



How to Set up Single Sign on with Onelogin

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

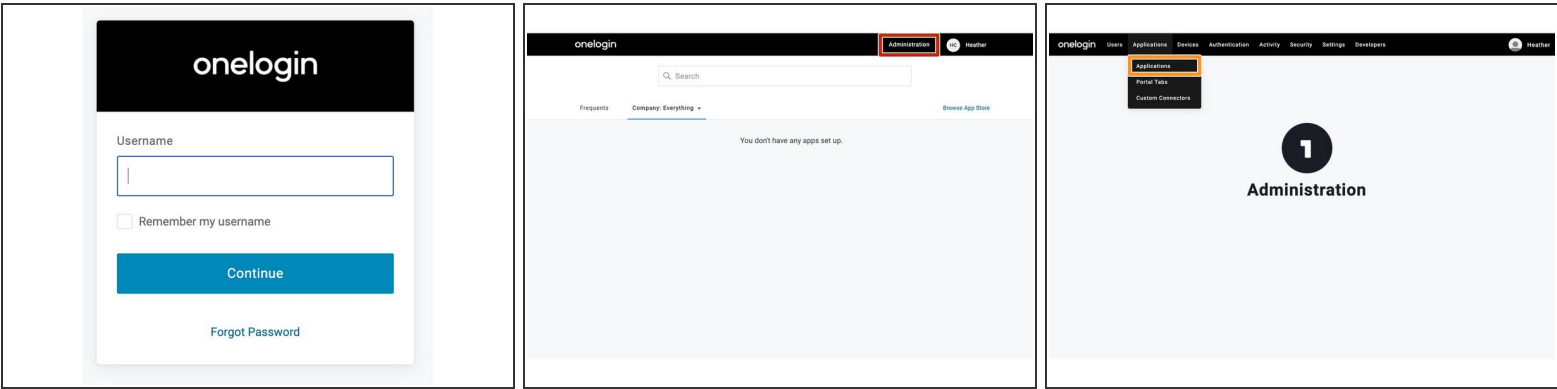
Written By: Dozuki System



INTRODUCTION

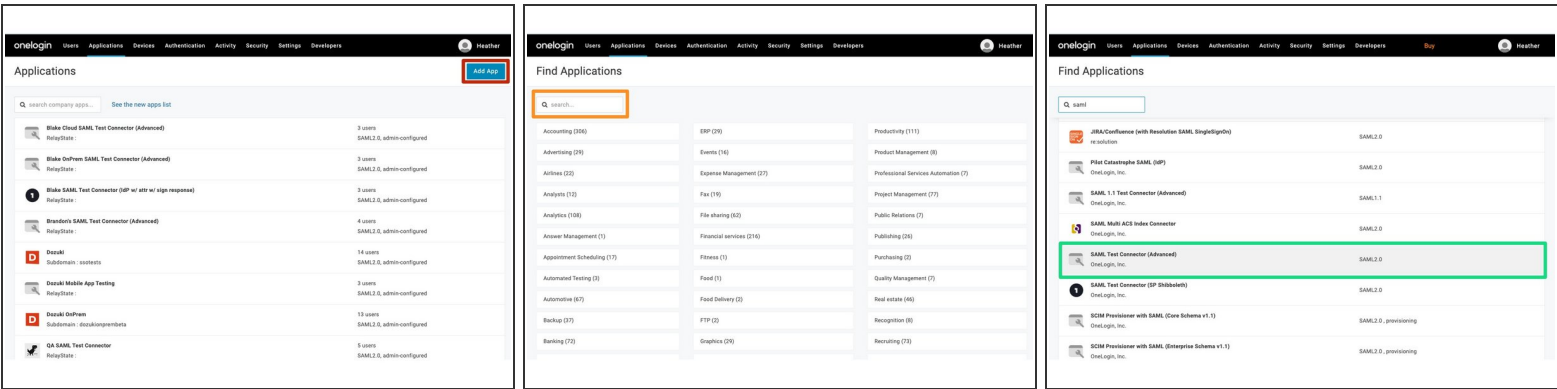
Dozuki sites support single sign-on (SSO) through the SAML 2.0 protocol. Use this guide to set up a SAML2 connection with OneLogin.

Step 1 — Log in to Onelogin



- Log in to the Onelogin admin portal for your organization.
 - ❗ If you do not have an internal login page, login from: <https://app.onelogin.com/login>
- Click on **Administration**.
- Click on **Applications** from the **Applications** list.

Step 2



- Click on **Add Application**.
- Search for **saml**.
- Choose **SAML Test Connector (Advanced)**

Step 3

onelogin Users Applications Devices Authentication Activity Security Settings Developers Buy Heather

App Listing / Add SAML Test Connector (Advanced) Cancel Save

Configuration

Portal

Display Name

Dozuki

Visible in portal

☒

Rectangular Icon

Upload an icon with an aspect-ratio of 2.64:1 as either a transparent .PNG or .SVG

Square Icon

Upload a square icon at least 512x512px as either a transparent .PNG or .SVG

Description

200 characters

- Type a display name for your Dozuki site into the **Display Name** field.
- *i* For customers with a single Dozuki site, we recommend using **Dozuki** as the display name.
- Click **Save**.

Step 4

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 a text editor.

Step 5

onelogin Users Applications Devices Authentication Activity Security Settings Developers Buy Heather

Applications / SAML Test Connector (Advanced) More Actions Save

Info Configuration Parameters Rules SSO Access Users Privileges Setup

Application details

RelayState

Audience (EntityID)

Recipient

ACS (Consumer) URL Validator*
^https://\V/heather\,dozuki\.com/V.*
*Required

ACS (Consumer) URL*
https://heather.dozuki.com/Guide/User/remote_login
*Required

Single Logout URL
https://heather.dozuki.com/Guide/logout

Login URL
heather.dozuki.com

- Under the **Configuration** Tab in Onelogin:
 - Enter the **ACS (Consumer) URL**.
 - ⓘ Refer to the AssertionConsumerService Location value in the SAML `metadata.xml` file.
 - Enter the **Single Logout (URL)**.
 - ⓘ Refer to the SingleLogoutService Location value in the SAML `metadata.xml` file.
 - Enter the **ACS (Consumer) URL Validator** setting.
 - ⓘ This should be formatted with your Dozuki site domain as shown in the image: `^https://\V/` the Dozuki site domain, followed by `V.*`. Additionally add a `\` before every `.`
- Under **Login URL**, enter the URL of the page on your Dozuki site that you want your users to reach once signing in.

Step 6

onelogin

UsersApplicationsDevicesAuthenticationActivitySecuritySettingsDevelopersBuy

Heather

Applications / SAML Test Connector (Advanced)

More ActionsSave

Info

ConfigurationParametersRulesSSOAccessUsersPrivilegesSetup

https://heather.dozuki.com/Guide/logout

Login URL

heather.dozuki.com

Only required if you select Service Provider as the SAML Initiator.

SAML not valid before

3

* Required - Specifies time period, in minutes, the assertion is valid for.

SAML not valid on or after

3

* Required - Specifies time period, in minutes, the assertion is valid for.

SAML initiator

OneLogin

Service Provider

OneLogin

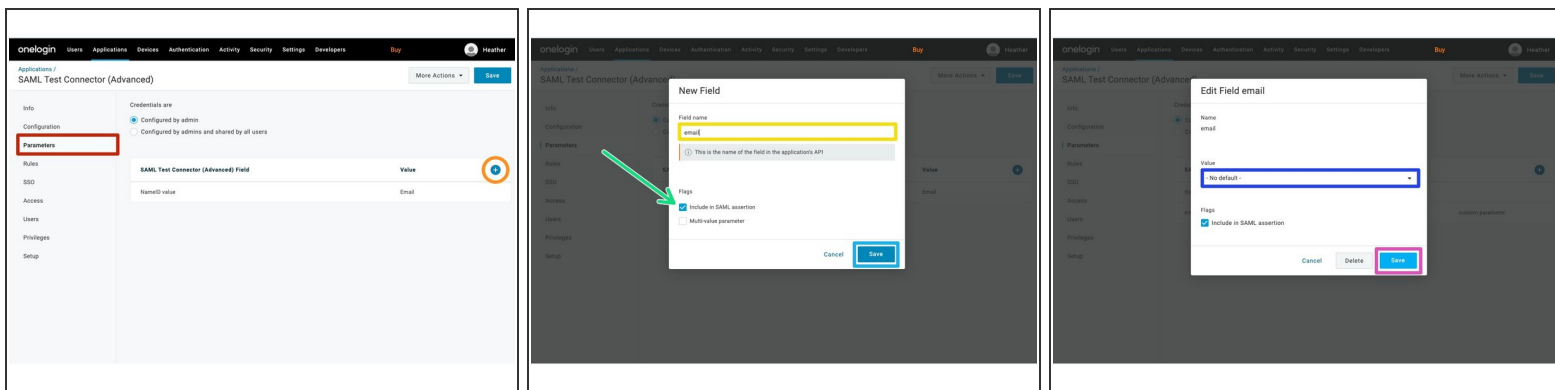
SAML issuer type

Specific

SAML signature element

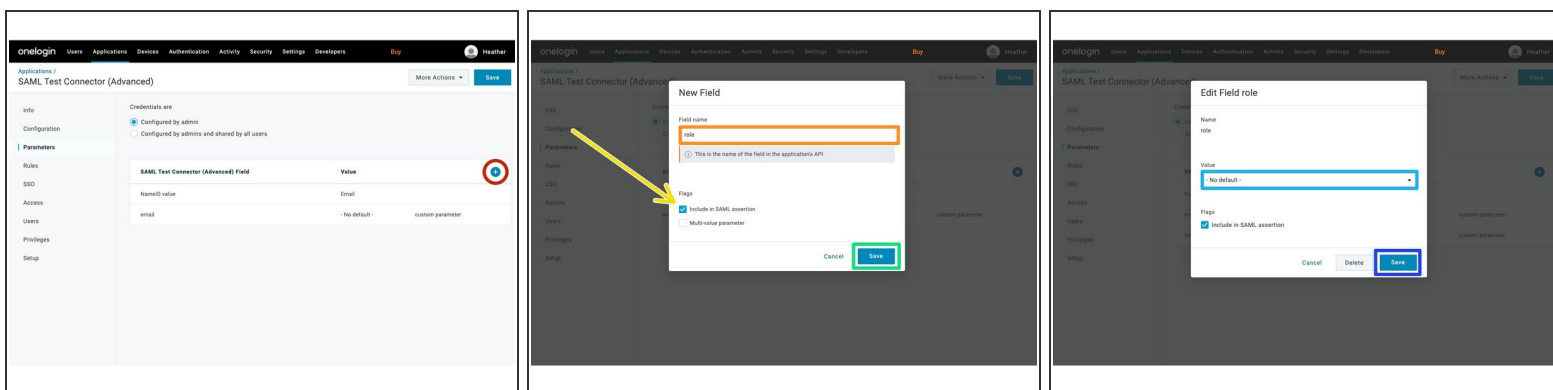
- Scroll down and set **SAML initiator** to **Service Provider**
- Click the **Save** to save all changes.

Step 7 — Set User Attributes and Claims



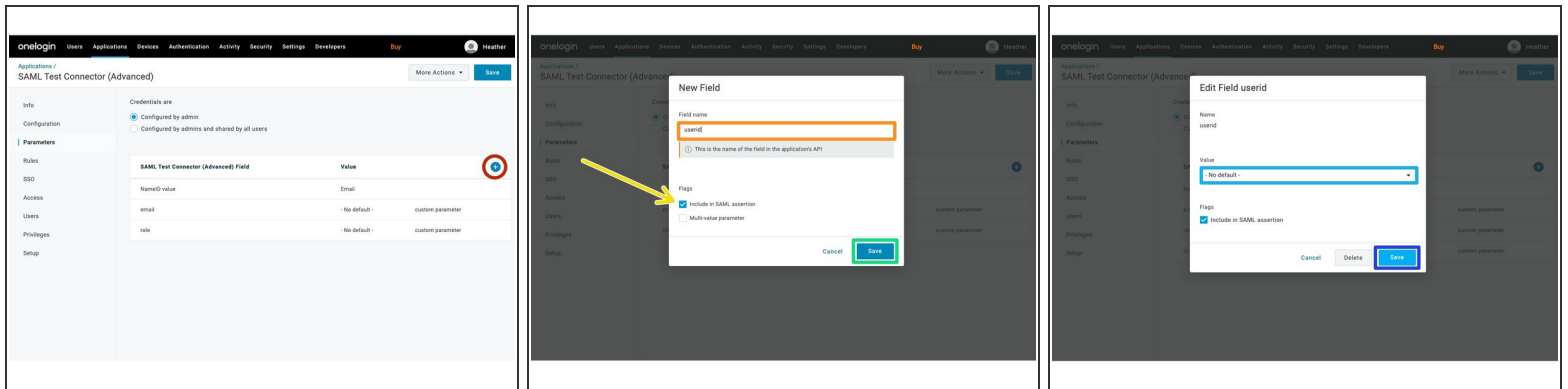
- Under the **Parameters** Tab in Onelogin:
- Click the **+** button to add SAML Test Connector (Advanced) Fields.
- Enter email into the **Field Name**.
- Under **Flags** verify **Include in SAML assertion** is checked.
- Click the **Save** button.
- Confirm the **Value** is set to **-No default-**.
- Click the **Save** button to add the field.

Step 8



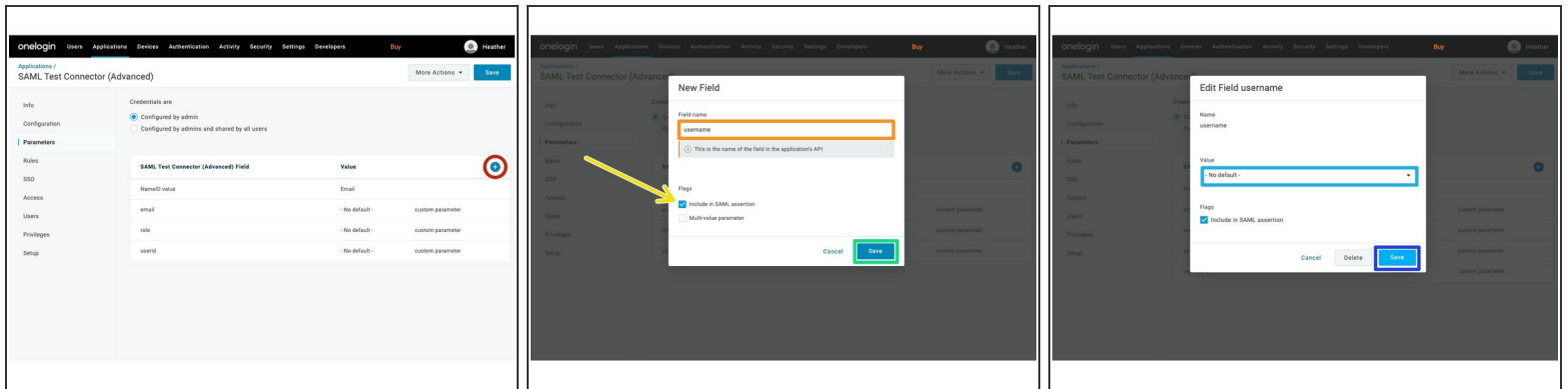
- Click the **+** button again to add an additional SAML Test Connector (Advanced) Fields.
- Enter role into the **Field Name**.
- Under **Flags** verify **Include in SAML assertion** is checked.
- Click the **Save** button.
- Confirm the **Value** is set to **-No default-**.
- Click the **Save** button to add the field.

Step 9



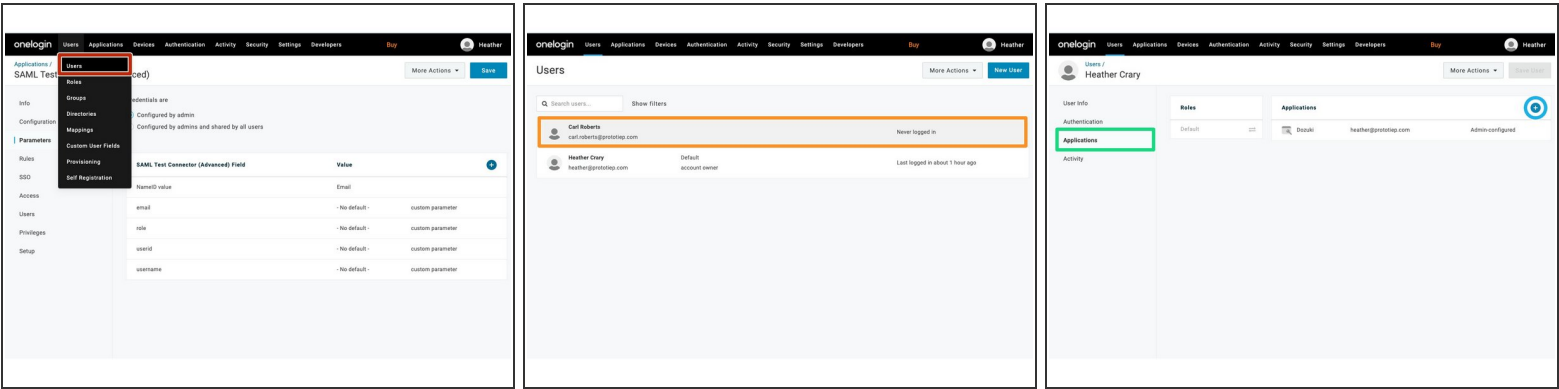
- Click the **+** button to add SAML Test Connector (Advanced) Fields.
- Enter **userid** into the **Field Name**.
- Under **Flags** verify **Include in SAML assertion** is checked.
- Click the **Save** button.
- Confirm the **Value** is set to **-No default-**.
- Click the **Save** button to add the field.

Step 10



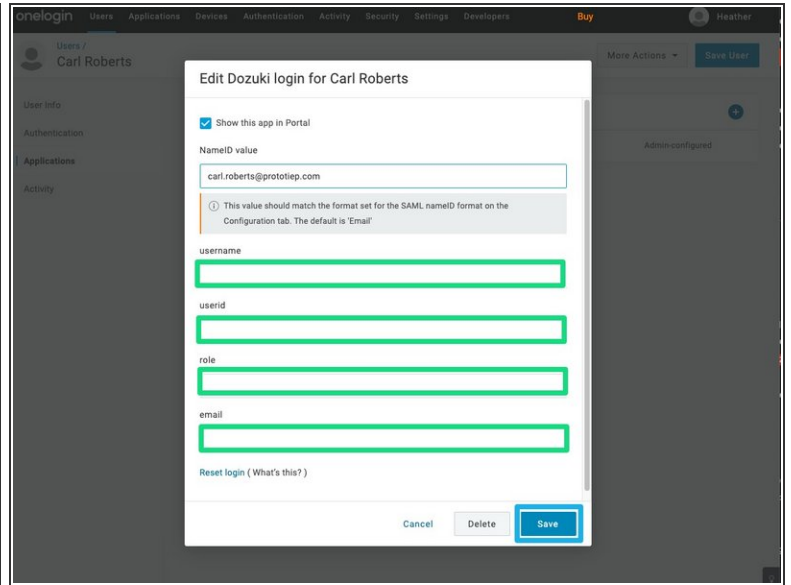
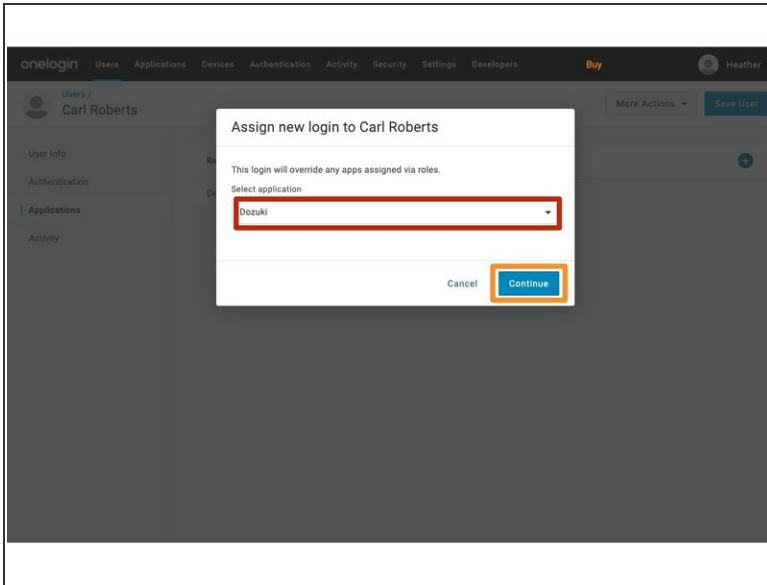
- Click the **+** button to add SAML Test Connector (Advanced) Fields.
- Enter username into the **Field Name**.
- Under **Flags** verify **Include in SAML assertion** is checked.
- Click the **Save** button.
- Confirm the **Value** is set to **-No default-**.
- Click the **Save** button to add the field.

Step 11 — Assign a User or Group



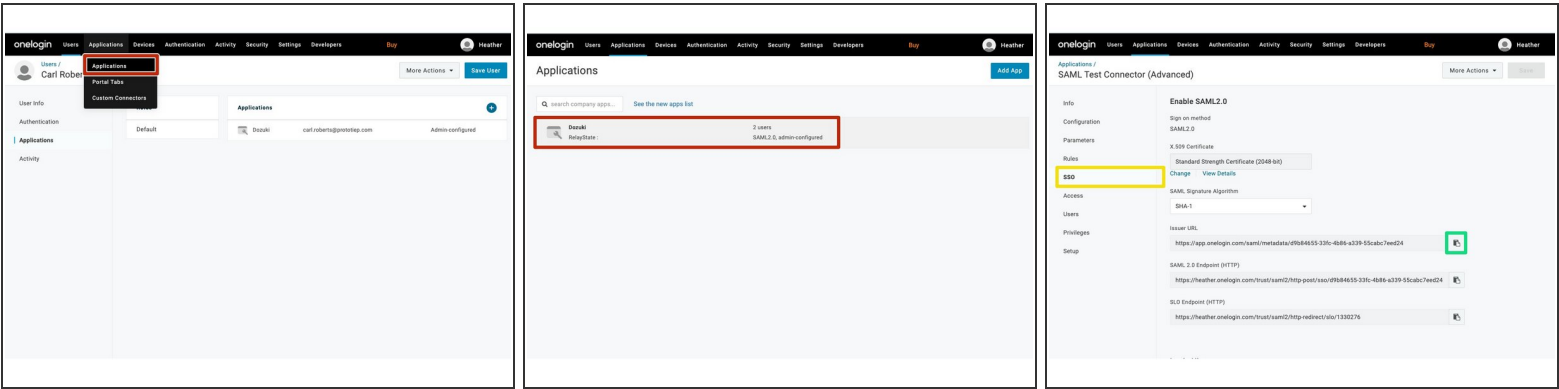
- From the page header, Click on **Users** and select **Users** or **Groups** from the dropdown list.
- Select the **User** or **Group** you to want to assign to the application.
- Click the **Applications** tab.
- Click the **+** button and add your Dozuki application.

Step 12



- Select the **Dozuki** application.
 - Click the **Continue** button.
 - Fill out the required user fields.
 - ❗ Only lowercase should be used when filling out the user fields.
 - ⚠ If you are adding a user that has an existing user account on your Dozuki site, the email field **must** match the Dozuki site user's email. If they do not match, a new user will be created upon logging in.
 - Click the **Save** button to save all entries.
- 📌 You can read more about [adding and assigning users](#) in Onelogin.

Step 13 — SAML Signing Certificate



- Select **Applications** from the **Applications** list in OneLogin.
- Select the **Dozuki** application.
- Click on the **SSO** tab.
- Copy the **Issuer URL**.

Step 14

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	8IfjggLYh0r aPZ48Nlr 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

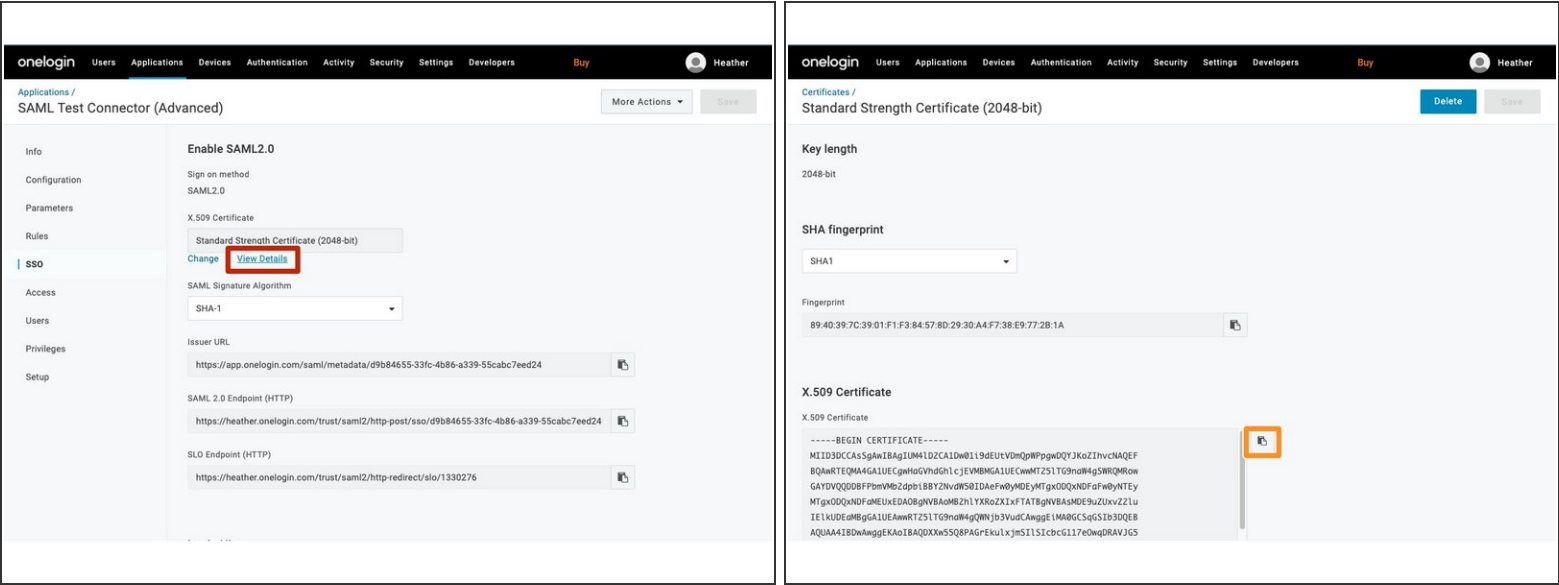
Single sign on: disabled. Login and account creation on this site happens normally.

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	<div>The unique identifier for your identity provider. This must be a URI and must match the Issuer field that is sent in your identity provider's SAML 2.0 responses.</div> <div>https://app.onelogin.com/saml/metadata/d9b84655-33fc-4b86-a339-5f</div> <div>Save</div>	Cancel
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

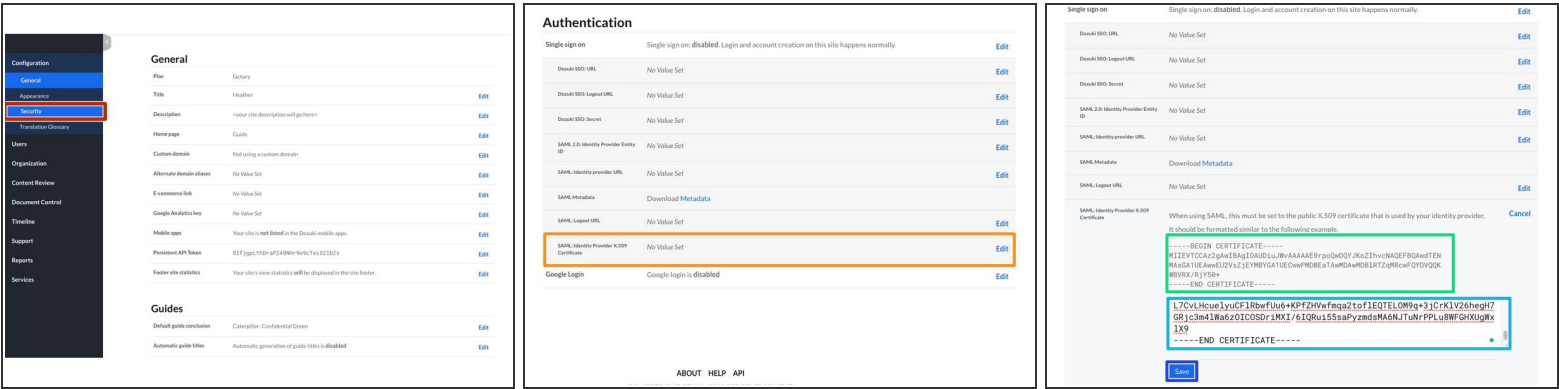
- Open the management console of your Dozuki site in another browser window.
- From the **Configuration** section in the sidebar menu, select **Security**.
- Under the **Authentication** heading section, paste the **Issuer URL** into the **SAML 2.0: Identity Provider ID** text field in your Dozuki site.
- Click the **Save** button to save your changes.

Step 15



- From the OneLogin site, click **View Details** of the **X.509 Certificate**.
- Copy the **X.509 Certificate**.

Step 16



- Open the management console of your Dozuki site.
- Under the **Authentication** heading section of the Dozuki Security page, click on **SAML: Identity Provider X.509 Certificate**.
 - 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 17 — Add Onelogin Logout URL

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.azure.com/ok2s0lCxp679FW5d6	Edit
SAML 2.0 Identity provider URL	https://dozukidozuki1.okta.com/app/iboukidozuki1_dozuki_1/ok2s0lCxp679FW5d6/so/saml	Edit
SAML Metadata	Download Metadata	
SAML Logout URL	No Value Set	Edit
SAML 2.0 Identity Provider X.509 Certificate	Valid certificate	Edit
Google Login	Google login is disabled	Edit

oneloginUsersApplicationsSessionsAuthenticationActivitySecuritySettingsDeveloperBuyHeather

Applications / SAML Test Connector (Advanced)

More ActionsSave

Info

Configuration

Parameters

Rules

SSO

Access

Users

Privileges

Setup

Enable SAML2.0

Sign on method

SAML2.0

ChangeView Details

X.509 Certificate

Standard Strength Certificate (2048 bit)

SAML Signature Algorithm

SIG-1

Issuer URL

https://app.onelogin.com/saml/metadata/49084455-33fc-4b86-a339-55cab7eed24

SAML 2.0 Endpoint (HTTP)

https://heather.onelogin.com/trust/saml2/http-post/sso/49084455-33fc-4b86-a339-55cab7eed24

SLO Endpoint (HTTP)

https://heather.onelogin.com/trust/saml2/http-redirect/slo/1330276

Authentication

Single sign on

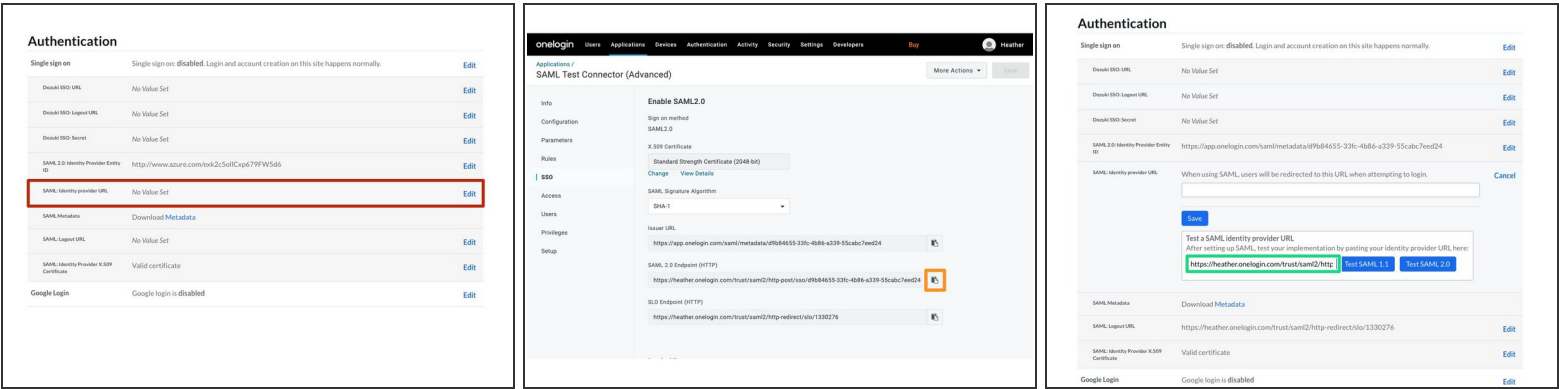
Single sign on: disabled. Login and account creation on this site happens normally.

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	https://app.onelogin.com/saml/metadata/49084455-33fc-4b86-a339-55cab7eed24	Edit
SAML 2.0 Identity provider URL	No Value Set	Edit
SAML Metadata	Download Metadata	
SAML Logout URL	When using SAML, users will be redirected to this URL after logging out. https://heather.onelogin.com/trust/saml2/http-redirect/slo/1330276	Cancel
SAML 2.0 Identity Provider X.509 Certificate	Valid certificate	Edit
Google Login	Google login is disabled	Edit

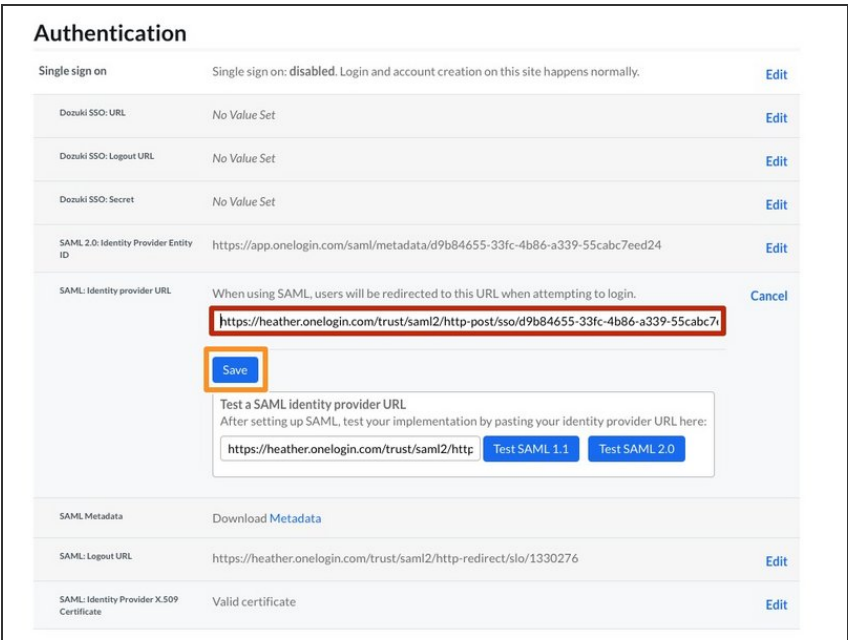
- Click on the **SAML: Logout URL** heading under **Authentication**.
- Under the **SSO** tab in Onelogin, click on the **Copy** icon next to **SLO Endpoint (HTTP)**.
- Paste the **SLO Endpoint** into the **SAML: Logout URL** text field in your Dozuki site.
- Click the **Save** button to save your changes.

Step 18 — Test Onelogin Connection



- Click on the **SAML: Identity provider URL** heading under **Authentication**.
- Under the **SSO** section in Onelogin, click on the **Copy** icon next to **SAML 2.0 Endpoint** .
- Paste the **SAML 2.0 Endpoint** 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.

Step 19 — Add Onelogin Connection



- Once the connection test succeeds, paste the **SAML 2.0 Endpoint** into the **SAML: Identity provider URL** field.
- Click the **Save** button to save your changes.

Step 20 — Enable Single Sign On

Authentication

Single sign on

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

Edit

Disco! SSO URL

No Value Set

Edit

Disco! SSO Logout URL

No Value Set

Edit

Disco! SSO Secret

No Value Set

Edit

SAML 2.0 Identity Provider Entity ID

https://app.onelogin.com/saml/metadata?id9b84655-33fc-4b86-a339-55cab7eed24

Edit

SAML Identity provider URL

https://heather.onelogin.com/trust/saml2/http-post/soa/99b84655-33fc-4b86-a339-55cab7eed24

Edit

SAML Metadata

Download Metadata

SAML Logout URL

https://heather.onelogin.com/trust/saml2/http-redirect/slo/1330276

Edit

SAML Identity Provider X.509 Certificate

Valid certificate

Edit

Google Login

Google login is disabled

Edit

Authentication

Single sign on

Single Sign On type: Disabled

Cancel

- How to use SSO

Save

Disco! SSO URL

No Value Set

Edit

Disco! SSO Logout URL

No Value Set

Edit

Disco! SSO Secret

No Value Set

Edit

SAML 2.0 Identity Provider Entity ID

https://app.onelogin.com/saml/metadata?id9b84655-33fc-4b86-a339-55cab7eed24

Edit

SAML Identity provider URL

https://heather.onelogin.com/trust/saml2/http-post/soa/99b84655-33fc-4b86-a339-55cab7eed24

Edit

SAML Metadata

Download Metadata

SAML Logout URL

https://heather.onelogin.com/trust/saml2/http-redirect/slo/1330276

Edit

SAML Identity Provider X.509 Certificate

Valid certificate

Edit

Google Login

Google login is disabled

Edit

Authentication

Single sign on

Single Sign On type: Disabled

Cancel

- How to use SSO

Save

Disco! SSO URL

No Value Set

Edit

Disco! SSO Logout URL

No Value Set

Edit

Disco! SSO Secret

No Value Set

Edit

SAML 2.0 Identity Provider Entity ID

https://app.onelogin.com/saml/metadata?id9b84655-33fc-4b86-a339-55cab7eed24

Edit

SAML Identity provider URL

https://heather.onelogin.com/trust/saml2/http-post/soa/99b84655-33fc-4b86-a339-55cab7eed24

Edit

SAML Metadata

Download Metadata

SAML Logout URL

https://heather.onelogin.com/trust/saml2/http-redirect/slo/1330276

Edit

SAML Identity Provider X.509 Certificate

Valid certificate

Edit

Google Login

Google login is disabled

Edit

- 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 21 — SSO: Role Attribute Prefix

Authentication

Single sign-on

Single sign on using SAML. Users are being redirected to your SAML endpoint when they try to log in.

Edit

SAML 2.0 Identity Provider Entity ID

No Value Set

Edit

SAML Identity provider URL

No Value Set

Edit

SAML Metadata

Download Metadata

Edit

SAML Logout URL

No Value Set

Edit

SAML Identity Provider X.509 Certificate

No Value Set

Edit

SSO Role Attribute Prefix

No Value Set

Edit

SSO auth for signoffs & approvals

SSO authentication is used for step signoffs and approval requests.

Edit

Google Login

Google login is disabled

Edit

Authentication

Single sign-on

Single sign on using SAML. Users are being redirected to your SAML endpoint when they try to log in.

Edit

SAML 2.0 Identity Provider Entity ID

No Value Set

Edit

SAML Identity provider URL

No Value Set

Edit

SAML Metadata

Download Metadata

Edit

SAML Logout URL

No Value Set

Edit

SAML Identity Provider X.509 Certificate

No Value Set

Edit

SSO Role Attribute Prefix

An optional prefix for roles passed via SSO. For example, a prefix of "dozuki-" will allow roles to be passed as "dozuki-admin", "dozuki-author", etc.

dozuki

Cancel

SSO auth for signoffs & approvals

SSO authentication is used for step signoffs and approval requests.

Edit

Google Login

Google login is disabled

Edit

Authentication

Single sign-on

Single sign on using SAML. Users are being redirected to your SAML endpoint when they try to log in.

Edit

SAML 2.0 Identity Provider Entity ID

No Value Set

Edit

SAML Identity provider URL

No Value Set

Edit

SAML Metadata

Download Metadata

Edit

SAML Logout URL

No Value Set

Edit

SAML Identity Provider X.509 Certificate

No Value Set

Edit

SSO Role Attribute Prefix

dozuki

Edit

SSO auth for signoffs & approvals

SSO authentication is used for step signoffs and approval requests.

Edit

Google Login

Google login is disabled

Edit

- i

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.)
- i

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 22 — 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: [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	https://app.onelogin.com/saml/metadata/d9b84655-33fc-4b86-a339-55cab7eed24	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

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](#)

Google Login

Google login is disabled

[Edit](#)

- 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.