

# Configuring LaunchDarkly

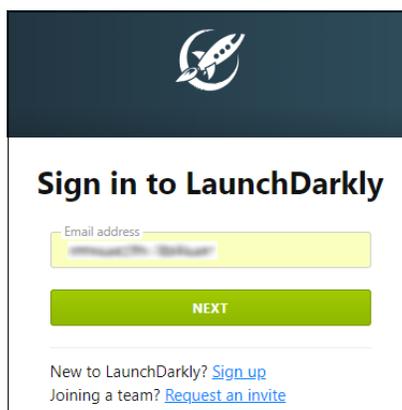
Configuring LaunchDarkly for single sign-on (SSO) enables administrators to manage users of Citrix ADC. Users can securely log on to LaunchDarkly by using the enterprise credentials.

## Prerequisite

Browser Requirements: Internet Explorer 11 and above

## To configure LaunchDarkly for SSO by using SAML:

1. In a browser, type <https://launchdarkly.com> and press **Enter**.
2. In the home page, click **Sign In**.
3. Type your admin credentials in **Email Address** and click **NEXT**.





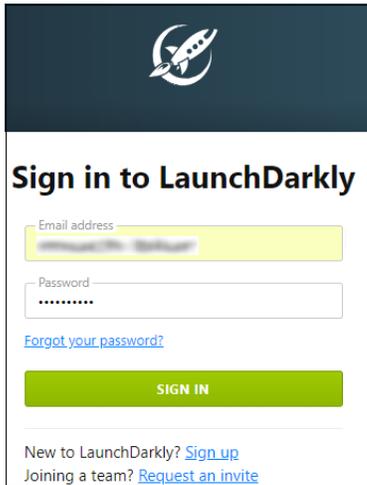
## Sign in to LaunchDarkly

Email address

**NEXT**

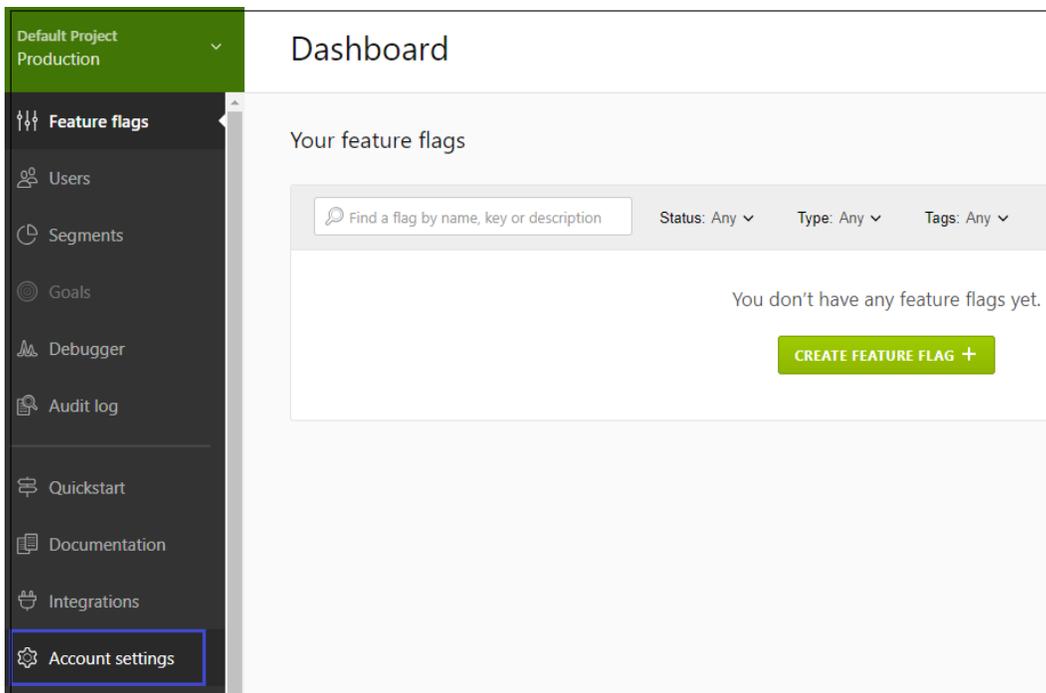
New to LaunchDarkly? [Sign up](#)  
Joining a team? [Request an invite](#)

4. Type your LaunchDarkly **Password** and click **SIGN IN**.



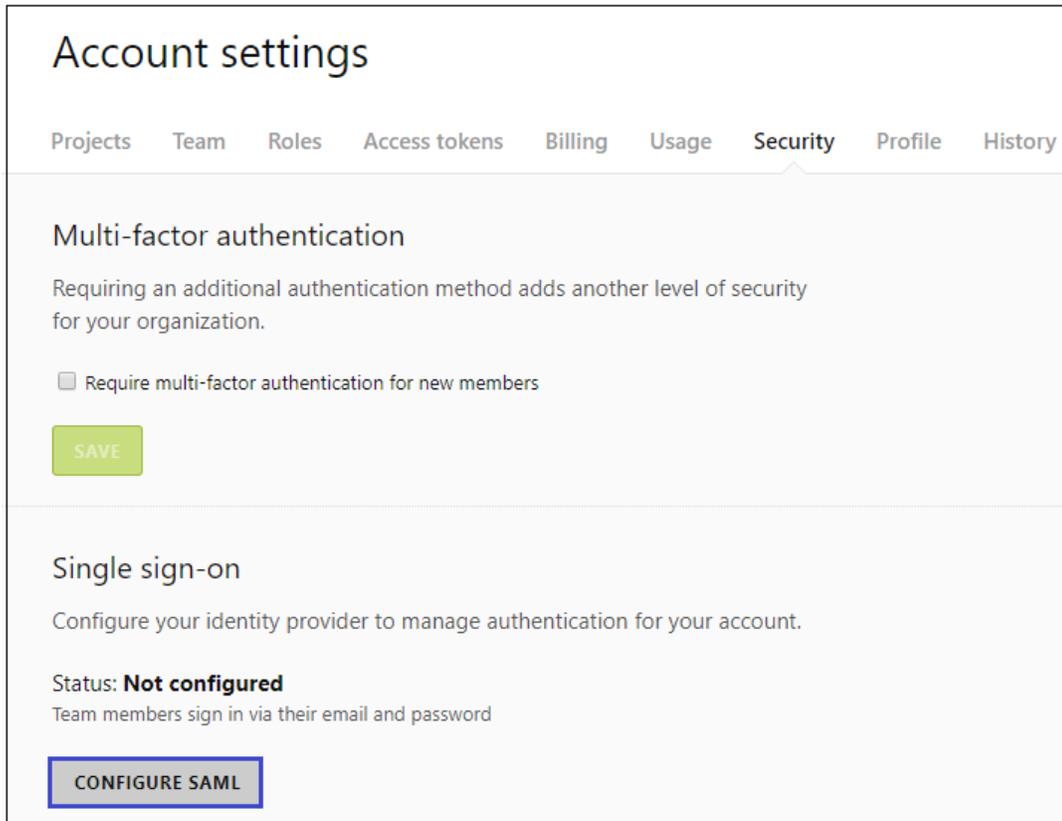
The image shows the LaunchDarkly sign-in page. At the top is the LaunchDarkly logo (a rocket) on a dark blue background. Below the logo is the heading "Sign in to LaunchDarkly". There are two input fields: "Email address" and "Password". The "Email address" field contains the text "example@citrix.com". The "Password" field contains a series of dots. Below the password field is a link that says "Forgot your password?". At the bottom of the form is a green "SIGN IN" button. Below the button, there are two links: "New to LaunchDarkly? Sign up" and "Joining a team? Request an invite".

5. Under **Default Project**, click **Account settings**.



The image shows the LaunchDarkly dashboard. On the left is a dark sidebar with a green header that says "Default Project Production" with a dropdown arrow. Below the header are several menu items: "Feature flags", "Users", "Segments", "Goals", "Debugger", "Audit log", "Quickstart", "Documentation", "Integrations", and "Account settings". The "Account settings" item is highlighted with a blue box. The main content area is titled "Dashboard" and "Your feature flags". It contains a search bar "Find a flag by name, key or description" and three dropdown menus: "Status: Any", "Type: Any", and "Tags: Any". Below these is a message that says "You don't have any feature flags yet." and a green button that says "CREATE FEATURE FLAG +".

6. In the **Account Settings** page, under **Single sign-on**, click **CONFIGURE SAML**.



The screenshot displays the 'Account settings' page with a navigation menu at the top including 'Projects', 'Team', 'Roles', 'Access tokens', 'Billing', 'Usage', 'Security', 'Profile', and 'History'. The 'Security' tab is active. Below the navigation, there are two main sections: 'Multi-factor authentication' and 'Single sign-on'. The 'Multi-factor authentication' section includes a checkbox for 'Require multi-factor authentication for new members' and a green 'SAVE' button. The 'Single sign-on' section includes a description, a status indicator 'Not configured', and a blue 'CONFIGURE SAML' button.

## Account settings

Projects Team Roles Access tokens Billing Usage **Security** Profile History

### Multi-factor authentication

Requiring an additional authentication method adds another level of security for your organization.

Require multi-factor authentication for new members

SAVE

### Single sign-on

Configure your identity provider to manage authentication for your account.

Status: **Not configured**  
Team members sign in via their email and password

CONFIGURE SAML

7. To create **Single Sign-On**, enter the values for the following fields:

Field	Description
Sign-on URL	IdP logon URL
X.309 certificate	Copy and paste the IdP certificate. The IdP certificate must begin and end with -----Begin Certificate----- and -----End Certificate----- <b>Note:</b> The IdP certificate is provided by Citrix and can be accessed from the link below: <a href="https://ssb4.mgmt.netscalergatewaydev.net/idp/saml/templatetest/idp_metadata.xml">https://ssb4.mgmt.netscalergatewaydev.net/idp/saml/templatetest/idp_metadata.xml</a>

### Set up your SAML configuration

---

#### Configure your SAML application

These values are required when setting up the LaunchDarkly application in your identity provider.

Assertion consumer service URL

Entity ID

Start URL

#### Enter your SAML identity provider details

Sign-on URL

X.509 certificate

Paste your certificate above or [upload one](#)

**SAVE** Support

8. Finally, click **SAVE**.