DocuSign

User Guide

DocuSign Admin for Organization Management

Published: March 04, 2022

Copyright

Table of Contents

Introduction to DocuSign Admin

This topic provides an introduction to DocuSign Admin, including the main capabilities and requirements, and how it can benefit your enterprise.

Note: To create an organization and set up single sign on (SSO), you must have DocuSign Admin enabled on your account. If you cannot follow the instructions provided in this guide, please contact DocuSign customer support for assistance.

What is DocuSign Admin?

DocuSign Admin is a management infrastructure that empowers you to control and manage how DocuSign is used by your company. Through centralized administrative tools, you can govern the use of DocuSign in an efficient and logical way, and control with confidence how the application is deployed at your company. DocuSign Admin changes the way you administer DocuSign by bringing together the accounts, users, and components necessary to support your workflows.

To learn how you can gain control of your company agreements with proven best practices and procedural guidelines, see Establish Control of your Company's DocuSign Agreements .

DocuSign Admin Capabilities

- View all of your accounts from a centralized location
- Self-service set up and management of your organization for identity management
- Administer just-in-time provisioning configurations
- Centralized user management
- Manage your organization’s administrative team

Requirements to Use DocuSign Admin

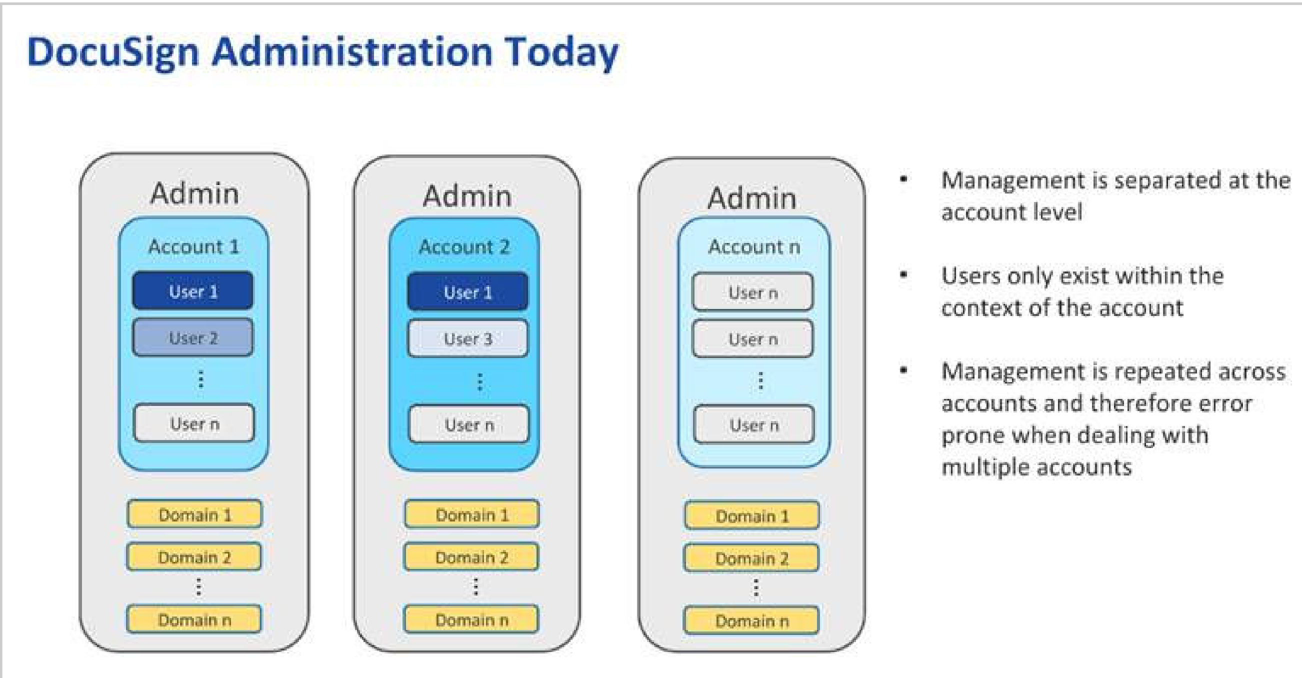
To use DocuSign Admin, your company must meet the following requirements:

- DocuSign Admin must be enabled on at least one account owned by your company. This requires the purchase of the appropriate package, Enterprise Pro with the Organization Management Add-On. From that account, any account administrator can create an organization.
- Any account that is managed or otherwise affected by DocuSign Admin and the customer’s use of the Enterprise Pro package must have the applicable plan enabled.

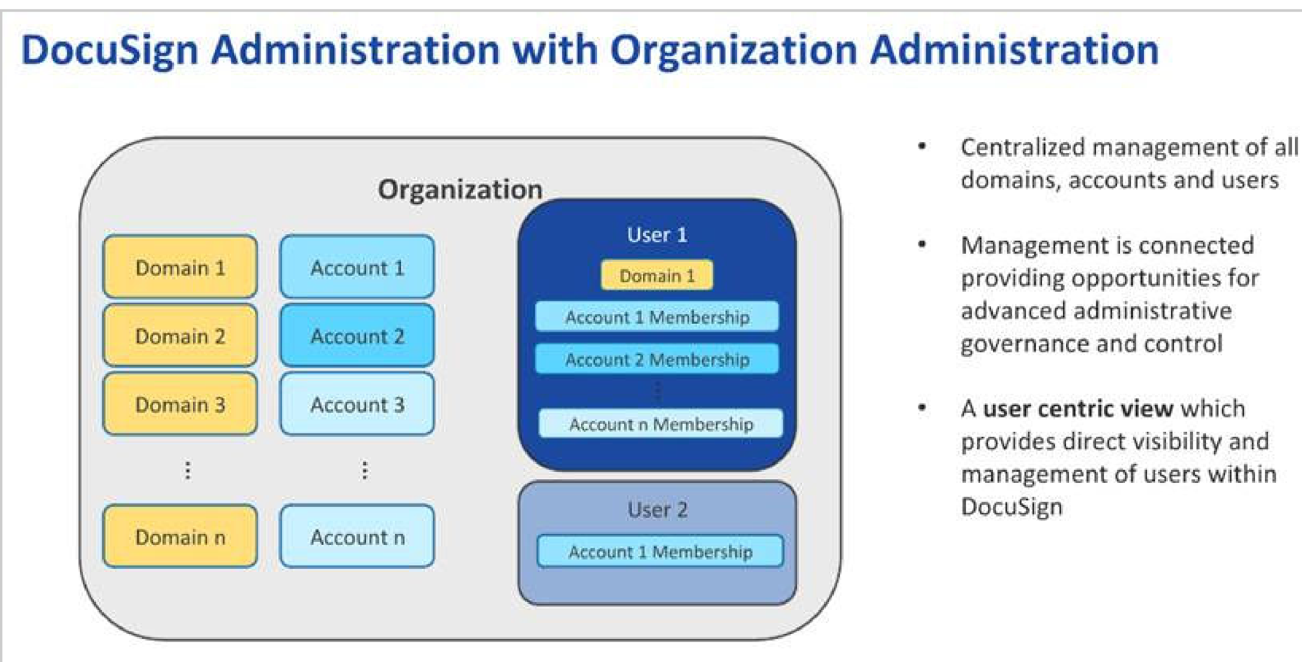
If you need assistance in securing the appropriate package and plan for your accounts, please contact DocuSign customer support.

Advantages of Centralized Management

A company with multiple DocuSign accounts must manage accounts and users from within each account. This siloed structure requires repeating configuration changes and user updates for all affected accounts, which can lead to errors and inconsistent implementation across the company.



With DocuSign Admin, your company gains instant visibility and control over domains and identity management (for SSO), accounts, and users from a centralized location. DocuSign Admin provides one place to manage your entire DocuSign implementation.



Getting Started

> **Note:** This guide is for DocuSign administrators who oversee multiple accounts. For administrators of individual accounts, see Welcome to Administration - DocuSign eSignature Admin.

To get started with DocuSign Admin, select the implementation plan that matches your company's situation.

Plan 1: Existing DocuSign Customer

Scenario: Your company has one or more active DocuSign accounts and access to DocuSign Admin.

Implementation Plan: Your organization is already set up and ready for you to explore.

- Access to an Organization: How to access the DocuSign Admin dashboard.
- Establish Control of your Company's DocuSign Agreements: Learn how you can gain control of your company's agreements with proven best practices and procedural guidelines.
- Domains: Manage email domains claimed for your organization.
- Identity Providers: Add and manage identity providers; edit the default account and permission profile used for just in time user provisioning.
- Accounts: See the accounts that are part of your organization and link additional accounts that you administer.
- Organization Administrators: Invite additional DocuSign users to be administrators for your organization.
- User Management: Manage users across multiple accounts and domains. Add and edit users, assign permission profiles and manage account access. Close users' account memberships.
- Connected Apps: Manage the applications that can access your DocuSign organization. Applications are authorized for all domain users and access is limited by the permissions you specify.

Plan 2: New DocuSign Customer

Scenario: Your company is new to DocuSign and will set up one or more active DocuSign Enterprise accounts and configure SSO. For visibility and control over your accounts and users, you will use DocuSign Admin.

Implementation Plan: You need to establish at least one DocuSign account with DocuSign Admin enabled on the account. Then you will create a DocuSign organization and set up SSO. From there, you will build out your organization, linking accounts to manage and adding DocuSign administrators to help you manage the organization and all of its users.

- Organizations: Create an organization from the DocuSign account with DocuSign Admin enabled. If not enabled, contact DocuSign customer support.
- Access to an Organization: How to access the DocuSign Admin dashboard.
- Establish Control of your Company's DocuSign Agreements: Learn how you can gain control of your company's agreements with proven best practices and procedural guidelines.
- DocuSign Single Sign-On Overview: Set up Single Sign-On (SSO):
    - Domains: Establish your email domain claims.
    - Identity Providers: Add your identity provider; edit the default account and permission profile used for just in time user provisioning.
    - Test SSO Configuration: Validate your SSO setup before enabling it for all domain users.
    - Change Domain Settings: Make SSO mandatory for all domain users.

  - Setting a User Login Policy: Set user login policy for individual users who need different access requirements.
- Accounts: Centralize management of your users by linking all corporate DocuSign accounts to your new organization.
- Organization Administrators: Invite additional DocuSign users to be administrators for your organization.
- User Management: Manage users across multiple accounts and domains. Add and edit users, assign permission profiles and manage account access. Close users' account memberships.
- Connected Apps: Manage the applications that can access your DocuSign organization. Applications are authorized for all domain users and access is limited by the permissions you specify.

Organizations

To create an organization you must be an eSignature account administrator with the All Administration Capabilities permissions. Also, the account you use to create the organization must be enabled with DocuSign Admin.

> **Note:** If you do not see the DocuSign Admin section in DocuSign eSignature Admin as shown in the procedure below, contact DocuSign customer support for assistance.

When you create an organization, you are automatically the administrator and the eSignature account used to create the organization is the default account. An organization's default account is used for just-in-time provisioning when new users are added.

After you create an organization, you can update the name and description at any time through the Overview tile.

For more information about creating an organization, see the following:

- Establish Control of your Company's DocuSign Agreements: Gain control of your company's agreements with proven best practices and procedural guidelines.
- Link accounts to an organization: Link accounts with DocuSign Admin.
- Default account for an organization: Manage the default account for just-in-time provisioning for new users.
- Access an organization: How to access your organization from the DocuSign eSignature Admin app and the DocuSign Admin dashboard.

Related information

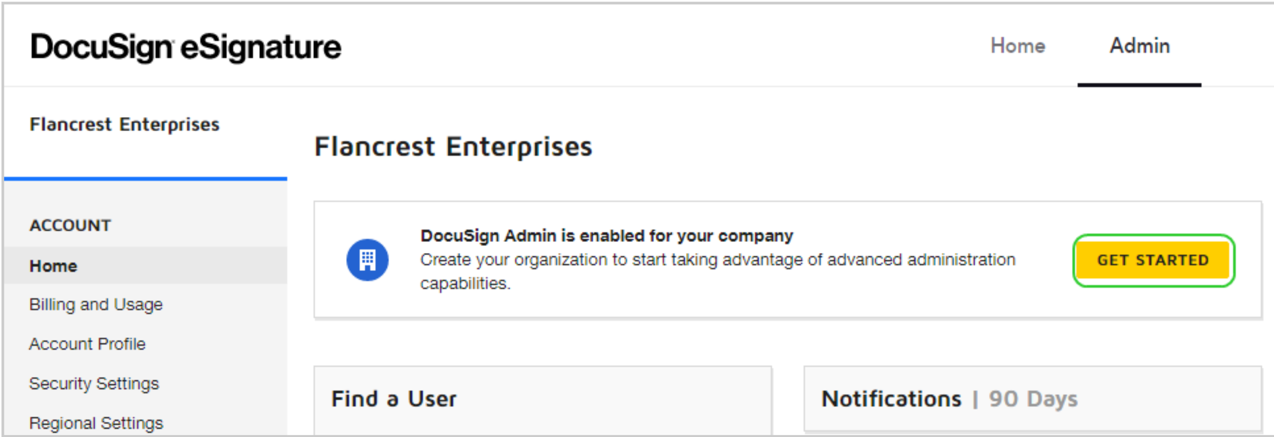
Create an Organization

Update an Organization Name or Description

Create an Organization

1. Log in to eSignature Admin for a DocuSign account that is enabled for DocuSign Admin.

2. From the eSignature Admin home page, click **GET STARTED**.

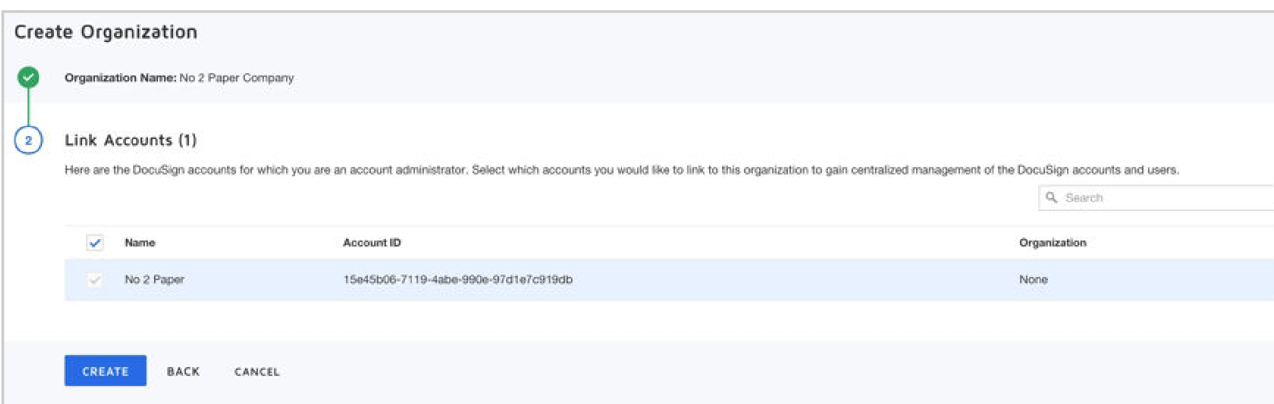


Note: If you do not see the **GET STARTED** section in your DocuSign account, then DocuSign Admin is not enabled on the account. Contact DocuSign customer support for assistance.

3. Enter an Organization Name and an optional Description in the fields provided, then click **NEXT**.

4. Link accounts to your organization. The account you used to create the organization is automatically linked. Select any additional accounts you and the other DocuSign administrators want to manage centrally through your organization.

All the accounts for which you are an account administrator with All Administration Capabilities permissions are listed. You can link additional accounts at any time. See Accounts.



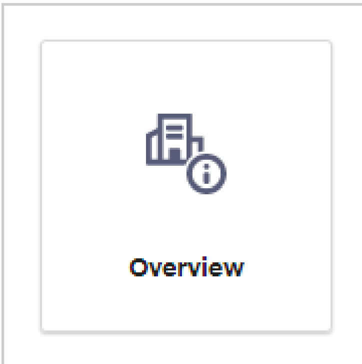
5. Click **CREATE** to finish creating your organization.

Your organization is created. The next time you log in to eSignature Admin, use the Admin Switcher to access the DocuSign Admin dashboard.

Update an Organization Name or Description

As a DocuSign administrator with the DocuSign Admin permission profile, you can update the organization name and description from the Overview tile.

1. From the DocuSign Admin dashboard, click the **Overview** tile.



2. On the Overview page, edit the Organization Name and Description fields.

3. Click **UPDATE**.

   Your organization profile details are updated.

Related Topics

For more information on topics related to creating an organization, see the following:

- Establish Control of your Company's DocuSign Agreements: Gain control of your company's agreements with proven best practices and procedural guidelines.
- Accounts: Link accounts with DocuSign Admin.
- Default Account and Just-in-Time Provisioning: Manage the default account for just-in-time provisioning for new users.
- Access to an Organization: How to access your organization from the DocuSign eSignature Admin app and the DocuSign Admin dashboard.

Access to an Organization

Once your organization is created, only the DocuSign users who have been added as DocuSign administrators and have activated their membership, can access and view the organization.

The main organization view is a dashboard that provides access to all other parts of the organization.

Note: See Establish Control of your Company's DocuSign Agreements to learn how you can gain control of your company's agreements with proven best practices and procedural guidelines.

Open the DocuSign Admin Dashboard

1. Log in to DocuSign eSignature as a DocuSign administrator.

2. Complete one of the following steps:

- From DocuSign eSignature, select the waffle menu in the upper left corner, and select **Admin**.
- From eSignature Admin, select **SWITCH TO...** in the upper left corner, and select **DOCUSIGN ADMIN**.

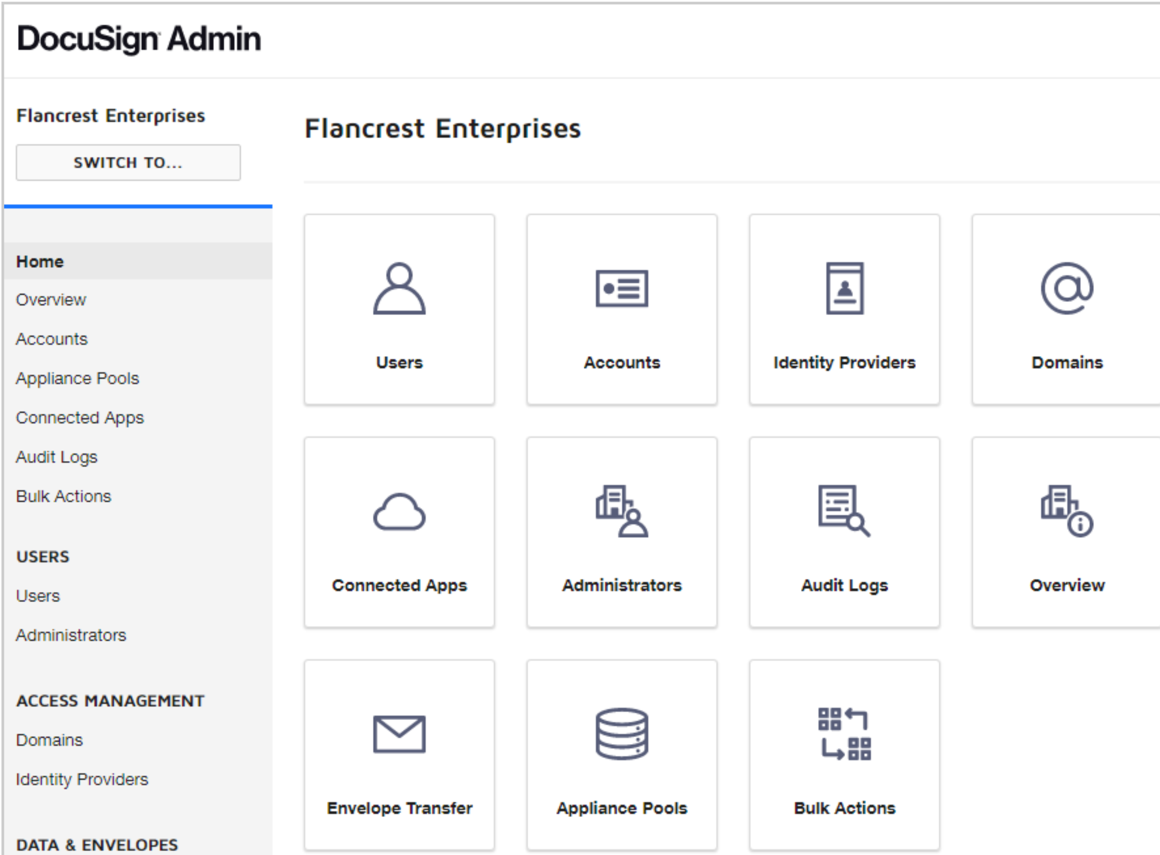
The organization dashboard appears.

The DocuSign Admin Dashboard

The dashboard provides access to all aspects of your organization.

- **To navigate to the different parts of your organization**, click on the dashboard tiles or use the left-hand navigation menu. For DocuSign administrators with the Administrator permission profile, the dashboard includes all available tiles. Delegated administrators will see tiles relevant to their permission profile. For more information on delegated administration, see Organization Administrators.

> **Note:** Your dashboard may differ depending on the features enabled for your organization. For more information, contact DocuSign Customer Support.



Troubleshooting

Why can't I access DocuSign Admin on all of my accounts within the organization?

This can happen if you are a member of accounts on more than one server environment (NA1, NA2, EU, AU, etc.).

If you can access DocuSign Admin on some, but not all of your associated accounts, or are unable to link an account for which you are an eSignature Administrator, follow these steps:

1. From the DocuSign Admin dashboard, click **Users**.
2. Enter your email address into the search bar, then click **SEARCH**.
3. From the user details page, click **EXTEND ORGANIZATION RIGHTS TO ALL MEMBERSHIPS**.
   All of your account memberships within the organization can now access DocuSign Admin.

Organization Features

As a DocuSign Administrator, you can manage the solutions and features available for your organization. Solutions are collections of related features aimed at solving specific business needs. For example, when a feature like user list exports is coupled with other related features, it enhances user management as a whole.

The organization overview displays a brief description for each solution and provides documentation for each feature. The organization features can also be viewed as a list, separate from their solutions. All changes made to features are tracked in the organization audit log.

Note: If a feature is marked as Not Available, contact your account management team to learn more.

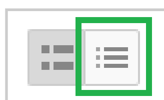
Enable or Disable Organization Features

If a feature is available for you organization, you can enable or disable it here. Changes made here will affect all DocuSign Administrators with the appropriate level of permissions. If you do not see the option to enable or disable features or features say 'Not Available,' contact DocuSign customer support assistance.

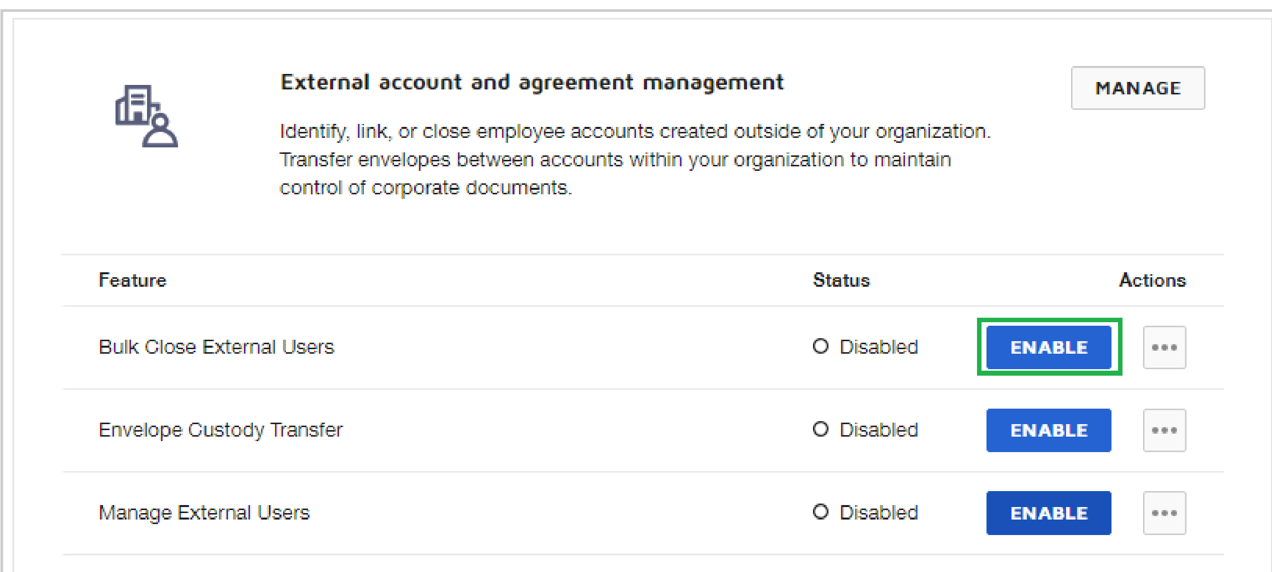
Note: Some organization features are related. Enabling or disabling a dependent feature will affect the related feature.

1. From the DocuSign Admin dashboard, click the **Overview** tile.

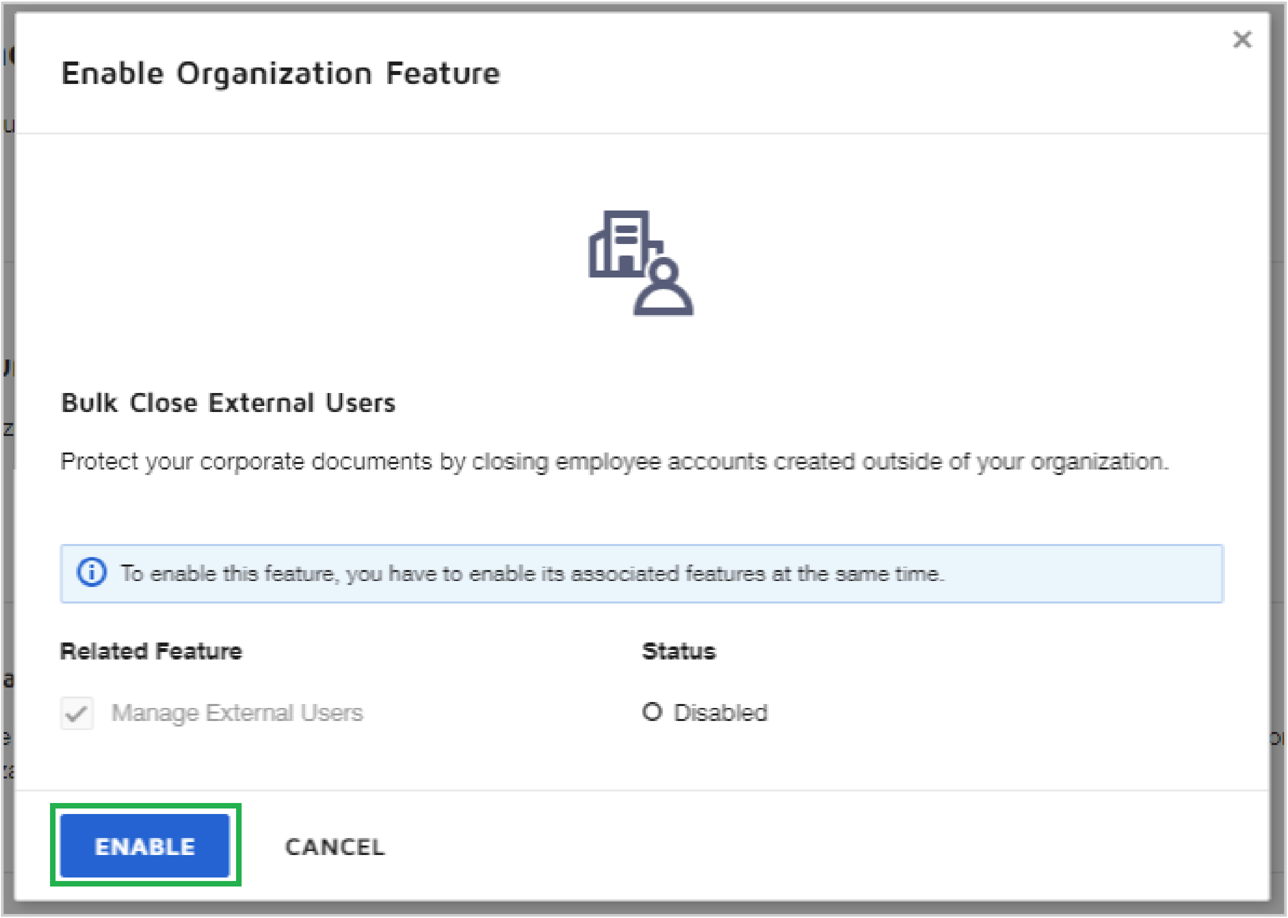
2. Locate the solution with a feature you'd like to enable and click **MANAGE**.

Note: Alternatively, click the list view button  to view individual features as a list.

3. Click **ENABLE**.



4. Click **ENABLE** to enable the feature.



> **Note:** If there is a dependent feature, you'll be prompted to enable that feature at the same time.

The feature is enabled for the organization.

5. To disable a feature, click the actions icon .

6. Click **Disable**.

> **Note:** If the option to disable does not appear, there is a dependent feature which must be disabled first. Disable the dependent feature to continue.

7. Click **DISABLE** again to disable the feature.

The feature is disabled for the organization.

DocuSign Single Sign-On Overview

Note: This guide is for DocuSign administrators. Single Sign-On requires DocuSign Admin.

With Single Sign-On (SSO), you can provision new users and enforce secure access management across all your corporate applications. SSO, also known as Federation, simplifies and secures user login, with just one password for all your SSO-enabled applications. With DocuSign Admin, you can set up and manage SSO at a global level to control all your DocuSign accounts.

SSO enables your company to manage access to DocuSign through an Identity Provider, such as Okta, Azure, Active Directory Federation Services, and OneLogin. With SSO, DocuSign users must use the Company Log In option. When they enter their domain email address, authentication is handled by an Identity Provider (IdP).

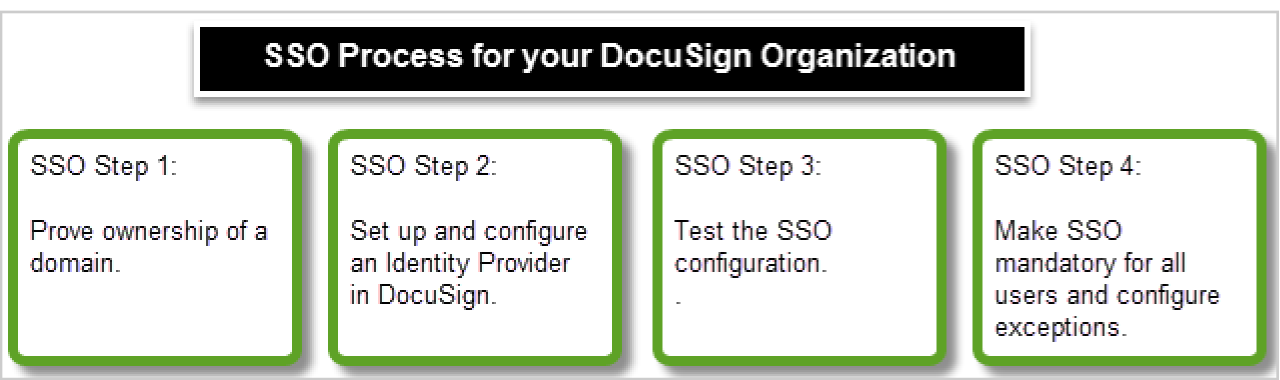
DocuSign Admin allows an administrator to manage users on their company's email domains. For example, suppose every user at a company has an email address at the domain @myorganization.com. By proving ownership of myorganization.com, an administrator can manage the identity for DocuSign users on that email domain. For example, a company can enable a security policy in a DocuSign organization to require all users with their email address to authenticate with the corporate Identity Provider.

Overview: Setting Up SSO for Your Organization

SSO functionality is managed through DocuSign Admin. In order to set up SSO, your company must already have created a DocuSign organization and you must be designated as an administrator with the DocuSign Administrator permission profile. To create a DocuSign organization, you must have an account that is enabled for this feature. If you cannot access the organization view from your DocuSign account, please contact DocuSign customer support for assistance.

Best Practice: DocuSign recommends setting up and testing SSO in a demo organization first. Then, when successful, repeat the steps in your production organization account.

Basic Steps to Setting up SSO for Your DocuSign Organization



1. **Prove ownership of a domain**.

   DocuSign administrators follow the process to claim and validate ownership of a reserved domain. See Domains.

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

   The DocuSign administrator provides SAML configuration to allow DocuSign to establish interoperability with the IdP. See Identity Providers.

3. **Test the SSO configuration**.

   Test the SSO configuration with a small group of users to ensure SAML is configured correctly. See Test SSO Configuration.

4. **Make SSO mandatory for all users and configure exceptions**.

   Make SSO mandatory to require all users on reserved domains to authenticate with the Identity Providers. Any pre-existing user names and passwords in DocuSign are no longer valid. See Change Domain Settings.

   For domain users or integration users who need to be able to log in without requiring IdP authentication, configure login policy exceptions on a per user basis. See Setting a User Login Policy.

Related Topics

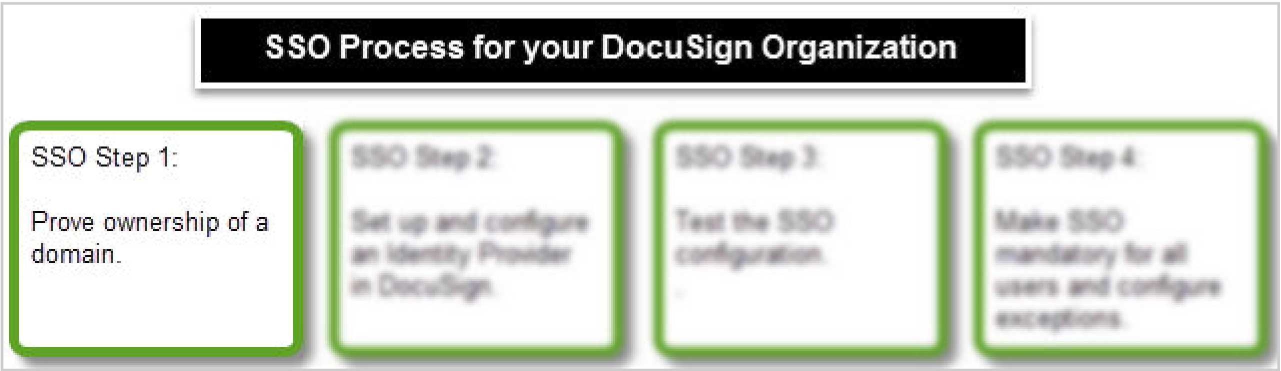
- Establish Control of your Company's DocuSign Agreements: Gain control of your company's agreements with proven best practices and procedural guidelines.
- Domains
- Identity Providers
- Setting a User Login Policy

Domains

> **Note:** This guide is for DocuSign administrators. Single Sign-On requires DocuSign Admin.

This section covers **Step 1** of the process to set up and enable SSO for your DocuSign organization and provides some supporting reference information about reserving domains. This step requires that you have already created your organization as described in creating an organization. An organization can claim the same domain in both the demo and production environments.

> **Note:** Claiming a domain is also part of the authorization process for connected applications. For more information, see Connected Apps.



Best Practice: DocuSign recommends setting up and testing SSO in a demo organization first. Then, when successful, repeat the steps in your production organization account.

As a DocuSign administrator, you can claim domains for use with DocuSign through the Domains page of your organization. When you claim and verify an email domain for your organization, you can manage all users for that domain, across all accounts linked to the organization.

You can restrict users from creating personal DocuSign accounts using an email address from a claimed domain. You can also grant administrative consent for connected applications on behalf of domain users.

Important: A domain can only be claimed by one DocuSign organization. If one organization has claimed and verified a domain, then another organization cannot claim it. An organization can claim the same domain in both the demo and production environments.

To start, you'll initiate a claim for your organization from the Domains page in DocuSign Admin. DocuSign then generates a special token that you add to the DNS (Domain Name System) for the domain. Once DocuSign verifies this token in the DNS, the domain is registered to the organization.

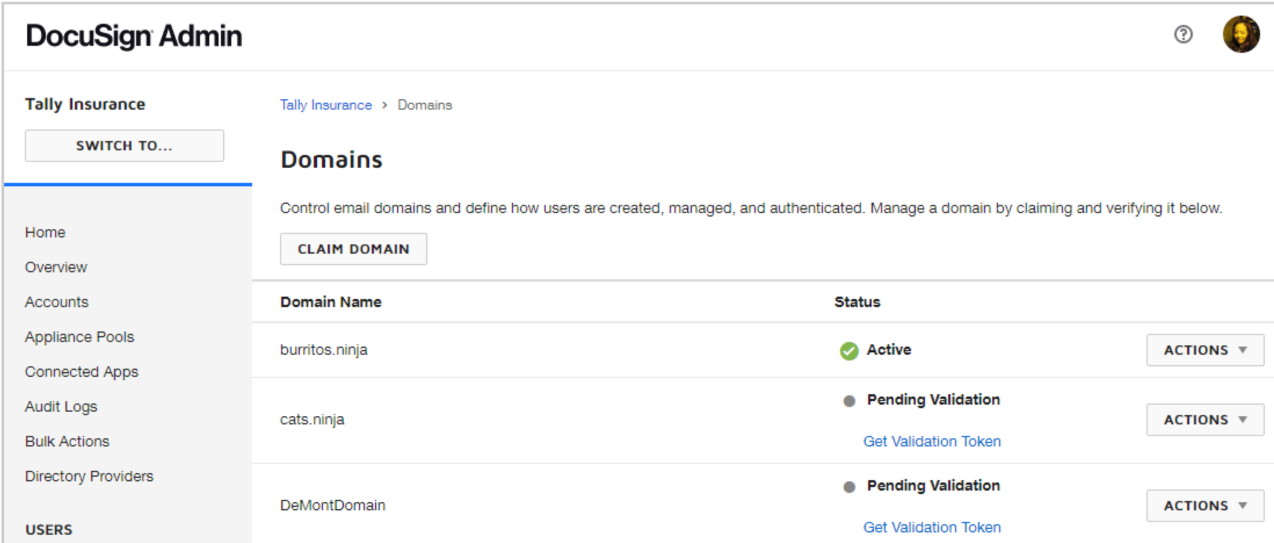
Note: You can choose to add a TXT record or a CNAME record to your domain's DNS. To ensure continuity of coverage, it is recommended to add both record types when claiming a domain.

CONTENTS

Prove Ownership of a Domain

1. In DocuSign Admin, click **Domains**.

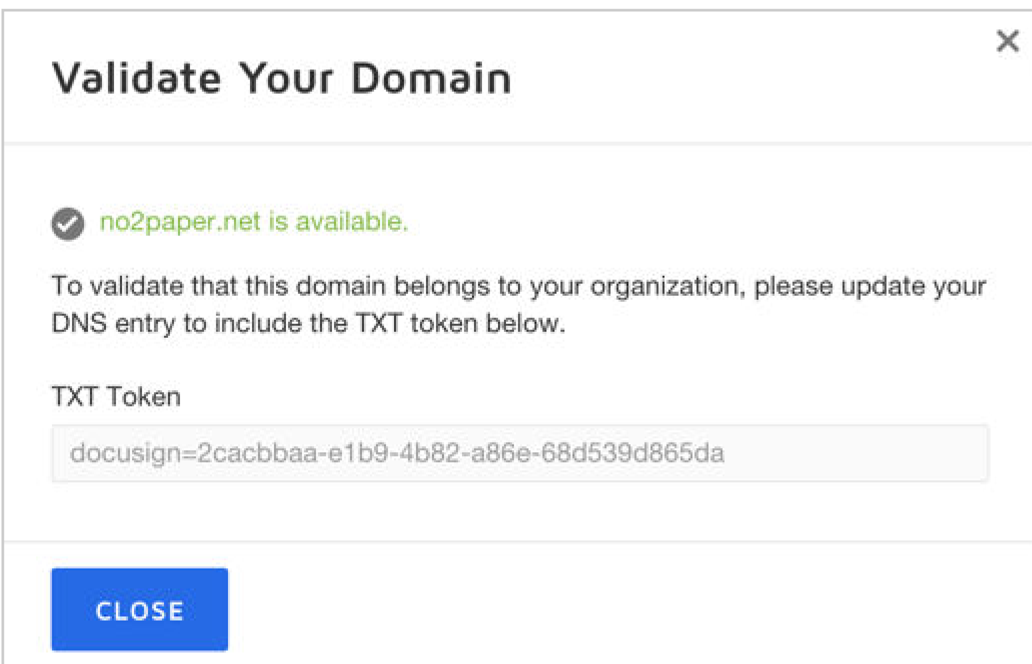
2. Click **CLAIM DOMAIN**.



3. Enter the Domain Name.

4. Click **CLAIM**.

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



5. Copy the generated TXT token so that it can be added to your domain's DNS entry.

6. Click **CLOSE**.

7. Outside of DocuSign Admin, update your domain's DNS entry to include the following:

To create a TXT record

a. Navigate to your domain's DNS record management page.

b. Add a new TXT record.

c. Name: @ or *

d. Text: TXT token from step 5 - Example: docusign=2cacbbaa-e1b9-4b82-a86e-68d539d865da

e. TTL: Default or 1 hour / 3600 seconds

To create a CNAME record

a. Navigate to your domain's DNS record management page.

b. Add a new CNAME record.

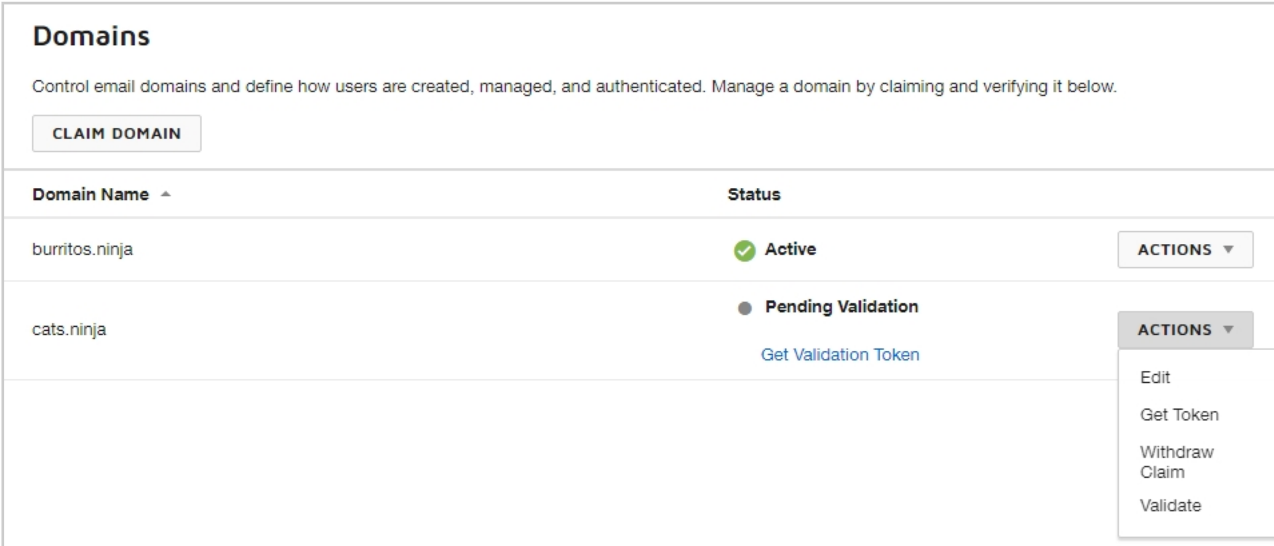
c. Name: 32-digit **GUID only** from the token in Step 5 - Example: 2cacbbaa-e1b9-4b82-a86e-68d539d865da

d. Domain Name: verifydomain.docusign.net.

> **Note:** The process of updating DNS entries 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. Coordinating ahead of time will ensure timely deployment of Single Sign-On.
>
> As a sanity check, you can confirm that your changes are active with the steps outlined in Additional Information for Claiming Domains.

8. Once the DNS changes are active, return to DocuSign Admin 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 tokens are part of the DNS record. If successful, the domain status changes to "Active."

Your domain ownership is proven.

> **Note:** DocuSign periodically reviews pending or active domain claims. It is possible that after updating your DNS, your domain claim can become active in DocuSign even if you have not clicked validate. If you've previously claimed a domain and removed the claim information from your DNS, these reviews would invalidate that claim.

Get a TXT Token for a Claimed Domain

1. In DocuSign Admin, click **Domains**.
2. In the list of domains, locate the domain for which you want to get the token.
3. Click **ACTIONS** on the same line as the domain name and select **Get Token**.
4. Copy the generated TXT token as needed.
5. 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 eSignature application. This operation should only be reserved for cases where you are certain there are no active users with an email address in the domain.

Important: There is no way to undo this change. Use caution when withdrawing an active domain claim.

1. In DocuSign Admin, click **Domains**.
2. In the list of domains, find the domain you want to relinquish.
3. Click **ACTIONS** on the same line as the domain name and select **Withdraw Claim**.
4. Click **CONFIRM** to withdraw your claim.

Additional Information for Claiming Domains

Domain DNS entry

- **TXT or CNAME token must remain in the domain's DNS entry**. For as long as you want to reserve the domain for your DocuSign organization, the token must remain in place. DocuSign periodically checks the DNS to ensure claims are valid, and removal of a token would prevent your users from accessing DocuSign.
- **The process of updating DNS entries 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.
- **Optional - perform a sanity check to confirm the DNS change is active using one of the following methods**.
    - For Windows users, open the command prompt and enter these commands:

      `nslookup -q=txt [myorganization.com]`

      `nslookup -q=CNAME [Guid].[myorganization.com]`

      Where *[myorganization.com]* is the domain you are checking.
    - For Mac users, open the terminal and enter these commands:

      `dig txt [myorganization.com]`

      `dig CNAME [Guid].[myorganization.com]`

      Where *[myorganization.com]* is the domain you are checking.

Identity Providers

Note: This guide is for DocuSign administrators. Single Sign-On requires DocuSign Admin.

This section covers **Step 2** of the process to set up and enable SSO for your DocuSign Organization and provides some supporting reference information on SAML specifications.

SSO enables your company to manage access to DocuSign through an Identity Provider, such as Okta, Azure, Active Directory Federation Services (ADFS), and OneLogin. With SSO, DocuSign users must use the Company Log In option. When they enter their domain email address, authentication is handled by an Identity Provider (IdP).

Once an email domain has been verified for your organization, the DocuSign administrator provides the SAML configuration to allow DocuSign to establish interoperability with the IdP. The domain status must be "Active" before you set up the SAML configuration for the IdP.

Once you have successfully configured your Identity Provider to work with your organization's DocuSign account, you can make SSO mandatory for all domain users to require any user on your email domain to authenticate with your Identity Provider, and configure any required exceptions on a per user basis.

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

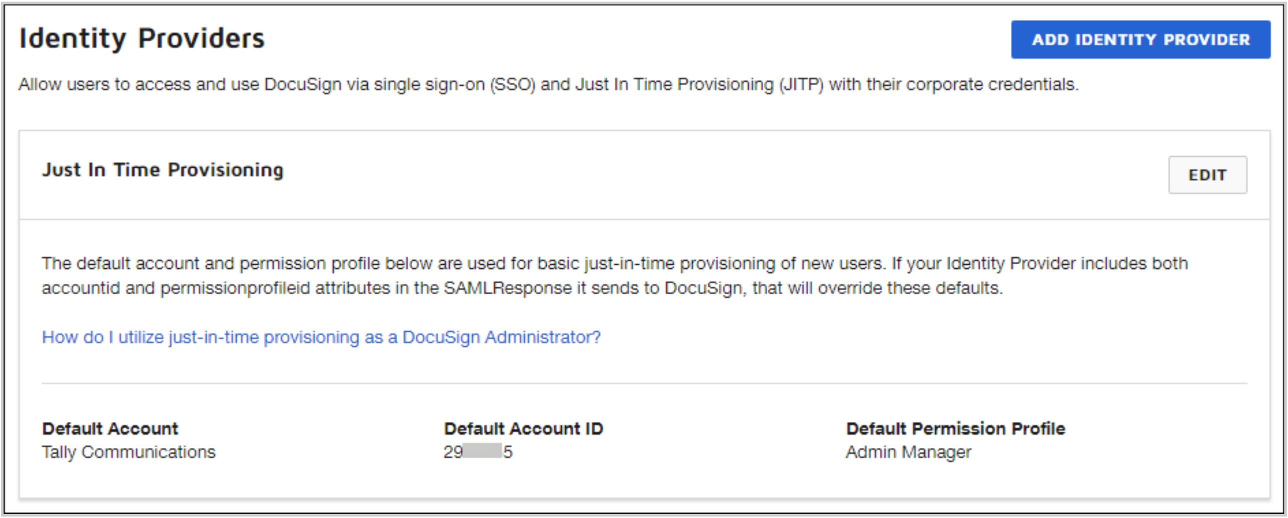
CONTENTS

Set Up an Identity Provider

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.

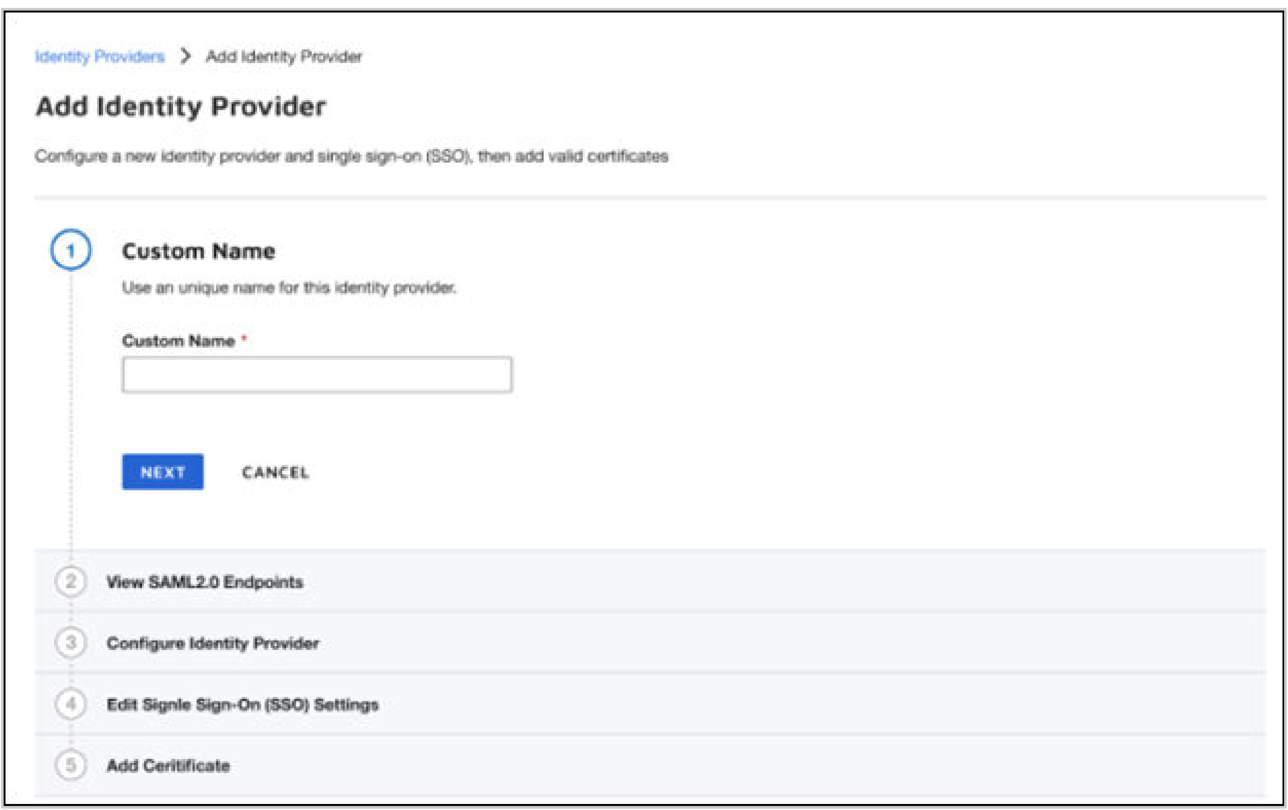
1. From the DocuSign Admin dashboard, click **Identity Providers**.

2. On the Identity Providers page, click **ADD IDENTITY PROVIDER**.



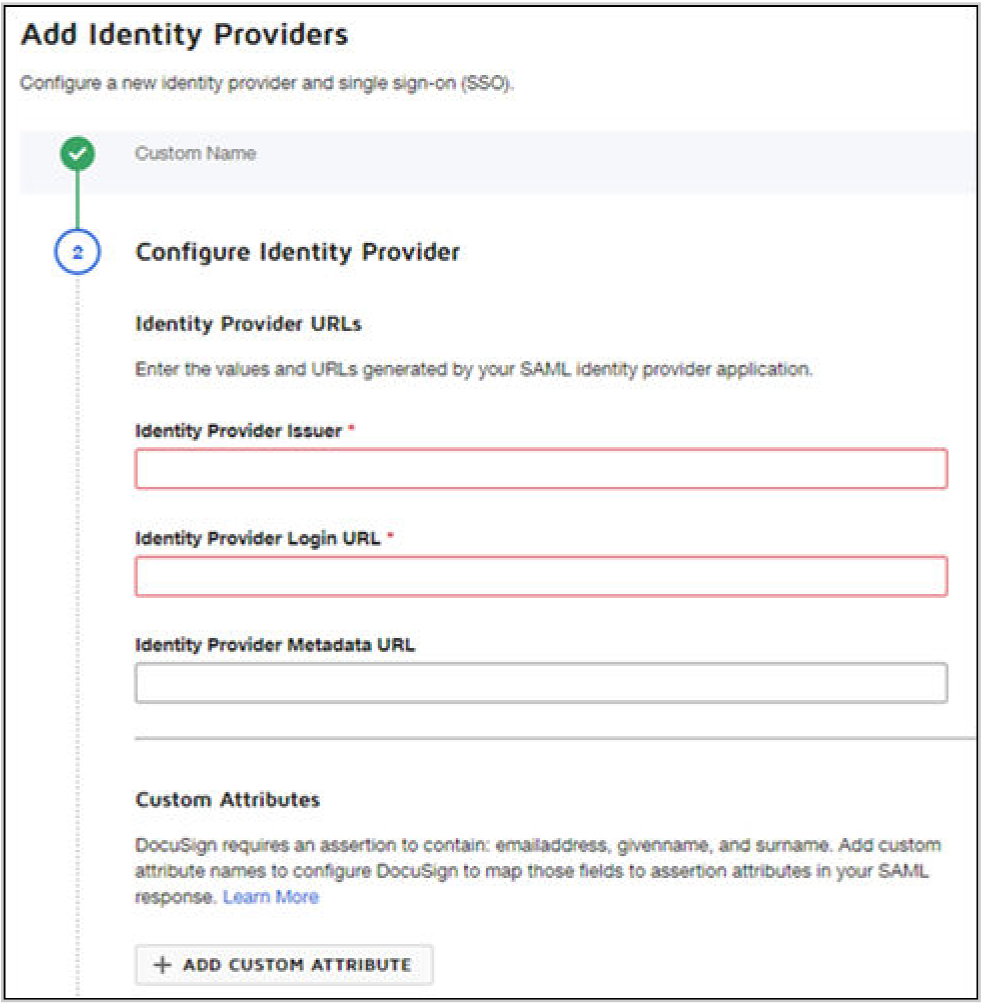
3. Type a custom name for the Identity Provider, and select **NEXT**.

The name must be unique within the DocuSign system. The name is a label for this specific Identity Provider setting and has no impact on the other settings.



4. Enter the values for the following required fields:

- **Identity Provider Issuer**. This must match the issuer field in any SAML assertions.
- **Identity Provider Login URL**. This is the endpoint that handles the SAML Authentication Request.



5. Add custom attribute mappings, and select **NEXT**.

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. If you do not set up custom attribute mapping, then the default value from the Just In Time Provisioning setting is used. If you specify both custom attribute mapping and the default Just In Time Provisioning setting, only the custom attribute mapping value is used.

a) Click **ADD NEW MAPPING** to add a field.

b) Select the appropriate DocuSign Field and then type the Attribute Name to map to the field.

c) Click **ADD NEW MAPPING** to add another field, and then select the appropriate DocuSign Field and then type the Attribute Name to map to the field.

6. Select **Enable Third-Party Login**.

   In most cases, SSO relies on claimed domain email addresses for authentication. With Third-Party Login, organizations can allow approved users with unclaimed domain email addresses such as @gmail.com or @hotmail.com to log in using SSO. To be eligible to log in with Third-Party Login, the user must be a member of an account within your organization and will need to be added to your identity provider (IdP). Once they've been added, these users can login to DocuSign using your organization's IdP.

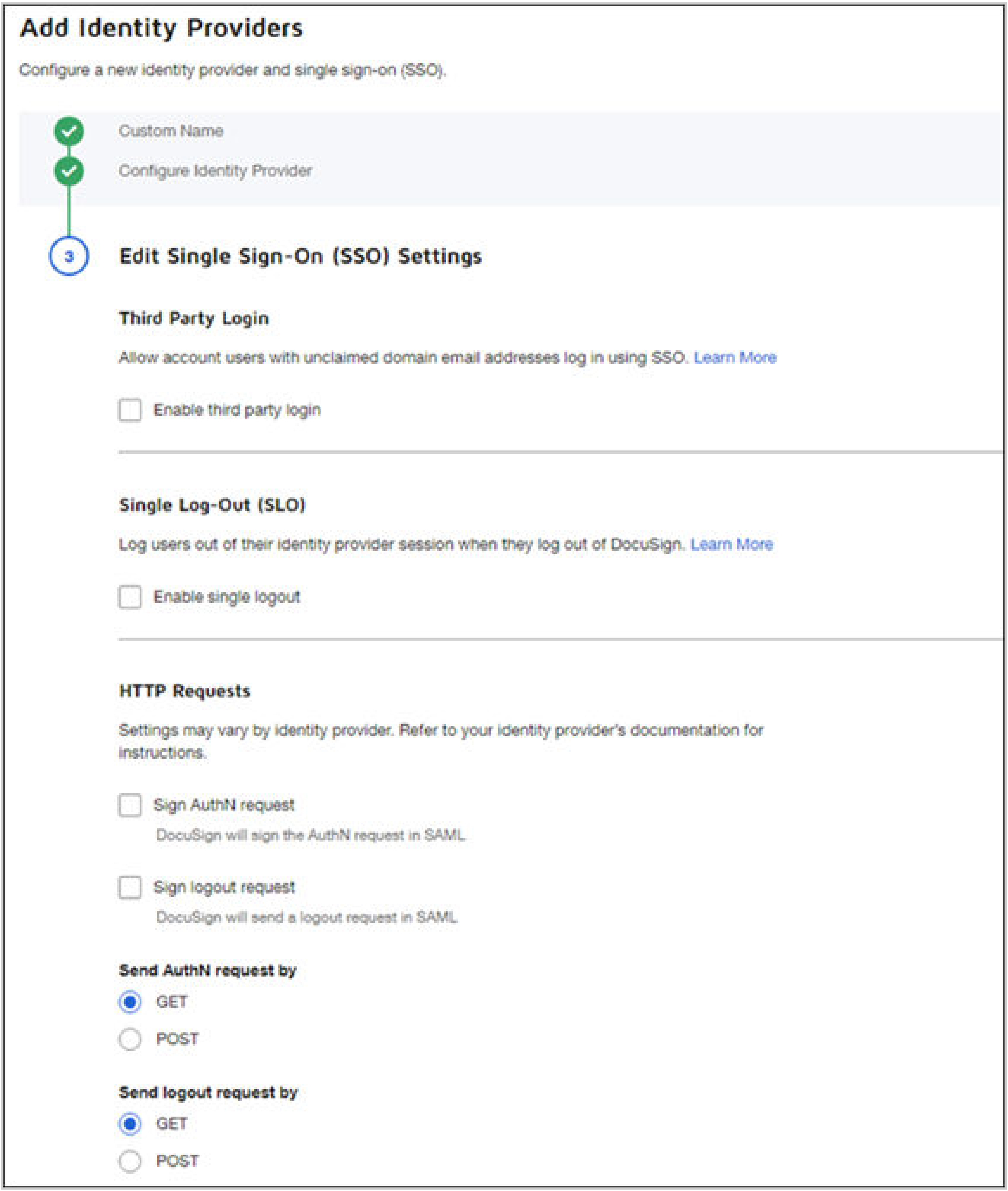
   > **Note:** If a user tries to log in to your IdP with an email address containing a domain claimed by another company, they will be logged in via the other company's IdP.

7. Select **Enable single logout**.

   Similar to the login URL, this is used in cases where a logout request is also processed, which can be handled by a specific URL. If you enable these settings and add an IdP logout URL, when users log out from DocuSign, they are also logged out from the IdP.

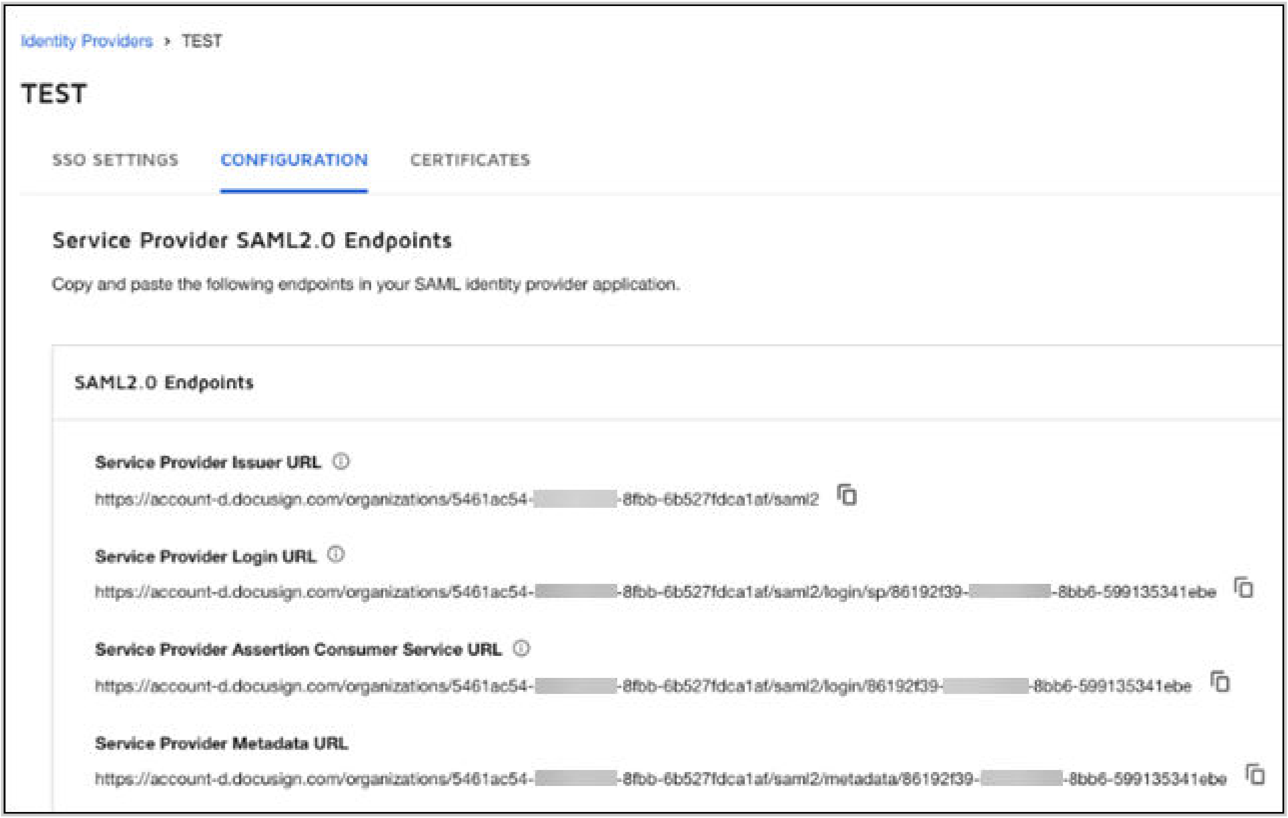
8. Select the HTTP request settings for your identity provider. HTTP Requests settings include:

- **Sign AuthN request:** Select this option to require that DocuSign signs the AuthN request in SAML.
- **Sign logout request:** Select this option to require that DocuSign sends a logout request.
- **Send AuthN request by:** Select either redirect (GET) or HTTP POST.
- **Send logout request by:** Select either redirect (GET) or HTTP POST.



9. Select **ADD IDENTITY PROVIDER**.

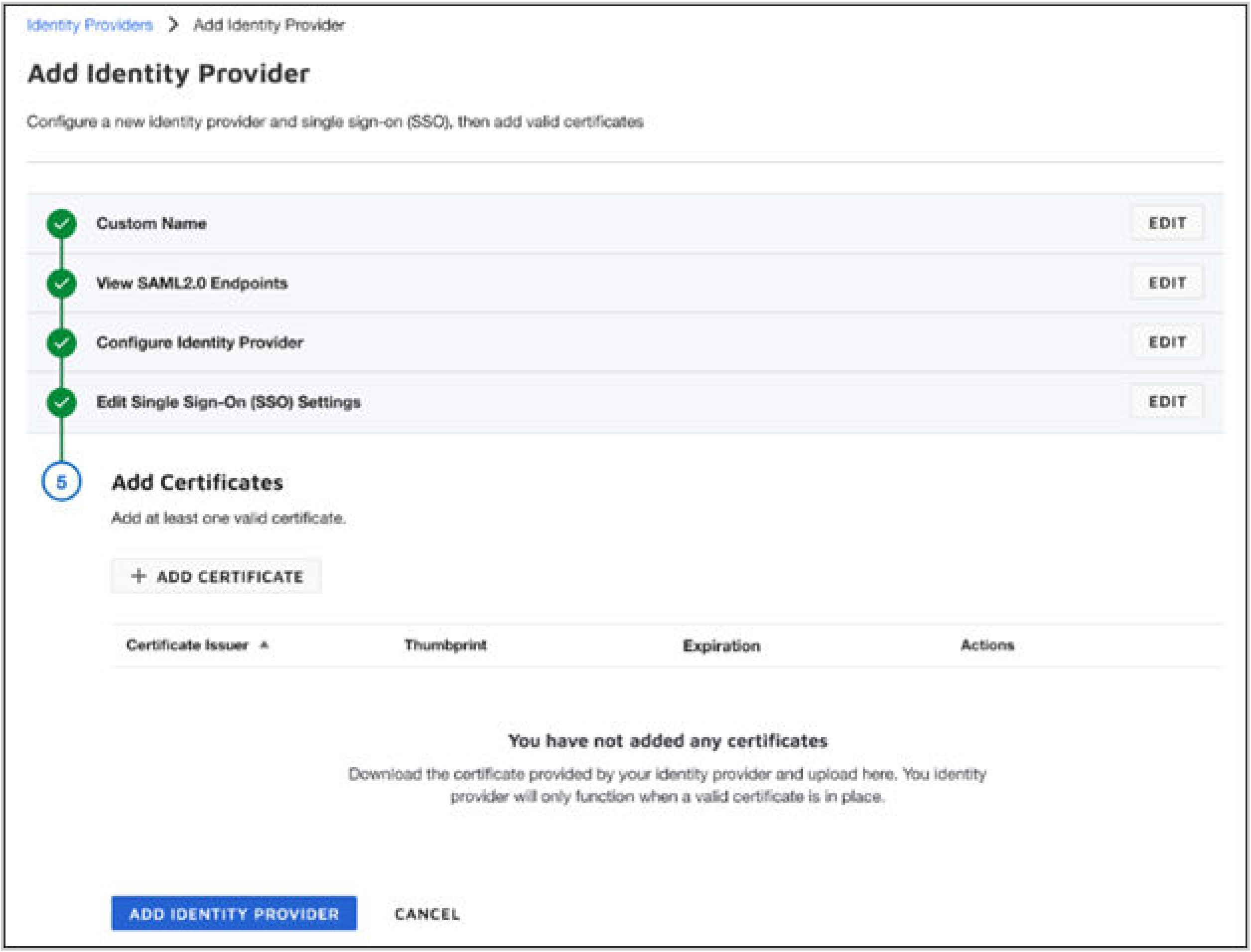
10. On the Identity Providers page, locate the identity provider, and select **ACTIONS** > **Endpoints**.



You can select the copy buttons to copy SAML2.0 endpoint information to your clipboard.

Refer to Service Provider Endpoints for more information on popular service providers.

11. Add at least one valid certificate used by the Identity Provider to sign SAML assertions.



12. Click **SAVE** to save the Identity Provider information.

Your IdP is set up and you can continue to **Step 3** of the SSO setup process and test your SSO configuration.

Service Provider Endpoints

After you setup an identity provider, you can view the service provider SAML endpoints.The SAML 2.0 endpoints listed for the Service Provider consist of the Issuer, Assertion Consumer Services, Metadata, and Login URLs. These URLs are necessary for configuring the IdP and might need sharing with your IT team.

Follow instructions from your IdP to copy this information to specific Service Provider endpoints. For more information on common IdPs, see the following resources:

- Okta https://saml-doc.okta.com/SAML_Docs/How-to-Configure-SAML-2.0-in-DocuSign.html
- Azure AD https://docs.microsoft.com/en-us/azure/active-directory/saas-apps/docusign-tutorial
- Ping https://docs.pingidentity.com/bundle/configuration_guides/page/kkw1621290623870.html
- OneLogin https://onelogin.service-now.com/kb_view_customer.do?sysparm_article=KB0010310

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 and provides an example for each. 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 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.

This identifier is recorded in DocuSign as the Federated ID in the user's Security details. If the NameID changes on your IdP, you must clear the recorded federated ID in order for the user to log in. The new identifier will be recorded the next time the user logs in through SSO.

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

emailaddress (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>
```

givenname (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>
```

surname (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 in 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/accountid" 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 Profile associated with the user. Permission Profiles 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 profile when they are added to the account. The ID information can be retrieved using the REST API.

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/permissionprofileid"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
      <saml:AttributeValue>1</saml:AttributeValue>
    </saml:Attribute>
```

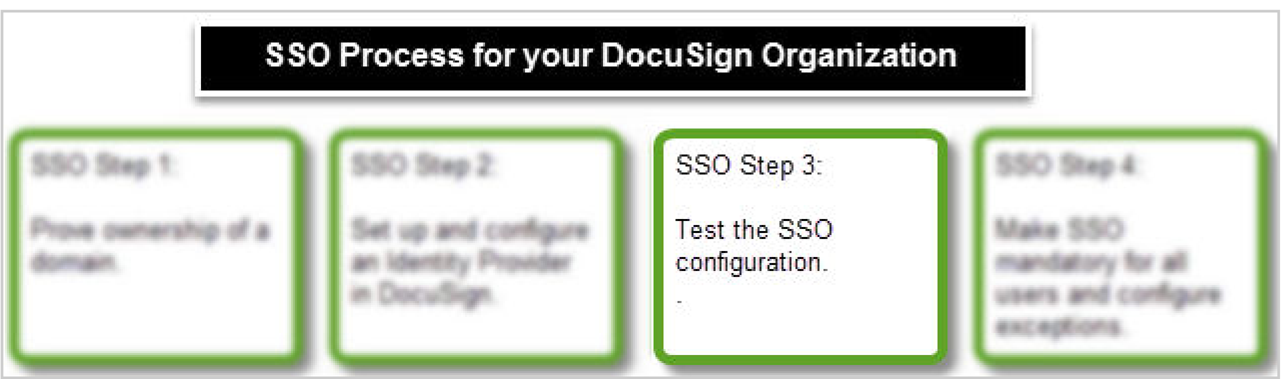
Related Topics

- DocuSign Single Sign-On Overview
- Domains
- Test SSO Configuration
- Setting a User Login Policy

Test SSO Configuration

Note: This guide is for DocuSign administrators. Single Sign-On requires DocuSign Admin.

This section covers **Step 3** of the process to set up and enable SSO for your DocuSign organization.



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 Test Their Logins

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

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

   Production: https://account.docusign.com

2. The user enters their email and clicks **Continue**.

3. Click **Company Login**.

   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 your 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.

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. You can proceed to **Step 4** of the SSO setup process, and change your domain settings to make SSO mandatory for all users and then configure any exceptions.

Best Practices Recommendations before Enforcing SSO

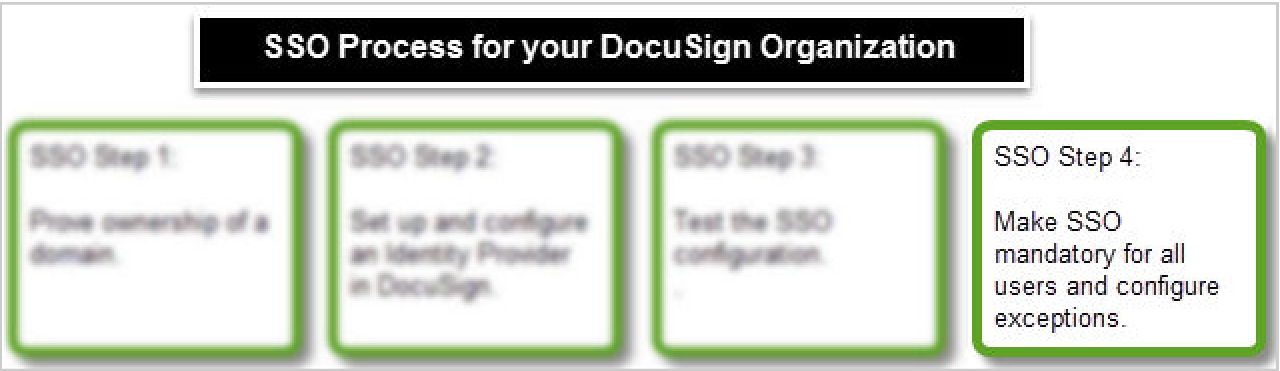
Before you enforce SSO, make sure you have completed the following tasks:

1. Test your Identity Provider configurations between your Identity Provider and DocuSign and completed a successful SSO login.
2. Grant access to all users you want to login to DocuSign using SSO.
3. If you have any service users for a third party integration, you want to make sure you have set the login policy to "Identity Provider or username/password".
4. Make sure at least one of your organization administrators has a Login Policy that is set to "Identity Provider or username/password" in case SSO is not functioning. It is recommended to have more than one Organization administrator.
5. Manage the following changes for any external users before enforcing SSO:
   a. Ensure you have linked all your corporate accounts to the organization.
   b. Enable "Prevent unmanaged signups" at the domain level. This prevents users from creating accounts outside of your corporate account.
   c. Enable "Require all users to authenticate with Identity Provider" on the domain. This removes the "Use company Login" button and automatically redirects your users to the Identity Provider.

Change Domain Settings

Note: This guide is for DocuSign administrators. Single Sign-On requires DocuSign Admin.

This section covers **Step 4** of the process to set up and enable SSO for your DocuSign organization.

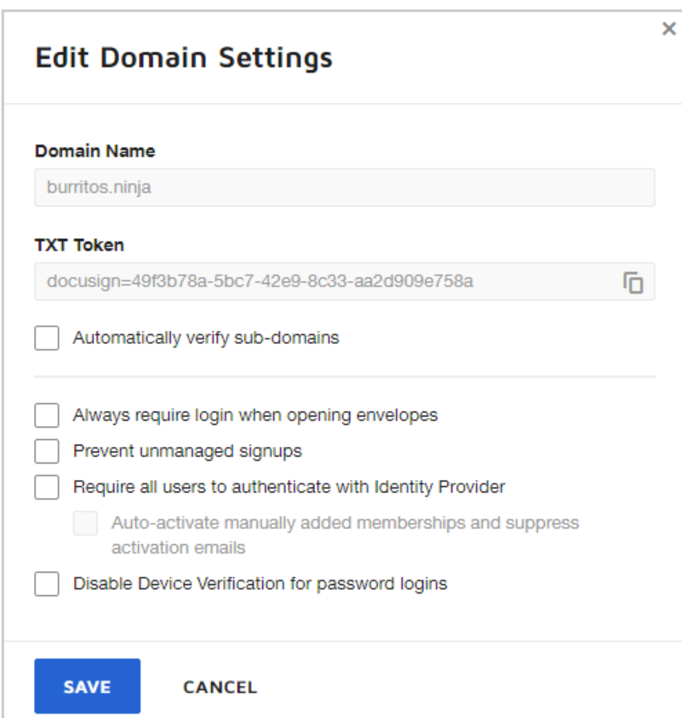


Enable SSO and Enforce Federated Login for All Users

1. In DocuSign Admin, click **Domains**.

2. In the list of domains, find the domain you want to edit.

3. Click the domain name or click **ACTIONS** on the same line as the domain name and select **Edit**.



4. Select the option **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.

   SSO is enabled and mandatory for all domain users. You should now set user login policy to configure any exceptions for users who need to be able to log in without requiring IdP authentication.

Apply Additional Domain Security Settings

Once SSO has been enabled for your domain, there are additional security options that you can apply to a reserved domain for your domain users.

1. In DocuSign Admin, click **Domains**.

2. In the list of domains, find the domain you want to edit.

3. Click the domain name or click **ACTIONS** on the same line as the domain name and select **Edit**.

4. Select the security options to enable for your domain.

   - **Always require login when opening envelopes:** When a user with the email domain receives a document, they must first log in before they can open the document.
   - **Prevent unmanaged signups:** Domain users cannot create individual accounts using their corporate email address. These users can only be added to accounts linked to your organization. They must either be created by your administrator or the Identity Provider.
   - **Disable Device Verification for password logins:** By default, DocuSign requires users logging in from an unrecognized device to reverify their email before continuing. Though it is recommended to keep this enabled, some domains may need to disable it if users are unable to verify their email address each time they log in. When checked, device verification will be disabled for all users on this domain.

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

Set Auto-Activation of New Memberships as the Default

When adding memberships to new or existing domain users, you can choose to activate memberships automatically by default. Memberships activated in this way will not receive an activation email. The administrator can choose to override this option when adding a new user.

Memberships for existing domain users with a 'Pending' status can be activated manually from the user details page. For more information, see User Management.

> **Note:** This option is only available if the domain setting **Require all users to authenticate with Identity Provider** is selected.

1. In DocuSign Admin, click **Domains**.

2. In the list of domains, find the domain you want to edit.

3. Click the domain name or click **ACTIONS** on the same line as the domain name and select **Edit**.

4. Select **Auto-activate memberships by default for Organization accounts**.

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

   New account memberships to organization accounts will default to automatic activation.

Setting a User Login Policy

Note: This guide is for DocuSign administrators. Single Sign-On requires DocuSign Admin.

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 DocuSign 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.

Note: It is also possible to prevent users from logging into personal DocuSign accounts while at work. For more information, see Prevent Access to Personal DocuSign Accounts.

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

- The DocuSign 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 without 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, DocuSign administrators have the option of setting login policies on a per user basis.

Important: This login policy 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.

Change the Login Policy for a User

1. In DocuSign Admin , click **Users**.

2. Click to select the **Domain Users** quick list.

   Note: A login policy only applies to domain users who can use SSO to log in.

3. Find the user that will bypass federation. Click the user to access their details.

4. Select the **Security** tab for the user. The available settings are:
   - **Default:** This setting uses the policies set for the user's email 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.
   - **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.

5. Click **SAVE** to save the change.

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

Prevent Access to Personal DocuSign Accounts

As an IT organization, you may have the requirement that employees should not have access to personal DocuSign accounts at work.

Typically, organizations use a proxy server to block URLs of web services employees shouldn't access at work. Unfortunately, this doesn't work for SaaS services, especially when the same web service is being used as an enterprise application within the organization. Blocking a URL may mean that certain DocuSign properties won't function properly or users may not be able to access the application, even with a legitimate work account.

DocuSign allows you to have your proxy server send a hint to DocuSign via an HTTP header to indicate what a user can access from this network. The solution is hard to circumvent, but still allows access for legitimate, professional use of the product.

You may need to work with your IT team to complete these steps, but the process is as follows:

1. Set up a proxy server to ensure all outbound traffic to access DocuSign is routed through this proxy.
2. Enable SSL interception at the proxy. Since the proxy will be intercepting SSL requests, you'll need to configure your employees' devices to trust your SSL proxy. This means deploying the Internal Root Certificate Authority used by the proxy and marking it as trusted. Failure to do so may cause some browsers to not load the page and/or display an error.
3. Enable the proxy to intercept each HTTP request and insert a special header. The content of the HTTP request does not need to be modified.

X-DocuSign-Allow-Organization Header

The header to be injected will use this format:

```
X-DocuSign-Allow-Organization: <organization id>
```

This allows users to log into DocuSign with an email address on a domain claimed by the organization.

> **Note:** For more information on the domain claim process, see Domains.

You may also need to include a proxy policy to overwrite/replace/drop this header if an end-user tries to specify this header themselves. This prevents a user from circumventing your proxy rules.

If the user tries to log in with an email address that does not belong to the organization, then they will see an error on the DocuSign login page indicating that their network administrator has blocked access to personal DocuSign accounts.

Example Configuration

These sample values represent your organization ID in the production or demo environments.

> **Note:** Find your organization ID in **DocuSign Admin** > **Overview** > **Details**. The ID differs between production and demo, so be sure to locate both if you intend to allow users to access both environments.

Table 1:

Environment	Example Organization ID
Demo	28abc869-df2d-4abc-b64d-573111abcd06
Production	39zyx869-df2d-4zyx-b64d-573111wzyx06

The proxy would include both values for demo and production so that all environments are covered.

For example, this is what header the proxy would include on all requests to DocuSign.com or DocuSign.net:

```
X-DocuSign-Allow-Organization: 28abc869-df2d-4abc-b64d-573111abcd06,39zyx869-
df2d-4zyx-b64d-573111wzyx06
```

Organization Administrators

An organization can have multiple DocuSign administrators. DocuSign administrators can have full rights to manage an organization, or be limited to managing organization users or account settings only.

DocuSign administrators with full administrative rights can manage Single Sign-On (SSO) details, including domains and identity providers. They can also manage all reserved domain users and all users belonging to the accounts linked to the organization, without requiring direct administrative rights on the accounts themselves.

> **Note:** See Establish Control of your Company's DocuSign Agreements to learn how you can gain control of your company's agreements with proven best practices and procedural guidelines.

CONTENTS

DocuSign administrators

Every organization has at least one DocuSign administrator. By default, this is the eSignature administrator who created the organization. If DocuSign professional services helped set up your organization, the DocuSign administrator may have been selected at that time instead. As a best practice, DocuSign recommends you have at least two DocuSign administrators to help ensure continuity and coverage in managing your organization.

DocuSign Admin permission profiles

To provide better control over administrative access to your organization, there are different permission profiles you can assign to administrators:

- **Administrator:** This permission profile grants full access to manage the organization. The administrator with this permission profile can control, manage, and edit all features and users available in the organization.
- **Users Administrator:** This delegated administrator permission profile limits the administrator's access to just managing organization users. The administrator with this permission profile can add, edit, and close any non-administrator user within the organization. When managing user memberships, this administrator is limited to applying and making changes to non-administrator permission profiles only. This administrator cannot assign an administrator permission profile to a user, nor can they change an administrator permission profile assigned to a user. This delegated user administrator cannot add, edit, or close other DocuSign administrators.
- **Settings Administrator:** This delegated administrator permission profile limits the administrator's access to viewing and managing organization accounts and account settings. The administrator with this permission profile can view, compare, export, and import account settings. They can also link and unlink accounts from the organization. They cannot perform any user management tasks and do not have access to any other organizational capabilities.
- **Product Reports Administrator:** This delegated administrator permission profile limits the administrator's access to exporting envelope reports and viewing envelope report export history. The administrator can select from a variety of reports that will pull data from all accounts in the organization. They cannot perform any user or account management tasks and do not have access to any other organizational capabilities. For more information, see Organization Reporting.
- **Security Reports Administrator:** This delegated administrator permission profile limits the administrator's access to event reporting with DocuSign Monitor. They cannot perform any user management tasks and do not have access to any other organizational capabilities. For more information, see Protect your DocuSign eSignature deployment with DocuSign Monitor.

Note: Access to these permission profiles is determined by your account plan. If you do not see all of the permission profiles described in this section it is because of the account plan options. Contact DocuSign customer support for more information.

DocuSign Administrator Permission Profiles

Users					
Section	**DocuSign Administrator**	**Users Administrator**	**Settings Administrator**	**Product Reports Administrator**	**Security Reports Administrator**
View All Users	Yes	Yes	No	No	No
Add Users	Yes	Yes	No	No	No
Edit User Profile - Non-Admin	Yes	Yes	No	No	No
Edit User Profile - DocuSign Admin or Account Admin	Yes	No	No	No	No

Users					
Section	**DocuSign Administrator**	**Users Administrator**	**Settings Administrator**	**Product Reports Administrator**	**Security Reports Administrator**
Edit Security Profile - All Users	Yes	Yes	No	No	No
Add/Edit/Close User Account Membership - Non-Admin	Yes	Yes	No	No	No
Add/Edit/Close User Account Membership - DocuSign Admin or Account Admin	Yes	No	No	No	No
Close Users	Yes	No	No	No	No
Accounts					
Section	**DocuSign Administrator**	**Users Administrator**	**Settings Administrator**	**Product Reports Administrator**	**Security Reports Administrator**
View All Accounts	Yes	Yes	Yes	No	No
Compare Account Settings	Yes	No	Yes	No	No
Link/Unlink Accounts to Organization	Yes	No	Yes	No	No
Bulk Actions					
Section	**DocuSign Administrator**	**Users Administrator**	**Settings Administrator**	**Product Reports Administrator**	**Security Reports Administrator**
Export Account Settings	Yes	No	Yes	No	No
Import Account Settings	Yes	No	Yes	No	No
Export Users	Yes	Yes	No	No	No
Import Users	Yes	Yes	No	No	No
View Account Settings Bulk Actions Activity	Yes	No	Yes	No	No
View Users Bulk Actions Activity	Yes	Yes	No	No	No

Reporting					
Section	**DocuSign Administrator**	**Users Administrator**	**Settings Administrator**	**Product Reports Administrator**	**Security Reports Administrator**
Export Envelope Reports	Yes	No	Yes	Yes	No
Access DocuSign Monitor	Yes	No	No	No	Yes
View Envelope Reports Bulk Actions Activity	Yes	No	Yes	Yes	No

The initial DocuSign administrator can create additional administrators for the organization, specifying which permission profile is granted to each new administrator. Each DocuSign administrator with the Administrator permission profile who accepts and activates their DocuSign administrator membership gains equal control over all SSO details and all users across all accounts linked to the organization. In order for them to also have administrative access to an account linked to the organization, they must have the All Administration Capabilities permissions for the account.

You must be both a DocuSign administrator with the Administrator permission profile and an account administrator to link an account to an organization. Therefore, assuming you want to link all of your corporate accounts to your organization, for each account, you will need to make at least one account administrator (with All Administration Capabilities permissions) a DocuSign administrator. If you are an administrator on each account, then you could link all accounts yourself and continue to manage the organization as the sole DocuSign administrator.

Users can be a DocuSign administrator for multiple organizations.

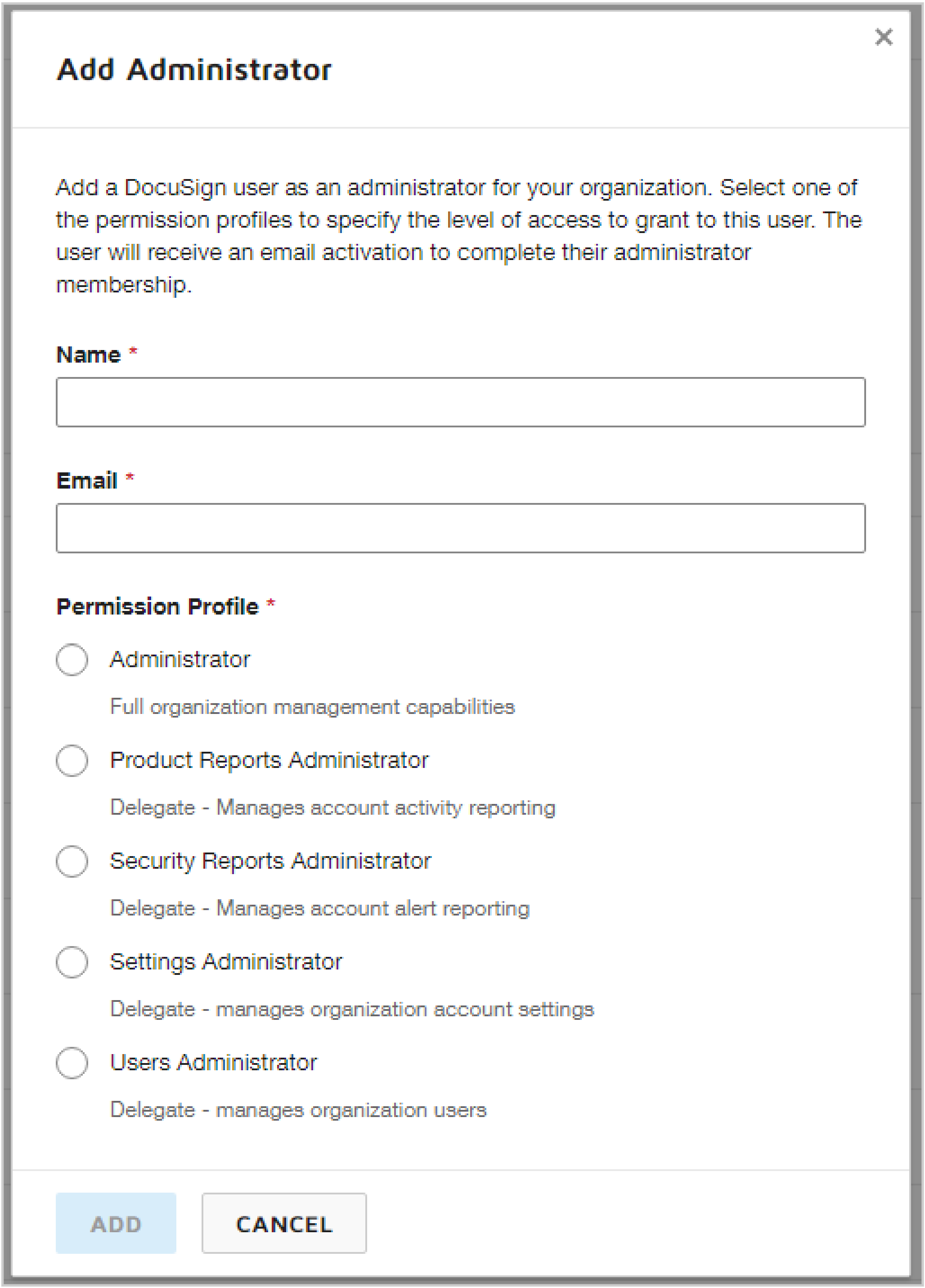
Add a DocuSign Administrator

Any DocuSign administrator with the Administrator permission profile can add additional DocuSign administrators by inviting other DocuSign users. To become a DocuSign administrator, a DocuSign account is required, but the account does not need to be associated with the organization.

1. From the DocuSign Admin dashboard, click **Administrators**.

2. In the DocuSign administrators list, click **ADD ADMIN**.

3. Fill in the user's name and email address to send an invitation to the user. Be sure to enter the user's email associated with their DocuSign account.



4. Select the Permission Profile to grant to the new administrator.

   - **Administrator:** Full control over the organization
   - **Users Administrator:** Delegated user manager
   - **Settings Administrator:** Delegated account settings manager
   - **Product Reports Administrator:** Delegated account-level reporting manager
   - **Security Reports Administrator:** Delegated alert reporting manager

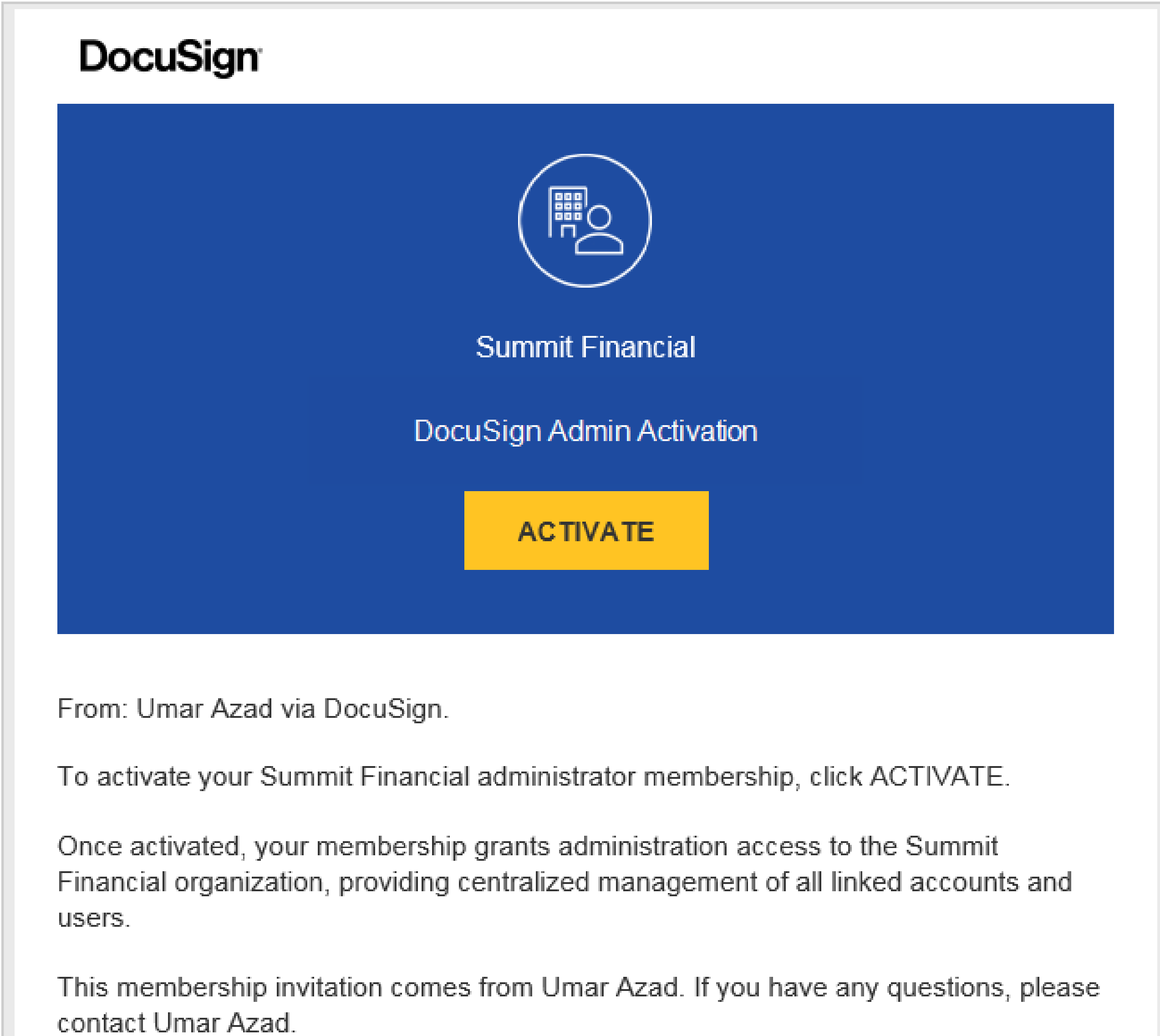
5. Click **ADD ADMINISTRATOR**.

   The user is added to the list of DocuSign administrators with the status "Pending". The user receives an email invitation and must activate their membership as described in To activate a DocuSign administrator membership.

Activate a DocuSign Administrator Membership

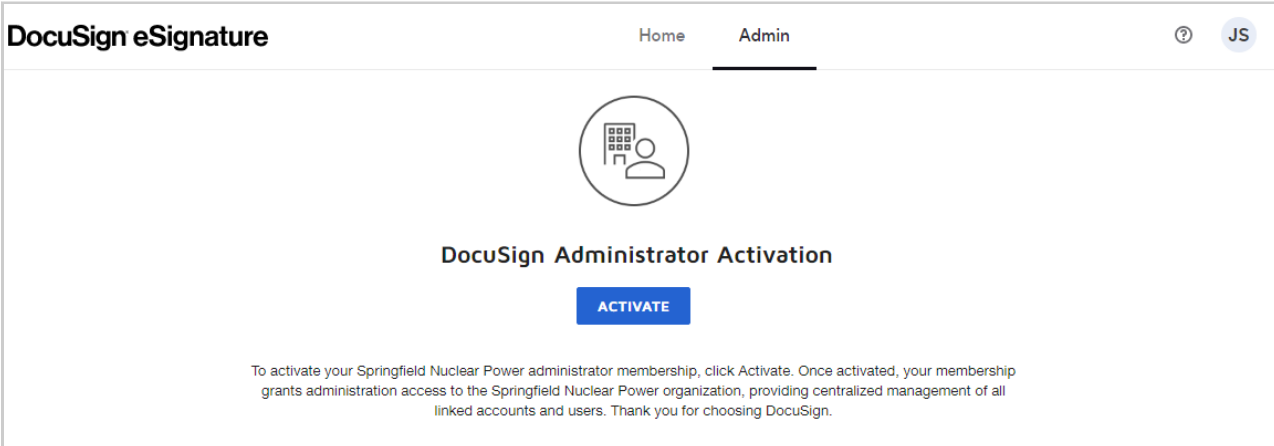
If you are invited to join an organization as a DocuSign administrator, you receive an email invitation to activate your administrator membership.

1. Open the DocuSign administrator membership activation email you received, and click **ACTIVATE**.



2. Enter your DocuSign account credentials to log in to your account.

3. The activation page opens where you can review your invitation details.



4. Click **ACTIVATE** to finalize your administrator membership.

Your membership is activated and you arrive at the DocuSign Admin dashboard.

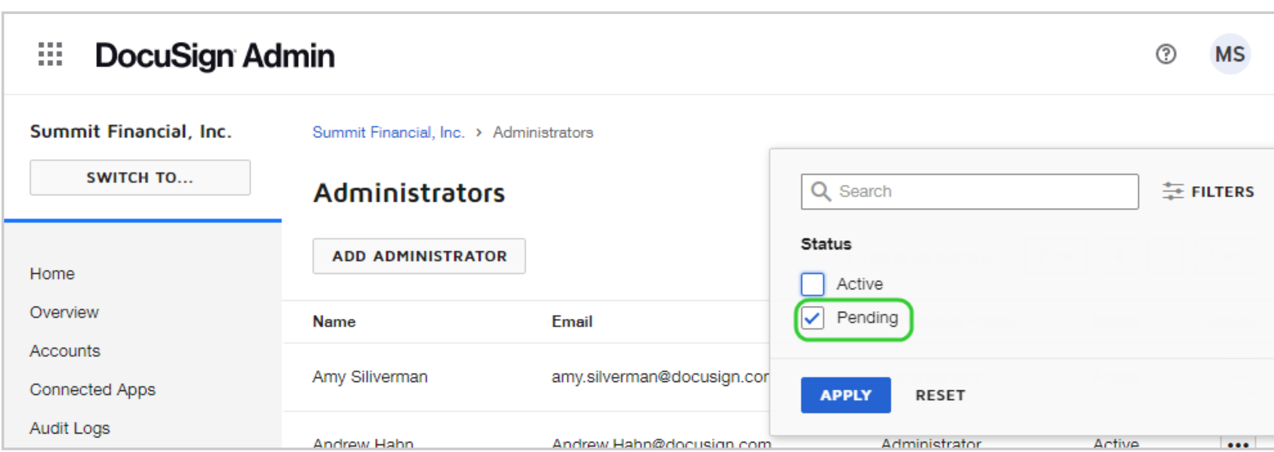
- The Administrator dashboard displays all tiles available for the organization.
- The Users Administrator dashboard is limited to the Users, Accounts, and Bulk Actions tiles.
- The Settings Administrator dashboard is limited to the Accounts and Bulk Actions tiles.
- The Product Reports Administrator dashboard is limited to the Bulk Actions tile.
- The Security Reports Administrator dashboard is limited to the DocuSign Monitor tile.

Resend, Cancel, or Edit a DocuSign Administrator Invitation

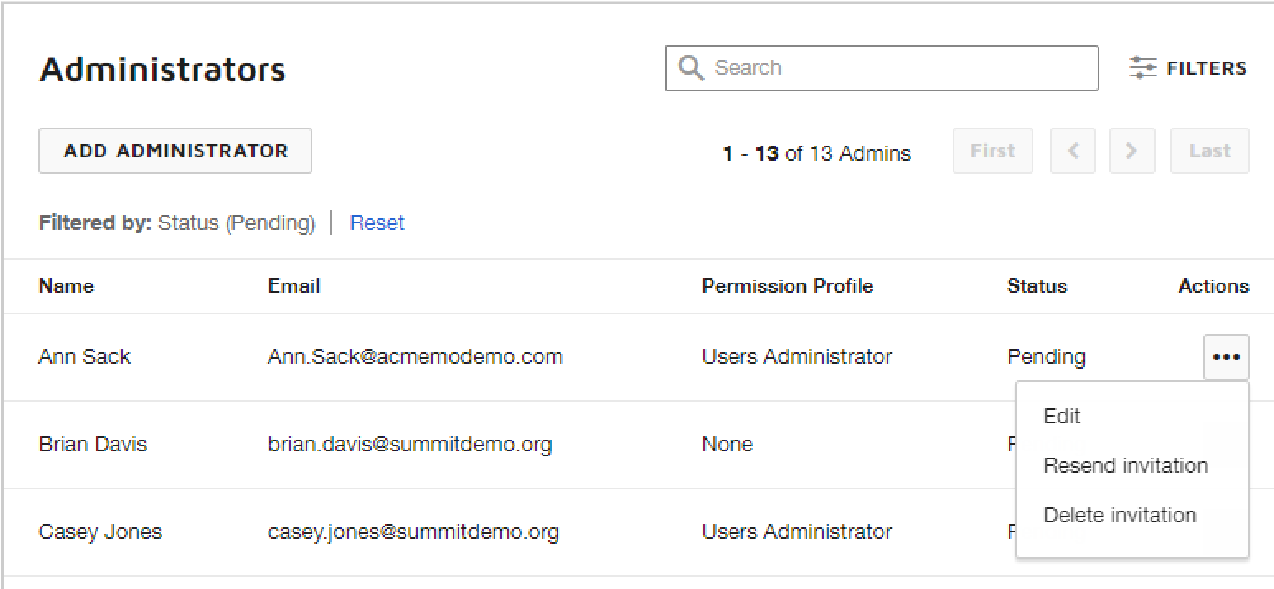
Any DocuSign administrator with the Administrator permission profile can resend or cancel invitations that are pending.

1. From the DocuSign Admin dashboard, click **Administrators**.

2. Locate the pending invitation. You can use the Filters to show only Pending status, or search by name or email.



3. Click the **Actions** menu and select to resend, cancel, or edit the invitation.



- **Edit**: Modify the pending administrator's name or permission profile. To change the email address, delete the original invitation and re-add the user as an administrator using the new email address.
- **Resend invitation**: Sends a new email invitation to the pending user.
- **Delete invitation**: Cancels the invitation. If the user tries to activate their membership, they get a message saying the invitation is no longer valid.

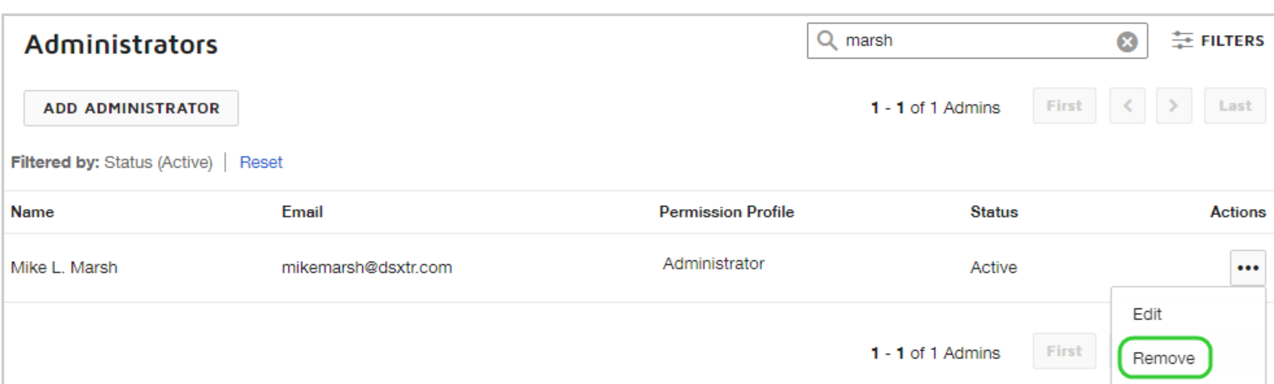
Remove a DocuSign Administrator

Any DocuSign administrator with the organization permission profile can remove any other active DocuSign administrator. When you remove a DocuSign administrator, the user loses all access to the organization.

1. From the DocuSign Admin dashboard, click **Administrators**.

2. Locate the administrator you want to remove from the organization. You can use the Filters to show only Active status, or search by name or email.

3. Click the **Actions** menu and select **Remove**.



4. Click **CONFIRM** to remove the administrator.

Bulk Actions

> **Note:** This guide is for DocuSign administrators who oversee multiple accounts. For administrators of individual accounts, see the DocuSign eSignature Admin guide, User Bulk Actions.

As a DocuSign administrator, you can view and manage details for multiple users or accounts at a time. Bulk actions enable DocuSign administrators to manage details for all users and all accounts within an organization.

Select a topic below for more information:

- User List Exports
- Bulk Add New Users
- Bulk Update Users
- Bulk Close Users
- Account Settings Export
- Account Settings Import
- Organization Reporting

For information on adding remote online notary users to your organization in bulk, see Upload Notaries: Add Remote Online Notaries in Bulk.

User List Exports

> **Note:** This guide is for DocuSign administrators who oversee multiple accounts. For administrators of individual accounts, see the DocuSign eSignature Admin guide, User Bulk Actions.

DocuSign Administrators and Users Administrators can export a list of users across all accounts in the organization as a comma-separated value (CSV) file. Exports include user details such as full name, email address, and permission profile.

Export types:

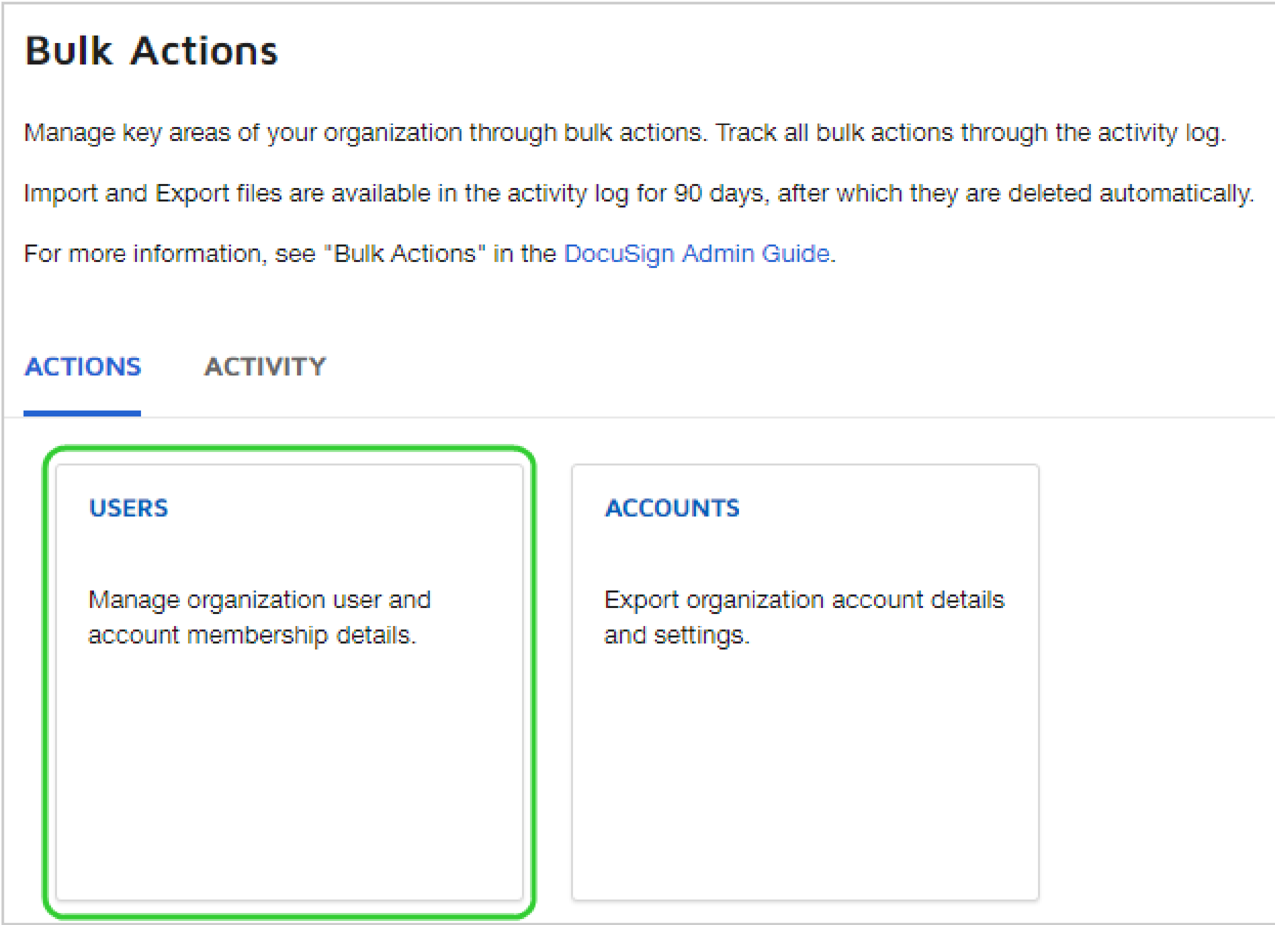
- **Users and Memberships:** All users and their memberships across all accounts in the organization.
- **Domain Users:** All domain users, their profile details, default account, and login policy.
- **External Domain Users:** All domain users memberships in accounts external to the organization.

> **Note:** Organizations without a claimed domain will see only the Users and Memberships export option.

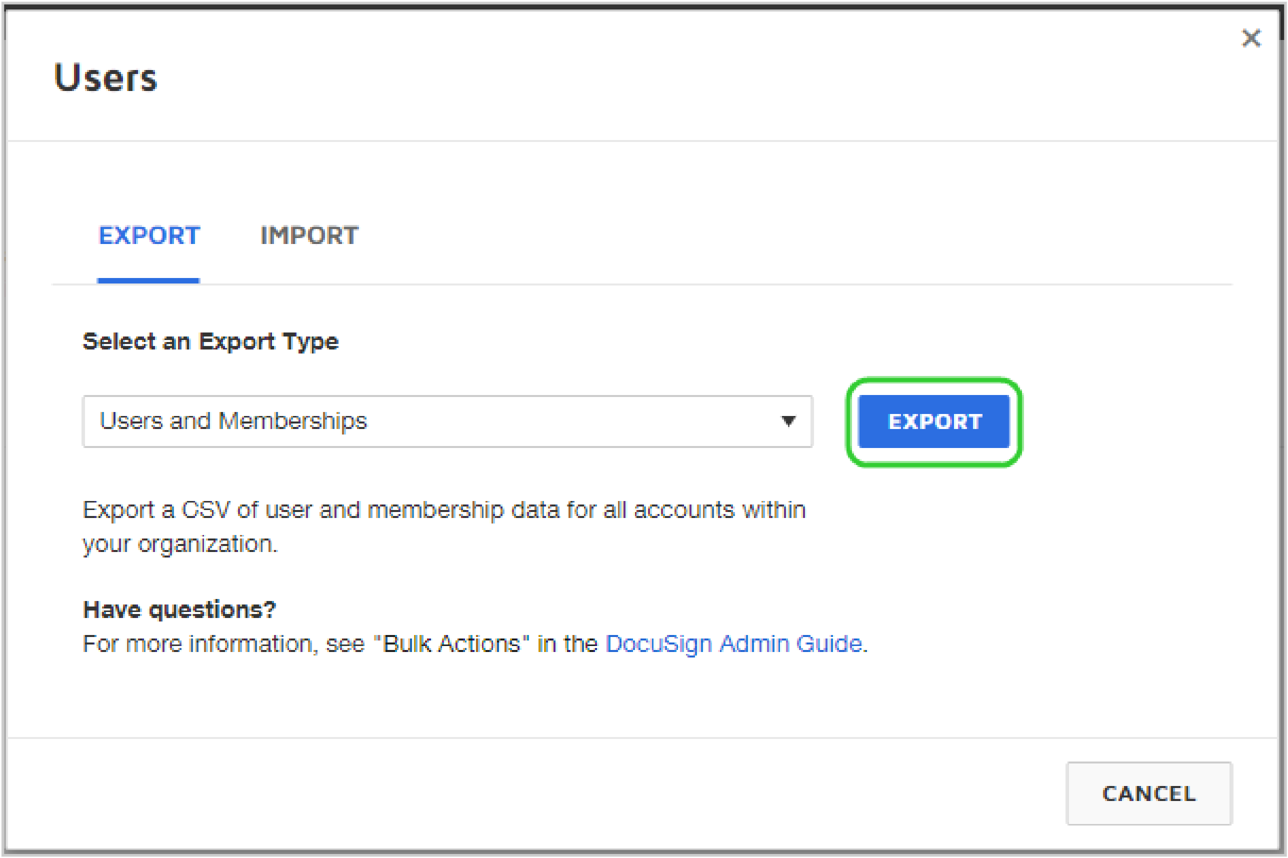
Export a List of Users

1. From the DocuSign Admin dashboard, click the **Bulk Actions** tile.

2. Click the **USERS** tile.



3. Select the export type from the drop-down menu.



Export types:

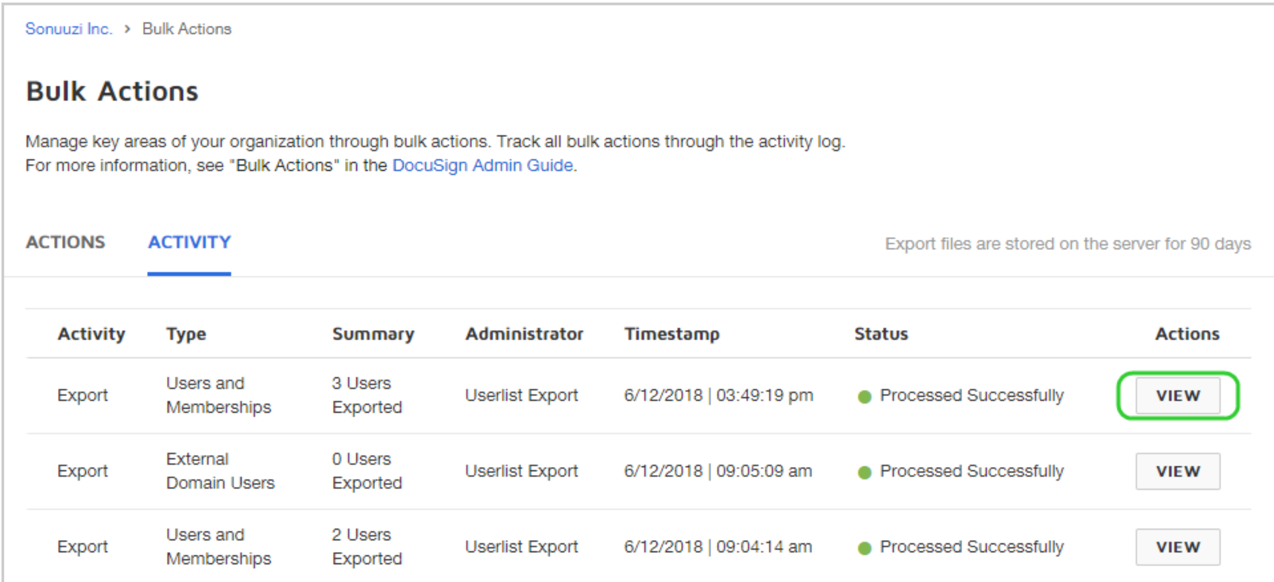
- **Users and Memberships:** All users and their memberships across all accounts in the organization.
- **Domain Users:** All domain users, their profile details, default account, and login policy.
- **External Domain Users:** All domain users memberships in accounts external to the organization.

> **Note:** Organizations without a claimed domain will see only the Users and Memberships export option.

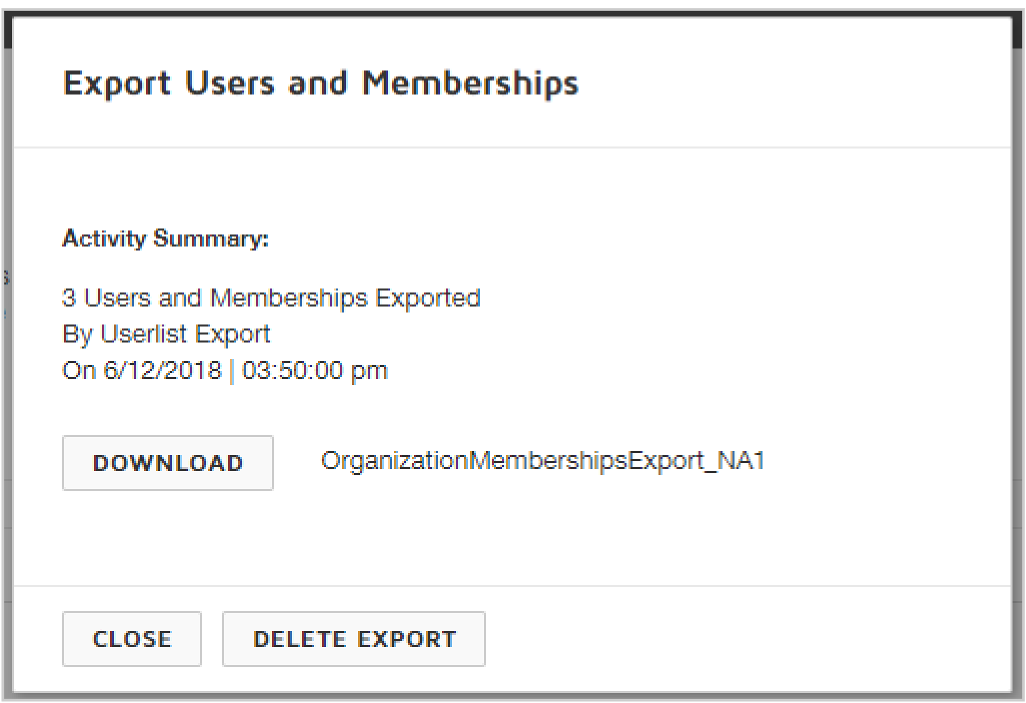
4. Click **EXPORT**.

> **Note:** Only one type of export or import can be in progress at a time.

5. From the ACTIVITY tab, you can view the status of the export. Click the refresh icon to update the export status. When the export is complete, click **VIEW**.



6. Click **DOWNLOAD** to download the export CSV. When finished, click **CLOSE**.



Note: Your organization can store a combination of up to 100 user exports and account settings exports at a time; both are retained for 90 days. To manually delete exports, click **DELETE EXPORT**, then click **DELETE**.

Bulk Add New Users

Note: This guide is for DocuSign administrators who oversee multiple accounts. For administrators of individual accounts, see the DocuSign eSignature Admin guide, User Bulk Actions.

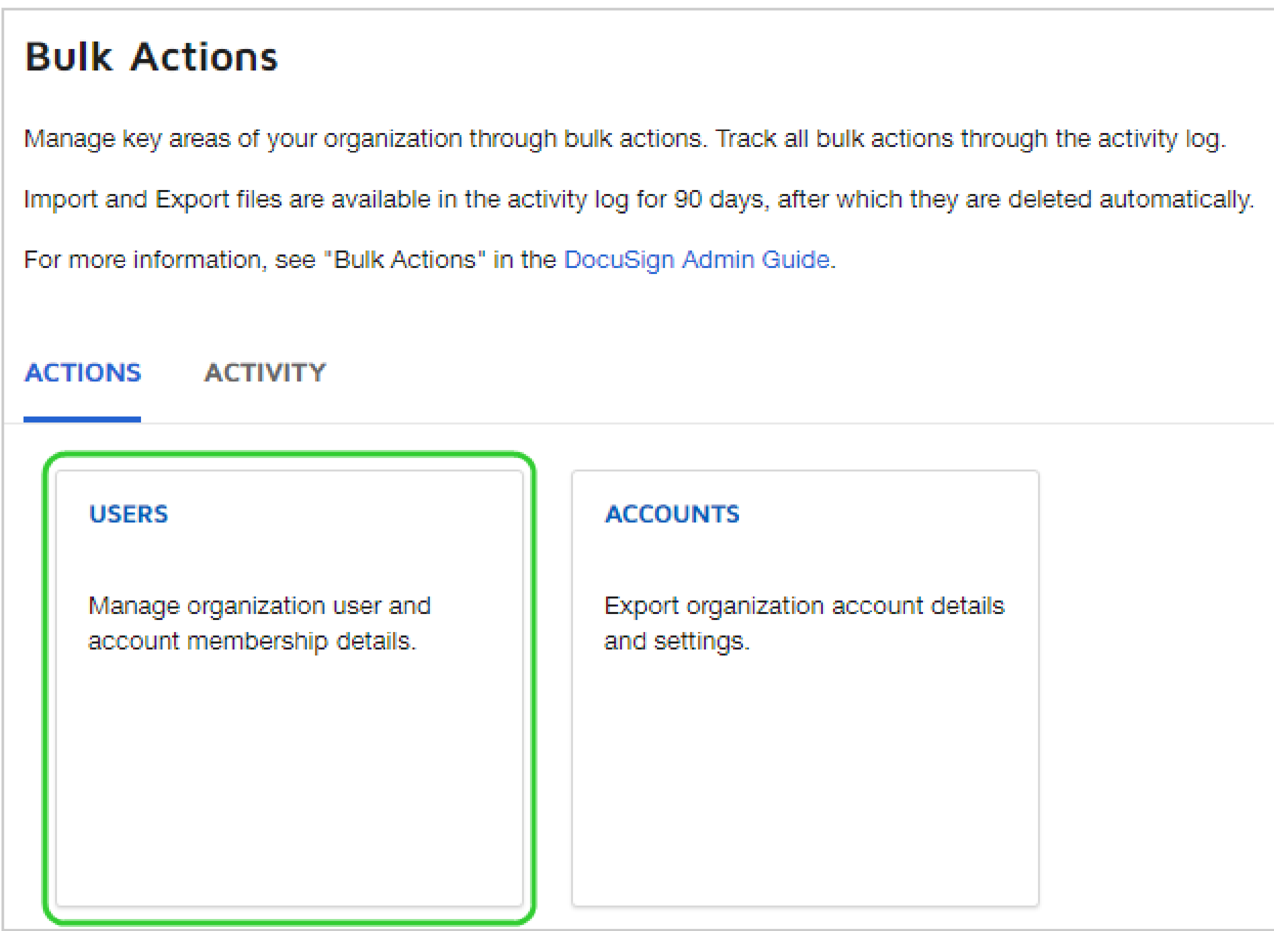
DocuSign Administrators and Users Administrators can bulk add new users to one or more accounts by uploading a comma-separated value (CSV) file. The format of the CSV must match the sample file. For more information on the CSV format, see Building a CSV.

You can add up to 2,000 users to an account and include up to 50 accounts per imported CSV. The maximum number of users per import is 8,000.

Add Multiple Users with Bulk Actions

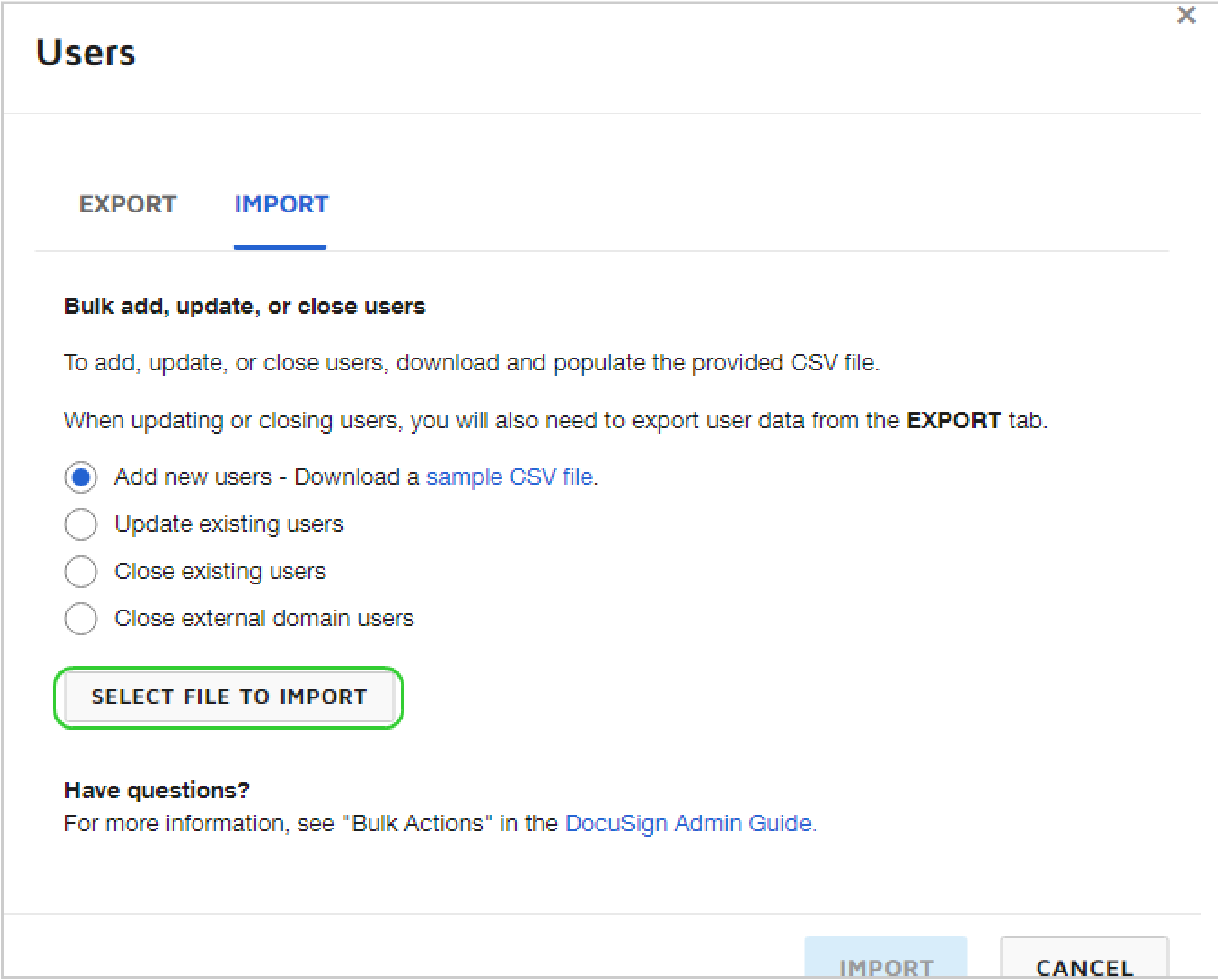
1. From the DocuSign Admin dashboard, click the **Bulk Actions** tile.

2. Click the **USERS** tile.



3. In the Users dialog, click to select the **IMPORT** tab.

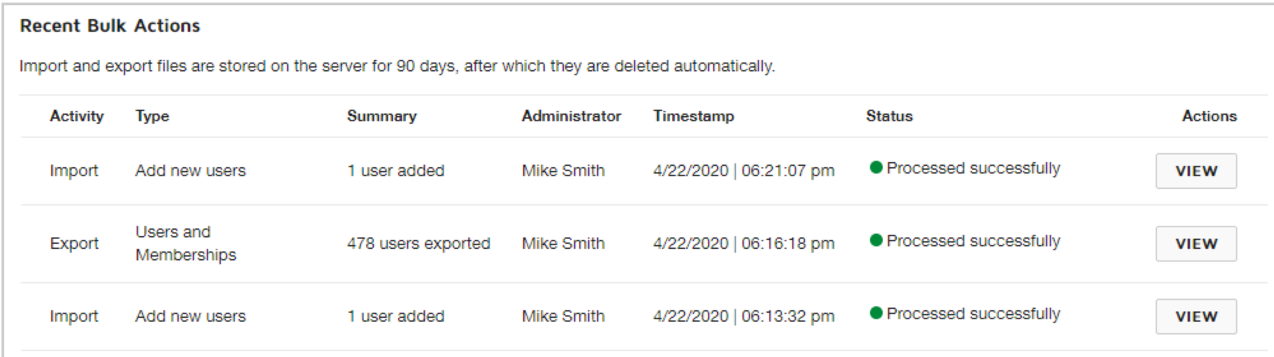
4. Select **Add new users**, then click **SELECT FILE TO IMPORT**.



Select the CSV file to import. Make sure the formatting matches the sample CSV provided. For more details, see Building a CSV.

5. Click **IMPORT**. The system asks you to confirm the import.

6. From the ACTIVITY tab, you can view the status of the import. Click the refresh icon to update the import status. When the import is complete, click **VIEW**.



Recent Bulk Actions

Import and export files are stored on the server for 90 days, after which they are deleted automatically.

Activity	Type	Summary	Administrator	Timestamp	Status	Actions
Import	Add new users	1 user added	Mike Smith	4/22/2020 | 06:21:07 pm	Processed successfully	VIEW
Export	Users and Memberships	478 users exported	Mike Smith	4/22/2020 | 06:16:18 pm	Processed successfully	VIEW
Import	Add new users	1 user added	Mike Smith	4/22/2020 | 06:13:32 pm	Processed successfully	VIEW

Build a CSV to Bulk Add Users

Your CSV import file is made up of a header row with the column headers and a row of user or account data for each user you want to add to an account. Only new users can be imported. Any changes to existing users will be ignored. To make changes to existing users, see Bulk Update Users.

To ensure your CSV is properly formatted, use the Sample Bulk Add CSV file as a template.

The header row for add users

The first line of the file is the header row which defines each of the columns. The header values are not required to be in the order listed and are not case-sensitive, but the text must match listed values.

***Required columns:** Your CSV file must contain these columns: AccountID, FirstName, LastName, UserEmail, and eSignPermissionProfile. The rest of the header values are optional.

> **Note:** For the user's name, you can use either the FirstName and LastName columns together, or the User Name column. Your spreadsheet should only contain one of these; if both FirstName/LastName and UserName columns are present in your CSV, the values entered in the UserName column take precedence.

The EnableCLM and CLMPermissionProfile columns are only applicable for organizations with the CLM product.

> **Note:** The LoginPolicy and AutoActivation columns only apply to organizations with a reserved domain and Single Sign-On (SSO) through an Identity Provider. For more information, see the DocuSign Single Sign-On Overview.

The acceptable column header values for an Add Users CSV file are:

Header Row Value	Description
AccountID	The 32 character API Account ID of the user's account in your organization. This can be found in the in the API and Keys section of the account. **Required column**.
AccountName	The name of the user's account in your organization. The account name must match the Account ID provided.

Header Row Value	**Description**
FirstName	The user's first name. **Required column**.
LastName	The user's last name. **Required column**.
UserName	The user's full name. This can be used instead of FirstName and LastName. This is useful for languages which place family names before given names. *****Required column.** If this column is used instead of FirstName and LastName, it is required.
UserEmail	The user's complete email address. **Required column**.
eSignPermissionProfile	The user's permission profile for the eSignature product. This value must match an existing permission profile for the account. This value is not case-sensitive.**Required column**.
EnableCLM	Grants the user access to the CLM product. If you grant a user access to CLM, you must also assign them a Permission profile for that product with the CLMPermissionProfile column. • TRUE - The user has access to CLM. • FALSE - The user does not have access to CLM.
CLMPermissionProfile	The user's permission profile for the CLM product. This value must match an existing permission profile for the account. This value is not case-sensitive. If you assign a user a CLM permission Profile, you must also grant them access to the CLM product with the EnableCLM column.
UserTitle	The user's job title.
CompanyName	The user's company name.
Group	The user's assigned groups. The Group values must match existing Group names for the account. Additional Group columns can be added to the file to add users to more than one group. You do not need to add users to the Everyone group, since all new users are automatically added to that group.
AddressLine1	The user's address - first line.
AddressLine2	The user's address - second line.
City	The user's city name.
StateRegionProvince	The user's regional location.
PostalCode	The user's postal code.
Phone	The user's phone number.

Header Row Value	Description
Language	The user's display language for their DocuSign account. See the list of language codes below.
LoginPolicy	The user's login policy. Valid values include the following: • Column left blank - The user is created with no policy assigned. • FedAuthRequired - The user must log in with an Identity Provider. • FedAuthBypass - The user may log in with an Identity Provider or their DocuSign username and password. For more information on login policies, see Setting a User Login Policy.
AutoActivate	For domain users, new users can be activated automatically for domain accounts using SSO by setting the value to TRUE. The user is activated automatically once the import is complete. Memberships activated in this way will not receive an activation email.

The access code option (adding an access code for authentication during user activation) cannot be used with this bulk action.

The user data

In the lines of the file below the header row, add the user information with commas used as the delimiter (separator) between each value.

If you are using Microsoft® Excel® to create your file, you can enter the header values (FirstName, LastName, UserEmail, etc.) in different columns on the first line, enter the user information on subsequent lines, and save the file as a CSV file. You do not need to add commas; Excel will automatically do this when you save the file.

Example Add Users - Excel:

	A	B	C	D	E	F
1	AccountID	AccountName	APIUserName	FirstName	LastName	UserEmail
2	8d4e68a3-d666-44b8-82c3-0011fbe8315e	Purchasing	42dabc1b-a9a0-477c-8079-4cf8aba0e017	Hans	Moleman	h.moleman@example.com
3	8d4e68a3-d666-44b8-82c3-0011fbe8315e	HR Department	14e68a20-69f3-47b9-8bdd-33686c6c5666	Frank	Grimes	f.grimes@example.com
4	8d4e68a3-d666-44b8-82c3-0011fbe8315e	Sales	78e9727b-1881-4681-8813-cee971e35d87	Mindy	Simmons	m.simmons@example.com

Display Language Values

The Language value is the default language for the user. The value can be any of the codes shown below:

Language = Code

- Chinese Simplified = zh_CN

- Chinese Traditional = zh_TW
- Dutch = nl
- English = en
- French = fr
- German = de
- Italian = it
- Japanese = ja
- Korean = ko
- Portuguese = pt
- Portuguese Brazil = pt_BR
- Russian = ru
- Spanish = es

Bulk Update Users

Note: This guide is for DocuSign administrators who oversee multiple accounts. For administrators of individual accounts, see the DocuSign eSignature Admin guide, User Bulk Actions.

DocuSign Administrators and Users Administrators can bulk update existing users across one or more accounts by uploading a comma-separated value (CSV) file. For more information on the CSV format, see Building a CSV.

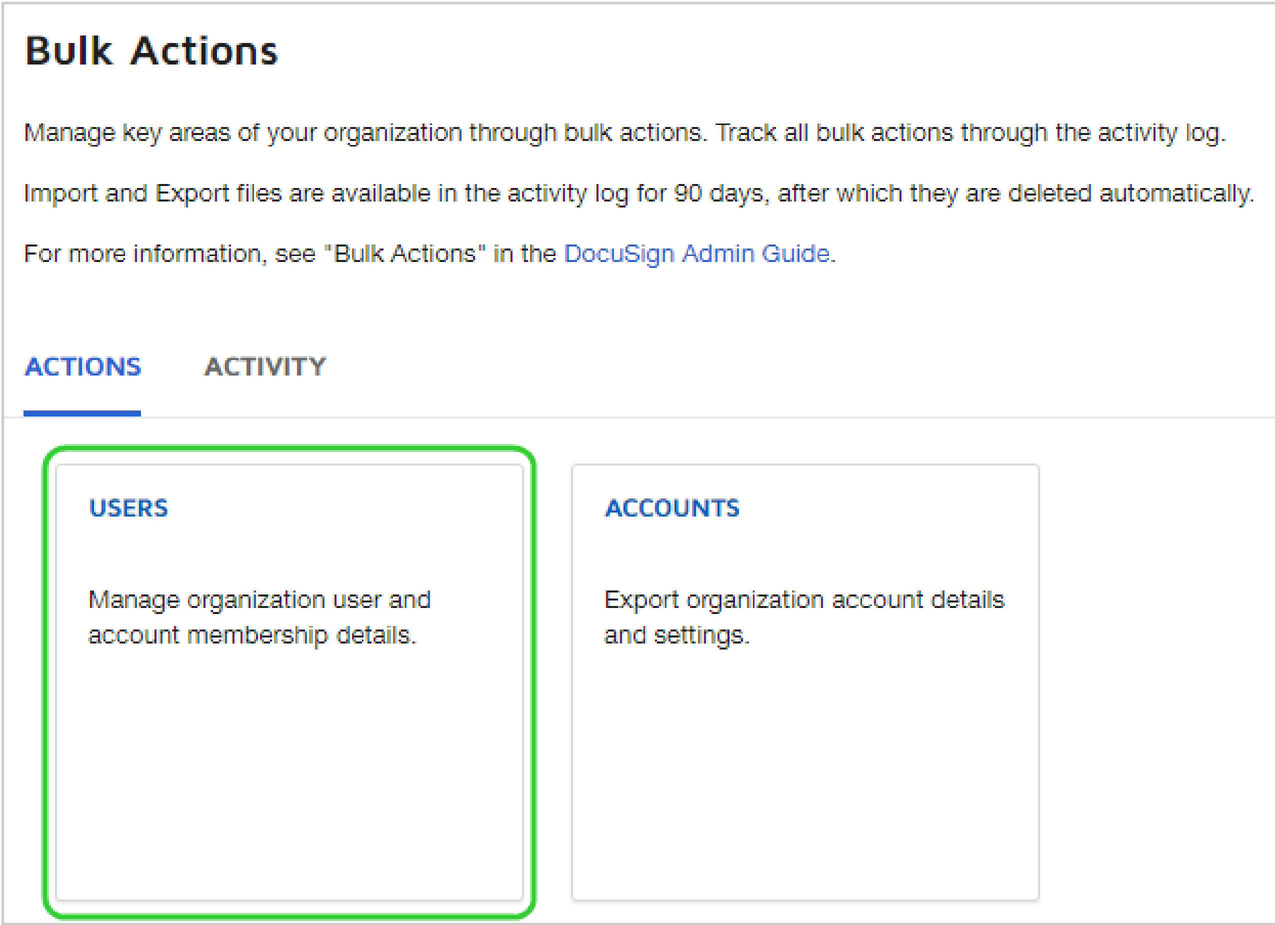
You can update up to 2,000 users on an account and include up to 50 accounts per imported CSV. The maximum number of updated users per import is 8,000.

Note: DocuSign administrators with a claimed domain can also update email addresses for users on their domain. For more information, see Updating user email addresses.

Update Multiple Users with Bulk Actions

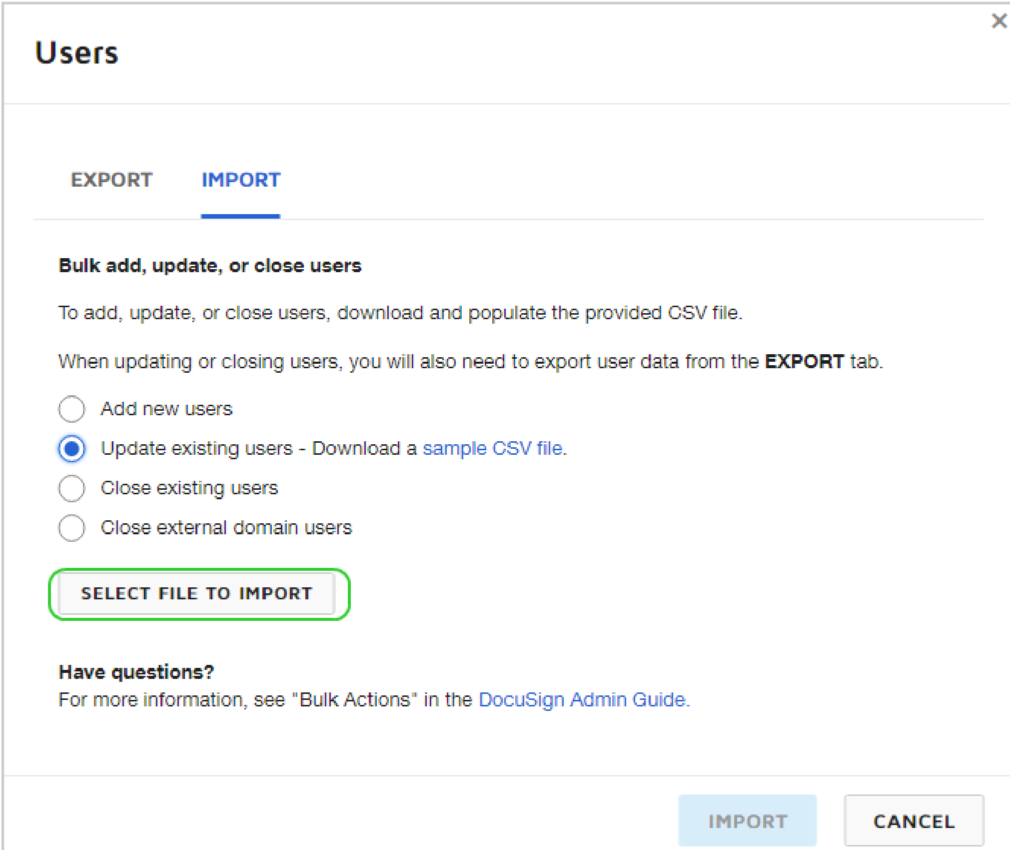
1. From the DocuSign Admin dashboard, click the **Bulk Actions** tile.

2. Click the **USERS** tile.



3. In the Users dialogue, click to select the **IMPORT** tab.

4. Select **Update existing users**, then click **SELECT FILE TO IMPORT**.



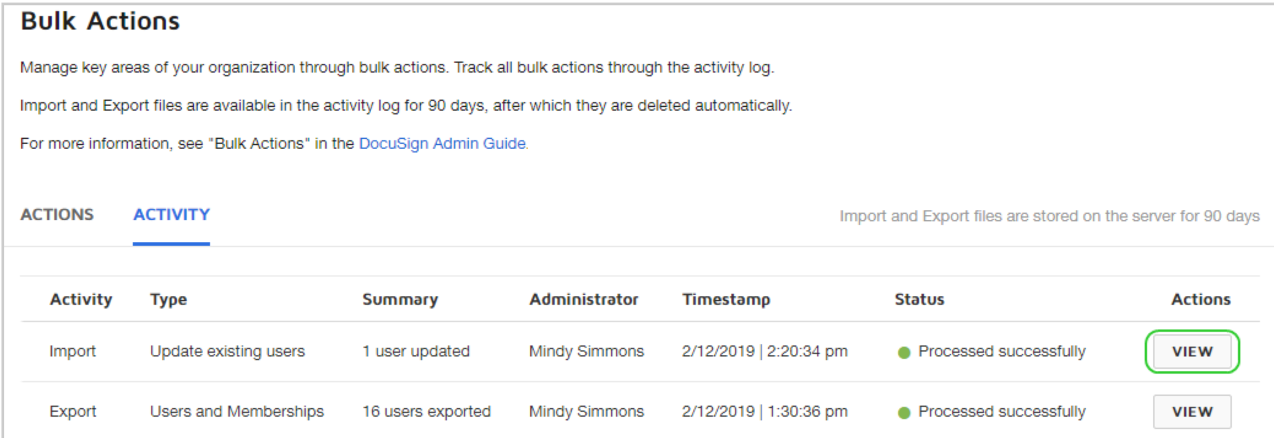
Select the CSV file to import. Make sure the formatting matches the sample CSV provided. For more details, see Building a CSV.

5. Click **IMPORT**. The system asks you to confirm the import.

- Click **CONFIRM** to continue
- Click **CANCEL** to replace the file or cancel the upload process

Note: Only one type of import or export can be in progress at a time.

6. From the ACTIVITY tab, you can view the status of the import. Click the refresh icon to update the import status. When the import is complete, click **VIEW**.



Build a CSV to Bulk Update Users

Your CSV import file is made up of a header row with the column headers and a row of account and user data for each user you want to update. Only existing users will be updated; to add new users, see bulk adding users.

Tip: To start, export a user list from accounts within your organization. The user data in this list can be used to populate your bulk update CSV file.

To ensure your CSV is properly formatted, use the Sample Bulk Update CSV file as a template.

The header row for update users

The first line of the file is the header row which defines each of the columns. The header values are not required to be in the order listed and are not case-sensitive, but the text must match listed values.

Note: If you're changing a user's name, use either the FirstName and LastName columns together, or the User Name column. Your spreadsheet should only contain one of these.

***Required columns**: Your CSV file must contain these columns: AccountID, APIUserName, and UserEmail. The rest of the header values are optional.

Note: All of the required columns must remain unchanged.

The acceptable column header values for an Update Users CSV file are:

Header Row Value*	Description
AccountID	The 32 character API Account ID of the user's account in your organization. **Required column**.
AccountName	The name of the account.
APIUserName	The unique user ID. **Required column**.
FirstName	The user's first name.

Header Row Value*	Description
LastName	The user's last name.
UserName	The user's full name.
UserEmail	The user's complete email address. To update the user's email address, use the UpdatedUserEmail column. **Required column**.
eSignPermissionProfile	The user's permission profile for the eSignature product. This value must match an existing permission profile for the account. This value is not case-sensitive.
EnableCLM	Grants the user access to the CLM product. If you grant a user access to CLM, you must also assign them a Permission profile for that product with the CLMPermissionProfile column. • TRUE - The user has access to CLM. • FALSE - The user does not have access to CLM.
CLMPermissionProfile	The user's permission profile for the CLM product. This value must match an existing permission profile for the account. This value is not case-sensitive. If you assign a user a CLM permission Profile, you must also grant them access to the CLM product with the EnableCLM column.
Language	The user's display language for their DocuSign account. See the list of language codes below.
UserTitle	The user's job title.
CompanyName	The user's company name.
AddressLine1	The user's address - first line.
AddressLine2	The user's address - second line.
City	The user's city name.
StateRegionProvince	The user's regional location.
PostalCode	The user's postal code.
Phone	The user's phone number.

Header Row Value*	**Description**
LoginPolicy	The user's login policy. Valid values include the following: • Column left blank = The user's login policy is updated to the Default for the domain. • FedAuthRequired = The user must log in with an Identity Provider. • FedAuthBypass = The user may log in with an Identity Provider or their DocuSign username and password. For more information on login policies, see Setting a User Login Policy.
Group (Used when adding users to groups)	The user's assigned groups. • Additional Group columns can be added to the file to add users to more than one group. • The Group values must match existing Group names for the account - one group per column. • No need to add users to the Everyone group, all users are automatically added to that group. **Note:** When the “Group” (singular) column is included in the CSV the “Groups” (plural) column is ignored.
Groups (Used when adding or removing users from groups)	The user's assigned groups. • The group values must match existing group names for the account using the following format: [Group 1],[Group2]. *One column per CSV*. • The system will add and/or remove the user from groups so that their list of groups matches the provided list. For example, if a user is in the ‘Everyone’ and ‘HR’ groups, to add them to the ‘Legal’ group, the cell should read [Everyone],[HR],[Legal]. • To remove the user from a group, delete that group from the cell. • Users cannot be removed from the Everyone group or the Administrators group. • No need to add users to the Everyone group, as all users are automatically added to that group.
UpdatedUserEmail	If updating domain user email addresses, use this column to enter the new email address. For more information see Updating user email addresses.

The user data

In the lines of the file below the header row, add the user information with commas used as the delimiter (separator) between each value.

If you are using Microsoft® Excel® to create your file, you can enter the header values (FirstName, LastName, UserEmail, etc.) in different columns on the first line, enter the user information on subsequent lines, and save the file as a CSV file. You do not need to add commas; Excel will automatically do this when you save the file.

Example Update Users - Excel:

	A	B	C	D	E	F
1	AccountID	AccountName	APIUserName	FirstName	LastName	UserEmail
2	8d4e68a3-d666-44b8-82c3-0011fbe8315e	Purchasing	42dabc1b-a9a0-477c-8079-4cf8aba0e017	Hans	Moleman	h.moleman@example.com
3	8d4e68a3-d666-44b8-82c3-0011fbe8315e	HR Department	14e68a20-69f3-47b9-8bdd-33686c6c5666	Frank	Grimes	f.grimes@example.com
4	8d4e68a3-d666-44b8-82c3-0011fbe8315e	Sales	78e9727b-1881-4681-8813-cee971e35d87	Mindy	Simmons	m.simmons@example.com

Update User Email Addresses

DocuSign Administrators and Users Administrators with a claimed domain can update email addresses for users on their domain.

You can update email addresses for your users if the following conditions are met:

- The organization has claimed the domain - for more information, see Domains.
- The user's email address is on the domain - for example, if your domain is www.example.com, the user's email would be user@example.com.
- If the organization has more than one claimed domain, you can also update the domain of the user to match another claimed domain.

> **Note:** You cannot change an email address for a user on a domain you have not claimed.

To change a user's email address, download and populate the sample CSV provided. The UserEmail column will remain unchanged and should contain the current user's email address.

In the UpdateUserEmail column, enter the new email address you'd like to use. After completing the import, the user's email address is updated.

Display Language Values

The Language value is the default language for the user. The value can be any of the codes shown below:

Language = Code

- Chinese Simplified = zh_CN
- Chinese Traditional = zh_TW
- Dutch = nl
- English = en
- French = fr
- German = de
- Italian = it
- Japanese = ja

- Korean = ko
- Portuguese = pt
- Portuguese Brazil = pt_BR
- Russian = ru
- Spanish = es

Bulk Close Users

> **Note:** This guide is for DocuSign administrators who oversee multiple accounts. This feature is not currently available for eSignature administrators. To close users on an individual account, see Manage Users.

DocuSign Administrators and Users Administrators can bulk close existing users across one or more accounts by uploading a comma-separated value (CSV) file. For more information on the CSV format, see Building a CSV.

If users created free or freemium accounts using a corporate email addresses, a DocuSign administrator may want to close these accounts. You can also bulk close these external domain accounts as long as they are not linked to an organization.

> **Note:** To learn more about managing domain users and other best practices, see Establish Control of your Company's DocuSign Agreements.

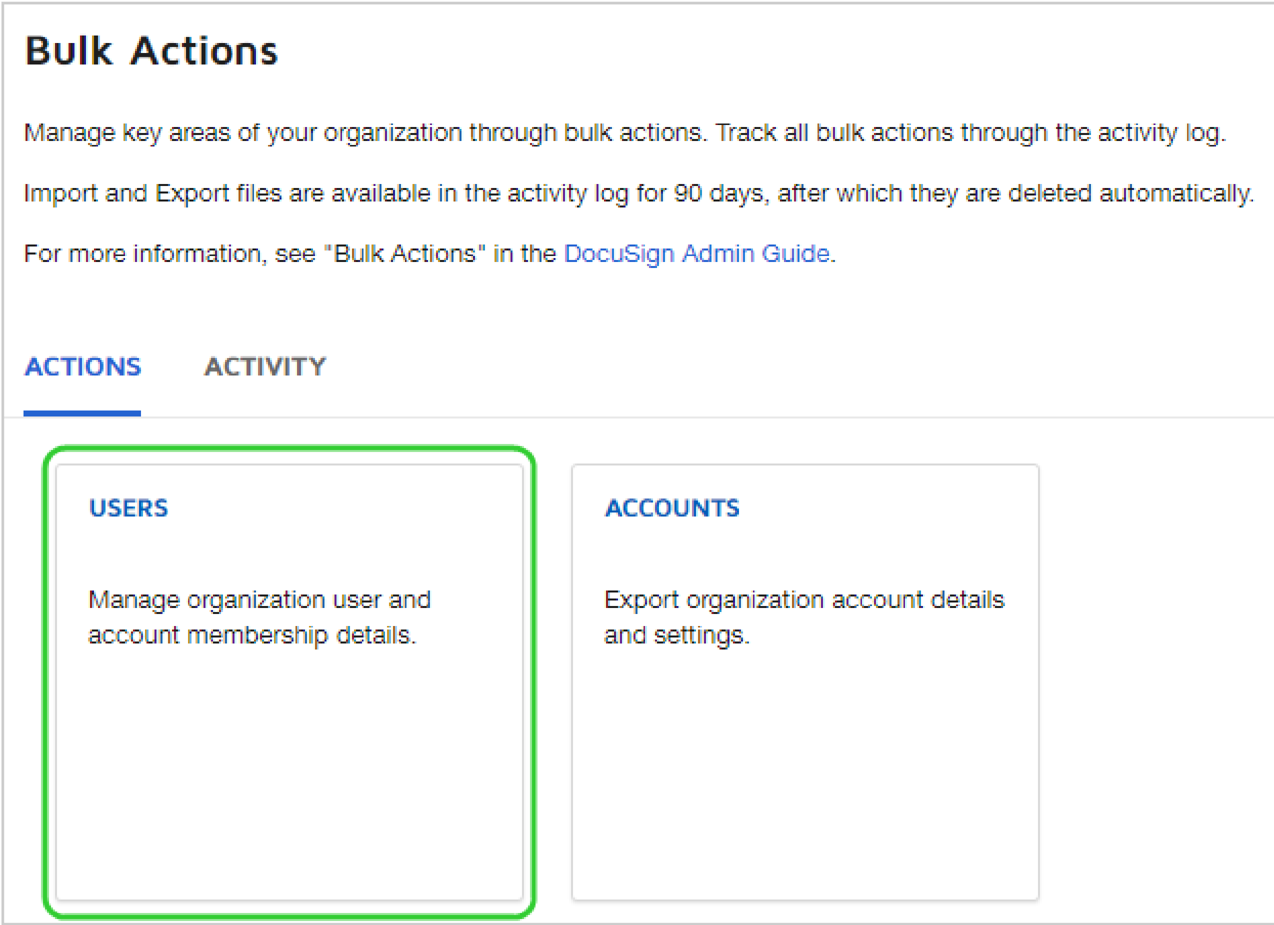
You can close up to 2,000 users on an account across up to 50 accounts per imported CSV. The maximum number of closed users per import is 8,000. When closing external domain users, you can close up to 2,000 users per site (NA1, NA2, EU, AU, etc.) with a single CSV.

CONTENTS

Close Organization Users

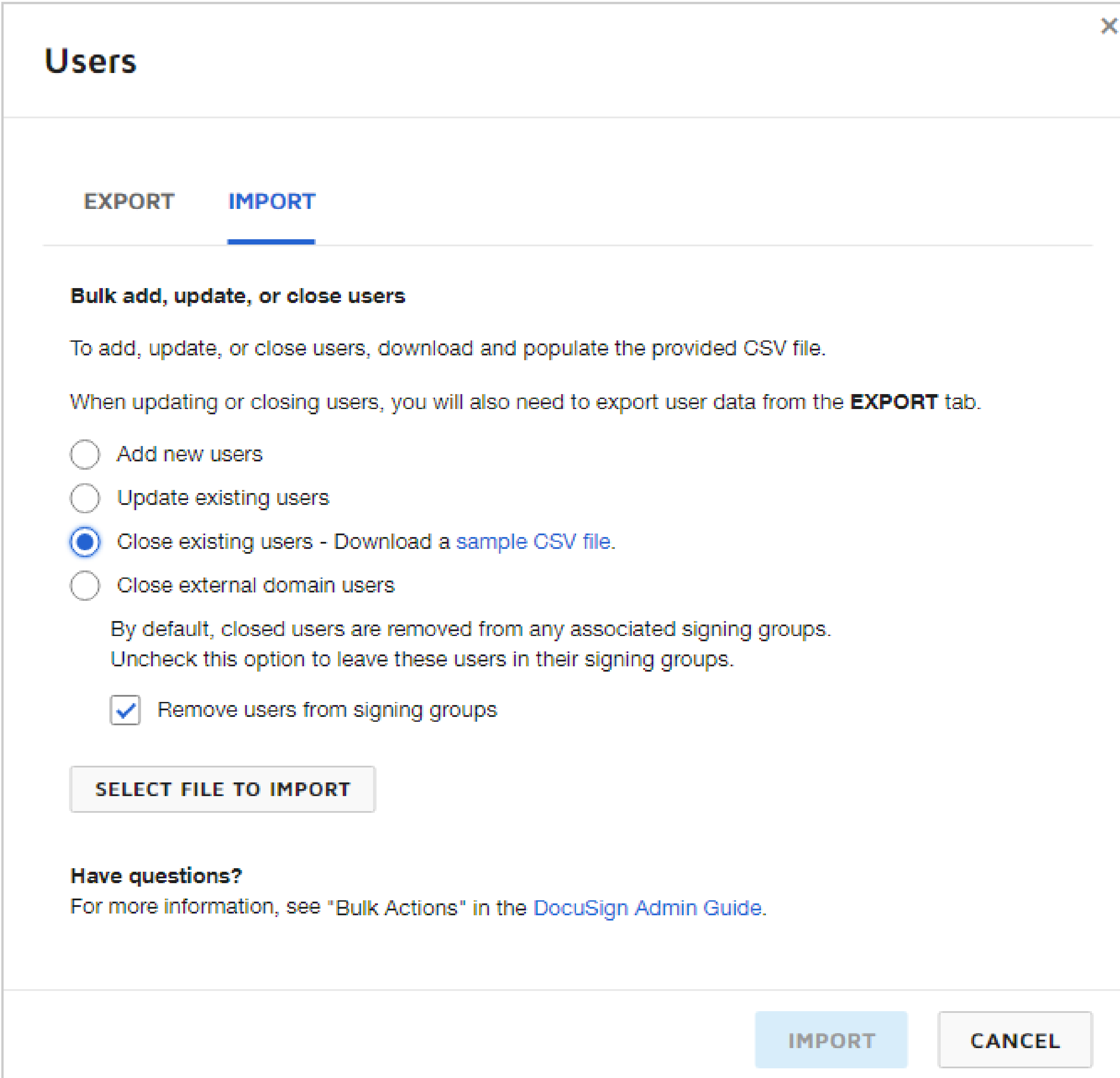
1. From the DocuSign Admin dashboard, click the **Bulk Actions** tile.

2. Click the **USERS** tile.



3. In the Users dialogue, click to select the **IMPORT** tab.

4. Select **Close existing users**.



5. (Optional) To remove the users from any signing groups they belong to, leave the **Remove users from signing groups** check box selected. If you leave them in signing groups, you can always edit the groups later to remove them. However, until you remove them, they can continue to receive any notifications sent to the signing groups they belong to.

6. Click **SELECT FILE TO IMPORT**.

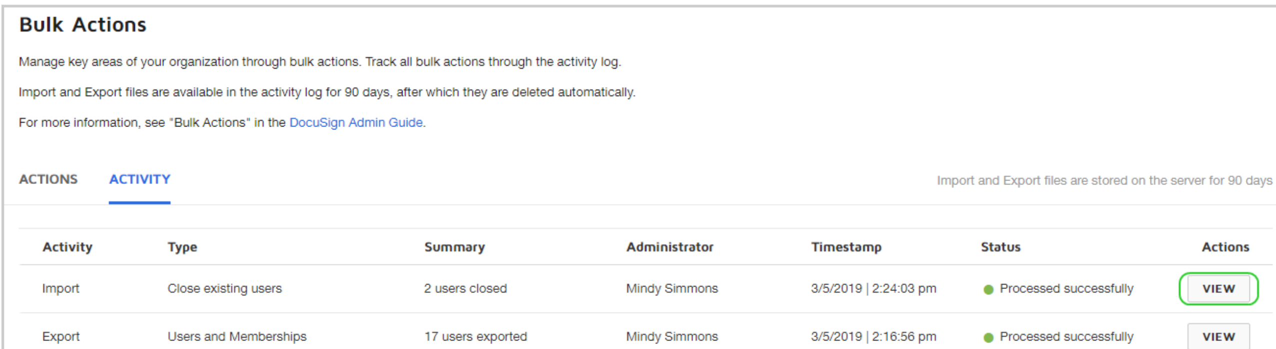
Select the CSV file to import. Make sure the formatting matches the sample CSV provided. For more details, see Building a CSV.

7. Click **IMPORT**. The system asks you to confirm the import.

- Click **CONFIRM** to continue
- Click **CANCEL** to replace the file or cancel the upload process

> **Note:** Only one type of import or export can be in progress at a time.

8. From the ACTIVITY tab, you can view the status of the import. Click the refresh icon to update the import status. When the import is complete, click **VIEW**.



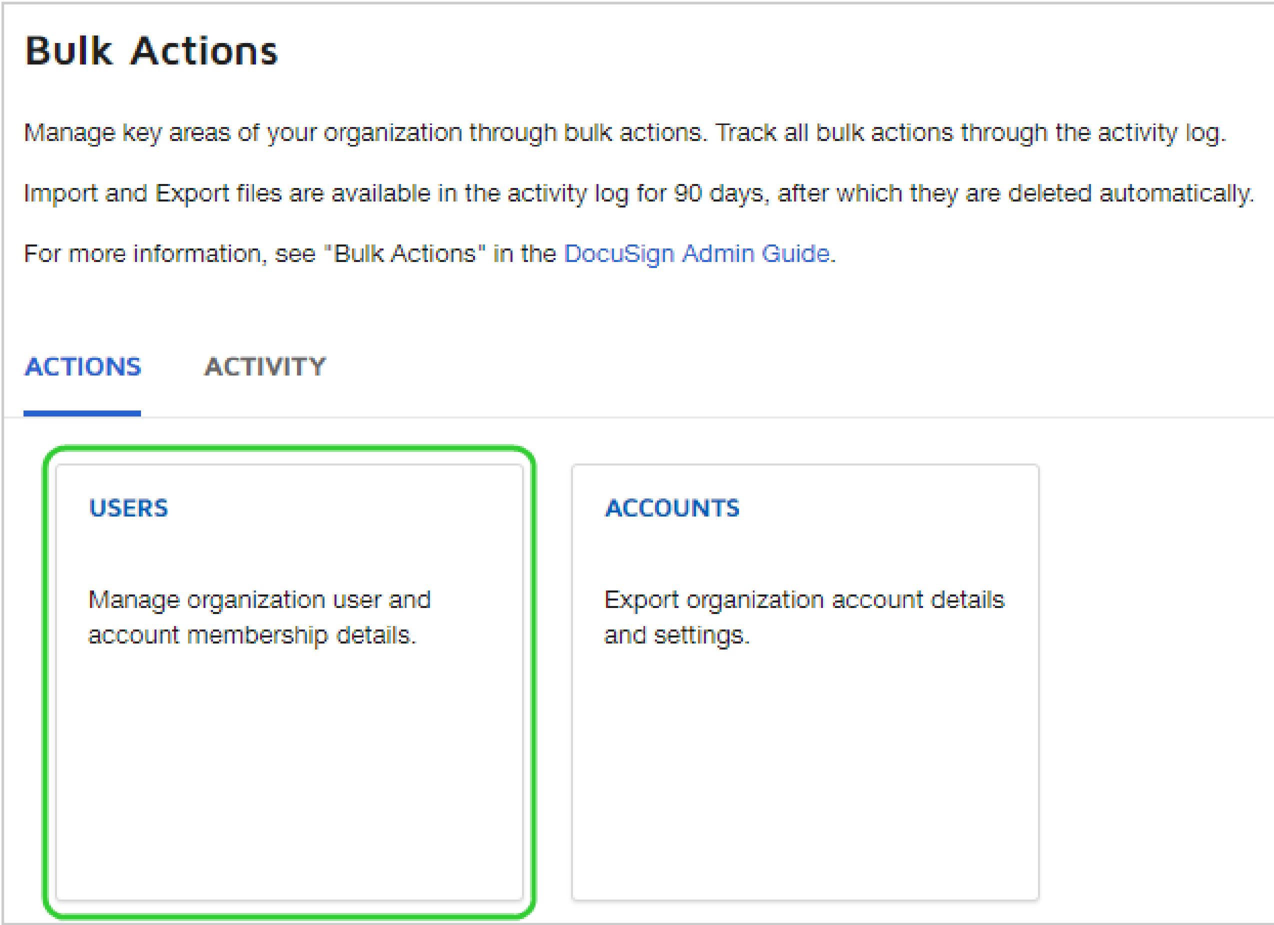
Close External Domain Users

In order to close an external domain user, the user must be on a free or freemium account that is not linked to an organization. A closed user will no longer have access to the account or any documents within the account.

> **Note:** You can close up to 2,000 external domain users per site (NA1, NA2, EU, AU, etc.) with a single CSV.

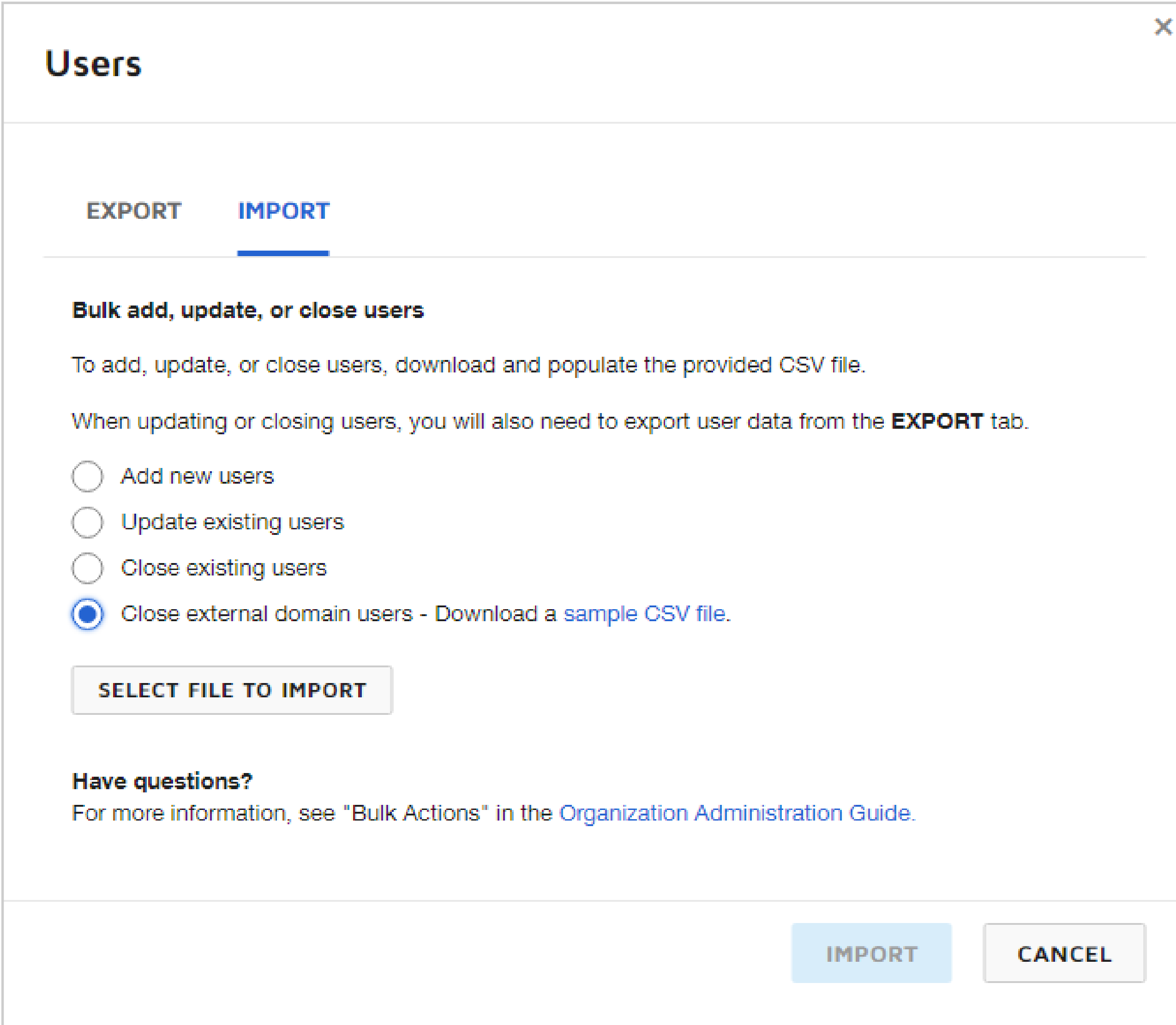
1. From the DocuSign Admin dashboard, click the **Bulk Actions** tile.

2. Click the **USERS** tile.



3. In the Users dialogue, click to select the **IMPORT** tab.

4. Select **Close external domain users**.



5. Click **SELECT FILE TO IMPORT**.

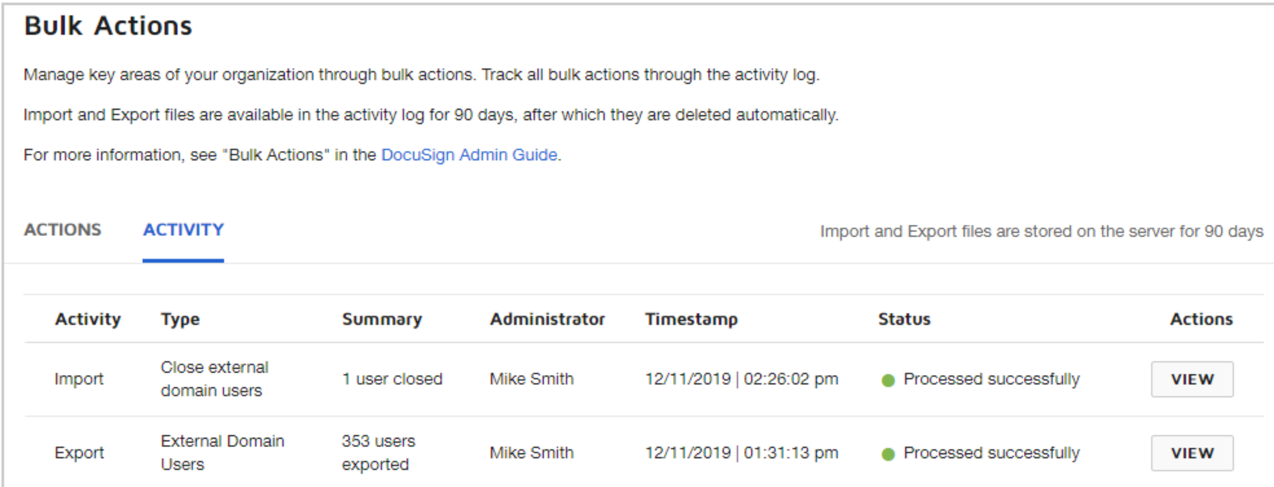
Select the CSV file to import. Make sure the formatting matches the sample CSV provided. For more details, see Building a CSV.

6. Click **IMPORT**. The system asks you to confirm the import.

- Click **CONFIRM** to continue
- Click **CANCEL** to replace the file or cancel the upload process

Note: Only one type of import or export can be in progress at a time.

7. From the ACTIVITY tab, you can view the status of the import. Click the refresh icon to update the import status. When the import is complete, click **VIEW**.



Build a CSV to Bulk Close Users

Your CSV file is made up of a header row with the column headers and a row of account and user data for each user you want to close.

Tip: Start by exporting a user list from your organization. The user data in this list can be used to populate your bulk close CSV file.

- For organization users, use the 'Users and Memberships' or 'Domain Users' export type.
- For external domain users, use the 'External Domain Users' export type.

To ensure your CSV is properly formatted, use the Sample Bulk Close CSV file as a template.

The header row for close users

The first line of the file is the header row which defines each of the columns. The AccountID column must be the first column in the file.

***Required columns:** Your CSV file must contain these columns: AccountID, APIUserName, and UserEmail. No other columns are necessary.

The acceptable column header values for a Close Users CSV file are:

Header Row Value*	Description
AccountID	The 32 character API Account ID of the user's account in your organization. **Required column**.
APIUserName	The unique user ID. **Required column**.
UserEmail	The user's complete email address. **Required column**

The user data

In the lines of the file below the header row, add the user information with commas used as the delimiter (separator) between each value.

If you are using Microsoft® Excel® to create your file, you can enter the header values (AccountID, APIUserName, UserEmail) in different columns on the first line, enter the user information on subsequent lines, and save the file as a CSV file. You do not need to add commas; Excel will automatically do this when you save the file.

Account Settings Export

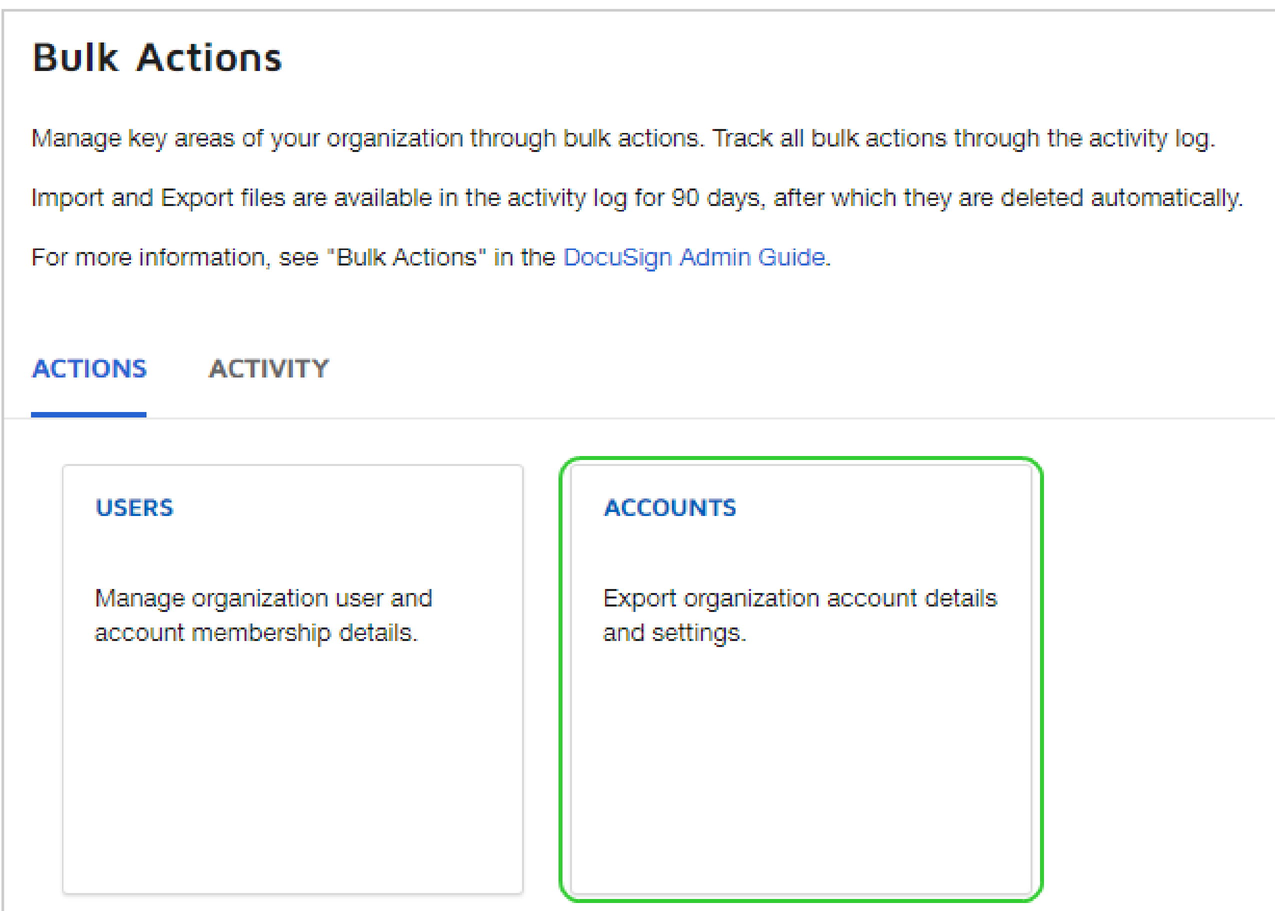
DocuSign administrators with the Administrator or Settings Administrator permission profiles can download and view all settings for eSignature accounts in the organization. This information can be used to compare settings across accounts and facilitate audits for compliance.

Exports are downloaded as a comma-separated value (CSV) file.

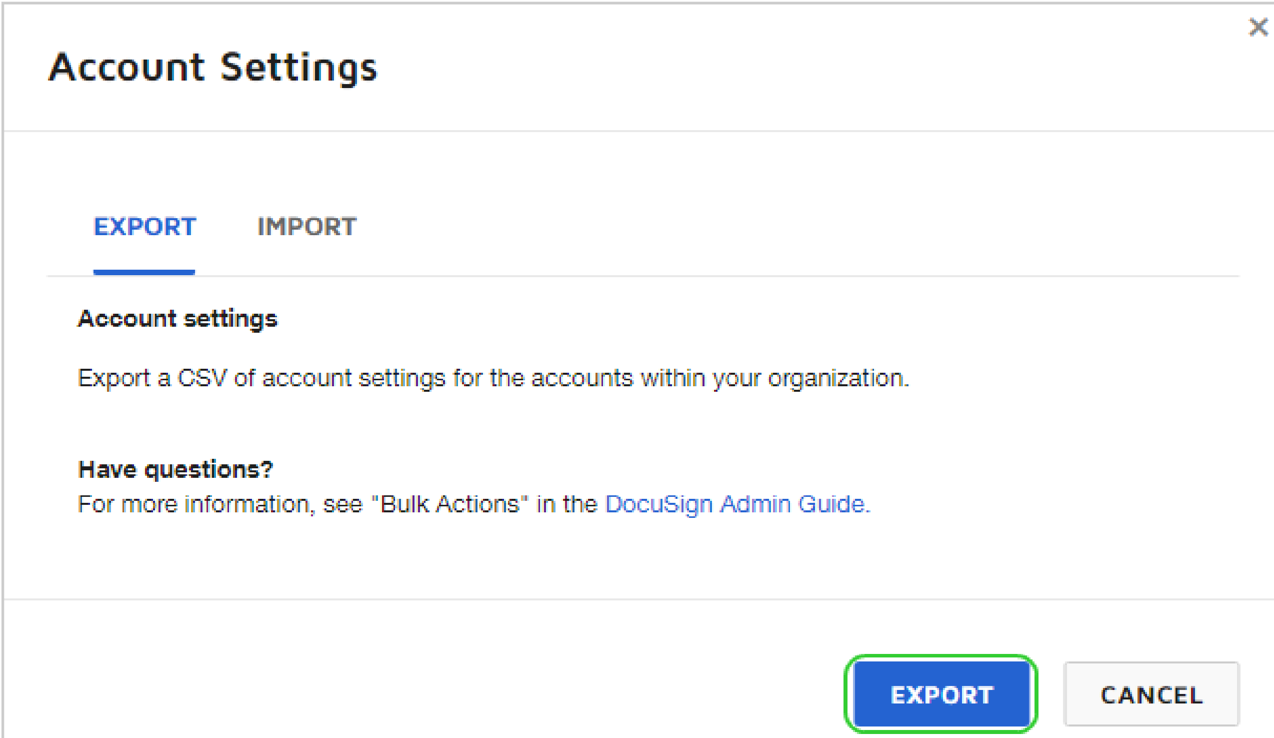
Export Account Settings

1. From the DocuSign Admin dashboard, click the **Bulk Actions** tile.

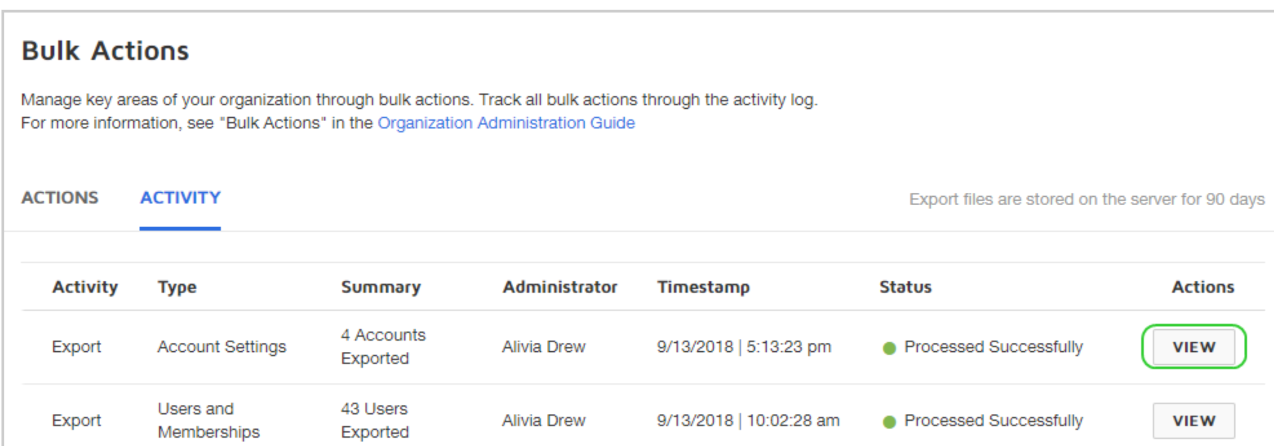
2. Click the **ACCOUNTS** tile.



3. Click **EXPORT**.

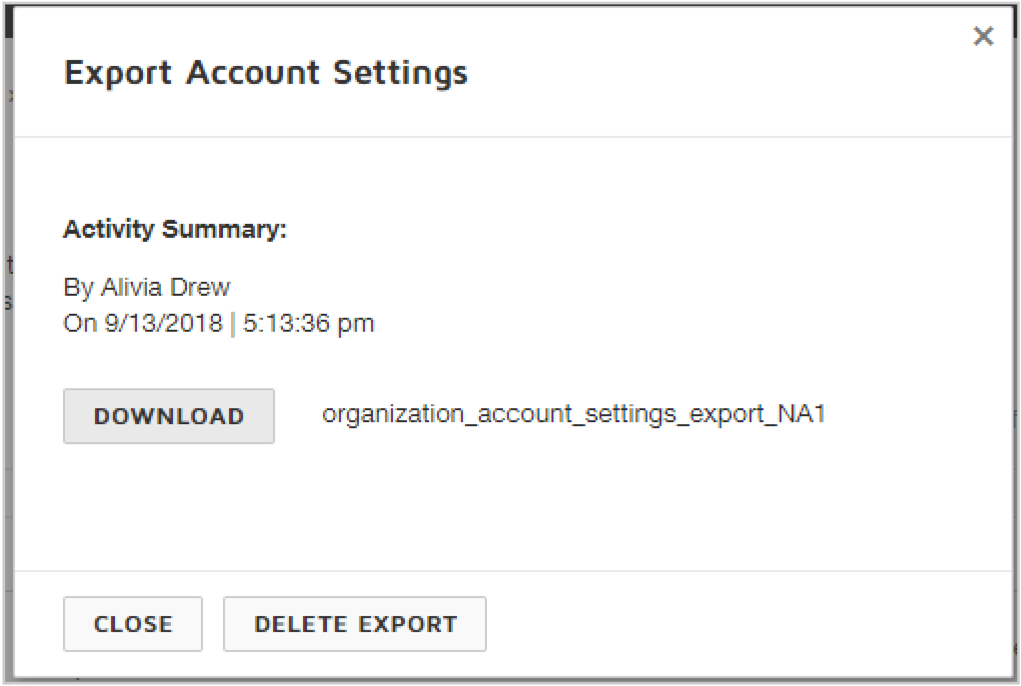


4. From the ACTIVITY tab, you can view the status of the export. Click the refresh icon to update the export status. When the export is complete, click **VIEW**.



Note: Only one type of import or export can be in progress at a time.

5. Click **DOWNLOAD** to download the export CSV. When finished, click **CLOSE**.



If your organization has accounts you do not want to export, export all accounts and remove rows for any additional accounts.

Your organization can store a combination of up to 100 account settings exports and user exports at a time. Both are retained for 90 days. To manually delete exports, click **DELETE EXPORT**, then click **DELETE**.

Account Settings Import

Note: This guide is for DocuSign administrators who oversee multiple accounts. This feature is not available for individual eSignature accounts.

DocuSign administrators with the Administrator or Settings Administrator permission profiles can import updated account settings for one or more eSignature accounts by uploading a comma-separated value (CSV) file. This is useful for making organization-wide changes to specific account settings and replicating settings across multiple accounts. It can also be used to clone account settings from the DocuSign Demo environment to accounts in Production.

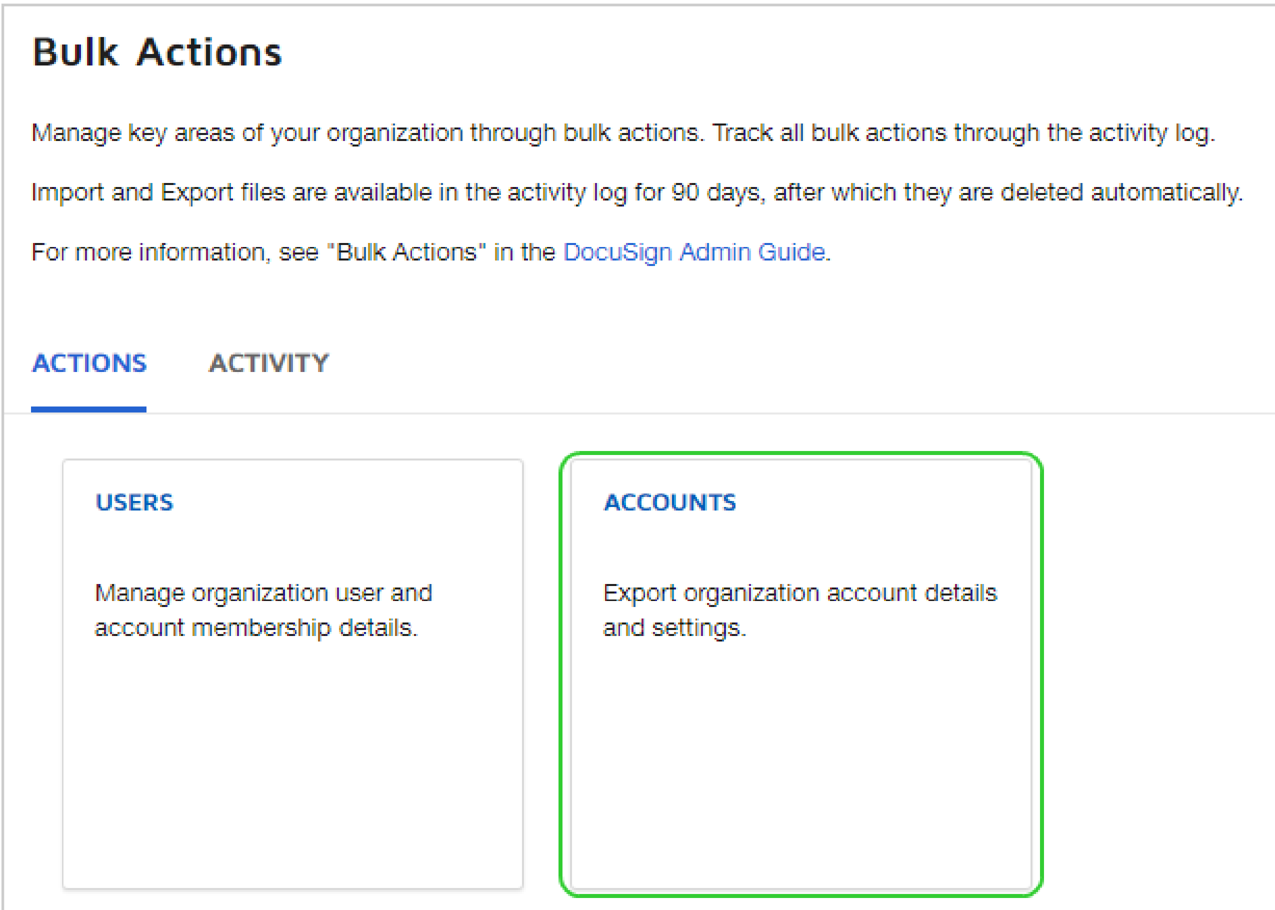
You can import settings for up to 40 accounts at a time.

Note: Export a CSV of settings for the accounts you want to modify by using Account Settings Export. With that file as a template, you can update and import the new settings. For more information on the CSV format, see Preparing a CSV.

Update Multiple Accounts Using Account Settings Import

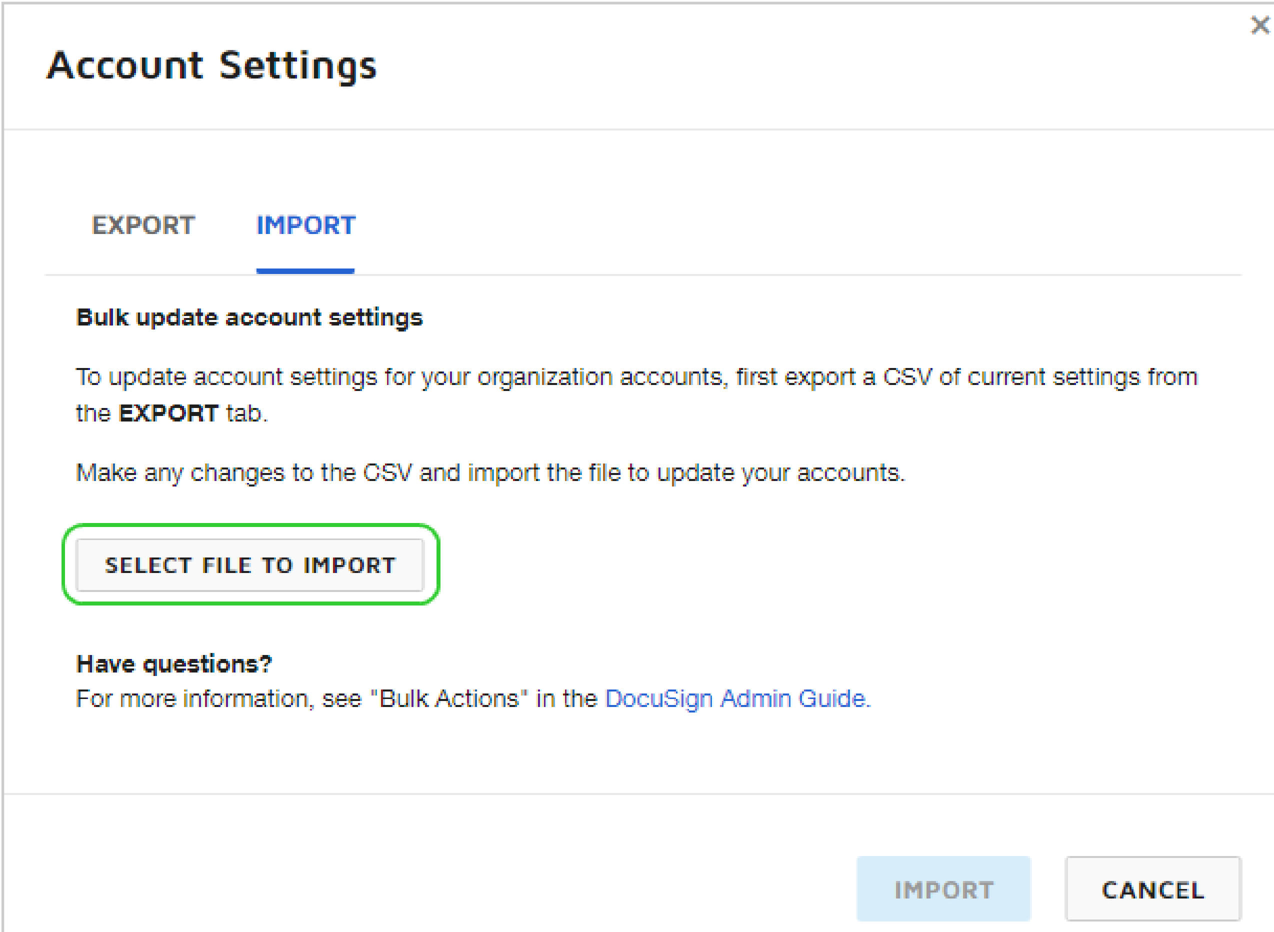
1. From the DocuSign Admin dashboard, click the **Bulk Actions** tile.

2. Click the **ACCOUNTS** tile.



3. In the Accounts dialogue, click the **IMPORT** tab.

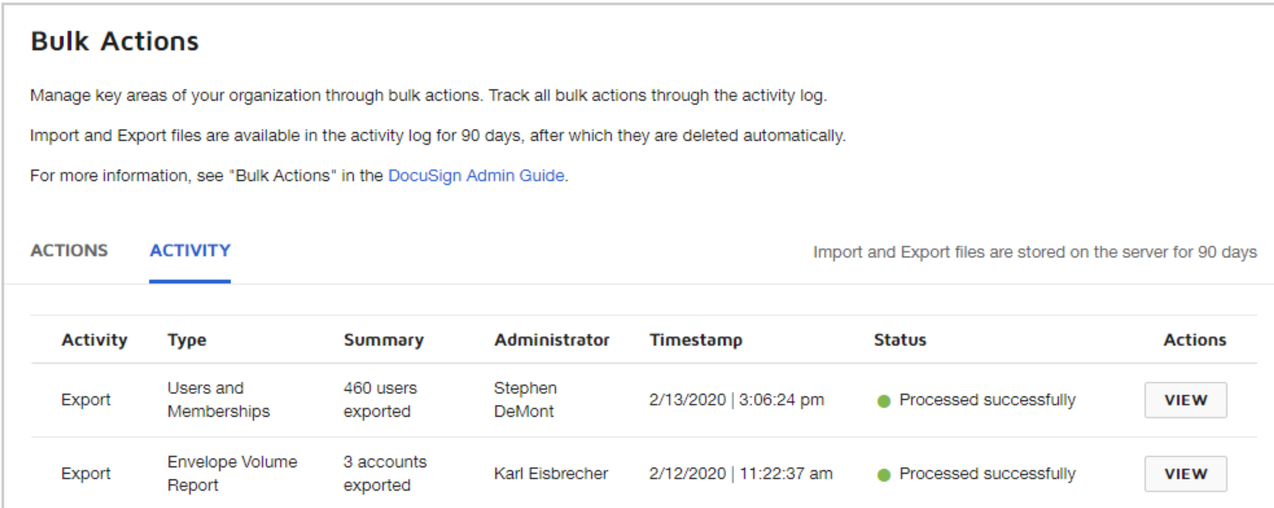
4. Click **SELECT FILE TO IMPORT**.



Select the CSV file to import. For more details on preparing an import, see Preparing a CSV.

5. Click **IMPORT**. The system asks you to confirm the import.

6. From the ACTIVITY tab, you can view the status of the import. Click the refresh icon to update the import status. When the import is complete, click **VIEW**.



Prepare a CSV for Account Settings Import

Your CSV import file is made up of a header row with three standard column headers and additional columns for each account. The rows of the CSV contain the settings available for your accounts and their values.

Because accounts and account plans differ, it is best to use an export of your accounts as a template.

To start, export a CSV of settings for the accounts you want to modify by using Account Settings Export. You can update settings for your accounts with the values provided in the settings mapping table.

The header row for account settings import

The first line of the file is the header row which defines each of the columns. The header values must be in the order listed.

Required columns: Your CSV file must contain these columns: Category, Key, and additional columns for any accounts to be updated. The Name column is optional and is provided for your information.

Each account listed must have the account name as the header, with the account number and the environment of the account (Demo or Production) below it.

	A	B	C	D	E
1	Category	Key	Name	Springfield Nuclear Purchasing	Springfield Nuclear HR
2				8675309	8675308
3				Demo	Demo
4	Comments	EnableSigningExtensionComments	Enable comments in envelopes sent from this account	FALSE	FALSE
5	Comments	CommentEmailShowMessageText	Include comment text in email notifications when a comment is posted	FALSE	FALSE

Note: When importing settings from demo accounts to production accounts, ensure that the account name, account ID, and environment are correct before uploading the file.

Account settings rows and their values

To view all potential account settings and their values, download the settings mapping table.

The table uses single quotation marks to distinguish various values; when changing a value on your import CSV, remove the quotation marks.

> **Note:** Because account plans differ, some of the settings displayed in this file may not appear on your account export. Contact DocuSign customer support with any questions.

There are three types of settings : Boolean, numeric, and text value.

Boolean: This setting can be enabled 'TRUE' or disabled 'FALSE.' It will only accept one of those two setting values.

Category	Key	Name	Value
Comments	EnableSigningExtensionComments	Enable comments in envelopes sent from this account	'TRUE' or 'FALSE'

Numeric: This setting must be a number. The range of numbers available for each setting is listed in the settings mapping table.

Category	Key	Name	Value
Security Settings	SessionTimeout	Web App Session Timeout (minutes)	A numeric value from 1-120 minutes - e.g. for 30 minutes, '30'

Text Value: This setting must be a text string. The string must match one of the text values listed in the settings mapping table, including any underscores.

Category	Key	Name	Value
Security Settings	SignerLoginRequirements	Login Requirements	**Not Required to Login:** 'login_not_required' **Login Required if Signer Has an Account:** 'login_required_if_account_holder' **Account Required – Login Once Per Session:** 'login_required_per_session' **Account Required – Login for Each New Envelope:** 'login_required_per_envelope'

Organization Reporting

> **Note:** This guide is for DocuSign administrators who oversee multiple accounts. Administrators of individual eSignature accounts should review Using Reports - eSignature User Guide.

DocuSign administrators can generate a variety of reports for envelope, user, and group activity. These reports can be run on any accounts in the organization. Data can be pulled from up to a year prior to the report date. Reports are exported in a CSV file with separate rows for each account and labeled columns containing the report results. Reports can be generated from the beginning of the previous year. A report can have a custom date range of up to a year at a time.

Report Types

> **Note:** If you do not see these reports in your organization, they may not be enabled. Contact DocuSign customer support for more information.

Organization reporting allows you to perform standard, account-level reports at the organization level. Each report is broken down per account, with multiple accounts in a single report. For more information on the contents of these standard reports, see our list of standard reports.

The following report types are available in DocuSign Admin:

- **Envelope Report:** Information on envelopes sent from all accounts.
- **Envelope Volume Report:** Envelope status totals for a specified time period
- **Envelope Recipient Report:** Sender and recipient information on sent envelopes
- **Envelope Status Report:** Totals based on envelope status
- **Envelope Velocity Report:** Totals based on envelope completion time
- **Recipient Activity Report:** Recipient activity on all sent envelopes

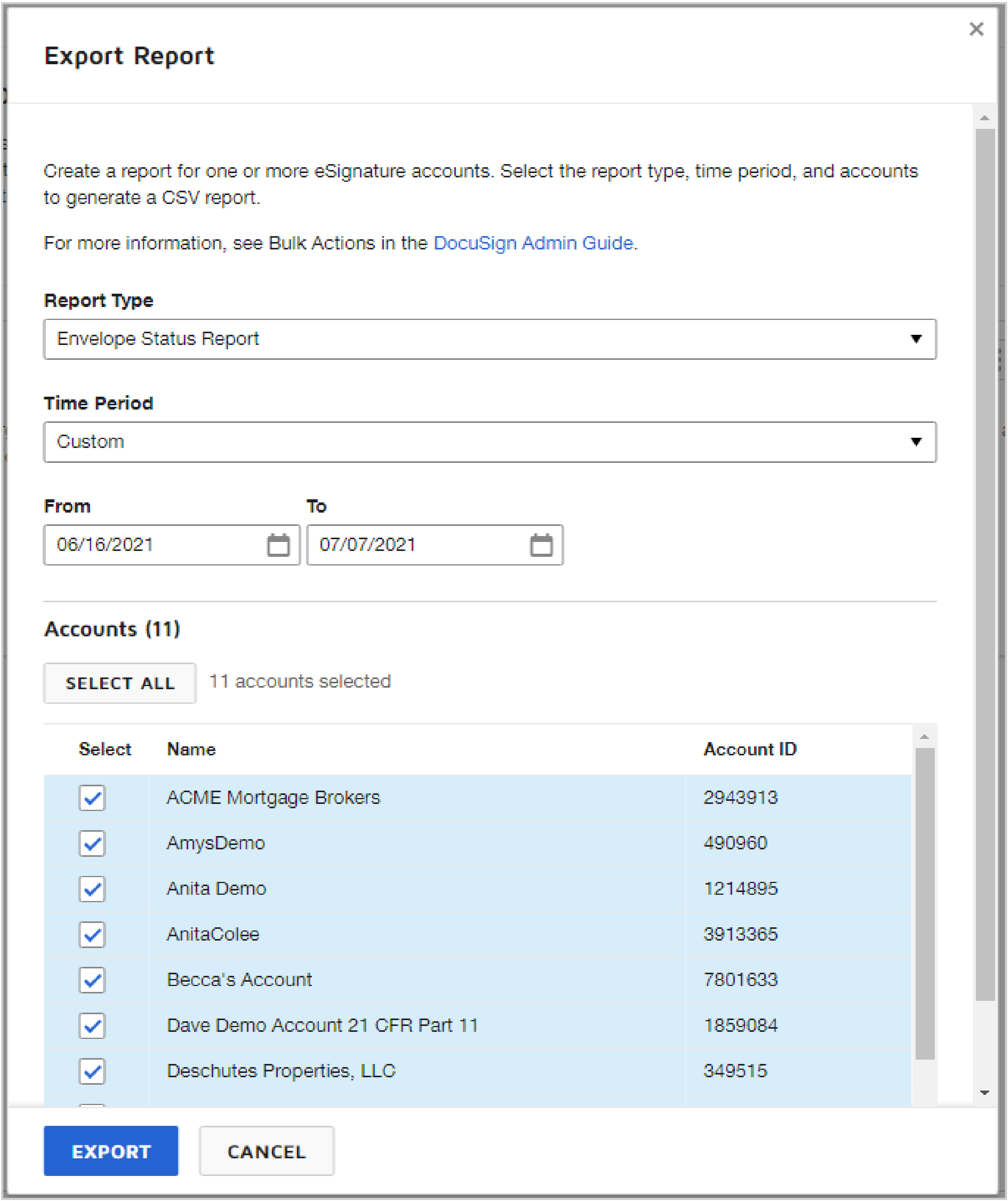
- **User Activity Report:** User activity across all accounts
- **Group Activity Report:** Activity broken down by group
- **Account Activity Report:** Summary of user, envelope, and template data across all accounts
- **Envelope Identity Verification Report:** Recipient, sender and authentication data on all envelopes sent across all accounts
- **Purged Envelope Report:** List of purged envelopes by envelope ID across all accounts
- **Account Authentication Report:** Summary authentication activity and results across all accounts
- **SMS Delivery Usage Report:** Envelope delivery by SMS for a specified time period across all accounts
- **Account Identity Verification Report:** Authentication attempts by category and type across all accounts
- **ID Verification Attempt Report:** Summary of ID verification attempted by recipients across all accounts
- **ID Verification for Standards-based Signatures Report:** ID verification attempts when using digital signature across all accounts
- **Template Report:** Overview of templates created across all accounts

Export an Organization Report

1. From the DocuSign Admin dashboard, click the **Bulk Actions** tile.
2. On the **ENVELOPE REPORTS** tile, select , then select **Export Report**.
3. Select the report type and the accounts you'd like to report on.

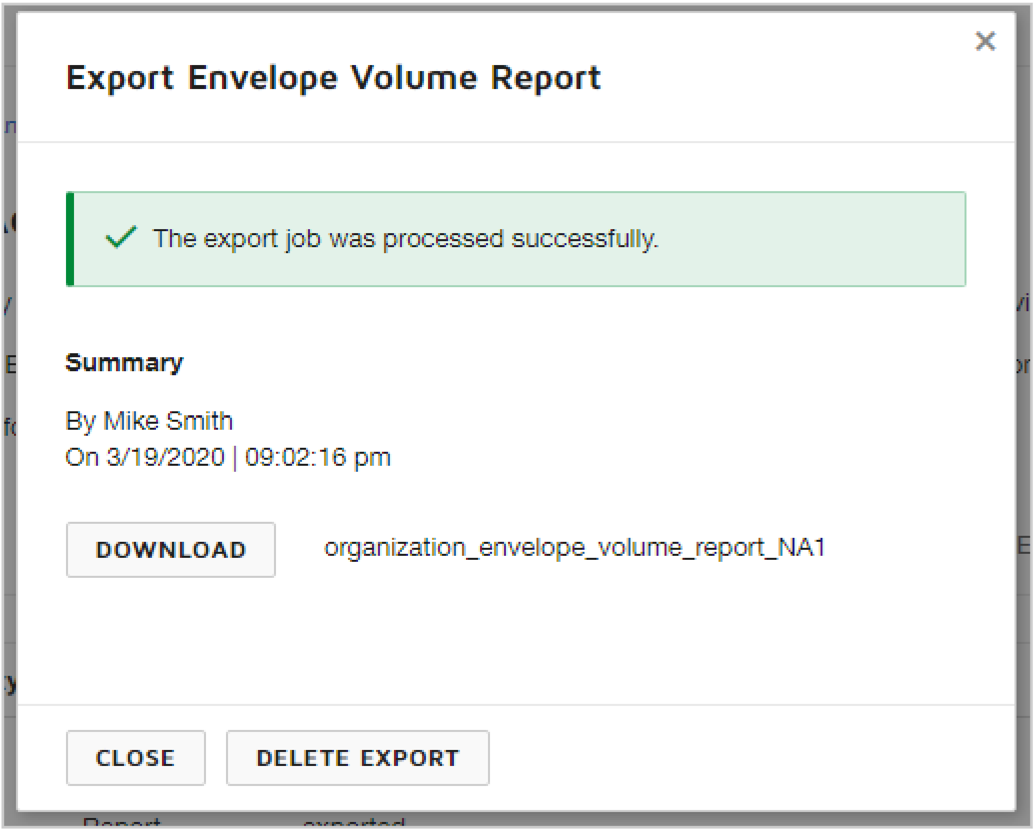
4. Select the time period you'd like to report on, then click **EXPORT**.

Note: Return up to 90 days of data at a time with a custom time period.



5. From the ACTIVITY tab, you can view the status of the report. Click the refresh icon to update the status. When the report is complete, click **VIEW**.

6. Click **DOWNLOAD** to download the report as a CSV file.



Accounts

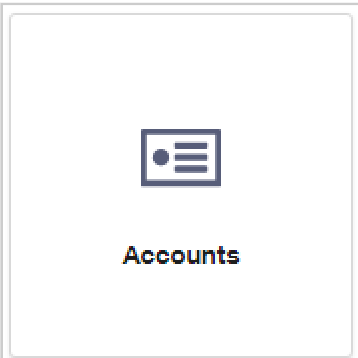
An organization is comprised of multiple DocuSign eSignature accounts. When you first create an organization, the account used in this process becomes the default account and is used for just-in-time provisioning of new users. You can consolidate management of the DocuSign eSignature accounts used across your company, and their users, by linking them to the organization.

You can also invite external domain accounts to link with your organization.

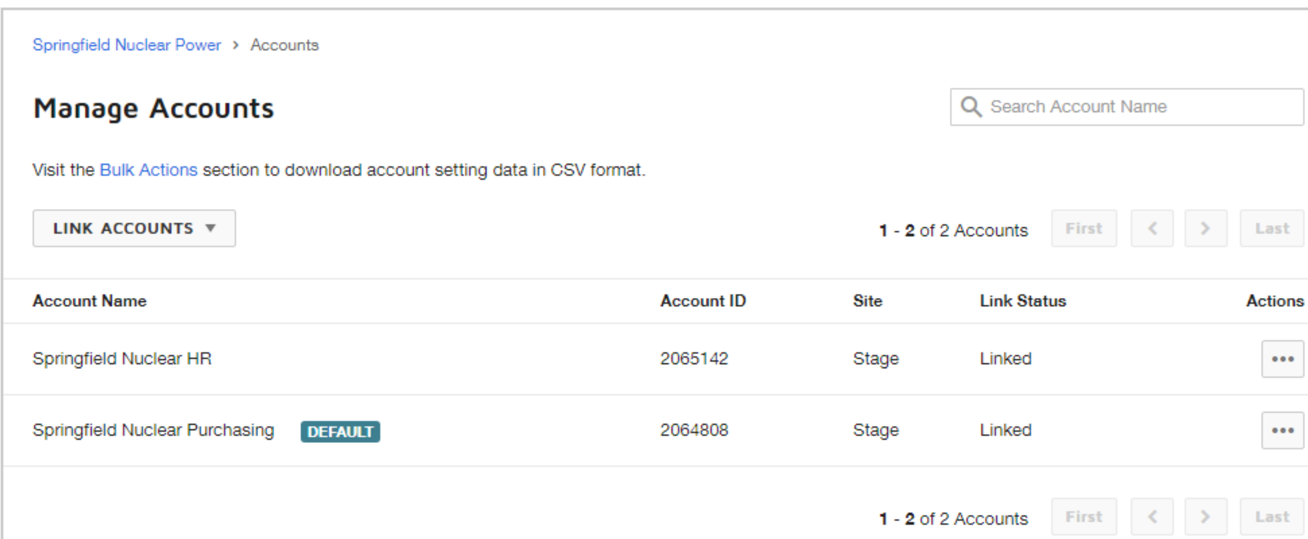
CONTENTS

View Organization Accounts

From the Accounts tile, you get a list of all the accounts that are part of the organization.



These are the accounts that take advantage of the SSO provisioning and identity management set up for your organization. The users in the accounts can all be viewed and managed through DocuSign Admin, and you can assign new account memberships to any account in the organization.



View and Compare Account Settings

A DocuSign administrator with either the Administrator or Settings permission profile can view and compare the settings for linked accounts.

You can search for settings by category or setting name and filter by matching or differing values.

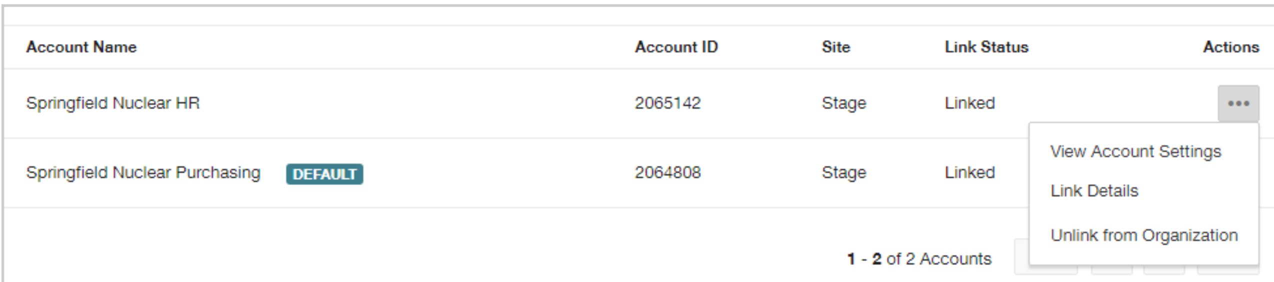
Note: If this feature is not available, it may not be enabled for your organization. Contact DocuSign customer support to enable this feature.

View and Compare Account Settings

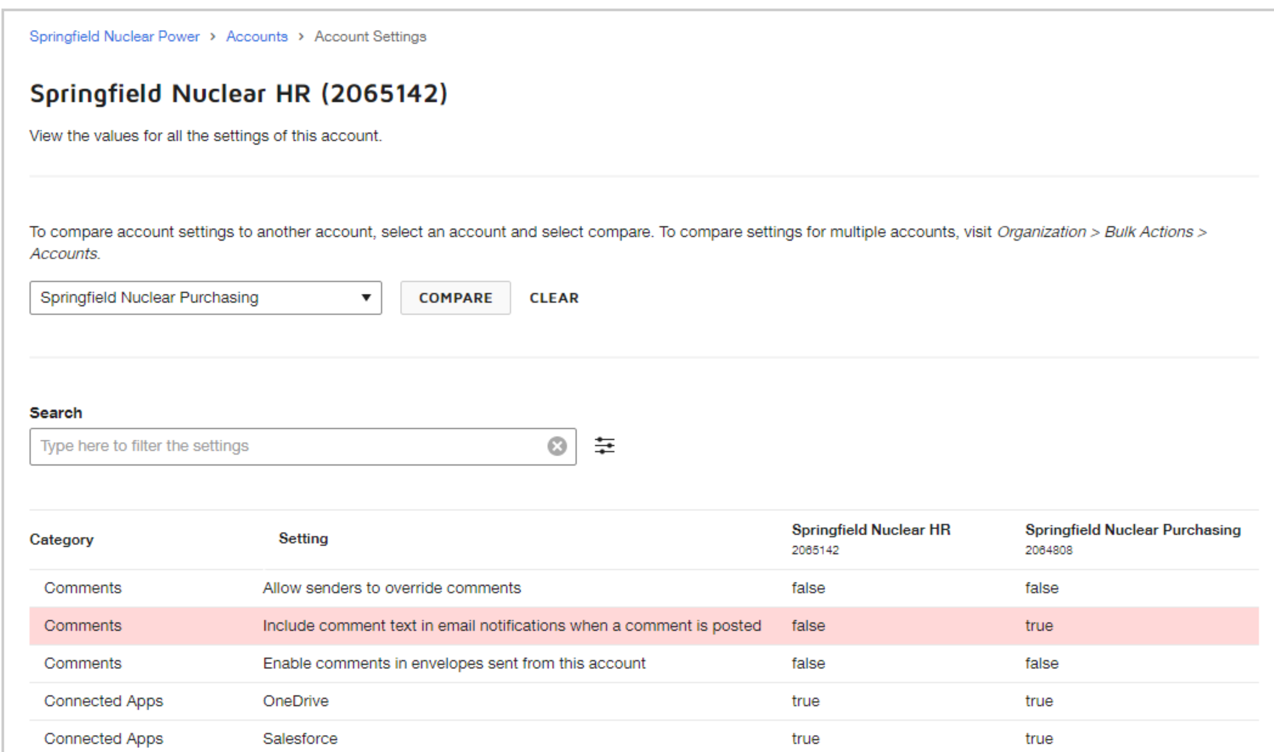
1. From the DocuSign Admin dashboard, click **Accounts**.

2. In the Manage Accounts list, locate the account you want to view by searching or scanning the list.

3. Click the Actions menu for the account select **View Details.**



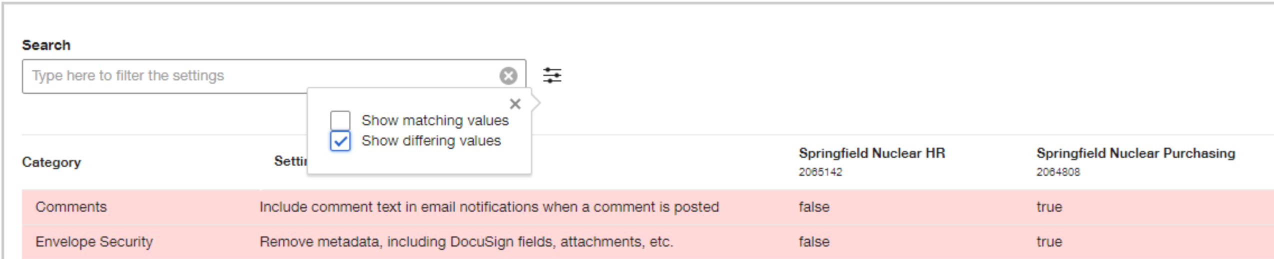
4. Select the account you want to compare from the drop-down list and click **COMPARE**. The settings for both accounts are displayed side by side. Settings that are different between the two accounts are highlighted in red.



5. Type a setting category or a setting name to filter the list of settings.

6. To search by only matching or differing values, click the filters icon.

7. Select the filter you want to apply. The corresponding settings for both accounts are displayed.



Linking Accounts to an Organization

The DocuSign administrator can link and unlink accounts to the organization, allowing them to manage the accounts in their organization on their own, without any need to engage DocuSign Professional Services.

Linking accounts, along with SSO identity management, is the critical activity in building out an organization. When you link accounts, you gain the following:

- **Builds the user base for management.** Users in linked accounts can be managed from the organization. Users can be granted memberships to multiple accounts in the organization.
- **SSO just-in-time provisioning**. When a user logs in using a reserved domain email, if they do not have an account membership on an account in the organization, then just-in-time provisioning creates an account for them in the default organization account.

Linking accounts allows your organization administrators to manage all account users with the centralized tools provided in DocuSign Admin.

> **Note:** You can also invite external domain accounts to link with your organization. To send an invitation, see Inviting external domain accounts to link.

Requirements for linking an account:

- You must be a DocuSign Administrator for your organization
- You must have full eSignature Administrator permissions on the account to be linked
- The account must not already be linked to an organization

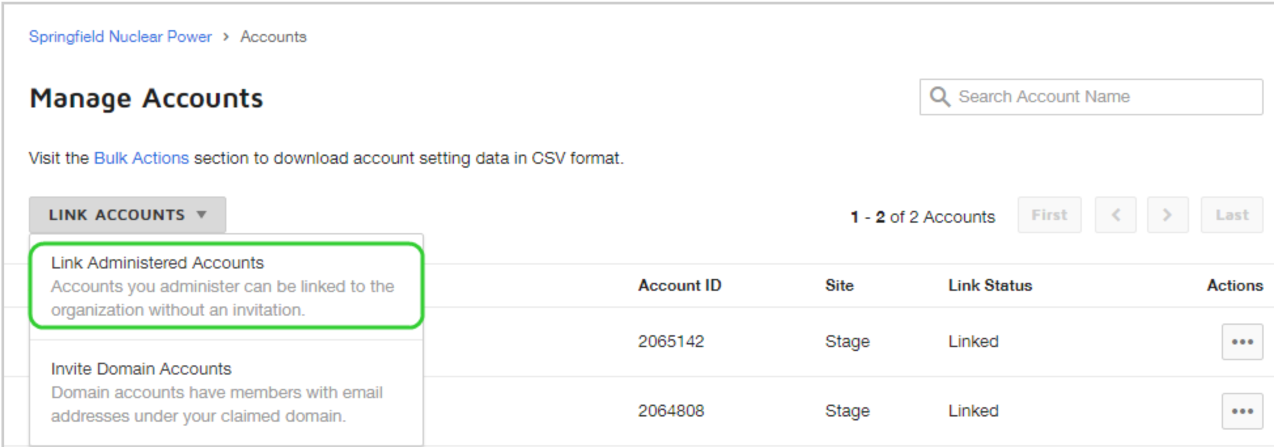
> **Note:** If you meet these criteria but do not see your account as available to link, you may need to extend membership rights to all of your memberships. For more information, see the troubleshooting information.

To link an account, you must be a full DocuSign eSignature administrator on that account. The account must not already be linked to an organization.

Link Administered Accounts to an Organization

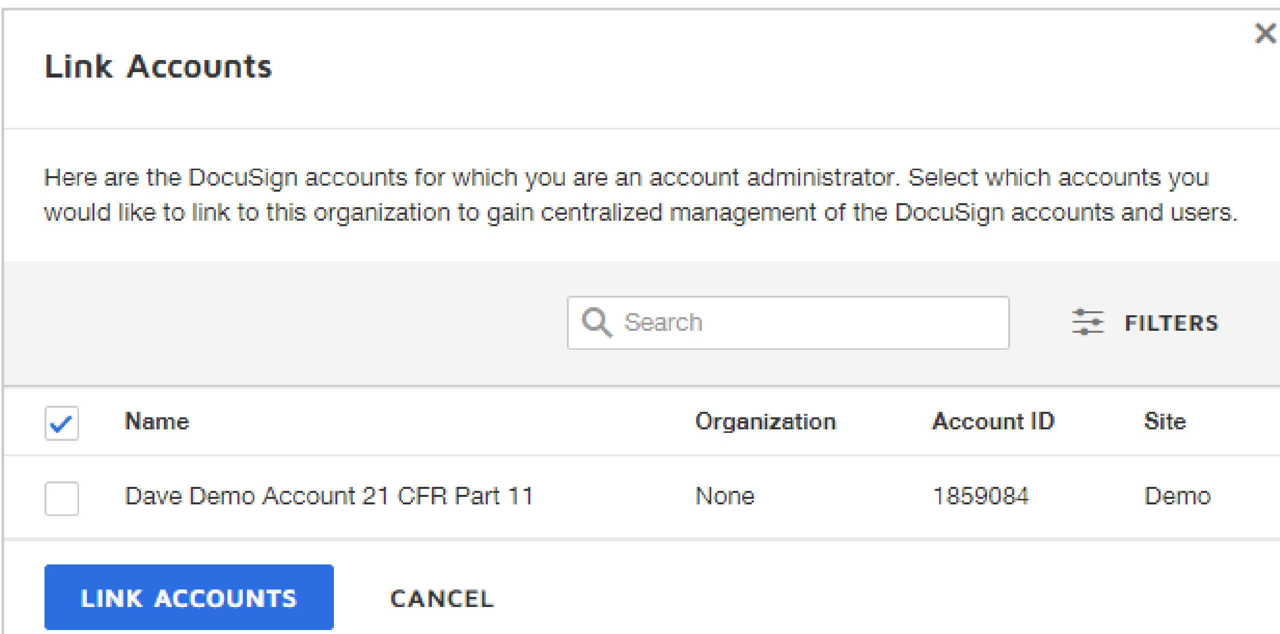
1. From the DocuSign Admin dashboard, click **Accounts**.

2. In the Manage Accounts list, click **Link Accounts** then select **Link Administered Accounts**.



Link Administered Accounts is available only if there are any accounts for which you have the necessary administrator permissions that are not already linked to an organization.

3. In the Link Accounts dialog, the accounts for which you are an account administrator with All Administration Capabilities permissions are displayed. Select the accounts you would like to link to the organization.

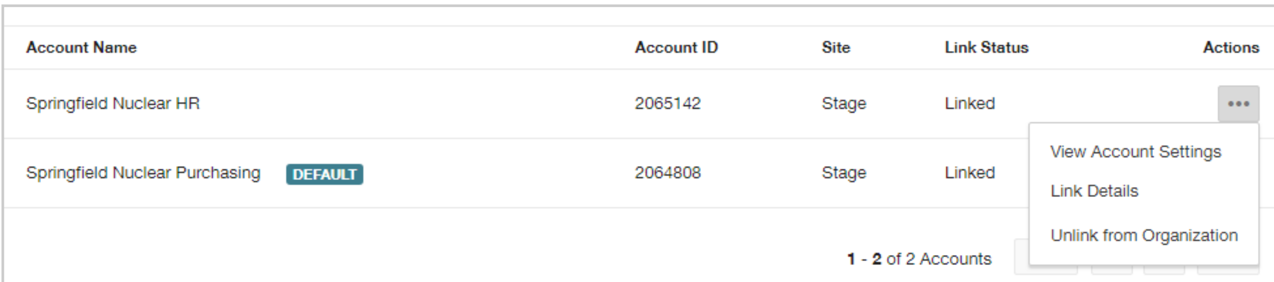


4. Click **LINK ACCOUNTS**.

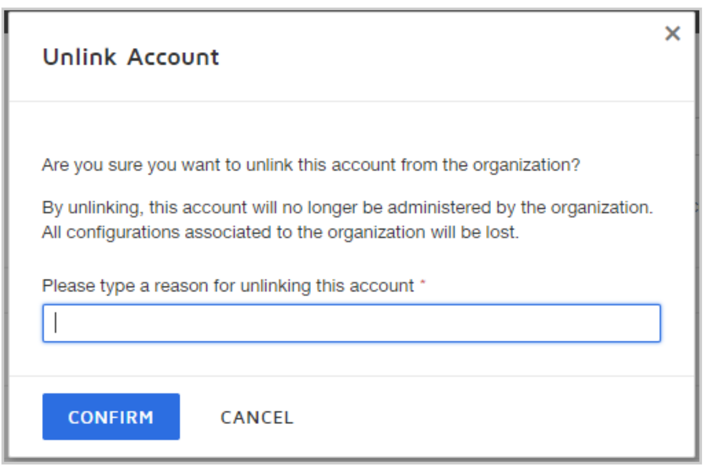
Unlink Accounts from an Organization

The DocuSign administrator can unlink accounts from the organization. You cannot unlink the organization's default account. When you unlink an account, the account and its users can no longer be managed through the organization.

1. From the DocuSign Admin dashboard, click **Accounts**.
2. In the Manage Accounts list, locate the account you want to unlink from the organization by searching or scanning the list.
3. Click the Actions menu for the account to modify and select **Unlink Account**.



4. Provide a reason for unlinking the account and click **Confirm**.



The account is unlinked from the organization.

Invite External Domain Accounts to Link

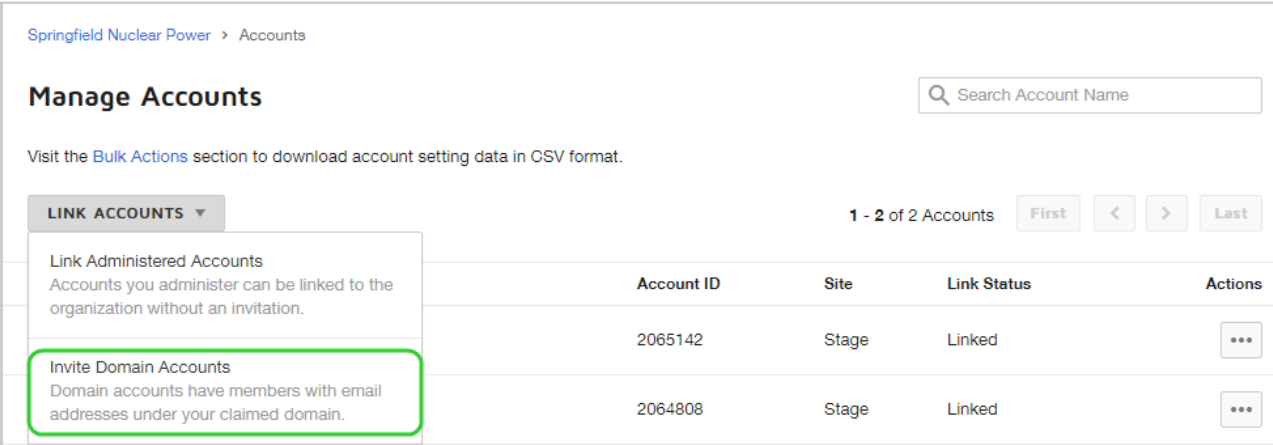
DocuSign administrators with the Administrator permission profile can invite external domain accounts to link with the organization. External domain accounts are eSignature accounts that contain a user whose email address is under your organization's claimed domain.

If the eSignature account has multiple administrators, the invitation will be sent to the five most recently active administrators. The administrator can choose to accept or decline the link, though if they decline, they must provide a reason.

Note: You can generate a report of all users with external domain accounts. For more information, see User List Exports.

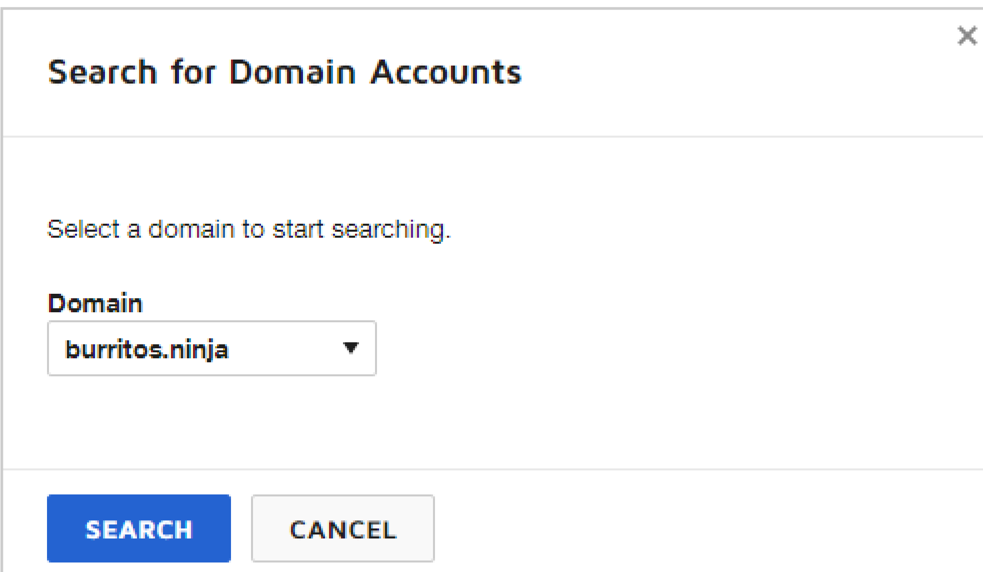
1. From the DocuSign Admin dashboard, click **Accounts**.

2. In the Manage Accounts list, click **Link Accounts** then select **Invite Domain Accounts**.



3. If prompted, select a domain to search under and click **SEARCH**.

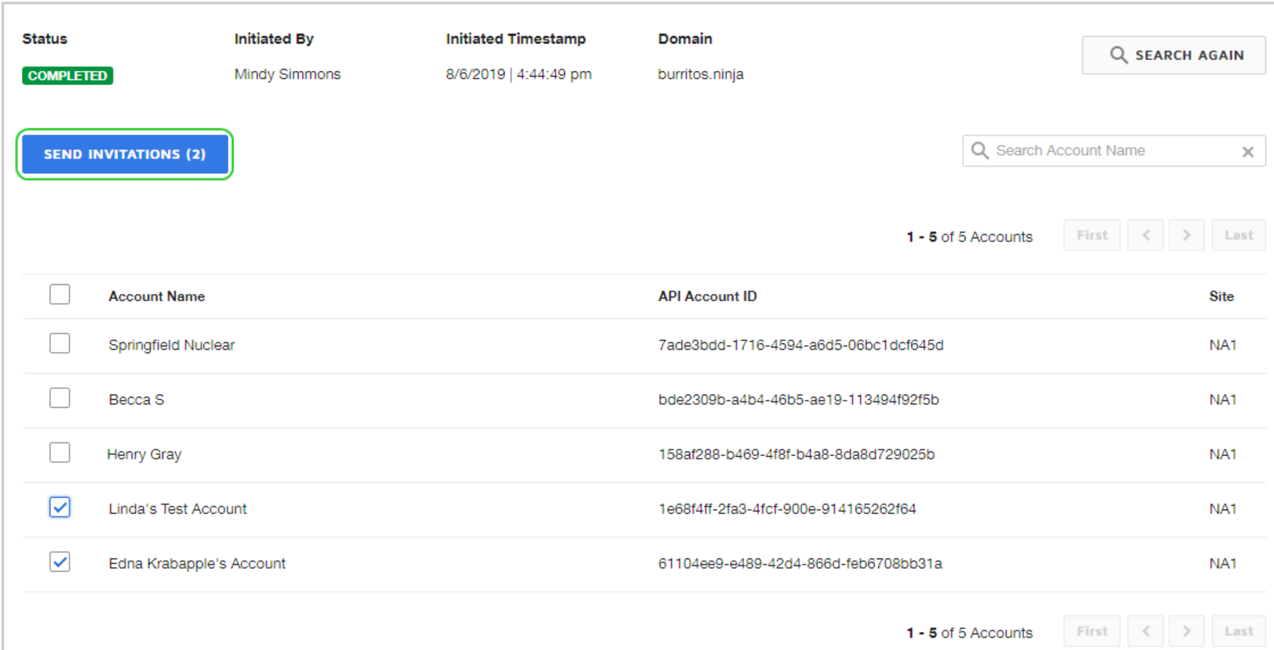
Note: If a search has already been completed, click **SEARCH AGAIN** to begin a new search.



4. Click **REFRESH** to reload the page with your search results.

Note: The search may take some time, you can leave the page. Return later by clicking **Link Accounts** and selecting **Invite Domain Accounts** on the Accounts page.

5. Select the accounts you want to invite to the organization, then click **SEND INVITATIONS**.



The accounts are added to the list of linked accounts with the status "Pending". The eSignature administrators receive an email invitation and must accept or decline to proceed.

Manage Invitations

View and manage pending, accepted, or declined invitations from the Manage Accounts list. You can resend or cancel pending invitations and delete declined invitations.

1. From the DocuSign Admin dashboard, click **Accounts**.

2. In the Manage Accounts list, locate the invited account you want to view by searching or scanning the list.

3. Click the Actions menu for the account and select one of the following:

    - Invitation Details - This provides information such as who sent the invitation, when it was sent, and when it was accepted or declined. If declined, it will also include the decline reason provided.
    - Resend Invitation - This action sends the invitation again.
    - Cancel Invitation - This action cancels the invitation. The invited eSignature administrator will no longer be able to accept or decline the invitation. This will also remove the account from the Manage Accounts list.
    - Delete Invitation - This action is only available for declined invitations. This removes the account from the Manage Accounts list.

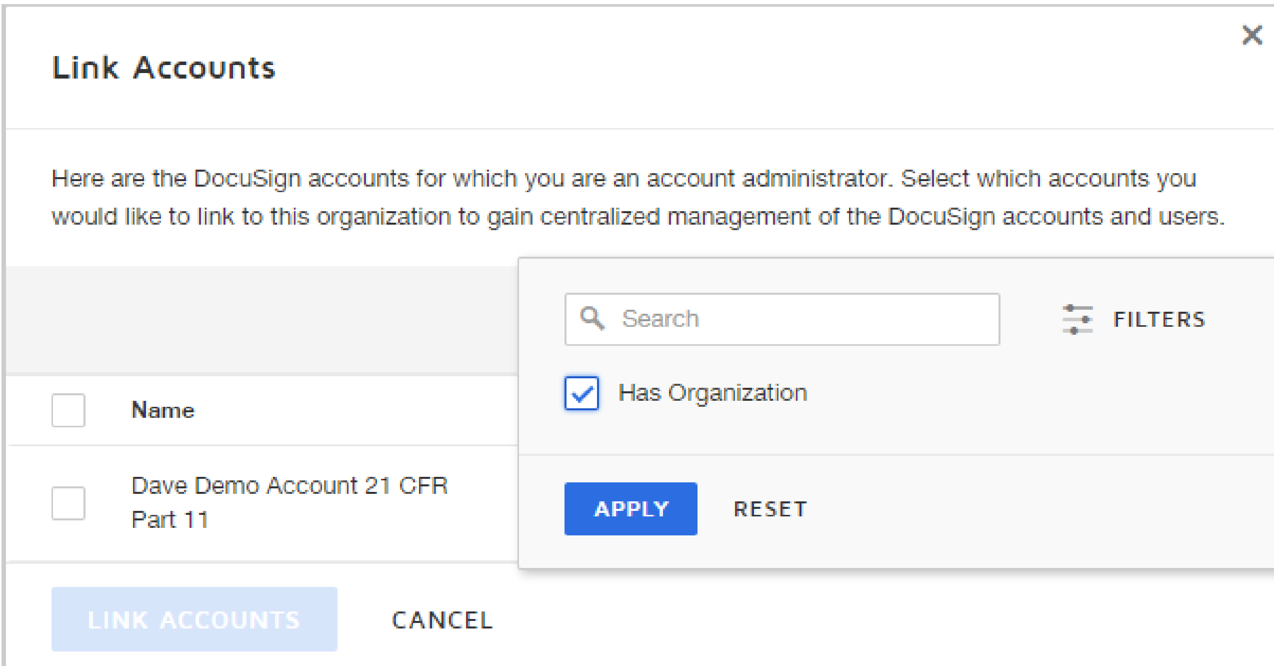
Find Accounts Linked to Another Organization

By default the list of accounts to link shows only those accounts for which you are an account administrator and that are not yet linked to an organization. If you have accounts that are linked to another organization, you can change the default filter to find them. Once you identify these accounts, if you want to link them to your current organization, you must first unlink them from the existing organization.

1. From the DocuSign Admin dashboard, click **Accounts**.

2. In the Manage Accounts list, click **Link Accounts** then select **Link Administered Accounts**.

3. In the Link Accounts dialog, click **FILTERS**.



4. Select the **Has Organization** check box and click **APPLY**.

   The list of accounts shows any accounts for which you are an administrator and that are already linked to an organization.

Related Topics

For more information on topics related to organization accounts, see the following:

- Establish Control of your Company's DocuSign Agreements: Gain control of your company's agreements with proven best practices and procedural guidelines.
- Default Account and Just-in-Time Provisioning: The default account for an organization is used for just-in-time provisioning of new users.
- Navigate to an Account: From DocuSign Admin, you can navigate back to the account administration app for any account on which you are an administrator.
- User Management: Linking accounts to your organization enables the administrators to manage users from central organization controls.
- Organization Administrators: Add DocuSign administrators to help manage and build out your organization, linking additional accounts which they control.

Navigate to an Account

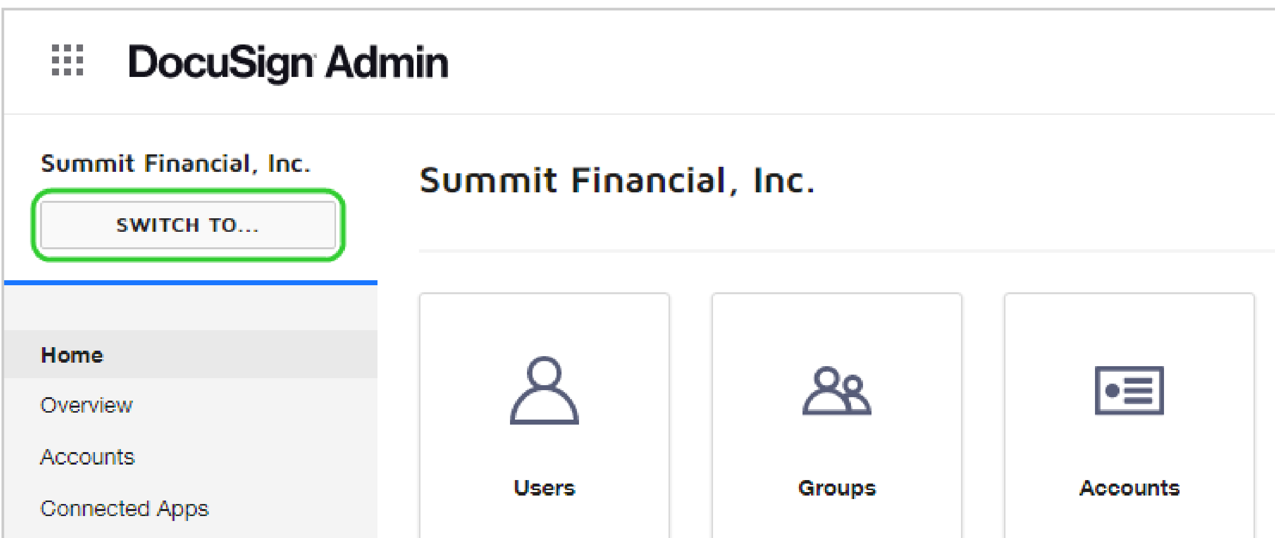
Note: This guide is for DocuSign administrators who oversee multiple linked accounts. For other administrators, see Switch Accounts - DocuSign User Guide.

Within DocuSign Admin, all DocuSign administrators can manage the users on any linked account. For the organization's reserved domains, administrators can also manage any users using a domain email for any DocuSign account. However, for full account administration of an account, you'll want to return to the DocuSign eSignature Admin view. You must be an administrator on an account in order to navigate to the account's administration view.

Switch Your View to an Account

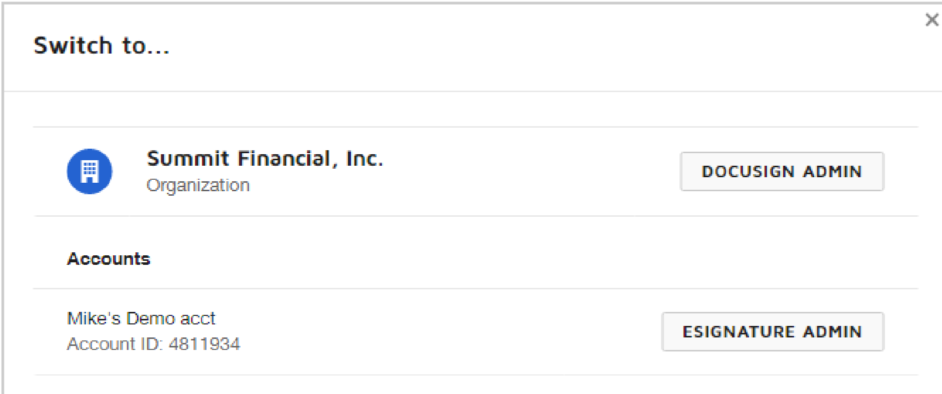
You can view a list of the accounts for which you are an account administrator. From this list, you can navigate to any one of the accounts.

1. In DocuSign Admin, select **SWITCH TO**.



A list shows all accounts for which you are an account administrator.

2. Select **ESIGNATURE ADMIN** to go to the eSignature Settings page for that account.

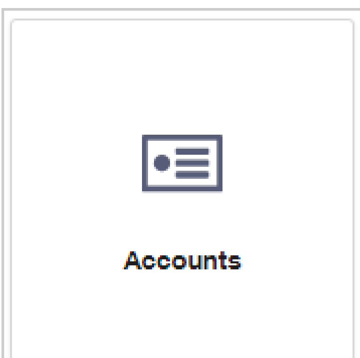


The eSignature account appears.

Navigate to a Linked Account

If your account is linked to the organization, you can also navigate to the DocuSign eSignature Admin view from the Accounts list.

1. From the DocuSign Admin dashboard, click the **Accounts** tile.



2. Locate your account in the list of accounts and click on it to navigate to the DocuSign eSignature Admin view for the selected account

> **Note:** To link additional accounts, review Accounts.

Default Account and Just-in-Time Provisioning

> **Note:** This guide is for DocuSign administrators who oversee multiple accounts. To set a default account as a user, see Switch Accounts.

When an organization is created, the eSignature account from which it was created becomes the default account. The default account cannot be unlinked from the organization and can be used for just-in-time provisioning of new users. Once you link additional accounts to the organization, you can change the default account to any of the other linked accounts.

The default account and permission profile is used for basic just-in-time provisioning of new users. For more advanced control, you can set up your identity provider to include provisioning details in SAML and add users to different accounts and permission profiles.

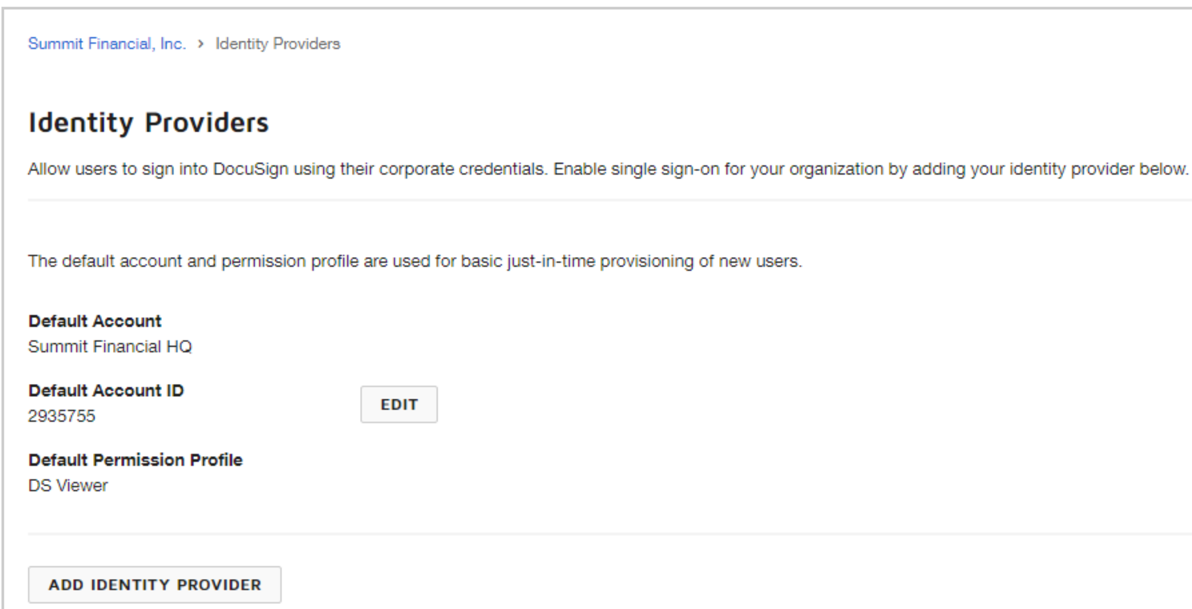
CONTENTS

Edit the Default Account and Permission Profile

You can edit the default account and permission profile from the Identity Providers page.

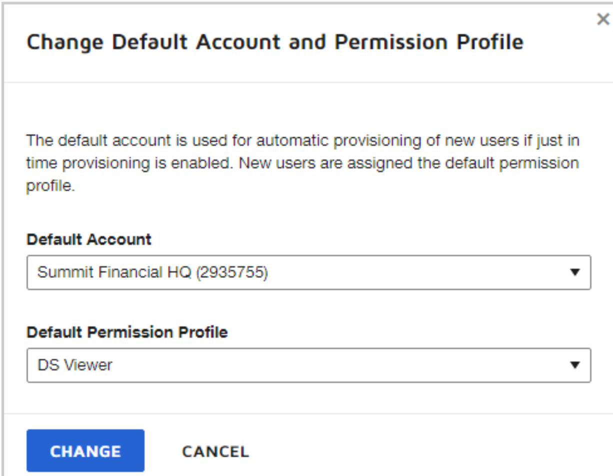
1. From the DocuSign Admin dashboard, click **Identity Providers**.

2. On the Identity Providers page, you can see the current selections for the default account and the default permission profile.



3. Click **Edit**.

4. In the Change Default Account and Permission Profile dialog, make new selections, and click **Change**.



Just-in-Time Provisioning

Through the organization's SSO setup, you can provision domain users with a DocuSign eSignature account the first time they log in. Just-in-time provisioning reduces the friction and administrative overhead for adding users to accounts in your organization.

When a user logs in using a reserved domain email, the system checks to see if the email exists in any of the organization accounts. If the email is not found, then a new user account is created in the organization. Typically, the new account is added to the organization's default account.

Just-in-time provisioning is defined on your Identity Provider setup and can be implemented in two ways:

- **Basic provisioning using the default account:** All new users are added to the organization's default account and assigned the default permission profile.
- **Advanced provisioning to specific accounts:** Set up your identity provider to include provisioning details in SAML and add users to specific accounts and permission profiles.

Related Topics

For more information on topics related to an organization's default account, see the following:

- Organizations: How to create an organization.
- Establish Control of your Company's DocuSign Agreements: Learn how you can gain control of your company's agreements with proven best practices and procedural guidelines.
- Accounts: Link and unlink organization accounts.
- DocuSign Single Sign-On Overview: An introduction to SSO and organizations.
- Identity Providers: How to set up and manage your organization's identity provider and define just-in-time provisioning.

User Management

Note: This guide is for DocuSign administrators who oversee multiple accounts. For administrators of individual accounts, see Manage Users - DocuSign eSignature Admin.

DocuSign Admin provides a unique and powerful view for managing your users and securing the company's use of DocuSign. From the Users page, DocuSign administrators can manage all organization users, and can add and close users. User details and account memberships can also be managed through the organization.

DocuSign administrators with the Users Administrator permission profile can manage non-administrator organization users only and only the account memberships with non-administrator permissions. DocuSign Administrators can manage all users and memberships, including other DocuSign Administrators and users who have administrator permissions on their account memberships.

CONTENTS

User Management

With DocuSign Admin, a user is the focal point of management. DocuSign administrators can search for a user within their organization and obtain information regarding that user, including language preference, security log in policy, and all their account memberships and associated permission profiles and groups. DocuSign administrators can directly manage a user from one location and gain confidence through knowledge of which accounts that user has access to and what permissions they have on those accounts. Administrators can also update users from this centralized view and have the changes propagated across all account memberships allowing for quicker and easier management of their users.

This centralized control is a significant advantage over managing a user from within a specific eSignature account. eSignature administrators can make changes to a user's membership only; they cannot modify other user profile details, and any changes affect a single membership only.

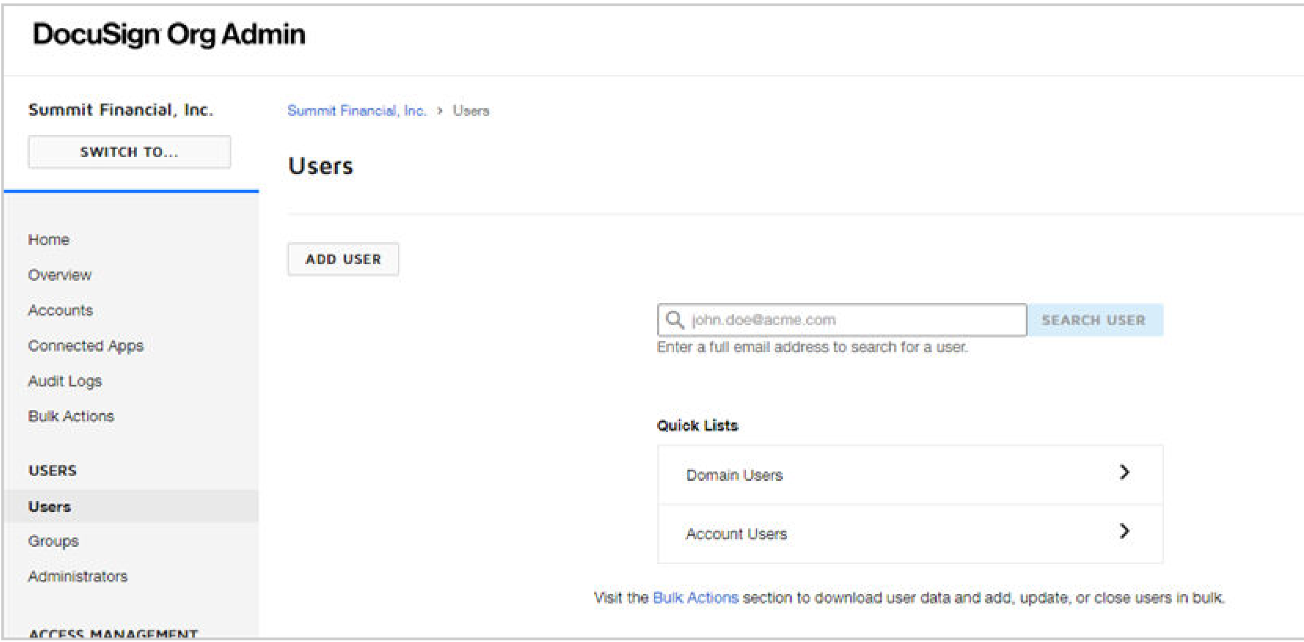
DocuSign Admin combines centralized user management with reserved domains, providing a unique and powerful view and management capabilities of domain-based users. Through reserved domains and centralized user management, DocuSign administrators have visibility into every corporate user with a DocuSign account. Quickly view all reserved domain based users by selecting the Domain Users. The list displays all users that have a DocuSign account using the reserved domain. A DocuSign administrator has additional management capabilities on a domain user including: change email address, define a security log-in policy, view all account memberships including those external to the organization, and define the default account to be used for signing and sending.

The Users Page

The Users page is where you can add a new user or locate an existing user to manage.

An organization can contain two categories of users:

- **Account Users:** These users are members of the accounts that are linked to the organization.
- **Domain Users:** These users are members of a specific domain. If your organization has any reserved domains, then all users with a DocuSign account that uses a reserved domain email automatically come under the organization.

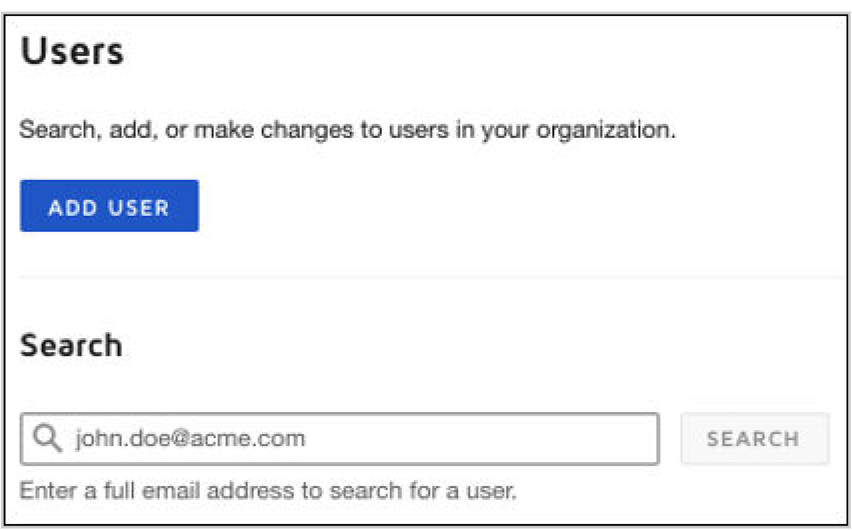


Search for a User by Email Address

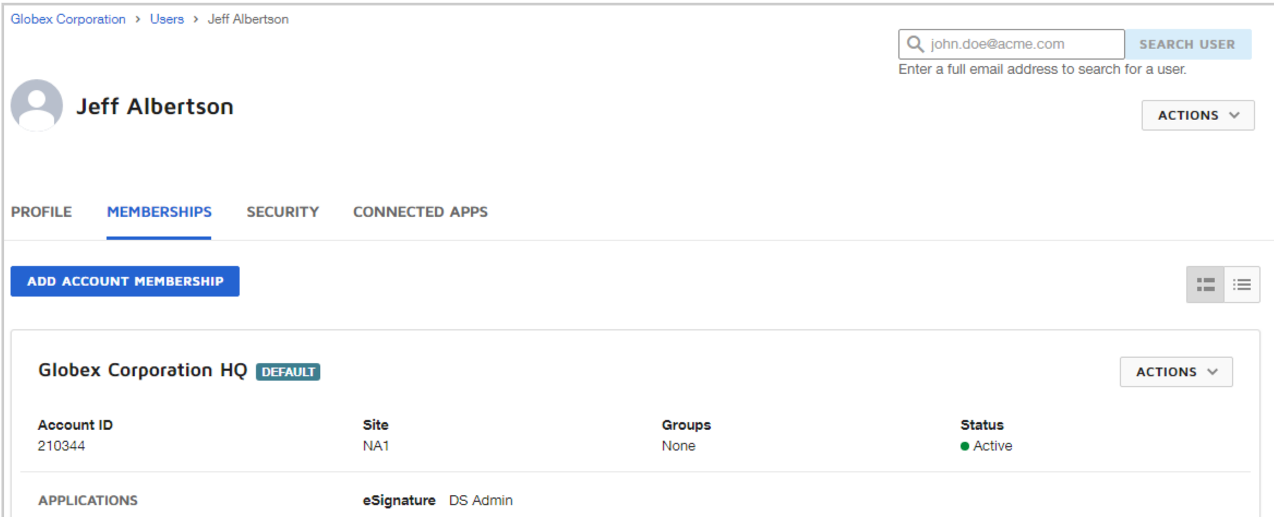
You can locate any user in your organization by their email address.

1. From the DocuSign Admin dashboard, click **Users**.

2. Enter the user's email address and press Enter to search.



3. If there is a match, the user's information appears.

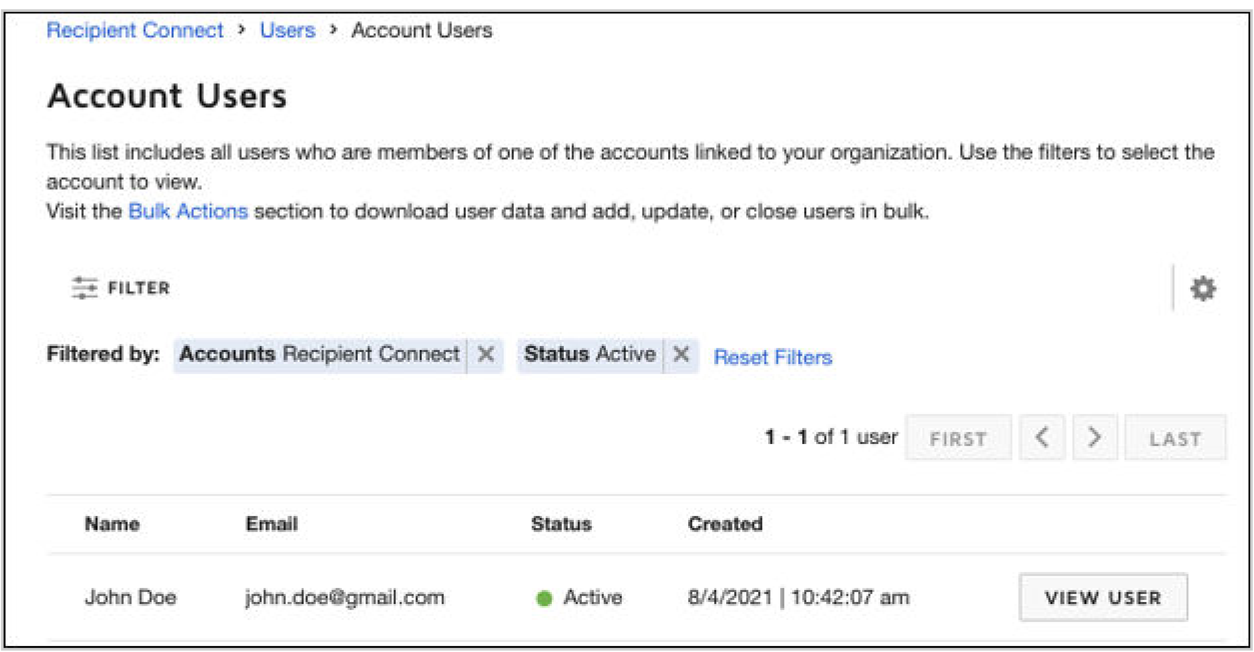


View All Users for an Account

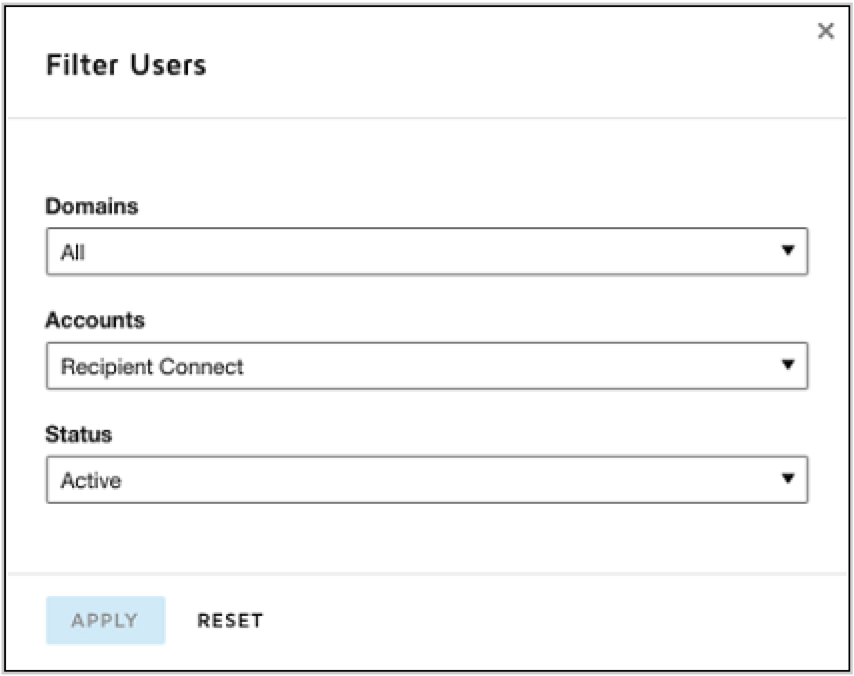
You can view all users who are members in an account that is linked to your organization.

1. From the DocuSign Admin dashboard, click **Users**.

2. Select **Account Users**. The Account Users page appears, showing the active users belonging to the default account for the Organization, and across all reserved domains.



3. To select a different account to view, click **FILTERS** to open the filter options. The Accounts list contains the accounts linked to your organization. Select an account and click **APPLY**.



You can also filter by a single domain and user status to show only Active, Pending, or Closed users for the selected domain and account.

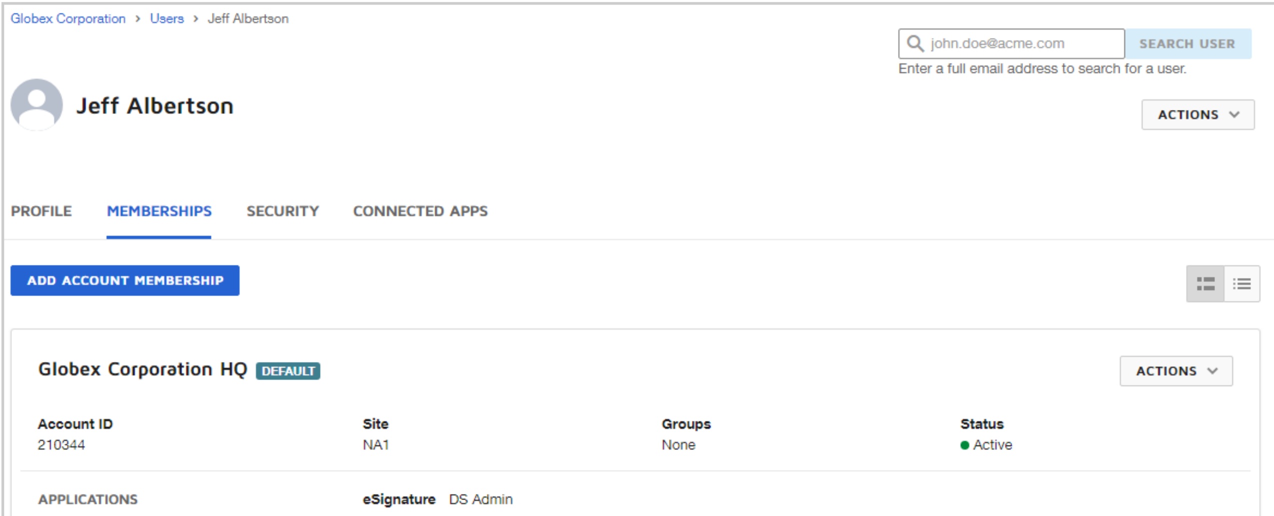
View User Details

The user details page provides information about a specific user. You can view and manage a user's profile and account memberships, security settings, and organization settings from the user details page.

1. From the DocuSign Admin dashboard, click **Users**.

2. Using either the Account Users list or the search bar, navigate to a user.

3. Click a user to view their details. Select one of the following items for more information:



- **ACTIONS:** Click **ACTIONS** on the user details page to add an account membership, make the user a DocuSign administrator, or close all of the user's account memberships.
- **MEMBERSHIPS:** Edit membership details for an account, close an account membership, reactivate a closed account membership, or resend an activation invitation to a pending account by clicking **Actions** on the account.
  - For domain users, you can also manually activate pending memberships and assign the user's default account for signing and sending. Domain users activated in this way will not receive an activation invitation.
  - You can add memberships to accounts within the organization by clicking **ADD ACCOUNT MEMBERSHIP**. If the user is already a member of all organization accounts, regardless of status (Active/Pending/Closed), this option is unavailable.

    Note: If ADD ACCOUNT MEMBERSHIP is unavailable, you can manage the user's membership details for each account by clicking **Actions** on the account.
- **PROFILE:** Edit the user's full name, preferred language, physical address, and job title. Changes to a user's physical address, job title, and phone number are populated across all of the user's accounts within the org.
  - For domain users, you can also modify the email address associated with the user. This is generally not recommended and should be done with great caution.
- **SECURITY:** Available for domain users only. Edit the domain user's login policy. See Setting a User Login Policy for more details.
- **ORGANIZATION:** If the user is a DocuSign administrator, you can modify their DocuSign administrator permission profile here.
- **CONNECTED APPS:** Available for domain users only. Authorize an application for a single domain user and limit access by specifying permissions. To authorize an application for all domain users, see Connected Apps.

Note: You must be a DocuSign administrator with DocuSign Administrator permissions to modify another DocuSign administrator's permissions.

Add Users

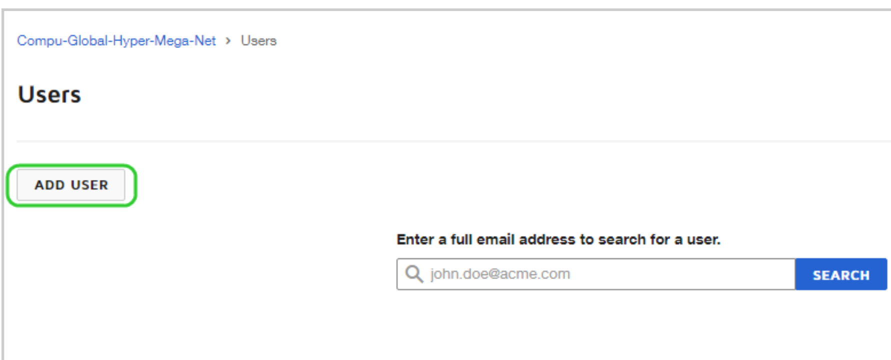
DocuSign eSignature administrators of linked accounts can continue to add users directly in their account using the standard DocuSign eSignature Admin app. DocuSign administrators can also add users through the organization controls.

You can also leverage your Single Sign-On configuration and use reserved domains and just-in-time provisioning to add new users automatically when they first log in to DocuSign.

DocuSign administrators with the User permission profile can add users and memberships with non-administrator permission profiles only. You must have the full DocuSign Admin permission profile to add memberships with an administrator permission profile. See Organization Administrators for more details.

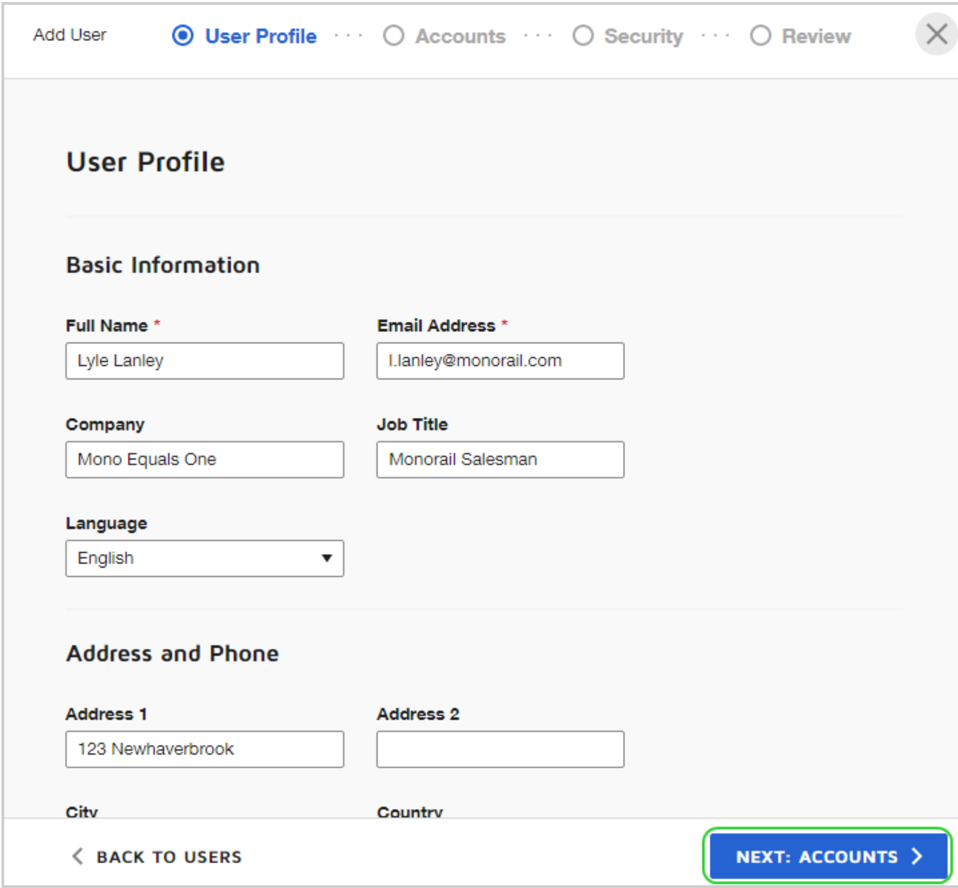
1. From the DocuSign Admin dashboard, click **Users**.

2. Click **Add User**.



3. Enter the user's full name, email address, and any other profile information, then click **NEXT: ACCOUNTS**.

   The user's profile information is applied to all account memberships.



> **Note:** If the user is already part of your reserved domain and has an existing DocuSign account, the Existing User dialog appears, allowing you to edit the user.

4. Add an account membership from the **Account** drop-down list. All accounts linked to the organization are available to choose from.

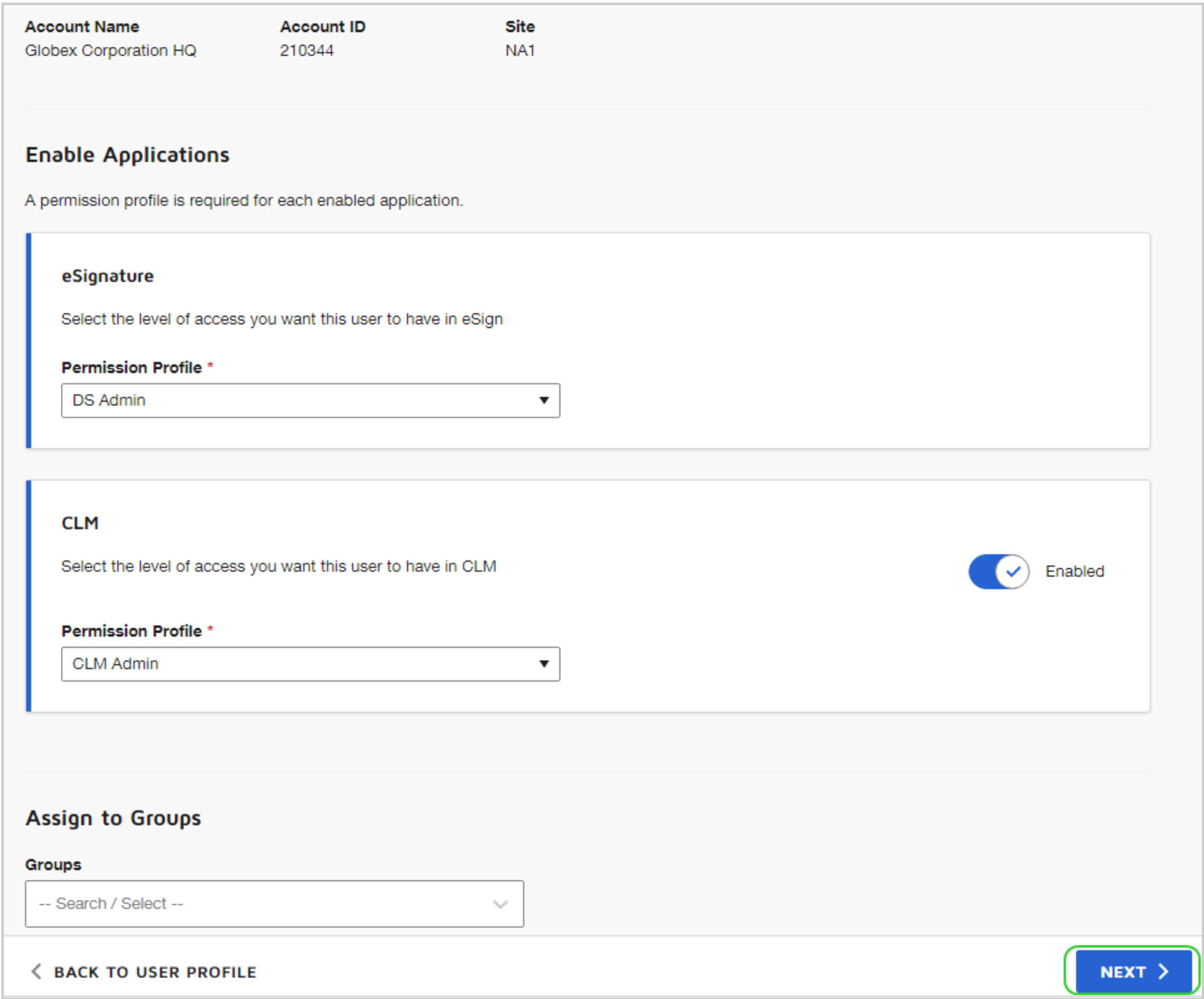
5. If necessary, enable applications for the user.

> **Note:** eSignature is enabled for all users by default. If CLM is available, click the toggle to enable access.

6. Give the user a permission profile for each enabled application.

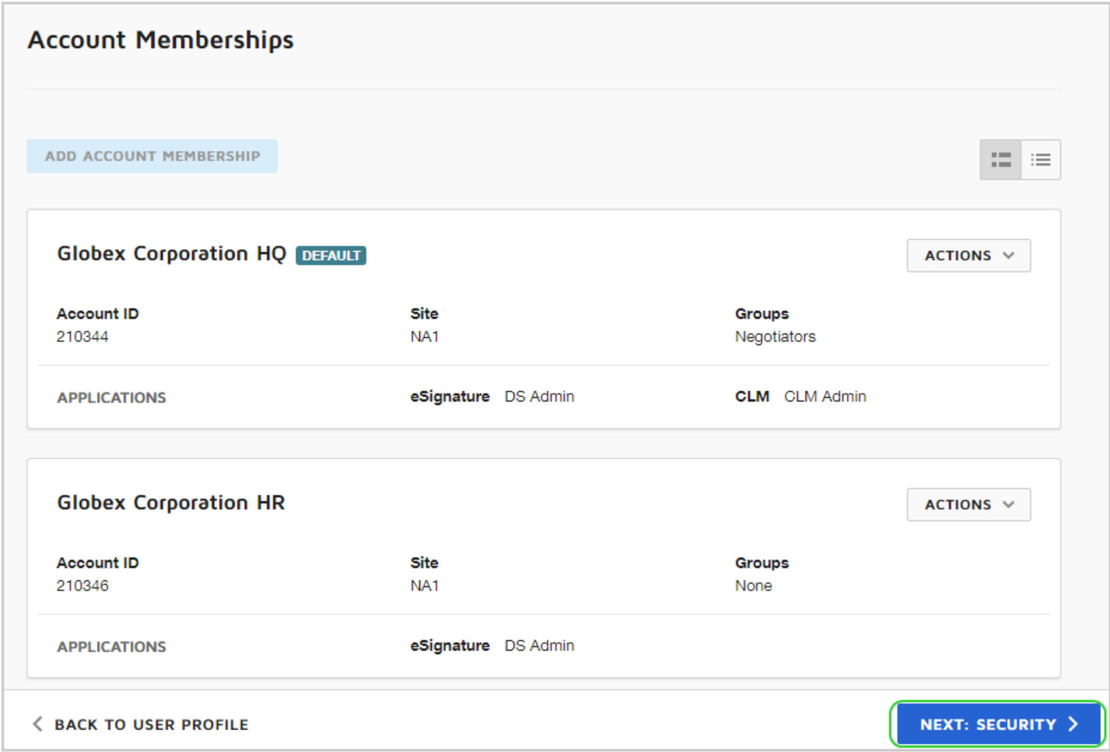
7. Assign the user to any necessary groups. This step is only available if the selected account has one or more defined groups.

8. Click **NEXT** to add the account membership.



9. If necessary, click **ADD ACCOUNT MEMBERSHIP** and repeat steps 4-8 to add the user to additional accounts.

10. Review the user's account memberships, then click **NEXT: SECURITY**.

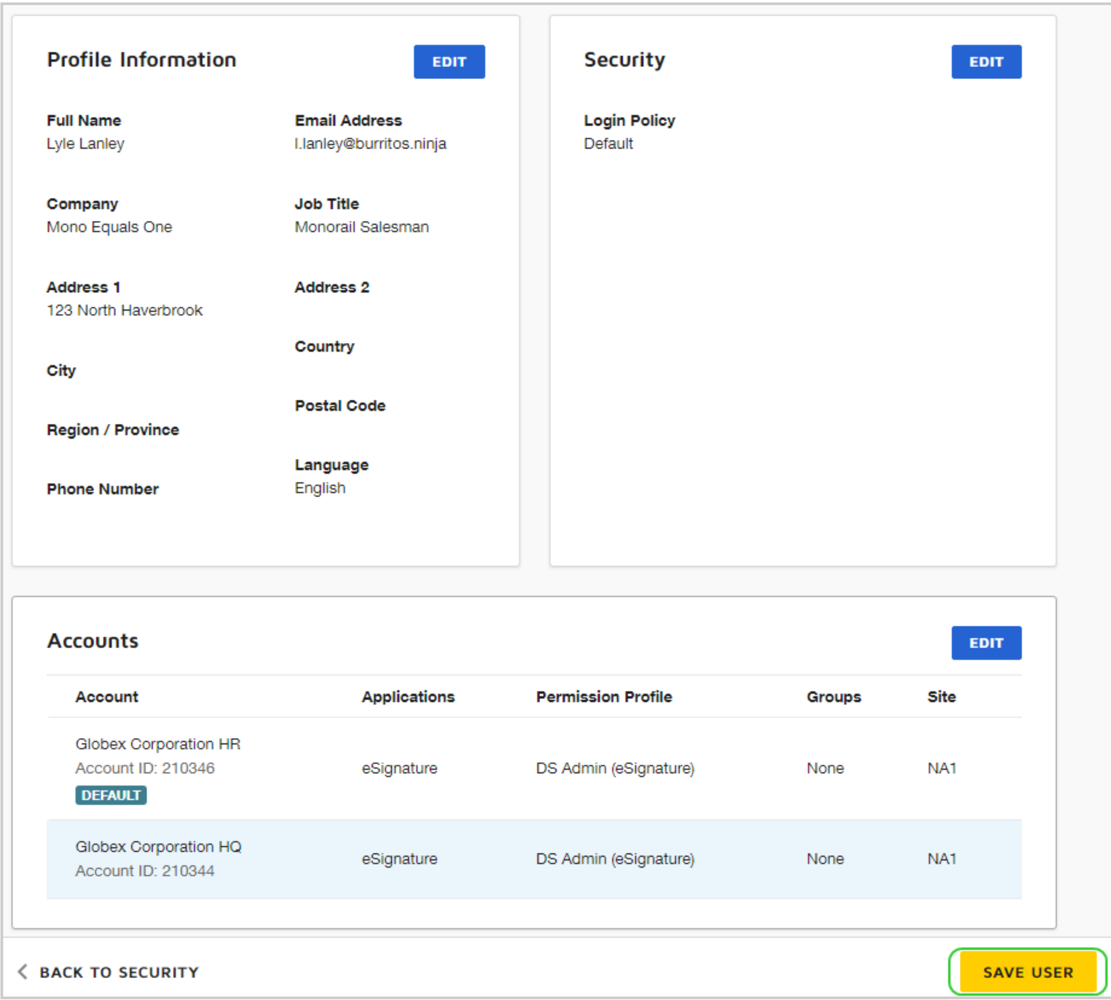


11. If necessary, adjust the user's security settings, then click **NEXT: REVIEW**.

- **For domain users:** You can specify the login policy. The login policy is based on the specifications defined by the domain. The default policy is generally recommended, but you may need to make exceptions for certain users, such as an SSO administrator.
- **For non-domain users:** You can add an access code to the account activation email. If you add a code, you must provide the code to the user in order for them to activate their account.

12. Review the user's information, then click **SAVE USER**.

> **Note:** You can modify the user's profile information, security settings, or account memberships by clicking **EDIT** on the area you'd like to update.



The user is created and added to the selected accounts.

- **For domain users with Auto-activate memberships enabled:** New users can be activated automatically for domain accounts using SSO. This can be enabled in the Domain Settings. If enabled, new memberships are activated automatically. Memberships activated in this way will not receive an activation email.
- **For all other users:** The user appears as Pending under the account list. The user receives an activation email and must complete the activation steps to activate their new account. Once they do so, their membership status changes to Active.

Related Topics

- DocuSign Single Sign-On Overview: Provision new users and enforce secure access management across all your corporate applications.
- Domains: Control domain users and accounts.

- Change Domain Settings: Modify the security settings for a domain.
- Setting a User Login Policy: Adjust the security settings for an individual user in your organization domain.
- Accounts: Adding users automatically to a default account.

Groups

> **Note:** This guide is for organizations that have DocuSign CLM. For organizations that have no linked accounts with DocuSign CLM, see Manage Groups - DocuSign eSignature Admin. For more information on DocuSign CLM, contact DocuSign customer support.

Groups are used to organize users into functional units within accounts. Accounts with CLM manage groups in DocuSign Admin.

DocuSign administrators can manage groups for both eSignature and CLM. They can create or delete groups and add or remove group members.

CLM accounts must use DocuSign Admin to manage groups. eSignature-only accounts can manage groups in DocuSign Admin or eSignature Admin.

- In eSignature, groups can be used to control access to templates and branding.
- In CLM, groups can be used to control access to folder security, tasks, and other views.

> **Note:** Signing brands are assigned to a group through eSignature Admin. For more information, see Assigning Brands to Groups - DocuSign eSignature Admin.

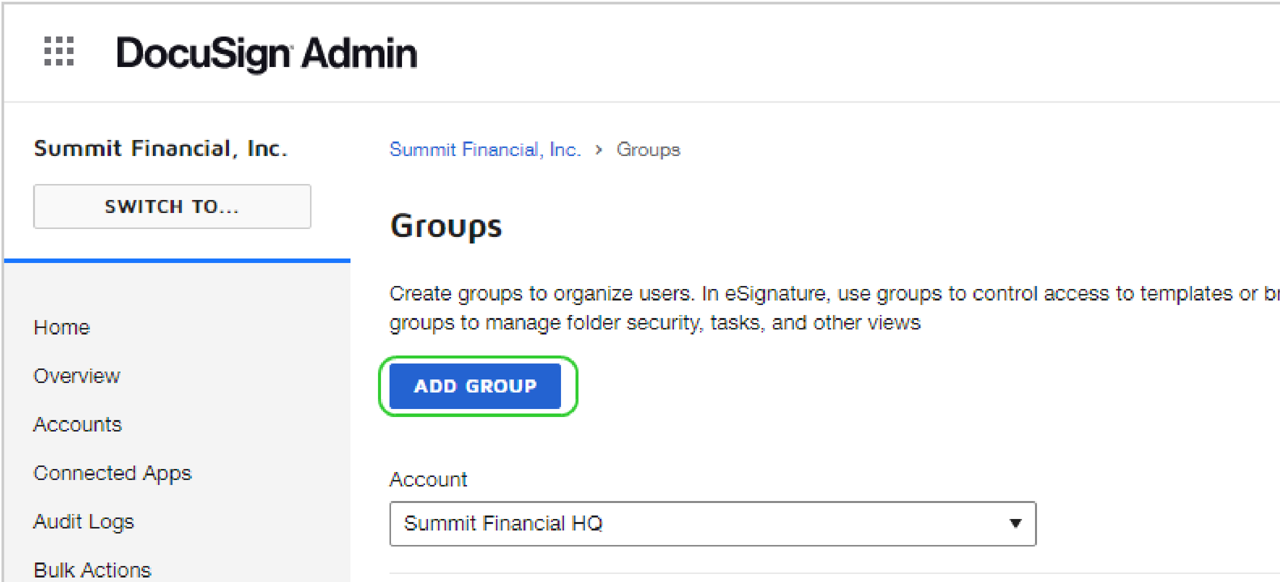
CONTENTS

Create a New Group

DocuSign administrators can create new groups and add users to the group.

1. From the DocuSign Admin dashboard, click **Groups**.

2. Click **ADD GROUP**.



3. Enter a name for the group and select an account.

> **Note:** Groups created for an account with CLM enabled will appear in both eSignature and CLM Admin.

4. When finished, click **ADD GROUP**.

5. Click **ASSIGN USERS**.

6. Select the users to add to the group, then click **ADD USERS**.

   The group is created and the selected users are added to the group.

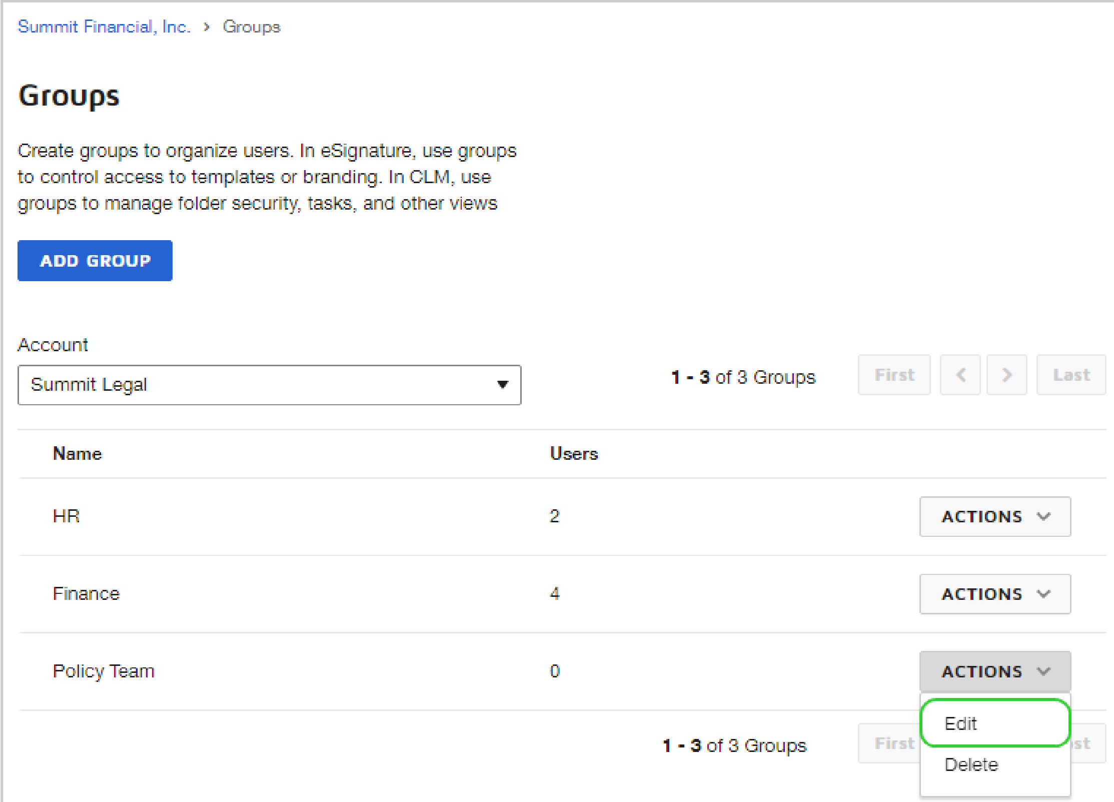
Edit an Existing Group

DocuSign administrators can update the group name and add or remove users.

1. From the DocuSign Admin dashboard, click **Groups**.

2. Select an account to and locate the group to edit.

3. Click **ACTIONS**, then click **Edit**.



4. If necessary, update the group name.

5. To add new users, click **ASSIGN USERS**.

6. Select the users to add to the group, then click **ADD USERS**.

   The selected users are added to the group.

7. To remove users, select the users from the list, then click **REMOVE USERS**.

   The selected users are removed from the group.

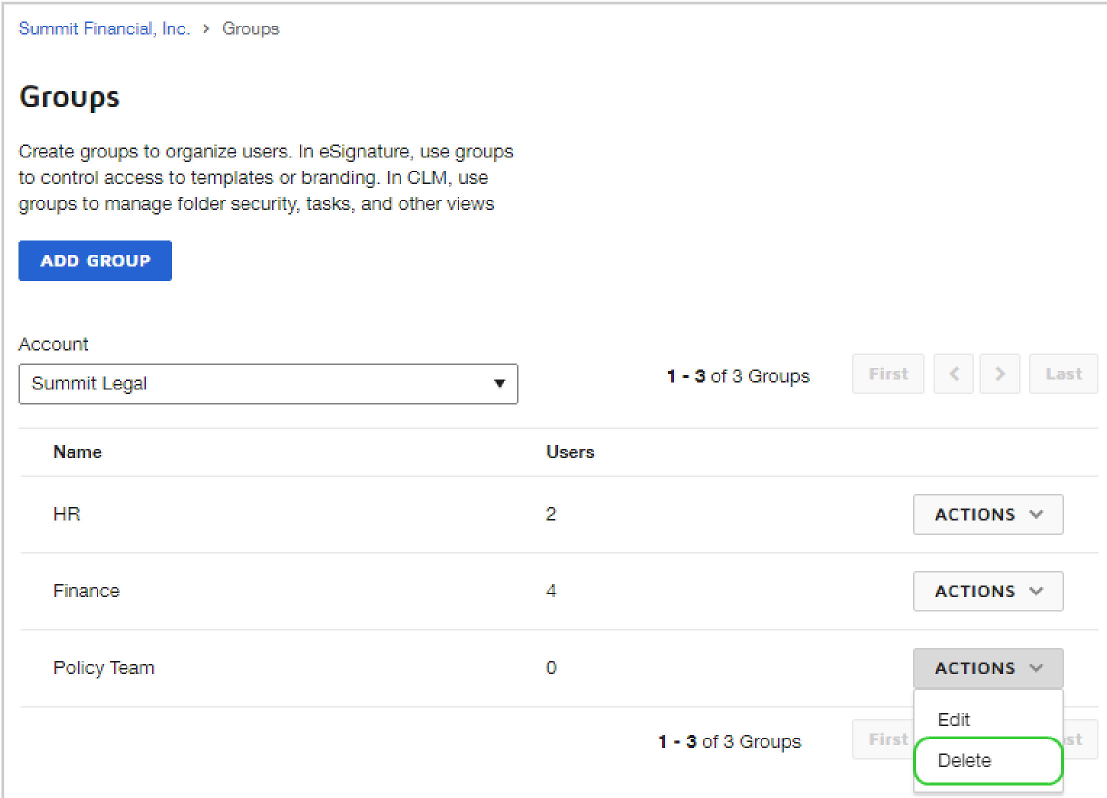
Delete a Group

Deleting a group removes it from the selected account. If the group is in an account with CLM enabled, it will be removed from both eSignature and CLM.

1. From the DocuSign Admin dashboard, click **Groups**.

2. Select an account to and locate the group to edit.

3. Click **ACTIONS**, then click **DELETE**.



4. Click **DELETE**.

   The group is deleted.

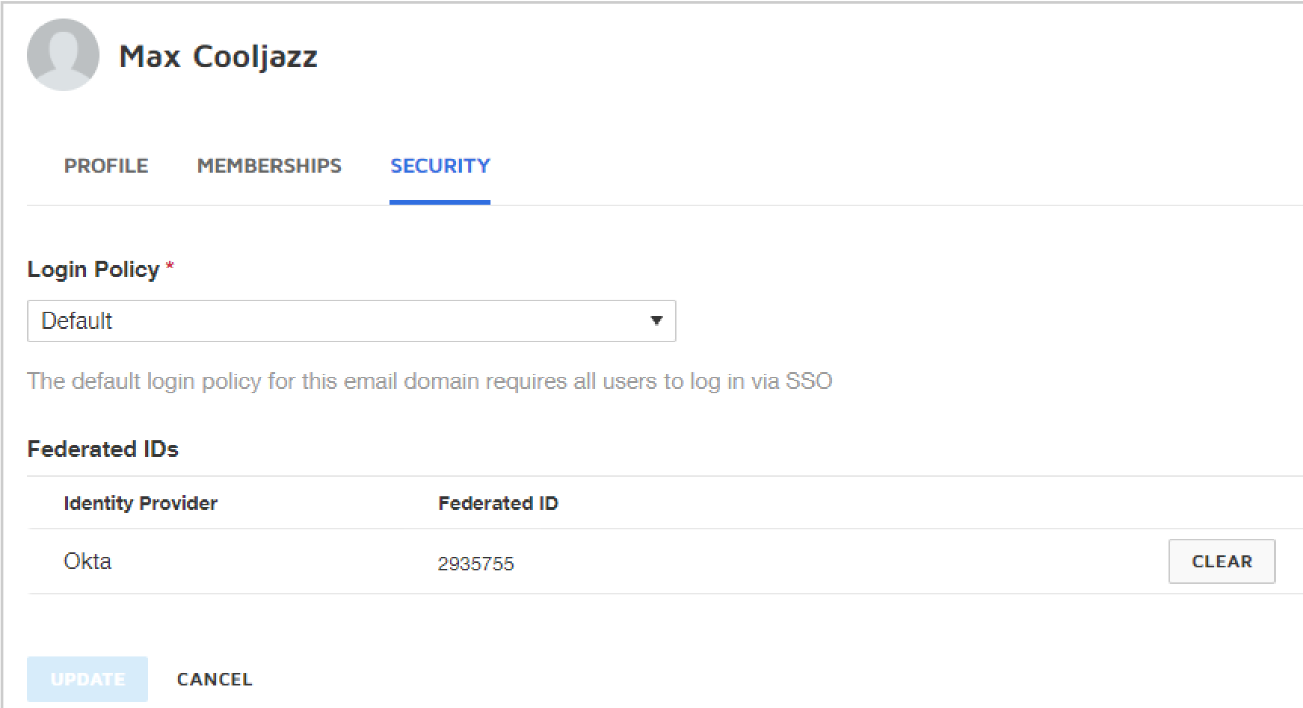
Related Topics

For more information on topics related to Groups, see the following:

- Manage Groups - DocuSign eSignature Admin
- Groups - DocuSign CLM
- Group User Management - DocuSign CLM

Federated ID

For domain users in your organization, for each user who authenticates through your identity provider (IdP), DocuSign receives and records a unique identifier. This identifier is the Federated ID seen on the user Security Profile.



The Federated ID is the unique identifier for a user in the DocuSign system and is defined and provided by your IdP. When a user logs in through SSO, this identifier is added to their user record in DocuSign. The Federated ID is the primary identifier for a user logging in to DocuSign through SSO and is combined with an email address to identify the user.

If your IdP changes the unique identifier for a user, the user cannot log in until you clear the stored Federated ID. After you clear the stored identifier, the next time the user logs in through SSO, the new Federated ID is automatically recorded for them.

For details on the underlying SAML specifications and best practices for this unique identifier, see Identity Providers and review the **NameID** specification details.

Clear a User's Federated ID

1. From the DocuSign Admin dashboard, click **Users** and locate the user by searching or using one of the quick lists.
2. On the user's page, click the **Security** link in the left-hand navigation.
3. In the Federated IDs section, click **CLEAR** for the identity provider identifier you need to remove.
4. Click **CONFIRM** to confirm your action and clear the recorded Federated ID.

   The Federated ID is cleared. The next time the user logs in through SSO, the new identifier is added automatically.

Bulk User Actions

> **Note:** This guide is for DocuSign administrators who oversee multiple accounts. For administrators of individual accounts, see User Bulk Actions - DocuSign eSignature Admin.

As a DocuSign administrator, you can view and manage details for multiple users at a time. Bulk user actions enable DocuSign administrators to manage details for all users within an organization. You can add or update users, export lists of existing users, or close users in bulk by uploading a CSV file.

CLM administrators can also manage users in bulk across all organization accounts. This includes managing CLM permissions for all eligible users.

These bulk actions require that you have an Enterprise Pro plan or above or have the Organization Management add-on.

> **Note:** CLM administrators without the required plan or add-on are also able to manage users with these bulk actions, though they are limited to working within a single account at a time.

The following bulk actions are available:

- Bulk Add New Users
- Bulk Update Users
- Bulk Close Users
- User List Exports

Bulk Add New Users

> **Note:** This guide is for DocuSign administrators who oversee multiple accounts. For administrators of individual accounts, see the DocuSign eSignature Admin guide Add and Update Users in Bulk.

DocuSign Administrators and Users Administrators can bulk add new users to one or more accounts by uploading a comma-separated value (CSV) file. The format of the CSV must match the sample file. For more information on the CSV format, see Build a CSV to Bulk Add Users.

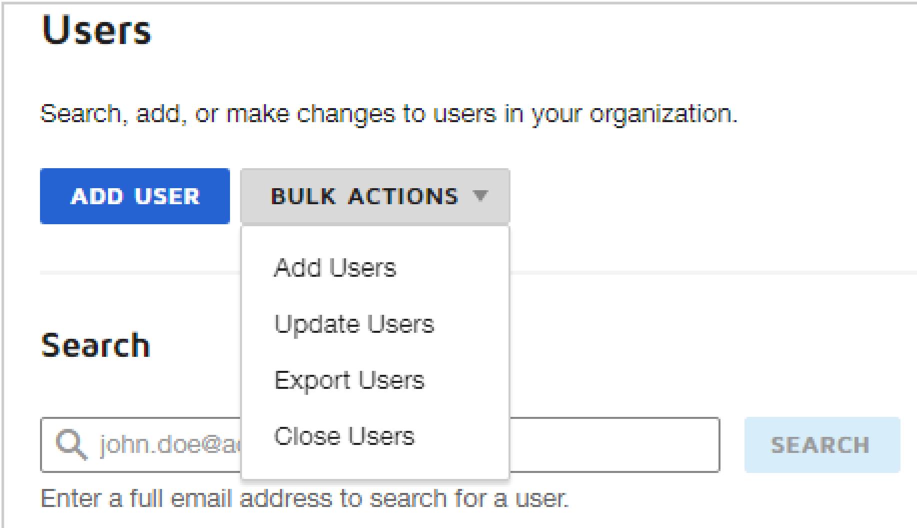
You can add up to 2,000 users to an account and include up to 50 accounts per imported CSV. The maximum number of users per import is 8,000.

> **Note:** Only one type of import or export can be in progress at a time.

Add Users in Bulk

1. From the DocuSign Admin dashboard, click the **Users** tile.

2. Click the **BULK ACTIONS** menu and select **Add Users**.



3. In the Add Users dialogue, click **UPLOAD FILE**.

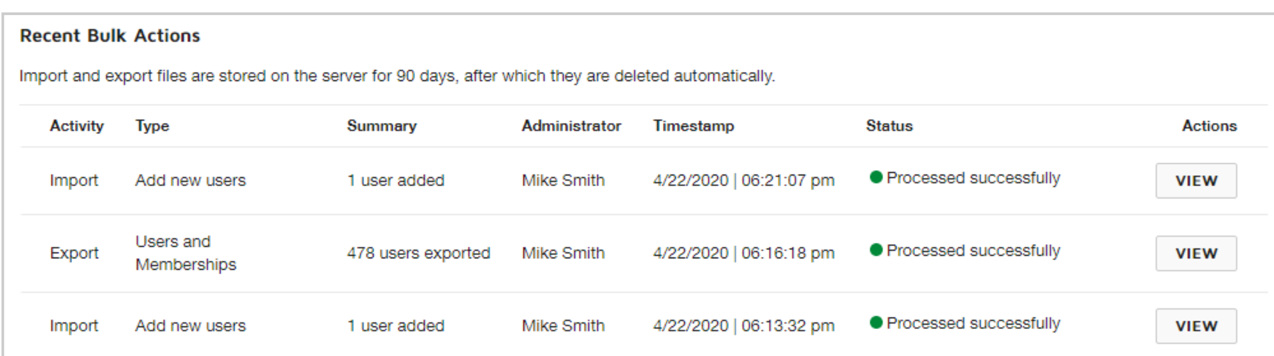
> **Note:** You can also drag and drop your prepared CSV file in the upload area.

4. Select the CSV file to import. Make sure the formatting matches the sample CSV provided. For more details, see Build a CSV to Bulk Add Users.

> **Note:** Click **DOWNLOAD TEMPLATE** to download a sample CSV file that you can use to build your import.

5. Click **SUBMIT**.

6. View the status of your import in the **Recent Bulk Actions** section on the Users page. Click the refresh icon to update the import status. When the import is complete, click **VIEW**.


Recent Bulk Actions

Import and export files are stored on the server for 90 days, after which they are deleted automatically.

Activity	Type	Summary	Administrator	Timestamp	Status	Actions
Import	Add new users	1 user added	Mike Smith	4/22/2020 | 06:21:07 pm	Processed successfully	VIEW
Export	Users and Memberships	478 users exported	Mike Smith	4/22/2020 | 06:16:18 pm	Processed successfully	VIEW
Import	Add new users	1 user added	Mike Smith	4/22/2020 | 06:13:32 pm	Processed successfully	VIEW

Build a CSV to Bulk Add Users

Your CSV import file is made up of a header row with the column headers and a row of user or account data for each user you want to add to an account. Only new users can be imported. Any changes to existing users will be ignored. To make changes to existing users, see Bulk Update Users.

To ensure your CSV is properly formatted, use the Sample Bulk Add CSV file as a template.

The header row for add users

The first line of the file is the header row which defines each of the columns. The header values are not required to be in the order listed and are not case-sensitive, but the text must match listed values.

***Required columns:** Your CSV file must contain these columns: AccountID, FirstName, LastName, UserEmail, and eSignPermissionProfile. The rest of the header values are optional.

> **Note:** For the user's name, you can use either the FirstName and LastName columns together, or the User Name column. Your spreadsheet should only contain one of these; if both FirstName/LastName and UserName columns are present in your CSV, the values entered in the UserName column take precedence.

The EnableCLM and CLMPermissionProfile columns are only applicable for organizations with the CLM product. If your organization doesn't have a CLM account, leave these columns blank.

> **Note:** The LoginPolicy and AutoActivation columns only apply to organizations with a reserved domain and Single Sign-On (SSO) through an Identity Provider. For more information, see the DocuSign Single Sign-On Overview.

The acceptable column header values for an Add Users CSV file are:

Header Row Value	Description
AccountID	The 32 character API Account ID of the user's account in your organization. This can be found in the in the API and Keys section of the account. **Required column**.
AccountName	The name of the user's account in your organization. The account name must match the Account ID provided.
FirstName	The user's first name. **Required column**.
LastName	The user's last name. **Required column**.
UserName	The user's full name. This can be used instead of FirstName and LastName. This is useful for languages which place family names before given names. *****Required column.** If this column is used instead of FirstName and LastName, it is required.
UserEmail	The user's complete email address. **Required column**.
eSignPermissionProfile	The user's permission profile for the eSignature product. This value must match an existing permission profile for the account. This value is not case-sensitive.**Required column**.

Header Row Value	**Description**
EnableCLM	Grants the user access to the CLM product. If you grant a user access to CLM, you must also assign them a Permission profile for that product with the CLMPermissionProfile column. • TRUE - The user has access to CLM. • FALSE - The user does not have access to CLM.
CLMPermissionProfile	The user's permission profile for the CLM product. This value must match an existing permission profile for the account. This value is not case-sensitive. If you assign a user a CLM permission Profile, you must also grant them access to the CLM product with the EnableCLM column.
UserTitle	The user's job title.
CompanyName	The user's company name.
Group	The user's assigned groups. The Group values must match existing Group names for the account. Additional Group columns can be added to the file to add users to more than one group. You do not need to add users to the Everyone group, since all new users are automatically added to that group.
AddressLine1	The user's address - first line.
AddressLine2	The user's address - second line.
City	The user's city name.
StateRegionProvince	The user's regional location.
PostalCode	The user's postal code.
Phone	The user's phone number.
Language	The user's display language for their DocuSign account. See the Display Language Values below.

Header Row Value	**Description**
LoginPolicy	The user's login policy. Valid values include the following: • Column left blank - The user is created with no policy assigned. • FedAuthRequired - The user must log in with an Identity Provider. • FedAuthBypass - The user may log in with an Identity Provider or their DocuSign username and password. For more information on login policies, see Setting a User Login Policy.
AutoActivate	For domain users, new users can be activated automatically for domain accounts using SSO by setting the value to TRUE. The user is activated automatically once the import is complete. Memberships activated in this way will not receive an activation email.

The access code option (adding an access code for authentication during user activation) cannot be used with this bulk action.

The user data

In the lines of the file below the header row, add the user information with commas used as the delimiter (separator) between each value.

If you are using Microsoft® Excel® to create your file, you can enter the header values (FirstName, LastName, UserEmail, etc.) in different columns on the first line, enter the user information on subsequent lines, and save the file as a CSV file. You do not need to add commas; Excel will automatically do this when you save the file.

Example Add Users - Excel:

	A	B	C	D	E	F
1	AccountID	AccountName	APIUserName	FirstName	LastName	UserEmail
2	8d4e68a3-d666-44b8-82c3-0011fbe8315e	Purchasing	42dabc1b-a9a0-477c-8079-4cf8aba0e017	Hans	Moleman	h.moleman@example.com
3	8d4e68a3-d666-44b8-82c3-0011fbe8315e	HR Department	14e68a20-69f3-47b9-8bdd-33686c6c5666	Frank	Grimes	f.grimes@example.com
4	8d4e68a3-d666-44b8-82c3-0011fbe8315e	Sales	78e9727b-1881-4681-8813-cee971e35d87	Mindy	Simmons	m.simmons@example.com

Display Language Values

The Language value is the default language for the user. The value can be any of the codes shown below:

Language = Code

- Chinese Simplified = zh_CN
- Chinese Traditional = zh_TW
- Dutch = nl

- English = en
- French = fr
- German = de
- Italian = it
- Japanese = ja
- Korean = ko
- Portuguese = pt
- Portuguese Brazil = pt_BR
- Russian = ru
- Spanish = es

Bulk Update Users

Note: This guide is for DocuSign administrators who oversee multiple accounts. For administrators of individual accounts, see the DocuSign eSignature Admin guide Add and Update Users in Bulk.

DocuSign Administrators and Users Administrators can bulk update existing users across one or more accounts by uploading a comma-separated value (CSV) file. For more information on the CSV format, see Build a CSV to Bulk Update Users.

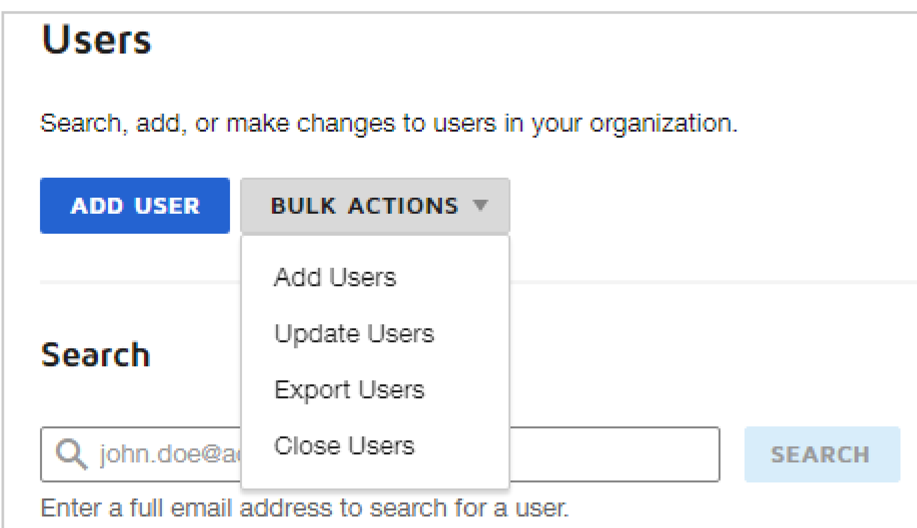
You can update up to 2,000 users on an account and include up to 50 accounts per imported CSV. The maximum number of updated users per import is 8,000. Only one type of import or export can be in progress at a time.

Note: DocuSign administrators with a claimed domain can also update email addresses for users on their domain. For more information, see Update User Email Addresses.

Update Users in Bulk

1. From the DocuSign Admin dashboard, click the **Users** tile.

2. Click the **BULK ACTIONS** menu and select **Update Users**.



3. In the Update Users dialogue, click **UPLOAD FILE**.

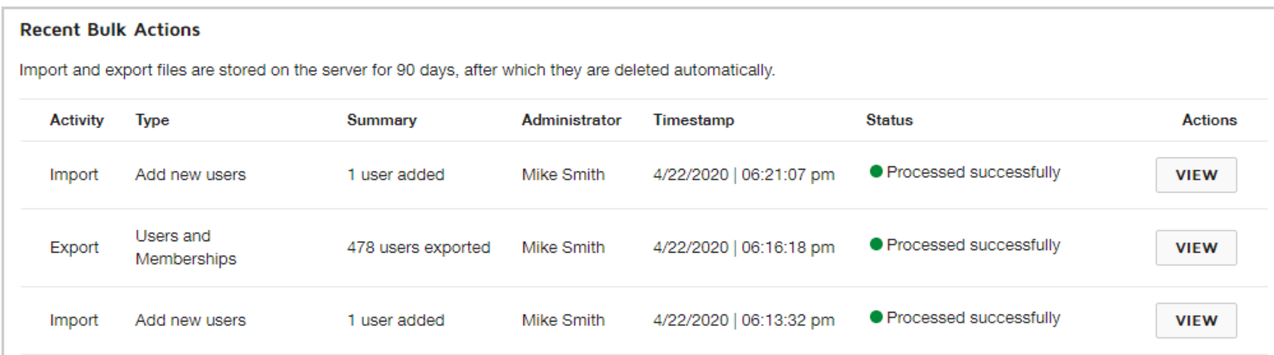
> **Note:** You can also drag and drop your prepared CSV file in the upload area.

4. Select the CSV file to import. Make sure the formatting matches the sample CSV provided. For more details, see Build a CSV to Bulk Update Users.

> **Note:** Click **EXPORT USERS**, select the user list type, then click **EXPORT** to export a CSV list of all users in your organization. You can use this list as a template to build your import. For more information on the various user list types, see User List Exports.

5. Click **SUBMIT**.

6. View the status of your import in the **Recent Bulk Actions** section on the Users page. Click the refresh icon to update the import status. When the import is complete, click **VIEW**.


Recent Bulk Actions

Import and export files are stored on the server for 90 days, after which they are deleted automatically.

Activity	Type	Summary	Administrator	Timestamp	Status	Actions
Import	Add new users	1 user added	Mike Smith	4/22/2020 | 06:21:07 pm	Processed successfully	VIEW
Export	Users and Memberships	478 users exported	Mike Smith	4/22/2020 | 06:16:18 pm	Processed successfully	VIEW
Import	Add new users	1 user added	Mike Smith	4/22/2020 | 06:13:32 pm	Processed successfully	VIEW

Build a CSV to Bulk Update Users

Your CSV import file is made up of a header row with the column headers and a row of account and user data for each user you want to update. Only existing users will be updated; to add new users, see Bulk Add New Users.

> **Tip:** To start, create a user list from accounts within your organization. The user data in this list can be used to populate your bulk update CSV file.

To ensure your CSV is properly formatted, use the Sample Bulk Add CSV file as a template.

The header row for update users

The first line of the file is the header row which defines each of the columns. The header values are not required to be in the order listed and are not case-sensitive, but the text must match listed values.

> **Note:** If you're changing a user's name, use either the FirstName and LastName columns together, or the User Name column. Your spreadsheet should only contain one of these.

***Required columns:** Your CSV file must contain these columns: AccountID, APIUserName, and UserEmail. The rest of the header values are optional.

Note: All of the required columns must remain unchanged.

The acceptable column header values for an Update Users CSV file are:

Header Row Value*	**Description**
AccountID	The 32 character API Account ID of the user's account in your organization. **Required column**.
AccountName	The name of the account.
APIUserName	The unique user ID. **Required column**.
FirstName	The user's first name.
LastName	The user's last name.
UserName	The user's full name.
UserEmail	The user's complete email address. To update the user's email address, use the UpdatedUserEmail column. **Required column**.
eSignPermissionProfile	The user's permission profile for the eSignature product. This value must match an existing permission profile for the account. This value is not case-sensitive.
EnableCLM	Grants the user access to the CLM product. If you grant a user access to CLM, you must also assign them a Permission profile for that product with the CLMPermissionProfile column. • TRUE - The user has access to CLM. • FALSE - The user does not have access to CLM.
CLMPermissionProfile	The user's permission profile for the CLM product. This value must match an existing permission profile for the account. This value is not case-sensitive. If you assign a user a CLM permission Profile, you must also grant them access to the CLM product with the EnableCLM column.
Language	The user's display language for their DocuSign account. See the Display Language Values below.
UserTitle	The user's job title.
CompanyName	The user's company name.
AddressLine1	The user's address - first line.
AddressLine2	The user's address - second line.
City	The user's city name.
StateRegionProvince	The user's regional location.
PostalCode	The user's postal code.
Phone	The user's phone number.

Header Row Value*	**Description**
LoginPolicy	The user's login policy. Valid values include the following: • Column left blank = The user is created with no policy assigned. • FedAuthRequired = The user must log in with an Identity Provider. • FedAuthBypass = The user may log in with an Identity Provider or their DocuSign username and password. For more information on login policies, see Setting a User Login Policy.
Group	The user's assigned groups. The Group values must match existing Group names for the account. Additional Group columns can be added to the file to add users to more than one group. You do not need to add users to the Everyone group, since all new users are automatically added to that group.
UpdatedUserEmail	If updating domain user email addresses, use this column to enter the new email address. For more information see Update User Email Addresses.

The user data

In the lines of the file below the header row, add the user information with commas used as the delimiter (separator) between each value.

If you are using Microsoft® Excel® to create your file, you can enter the header values (FirstName, LastName, UserEmail, etc.) in different columns on the first line, enter the user information on subsequent lines, and save the file as a CSV file. You do not need to add commas; Excel will automatically do this when you save the file.

Example Update Users - Excel:

	A	B	C	D	E	F
1	AccountID	AccountName	APIUserName	FirstName	LastName	UserEmail
2	8d4e68a3-d666-44b8-82c3-0011fbe8315e	Purchasing	42dabc1b-a9a0-477c-8079-4cf8aba0e017	Hans	Moleman	h.moleman@example.com
3	8d4e68a3-d666-44b8-82c3-0011fbe8315e	HR Department	14e68a20-69f3-47b9-8bdd-33686c6c5666	Frank	Grimes	f.grimes@example.com
4	8d4e68a3-d666-44b8-82c3-0011fbe8315e	Sales	78e9727b-1881-4681-8813-cee971e35d87	Mindy	Simmons	m.simmons@example.com

Update User Email Addresses

DocuSign Administrators and Users Administrators with a claimed domain can update email addresses for users on their domain.

You can update email addresses for your users if the following conditions are met:

- The organization has claimed the domain. For more information, see Domains.

- The user's email address is on the domain. For example, if your domain is www.example.com, the user's email would be user@example.com.
- If the organization has more than one claimed domain, you can also update the domain of the user to match another claimed domain.

> **Note:** You cannot change an email address for a user on a domain you have not claimed.

To change a user's email address, download and populate the sample CSV provided. The UserEmail column will remain unchanged and should contain the current user's email address.

In the UpdateUserEmail column, enter the new email address you'd like to use. After completing the import, the user's email address is updated.

Display Language Values

The Language value is the default language for the user. The value can be any of the codes shown below:

Language = Code

- Chinese Simplified = zh_CN
- Chinese Traditional = zh_TW
- Dutch = nl
- English = en
- French = fr
- German = de
- Italian = it
- Japanese = ja
- Korean = ko
- Portuguese = pt
- Portuguese Brazil = pt_BR
- Russian = ru
- Spanish = es

Bulk Close Users

> **Note:** This guide is for DocuSign administrators who oversee multiple accounts. This feature is not currently available for eSignature administrators. To close users on an individual account, see Manage Users.

DocuSign Administrators and Users Administrators can bulk close existing users across one or more accounts by uploading a comma-separated value (CSV) file. For more information on the CSV format, see Build a CSV to Bulk Close Users.

If users created free or freemium accounts using a corporate email addresses, a DocuSign administrator may want to close these accounts. You can also bulk close these external domain accounts as long as they are not linked to an organization.

> **Note:** To learn more about managing domain users and other best practices, see Establish Control of your Company's DocuSign Agreements.

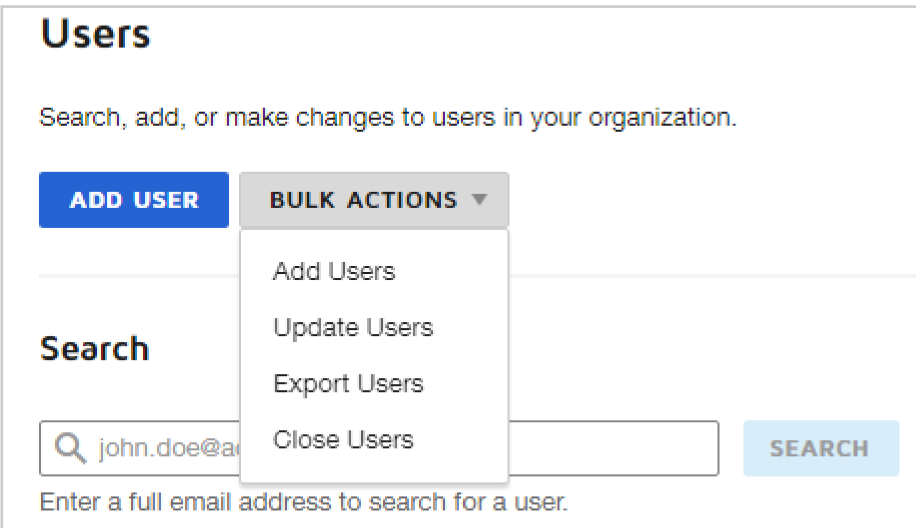
You can close up to 2,000 users on an account across up to 50 accounts per imported CSV. The maximum number of closed users per import is 8,000.

CONTENTS

Close Organization Users in Bulk

1. From the DocuSign Admin dashboard, click the **Users** tile.

2. Click the **BULK ACTIONS** menu and select **Close Users**.



3. In the Close Users dialogue, select **Close existing users**.

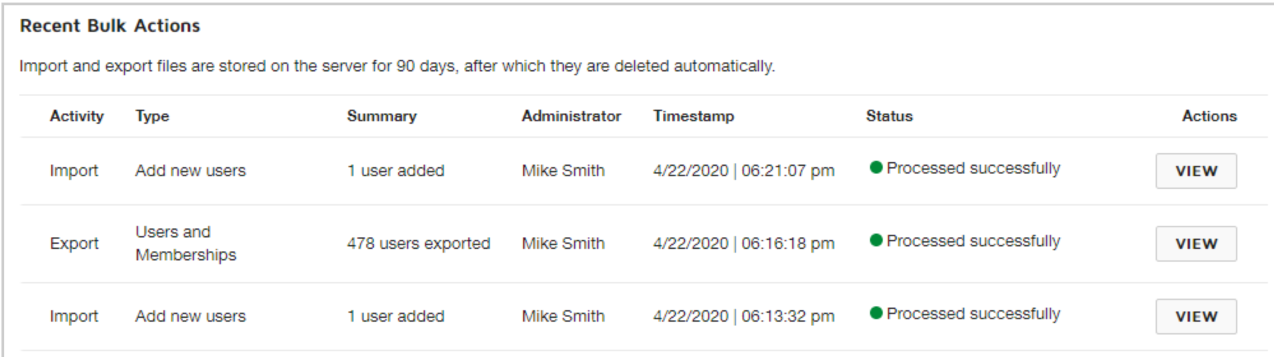
> **Note:** Users closed in this manner will also automatically be removed from any signing groups. If you'd like to leave these users in signing groups, Uncheck **Remove users from signing groups**.

4. Select the CSV file to import. Make sure the formatting matches the sample CSV provided. For more details, see Build a CSV to Bulk Close Users.

> **Note:** Click **EXPORT USERS**, select the user list type, then click **EXPORT** to export a CSV list of all users in your organization. You can use this list as a template to build your import. For more information on the various user list types, see User List Exports.

5. Click **SUBMIT**.

6. View the status of your import in the **Recent Bulk Actions** section on the Users page. Click the refresh icon to update the import status. When the import is complete, click **VIEW**.



Recent Bulk Actions

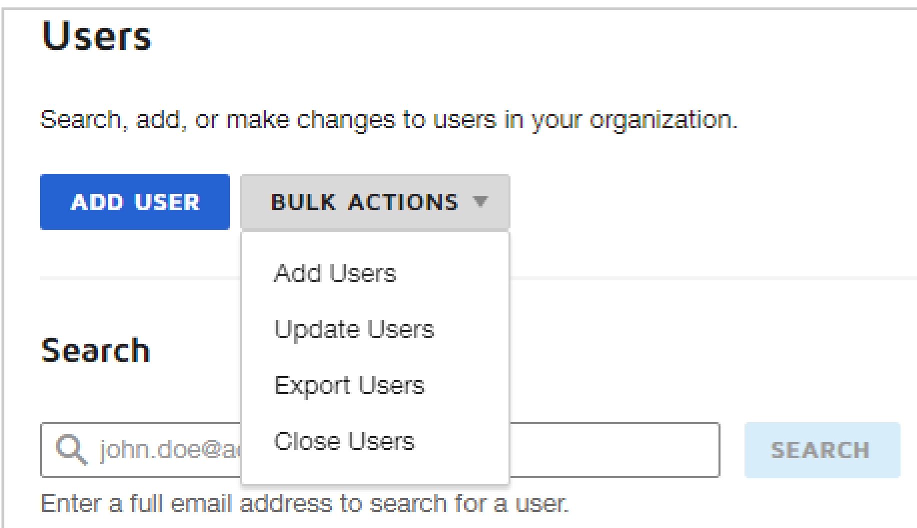
Import and export files are stored on the server for 90 days, after which they are deleted automatically.

Activity	Type	Summary	Administrator	Timestamp	Status	Actions
Import	Add new users	1 user added	Mike Smith	4/22/2020 | 06:21:07 pm	Processed successfully	VIEW
Export	Users and Memberships	478 users exported	Mike Smith	4/22/2020 | 06:16:18 pm	Processed successfully	VIEW
Import	Add new users	1 user added	Mike Smith	4/22/2020 | 06:13:32 pm	Processed successfully	VIEW

Close External Domain Users in Bulk

1. From the DocuSign Admin dashboard, click the **Users** tile.

2. Click the **BULK ACTIONS** menu and select **Close Users**.



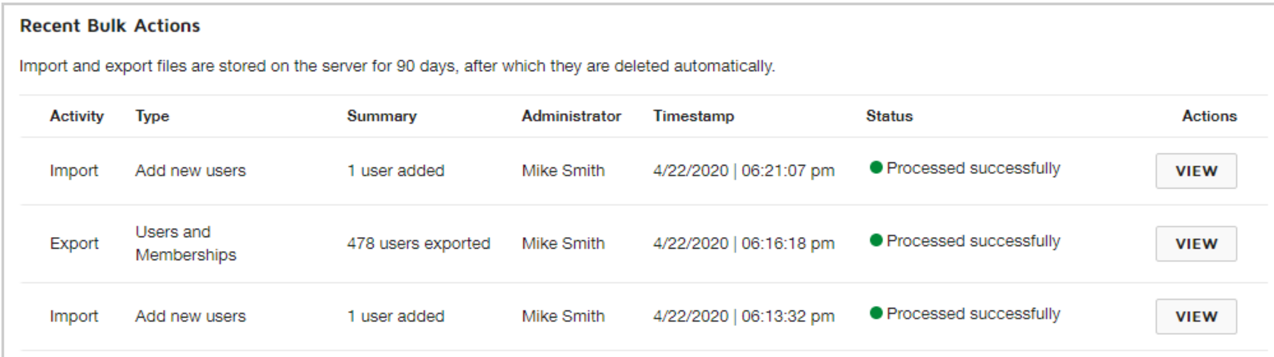
3. In the Close Users dialogue, select **Close external domain users**.

4. Select the CSV file to import. Make sure the formatting matches the sample CSV provided. For more details, see Build a CSV to Bulk Close Users.

> **Note:** Click **EXPORT USERS**, select the user list type, then click **EXPORT** to export a CSV list of all users in your organization. You can use this list as a template to build your import. For more information on the various user list types, see User List Exports.

5. Click **SUBMIT**.

6. View the status of your import in the **Recent Bulk Actions** section on the Users page. Click the refresh icon to update the import status. When the import is complete, click **VIEW**.



Build a CSV to Bulk Close Users

Your CSV file is made up of a header row with the column headers and a row of account and user data for each user you want to close.

> **Tip:** Start by exporting a user list from your organization. The user data in this list can be used to populate your bulk close CSV file.
>
> - For organization users, use the 'Users and Memberships' or 'Domain Users' export type.
> - For external domain users, use the 'External Domain Users' export type.

To ensure your CSV is properly formatted, use the Sample Bulk Close CSV file as a template.

The header row for close users

The first line of the file is the header row which defines each of the columns. The AccountID column must be the first column in the file.

***Required columns:** Your CSV file must contain these columns: AccountID, APIUserName, and UserEmail. No other columns are necessary.

The acceptable column header values for a Close Users CSV file are:

Header Row Value*	Description
AccountID	The 32 character API Account ID of the user's account in your organization. **Required column**.
APIUserName	The unique user ID. **Required column**.
UserEmail	The user's complete email address. **Required column**

The user data

In the lines of the file below the header row, add the user information with commas used as the delimiter (separator) between each value.

If you are using Microsoft® Excel® to create your file, you can enter the header values (AccountID, APIUserName, UserEmail) in different columns on the first line, enter the user information on subsequent lines, and save the file as a CSV file. You do not need to add commas; Excel will automatically do this when you save the file.

User List Exports

Note: This guide is for DocuSign administrators who oversee multiple accounts. For administrators of individual accounts, see the DocuSign eSignature Admin guide Add and Update Users in Bulk.

DocuSign Administrators and Users Administrators can export a list of users across all accounts in the organization as a comma-separated value (CSV) file. Exports include user details such as full name, email address, and permission profile.

Export types:

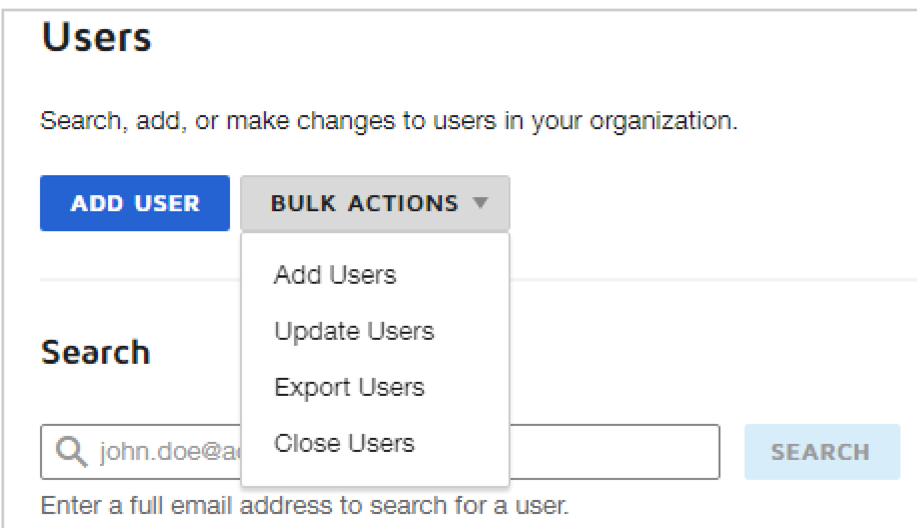
- **Users and Memberships:** All users and their memberships across all accounts in the organization.
- **Domain Users:** All domain users, their profile details, default account, and login policy.
- **External Domain Users:** All domain users memberships in accounts external to the organization.

Note: Organizations without a claimed domain will see only the Users and Memberships export option.

Export a List of Users

1. From the DocuSign Admin dashboard, click the **Users** tile.

2. Click the **BULK ACTIONS** menu and select **Export Users**.



3. Select the export type and click **EXPORT**.

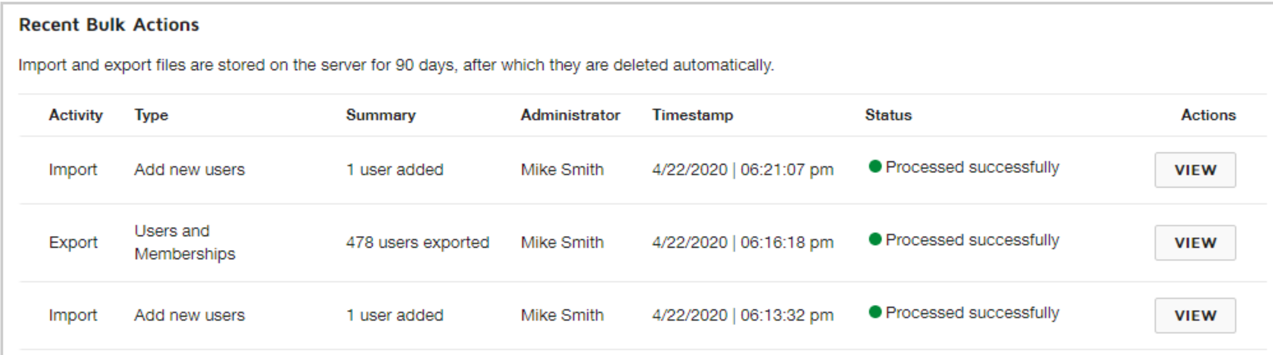
   Export types:

   - **Users and Memberships:** All users and their memberships across all accounts in the organization.
   - **Domain Users:** All domain users, their profile details, default account, and login policy.
   - **External Domain Users:** All domain users memberships in accounts external to the organization.

   Note: Organizations without a claimed domain will see only the Users and Memberships export option.

4. View the status of your export in the **Recent Bulk Actions** section on the Users page. Click the refresh icon to update the import status. When the export is complete, click **VIEW**.

5. Click **DOWNLOAD** to download the export CSV file.



Recent Bulk Actions

Import and export files are stored on the server for 90 days, after which they are deleted automatically.

Activity	Type	Summary	Administrator	Timestamp	Status	Actions
Import	Add new users	1 user added	Mike Smith	4/22/2020 | 06:21:07 pm	Processed successfully	VIEW
Export	Users and Memberships	478 users exported	Mike Smith	4/22/2020 | 06:16:18 pm	Processed successfully	VIEW
Import	Add new users	1 user added	Mike Smith	4/22/2020 | 06:13:32 pm	Processed successfully	VIEW

Data Feeds

Note: This guide is for DocuSign administrators who oversee multiple accounts. For administrators of individual accounts, see the DocuSign eSignature User guide Using Reports.

Once configured by your development team, your organization can retrieve data from all of your accounts. This data can be stored in your data warehouse and used as needed.

Note: Setting up a data feed requires additional steps DocuSign support and your development team. For more information, contact DocuSign customer support.

Add an Integration Key

The data feed requires an integration key from an account within the organization.

1. Generate and copy an integration key from the API and Keys page on an account within the organization.

   Note: You must be an administrator on an account within your organization to generate an integration key. For more information, review Apps and Keys in the DocuSign eSignature Admin Guide.

2. Click **SWITCH TO...** and select **DOCUSIGN ADMIN** to return to DocuSign Admin.

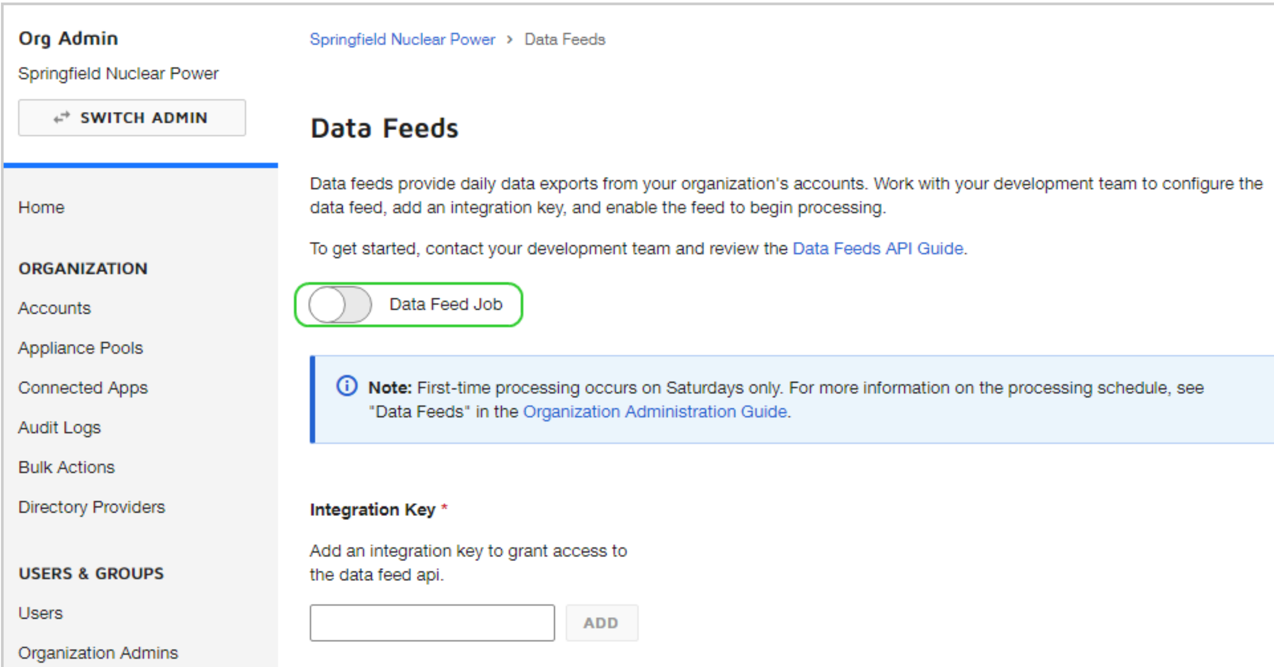
3. From the DocuSign Admin dashboard, click the **Data Feeds** tile.

4. Paste the integration key into the text field and click **ADD**.

Enable or Disable the Data Feed

1. From the DocuSign Admin dashboard, click the **Data Feeds** tile.

2. Click the **Data Feed Job** toggle to begin processing.



The data feed begins processing when an integration key is present and the feed has been configured.

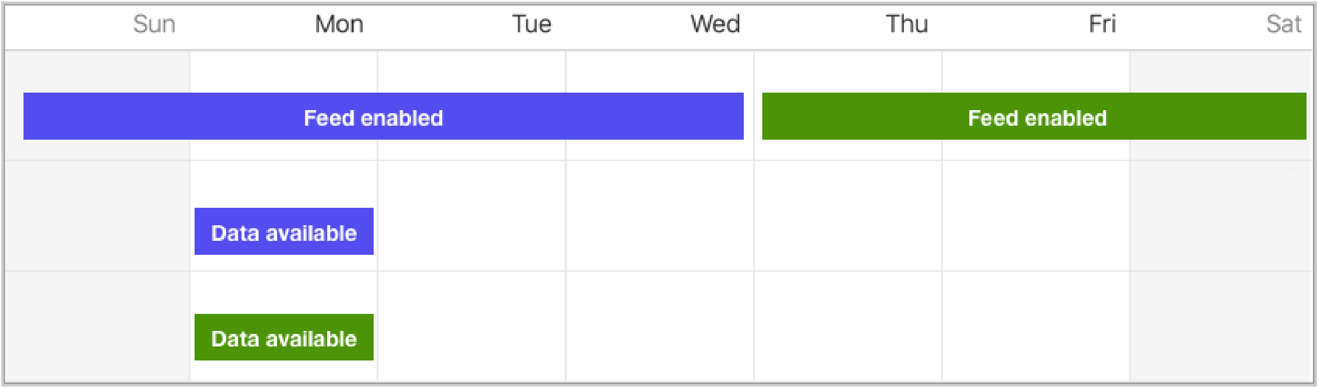
Data Feed Processing Schedule

Once configured, your data feed begins to process. Extra time is needed to collect data for the first time. Subsequent changes to the feed are available within 24 hours.

The first data feed process uses the following schedule:

Feed is Enabled On	Data is Available On
Sunday through Wednesday	Next Monday (5 days after Wednesday)
Thursday through Saturday	Second Monday (9 days after Saturday)

For example:



Envelope Transfer

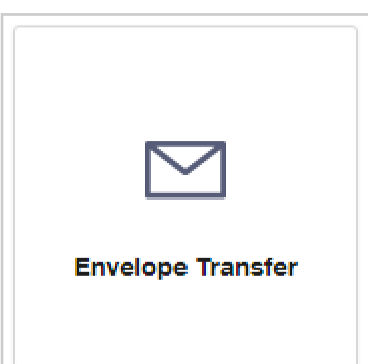
Note: This guide is for DocuSign administrators who oversee multiple accounts. For administrators of individual accounts, see Transfer Envelopes and Templates.

As a DocuSign Administrator, you can transfer envelopes between users on any organization accounts that are on the same DocuSign environment site. With envelope transfer, if you have employees who move between organization accounts, you can transfer some or all of their envelopes to go with them. Or you can transfer ownership of envelopes to a new user on any other organization account that is on the same site. You can transfer up to 2,000 eligible envelopes at one time.

CONTENTS

Envelope Transfer Overview

From the Envelope Transfer tile, you can initiate transfers and view transfer logs.



When you transfer ownership of envelopes, the transferred items are removed from the original owner's account and moved to the new owner's account. You must have All Administration Capabilities on the account you want to transfer envelopes from. You can transfer to any user's account that is part of your organization and that is on the same environment site as the originating account (e.g., NA1, NA2, NA3, EU).

> **Note:** Access to the envelope transfer feature must be enabled on your organization by DocuSign. If you do not see the Envelope Transfer tile on your DocuSign Admin dashboard, contact DocuSign customer support for more information.

What can you transfer?

You can transfer envelopes belonging to a user in an organization account for which you have All Administration Capabilities. The envelopes can be in any status except Draft. Draft envelopes cannot be transferred.

> **Note:** You can transfer up to 2,000 eligible envelopes at a time. You cannot transfer envelopes across sites (e.g. NA1 >NA2).

Who owns envelopes?

Users own the envelopes that they send. Ownership can be transferred by an administrator to another user. Received envelopes are owned by the sender and cannot be transferred to a different recipient.

Who can you transfer envelopes to?

You can transfer an envelope to any user on any account that is:

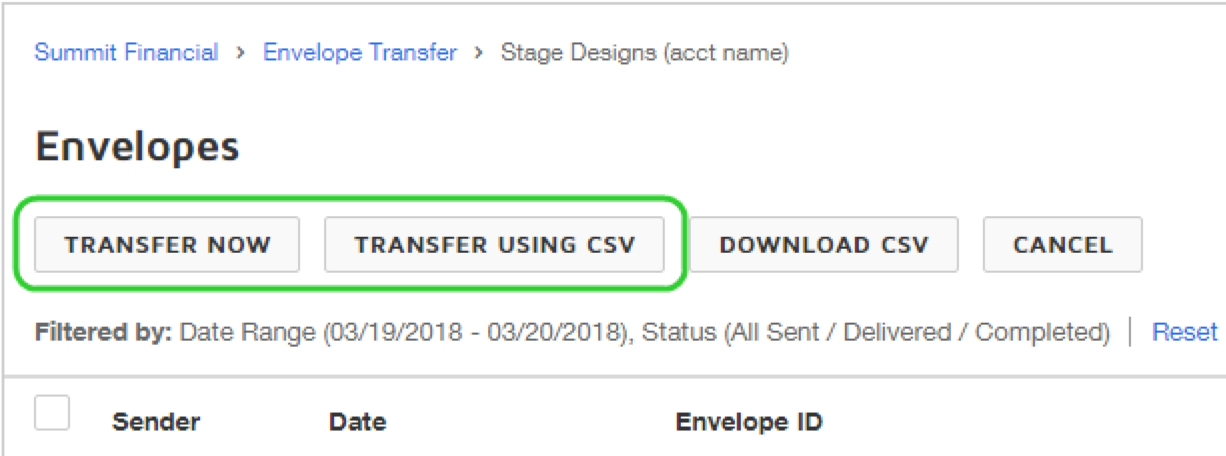
- Linked to your organization
- On the same DocuSign site environment as the originating account (e.g., NA1 -> NA1)

What happens when you transfer an envelope?

Transferring an envelope is a complete transfer of ownership. The envelope history retains all of the actions by the original sender, and includes a "Transfer envelope ownership" action indicating the new owner and account membership for the envelope.

Transfer options: Transfer Now and Transfer Using CSV

You can filter, search, and select one or more envelopes to transfer with the **Transfer Now** function. Or you can prepare and upload a CSV with a list of envelope IDs to **Transfer Using CSV**.



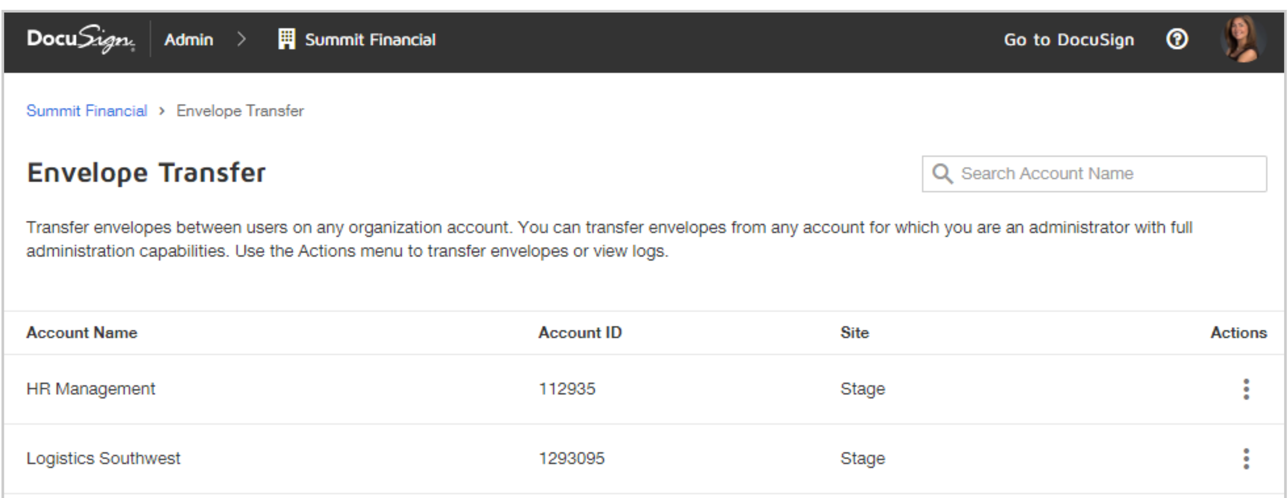
Transfer a Selection of Envelopes using Transfer Now

Select one or more envelopes to transfer manually from one user's account to any other user account within your organization. You must have All Administration Capabilities permissions on the account you are transferring from.

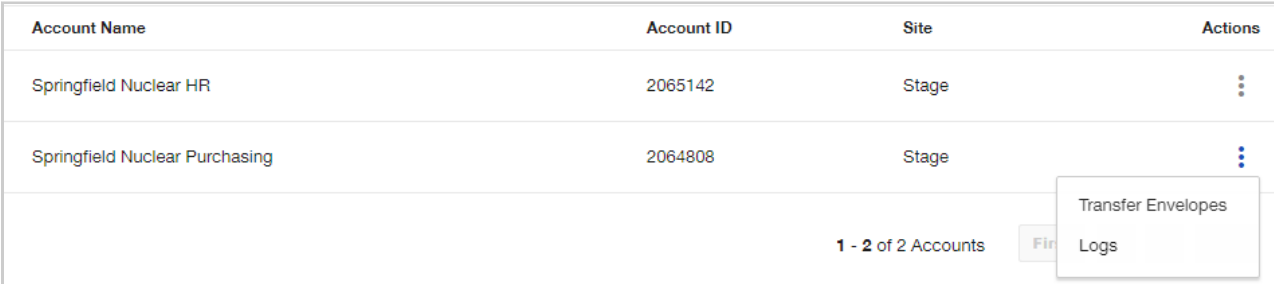
1. From the DocuSign Admin dashboard, click **Envelope Transfer**.

2. The Envelope Transfer view lists the linked accounts for which you have All Administration Capabilities permissions.

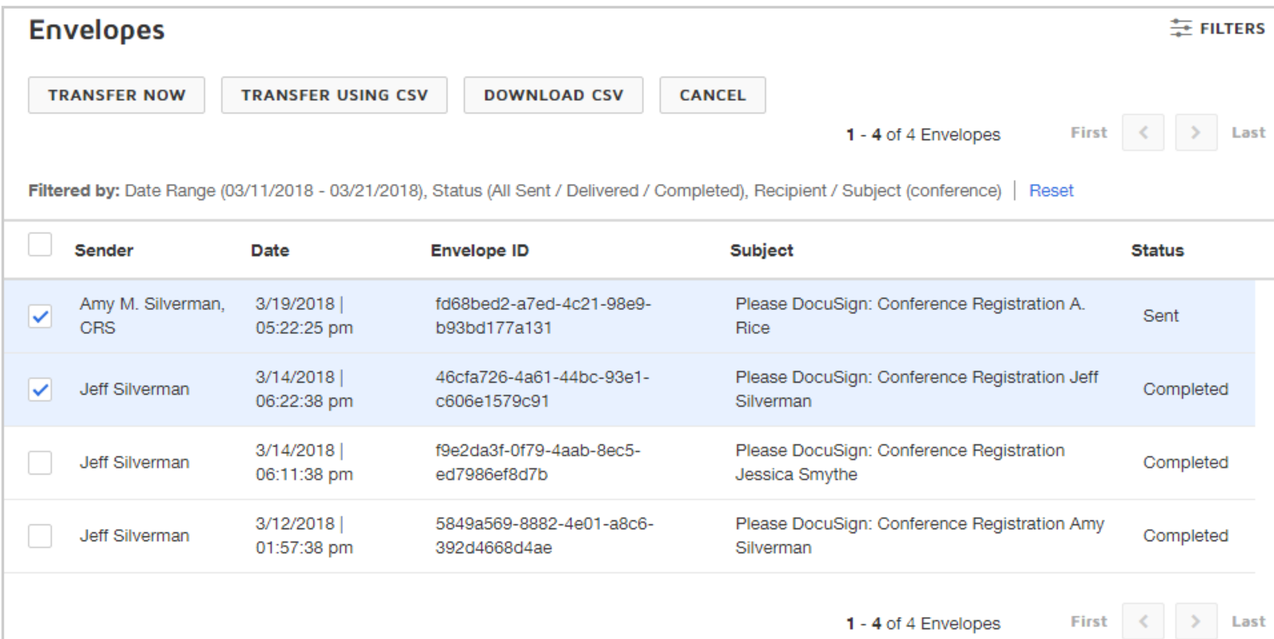
   If you do not see an account, it either needs to be linked to your organization, or you do not have the necessary permissions to initiate a transfer.



3. Locate the account you want to transfer from and click the **Actions** menu and select **Transfer Envelopes**.

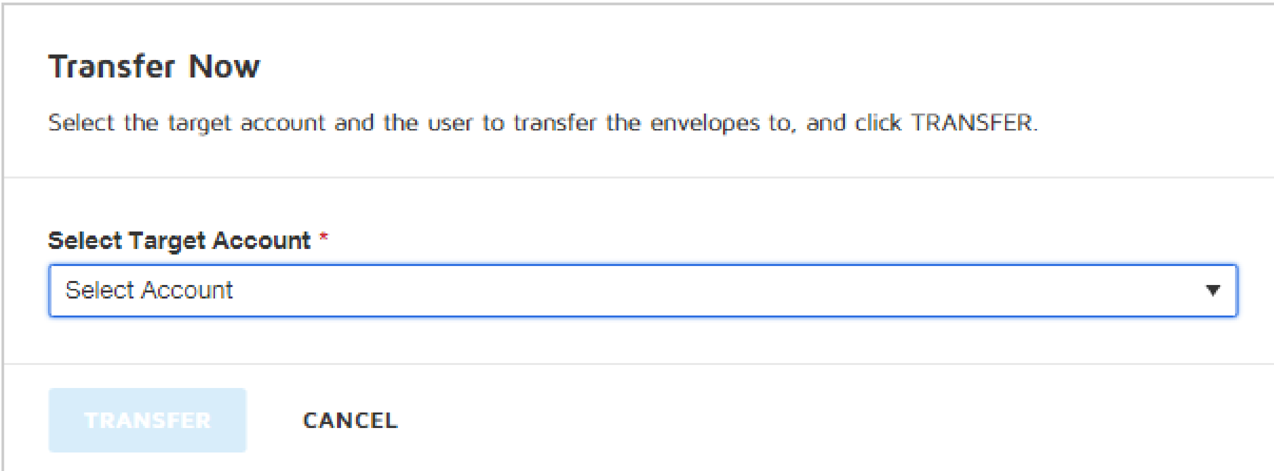


4. Select the items you want to transfer by selecting the check box on the corresponding rows. Use the **FILTERS** settings to change the list of items shown.



5. Click **TRANSFER NOW**.

6. In the Transfer Now dialog, select the target account you want to transfer the envelopes to. All linked accounts in the organization that are on the same site as the originating account are listed.

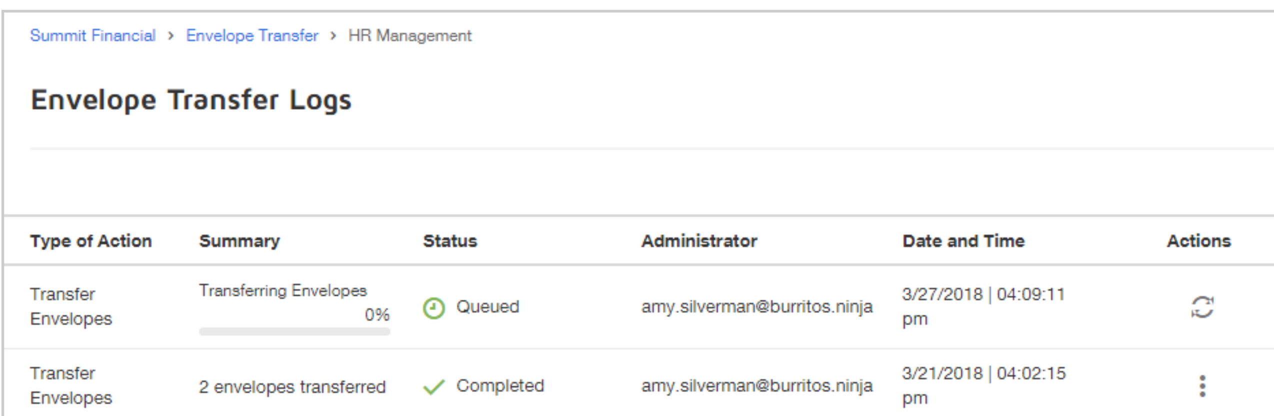


7. Click **TRANSFER**.

8. Select the user in the target account you want to transfer the envelopes to and click **TRANSFER**.

9. Confirm the transfer action.

   The job is placed in a queue for processing and listed in the Envelope Transfer Logs. This log shows a list of transfers for your organization. At the top of the list is the new transfer.



10. When the transfer is complete, the transferred envelopes are available in the new owner's account.

    - Click the **refresh icon** in the Actions column to update the status of the transfer.
    - Once the transfer completes, click the **Actions** menu and select **Details** to review the transfer information or download a copy of the CSV file with the transfer information.

Download Envelope IDs to Transfer Using CSV

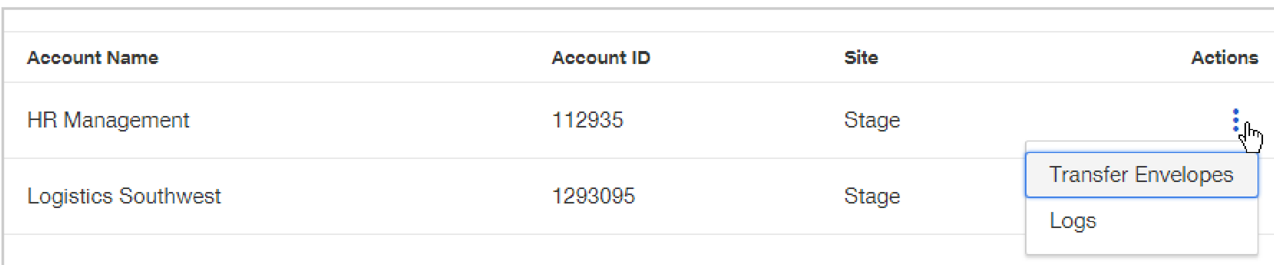
You can transfer envelopes in bulk to a single new owner by using a comma-separated value (CSV) file containing the envelope IDs to be transferred. The CSV file must contain a column with each envelope ID entered on a different row. The envelopes in the file must all exist in the same account but can belong to different users.

A common workflow for bulk transfer is:

- Use the Envelope Transfer page to filter for the envelopes you want to transfer.
- Download the list of envelopes using the Download CSV option.
- Review the download file and remove any unwanted data and remove all columns except for EnvelopeId.
- Use the Transfer Using CSV option to transfer the envelopes in bulk to the new owner.

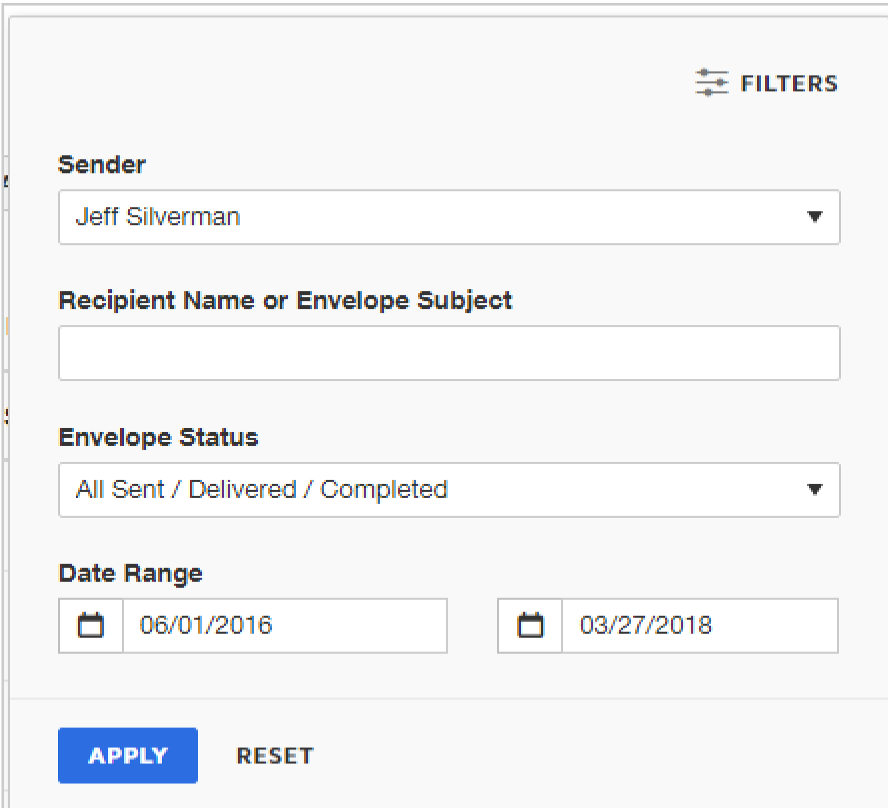
Download a CSV File of Envelope Information

1. From the Envelope Transfer page in DocuSign Admin, locate the account you want to transfer from and click the **Actions** menu and select **Transfer Envelopes**.



2. Select the items you want to transfer by using the **FILTERS** settings to change the list of items shown.

   For example, if you want to transfer ownership of all envelopes sent from one employee to another employee, select the employee's name in the Sender filter, and adjust the Date Range as needed.



3. Click **DOWNLOAD CSV** and select if you want to include recipient information or custom fields.

   These details are not used in the transfer process, but you may find them helpful for other purposes. For instance, you can use the envelope custom fields to help sort envelopes and identify the ones you want to transfer.

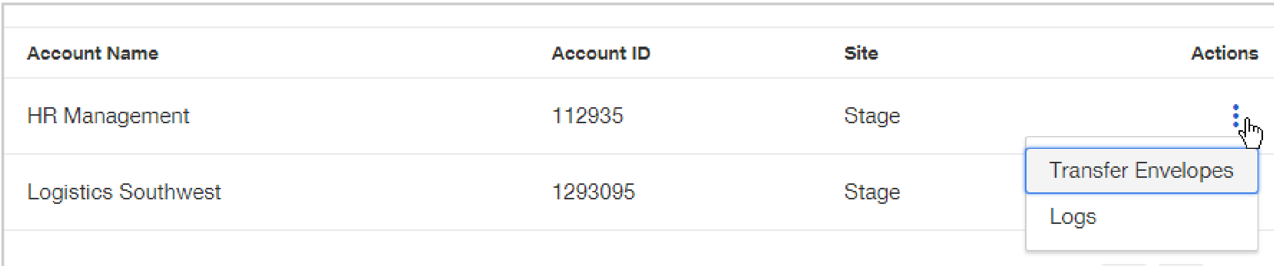
4. Click **DOWNLOAD**.

   The CSV is saved to your Downloads folder. Once you review it and make any changes to the list of envelope IDs, you can use the CSV to transfer the envelopes to another user.

Transfer Envelopes Using a CSV

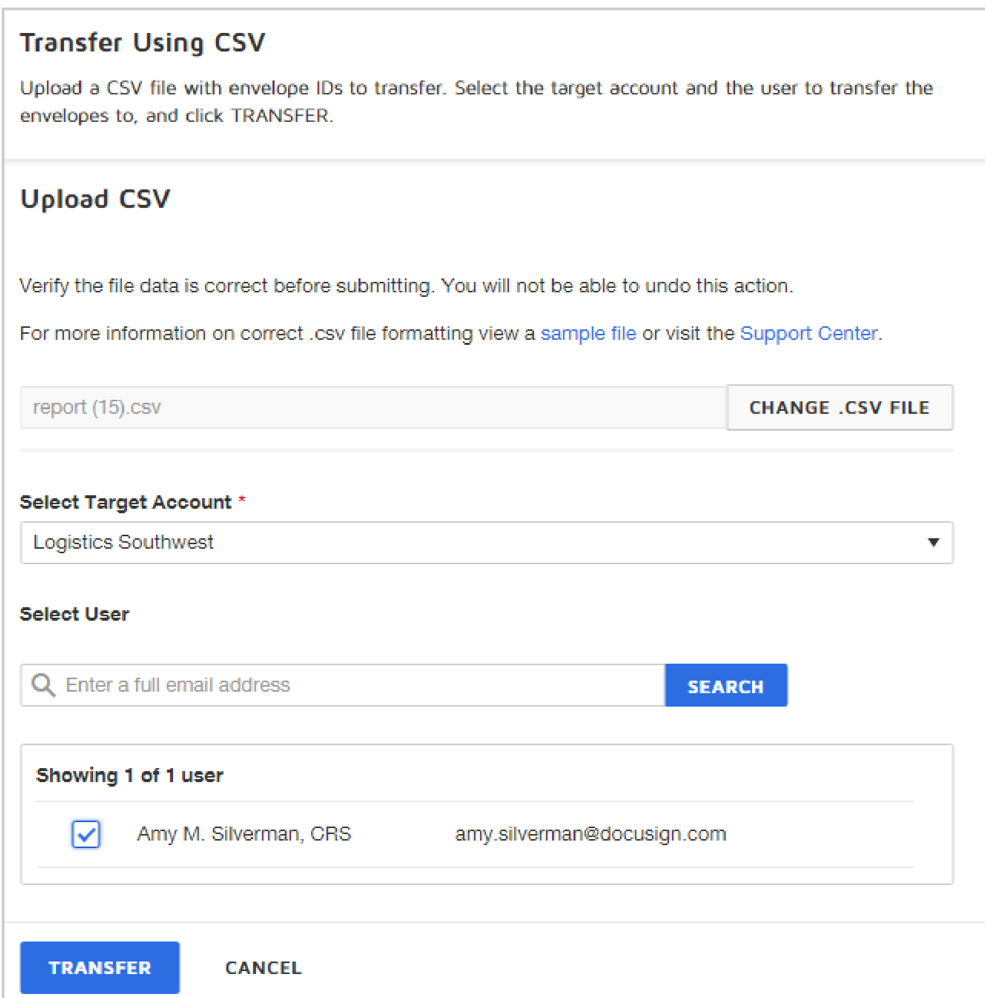
You can transfer envelopes in bulk using a prepared CSV with the envelope IDs to be transferred. All envelopes must be in the same organization account, and you can transfer them all to a single user in any organization account on the same site. You must have All Administration Capabilities permission on the originating account. Typically, you would download a list of envelope IDs to transfer as described in Download envelope IDs to transfer using CSV.

1. From the Envelope Transfer page in DocuSign Admin, locate the account you want to transfer from and click the **Actions** menu and select **Transfer Envelopes**.



2. Click **TRANSFER USING CSV** to initiate the transfer.

3. In the Transfer dialog:
   a) Upload the CSV containing the envelope IDs you want to transfer.
   b) Select the target account for the user you want to transfer the envelopes to.
   c) Select the user in the target account to transfer to.



   d) Click **TRANSFER**.

4. Confirm the transfer action.

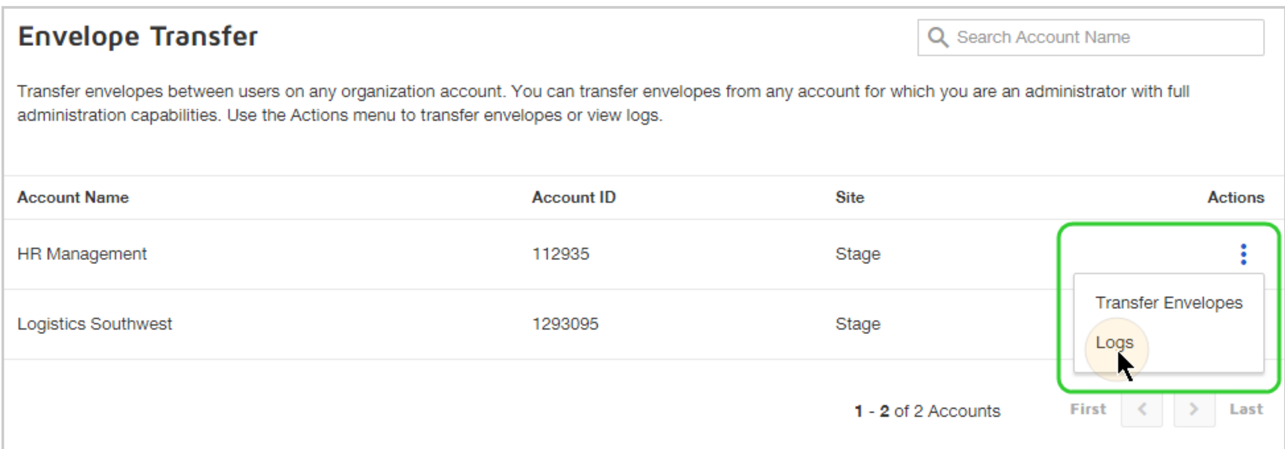
   The job is placed in a queue for processing and listed in the Envelope Transfer Logs. This log shows a list of transfers for your organization. At the top of the list is the new transfer.

View Envelope Transfer Logs

When you execute an envelope transfer, an entry for the job is added to the envelope transfer logs for the account you transferred envelopes from. You can review these logs for details of the transfer, including an option to download a CSV containing the envelope IDs and the processing results.

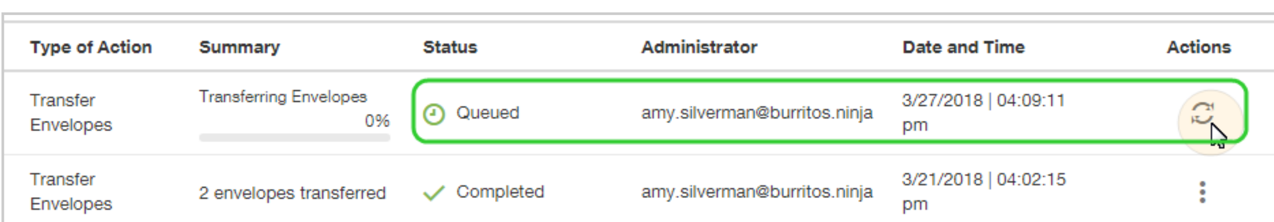
1. From the Envelope Transfer list, locate the account where the envelopes were transferred from.

2. Click the **Actions** menu and select **Logs**.



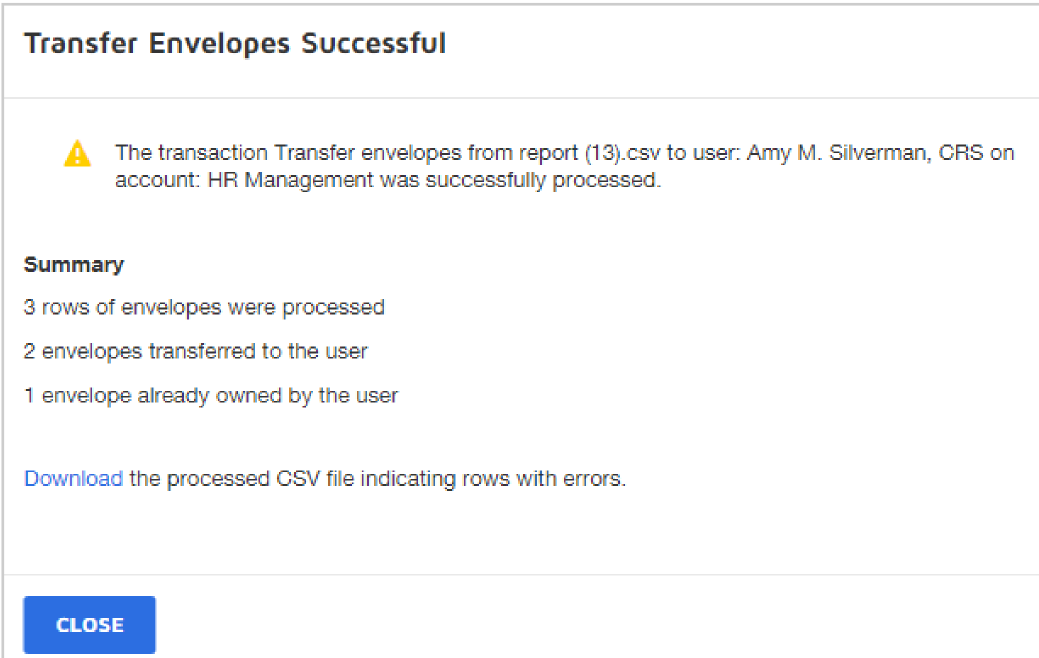
3. The list of available logs for the selected account are shown. The Status column provides a result summary.

4. For transfers with an incomplete status (Queued), click the **refresh icon** in the Actions column to update the transfer status.



5. For completed transfers, to see detailed results, click the **Actions** menu and select **Details**.

   The details dialog provides a summary of the successful transfers, as well as details around any rows with issues or errors.



6. To download a CSV with a list of all envelope IDs in the transfer job and the processing results for each, click **Download** from the transfer details dialog, or click the **Actions** menu for the transfer job and select **Download CSV**.

Related Topics

For more information related to envelope transfer, see the following:

- Link accounts: Accounts must be linked to your organization in order to transfer or receive envelopes.
- Establish Control of your Company's DocuSign Agreements: Gain control of your company's agreements with proven best practices and procedural guidelines.

Connected Apps

Manage the applications that can access your DocuSign organization. Connected applications are authorized for all domain users and access is limited by the permissions you specify.

You can authorize any application for which there is an existing integrator key in any account that is linked to your organization.

In order to authorize an application for your domain users, you must first claim a domain for your DocuSign organization. To learn more the domain claim process, see Claiming and validating a domain.

Note: For more information on integrator keys, see API and Keys. For more information about using your integrator key with the DocuSign API, visit the DocuSign Developer Center.

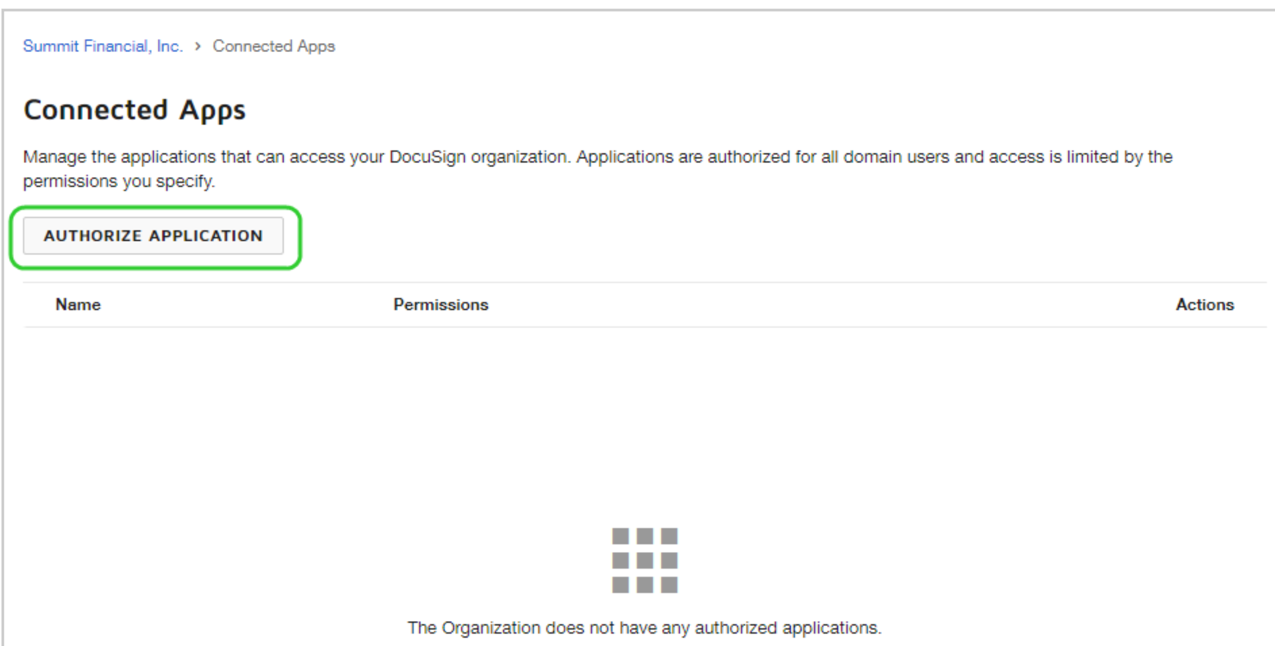
CONTENTS

Authorize an Application

Authorize integration applications for your domain users.

1. From the DocuSign Admin dashboard, click **Connected Apps**.

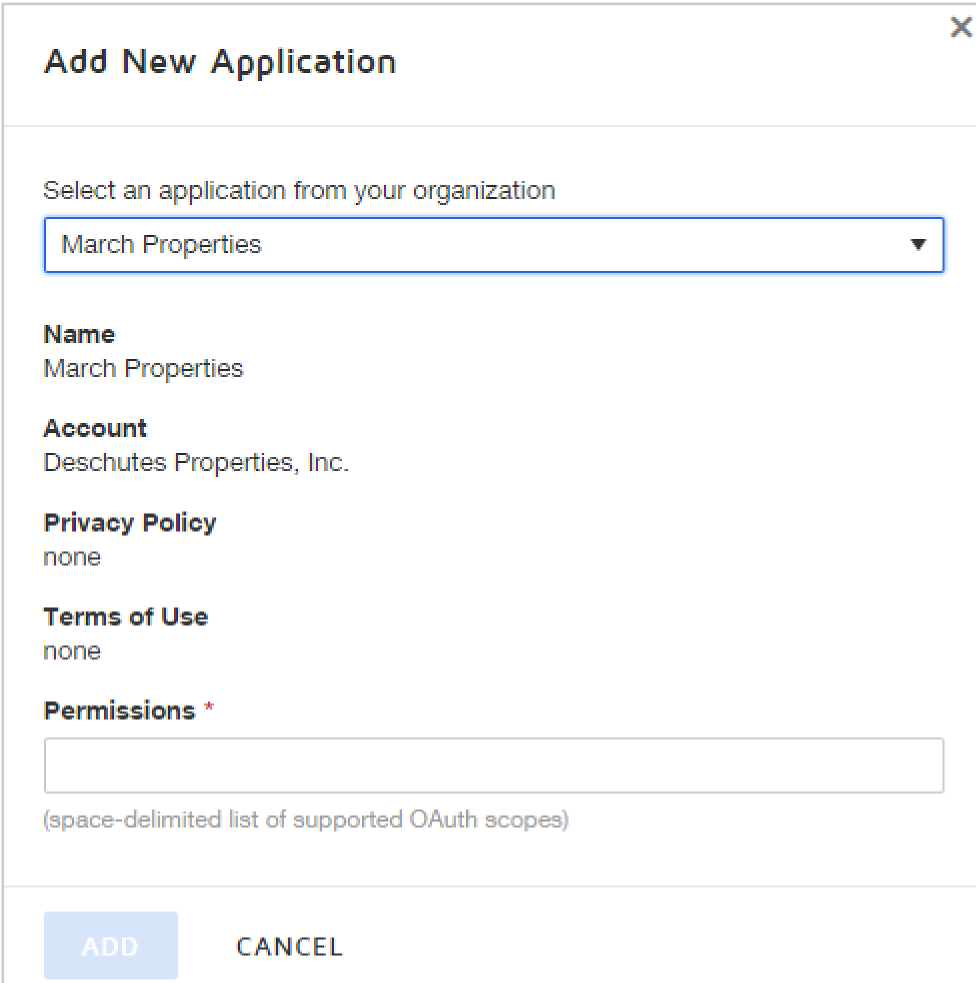
2. On the Applications page, click **Authorize Application**.



3. In the Add New Application dialog, select an application from the drop-down list. The list includes all applications for which there is an existing integrator key in any account that is linked to your organization.

   The dialog expands to show information about the selected application.

4. Enter the permissions for the application. These permissions define the OAuth scopes the application can access. Example: "signature"



Note: If adding more than one permission, separate them with a single space. For eSignature applications that use the OAuth JWT flow, add both the 'signature' and 'impersonation' permissions.

5. Click **Add**.

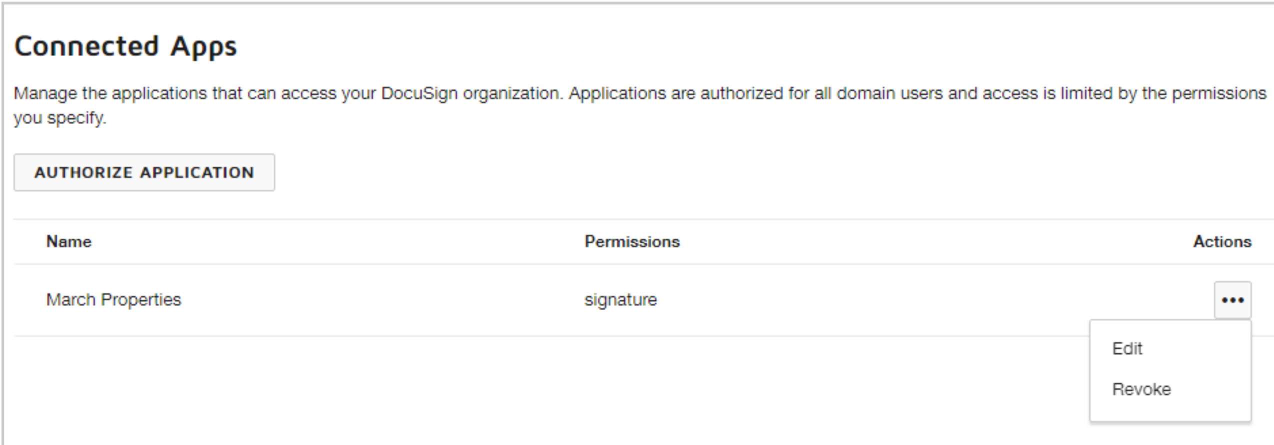
   The application is authorized and added to the list of Applications for the organization.

Edit an Authorized Application

You can edit the Permissions settings for an authorized application.

1. From the DocuSign Admin dashboard, click **Applications**.

2. Click the **Actions** menu for the application you want to edit, and select **Edit**.



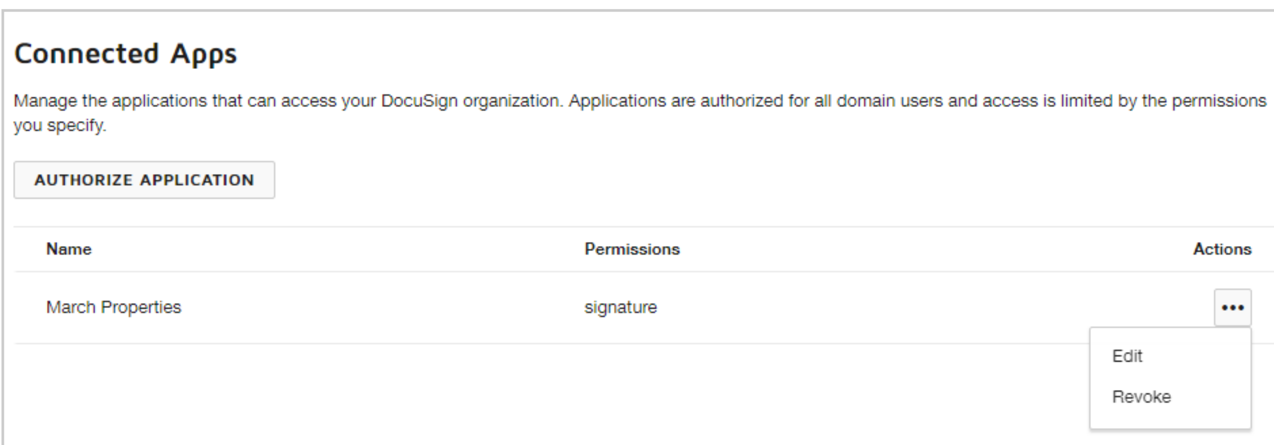
3. Modify the Permissions settings as needed, and click **Save**.

Revoke Authorization for an Application

You can revoke any previously authorized application.

1. From the DocuSign Admin dashboard, click **Applications**.

2. Click the **Actions** menu for the application you want to edit, and select **Revoke**.



The application is removed from your organization and access is revoked for all domain users.

Domains

Claiming domains requires that you have already created your organization as described in creating an organization. In order to claim a domain, you must have access to DocuSign Admin and have the Administrator permission profile.

> **Note:** Claiming a domain is also part of the authorization process for connected applications. For more information, see Connected Apps.

As a DocuSign administrator, you can claim domains for use with DocuSign through the Domains page of your organization. When you claim and verify an email domain for your organization, you can manage all users for that domain, across all accounts linked to the organization.

You can restrict users from creating personal DocuSign accounts using an email address from a claimed domain. You can also grant administrative consent for connected applications on behalf of domain users.

> **Important:** A domain can only be claimed by one DocuSign organization. If one organization has claimed and verified a domain, then another organization cannot claim it. An organization can claim the same domain in both the demo and production environments.

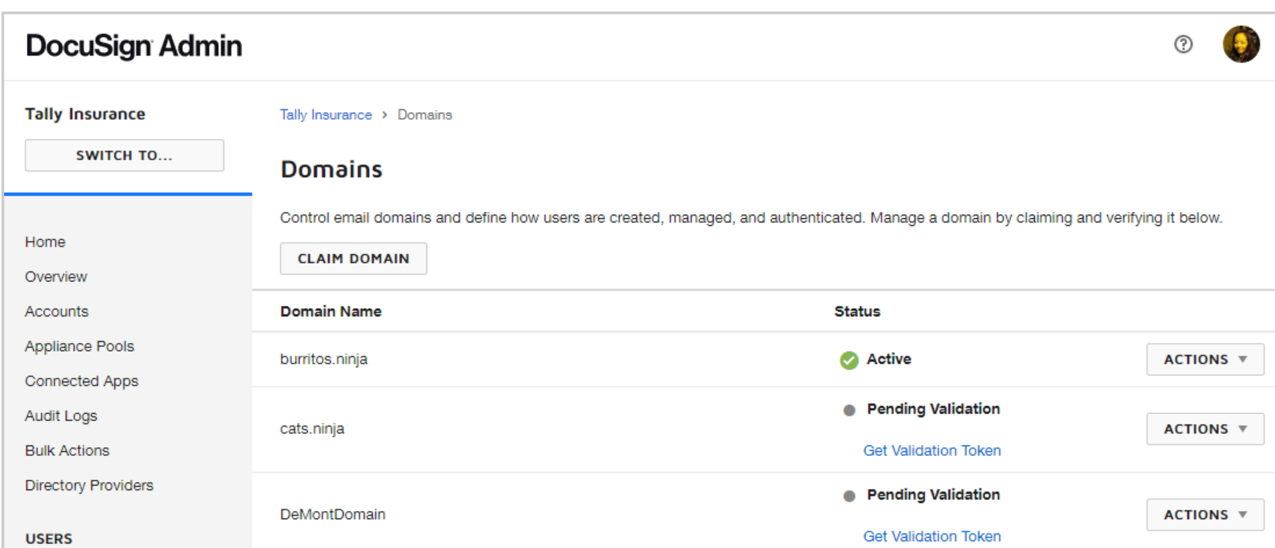
To start, you'll initiate a claim for your organization from the Domains page in DocuSign Admin. DocuSign then generates a special token that you add to the DNS (Domain Name System) for the domain. Once DocuSign verifies this token in the DNS, the domain is registered to the organization.

> **Note:** You can choose to add a TXT record or a CNAME record to the DNS of your domain. To ensure continuity of coverage, it is recommended to add both record types when claiming a domain.

Prove Ownership of a Domain

1. In DocuSign Admin, click **Domains**.

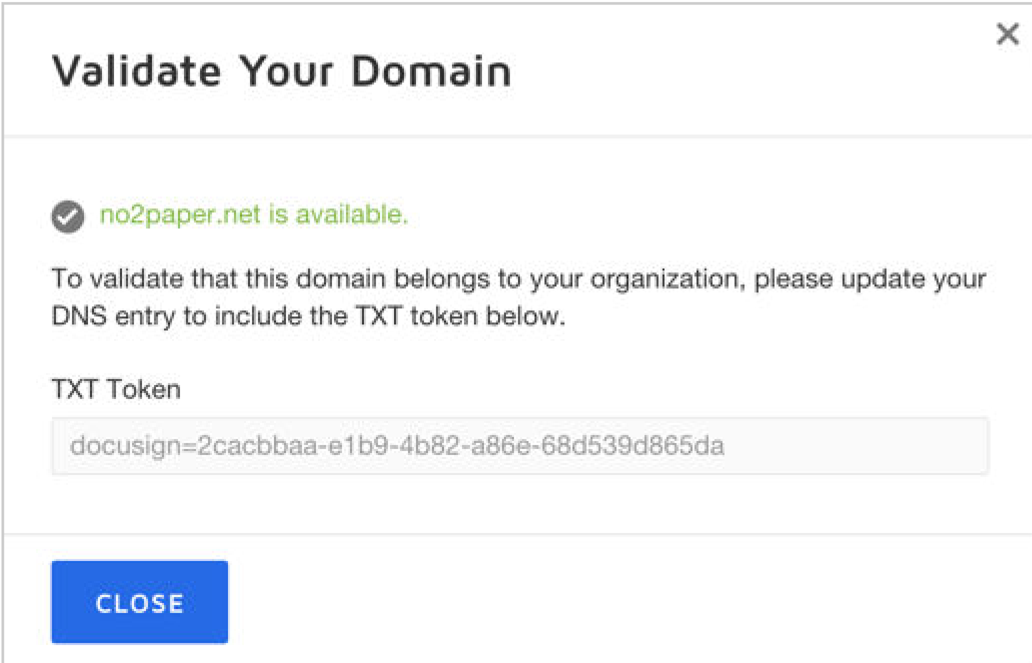
2. Click **CLAIM DOMAIN**.



3. Enter the Domain Name.

4. Click **CLAIM**.

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



5. Copy the generated TXT token so that it can be added to your domain's DNS entry.

6. Click **CLOSE**.

7. Outside of DocuSign Admin, update your domain's DNS entry to include the following:

To create a TXT record

a. Navigate to your domain's DNS record management page.

b. Add a new TXT record.

c. Name: @ or *

d. Text: TXT token from step 5 - Example: docusign=2cacbbaa-e1b9-4b82-a86e-68d539d865da

e. TTL: Default or 1 hour / 3600 seconds

To create a CNAME record

a. Navigate to your domain's DNS record management page.

b. Add a new CNAME record.

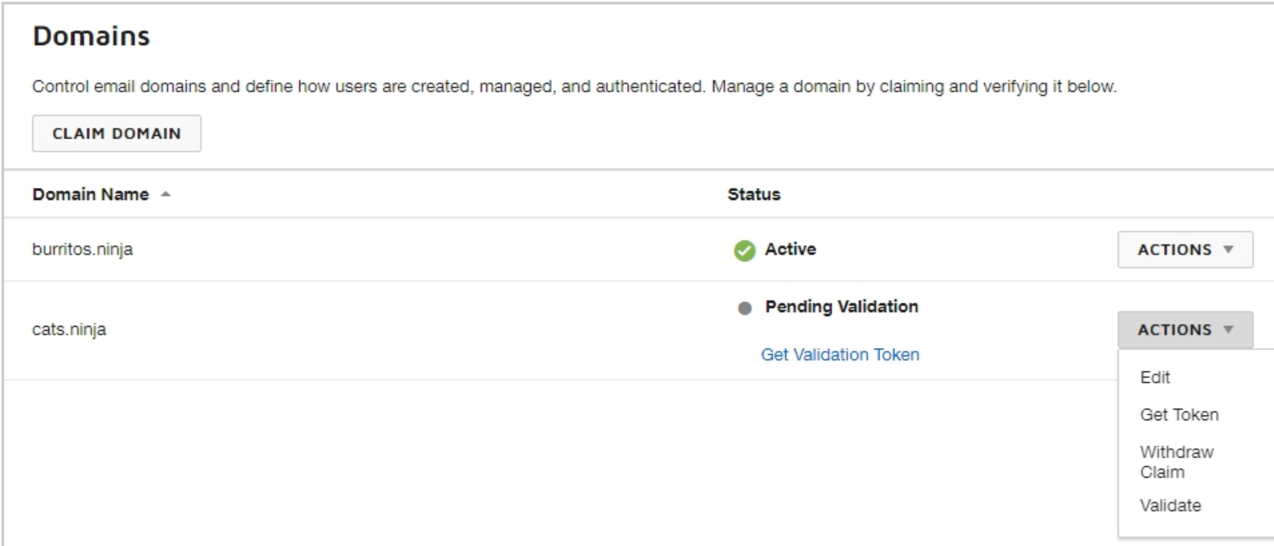
c. Name: 32-digit **GUID only** from the token in Step 5 - Example: 2cacbbaa-e1b9-4b82-a86e-68d539d865da

d. Domain Name: verifydomain.docusign.net.

> **Note:** The process of updating DNS entries 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. Coordinating ahead of time will ensure timely deployment of Single Sign-On.
>
> As a sanity check, you can confirm that your changes are active with the steps outlined in Additional Information for Claiming Domains.

8. Once the DNS changes are active, return to DocuSign Admin 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 tokens are part of the DNS record. If successful, the domain status changes to "Active."

Your domain ownership is proven.

> **Note:** DocuSign periodically reviews pending or active domain claims. It is possible that after updating your DNS, your domain claim can become active in DocuSign even if you have not clicked validate. If you've previously claimed a domain and removed the claim information from your DNS, these reviews would invalidate that claim.

Get a TXT Token for a Claimed Domain

1. In DocuSign Admin, click **Domains**.
2. In the list of domains, locate the domain for which you want to get the token.
3. Click **ACTIONS** on the same line as the domain name and select **Get Token**.
4. Copy the generated TXT token as needed.
5. 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 eSignature application. This operation should only be reserved for cases where you are certain there are no active users with an email address in the domain.

Important: There is no way to undo this change. Use caution when withdrawing an active domain claim.

1. In DocuSign Admin, click **Domains**.

2. In the list of domains, find the domain you want to relinquish.

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

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

Additional Information for Claiming Domains

Domain DNS entry

- **TXT or CNAME token must remain in the domain's DNS entry**. For as long as you want to reserve the domain for your DocuSign organization, the token must remain in place. DocuSign periodically checks the DNS to ensure claims are valid, and removal of a token would prevent your users from accessing DocuSign.
- **The process of updating DNS entries 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.
- **Optional - perform a sanity check to confirm the DNS change is active using one of the following methods**.
  - For Windows users, open the command prompt and enter these commands:

    ```
    nslookup -q=txt [myorganization.com]
    ```

    ```
    nslookup -q=CNAME [Guid].[myorganization.com]
    ```

    Where *[myorganization.com]* is the domain you are checking.
  - For Mac users, open the terminal and enter these commands:

    ```
    dig txt [myorganization.com]
    ```

    ```
    dig CNAME [Guid].[myorganization.com]
    ```

    Where *[myorganization.com]* is the domain you are checking.

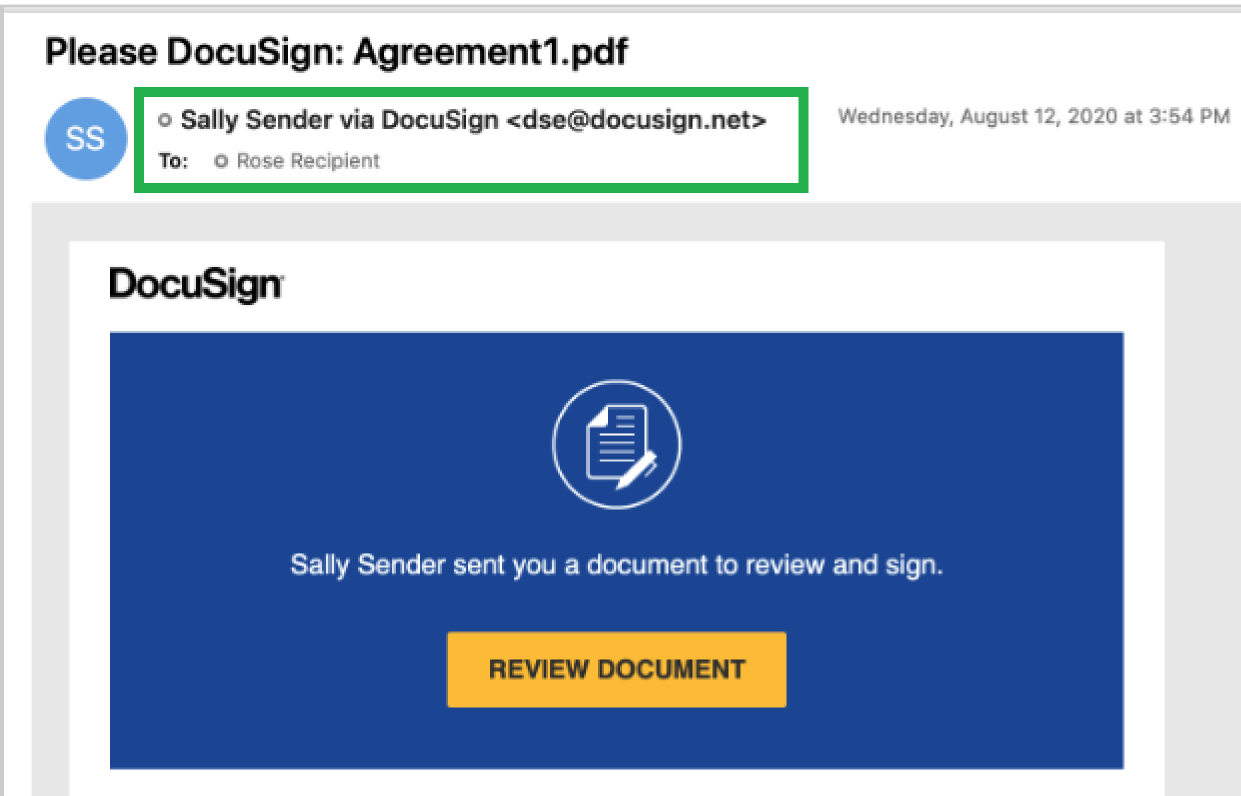
Customize DocuSign Notification Emails for Accounts with Custom Email Domains

By default, when a notification email is sent to a recipient, it is sent from the appropriate DocuSign server email address (e.g. dse@docusign.net, dse-demo@docusign.net, etc.). With Custom Email Domain (CED) all outbound emails can be updated to show a customized name and email address. This allows organizations to maintain trust by sending emails from their verified email domains.

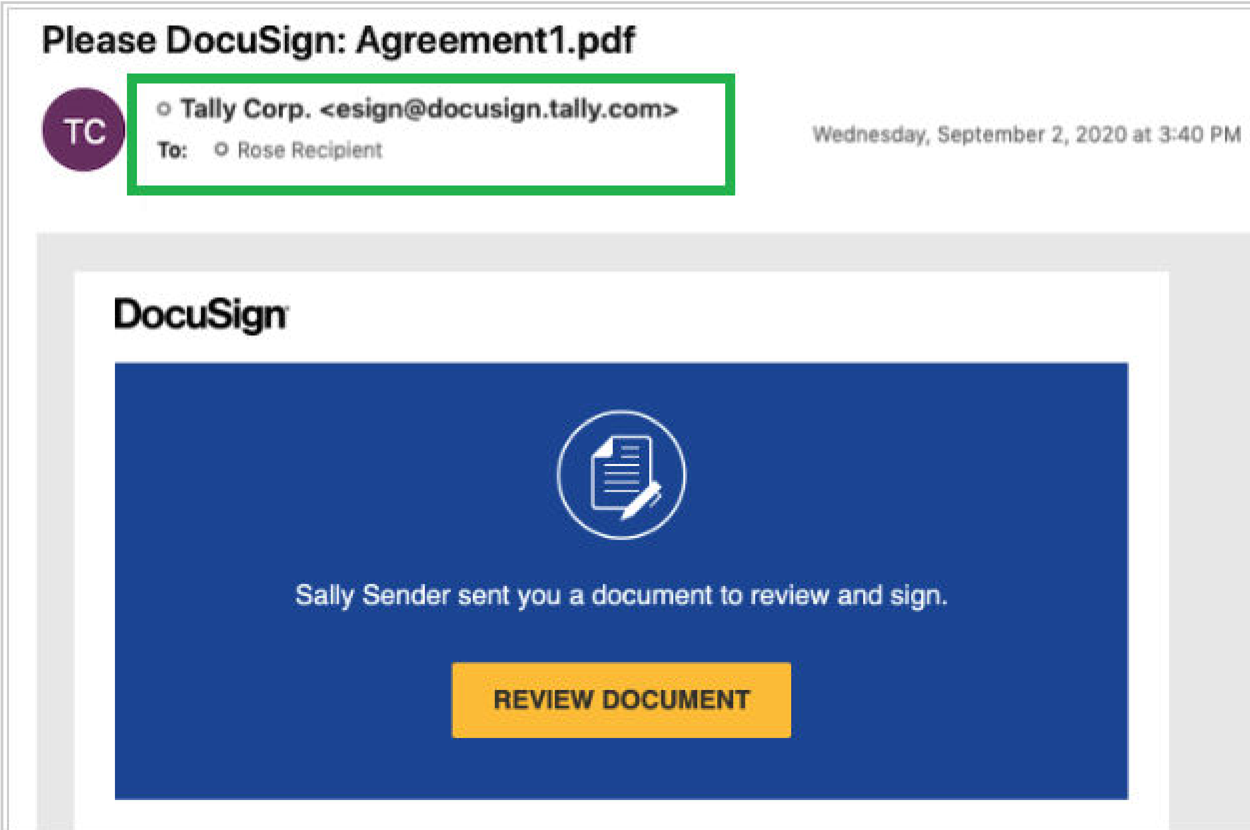
Note: A claimed and verified top-level domain (TLD) is required to create a subdomain. Subdomains already used for SSO cannot be used for custom email addresses.

Tally Communications sends thousands of envelopes to customers each day. Sometimes, customers unfamiliar with DocuSign may wonder why they are receiving email from DocuSign on behalf of Tally. To address this, an administrator creates a custom email domain and updates outbound email addresses for accounts within their organization. Now, customers will receive all DocuSign email notifications from a custom email address. For example, if Tally owns the domain 'tally.com', they can create a custom domain such as 'docusign.tally.com' and send all outbound DocuSign emails from that domain.

Default notification email



Custom notification email using CED



Add and Verify a Subdomain to Use as a Custom Email Domain

- Log in as a DocuSign Administrator
- Claim and verify a top-level domain - Domains
- Have access to edit DNS records in your organization's domain registrar. This is done through a 3rd party site and may require IT assistance from within your organization.

After claiming a domain, create a subdomain and update your DNS records to verify and configure for CED.

> **Note:** This process does not use an existing subdomain. A new subdomain is created through the verification process. Subdomains already used for SSO cannot be used for custom email addresses.

1. In DocuSign Admin, select **Overview**.
2. Scroll down to Custom Email Domain, and select **Manage**.
3. Select **Actions** > **Enable**.

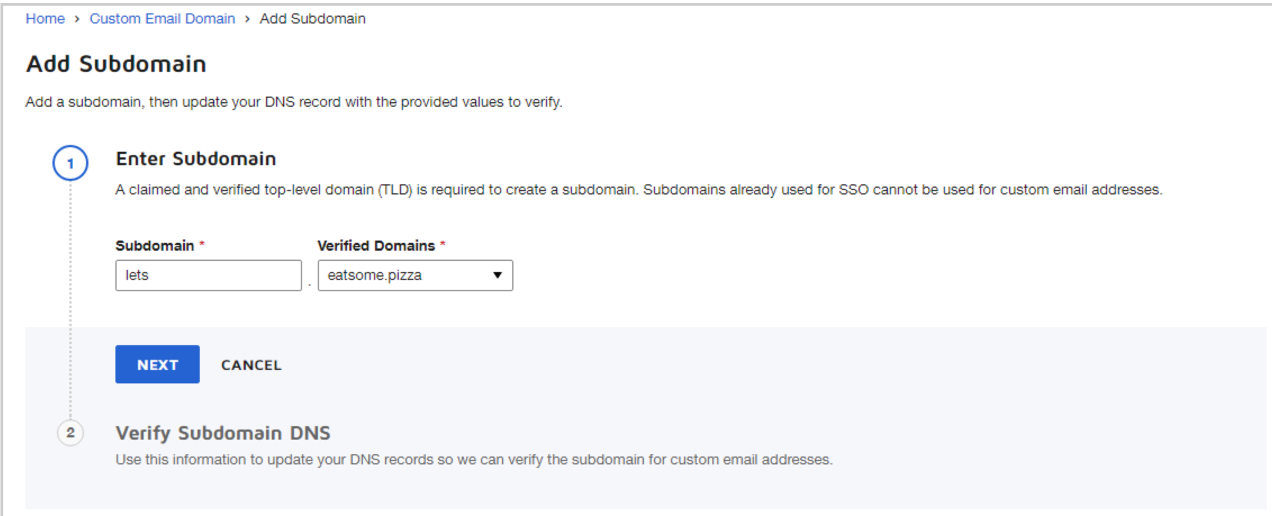
   The Custom Email Domain menu item and tile are added to DocuSign Admin.
4. In DocuSign Admin, select **Custom Email Domain**.

5. Select **ADD DOMAIN**.

6. Enter a name for the new subdomain.

> **Note:** The subdomain name appears in front of the verified top-level domain. For example, if the top-level domain is 'example.com' and the subdomain is 'docusign', your DocuSign custom email addresses will be [username]@docusign.example.com.

7. Select an available verified top-level domain, then select **NEXT**.



8. Log in to your domain registrar and navigate to the DNS records for the selected verified domain.

9. Using the DocuSign-provided values, create two CNAME/DKIM records, one TXT/SPF record, and one MX record.

> **Note:** Refer to your domain registrar for instructions on updating DNS records. This process is performed outside of DocuSign and may differ between registrars. If you do not have access to your domain registrar, you may need to work with your organization's IT team to complete these steps.

10. Select **VERIFY DNS NOW**.

> **Note:** It may take up to 24 hours for changes to your DNS to be published by your domain registrar. If you are unable to verify the domain shortly after updating the DNS records, select **SAVE DOMAIN AND VERIFY DNS LATER**. If the domain cannot be verified more than 24 hours after updating the DNS, review the records to ensure accuracy or contact your domain registrar for more information.

The subdomain is saved and verified.

Add a Custom Email Address and Link It to an Account

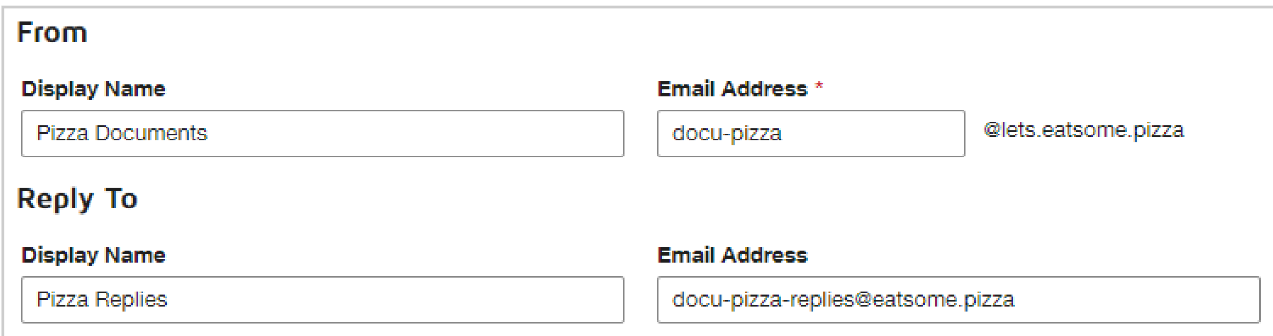
- Log in as a DocuSign Administrator
- Add and verify a subdomain - Add and Verify a Subdomain to Use as a Custom Email Domain

After adding and verifying a subdomain, you'll need to add a custom email address and link it to accounts.

1. In DocuSign Admin, select **Custom Email Domain**.

2. On the verified subdomain you'd like to use, select and select **Add email address**.

3. Enter the **Display Name** and the **Email Address** for the **From** and **Reply To** sections, then click **NEXT**.



> **Note:** The reply-to address will receive all replies from recipients and does not need to use the subdomain. For example, if all replies are directed to the IT team, use an existing email alias as the reply-to address. A no-reply address is also commonly used.

4. Select one or more accounts to link to this new email address, then select **NEXT**.

5. Review the details and select **SAVE EMAIL ADDRESS**. After saving, it can take up to 60 minutes for the changes to be applied.

   The custom email address is saved. Future notification emails will be delivered using the new address for all linked accounts.

Manage Details for an Existing Custom Email Address

Before your begin:

- Log in as a DocuSign Administrator
- Add and verify a subdomain - Add and Verify a Subdomain to Use as a Custom Email Domain
- Add a custom email address - Add a Custom Email Address and Link It to an Account

After adding a custom email address, you may want to edit related details.

1. In DocuSign Admin, select **Custom Email Domain**.

2. On the verified subdomain you'd like to use, select and select **Edit**
3. Select an email address to edit.
4. Update the Display Name and Email Address fields as needed.
5. Add or remove linked accounts.

   > **Note:** After adding or removing linked accounts, there may be a delay of up to one hour for changes to take effect.

6. Select **SAVE**.

   The custom email address is updated.

Enable, Disable, or Delete an Existing Subdomain or Custom Email Address

Before your begin:

- Log in as a DocuSign Administrator
- Add and verify a subdomain - Add and Verify a Subdomain to Use as a Custom Email Domain
- Add a custom email address - Add a Custom Email Address and Link It to an Account

By default, subdomains are automatically enabled when created and verified. Disabling a subdomain reverts all accounts using any associated custom email addresses to the default DocuSign notification email addresses.

1. In DocuSign Admin, select **Custom Email Domain**.
2. On the verified subdomain you'd like to use, select .
3. Select an option:
   - Enable/Disable: When disabled, any email addresses associated with the custom domain will be turned off and all notifications will be sent by the default DocuSign notification service.
   - Delete: Deleting a subdomain also deactivates and deletes all email addresses created using that domain.

Audit Logs

> **Note:** This guide is for DocuSign administrators who oversee multiple accounts. For administrators of individual accounts, see the DocuSign eSignature Admin guide .

Audit logs capture key events for changes to an organization made from within the organization. The Organization audit log provides an easy way for administrators to see changes to the accounts linked to the organization and user management actions (such as adding, removing, and editing users), and updates to DocuSign administrators.

Delegated Administrators and Audit Logs

If your organization assigns delegated permissions, these administrators have limited visibility into the organization audit logs.

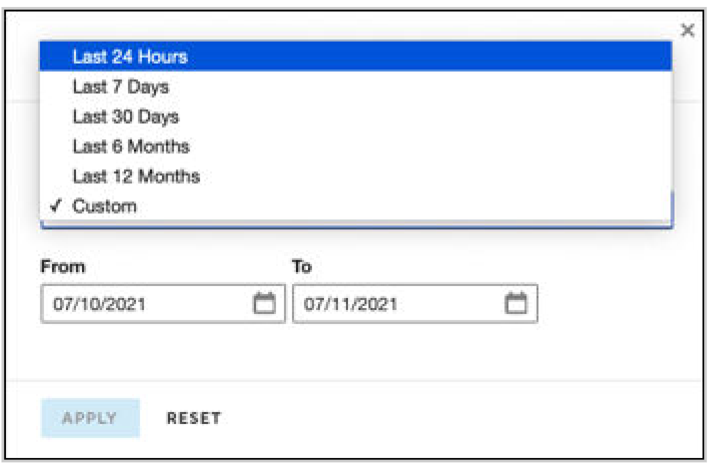
DocuSign Administrators who have full administration capabilities can see all audit log entries.

View Audit Logs

1. From the DocuSign Admin dashboard, select **Audit Logs**.

   The Audit Logs view lists the audit events for the last 24 hours. The DocuSign Administrator permission profile grants access to all audit events.

2. Change the date range to view older events.



3. Select **VIEW** to view the details of an event.

The Event Details window opens.

Appliance Pools

DocuSign Admin enables organizations to centrally manage external appliances.

CONTENTS

About the DocuSign Security Appliance

The DocuSign Security Appliance is a software package for a self-managing appliance. The appliance is designed to address the most sensitive scenarios requiring the highest level of security.

The software runs remotely from the DocuSign service that manages the storage and release of cryptographic keys. The DocuSign Security Appliance offloads the key storage and release policies from the DocuSign cloud to a customer's private network.

DocuSign Professional Services installs the DocuSign Security Appliance on your network through a services engagement. The DocuSign administrator then manages the security appliances in DocuSign Admin by following the steps in this guide. DocuSign Professional Services maintains separate documentation for installing the Security Appliance software.

Prerequisites for managing the DocuSign Security Appliance

- The DocuSign Security Appliance must be enabled for your DocuSign organization. If you do not see the security appliance management features in DocuSign Admin, contact DocuSign Support.
- The DocuSign Security Appliance must be installed and configured on your network.
- You must be a DocuSign organization administrator to manage the DocuSign Security Appliance.

Related information

Appliance Pools

About Security Appliance Pools

After the DocuSign Security Appliance is installed, you create one or more *security appliance pools* in DocuSign Admin. You then add security appliances to the pools. A security appliance *pool* enables you to group security appliances, and then share access to those appliances with multiple organization accounts. All of the appliances in a pool must have the same checksums, hardware security module (HSM), and key count.

> **Note:** You cannot delete a pool to which accounts have been assigned. After an account is assigned and envelopes are sent, the pool must be able to view those sent envelopes.

Related information

Appliance Pools

Create a Security Appliance Pool

A security appliance pool enables your organization to group security appliances. Multiple organization accounts can then share access to those appliances. Read more about security appliance pools before you start.

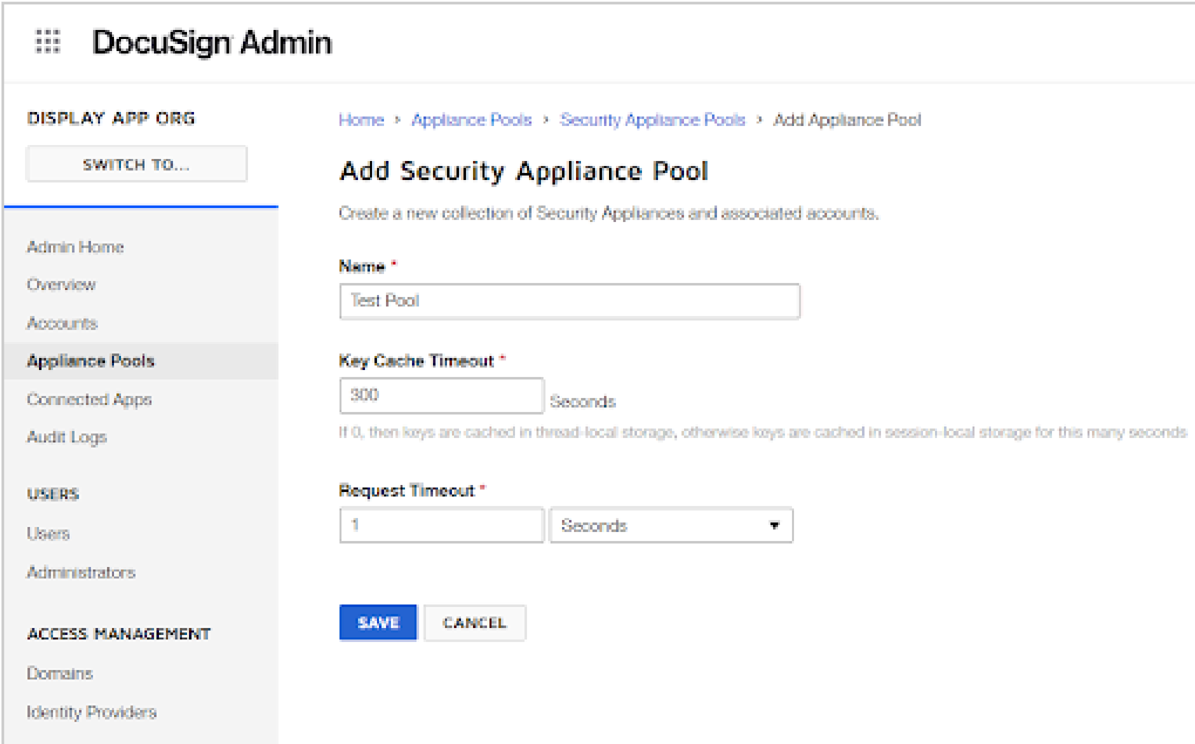
1. Log in to DocuSign Admin and select the **Appliance Pools** tile.

2. Select **Security Appliances**.

3. Select **ADD APPLIANCE POOL**.

   The **Add Security Appliance Pool** window opens.

4. Enter the settings for the pool and select **SAVE**.



The new appliance pool saves.

Related information

About Security Appliance Pools

Appliance Pools

Add Appliances to a Security Appliance Pool

This topic shows you how to add security appliances to a security appliance pool. All appliances in a pool must have the same configuration, including matching checksums, hardware security module (HSM), and key count.

1. Log in to DocuSign Admin and select the **Appliance Pools** tile.

2. Select **Security Appliances**.

   A list of security appliance pools opens.

3. Select **ACTIONS** > **Manage Appliances** next to the pool to which you want to add an appliance.

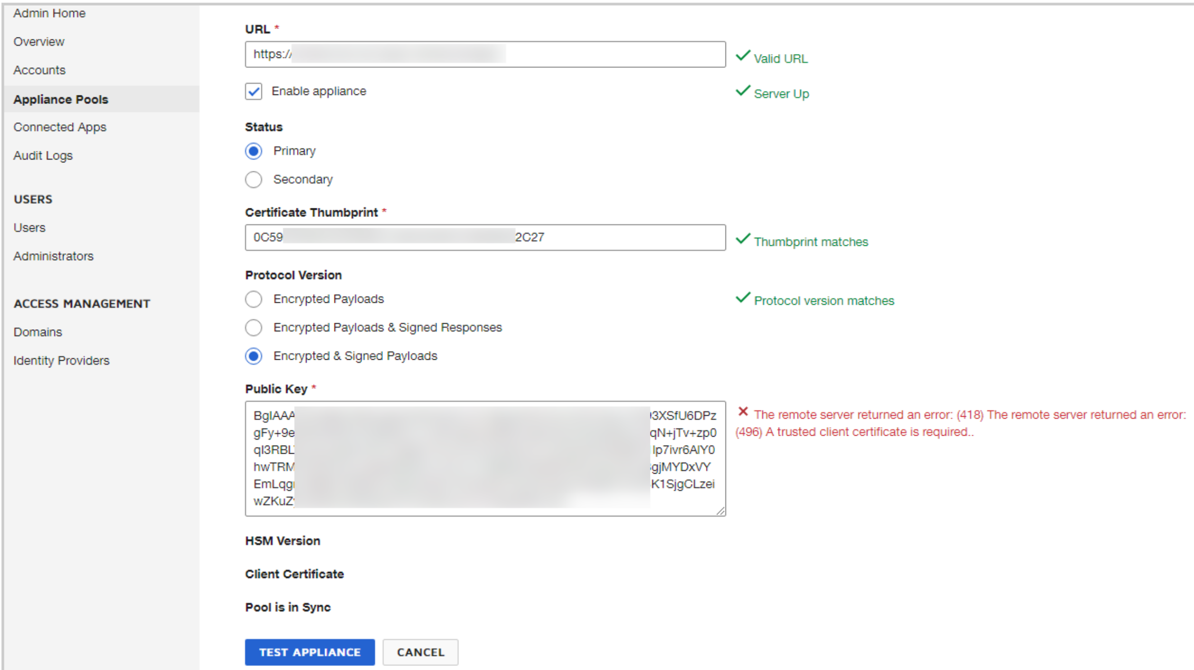
   The **Manage** page for the appliance pool opens.

4. Select **ADD APPLIANCE**.

5. Enter the settings for the new appliance.

6. Select **TEST APPLIANCE**.

   The system tests the configuration. Green checkmarks display next to the appliance details you entered if the test is successful. This result means that you configured the appliance correctly. If you receive any error messages, contact DocuSign Support for help.



7. Select **SAVE**.

The new security appliance saves. All accounts assigned to the pool can access the new appliance.

Related information

Create a Security Appliance Pool

About Security Appliance Pools

Configure Your Hardware Security Module and Derived Keys

This topic shows you how to configure your security appliance pool to use derived keys. You must use a hardware security module (HSM) with your security appliance.

1. Create a security appliance pool.

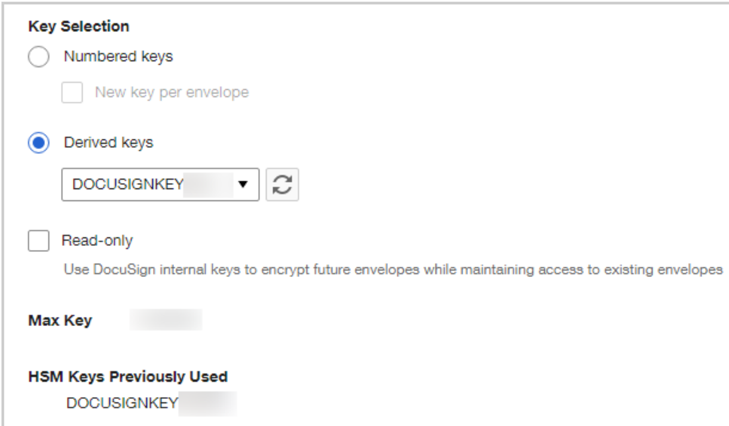
2. Add an appliance that has an HSM configured to the pool.

   > **Note:** If the pool isn't enabled for derived keys, you will see the message "No HSM configured" when you test the appliance. You receive this message even if the appliance does have an HSM configured.

3. Select **ACTIONS** > **Edit Pool Settings** next to the appliance pool.

4. Select **Use Derived Keys** under Key Selection.

5. Select a key from the drop-down list.



6. Select **SAVE**.

The changes save. The HSM and derived keys are configured for the security appliance pool.
Related information

Create a Security Appliance Pool

About Security Appliance Pools

About the DocuSign Security Appliance

Assign Accounts to a Security Appliance Pool

A security appliance pool enables you to group appliances. Then, you assign linked organization accounts to the appliance pool. After you add an account to an appliance pool, all the security appliances in the pool secure the account envelopes.

You can only assign an account to one of each type of pool. For example, an account can be assigned to one security appliance pool and one display appliance pool. You can't remove accounts from a pool. Make sure you are making the proper assignments when adding accounts to a pool. If changes are required, you must engage DocuSign Professional Services.

When you link new accounts to your organization, you must also add them to a security appliance pool. This step applies your external key management policies to the envelopes that the new accounts generate.

1. Log in to DocuSign Admin and select the **Appliance Pools** tile.

2. Select **Security Appliances**.

A list of security appliance pools opens.

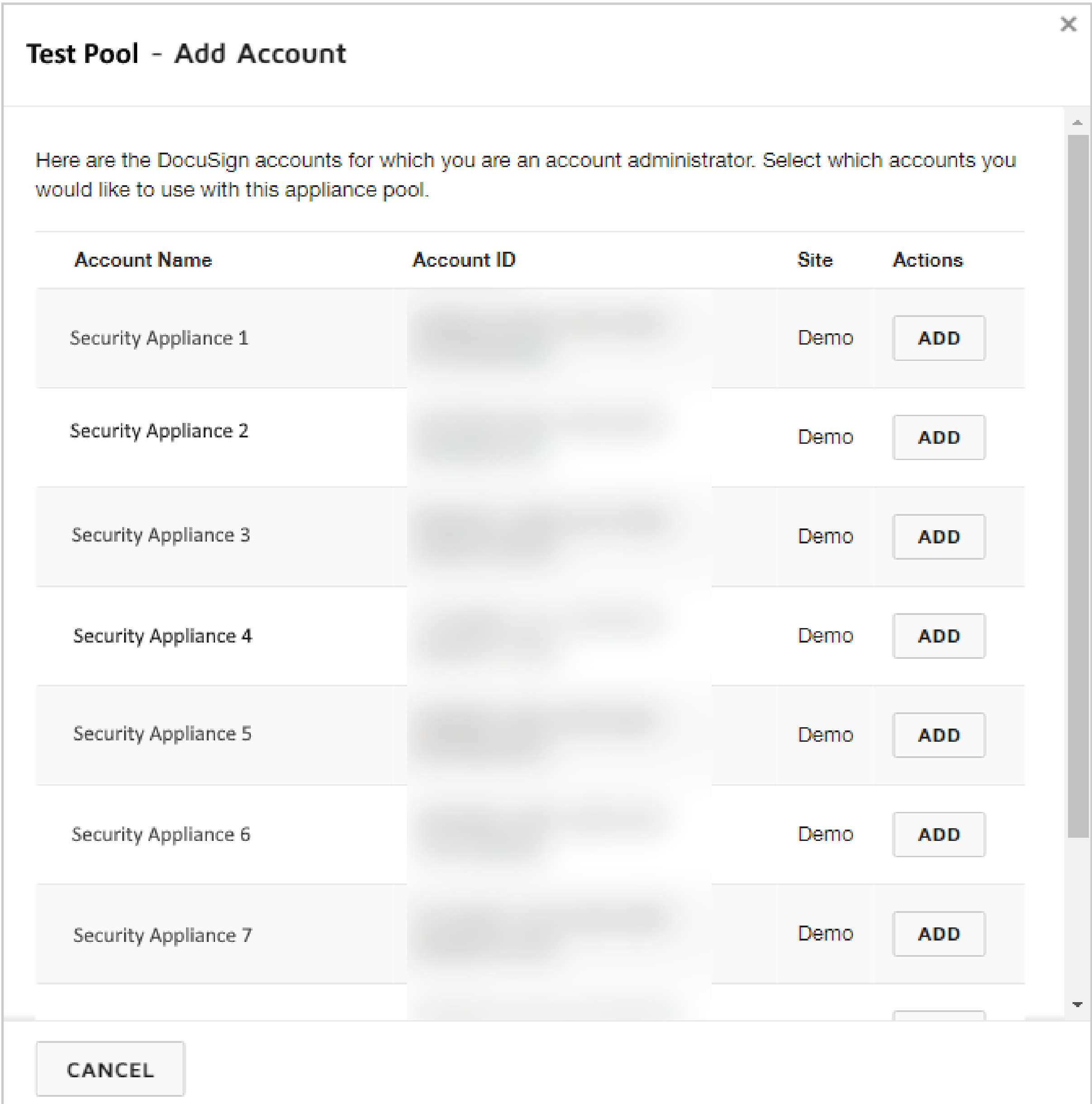
3. Select **ACTIONS** > **Manage Accounts** next to the pool to which you want to add accounts.

The **Manage** page opens and lists any accounts that are already assigned to the pool.

4. Select **ADD ACCOUNT**.

The **Add Account** window opens. It lists the accounts for which you are an account administrator and that are linked to the organization.

5. Select **ADD** next to the accounts to which you want to grant access to the security pool.



A confirmation message displays after you add each account. The accounts you selected are added to the security pool. The accounts have access to all of the appliances in the pool.

6. Select **CANCEL** or the close icon at the top right to exit the window.

Related information

Appliance Pools

Edit a Security Appliance Pool

This topic shows you how to edit a security appliance pool. You might want to edit a pool to change the durations before timeouts or other settings.

1. Log in to DocuSign Admin and select the **Appliance Pools** tile.

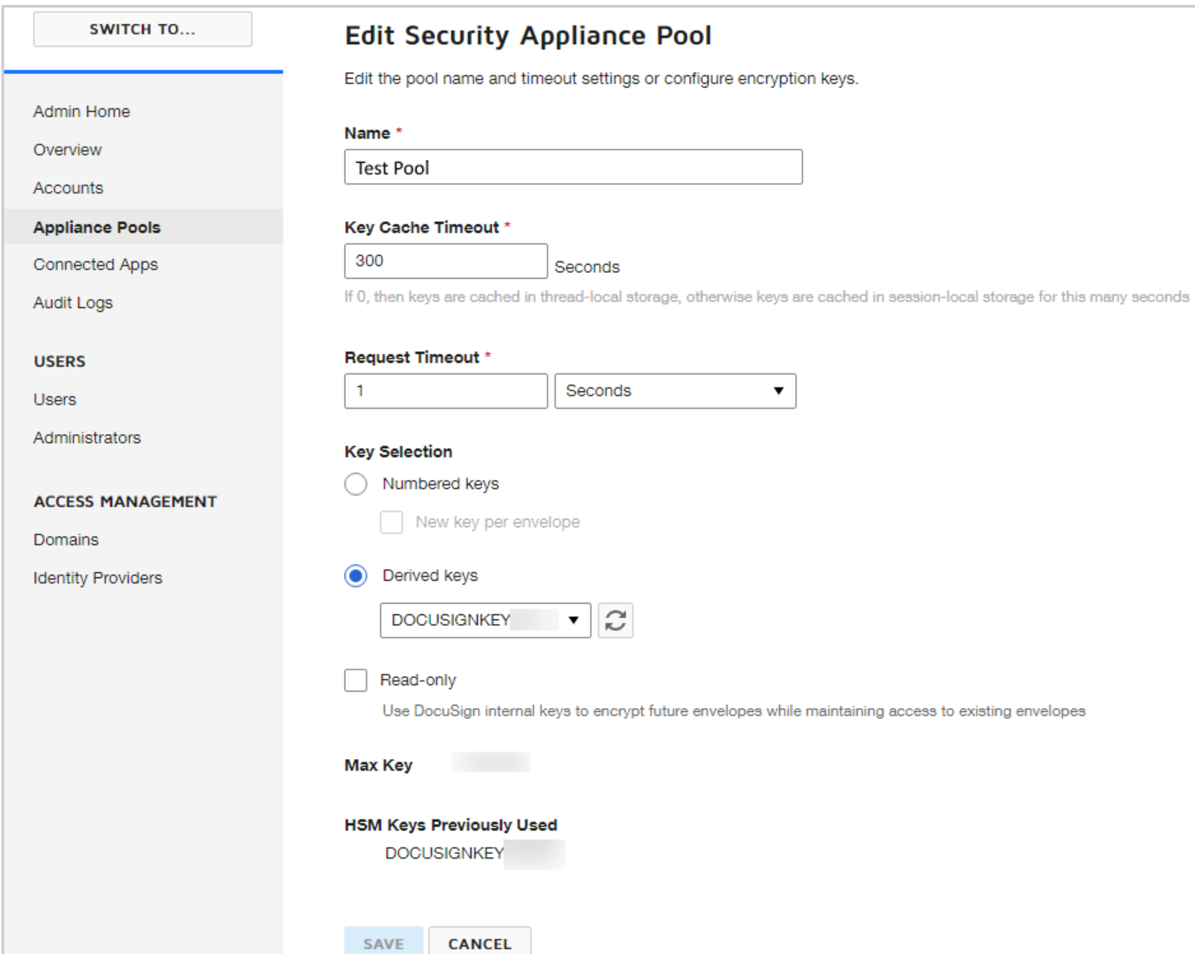
2. Select **Security Appliances**.

   A list of security appliance pools opens.

3. Select **ACTIONS** > **Edit Pool Settings** next to the pool you want to edit.

   The **Appliance Pool Settings** window opens.

4. Update the settings.



5. Select **SAVE**.

The changes to the appliance pool save.

Related information

About Security Appliance Pools

Run a Health Check on All Security Appliances in a Pool

Any time you add or edit a security appliance, you must successfully test your changes to save them. You can also run a health check on all security appliances in a pool simultaneously. The health check tests and confirms the connection details for each appliance in the pool. The pass or fail results display on the security appliances list under the Health Check column.

1. Log in to DocuSign Admin and select the **Appliance Pools** tile.

2. Select **Security Appliances**.

   A list of security appliance pools opens.

3. Select **ACTIONS** > **Manage Appliances** next to the pool for which you want to run a health check.

   The **Manage Security Pool Appliances** page opens.

4. Select **MORE ACTIONS** > **Test All Appliances**.

The health check evaluates all of the security appliances in the pool. The results display in the Health Check column.

Related information

Appliance Pools

Update the DocuSign Security Appliance Software on Your Appliances

This topic shows you how to update the DocuSign Security Appliance software on the appliances in a pool. Follow the procedure in this topic to minimize impact on users. Update the appliances in a pool one at a time. This approach ensures that there is always a working appliance to handle key requests.

1. Contact DocuSign Support to request the URL for the latest Security Appliance MSI installer file. Download the file.

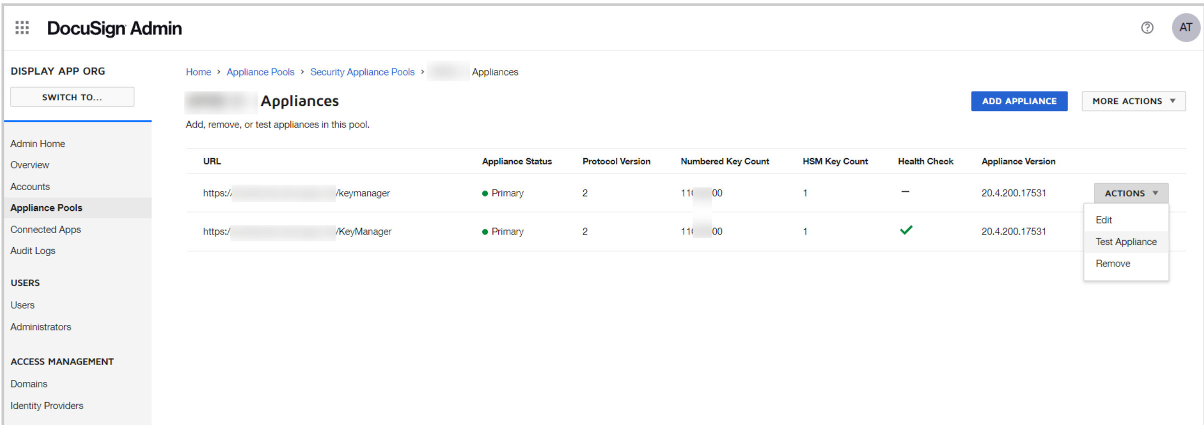
2. Log in to DocuSign Admin and select the **Appliance Pools** tile.

3. Select **Security Appliances**.

4. Select **Actions** > **Manage Appliances** next to the pool that contains the appliance.

5. Select **Actions** > **Test Appliance** next to the appliance in the list.

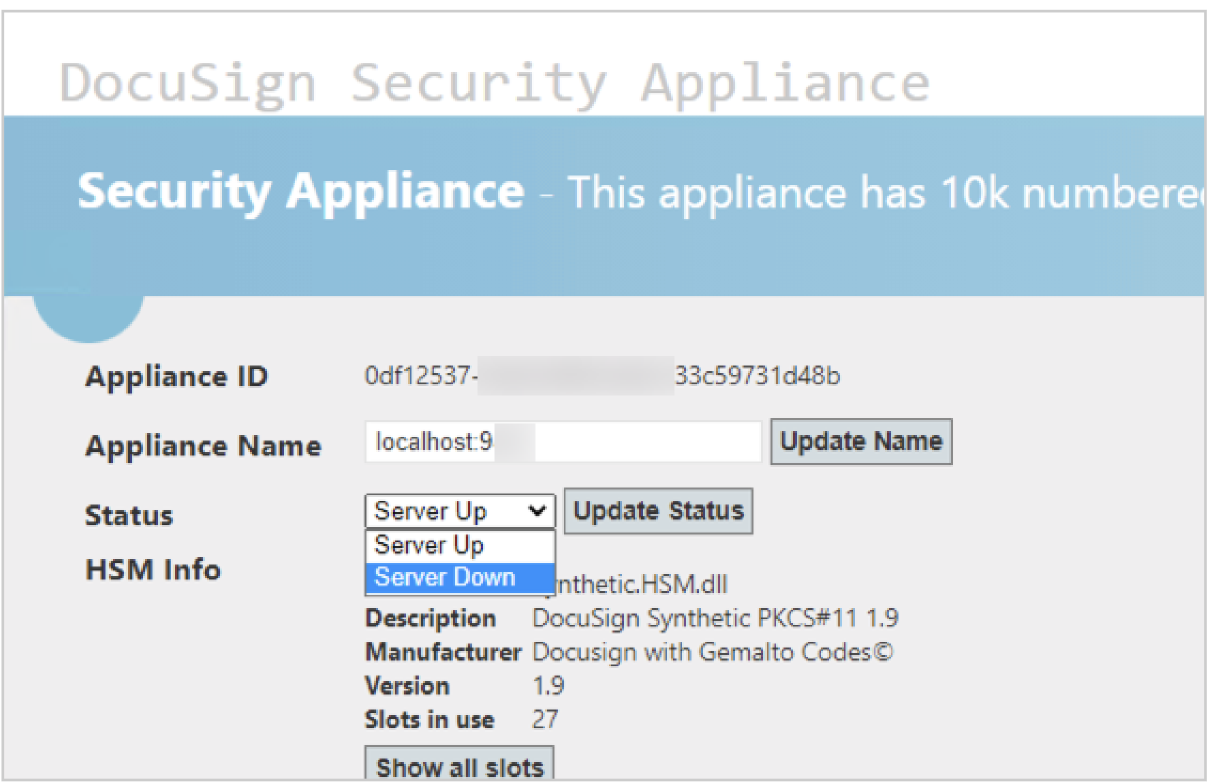
   A green checkmark should display next to the appliance in the Health Check column. This icon verifies that the security appliance is currently working. If a red icon displays the test failed. Contact DocuSign Support for assistance.



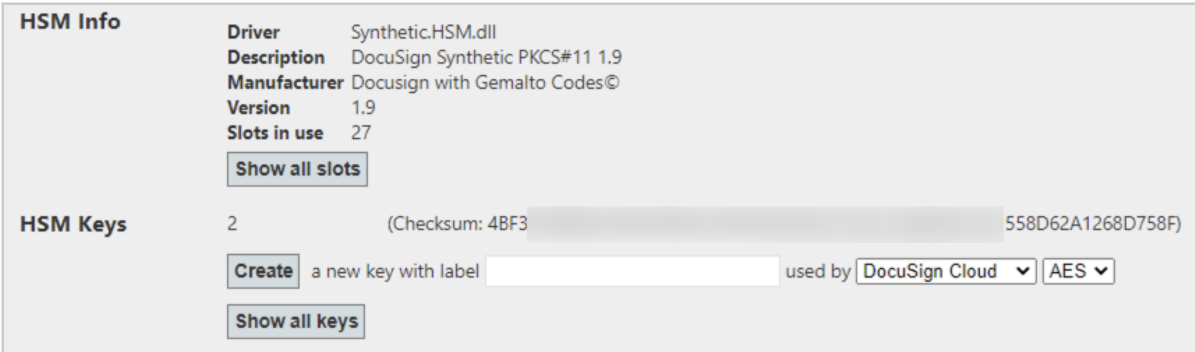
6. Log in to the Microsoft Windows server where the appliance is installed. Then, open a new browser window and navigate to https://localhost/admin.

   The local admin page for the appliance opens.

7. Set the **Status** of the appliance to **Server Down**, then select **Update Status**.



8. (Optional) If you are using a hardware security module (HSM) with the appliance, note the number of **HSM Keys** on the local appliance admin page.



9. Run the Security Appliance MSI file you downloaded in step 1. To run the file, double-click on it or use the command line.

10. Verify that there are no errors on the local appliance admin page. Errors display in red at the top of the page.

11. (Optional) If you are using an HSM, verify that the number of **HSM Keys** matches what it was before the upgrade.

12. Set the **Status** of the appliance to **Server Up** and select **Update Status**.

13. Verify that the appliance is working using DocuSign Admin the same way that you did in step 2.

The appliance updates the software and activates.

Security Appliance Settings

The DocuSign Security Appliance is a software package for a self-managing appliance. The appliance is designed to address the most sensitive scenarios requiring the highest level of security. This topic defines the settings an organization administrator uses to configure a security appliance.

Option	Description
URL	The URL for the appliance. Required.
Enable appliance	When selected, the appliance is enabled.
Status	The status of the appliance. • **Primary**: The appliance is a primary appliance. You can have multiple primary appliances. • **Secondary**: A standby appliance that is only tried if all of the primary appliances fail. Consider using this option for a hot-standby appliance that should take traffic only in an emergency.
Certificate Thumbprint	The certificate thumbprint is available in the Security Appliance Admin Web UI. Copy the certificate information and paste it into this field. Required.

Option	Description
Protocol Version	This value must match the Security Appliance version. • **Encrypted Payloads**: Key request and response payloads are encrypted. Protocol Version = 0. • **Encrypted Payloads & Signed Responses**: Key request payloads are encrypted and key response payloads are both encrypted and signed. Protocol Version = 1. • **Encrypted & Signed Payloads**: The key request and response are both encrypted and signed. Protocol Version = 2. To determine the protocol version, look in this file: `%KM_DIR%\Service\bin \DocuSign.KeyManager.Service.Shell.exe.config` `KM_DIR` in the file path is the location where the Security Appliance installed. The default location is `C:\Program Files (x86)\DocuSign \KeyManager`. Look for the Protocol Version value.
Public Key	To obtain the public key, log in to the Security Appliance Admin Web UI. Copy the key and paste it into the field provided. Required.
HSM Version	When you select **TEST APPLIANCE**, this field shows the version and description of the hardware security module (HSM) that is configured for the appliance, if any. If no HSM is configured, this field displays the message “HSM Not Configured”.
Client Certificate	The DocuSign Security Appliance uses mutual TLS to authenticate connections from the DocuSign Cloud. The DocuSign Cloud passes a client certificate that the appliance validates. If the appliance is configured to to ignore this client certificate check, this field displays the message “Warning: Client Certificate not required”.
Pool is in Sync	All of the appliances in a security appliance pool must have the same keys. If the appliance does not have the same keys as the other appliances already in the pool, this field displays an error message when you select **TEST APPLIANCE**.

Security Appliance Pool Settings

The DocuSign Security Appliance is a software package for a self-managing appliance. The appliance addresses the most sensitive scenarios requiring the highest level of security. This topic defines the settings an organization administrator uses to configure a security appliance pool, or group. All of the accounts you add to this pool can access the appliances in the pool.

Option	Description
Name	A name for the security appliance pool. Required.
Key Cache Timeout	The number of seconds before the key cache expires. If 0, use a thread cache (where the key is cached for each API call). If non-zero, use a global memory cache (where the key is cached for an entire signing session if the value is high enough). The recommended value is 300 seconds. Required.
Request Timeout	The number of seconds to wait for a response before retrying the key request. We recommend that you set this duration to two to three times your average key request duration. The recommended value is 1 second. Required.
Key Selection	The type of cryptographic keys to use: • **Numbered Keys**: The security appliance creates a fixed set of keys in advance. It assigns each key a number, starting at 1. For each new envelope, the appliance chooses a key from this set of keys. The appliance may select a key either sequentially or randomly. If **New key per envelope** is also selected, each envelope gets a new key sequentially starting at 1 until the **Max Key** is reached. After the **Max Key** is reached, new envelope creation fails. If **New key per envelope** is not also selected, each new envelope is assigned a random key between 1 and the **Max Key**. • **Derived Keys**: Keys are derived, or calculated, from a seed value using a cryptographic algorithm and public and secret data.
Read-only	Docusign internal keys encrypt future envelopes while maintaining access to existing envelopes.
Max Key	The count of numbered keys that exist across a pool. For example, if appliance A has 10k keys and appliance B has 20k keys, the max key that can be requested from every appliance in the pool is 10k.
HSM Keys Previously Used	A list of all hardware security module (HSM) keys currently or previously used for the pool.