



How to Set up Single Sign On with Okta

Set up single sign-on for your Dozuki site using Okta.

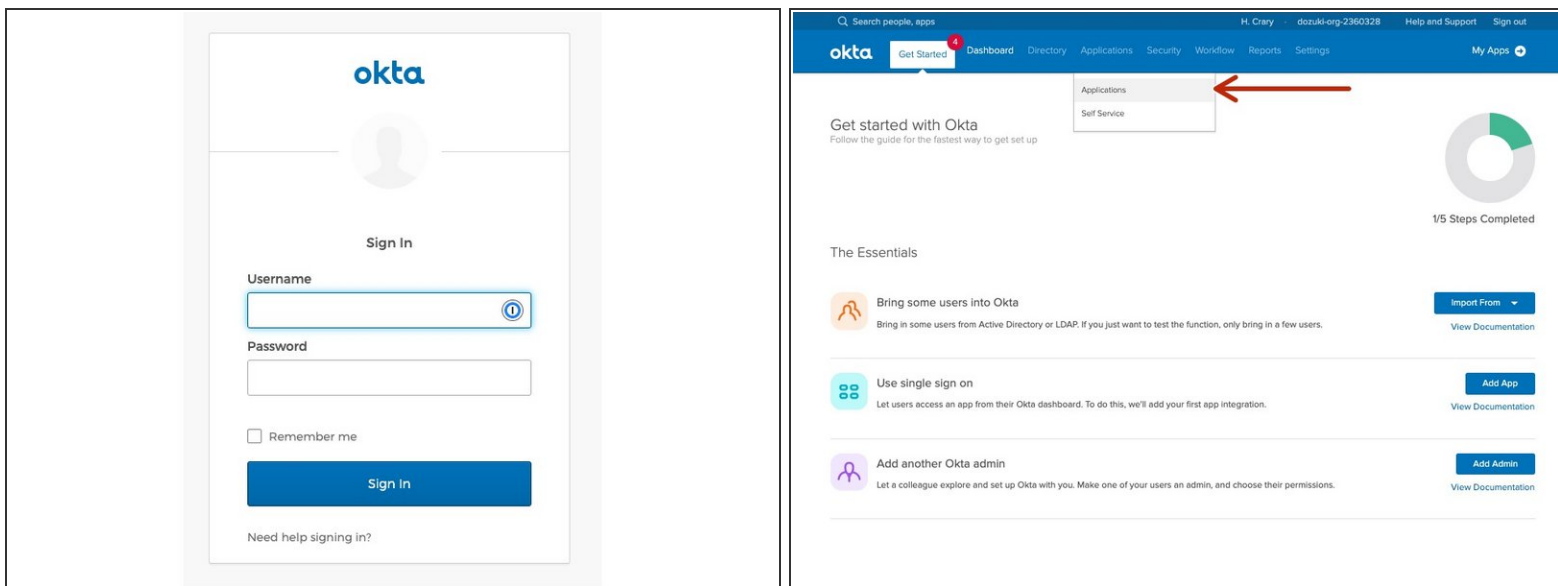
Written By: Dozuki System



INTRODUCTION

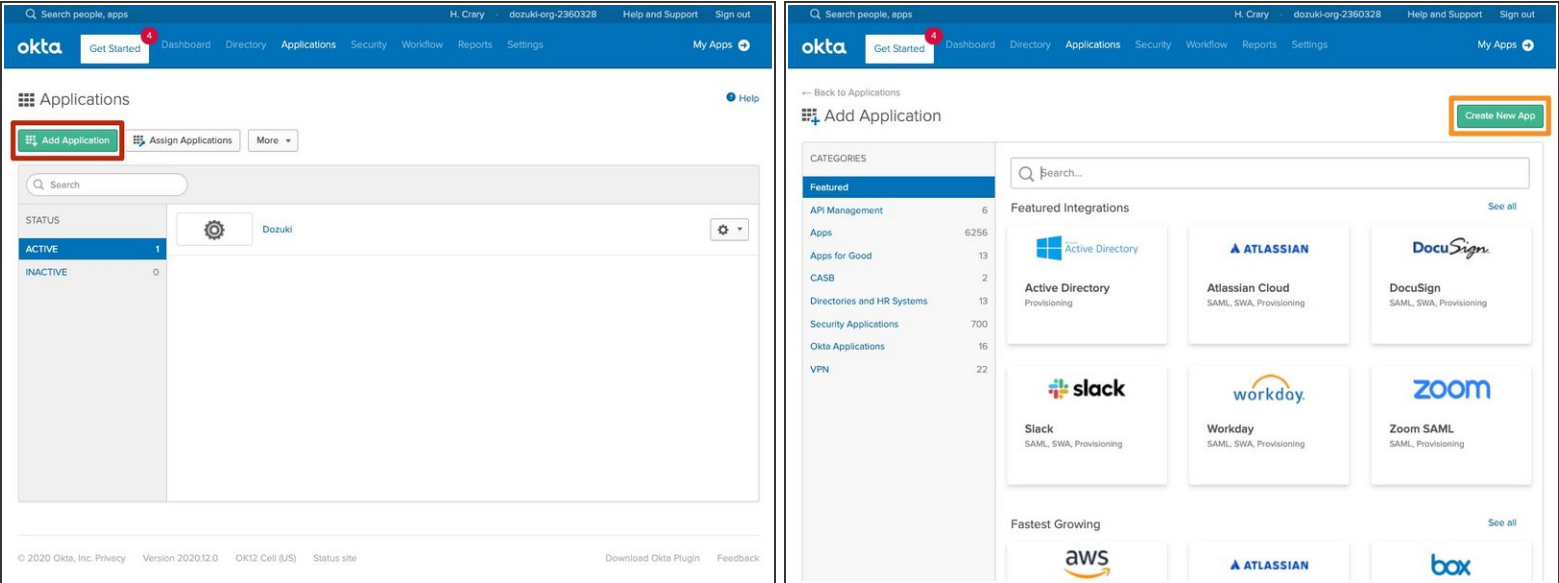
Dozuki sites support single sign-on (SSO) through the SAML 2.0 protocol. Use this guide to set up a SAML2 connection with Okta.

Step 1 — Log in to Okta



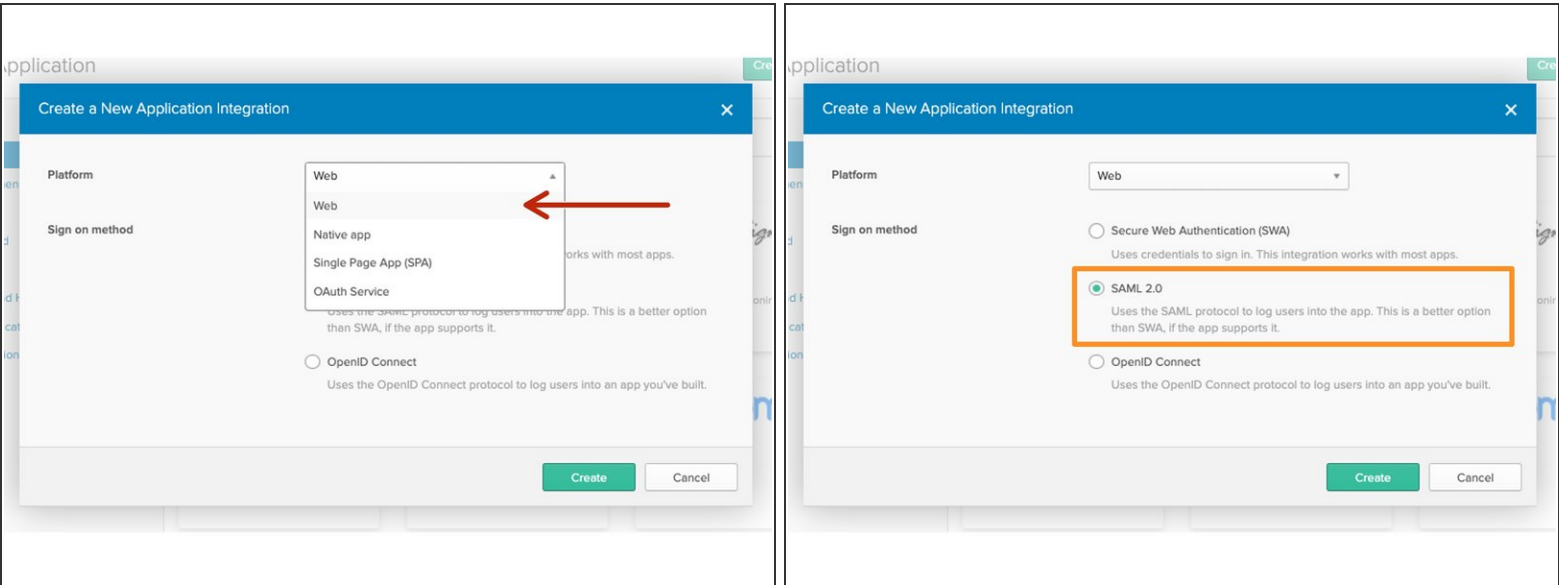
- Log in to the Okta admin dashboard for your organization.
 - ❗ For most companies, the login page will be <https://login.okta.com/>.
- Click on **Applications** in the **Applications** list.

Step 2



- Click on **Add Application**.
- Click on **Create New App**.

Step 3



- Select **Web** from the **Platform** options.
- Select **SAML 2.0** as the **Sign on method**.

Step 4

Create SAML Integration

1 General Settings 2 Configure SAML 3 Feedback

1 General Settings

App name

App logo (optional) ⓘ

Upload Logo

Requirements

- Must be PNG, JPG or GIF
- Less than 1MB

For Best Results, use a PNG image with

- Minimum 420px by 120px to prevent upscaling
- Landscape orientation
- Transparent background

App visibility

- ☐ Do not display application icon to users
- ☐ Do not display application icon in the Okta Mobile app

Cancel Next

- Type a display name for your Dozuki site into the **App name** field.
- ⓘ For customers with a single Dozuki site, we recommend using **Dozuki** as the display name.
- Click the **Next** button at the bottom of the window.

Step 5

Configuration

General

Appearance

Security

Translation Glossary

Users

Organization

Content Review

Document Control

Timeline

Support

Reports

Services

General

Plan	factory	
Title	Heather	Edit
Description	<your site description will go here>	Edit
Home page	Guide	Edit
Custom domain	Not using a custom domain	Edit
Alternate domain aliases	No Value Set	Edit
E-commerce link	No Value Set	Edit
Google Analytics key	No Value Set	Edit
Mobile apps	Your site is not listed in the Dozuki mobile apps.	Edit
Persistent API Token	8IfjgplYH0r aPZ48N0ir 9e9cTe1S23bZs	Edit
Footer site statistics	Your site's view statistics will be displayed in the site footer.	Edit

Guides

Default guide conclusion	Caterpillar: Confidential Green	Edit
Automatic guide titles	Automatic generation of guide titles is disabled	Edit

Authentication

Single sign on

Single sign on: disabled. Login and account creation on this site happens normally.

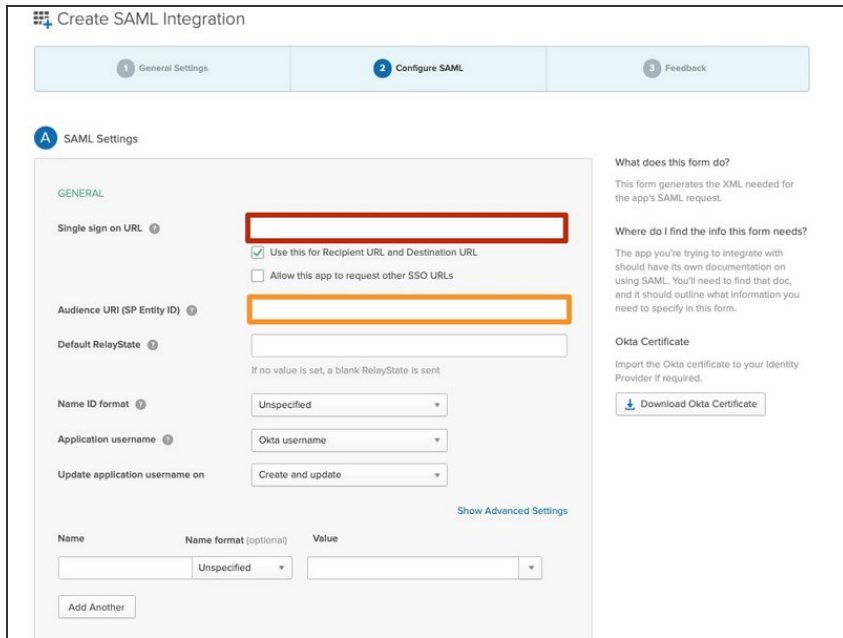
Edit

Dozuki SSO: URL	No Value Set	Edit
Dozuki SSO: Logout URL	No Value Set	Edit
Dozuki SSO: Secret	No Value Set	Edit
SAML 2.0: Identity Provider Entity ID	No Value Set	Edit
SAML: Identity provider URL	No Value Set	Edit
SAML Metadata	Download Metadata	
SAML: Logout URL	No Value Set	Edit
SAML: Identity Provider X.509 Certificate	No Value Set	Edit
Google Login	Google login is disabled	Edit

ABOUT HELP API

- Open the management console of your Dozuki site in another browser window.
- From the **Configuration** section in the sidebar menu, select **Security**.
- Download the SAML `metadata.xml` file.
- 📁 Open this file with text editor.

Step 6



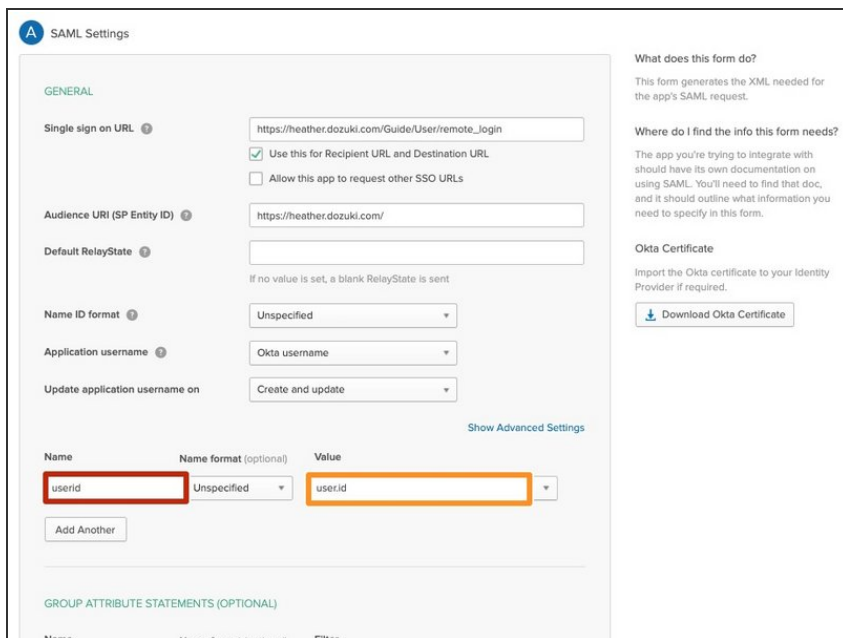
- Under **Single sign on URL**, enter the URL of the page on your Dozuki site that you want your users to reach once signing in.

- Enter the **SP Entity ID**.

i Refer to the values in the SAML `metadata.xml` file.

i Leave **Advance Setting** at default.

Step 7 — Set User Attributes and Claims



- Enter userid into the **Name** field.

- Enter user.id into the **Value** field.

i If your company uses additional unique identifiers for your users, you can use those attributes instead of user.id.

Step 8

SAML Settings

GENERAL

Single sign on URL ⓘ

☒ Use this for Recipient URL and Destination URL
☐ Allow this app to request other SSO URLs

Audience URI (SP Entity ID) ⓘ

Default RelayState ⓘ

The app you're trying to integrate with should have its own documentation on using SAML. You'll need to find that doc, and it should outline what information you need to specify in this form.

Okta Certificate
Import the Okta certificate to your Identity Provider if required.
[Download Okta Certificate](#)

Name ID format ⓘ

Application username ⓘ

Update application username on

Show Advanced Settings

Name	Name format (optional)	Value
userid	<input type="text" value="Unspecified"/>	<input type="text" value="user.id"/>
Add Another		

GROUP ATTRIBUTE STATEMENTS (OPTIONAL)

Name	Name format (optional)	Filter
------	------------------------	--------

SAML Settings

GENERAL

Single sign on URL ⓘ

☒ Use this for Recipient URL and Destination URL
☐ Allow this app to request other SSO URLs

Audience URI (SP Entity ID) ⓘ

Default RelayState ⓘ

The app you're trying to integrate with should have its own documentation on using SAML. You'll need to find that doc, and it should outline what information you need to specify in this form.

Okta Certificate
Import the Okta certificate to your Identity Provider if required.
[Download Okta Certificate](#)

Name ID format ⓘ

Application username ⓘ

Update application username on

Show Advanced Settings

Name	Name format (optional)	Value
userid	<input type="text" value="Unspecified"/>	<input type="text" value="user.id"/>
username	<input type="text" value="Unspecified"/>	<input type="text" value="user.displayName"/>
Add Another		

GROUP ATTRIBUTE STATEMENTS (OPTIONAL)

Name	Name format (optional)	Filter
------	------------------------	--------

- Click on **Add Another**.
- Enter username into the **Name** field.
- Enter user.displayName into the **Value** field.

Step 9

SAML Settings

GENERAL

Single sign on URL ⓘ

☒ Use this for Recipient URL and Destination URL
☐ Allow this app to request other SSO URLs

Audience URI (SP Entity ID) ⓘ

Default RelayState ⓘ

If no value is set, a blank RelayState is sent

Name ID format ⓘ

Unspecified ▼

Application username ⓘ

Okta username ▼

Update application username on

Create and update ▼

Show Advanced Settings

Name	Name format (optional)	Value
userid	Unspecified ▼	user.id ▼
username	Unspecified ▼	user.displayName ▼ ×
Add Another		

GROUP ATTRIBUTE STATEMENTS (OPTIONAL)

What does this form do?

This form generates the XML needed for the app's SAML request.

Where do I find the info this form needs?

The app you're trying to integrate with should have its own documentation on using SAML. You'll need to find that doc, and it should outline what information you need to specify in this form.

Okta Certificate

Import the Okta certificate to your Identity Provider if required.

Download Okta Certificate

SAML Settings

GENERAL

Single sign on URL ⓘ

☒ Use this for Recipient URL and Destination URL
☐ Allow this app to request other SSO URLs

Audience URI (SP Entity ID) ⓘ

Default RelayState ⓘ

If no value is set, a blank RelayState is sent

Name ID format ⓘ

Unspecified ▼

Application username ⓘ

Okta username ▼

Update application username on

Create and update ▼

Show Advanced Settings

Name	Name format (optional)	Value
userid	Unspecified ▼	user.id ▼
username	Unspecified ▼	user.displayName ▼ ×
email	Unspecified ▼	user.email ▼ ×
Add Another		

What does this form do?

This form generates the XML needed for the app's SAML request.

Where do I find the info this form needs?

The app you're trying to integrate with should have its own documentation on using SAML. You'll need to find that doc, and it should outline what information you need to specify in this form.

Okta Certificate

Import the Okta certificate to your Identity Provider if required.

Download Okta Certificate

- Click on **Add Another**.
- Enter email into the **Name** field.
- Enter user.email into the **Value** field.

Step 10 — Verify Advanced Settings

SAML Settings

GENERAL

Single sign on URL

☒ Use this for Recipient URL and Destination URL.

☐ Allow this app to request other SSO URLs

Audience URI (SP Entry ID)

Default RelayState

If no value is set, a blank RelayState is sent.

Name ID format

Application username

Update application username on

[Show Advanced Settings](#)

What does this form do?

This form generates the XML needed for the app's SAML request.

Where do I find the info this form needs?

The app you're trying to integrate with should have its own documentation on using SAML. You'll need to find that doc, and it should outline what information you need to specify in this form.

Okta Certificate

Import the Okta certificate to your Identity Provider if required.

[Download Okta Certificate](#)

Advanced Settings

Name ID format

Application username

Update application username on

[Hide Advanced Settings](#)

Response

Assertion Signature

Signature Algorithm

Digest Algorithm

Assertion Encryption

Enable Single Logout ☐ ☐ Allow application to initiate Single Logout

Assertion Inline Hook

Authentication context class

Honor Force Authentication

SAML Issuer ID

Name **Name format (optional)** **Value**

userid	Unspecified	userid
username	Unspecified	user.displayName
email	Unspecified	user.email

[Add Another](#)

- Verify the **Response** is signed.

- While Dozuki will accept the either the entire Reponse or the Assertion Signature, signing the Response provides an additional level of protection for the Response message while being sent over the network.

- Verify **Assertion Encryption** is **Unencrypted**.

- Dozuki does not currently support encrypted assertions.

- Verify **Single Logout** (SLO) is **unchecked**.

- Dozuki does not currently provide a public certification that Okta requires to support SLO.

- Verify **Honor Force Authentication** is set to **Yes**.

- In order to support SSO signoffs, Dozuki requires the re-entry of credentials for sign-offs. **If set to No**, when a user clicks the sign-off button, the sign-off would be completed without requiring the user to re-enter their credentials.

Step 11 — SAML Signing Certificate

A

SAML Settings

GENERAL

Single sign on URL ⓘ

☒ Use this for Recipient URL and Destination URL
☐ Allow this app to request other SSO URLs

Audience URI (SP Entity ID) ⓘ

Default RelayState ⓘ

If no value is set, a blank RelayState is sent

Name ID format ⓘ

Unspecified ▼

Application username ⓘ

Oka username ▼

Update application username on

Create and update ▼

Show Advanced Settings

Name	Name format (optional)	Value
userid	Unspecified ▼	user.id ▼
username	Unspecified ▼	user.displayName ▼ ×
email	Unspecified ▼	user.email ▼ ×
Add Another		

What does this form do?

This form generates the XML needed for the app's SAML request.

Where do I find the info this form needs?

The app you're trying to integrate with should have its own documentation on using SAML. You'll need to find that doc, and it should outline what information you need to specify in this form.

Okta Certificate

Import the Okta certificate to your Identity Provider if required.

Download Okta Certificate

B

Preview the SAML assertion generated from the information above


<> Preview the SAML Assertion

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

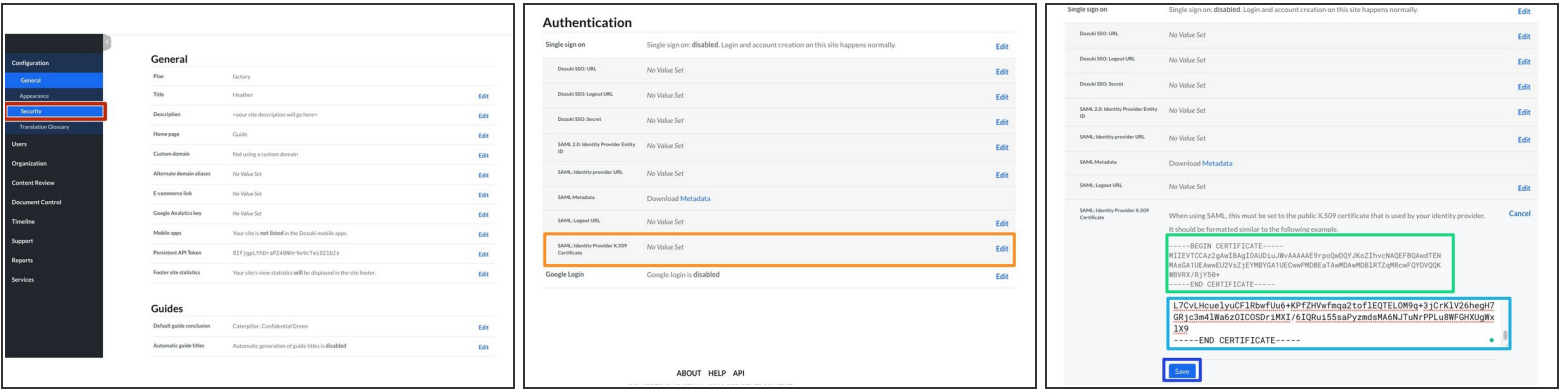
Previous

Cancel

Next

- In the **SAML Settings** setup section, click the **Download Okta Certificate**.
- Save the certificate file when prompted.
-  Open the certificate in a text editor.
- Scroll down and click the **Next** button to save your changes and continue with the setup.

Step 12



- Open the management console of your Dozuki site in another browser window.
- From the **Configuration** section in the sidebar menu, select **Security**.
- Under the **Authentication** heading section of the Security page, click on **SAML: Identity Provider X.509 Certificate**.
- Copy the body of certificate from your text editor.
 - The certificate should be formatted similar to the example shown under the **Authentication** section.
- Paste the certificate into the text field.
- Click the **Save** button to save your changes.

Step 13 — Add Okta Login URL

Authentication

Single sign on

Dozuki SSO URL	No Value Set	Edit
Dozuki SSO Logout URL	No Value Set	Edit
Dozuki SSO Secret	No Value Set	Edit
SAML 2.0 Identity Provider Entity ID	No Value Set	Edit
SAML Identity provider URL	No Value Set	Edit
SAML Metadata	Download Metadata	
SAML Logout URL	No Value Set	Edit
SAML Identity Provider X.509 Certificate	Valid certificate	Edit
Google Login	Google login is disabled	Edit

Applications

16pg

Add Application Assign Applications More

Search

STATUS		
ACTIVE	1	
INACTIVE	0	

Details

Dozuki

Back to Applications

Active View Logs

General Sign On Import Assignments

Settings

Edit

Sign On METHODS

The sign-on method determines how a user signs in and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.

Application username is determined by the user profile mapping. [Configure profile mapping](#)

SAML 2.0

Default Relay State

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

[View Setup Instructions](#)

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

About

SAML 2.0 establishes the end user experience by not requiring the user to know their credentials. Users cannot enter their credentials when SAML 2.0 is configured for this application. Additional configurations in the 3rd party application may be required to complete the integration with Okta.

Application Username

Choose a format to use as the default username value when assigning the application to users.

If you select Name you will be prompted to enter the username manually when assigning an application with password or profile push provisioning features.

- Click on the **SAML: Identity provider URL** heading under **Authentication**.
- Under the **Application** section in the Okta portal, click on the app icon for Dozuki.
- Select the **Sign On** Tab.
- Click on the **View Setup Instructions** button.

Step 14

[illegible]

- Paste the **Identity Provider Issuer** into the **SAML 2.0: Identity Provider ID** text field in your Dozuki site.
- Click the **Save** button to save your changes.

Step 15 — Test and Add Okta Connection

Authentication

Single sign on

Single sign on: disabled. Login and account creation on this site happens normally.

Edit

Dozuki SSO URL

No Value Set

Edit

Dozuki SSO Logout URL

No Value Set

Edit

Dozuki SSO Secret

No Value Set

Edit

SAML 2.0 Identity Provider Entity ID

http://www.okta.com/ok2c5oIICxp679FW5d6

Edit

SAML Identity provider URL

No Value Set

Edit

SAML Metadata

Download Metadata

SAML Logout URL

No Value Set

Edit

SAML Identity Provider X.509 Certificate

Valid certificate

Edit

Google Login

Google login is disabled

Edit

Authentication

Single sign on

Single sign on: disabled. Login and account creation on this site happens normally.

Edit

Dozuki SSO URL

No Value Set

Edit

Dozuki SSO Logout URL

No Value Set

Edit

Dozuki SSO Secret

No Value Set

Edit

SAML 2.0 Identity Provider Entity ID

http://www.okta.com/ok2c5oIICxp679FW5d6

Edit

SAML Identity provider URL

When using SAML, users will be redirected to this URL when attempting to login.

Cancel

Save

Test a SAML identity provider URL

After setting up SAML, test your implementation by pasting your identity provider URL here:

https://dozukiidzoku11.okta.com/app/idozukiido

Test SAML 1.1

Test SAML 2.0

SAML Metadata

Download Metadata

SAML Logout URL

No Value Set

Edit

Authentication

Single sign on

Single sign on: disabled. Login and account creation on this site happens normally.

Edit

Dozuki SSO URL

No Value Set

Edit

Dozuki SSO Logout URL

No Value Set

Edit

Dozuki SSO Secret

No Value Set

Edit

SAML 2.0 Identity Provider Entity ID

http://www.okta.com/ok2c5oIICxp679FW5d6

Edit

SAML Identity provider URL

When using SAML, users will be redirected to this URL when attempting to login.

Cancel

Save

Test a SAML identity provider URL

After setting up SAML, test your implementation by pasting your identity provider URL here:

https://dozukiidzoku11.okta.com/app/idozukiido

Test SAML 1.1

Test SAML 2.0

SAML Metadata

Download Metadata

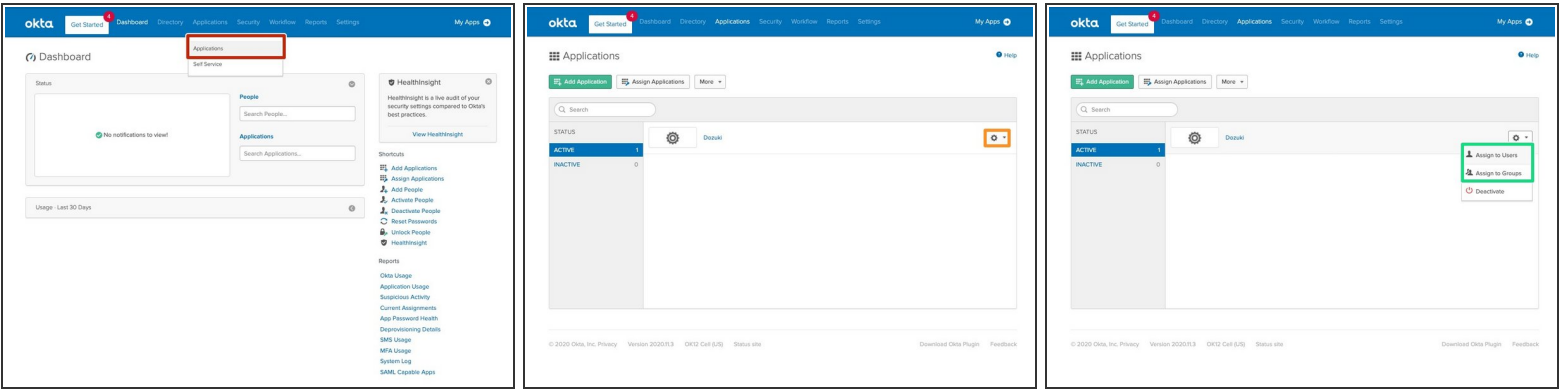
SAML Logout URL

No Value Set

Edit

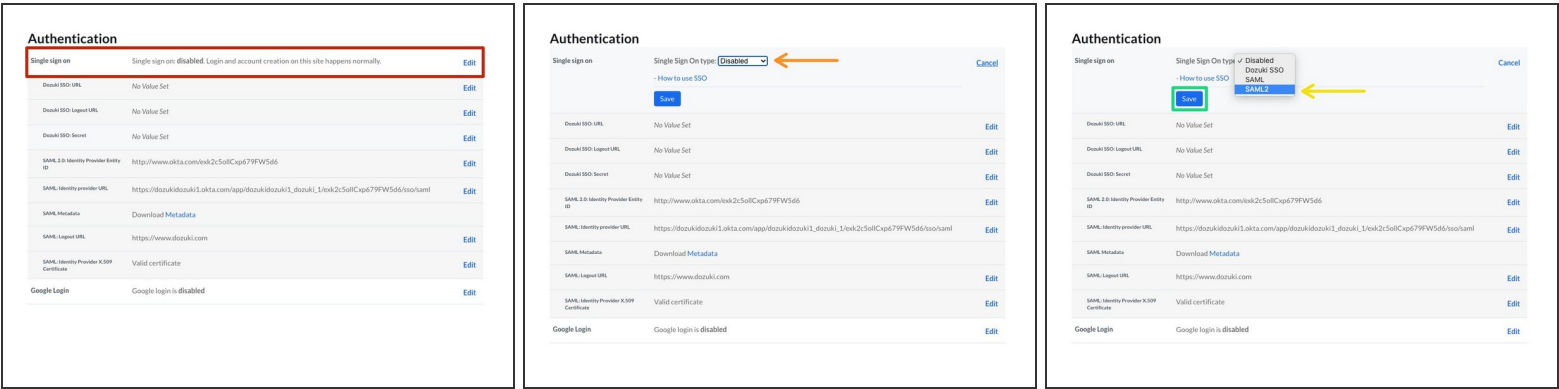
- Click on the **SAML: Identity provider URL** heading under **Authentication**.
- From the **Set up Instructions** in the Okta portal, Copy the **Identity Provider Single Sign-On URL**.
- Paste the **Identity Provider Single Sign-On URL** into the **Test a SAML identity provider URL** text field in your Dozuki site to test the SSO connection.
- ⓘ We recommend testing the SAML connection through your Dozuki site before enabling SAML 2.0 as the authentication mechanism. Testing the connection from within Dozuki will prevent disruption to your active site and current users.
- Once the connection test succeeds, paste the **Identity Provider Single Sign-On URL** into the **SAML: Identity provider URL** field.
- Click the **Save** button to save your changes.

Step 16 — Assign a User or Group



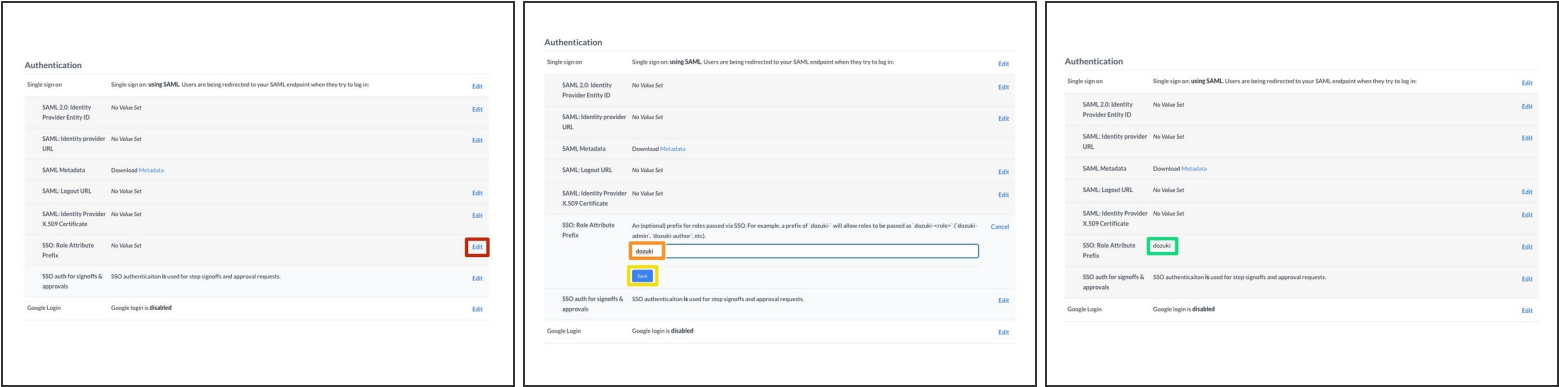
- In the Okta portal, Click on the **Application** section from the header.
- Click the Dropdown button next to your application.
- Select **Assign to Users** or **Assign to Groups** to add users and groups.
- ① You can read more about [assigning users](#) and [assigning groups](#) in Okta.

Step 17 — Enable Single Sign On



- Click on the **Single sign on** heading under **Authentication**.
- Click on the **Single Sign On type** dropdown menu.
- Select **SAML 2** from the dropdown menu.
- Click the **Save** button to save your changes.

Step 18 — SSO: Role Attribute Prefix



- ❗ Once SSO is enabled on your Dozuki site, you have the option to add a role attribute prefix. This helps when syncing to third-party IdPs and will allow roles to be passed as `dozuki-<role>` (`dozuki-admin`, `dozuki-author`, etc.)
- ❗ *Dozuki defined roles (admin, author, user, etc.) **cannot** be customized.*
- Click **Edit**.
 - Add your desired role attribute prefix.
 - Click **Save**.
 - Your role attribute prefix will be displayed.

Step 19 — SSO Authentication for Signoffs & Approvals

Authentication

Single sign on

Single sign on: using SAML. Users are being redirected to your SAML endpoint when they try to log in:
https://dozukidozuki1.okta.com/app/dozukidozuki1_dozuki_1/exk2c5ollCxp679FW5d6/sso/saml

Edit

Dozuki SSO URL	No Value Set	Edit
Dozuki SSO Logout URL	No Value Set	Edit
Dozuki SSO Secret	No Value Set	Edit
SAML 2.0 Identity Provider Entity ID	http://www.okta.com/exk2c5ollCxp679FW5d6	Edit
SAML Identity provider URL	https://dozukidozuki1.okta.com/app/dozukidozuki1_dozuki_1/exk2c5ollCxp679FW5d6/sso/saml	Edit
SAML Metadata	Download Metadata	
SAML Logout URL	https://dozukidozuki1.okta.com/app/dozukidozuki1_dozuki_1/exk2c5ollCxp679FW5d6/sso/saml	Edit
SAML Identity Provider X.509 Certificate	Valid certificate	Edit

SSO auth for signoffs & approvals

Enables users to authenticate step signoffs and approval requests with SSO instead of using Dozuki passwords.

Cancel

☒ Use SSO authentication for step signoffs and approval requests.

Save

- Once Single Sign On is enabled, **SSO auth for signoffs & approvals** will appear in the Authentication section of the Security settings.
- ⓘ This feature allows users to enter their SSO authentication for Signoffs and Approvals instead of a separate Dozuki password.
- SSO auth for signoffs & approvals is enabled by default when you enable SSO authentication.
- ⓘ Only disable SSO authentication for signoffs & approvals if you want your users to enter a **separate Dozuki password** for signoffs and approvals.