing a single set of credentials to be used to access multiple applications. When an organization enables Single Sign On (SSO) for their DocuSign account, it allows members to use their organization's credentials to access DocuSign.

DocuSign allows administrators to manage users in a specific email domain. Suppose every user at an organization has an email address at the domain @myorganization.com. By proving ownership of myorganization.com, an administrator can manage the identity for DocuSign users on that email domain. For example, an organization can enable a security policy in DocuSign to require all users with their email address to authenticate with the corporate Identity Provider. This process is known as federation or SSO.

With SSO administrators can manage DocuSign users from their organization's Identity Provider. This streamlines the process of managing users by allowing the use of a central system for administration, provisioning new users, resetting passwords, changing logon policies, and deactivating users. For account users this is beneficial because it allows them to only need one user name and password for everything at work from computer, email, to DocuSign.

This guide provides information about setting up and managing SSO with your DocuSign account. The information in this guide is also available in the DocuSign Support Center.

Note: SSO only controls authentication and user access into DocuSign. It is not a replacement for setting user permissions. Administrators will still need to modify permissions through the DocuSign web application or DocuSign API.

Setting Up Single Sign On for Your Organization

Important: Single Sign On functionality is only supported in DocuSign Enterprise plans. Your account might not support this option. To access this functionality, contact your Account Manager.

This section provides a high-level overview that most organizations will follow to enable Single Sign On (SSO). Before setting up SSO, you should review the DocuSign Single Sign On Permissions for additional aspects that SSO administrators should consider when setting up SSO.

Note: These actions can only be taken by users who have been designated as the organization administrators. This is a special configuration that can only be enabled internally by DocuSign. Please contact your account manager to enable these privileges or change organization administrators.

The basic steps to setting up SSO for your organization:

Note: DocuSign recommends doing these steps in your Demo account first. Then, when successful, repeat the same steps in your Production account.

1. An organization must, first, prove ownership of the domain in order to manage it.

   During this step organization administrators follow the process in DocuSign Admin to create a reserved domain. Refer to Claim a Domain for the procedure and details for doing this.

2. Set up and configure an Identity Provider in DocuSign.

   In this step the organizational administrator provides SAML configuration to allow DocuSign to establish interoperability with the Identity Provider. Refer to Set up an Identity Provider for the procedure and details for doing this.

3. Test the SSO configuration with a select group of users.

   Before making SSO mandatory for all users in the organizations, you will test the SSO configuration with a small group of users to ensure SAML has been configured correctly. Refer to Testing an Identity Provider Configuration for the procedure and details on doing this.

4. Make SSO mandatory for all users.

   The final step is to make SSO mandatory. This requires all users on the domain to authenticate with the Identity Providers. Any pre-existing user names and passwords in DocuSign are no longer valid. Refer to the Change Domain Level Settings procedure to set the security options for your account.

Supported Protocols

DocuSign SSO currently supports the following SAML protocols:

- OASIS SAML 2.0 with HTTP POST binding

DocuSign Single Sign On Permissions

With a basic understanding of how Single Sign On (SSO) works, it's now important to reflect on the permissions and authorization rules that an organization may want to enforce. Such policies could change the way you configure DocuSign or the Identity Provider.

This section covers several aspects that SSO administrator should consider when setting up SSO.

DocuSign Access - Which users should have access to DocuSign?

Every DocuSign customer might have different preferences or policies regarding which users are allowed to access DocuSign. Some organizations might allow every user to have the ability to access DocuSign to send and receive documents. However, some customers only want to provision DocuSign for certain groups of users in the organization.

When using SSO, the limited access type of policy is configured within the Identity Provider. If a user tries to access DocuSign and they are not permitted to use DocuSign, then the Identity Provider should deny its access by rejecting the SAML authentication request for that user.

Checklist Item:

- □ Ensure your Identity Provider has been configured correctly. Either it allows access for all users or the Identity Provider is configured to restrict DocuSign access to specific security groups.

Login Policy - How do you want users to log in?

For SSO, most organizations require users to log on with their Identity Provider via SAML. In almost all cases, once SSO is turned on it replaces username/password as the method for the authentication. This makes any existing username/password combinations in DocuSign unusable.

However, there is an exception to this rule. There can be circumstances where certain users still retain a username/password within DocuSign that would be active even when SSO is enabled. Such scenarios could include giving the SSO administrator the ability to log on in the event that there is an SSO configuration problem or there might be a need for certain client integrations to have a username/password so it can work with DocuSign's APIs. In general, there is a way to provide an exception to the SSO policy for certain users. However, it should only be done for highly privileged users since it creates an exception to your SSO policies.

Checklist Item:

- □ Identify the users and integrations that might need the privilege of retaining a direct username/password log on into DocuSign.

Account Membership and Permissions

When a user logs on for the first time, they may not have an existing identity in DocuSign. For this case DocuSign will create a user in the system on the fly. This feature is called Just-In-Time Provisioning. Part of this process requires DocuSign to make a decision on which account the user should be a member of and the allowed permissions for that user.

There are two main patterns that can be implemented:

1. DocuSign internally configures a single default account and permissions set for any user that is created with Just In Time provisioning. After a user is created, they may be manually added to other accounts or given different permissions using DocuSign Admin or the DocuSign API.

   Pros:

   - This is the simplest method to configure SSO and requires no additional configuration in the Identity Provider.
   - Great for keeping users in a default account, until they can follow the organization's approval process to be given additional permissions or access to other accounts. This process would happen outside of SSO.

   Cons:

   - This means all users will start with the same account memberships and same set of permissions.

2. The Identity Provider specifies the account and permissions in the in the incoming SAML assertion when the user is created.

   Pros:

   - This provides greater flexibility, ensuring each user is specifically created in the appropriate account with appropriate permissions.
   - This can be tied to permission and security policies within your Identity Provider so that rules such as "People in HR, get added to the HR account" can be followed.

   Cons:

   - This requires custom configuration in your Identity Provider to specify the attributes and rules applied for each new user.
   - This is more complicated and harder to troubleshoot since policies are configured in a system outside of DocuSign's control.

Checklist Item:

□ Talk with application administrators about what configurations must be enforced to comply with the organization’s policies. It is likely that pattern #1 will be sufficient for most customers. As an organization’s adoption of DocuSign matures, the more sophisticated measures of pattern #2 can be implemented.

Domains

DocuSign allows organization administrators to reserve domains for use with DocuSign. This allows the system administrators to manage users for specific email domains. An organization can reserve multiple domains.

DocuSign verifies domain ownership before any organization can manage it.

To reserve a domain, the administrator adds the domain to their organization DocuSign Admin. DocuSign then generate a special token that must be added to the DNS record for the domain. Once DocuSign recognizes this token in the DNS entry, this confirms that the organization owns and operates the domain.

IMPORTANT: A domain can only be managed by one organization. If one organization has claimed and verified a domain, then another organization cannot claim or manage it.

From this page you can do the following:

- Reserve a domain
- Get a Token
- Withdraw a claim
- Change domain level settings

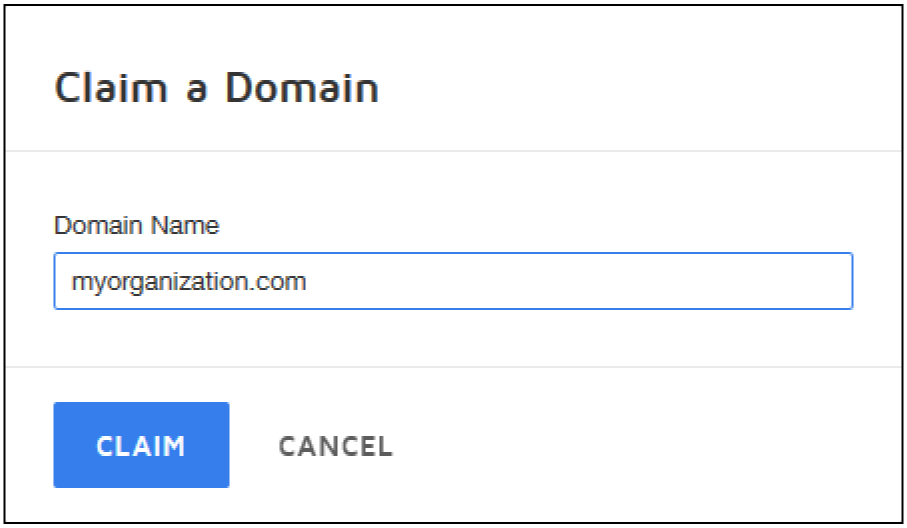
This topic also provides information on Setting User Login Policy.

Note: These options can only be modified by users who have been designated as the organization admin. This is a special configuration that can only be enabled internally by DocuSign. Please contact your account manager to acquire these privileges.

Reserve a Domain

Note: An organization can reserve multiple domains. DocuSign recommends that you repeat steps 2 – 6 of the following procedure for each domain, so you only need to update your DNS once (step 7) and can validate domains (step 8) at the same time.

1. In the DocuSign Admin application, click **Domains**.
2. Click **CLAIM DOMAIN**.



Claim a Domain

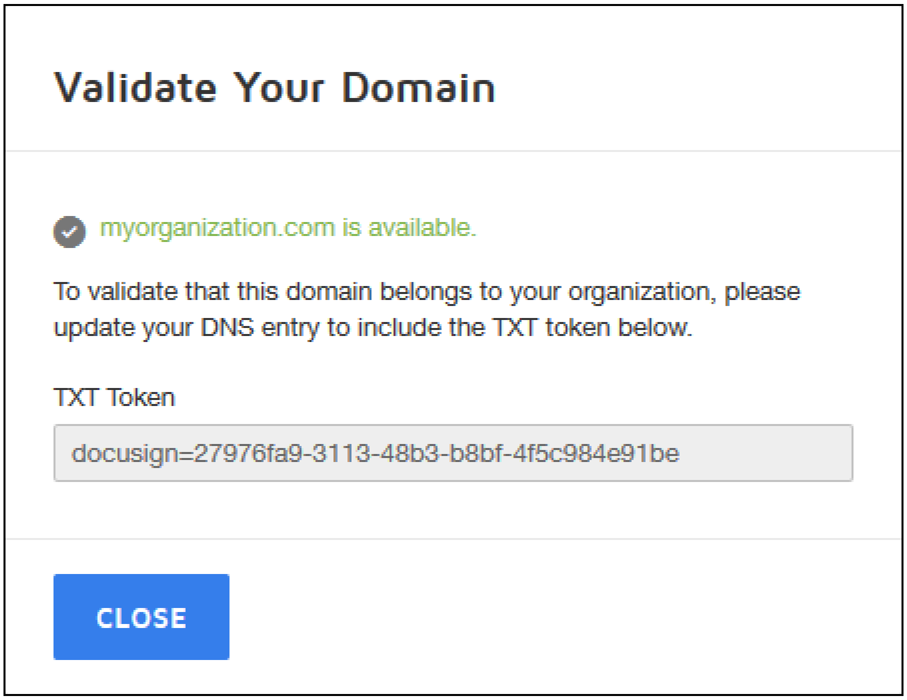
Domain Name

myorganization.com

3. Enter the Domain Name.
4. Click **CLAIM**.

   If the domain has already been verified by another organization, you must enter a different name. If you have questions about domain names, contact your account manager.

   If the domain is available, a TXT token is generated and shown in the dialog box. Continue to step 5.



Validate Your Domain

✓ myorganization.com is available.

To validate that this domain belongs to your organization, please update your DNS entry to include the TXT token below.

TXT Token

docusign=27976fa9-3113-48b3-b8bf-4f5c984e91be

5. Copy the generated TXT token so that it can be added to your domain's DNS entry.
6. Click **CLOSE**.
7. Outside of the DocuSign Admin application, update your domain's DNS entry to include the generated TXT token.

   The TXT token cannot be removed from the DNS record. DocuSign periodically checks the DNS to ensure claims are valid and removal of the TXT token would prevent your users from accessing DocuSign.

   > **Note:** The process of updating DNS records varies by vendor. You might need to coordinate with your network administrator in order to make this change. Also, it may take up to 72 hours for DNS changes to propagate over the Internet. Therefore coordinating ahead of time will ensure timely deployment of Single Sign On. As a sanity check, you check if the DNS change is active by opening command prompt in Windows and typing in this command:
   >
   > ```
   > nslookup -q=txt [myorganization.com]
   > ```
   >
   > Where *[myorganization.com]* is the domain you are checking.

8. Once the DNS change is active, return to the DocuSIgn Admin application and click **DOMAINS**.
9. Find the domain in the list, click **ACTIONS** on the same line as the domain name and select **Validate**.

   DocuSign checks to see if the generated token is part of the DNS entry. If successful the domain is marked with an active status.

   > **Note:** DocuSign periodically validates any pending domain claims. So it is possible that, after updating your DNS, your domain claim can become active in DocuSign even if you haven't clicked validate.

Get a Token

Use the following steps to .

1. In the DocuSign Admin application, click **Domains**.
2. In the list of domains, find the domain for which you want to get the token.

   Click **ACTIONS** on the same line as the domain name and select **Get Token**.
3. Copy the generated TXT token as needed.
4. Click **CLOSE**.

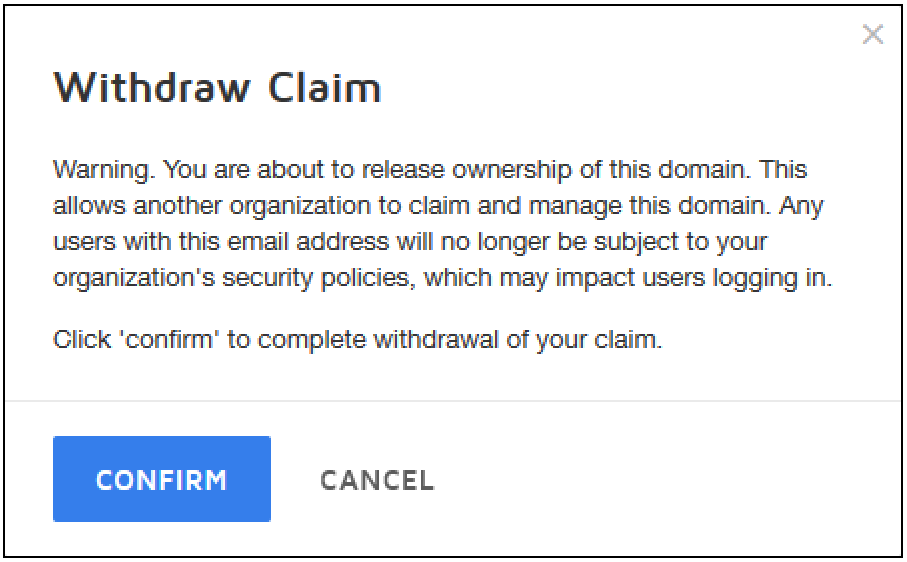
Withdraw a Domain Claim

You can relinquish control of a domain by withdrawing your domain claim. Releasing a domain removes any security policies and may prevent users from logging on to the DocuSign web application. This operation should only be reserved for cases where you are certain there are no active users with this email address.

IMPORTANT: There is no way to undo this change. Organizational administrators must be cautious about withdrawing any active domain claims.

1. In the DocuSign Admin application, click **Domains**.
2. In the list of domains, find the domain you want to relinquish.

   Click **ACTIONS** on the same line as the domain name and select **Withdraw Claim**.



Withdraw Claim

Warning. You are about to release ownership of this domain. This allows another organization to claim and manage this domain. Any users with this email address will no longer be subject to your organization's security policies, which may impact users logging in.

Click 'confirm' to complete withdrawal of your claim.

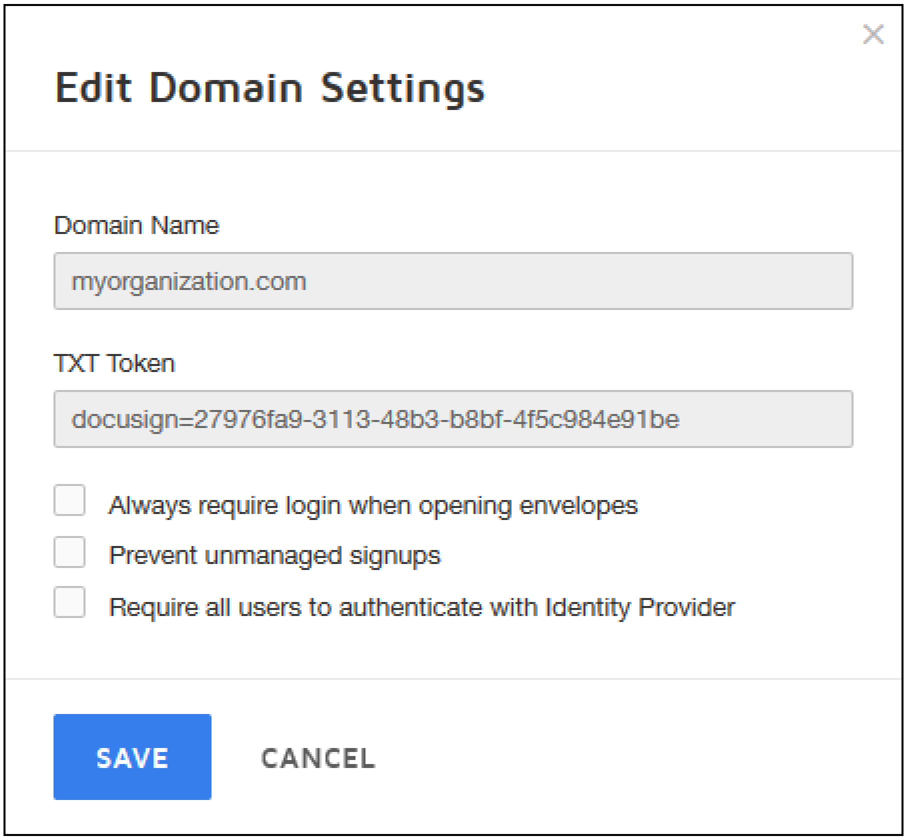
3. Click **CONFIRM** to withdraw your claim.

Change Domain Level Settings

Once a domain has been successfully validated you can modify the security settings for the domain.

1. In the DocuSign Admin application, click **Domains**.
2. In the list of domains, find the domain you want to modify.

   Click the domain name or click **ACTIONS** on the same line as the domain name and select **Edit**.
3. Select the security options you’d like to enable.



Edit Domain Settings

Domain Name

myorganization.com

TXT Token

docusign=27976fa9-3113-48b3-b8bf-4f5c984e91be

□ Always require login when opening envelopes

□ Prevent unmanaged signups

□ Require all users to authenticate with Identity Provider

Select the appropriate options for this domain:

- **Always require login when opening envelopes:** When a user with the email domain receives a document, they must first log on before they can open the document.
- **Prevent unmanaged signups:** This prevents users from using the self-serve sign up to register for a new DocuSign account using your domain. All users must either be created by the administrator or the Identity Provider.
- **Require all users to authenticate with identity provider:** All users are required to use the Company Login button to log on to the DocuSign web application with your organization's Identity Provider. Only enable this setting once you have added and tested an Identity Provider configuration, otherwise users may not be able to log on to DocuSign.

4. Click **SAVE** to save the changes.

Setting User Login Policy

When SSO is enabled for an organization, all account users follow the policy settings specified for the domain. For example, an organization's email domain is myorganization.com. If the organization administrator requires all users to authenticate with an Identity Provider, then all users with an @myorganization.com email address are required to authenticate with their corporate credentials.

There might be cases where using the default policy might not be appropriate for all users. Some examples of this are:

- The organization administrator might want to retain the ability to maintain a username and password in DocuSign. This is helpful for cases where the administrator needs to access DocuSign to make updates to the organization's SSO configuration going through the Identity Provider.
- An application or integration user cannot log in through an Identity Provider because that particular application does not currently support SSO.

For these cases, organization administrators have the option of setting login policies on a per user.

To change the login policy for users the organization administrator follows these steps:

Important: Only organization administrators can change the Login Policy for users. This setting deliberately overrides any policies that are enforced on the email domain and administrators should primarily use this as an exception rather than a standard rule for all users.

1. In the DocuSign Admin application, click **Users**.
2. Find the user that will bypass federation. Click the user name or click **ACTIONS** adjacent to the name and select **Edit**.
3. Select the **Logon Policy** option for the user. The available settings are:
   - **Default:** This setting uses the policies set for the user's email domain.
   - **Identity Provider or Username/Password:** This setting allows a user to maintain a username and password within DocuSign, even when SSO is required for all users in the domain.
   - **Identity Provider only:** This setting requires a user to log on with an Identity Provider when SSO is optional for users in the domain.
4. Click **SAVE** to save the change.

5. Reset the password for this user or instruct the user to request a password reset by clicking the link in the log in page.

Identity Providers

This page is used to manage Identity Providers for an account.

An Identity Provider (IdP) is an enterprise service that manages identity and provides identity information to Service Providers so that users can access applications. IdP's communicate with DocuSign via the SAML protocol and may optionally provide a set of claims which are used to map to various business functions at DocuSign.

Note: DocuSign Federation supports SAML 2.0 and all assertions must be sent with HTTP POST.

From this page you can do the following:

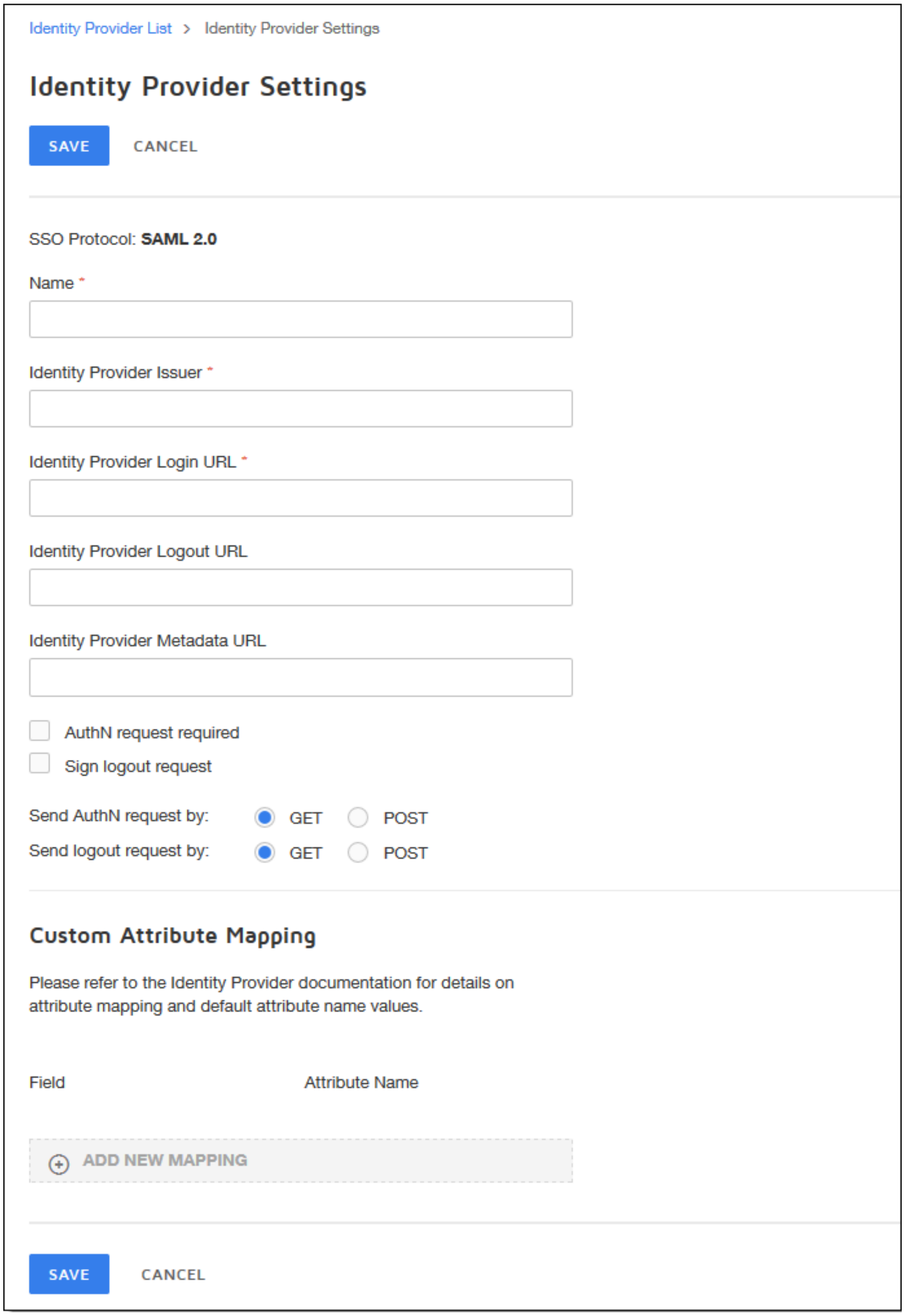
- Set up an Identity Provider
- Edit an Identity Provider
- Add or Update an Identity Provider Certificate

This topic also provides information on testing an Identity Provider configuration and the SAML specifications for Single Sign On.

Set Up an Identity Provider

Note: An organization must claim ownership of their email domain before setting up an Identity Provider. This is to ensure that only domain owners have the ability to change the authentication method for its users. Setting up a SAML configuration without claiming a domain will not result in any changes. See Domains for more information on claiming a domain.

1. In the DocuSign Admin application, click **Identity Providers**.
2. In the Identity Provider view, click **ADD IDENTITY PROVIDER**.



Identity Provider List > Identity Provider Settings

Identity Provider Settings

SAVE CANCEL

SSO Protocol: **SAML 2.0**

Name *

Identity Provider Issuer *

Identity Provider Login URL *

Identity Provider Logout URL

Identity Provider Metadata URL

□ AuthN request required

□ Sign logout request

Send AuthN request by: ● GET ○ POST

Send logout request by: ● GET ○ POST

Custom Attribute Mapping

Please refer to the Identity Provider documentation for details on attribute mapping and default attribute name values.

Field Attribute Name

⊕ ADD NEW MAPPING

SAVE CANCEL

3. Enter a Name. The name must be unique within the DocuSign system. The name is a label for this particular Identity Provider setting and has no impact on the other settings.
4. Enter the Identity Provider Issuer. This must match the issuer field in any SAML assertions.

5. Enter the Identity Provider Login URL. This is the endpoint that handles the SAML Authentication Request.
6. Optionally, enter the Identity Provider Logout URL.
7. Optionally, enter the Identity Provider Metadata URL.
8. Optionally, enable or disable the following settings as needed:
    - **AuthN request:** Select this option to require that DocuSign sign the AuthN request in SAML.
    - **Sign logout request:** Select this option to require that DocuSign send a logout request.
9. Select how the AuthN request and logout request are sent. They can be sent via a redirect (GET) or with HTTP POST.
10. Optionally, add any Custom Attribute Mapping.

    DocuSign requires an assertion to contain the NameID, email, first name, and last name of a user and can accept other optional fields (for more details, see the SAML Specifications). You can configure your Identity Provider to match the standard configuration in DocuSign or you can use the Custom Attribute Mapping to configure DocuSign to map those fields to other assertion attributes in your SAML response.

    - Click **ADD NEW MAPPING** to add a field.
    - Select the appropriate DocuSign Field and then type the Attribute Name that should be mapped to the field.
    - Click **ADD NEW MAPPING** to add another field, and then select the appropriate DocuSign Field and then type the Attribute Name that should be mapped to the field.
11. Upload at least one valid certificate used by the Identity Provider to sign SAML assertions.
12. Click **SAVE** to save the Identity Provider information.
13. Add the certificate for the Identity Provider.
14. Test the Identity Provider configuration.
15. Update your Domain level settings as needed.

    Once you have successfully configured your Identity Provider to work with your organization’s DocuSign account, there are additional security options you can set for your account.

    One security option is to enforce federated log on by requiring any user on your email domain to authenticate with Identity Provider. If a user tries to log on with a DocuSign password, an error indicates that the domain is federated and the user is required to use the Company Login button.

Refer to the Change Domain Level Settings procedure to set the security options for your account.

Edit an Identity Provider

1. In the DocuSign Admin application, click **Identity Providers**.
2. In the Identity Provider view, find the Identity Provider you want to modify.

   Click the Identity Provider name or click **ACTIONS** adjacent to the name and select **EDIT**.
3. Make the needed changes to the Identity Provider.
4. Click **SAVE** to save the changes.

Adding and Updating Certificates

1. In the DocuSign Admin application, click **Identity Providers**.
2. In the Identity Provider view, find the Identity Provider you want to modify.

   Click the Identity Provider name or click **ACTIONS** adjacent to the name you want to modify and select **Edit**.
3. In the Identity Provider Certificates section, click **Add Certificate**.
4. A dialog box opens, select the new certificate and click Open.
5. The certificate is added to the list of certificates.
6. Click **SAVE** to save the changes.

Testing an Identity Provider Configuration

Once you have successfully claimed a domain and configured an Identity Provider, you can test Single Sign On with your users. DocuSign recommends having a group of users test the configuration in demo and, after that is successful, switch to Production.

Instruct your users to do the following:

1. Go to the DocuSign log on page. The log on page used depends on the environment being tested.

   DocuSign Demo Environment: https://account-d.docusign.com

   DocuSign Production Environment: https://account.docusign.com
2. Click **Company Login**.
3. The user enters their email and clicks **Continue**.

DocuSign checks the email to determine the appropriate domain. The user is then redirected to the Identity Provider, via SAML, to complete the logon process.

After successfully authenticating, the user is taken to the appropriate account in the DocuSign web application.

For new users (users that have not been added to you r DocuSign account), DocuSign will provision them as a new user under your organization's default account; all of this happens automatically without any need for administrator action.

Note: DocuSign's just in time provisioning can be configured to create new users in a specific DocuSign account with a specific permission profile. Please consult with DocuSign Support to configure the provisioning settings correctly for your organization.

If the tests were successful for all claimed domains, then you can be sure that all users on your domains will be able to successfully log in with your Identity Provider configurations.

SAML Specifications

DocuSign requires the following SAML configuration in order for federation to work.

The list below shows the attributes that are required in your SAML assertions. If the attribute names are different than what has been specified, you can configure DocuSign to capture this data from other attributes in the assertion by mapping the attribute name. See To Set up an Identity Provider for more information on Custom Attribute Mapping.

NameId (Required): DocuSign requires a unique identifier for a user. This unique identifier must be immutable and cannot change for a user. In addition to that, this unique identifier cannot be recycled. An email address is not a recommended for use as an identifier, since a user can change emails or the email may be reissued. Instead, DocuSign recommends that customers either use the employee ID or some other unique identifier. A SAML example is provided below:

```
<saml:Subject>
  <saml:NameID>1234567890</saml:NameID>
  <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
  <saml:SubjectConfirmationDataRecipient="https://account.DSW004886.docusignh
q.com/saml2/login"/>
  </saml:SubjectConfirmation>
</saml:Subject>
```

Email Address (Required): The user's email address.

```
<saml:Attribute
Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
  <saml:AttributeValue>john.jones@mycompany.com</saml:AttributeValue>
</saml:Attribute>
```

First Name (Required): The user's first name.

```
<saml:Attribute
Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
<saml:AttributeValue>John</saml:AttributeValue>
</saml:Attribute>
```

Last Name (Required): The user’s last name.

```
<saml:Attribute
Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
<saml:AttributeValue>Jones</saml:AttributeValue>
</saml:Attribute>
```

AccountId (Optional): The DocuSign ID for the account associated with the user. If specified, this accountId will be used during just-in-time provisioning. This is the account that the user will be provisioned into when the user is created on first login. The accountId must be the account GUID format. This must be specified in conjunction with the PermissionProfileId below, otherwise login will fail.

```
<saml:Attribute
Name="http://schemas.account.docusign.com/ws/2015/09/identity/claims/accounti
d" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
  <saml:AttributeValue>bb151f08-c631-46c7-b2c2-
44a5dca243dd</saml:AttributeValue>
</saml:Attribute>
```

PermissionProfileId (Optional): The DocuSign ID of the Permission Set associated with the user. Permission Sets are sets of account permission settings that can be applied to individual users. Using this option allows new users to be assigned to a permission set when they are added to the account.

If specified, this is the permission profile that will be assigned to the user in the above account when the user is created on first login. This must be specified in conjunction with the AccountId above, otherwise login will fail.

```
<saml:Attribute
Name="http://schemas.account.docusign.com/ws/2015/09/identity/claims/permissi
onprofileid" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
  <saml:AttributeValue>1</saml:AttributeValue>
</saml:Attribute>
```