iTimekeep

iTimekeep SSO Management and Configuration

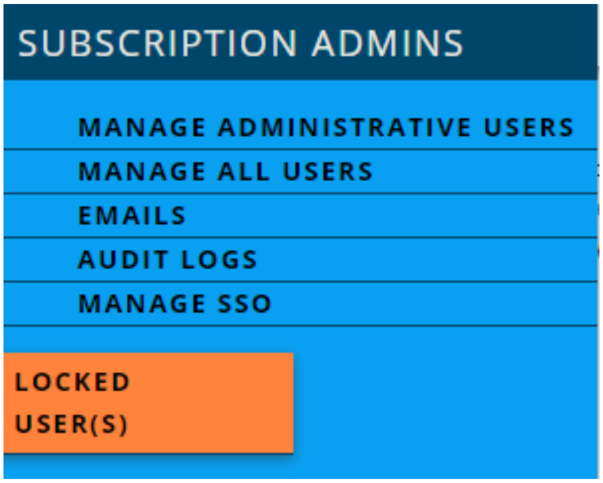
iTimekeep offers several options for users to login via their firms' Single Sign On system, eliminating the need for users to remember a password for iTimekeep. This document details the steps for adding and configuring SSO for iTimekeep.

iTimekeep SSO Overview

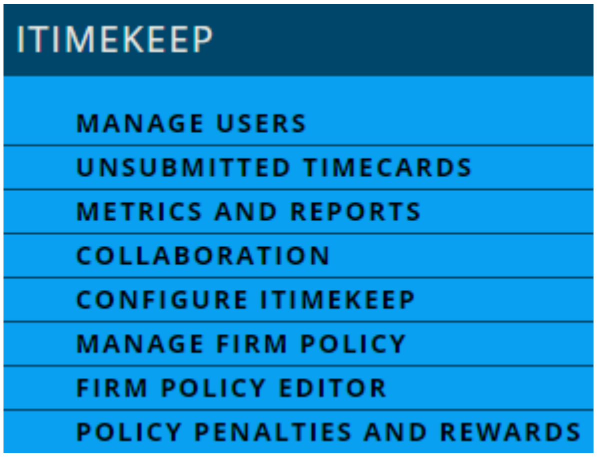
- iTimekeep SSO is domain based. By default, enabling iTimekeep SSO enables it for all domain users who have been defined for the entire iTimekeep subscription.
- iTimekeep SSO supports enabling SSO for a limited number of users during the iTimekeep SSO testing phase.
- iTimekeep SSO supports multiple domains (for example, users for an acquired firm or international users on a different domain). Each domain can be handled by different SSO providers.
- iTimekeep SSO supports multiple SSO providers (for example, while migrating to a new SSO provider).
- iTimekeep SSO supports disabling an SSO provider (for example, in case an SSO provider has an outage). If all the iTimekeep SSO providers are disabled, users will be able to login with a password.

Enabling SSO Management Options For Subscription Admins

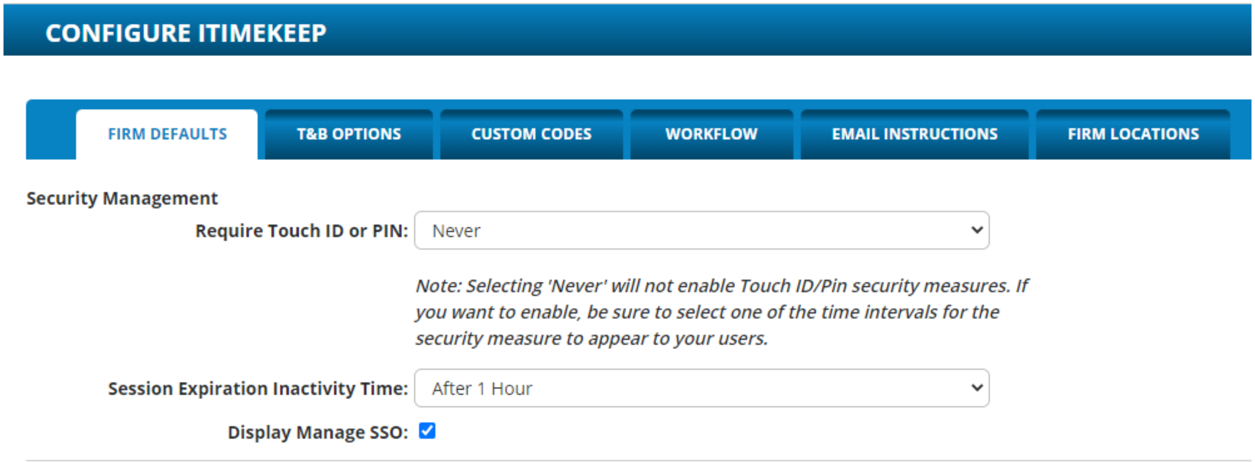
Subscription administrators are able to configure and manage iTimekeep SSO via a self-service page on the iTimekeep Portal. The page is available to all subscription administrators; however, it is only visible when SSO has been enabled for a subscription. To begin iTimekeep SSO setup, first check to see if the Manage SSO page appears as a menu option for subscription administrators:



If the page appears as a menu option skip the instructions for the rest of this section. Otherwise, navigate to the Configure iTimekeep page in the Portal.



Locate the Display Manage SSO checkbox in the Security Management section of the Firm Defaults tab.



Security Management

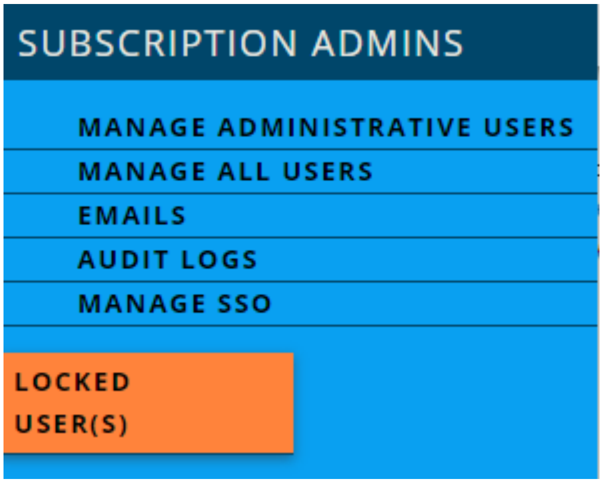
Require Touch ID or PIN: Never

Note: Selecting 'Never' will not enable Touch ID/Pin security measures. If you want to enable, be sure to select one of the time intervals for the security measure to appear to your users.

Session Expiration Inactivity Time: After 1 Hour

Display Manage SSO: ☑

Make sure the Display Manage SSO option is checked, then click the Save button at the bottom of the page. The Manage SSO page should appear as an option in the Subscription Admins section of the menu in a few seconds.



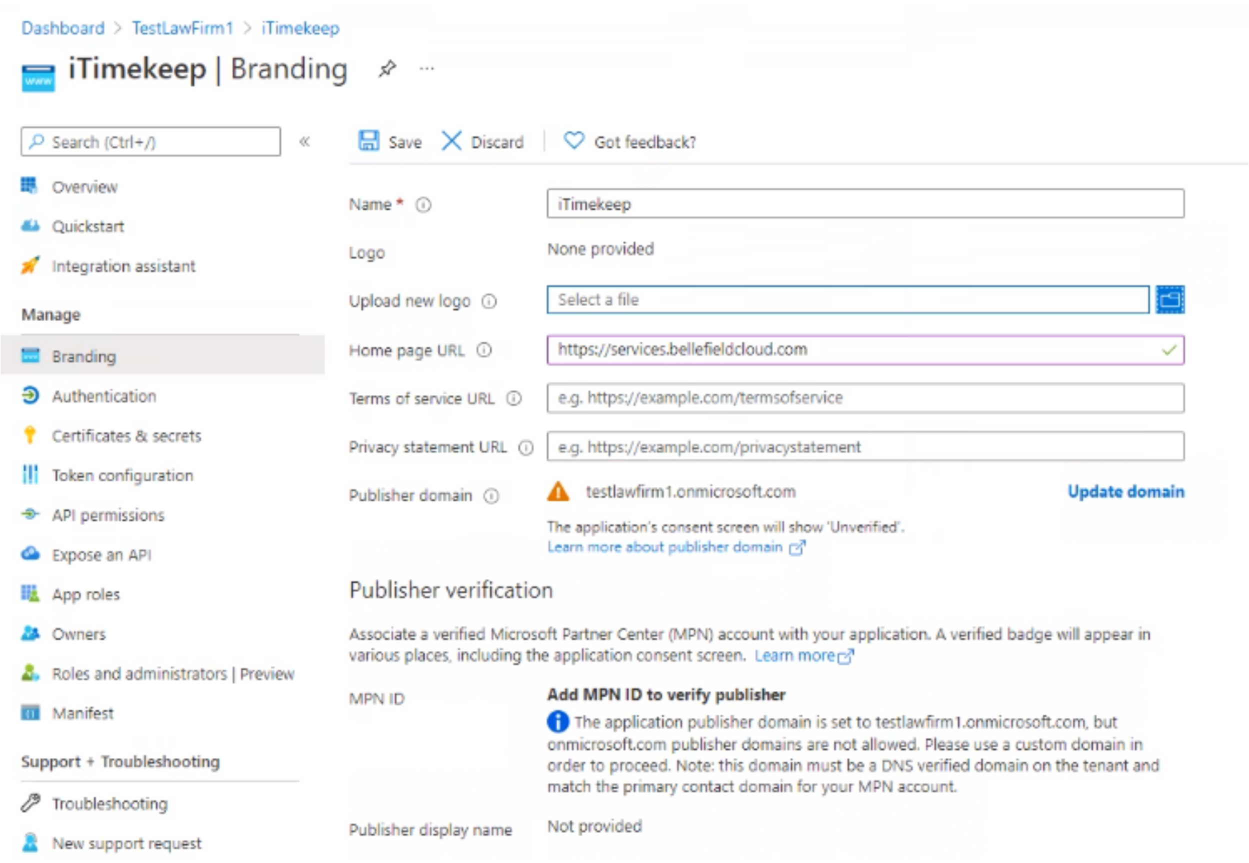
Configuring SSO Via Azure Active Directory

iTimekeep was developed using the Microsoft Authentication Library (MSAL), which is designed to work with the Microsoft identity platform endpoint, Azure Active Directory (Azure AD).

iTimekeep SSO currently requires that the Azure AD username (UPN) and the users' email addresses must match. iTimekeep accounts are defined with the email address as the iTimekeep username.

The iTimekeep application must be registered within Azure AD using the App Registration in the Azure Portal. You must add the Home page URL to the App Branding page with the base URL that you use for logging in to iTimekeep:

- US: https://services.bellefieldcloud.com
- Canada: https://itimekeep.aderant.ca
- Europe: https://itimekeep.aderant.eu
- UK: https://itimekeep.aderant.co.uk
- APA: https://itimekeep.aderant.com.au



Name * : iTimekeep

Logo: None provided

Upload new logo: Select a file

Home page URL: https://services.bellefieldcloud.com ✓

Terms of service URL: e.g. https://example.com/termsofservice

Privacy statement URL: e.g. https://example.com/privacystatement

Publisher domain: testlawfirm1.onmicrosoft.com Update domain

The application's consent screen will show 'Unverified'.
Learn more about publisher domain

Publisher verification

Associate a verified Microsoft Partner Center (MPN) account with your application. A verified badge will appear in various places, including the application consent screen. Learn more

MPN ID: **Add MPN ID to verify publisher**

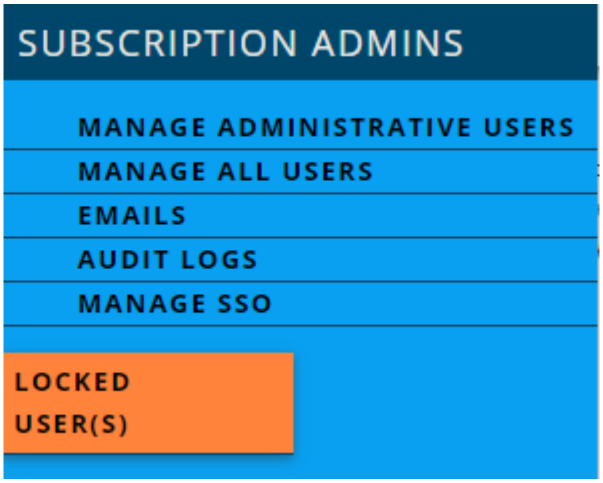
The application publisher domain is set to testlawfirm1.onmicrosoft.com, but onmicrosoft.com publisher domains are not allowed. Please use a custom domain in order to proceed. Note: this domain must be a DNS verified domain on the tenant and match the primary contact domain for your MPN account.

Publisher display name: Not provided

As an optional step based on the firm's security requirements, the newly-registered iTimekeep application may be assigned to users or groups in Azure AD.

Once the iTimekeep application has been created in Azure AD, note your Azure AD Tenant ID, which will be needed in the following steps for configuring and enabling SSO in the iTimekeep Portal.

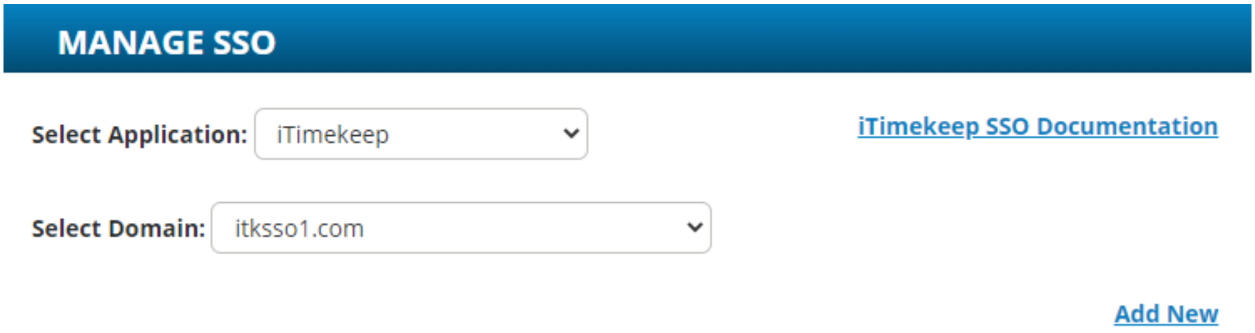
Login to the iTimekeep Portal and navigate to the Manage SSO page.



Select iTimekeep from the Select Application dropdown.

Select the appropriate domain name from the dropdown, which has been populated based on the email addresses for users that have been added to your iTimekeep subscription.

Click the Add New link on the right side of the page.



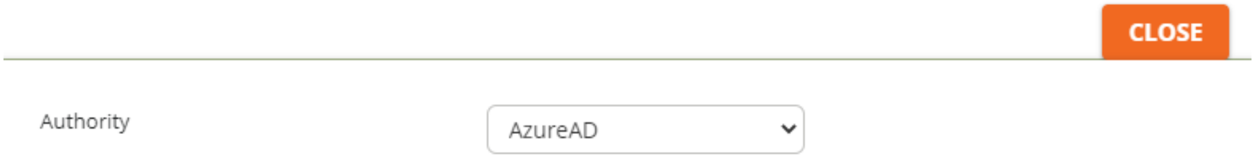
Select Application: iTimekeep

Select Domain: itksso1.com

Select AzureAD from the Authority dropdown on the popup.

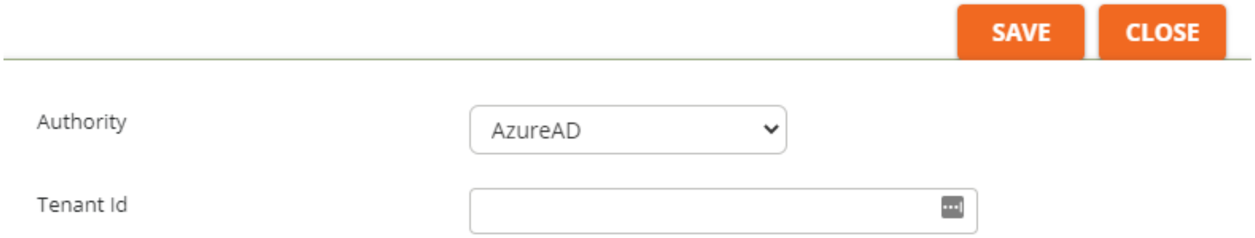
The Select Domain dropdown will be prepopulated based on the domain names associated with the iTimekeep users' email addresses. Select the appropriate value from the dropdown.

The Manage SSO page will now display a popup for entering configuration values obtained from the Azure Portal.



Authority: AzureAD

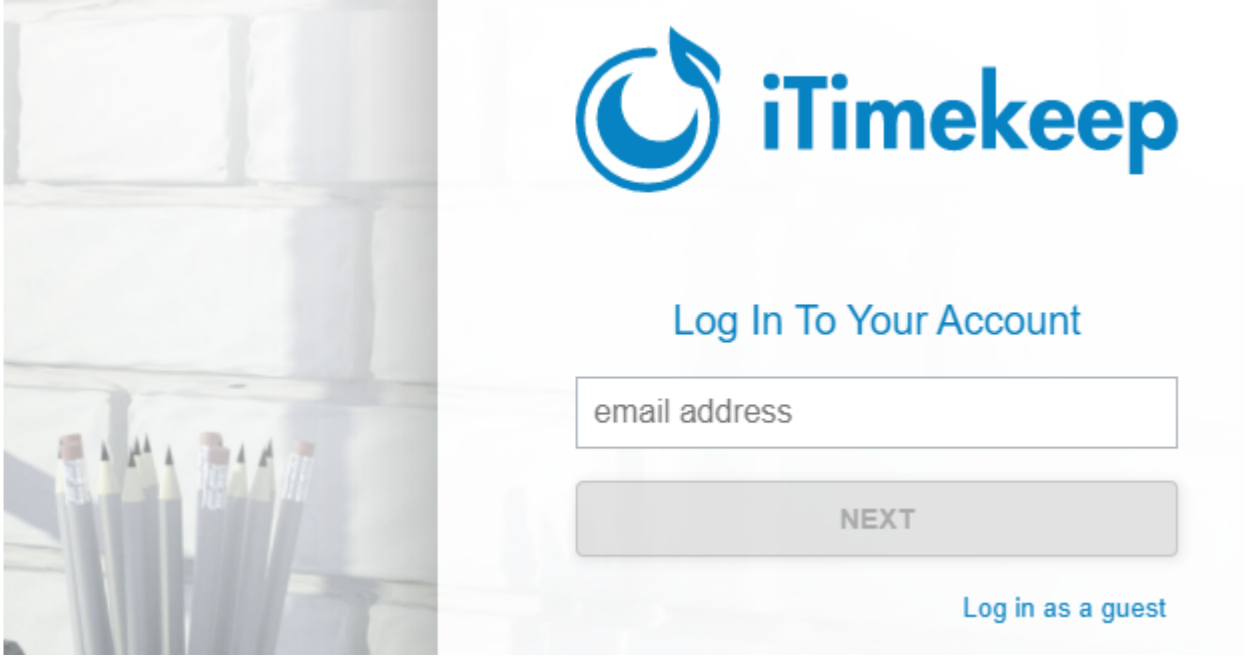
Copy the Azure AD tenant ID that you obtained from the Azure Portal and paste the ID into the Tenant Id textbox on the popup. Click the SAVE button.



Authority: AzureAD

Tenant Id:

Azure AD will now require you to accept the iTimekeep application's permissions. Open iTimekeep Desktop in a browser window, enter your email address and click the NEXT button.



The browser should redirect to the Azure AD sign-in page. Enter your Azure AD password.

Since this is the first time logging in via Azure AD, you should receive a popup asking you to accept permissions for the iTimekeep application on behalf of your domain. Accept the permissions. Azure AD requires this step only until the Azure AD administrator has accepted the permissions on behalf of the entire domain, so the popup should not appear during subsequent logins.

Verify that you are able to login to the iTimekeep Portal site and the Mobile application. You should see the same user experience for those environments: you will enter your email address on the iTimekeep login page, then be redirected to the Azure AD sign-in page to enter your Azure AD password. If those logins are successful, then iTimekeep SSO has been successfully configured.

Configuring SSO Via SAML2

Security Assertion Markup Language 2.0 (SAML 2.0) is a standard the enables a Service Provider (SP) such as iTimekeep and an Identity Provider (IP) to exchange authentication and authorization identities between security domains. iTimekeep currently supports the following SAML2 Identity Providers:

- Okta
- Duo

Logins may be initiated by either the Service Provider or the Identity Provider. SP-initiated logins are from the iTimekeep Desktop, Portal and Mobile login pages as well as the login pages for Thrive and OCG Live.

IP-Initiated logins typically involve logging in to the Identity Provider, then clicking on an “application”. For example, logging in to the Okta Dashboard or Duo Central, then clicking on the icon or tile for iTimekeep.

iTimekeep, Thrive and OCG Live support both SP-initiated and IP-initiated logins. If all three applications should be available for IP-initiated logins, you will need to configure SSO for all three applications. The following documentation is for the iTimekeep application. The other two applications have been omitted for brevity, but you will follow the same steps to enable SSO for them.

Configuring SSO Via SAML2 Using Okta

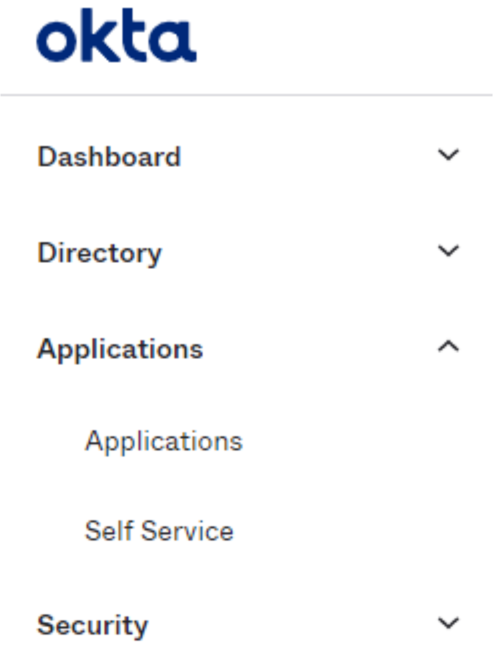
iTimekeep SSO supports:

- SP-initiated logins from the iTimekeep Desktop, Portal and Mobile login pages.
- IP-initiated logins for iTimekeep Desktop and Portal via an iTimekeep “tile” on the firm’s Okta SSO page or dashboard.

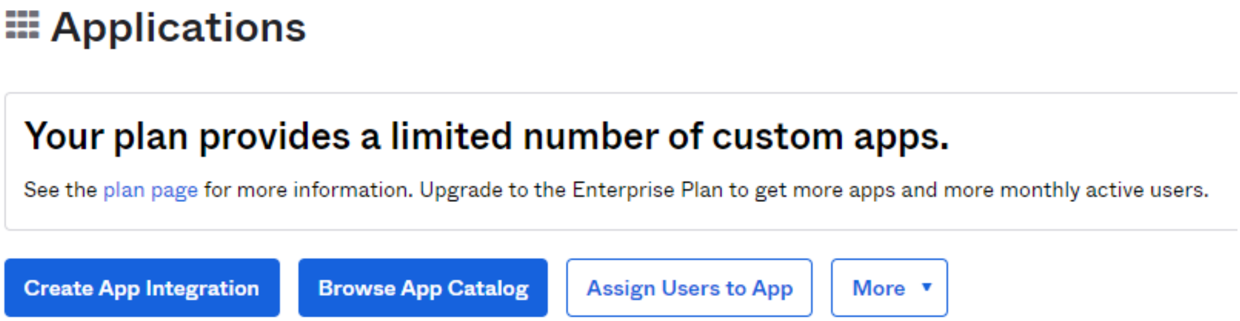
iTimekeep does not currently support:

- Just-in-time user provisioning from Okta.

To configure Okta and iTimekeep for SSO logins via Okta, login to the Okta administrator site and navigate to the Applications page from the Applications section of the menu.



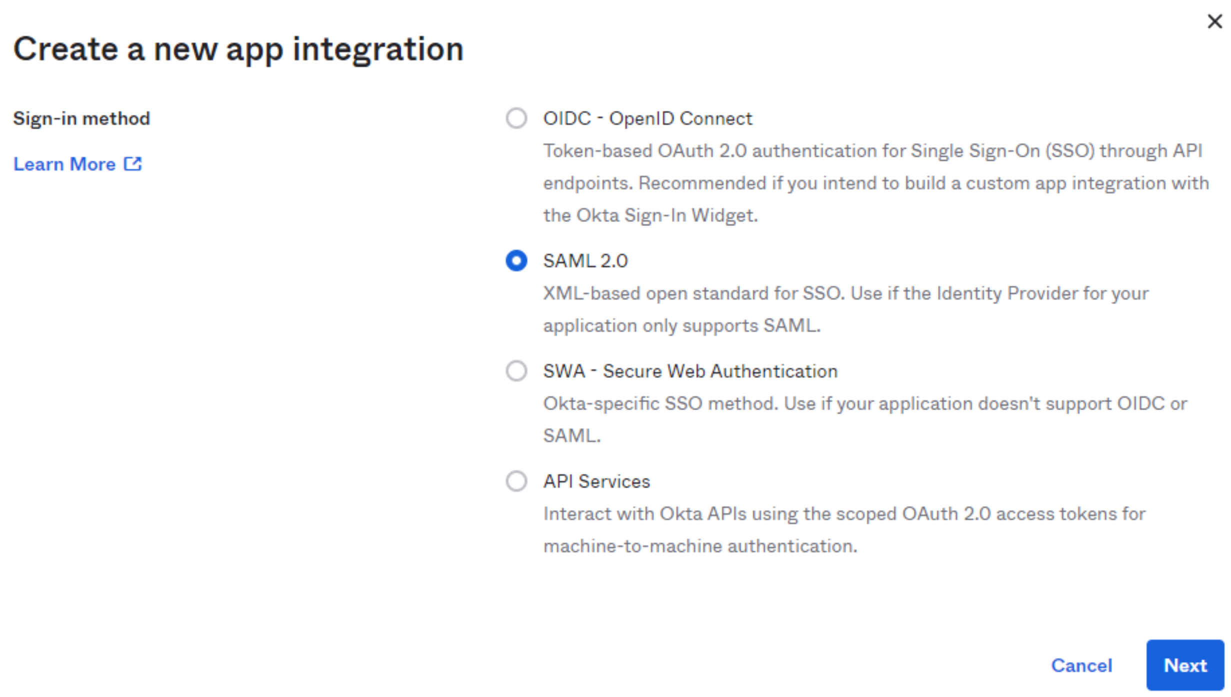
Click the Create App Integration button.



Your plan provides a limited number of custom apps.

See the plan page for more information. Upgrade to the Enterprise Plan to get more apps and more monthly active users.

Select SAML 2.0 on the popup for creating the new application, then click the Next button.



Create a new app integration

Sign-in method

○ OIDC - OpenID Connect
Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.

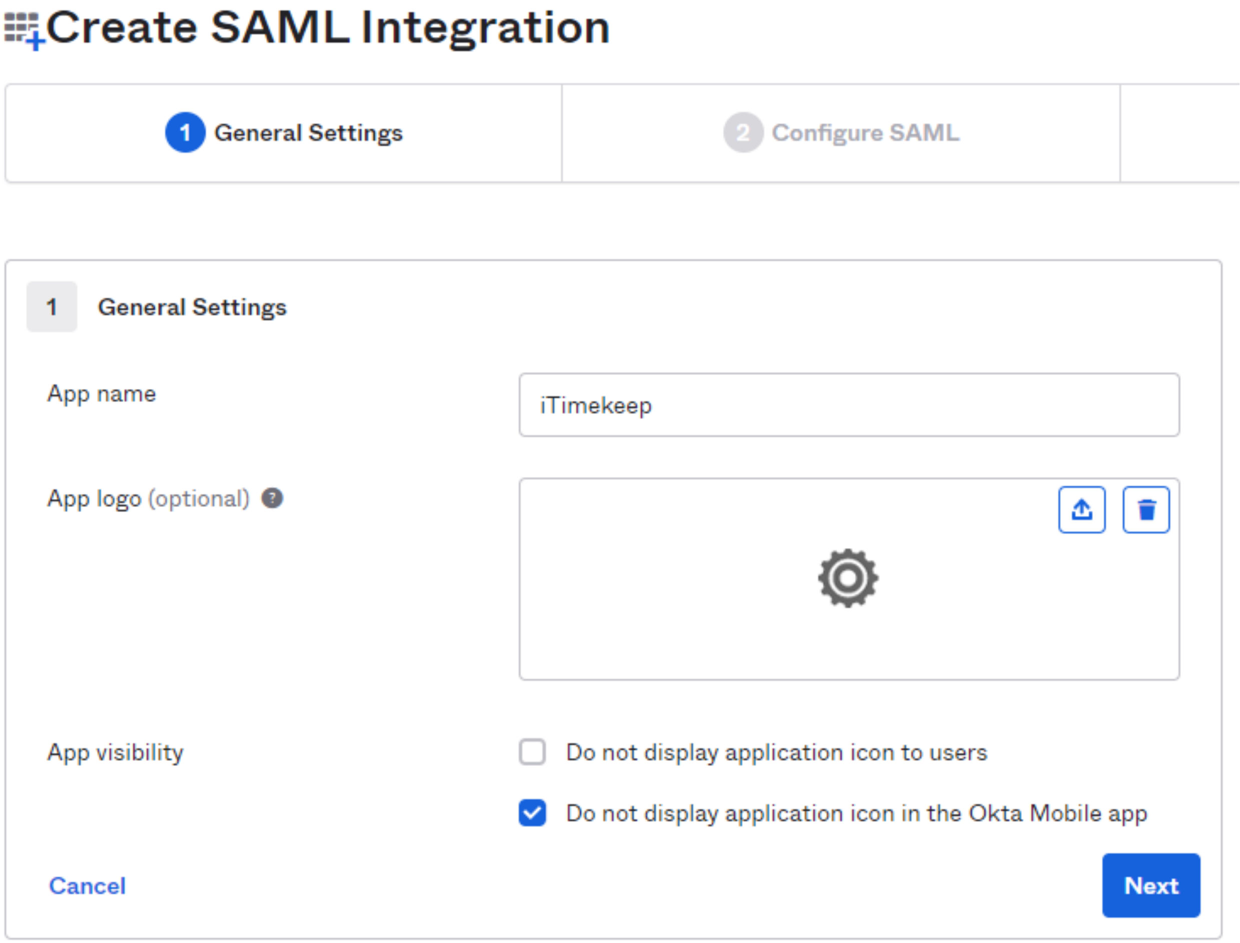
● SAML 2.0
XML-based open standard for SSO. Use if the Identity Provider for your application only supports SAML.

○ SWA - Secure Web Authentication
Okta-specific SSO method. Use if your application doesn't support OIDC or SAML.

○ API Services
Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.

Enter the following values on the General Settings tab on the Create SAML Integration popup:

- App name: iTimekeep
- App visibility: check the “Do not display application icon in the Okta Mobile app”
- Click the Next button.



Create SAML Integration

1 General Settings

2 Configure SAML

1 General Settings

App name: iTimekeep

App logo (optional)

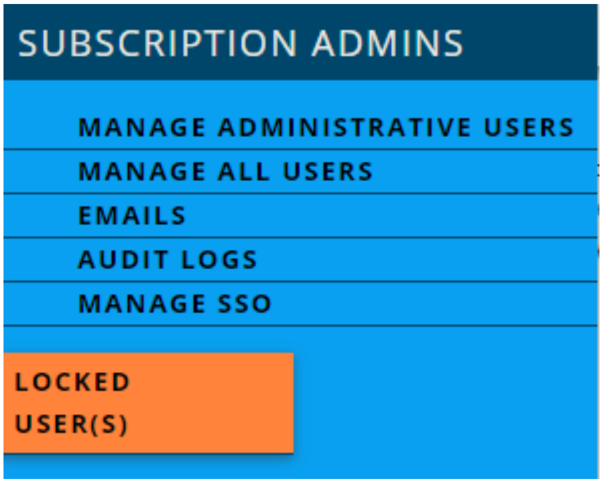
App visibility

☐ Do not display application icon to users

☑ Do not display application icon in the Okta Mobile app

The Configure SAML tab will now be visible. Keep this browser window open since you will need to copy some iTimekeep settings.

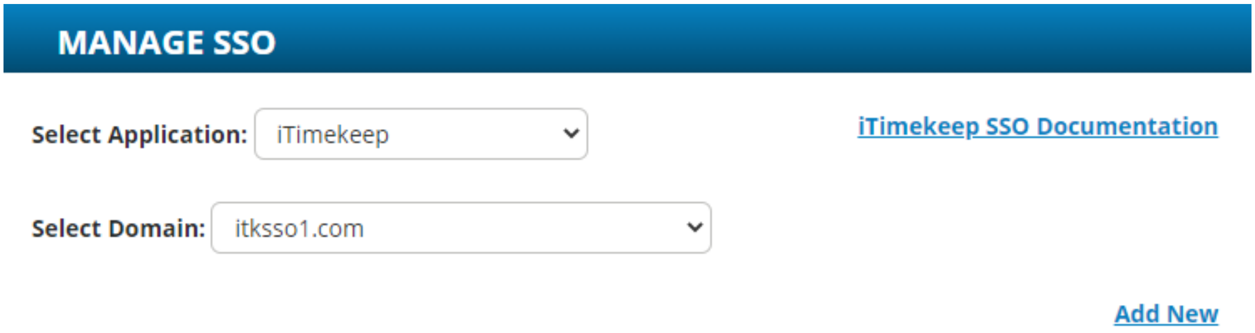
In another browser window or tab, also login to the iTimekeep Portal and navigate to the Manage SSO page.



Select iTimekeep from the Select Application dropdown.

Select the appropriate domain name from the dropdown.

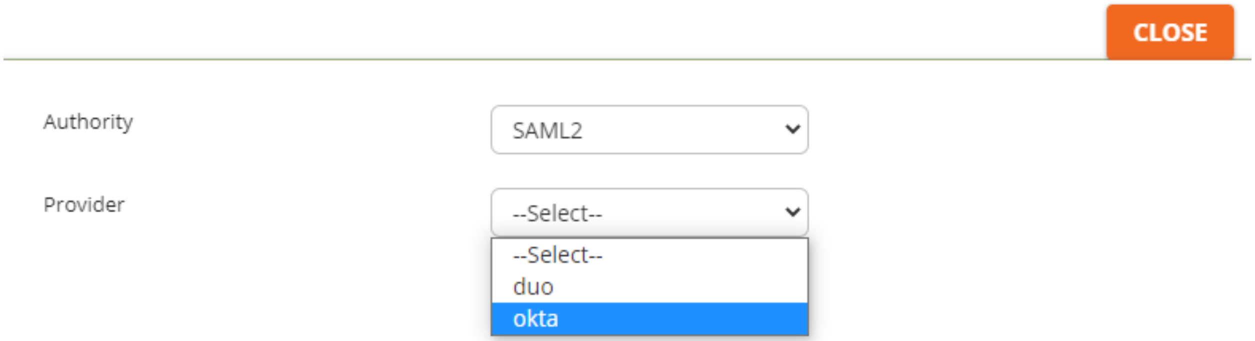
Click the Add New link on the right side of the page.



Select Application: iTimekeep

Select Domain: itksso1.com

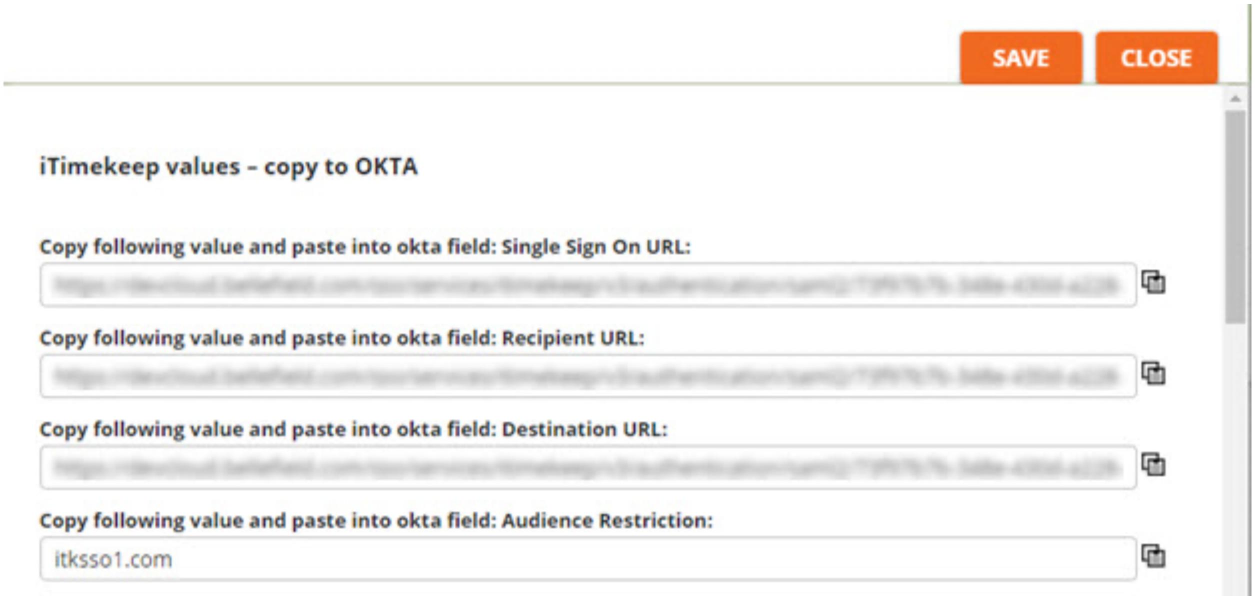
Select SAML2 from the Authority dropdown, then select Okta from the Provider dropdown.



Authority SAML2

Provider --Select--

You should now see a popup with iTimekeep values for copying to Okta and Okta values that must be copied from Okta. All of the values in the “iTimekeep values – copy to OKTA” section are prepopulated with settings that are customized to your iTimekeep subscription, your email domain and the iTimekeep application that you selected for configuration (i.e. iTimekeep, Thrive or OCG Live).



iTimekeep values – copy to OKTA

Copy following value and paste into okta field: Single Sign On URL:
[redacted]

Copy following value and paste into okta field: Recipient URL:
[redacted]

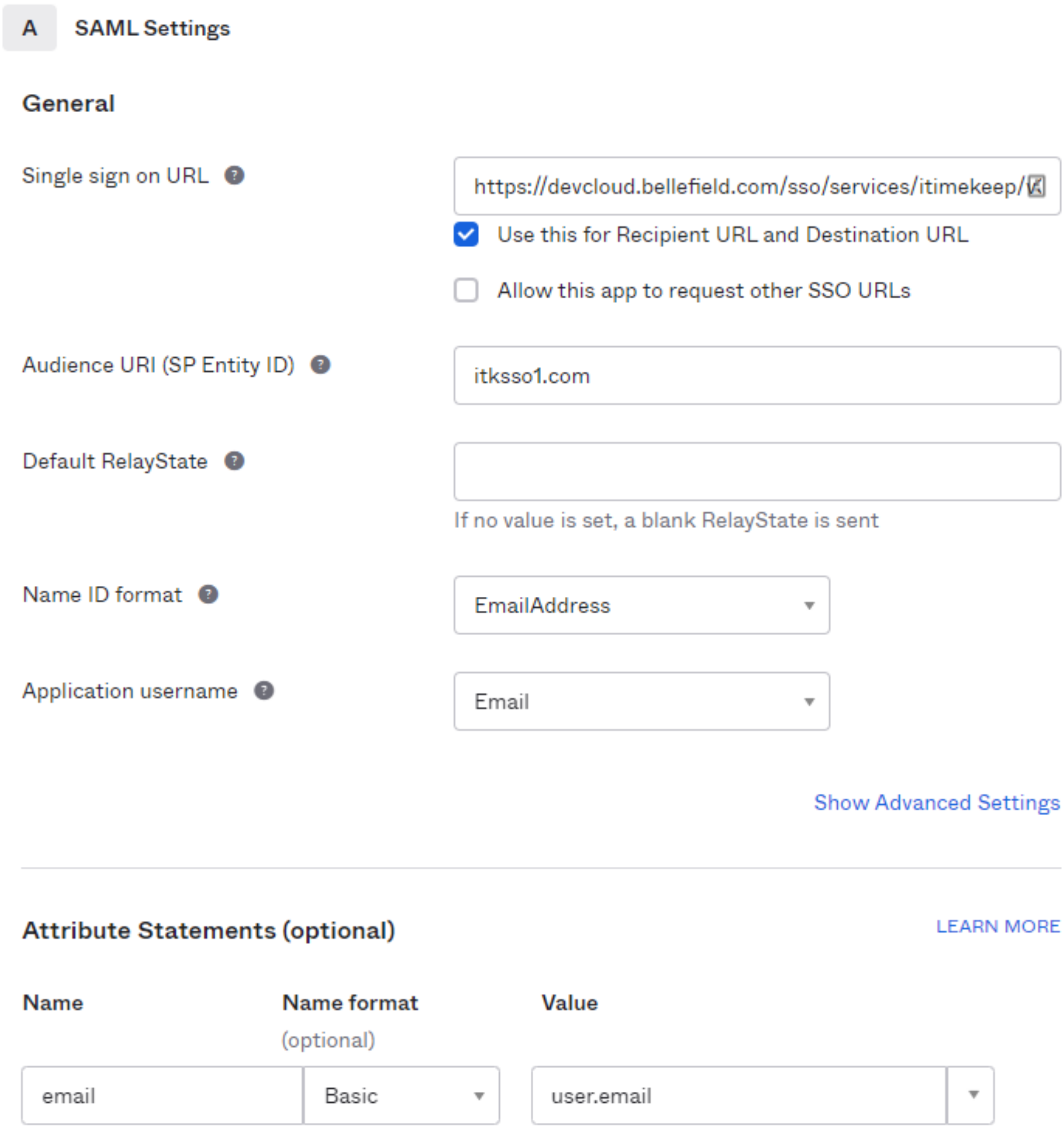
Copy following value and paste into okta field: Destination URL:
[redacted]

Copy following value and paste into okta field: Audience Restriction:
itksso1.com

Using the copy icons on the right side of each textbox and then paste the value into the specified field in the SAML settings page for the Okta application. This is the Okta page that you left open in a previous step. Set the following fields on the Okta page:

- Single sign on URL: paste the value from the Single Sign On URL field on the iTimekeep popup
- Use this for Recipient URL and Destination URL: the checkbox should checked
- Allow this app to request other SSO URLs: this checkbox should be unchecked
- Audience URI (SP Entity ID): paste the value from the Audience Restriction field on the iTimekeep popup
- Default RelayState: leave this field blank
- Name ID format: select EmailAddress from the dropdown
- Application username: Email
- In the Attribute Statements (optional) section, enter these values:
    - Name: email
    - Name format: select Basic from the dropdown
    - Value: select user.email from the dropdown
- In the Group Attribute Statements (optional) section, leave all fields blank.

The completed form should look similar to the following:



A SAML Settings

General

Single sign on URL: https://devcloud.bellefield.com/sso/services/itimekeep/

☑ Use this for Recipient URL and Destination URL

□ Allow this app to request other SSO URLs

Audience URI (SP Entity ID): itksso1.com

Default RelayState:

If no value is set, a blank RelayState is sent

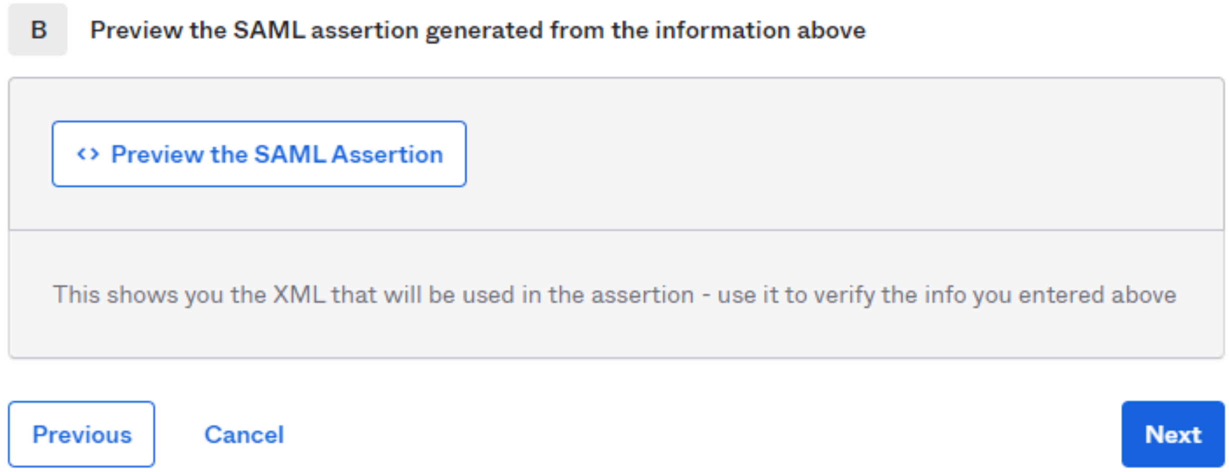
Name ID format: EmailAddress

Application username: Email

Attribute Statements (optional)

Name	Name format (optional)	Value
email	Basic	user.email

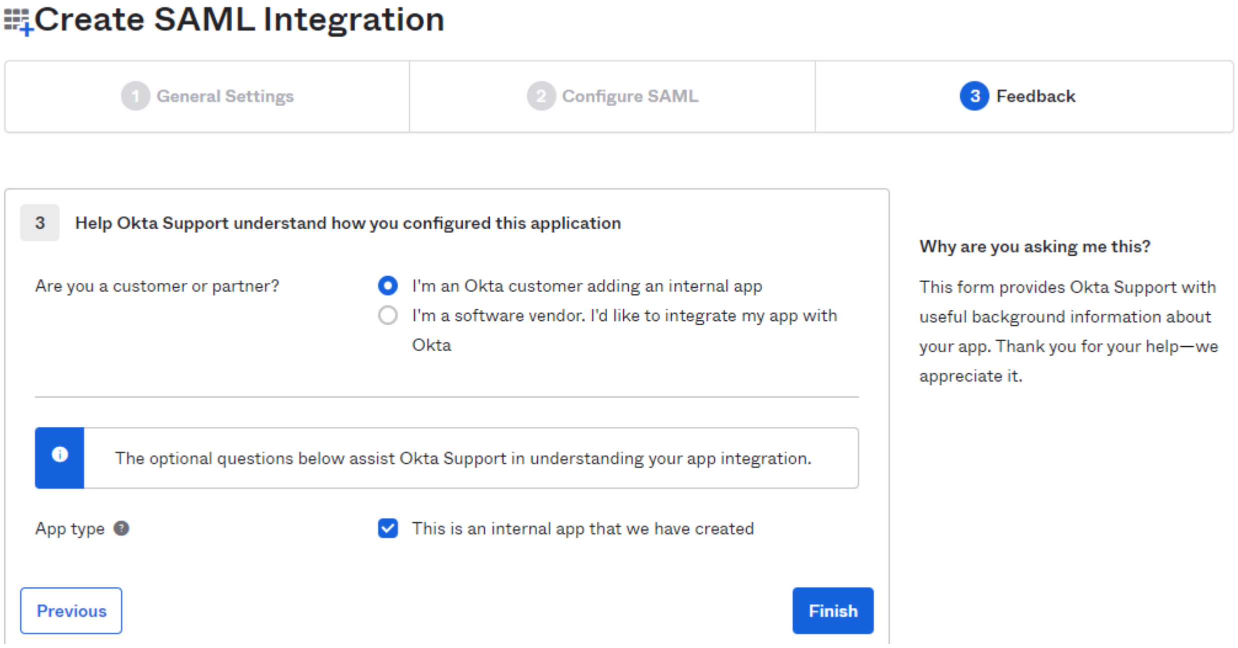
Scroll down to the "Preview the SAML Assertion Generated from the Information Above" section and click the "Preview the SAML Assertion" button. You should see a new window or tab with a valid XML document. If you see any error messages, correct the settings and try again. Contact iTimekeep's support team if you need any assistance.



Preview the SAML assertion generated from the information above

This shows you the XML that will be used in the assertion - use it to verify the info you entered above

If valid XML was displayed, click the Next button. Okta will display the Feedback tab. Click the "I'm an Okta customer adding an internal app" option, then check the "This is an internal app that we have created" option for the App Type.



Create SAML Integration

Help Okta Support understand how you configured this application

Are you a customer or partner?
● I'm an Okta customer adding an internal app
○ I'm a software vendor. I'd like to integrate my app with Okta

The optional questions below assist Okta Support in understanding your app integration.

App type
☑ This is an internal app that we have created

Why are you asking me this?

This form provides Okta Support with useful background information about your app. Thank you for your help—we appreciate it.

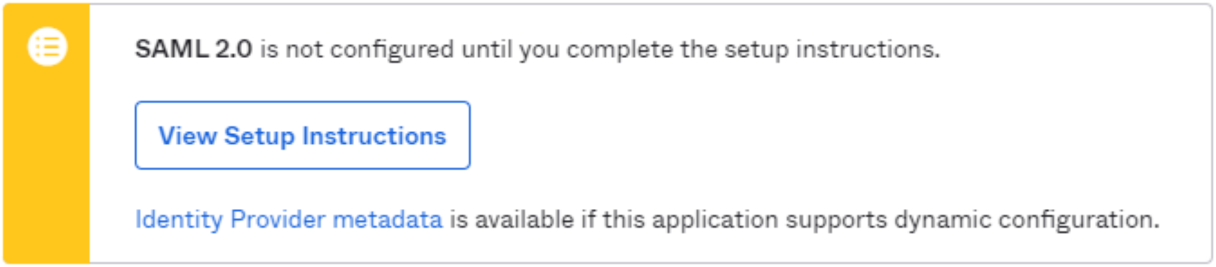
Click the Finish button.

Okta will now display the new application's Sign On tab. Locate the View Setup Instructions button in the yellow section of the page. iTimekeep supports two methods for copying Okta's settings to the corresponding iTimekeep configuration fields:

1. Download an Identity Provider metadata file from Okta, then upload the file to iTimekeep.
2. Copy the configuration settings from the Okta page to the iTimekeep popup.

Option 1: Use an Identity Provider metadata file from Okta

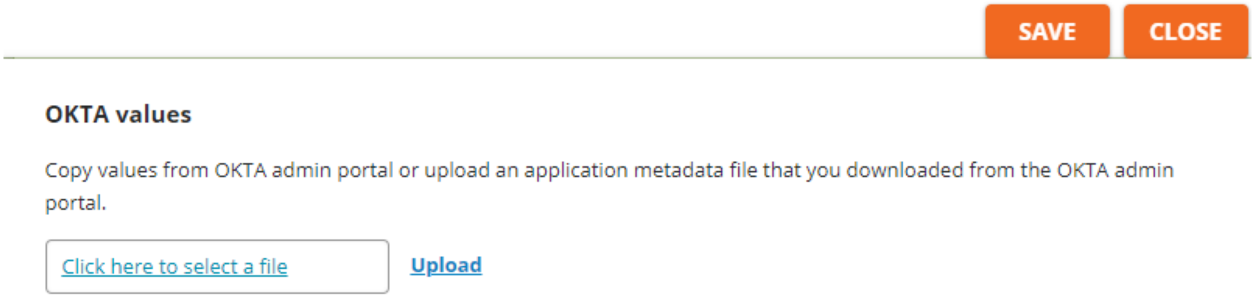
In the yellow section on Okta’s page, right-click the “Identity Provider metadata” link and select the “Save link as…” option to save the file to your local computer.



SAML 2.0 is not configured until you complete the setup instructions.

Identity Provider metadata is available if this application supports dynamic configuration.

On iTimekeep’s popup, scroll down to the OKTA Values section of the popup. Click the “Click here to select a file” link.



OKTA values

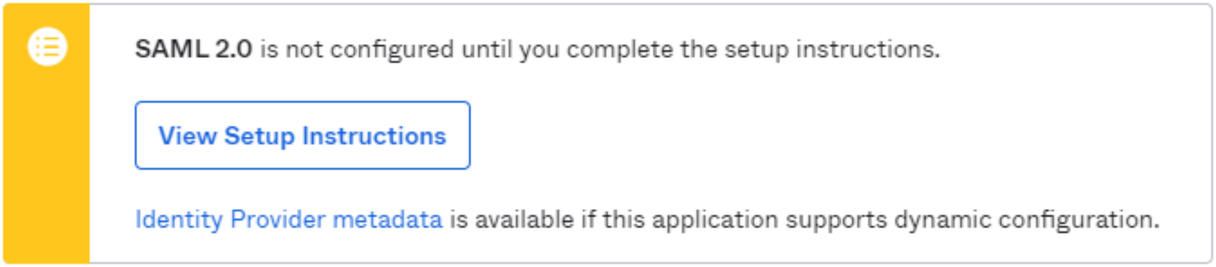
Copy values from OKTA admin portal or upload an application metadata file that you downloaded from the OKTA admin portal.

Select the metadata file that you downloaded from Okta, then click the Upload link. All fields in the OKTA Values section of the popup should be populated. Click the Save button.

Skip to the **Continuing The Okta Configuration** section.

Option 2: Copy settings from the Okta page to the iTimekeep popup

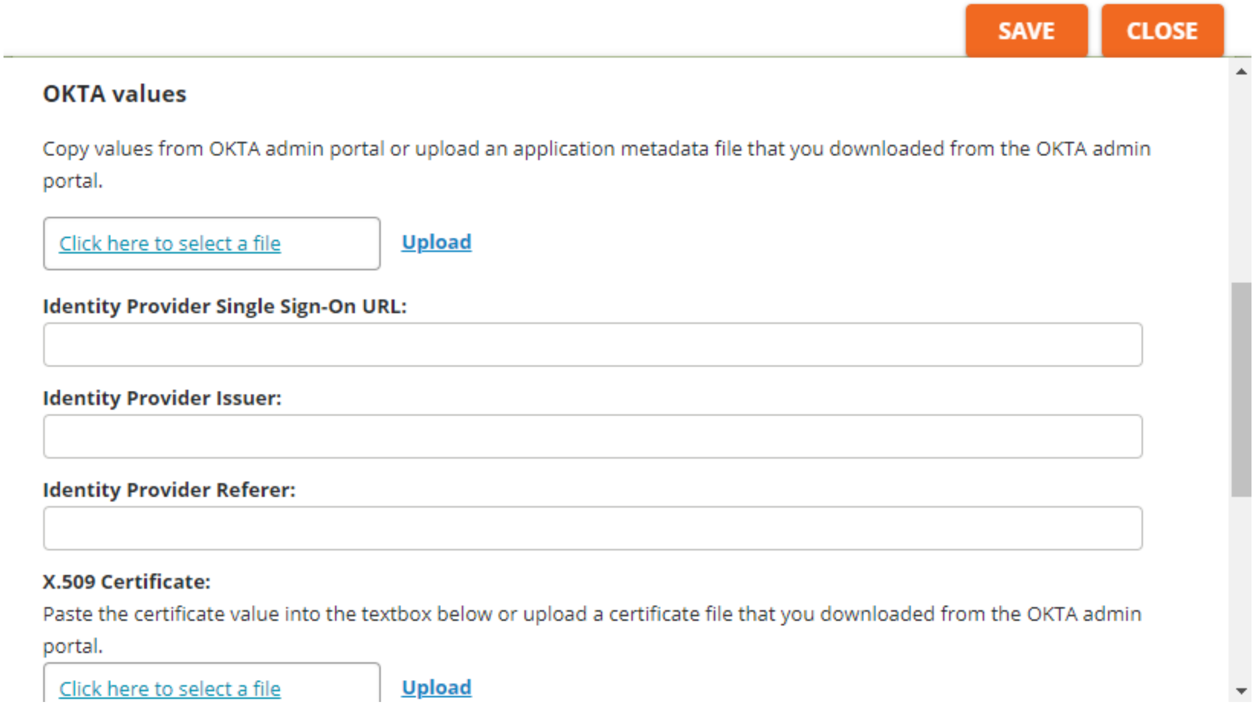
Click the View Setup Instructions button in the yellow section on the Okta page.



SAML 2.0 is not configured until you complete the setup instructions.

Identity Provider metadata is available if this application supports dynamic configuration.

You will now copy values from Okta’s “The following is needed to configure iTimekeep” into fields on the popup that should still be visible on the tab with the iTimekeep page.



OKTA values

Copy values from OKTA admin portal or upload an application metadata file that you downloaded from the OKTA admin portal.

Identity Provider Single Sign-On URL:

Identity Provider Issuer:

Identity Provider Referer:

X.509 Certificate:

Paste the certificate value into the textbox below or upload a certificate file that you downloaded from the OKTA admin portal.

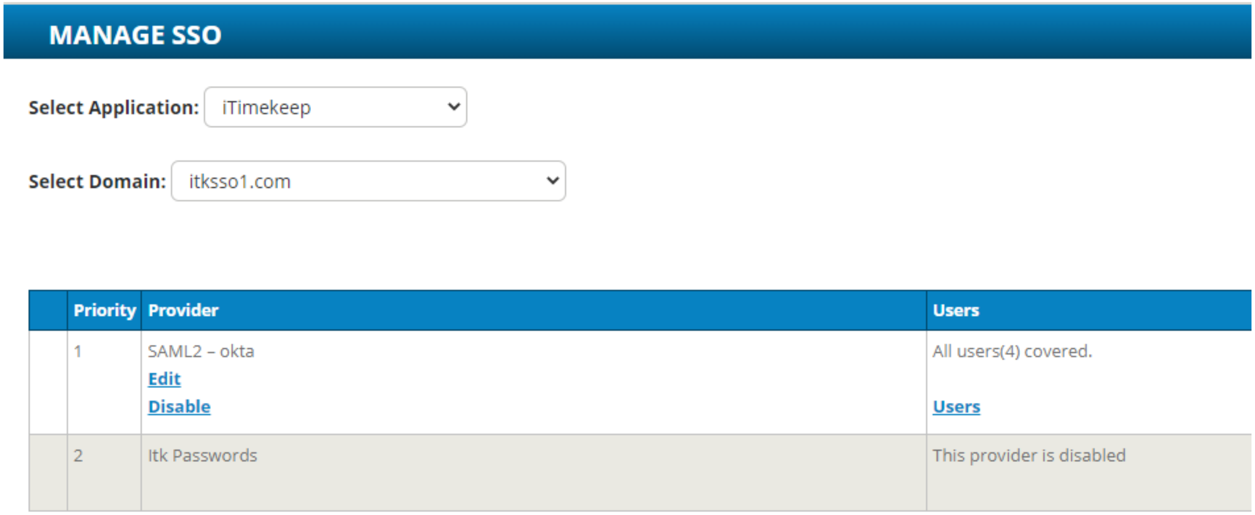
Copy values from the Okta page and paste into iTimekeep's popup as follows:

- Identity Provider Single Sign-On URL: paste into the "Identity Provider Single Sign-On URL" textbox.
- Identity Provider Issuer: paste into the "Identity Provider Issuer" textbox.
- Leave the "Identity Provider Referer" textbox empty.
- X.509 Certificate: paste into the "X.509 Certificate" textbox.

Click the Save button.

Continuing The Okta Configuration

Regardless of whether you entered the Okta configuration values into iTimekeep's popup by importing a metadata file or by copying/pasting values, you should now see the following page:



MANAGE SSO

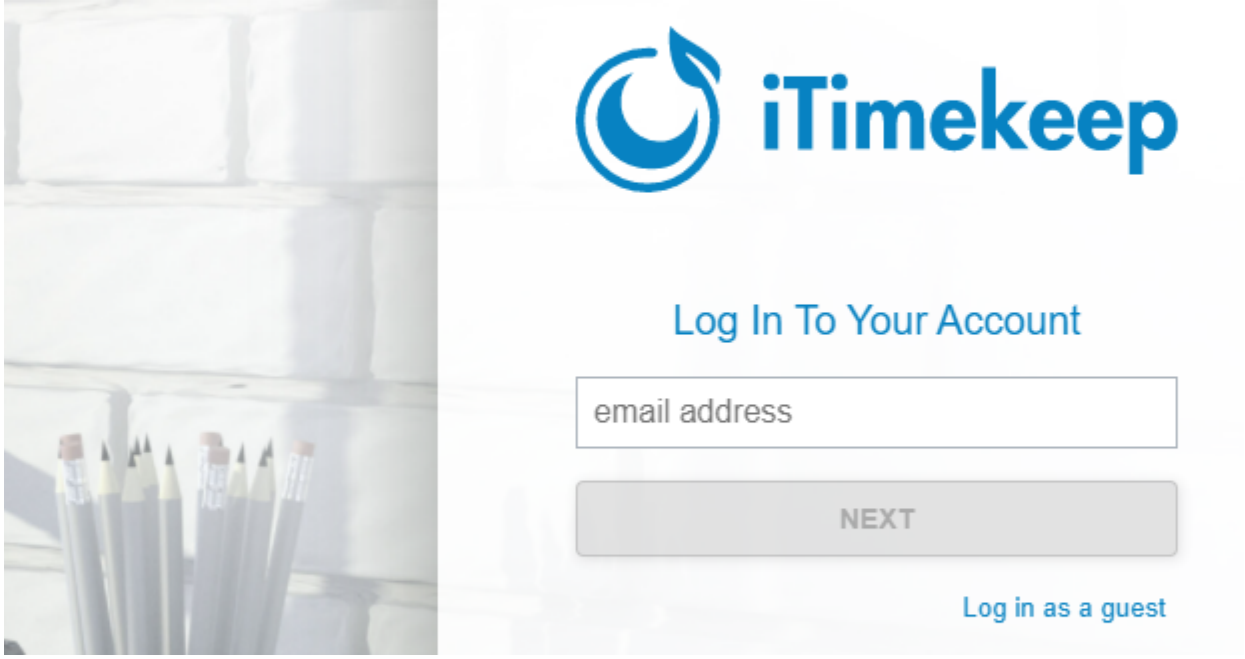
Select Application: iTimekeep

Select Domain: itksso1.com

	Priority	Provider	Users
	1	SAML2 – okta Edit Disable	All users(4) covered. Users
	2	Itk Passwords	This provider is disabled

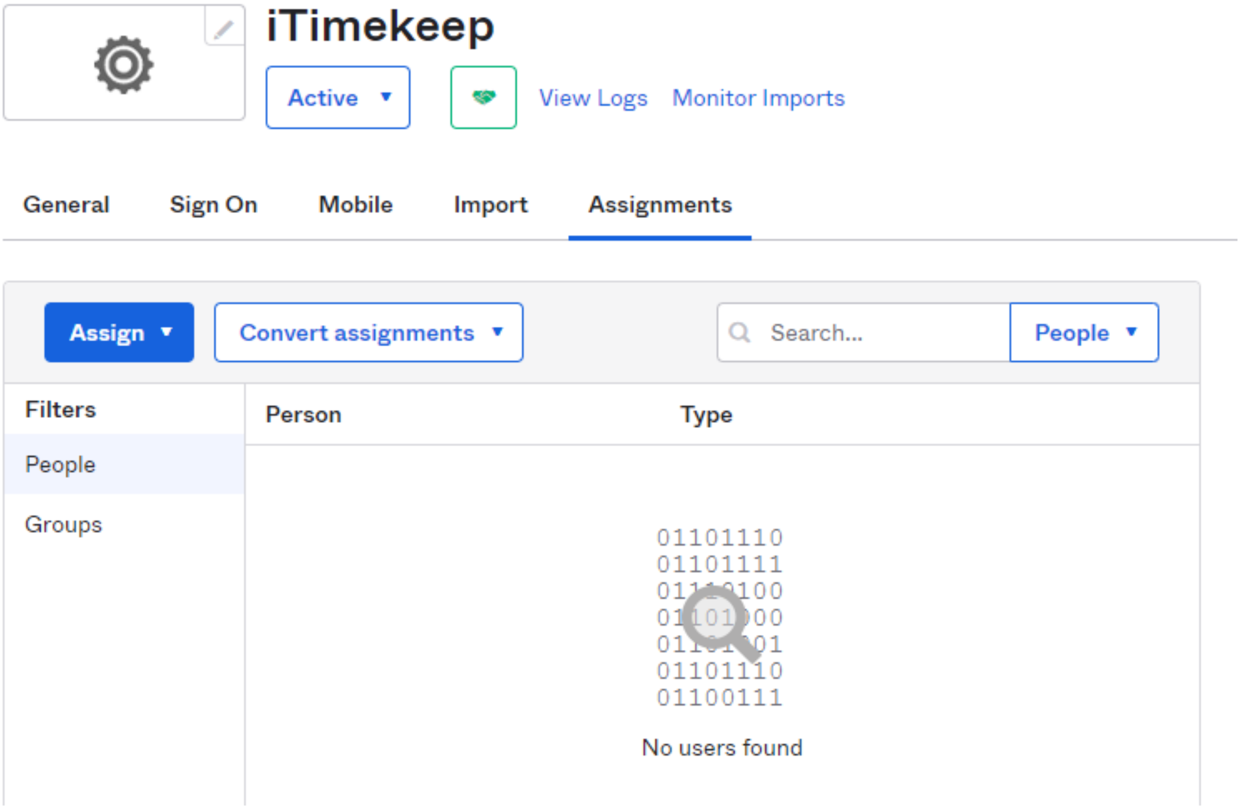
SSO logins via Okta are now enabled for all iTimekeep users with email addresses matching the selected domain. If you plan to limit SSO logins for iTimekeep to a limited number of users initially, refer to the **Configuring SSO For Limited Users** section for specifying the users.

To test SP-initiated logins from iTimekeep Desktop, open iTimekeep Desktop in a browser window, enter your email address and click the NEXT button.



The browser should redirect to the Okta's sign-in page. Enter your Okta password. The browser should redirect back to iTimekeep's My Time page.

If the browser was not redirected back to the My Time page, you may need to change the user and/or group assignments for the Okta application. On Okta's application configuration page for the iTimekeep application, click the Assignments tab, then use your usual procedures for assigning users and/or groups to the iTimekeep application.



No users found

You should also test iTimekeep Mobile logins by opening the app on a phone and entering your email address as usual. The app should redirect to Okta's login page, which should redirect back to the My Time screen on the iTimekeep app.

If your firm plans to allow users to access iTimekeep from their Okta dashboard, test those logins by logging into Okta from a browser. Click on iTimekeep's tile. The browser should redirect to the My Time page.

If Thrive and OCG Live should be available for IP-initiated logins from the Okta Dashboard, repeat the setup process for each application, but select Thrive or OCG Live as the application on the first step.

Skip to the **Advanced Topics** for additional optional configuration steps.

Configuring SSO Via SAML2 Using Duo

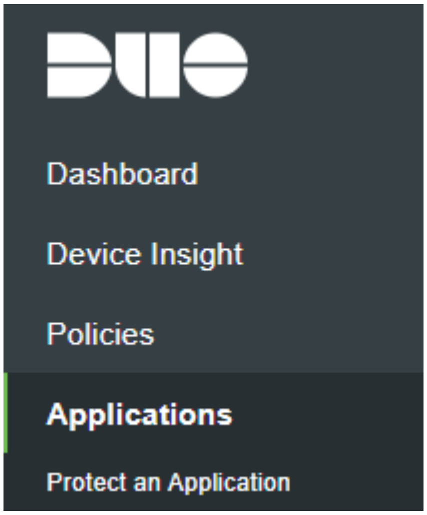
iTimekeep SSO supports:

- SP-initiated logins from the iTimekeep Desktop, Portal and Mobile login pages.
- IP-initiated logins for iTimekeep Desktop and Portal via an iTimekeep "tile" on the firm's Duo Central page or dashboard.

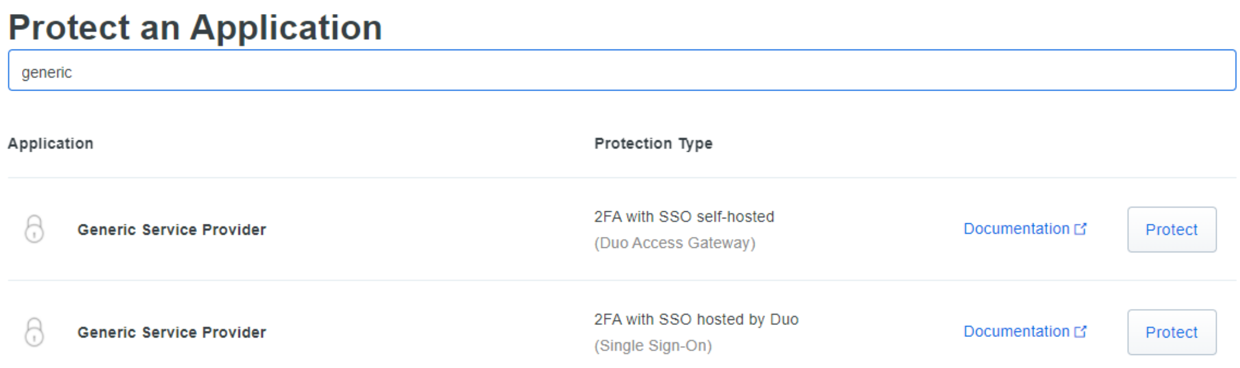
iTimekeep does not currently support:

- Just-in-time user provisioning from Duo.

To configure Duo and iTimekeep for SSO logins via Duo, login to the Duo administrator site and navigate to the Protect An Application page from the Applications section of the menu.



Enter "generic" in the Filter By Keywords, VPN, Microsoft, SAML textbox. The list will filter to a few generic service providers.

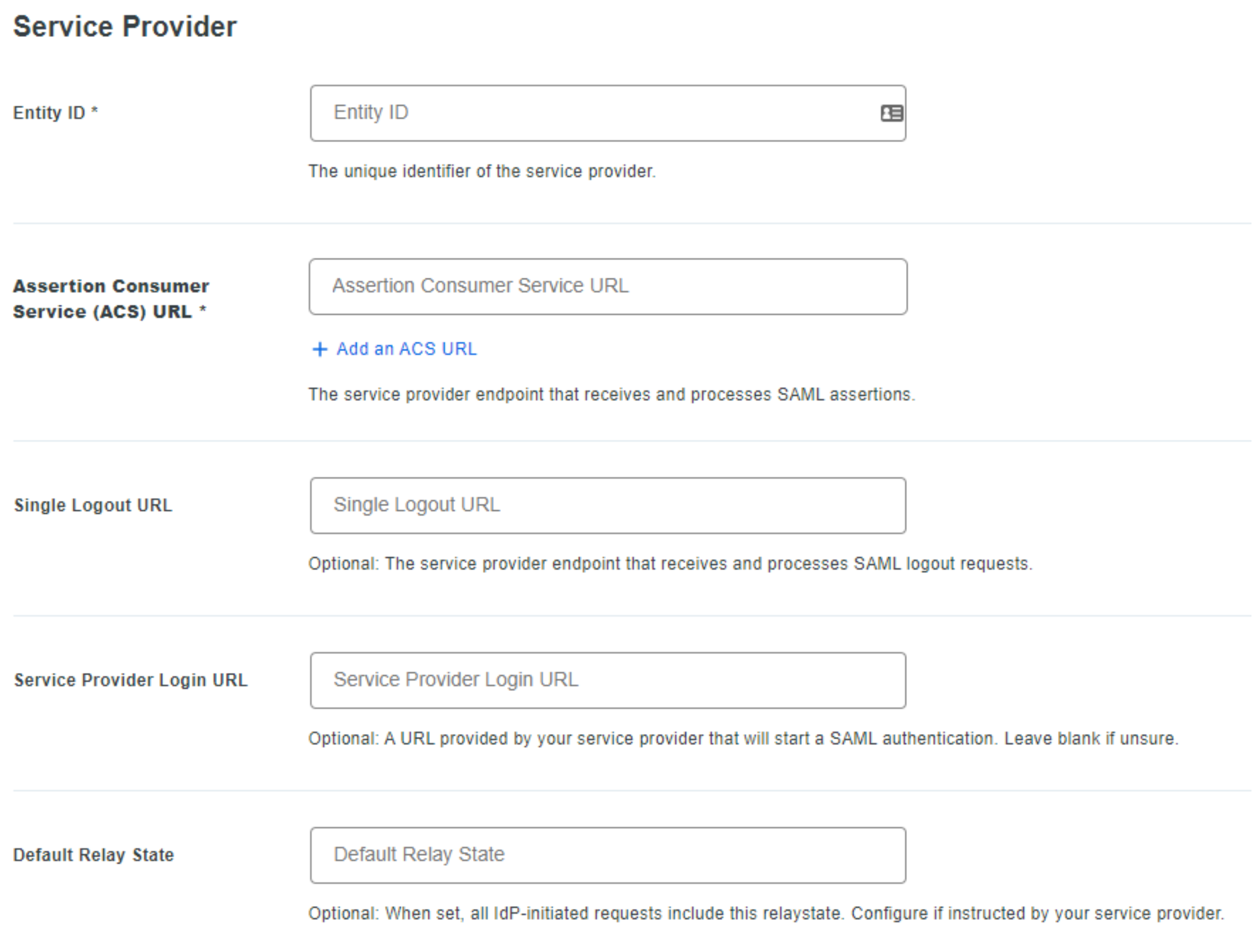


Protect an Application

generic

Application	Protection Type		
Generic Service Provider	2FA with SSO self-hosted (Duo Access Gateway)	Documentation	Protect
Generic Service Provider	2FA with SSO hosted by Duo (Single Sign-On)	Documentation	Protect

Depending on your Duo configuration and license, click the Protect button for either "2FA with SSO self-hosted" or "2FA with SSO hosted by Duo". For the sake of this example, assume the latter option. The Generic Service Provider – Single Sign-On page will now be displayed.



Service Provider

Entity ID *: Entity ID

The unique identifier of the service provider.

Assertion Consumer Service (ACS) URL *: Assertion Consumer Service URL

+ Add an ACS URL

The service provider endpoint that receives and processes SAML assertions.

Single Logout URL: Single Logout URL

Optional: The service provider endpoint that receives and processes SAML logout requests.

Service Provider Login URL: Service Provider Login URL

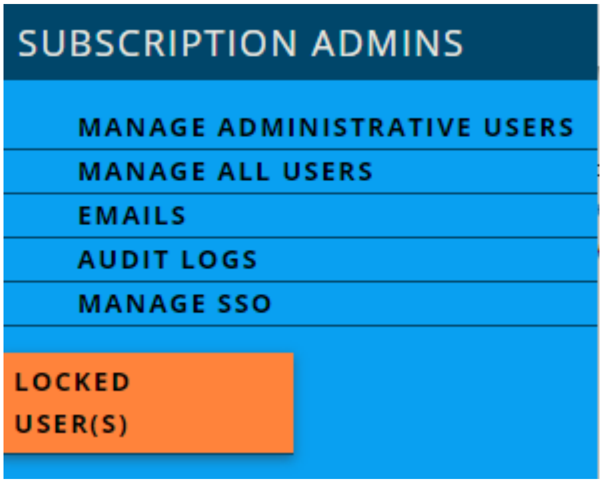
Optional: A URL provided by your service provider that will start a SAML authentication. Leave blank if unsure.

Default Relay State: Default Relay State

Optional: When set, all IdP-initiated requests include this relaystate. Configure if instructed by your service provider.

Keep this browser window open since you will need to copy some iTimekeep settings.

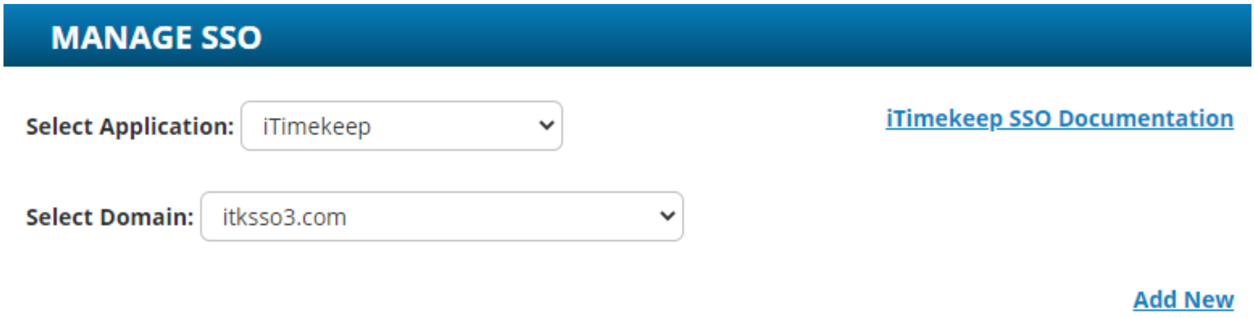
In another browser window or tab, also login to the iTimekeep Portal and navigate to the Manage SSO page.



Select iTimekeep from the Select Application dropdown.

Select the appropriate domain name from the dropdown.

Click the Add New link on the right side of the page.

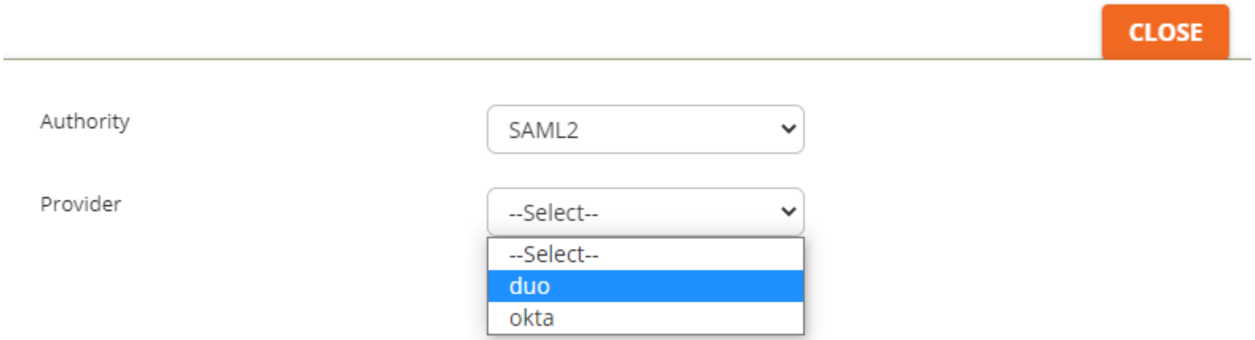


MANAGE SSO

Select Application: iTimekeep

Select Domain: itksso3.com

Select SAML2 from the Authority dropdown, then select Duo from the Provider dropdown.



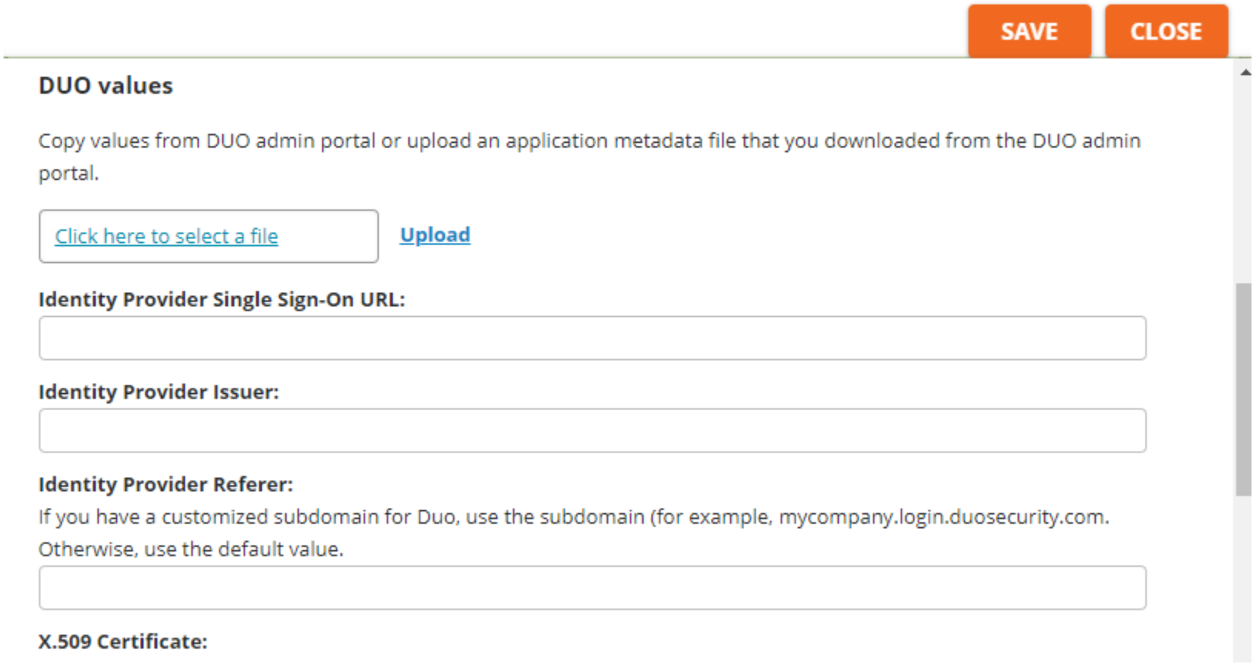
Authority: SAML2

Provider: --Select--

You should now see a popup with iTimekeep values for copying to Duo and Duo values that must be copied from Duo. All of the values in the “iTimekeep values – copy to DUO” section are prepopulated with settings that are customized to your iTimekeep subscription, your email domain and the iTimekeep application that you selected for configuration (i.e. iTimekeep, Thrive or OCG Live).

Copy Duo’s Settings Into Itimekeep

Scroll down to the DUO Values section of the page to add values from the Duo page that is still open in the other window or tab.



DUO values

Copy values from DUO admin portal or upload an application metadata file that you downloaded from the DUO admin portal.

Identity Provider Single Sign-On URL:

Identity Provider Issuer:

Identity Provider Referer:

If you have a customized subdomain for Duo, use the subdomain (for example, mycompany.login.duosecurity.com. Otherwise, use the default value.

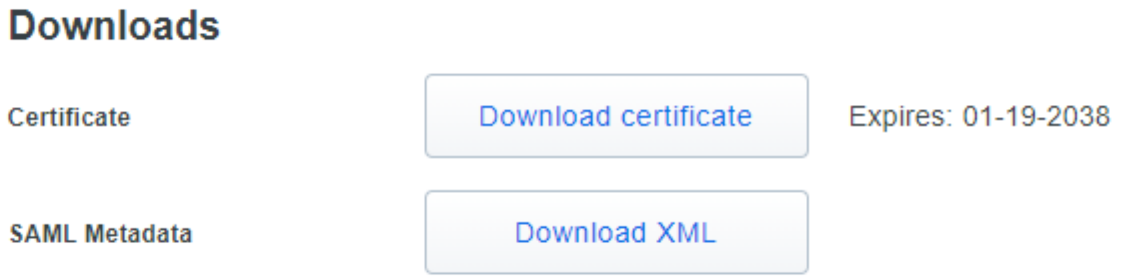
X.509 Certificate:

iTimekeep supports two methods for copying Duo's settings to the corresponding iTimekeep configuration fields:

1. Download an Identity Provider metadata file from Duo, then upload the file to iTimekeep.
2. Copy the configuration settings from the Duo page to the iTimekeep popup.

Option 1: Use an Identity Provider metadata file from Duo

Locate the Downloads section on the Duo window/tab, then click the Download XML button next to SAML Metadata. A configuration XML file will be downloaded to your local computer.



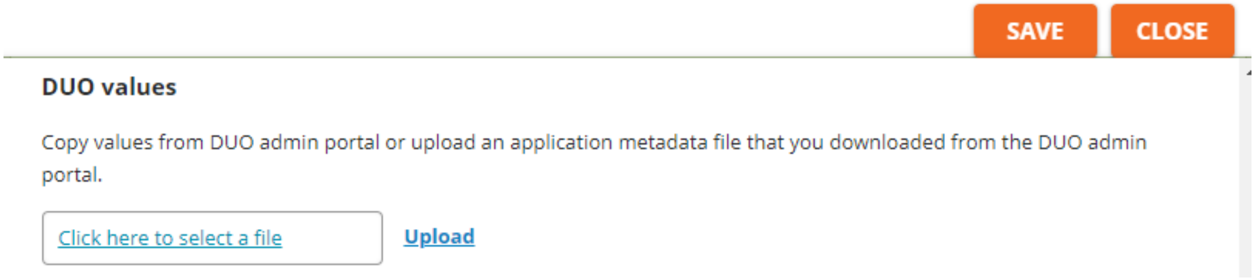
Downloads

Certificate

Expires: 01-19-2038

SAML Metadata

On iTimekeep's popup, scroll down to the DUO Values section of the popup. Click the "Click here to select a file" link.



DUO values

Copy values from DUO admin portal or upload an application metadata file that you downloaded from the DUO admin portal.

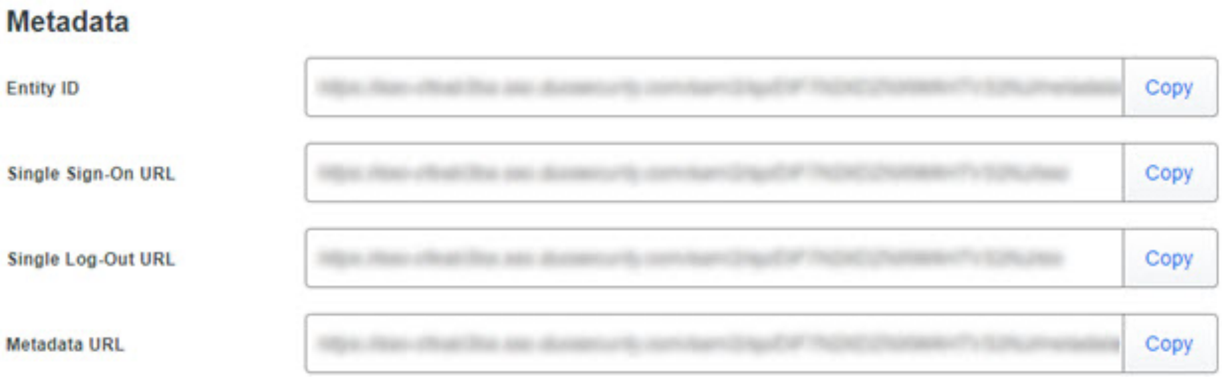
Select the metadata file that you downloaded from Duo, then click the Upload link. All fields in the DUO Values section of the popup should be populated.

IMPORTANT: Importing the settings populates the Identity Provider Referrer field based on the host name that was imported into the Identity Provider Single Sign-On URL field. If your Duo license includes a custom Single Sign On subdomain such as myfirm.login.duosecurity.com, you must specify that subdomain in the Identity Provider Referrer field on the form. For this example, enter myfirm.login.duosecurity.com as the referrer. Do not change any other imported fields.

Skip to the next step, **Copying Itimekeep's Settings Into Duo**

Option 2: Copy settings from the Duo page to the iTimekeep popup

You will now copy values from the Metadata section of the Duo page into fields on the popup that should still be visible on the tab with the iTimekeep page. Locate this section of the Duo page:



Metadata

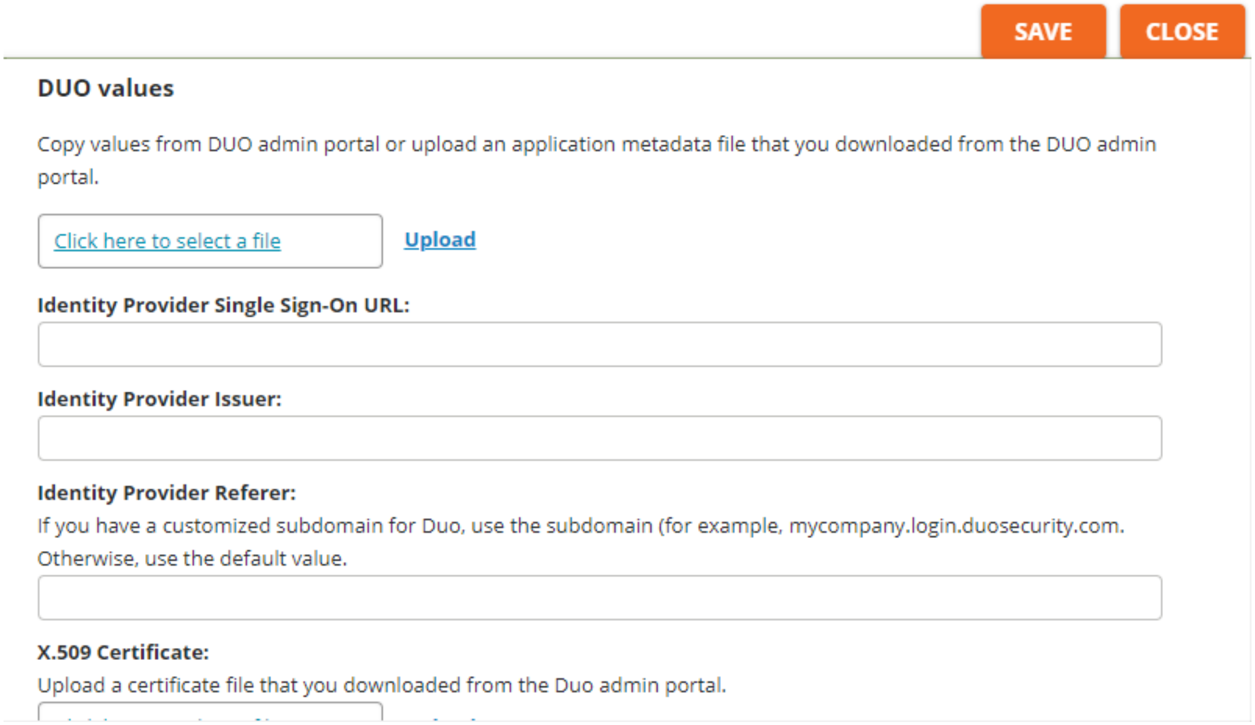
Entity ID [redacted]

Single Sign-On URL [redacted]

Single Log-Out URL [redacted]

Metadata URL [redacted]

Locate the DUO Values section on the iTimekeep popup.



DUO values

Copy values from DUO admin portal or upload an application metadata file that you downloaded from the DUO admin portal.

Identity Provider Single Sign-On URL:

Identity Provider Issuer:

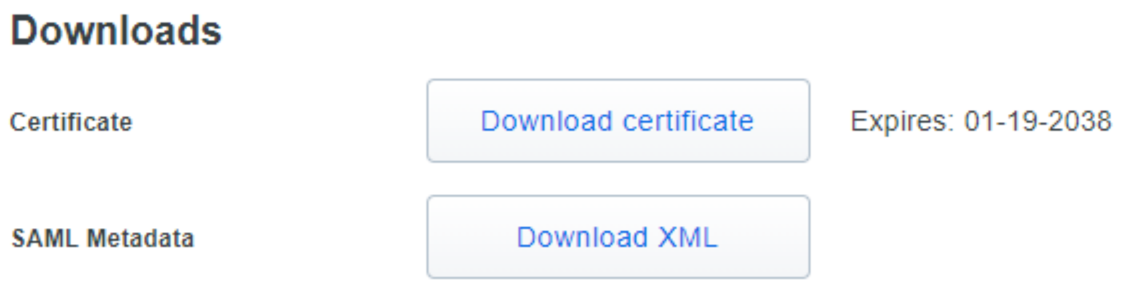
Identity Provider Referer:
If you have a customized subdomain for Duo, use the subdomain (for example, mycompany.login.duosecurity.com. Otherwise, use the default value.

X.509 Certificate:
Upload a certificate file that you downloaded from the Duo admin portal.

Copy values from the Duo page and paste into iTimekeep's popup as follows:

- Entity ID: paste into the "Identity Provider Issuer" textbox on the iTimekeep popup.
- Single Sign-On URL: paste into the "Identity Provider Single Sign-On URL" textbox on the iTimekeep popup.
- Set "Identity Provider Referrer" textbox as follows:
    - If your Duo license includes a custom Single Sign On subdomain such as myfirm.login.duosecurity.com, you must specify that subdomain in the Identity Provider Referrer field on the form. For this example, enter myfirm.login.duosecurity.com as the referrer.
    - Otherwise, use part of the value that you pasted into the "Identity Provider Single Sign-On URL" textbox. That value should start with something similar to "https://sso-random.sso.duosecurity.com/saml2/....". Copy the "sso-random.sso.duosecurity.com" portion of the URL and paste into the referrer textbox.

Scroll down to the Downloads section of the Duo page.

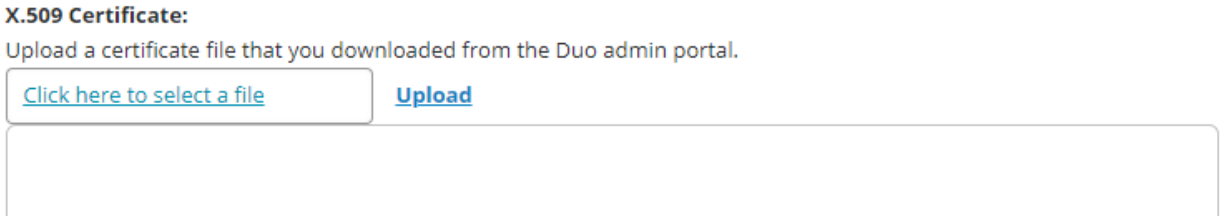


Downloads

Certificate — Expires: 01-19-2038

SAML Metadata

Click the Download Certificate button to download the certificate to your local computer. On the iTimekeep popup, scroll down to the X.509 Certificate section under DUO Values.



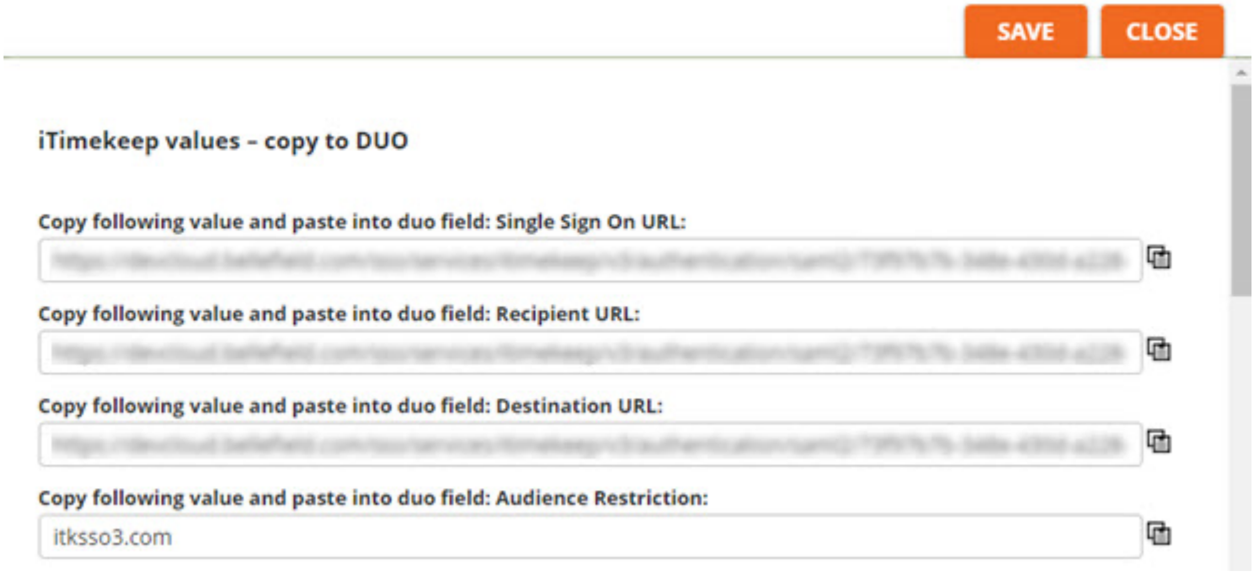
X.509 Certificate:

Upload a certificate file that you downloaded from the Duo admin portal.

Click the “Click here to select a file” link, then select the certificate file that you downloaded from Duo, then click Upload. The certificate will be imported into the textbox.

Copying Itimekeep’s Settings Into Duo

Next, you will copy iTimekeep’s setting into Duo. Scroll to the top of the iTimekeep popup to the “iTimekeep values – copy to DUO” section.



iTimekeep values - copy to DUO

Copy following value and paste into duo field: Single Sign On URL:

[redacted]

Copy following value and paste into duo field: Recipient URL:

[redacted]

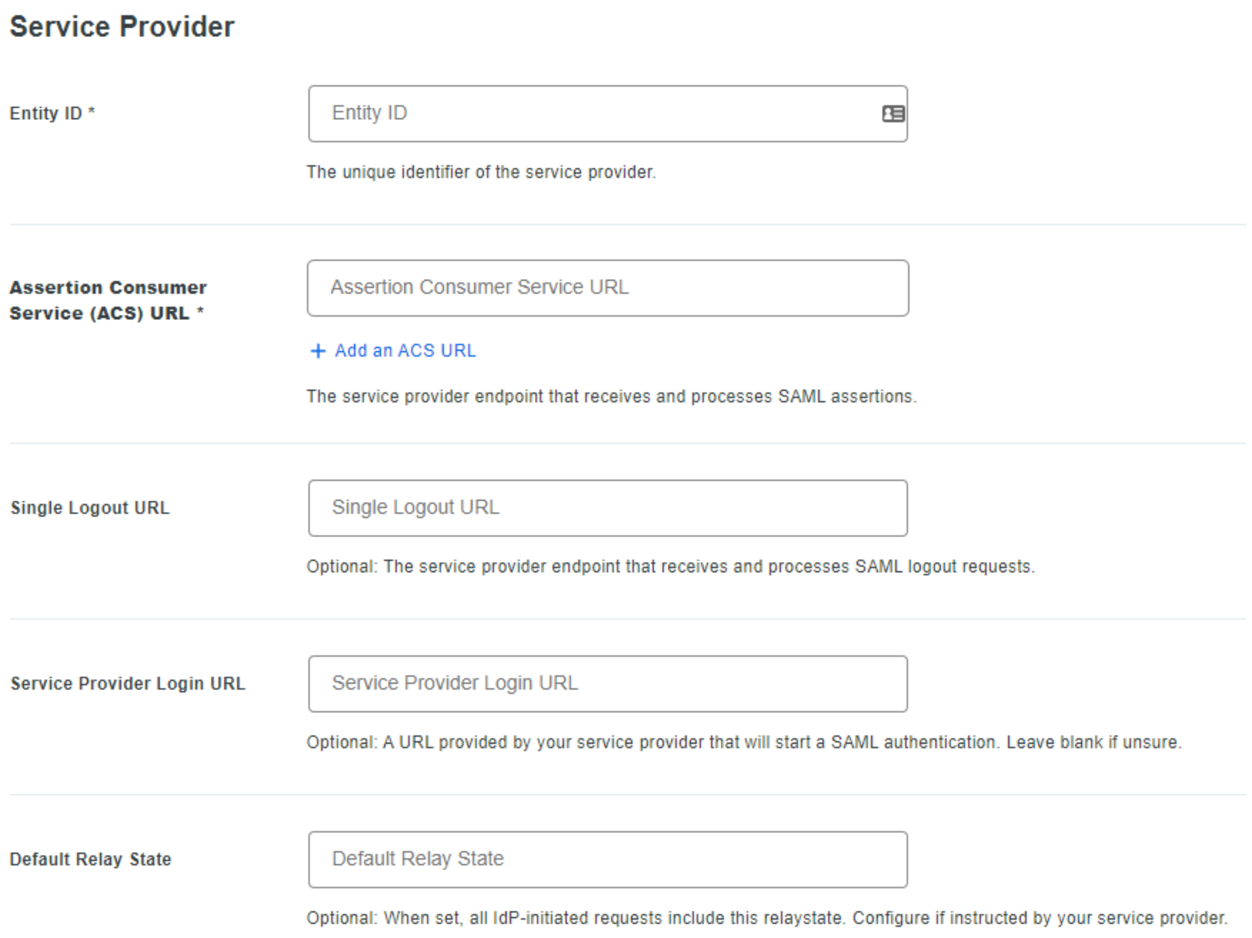
Copy following value and paste into duo field: Destination URL:

[redacted]

Copy following value and paste into duo field: Audience Restriction:

itksso3.com

Scroll down to the Service Provider section of the Duo page.



Service Provider

Entity ID *: Entity ID

The unique identifier of the service provider.

Assertion Consumer Service (ACS) URL *: Assertion Consumer Service URL

+ Add an ACS URL

The service provider endpoint that receives and processes SAML assertions.

Single Logout URL: Single Logout URL

Optional: The service provider endpoint that receives and processes SAML logout requests.

Service Provider Login URL: Service Provider Login URL

Optional: A URL provided by your service provider that will start a SAML authentication. Leave blank if unsure.

Default Relay State: Default Relay State

Optional: When set, all IdP-initiated requests include this relaystate. Configure if instructed by your service provider.

Click the copy icons on the right side of each textbox on the iTimekeep popup and then paste the value into the specified field in the SAML settings page for the Duo application. Set the following fields in the Service Provider section of the Duo page:

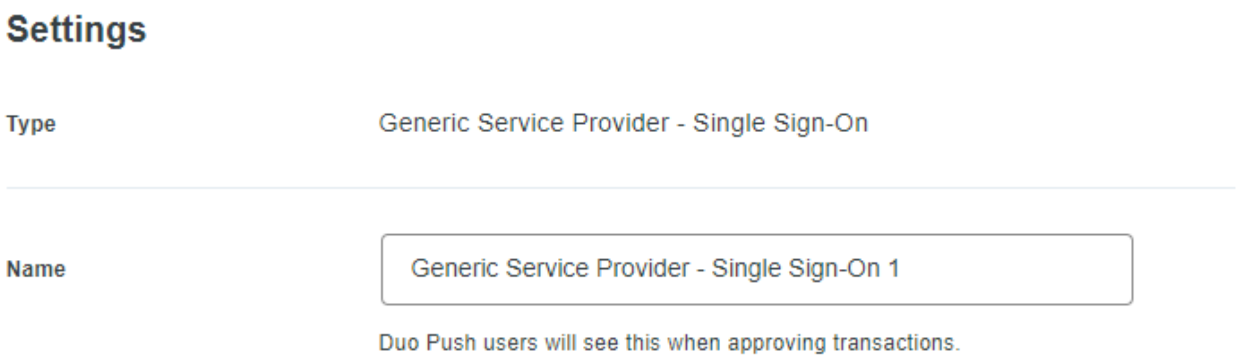
- Entity ID: paste the value from the Audience Restriction field on the iTimekeep popup
- Assertion Consumer Service (ACS) URL: paste the value from the Single Sign On URL field on the iTimekeep popup
- Single Logout URL: leave this field blank
- Service Provider Login URL: leave this field blank
- Default RelayState: leave this field blank

Set the following fields in the SAML Response section of the Duo page:

- Name ID format: select urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress from the dropdown
- NameId attribute: select <EmailAddress>
- Signature algorithm: select SHA256 from the dropdown
- Signing options:
  - Sign Response should be checked
  - Sign Assertion should be checked

- Map attributes:
  - IdP Attribute: click in the box, then select <EmailAddress>
  - SAML Response Attribute: email
- Create attributes: leave both boxes blank
- Role attributes: leave all boxes blank
- Universal Prompt: click the option for Show Traditional Prompt

Follow your firm's security standards for setting up the various settings in the Policy section on the Duo page, then scroll down to the Settings section on the Duo page.



Settings

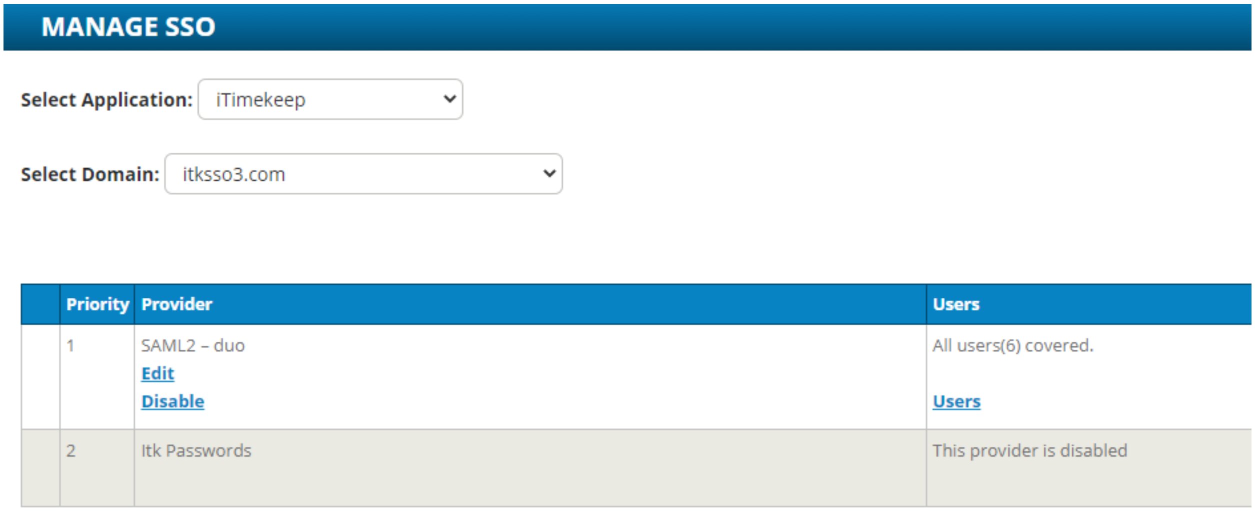
Type: Generic Service Provider - Single Sign-On

Name: Generic Service Provider - Single Sign-On 1

Duo Push users will see this when approving transactions.

Change the Name field to the name of the iTimekeep application that you are currently configuring (i.e. iTimekeep, Thrive or OCG Live).

Click the Save button the Duo page, then click the Save button on the iTimekeep popup. iTimekeep's Manage SSO page will now show the newly added SAML2 provider.



MANAGE SSO

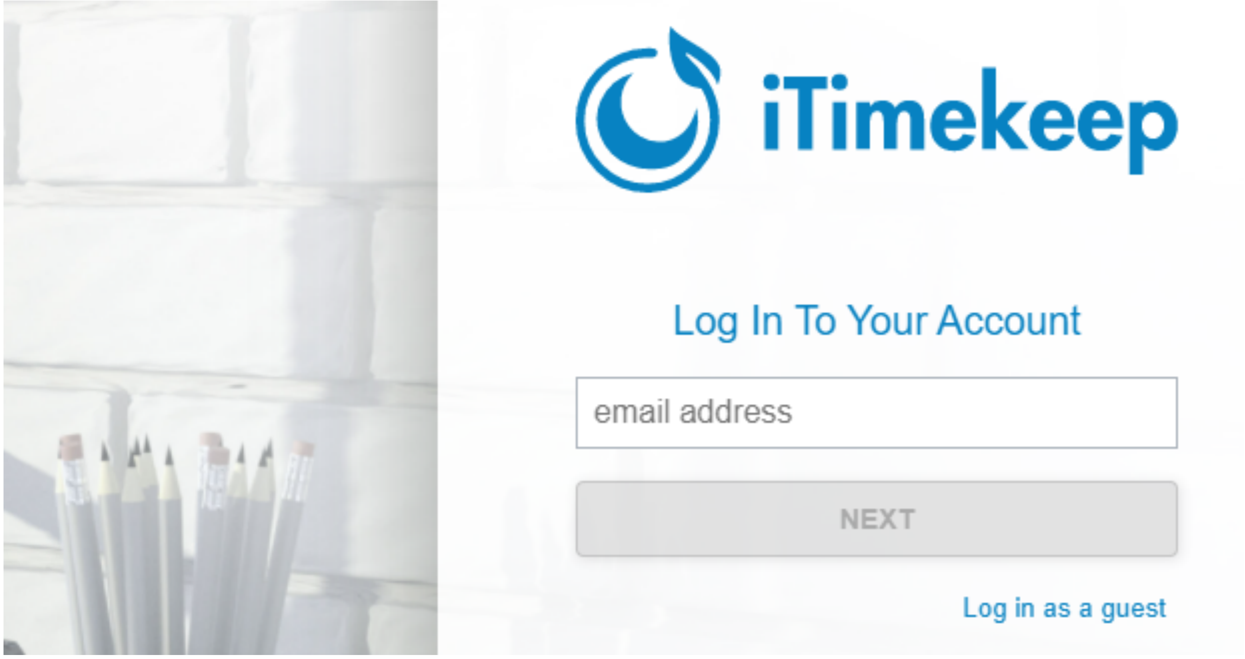
Select Application: iTimekeep

Select Domain: itksso3.com

	Priority	Provider	Users
	1	SAML2 – duo Edit Disable	All users(6) covered. Users
	2	Itk Passwords	This provider is disabled

SSO logins via Duo are now enabled for all iTimekeep users with email addresses matching the selected domain. If you plan to limit SSO logins for iTimekeep to a limited number of users initially, refer to the **Configuring SSO For Limited Users** section for specifying the users.

To test SP-initiated logins from iTimekeep Desktop, open iTimekeep Desktop in a browser window, enter your email address and click the NEXT button.



The browser should redirect to Duo's sign-in page. Enter your Duo password or respond to a Duo push or text. The browser should redirect back to iTimekeep's My Time page.

You should also test iTimekeep Mobile logins by opening the app on a phone and entering your email address as usual. The app should redirect to Duo's login page, which should redirect back to the My Time screen on the iTimekeep app.

If your firm plans to allow users to access iTimekeep from their Duo Central page, test those logins by logging into Duo from a browser. Click on iTimekeep's tile. The browser should redirect to the My Time page.

If Thrive and OCG Live should be available for IP-initiated logins from Duo Central, repeat the setup process for each application, but select Thrive or OCG Live as the application on the first step.

Skip to the **Advanced Topics** for additional optional configuration steps.

Configuring SSO Via SAML2 Using Other Identity Providers

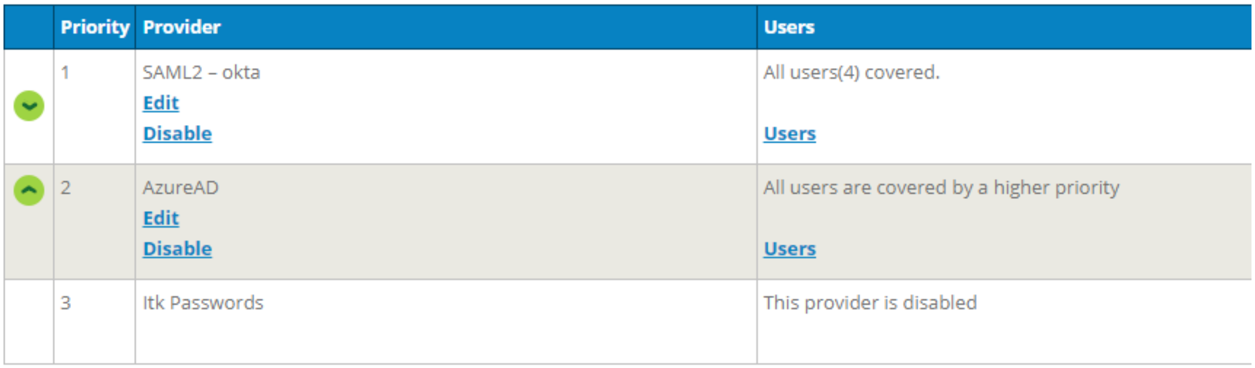
Aderant plans to add iTimekeep SSO support for additional SAML2 identity providers. If your SAML2 identity provider is not listed in one of the previous sections, please contact the iTimekeep Support team for assistance.

Advanced Topics

Some optional configuration steps may be needed based on your firm's environment and security requirements.

Configuring SSO For Multiple SSO Identity Providers For A Domain

iTimekeep supports multiple SSO providers for a single domain, a scenario that may be useful when migrating to a new SSO identity provider. To add a second SSO identity provider for a domain, simply follow the documentation in the previous sections for adding and configuring the appropriate SSO identity provider. Once the second SSO identity provider has been added, the Manage SSO page shows all of the SSO identity providers for the domain plus iTK Passwords, which is the default identity provider:



	Priority	Provider	Users
⌄	1	SAML2 – okta Edit Disable	All users(4) covered. Users
⌃	2	AzureAD Edit Disable	All users are covered by a higher priority Users
	3	Itk Passwords	This provider is disabled

When a domain user logs in to iTimekeep, iTimekeep will find the provider responsible for authenticating the user by starting at the top of the table for the provider with Priority=1, then working down the table checking each enabled provider for the first provider that will handle the user's email address or that has "all users covered" for the listed users. Refer to **Configuring SSO For Limited Users** for details on configuring the users that will be authenticated by each provider.

Use the up and down arrow icons to change a provider's priority.

Configuring SSO For Multiple Domains

iTimekeep supports configuring identity providers for multiple domains. For example, international users may have email addresses on an international domain or an acquired firm may have users on a different domain. Each of the domains can be configured as follows:

Example 1

For this example, assume that the firm has two domains: firm1.com and firm2.com. For firm1.com users, authentication will be handled by an SSO identity provider. For firm2.com users, authentication will be handled by iTK passwords.

To configure authentication for this scenario, follow the SSO configuration for firm1.com for the appropriate identity provider using the instructions on the following pages. No configuration will be needed for firm2.com users since iTK passwords is the default identity provider. iTimekeep will automatically route authentication requests to the appropriate identity provider based on users' email addresses.

Example 2

For this example, assume that the firm has the same two domains: firm1.com and firm2.com. However, for this example, authentication for firm1.com users will be handled by an SSO identity provider. Authentication for firm2.com users will also be handled by an SSO identity provider.

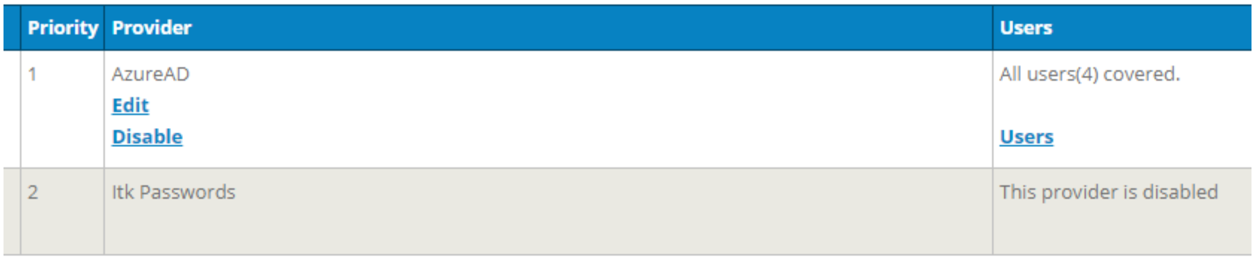
To configure authentication for this scenario, follow the SSO configuration for firm1.com for the appropriate identity provider using the instructions for the following pages, then repeat the process for configuring SSO for firm2.com for the corresponding identity provider. Note that you will need to configure SSO for both domains even if they use the same SSO provider. Once both domains have been configured, iTimekeep will automatically route authentication requests to the appropriate identity provider based on users' email addresses.

Configuring SSO For Limited Users

iTimekeep supports configuring SSO for a limited set of users, for example to limit SSO logins to a limited number of test users during the initial testing phase for iTimekeep SSO or while converting to a new SSO identity provider.

Scenario 1: Enabling user routing with a single SSO provider

This scenario will typically be used during the initial testing phase for iTimekeep SSO. Once the SSO provider has been configured as detailed in the previous sections, the Manage SSO will look similar to the following:

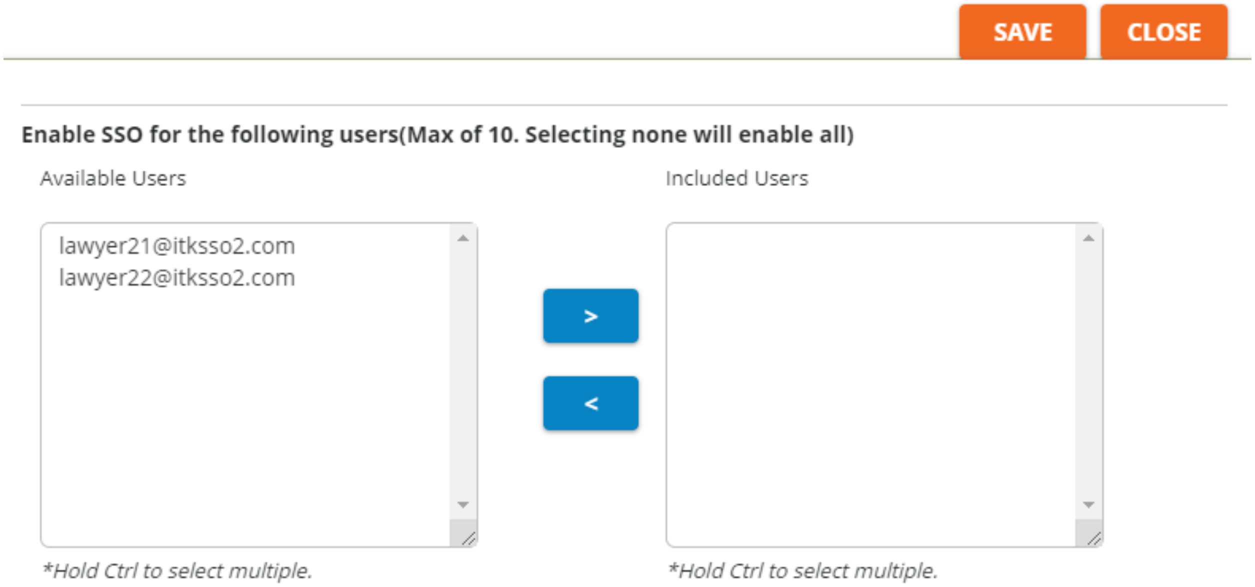


Priority	Provider	Users
1	AzureAD Edit Disable	All users(4) covered. Users
2	Itk Passwords	This provider is disabled

Once the initial SSO configuration has been completed, iTimekeep will route all logins to the Azure AD identity provider. To enable user routing, click the Users link in the AzureAD section. A popup will appear for mapping specific users to that SSO identity provider. Initially, all iTimekeep users' email addresses matching the currently selected domain will appear in the left column.

- To enable SSO logins for a specific user, click an email address in the left column then click the right arrow. Select multiple email addresses by holding the Ctrl key while clicking on each email address.
- To disable SSO logins for a specific user, click an email address in the right column then click the left arrow. Select multiple email addresses by holding the Ctrl key while clicking on each email address.
- As long as one user is listed in the right column, user routing is enabled for the SSO identity provider. To disable user routing so that all users will use the SSO identity provider, select all users in the right column and click the left arrow.

For example, with the following configuration, user routing is disabled, so all users will use the SSO identity provider:



Enable SSO for the following users(Max of 10. Selecting none will enable all)

Available Users

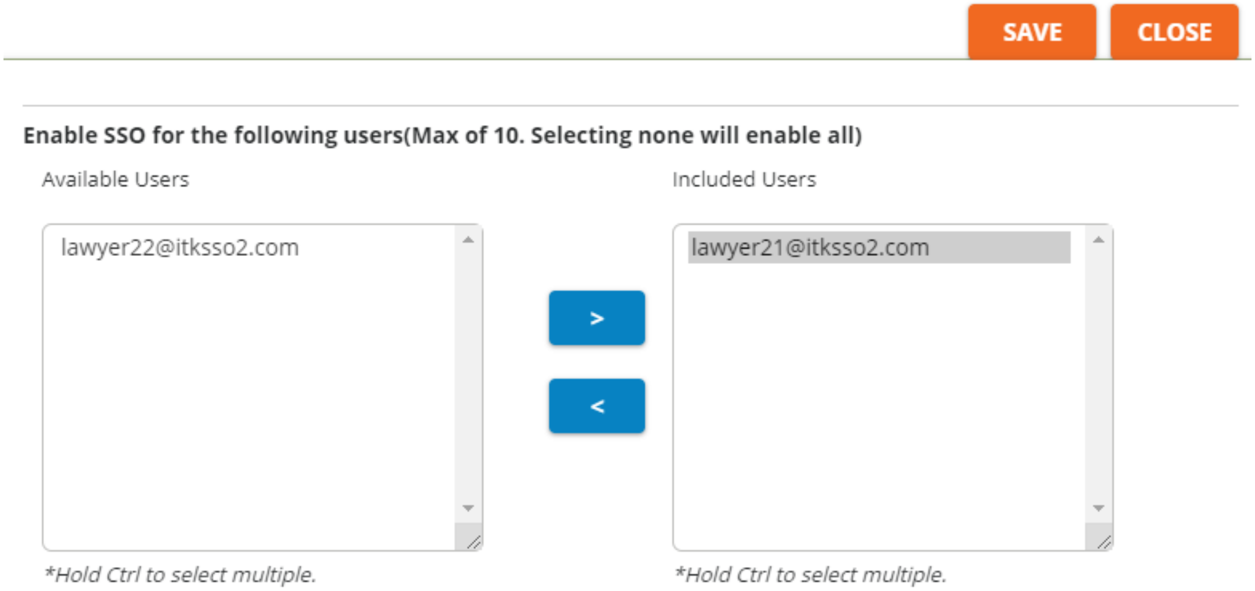
lawyer21@itksso2.com
lawyer22@itksso2.com

*Hold Ctrl to select multiple.

Included Users

*Hold Ctrl to select multiple.

With the following configuration, user routing to the SSO provider is enabled only for user lawyer21@itksso2.com. All other users will be routed to the next provider (see below for details).



Enable SSO for the following users(Max of 10. Selecting none will enable all)

Available Users

lawyer22@itksso2.com

*Hold Ctrl to select multiple.

Included Users

lawyer21@itksso2.com

*Hold Ctrl to select multiple.

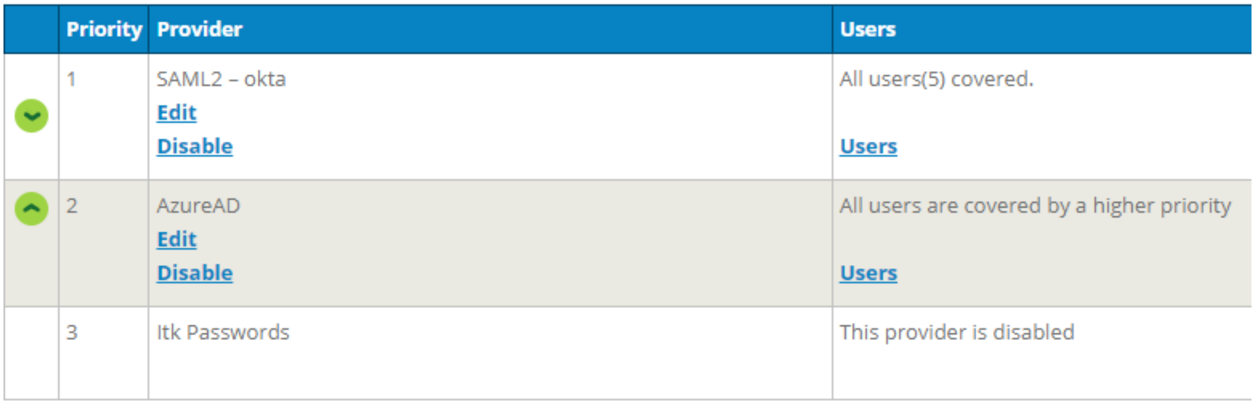
Scenario 2: Enabling user routing with multiple SSO providers

This scenario will typically be used while converting to a new SSO identity provider. Assume that Okta and Azure AD have been configured using the instructions in the previous sections. The Manage SSO lists each of SSO providers. iTimekeep will route users to find the **first** provider mapped to the user as follows:

1. Starting with the provider with Priority=1, find the first provider that is enabled.

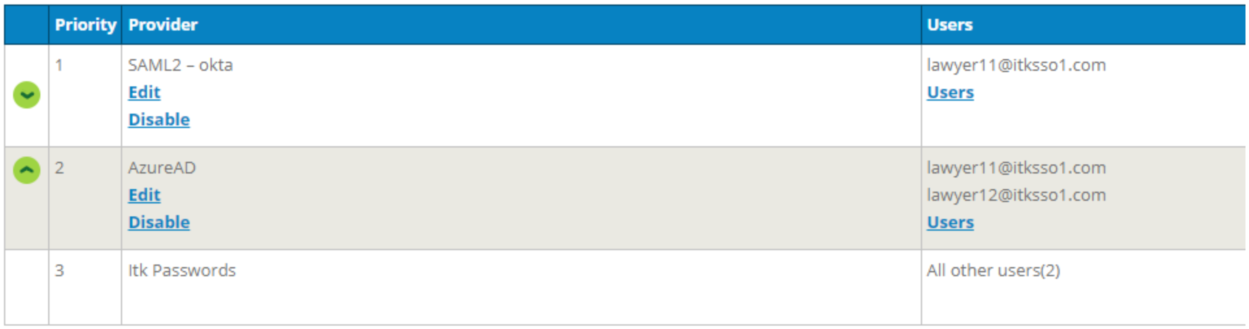
2. If the provider has ANY users listed and the email address entered on the login screen matches one of the providers’ users, use this provider for authenticating the login.
3. If the provider has “All users covered” or “All other users”, use this provider for authenticating the login.
4. Otherwise repeat the process for the next provider in the table.

The following table shows the initial user mapping after both SSO providers have been configured. The SAML2 Okta provider will be selected for authenticating all logins.



	Priority	Provider	Users
▼	1	SAML2 – okta Edit Disable	All users(5) covered. Users
▲	2	AzureAD Edit Disable	All users are covered by a higher priority Users
	3	Itk Passwords	This provider is disabled

Configure user routing for the SSO providers by following the instructions in the previous scenario. Note that user routing can be configured for each provider in the table except for ITK Passwords (that is the default provider). Here is the providers table after configuring user routing (details omitted).



	Priority	Provider	Users
▼	1	SAML2 – okta Edit Disable	lawyer11@itksso1.com Users
▲	2	AzureAD Edit Disable	lawyer11@itksso1.com lawyer12@itksso1.com Users
	3	Itk Passwords	All other users(2)

Here are some examples that show which provider will handle login authentication:

User	Provider
lawyer11@itksso1.com	SAML2 – okta • The SAML2 – okta provider is enabled, has users defined, and has an exact match for the email address. No other providers will be checked.
lawyer12@itksso1.com	AzureAD • The SAML2 – okta provider is enabled, has users defined, but does not have an exact match for the email address. • The AzureAD provider is enabled, has users defined, and has an exact match for the email address. No other providers will be checked.

lawyer13@itksso1.com	ITK Passwords • The SAML2 – okta provider is enabled, has users defined, but does not have an exact match for the email address. • The AzureAD provider is enabled, has users defined, but does not have an exact match for the email address. • The ITK Passwords provider is enabled and has "All other users", so this provider will be selected.

Special considerations for iTimekeep's Outlook Plug-In and SSO

iTimekeep's Outlook Plug-In does not currently support logging in via an SSO identity provider. Therefore, users must use their iTimekeep password when logging in for iTimekeep's Outlook Plug-In:

- For users who were already defined to iTimekeep prior to enabling SSO, those users will continue to use their current iTimekeep password.
- For users who are added to iTimekeep after enabling SSO, those users will need to click on the Forgot Password link on the login page. iTimekeep will send an email instructions and a link for setting the initial login password.

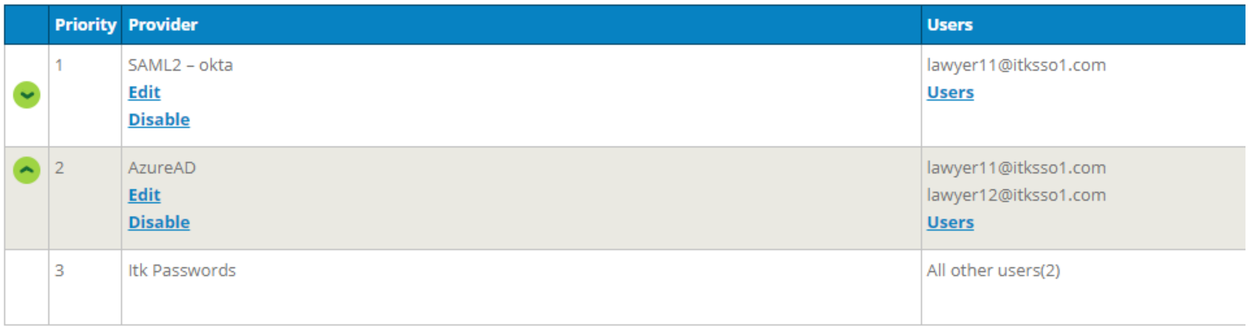
Creating an emergency "backdoor" username for logging in without SSO

Once SSO logins have been enabled for a domain, all iTimekeep users with email addresses matching that domain will be handled by the SSO identity provider. Creating an iTimekeep subscription administrator account will enable the administrator to change SSO settings or even disable SSO if there are any SSO issues. This subscription administrator account must be created with an email address that does not match the domain that was configured for SSO logins (e.g. a personal email address).

For example, if the SSO configuration is for example.com, create an account such as me@mypersonalsite.com. That account will require an iTimekeep password during login.

Disabling An SSO Provider

iTimekeep supports disabling an SSO provider (e.g. when there is a problem with that provider). The Manage SSO page lists all of the SSO providers, and possibly their user mappings, that were configured with the previous instructions. Clicking the Disable link for a particular provider will disable that provider as well as its associated user mappings.



	Priority	Provider	Users
▼	1	SAML2 – okta Edit Disable	lawyer11@itksso1.com Users
▲	2	AzureAD Edit Disable	lawyer11@itksso1.com lawyer12@itksso1.com Users
	3	Itk Passwords	All other users(2)

1. Initially, the SAML2 – okta provider handles logins for lawyer11@itksso1.com. AzureAD handles logins for lawyer12@itksso1.com. All other users will login with ITK passwords.

2. Clicking the Disable link for SAML2 – okta disables that provider. Logins for lawyer11@itksso1.com will now be handled by the AzureAD provider, which will continue to handle logins for lawyer12@itksso1.com.
3. Clicking the Disable link for both the SAML2 – okta and the Azure AD providers will completely disable SSO logins, so all users will now use ITK Passwords. It is important to note that iTimekeep might not have passwords for all users in this scenario (e.g. users that were added while SSO was active). In this case, the users must click the Forgot Password on the iTimekeep login page to set their initial password.