**Okta-Atlassian Cloud Integration**

# Background

This section aims at providing a detailed description on integrating Atlassian Cloud and Okta and configure SAML for setting up SSO for the users along with configuring user account provisioning for Confluence/Jira.

The purpose of integrating Okta and Atlassian Cloud is to allow the users to have Single Sign-on setup(SSO) so that the users can access the Confluence/Jira applications from Okta in one single login. Configuring user provisioning helps to manage all user attributes and group memberships from Okta.

# Prerequisites

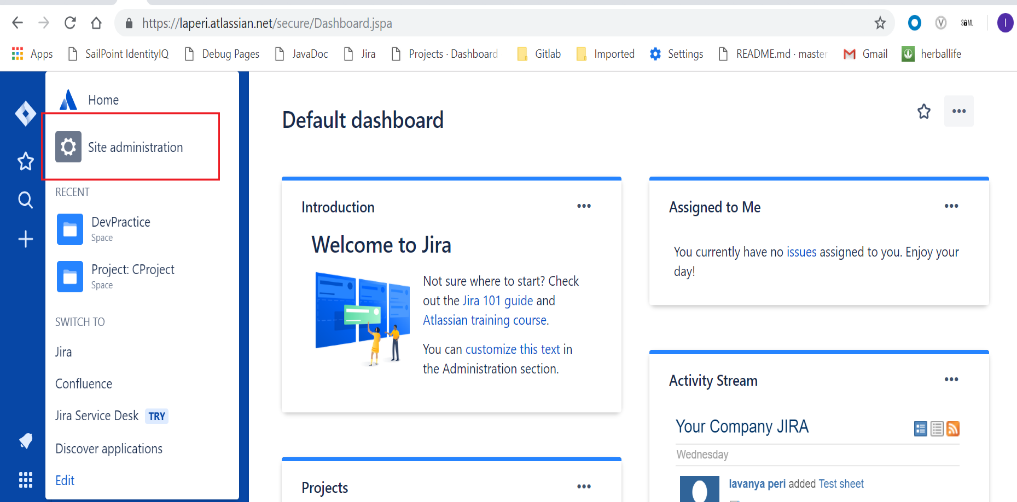
Have an administrator account in Atlassian Cloud (Confluence/Jira) to enable SAML single sign-on and Provisioning to user’s Atlassian accounts.

## 2.1 Setup an Atlassian organization

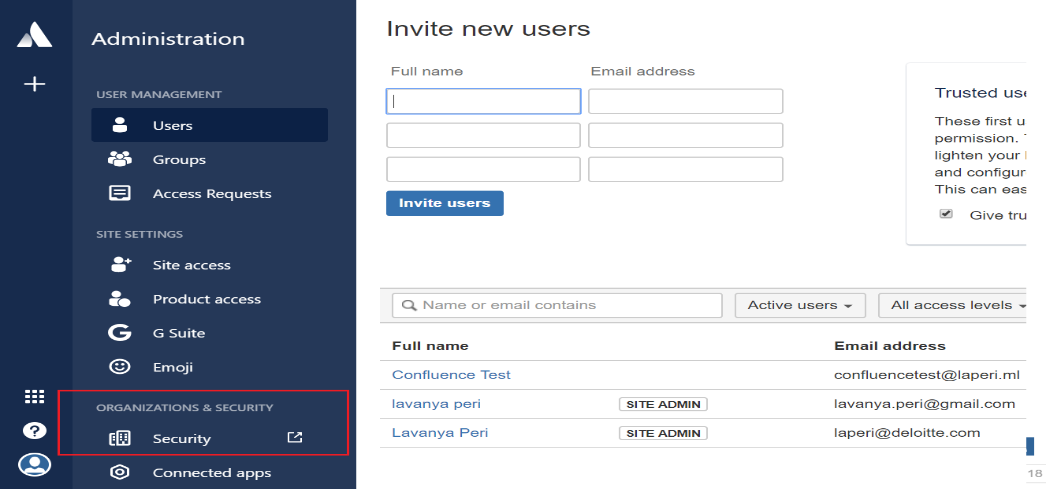
An Atlassian organization provides a centralized place for managing your domains and users. Organizations are particularly helpful if your company manages more than one site and wants insight into all your sites and products and the users who can access them.

To create an organization:

1. Log into your Atlassian account.
2. Navigate to **Site administration.**

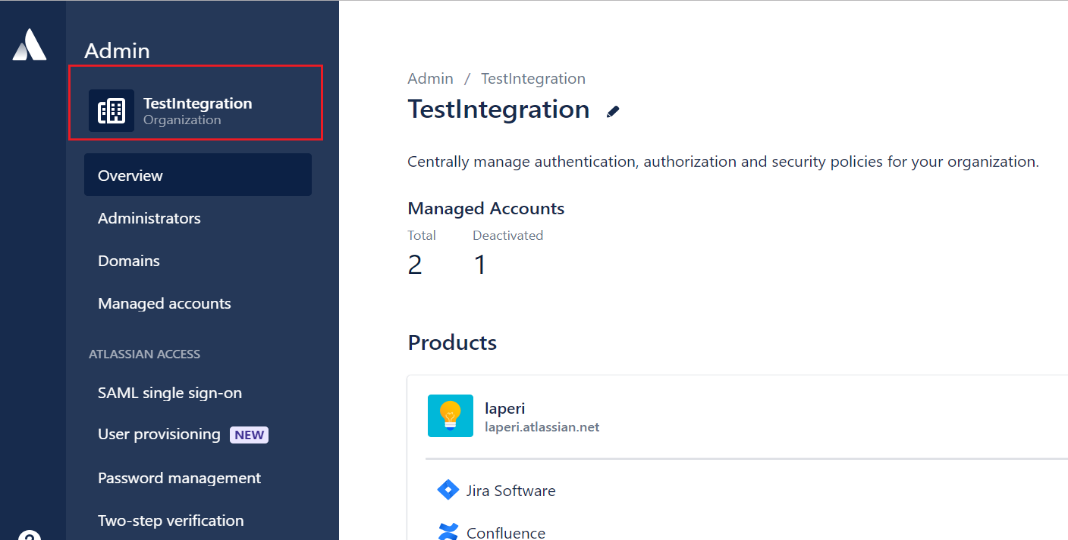


1. From **Site administration,** click **Security** under **Organizations &Security.**



1. Click **Try Atlassian Access**. This link takes you to [admin.atlassian.com](https://admin.atlassian.com/).
2. Choose **Create organization**, and then enter a name for your new organization.

As the creator of an organization, you’re the first organization admin, and you can add others as organization admins.



**Note**:

* To rename an organization, from the **Overview** page, click the **edit** (pencil) icon.
* Update the name and click **Rename**.
* Renaming an organization has no impact on users or any security policies.

## 2.2 Verify a Domain for your Organization

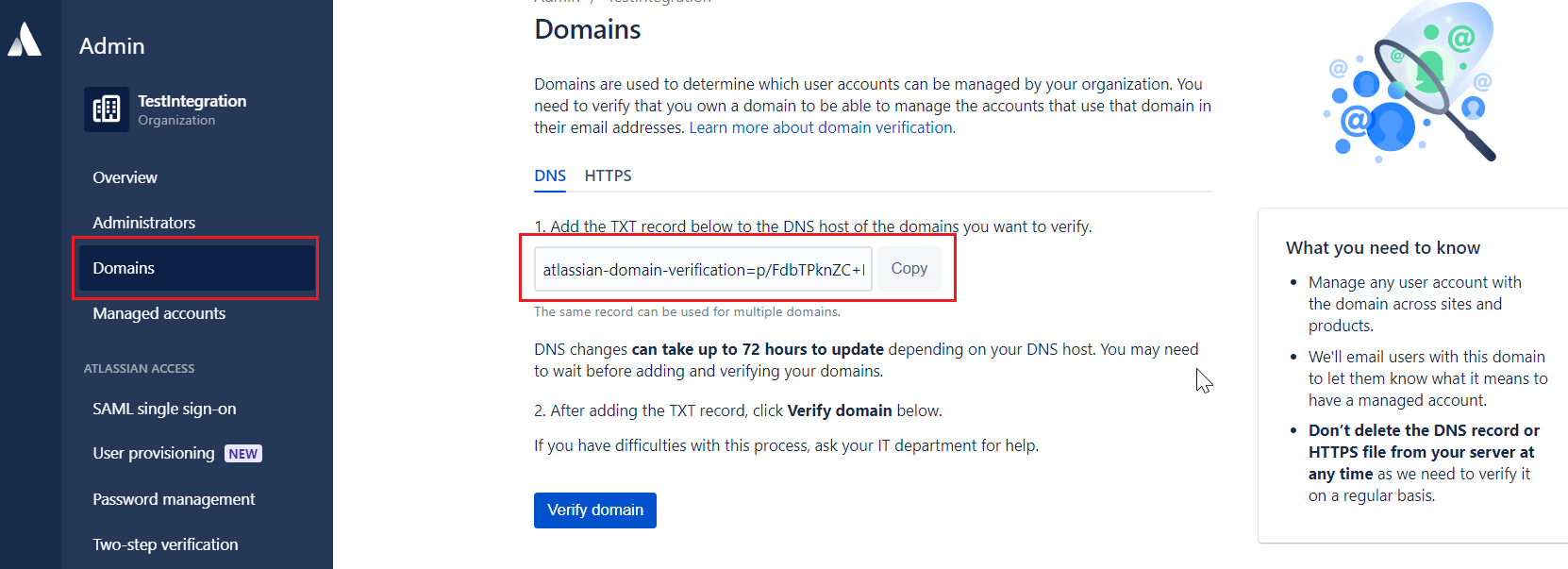
* Once you've [created an organization](https://confluence.atlassian.com/cloud/set-up-an-atlassian-organization-938859734.html) in Atlassian Cloud, you can verify ownership of the domains associated with your user's Atlassian accounts.
* Verifying a domain allows you to have control over the Atlassian accounts that access your Atlassian Cloud products (those accounts are called as *managed accounts*).
* All the Atlassian accounts with email addresses from those domains become managed by your organization.

### 2.2.1 Verify a Domain using DNS

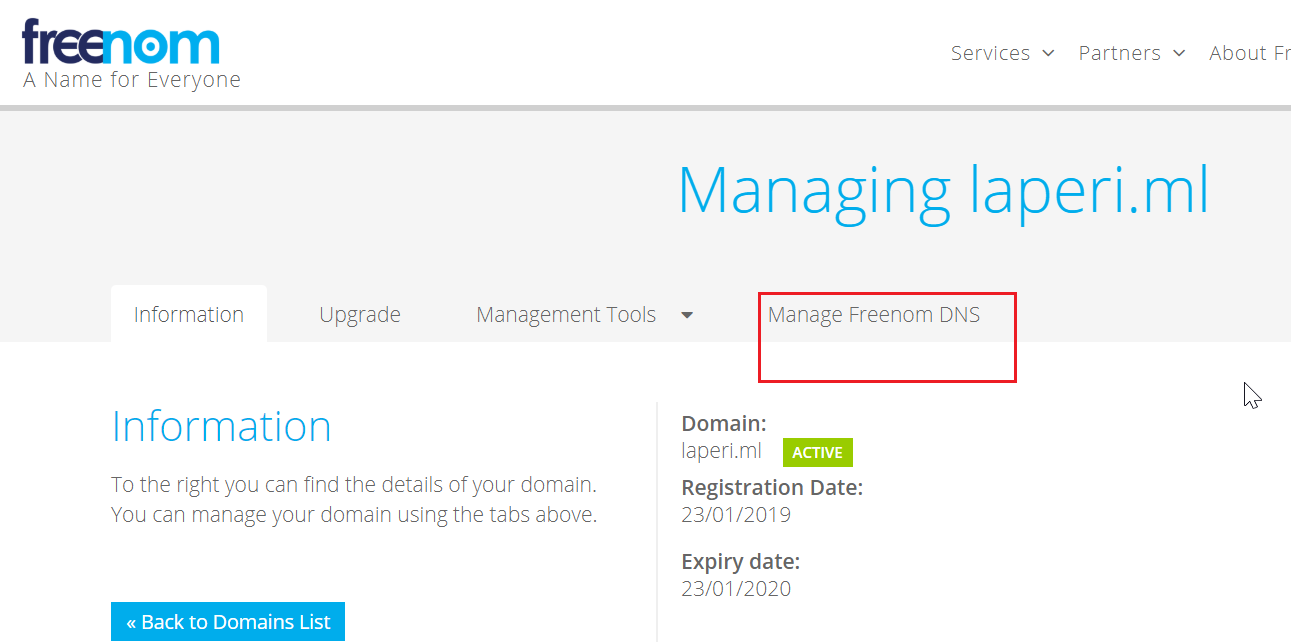
This validation method allows you to demonstrate control over your domain by creating a DNS TXT record containing a randomly generated token as the value.

**To verify a domain using DNS:**

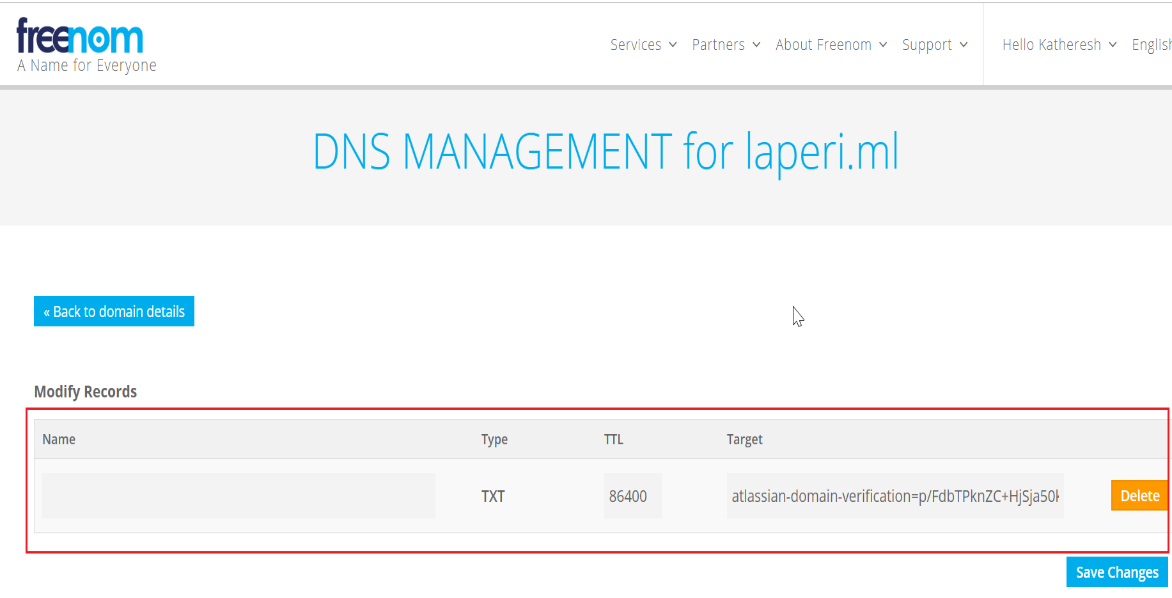
1. Log in to [admin.atlassian.com](http://admin.atlassian.com/) and choose your organization.
2. Choose **Domains** and click the **DNS tab.**
3. Copy the txt record to your clipboard.



1. Go to your DNS host and find the settings page for adding a new record.



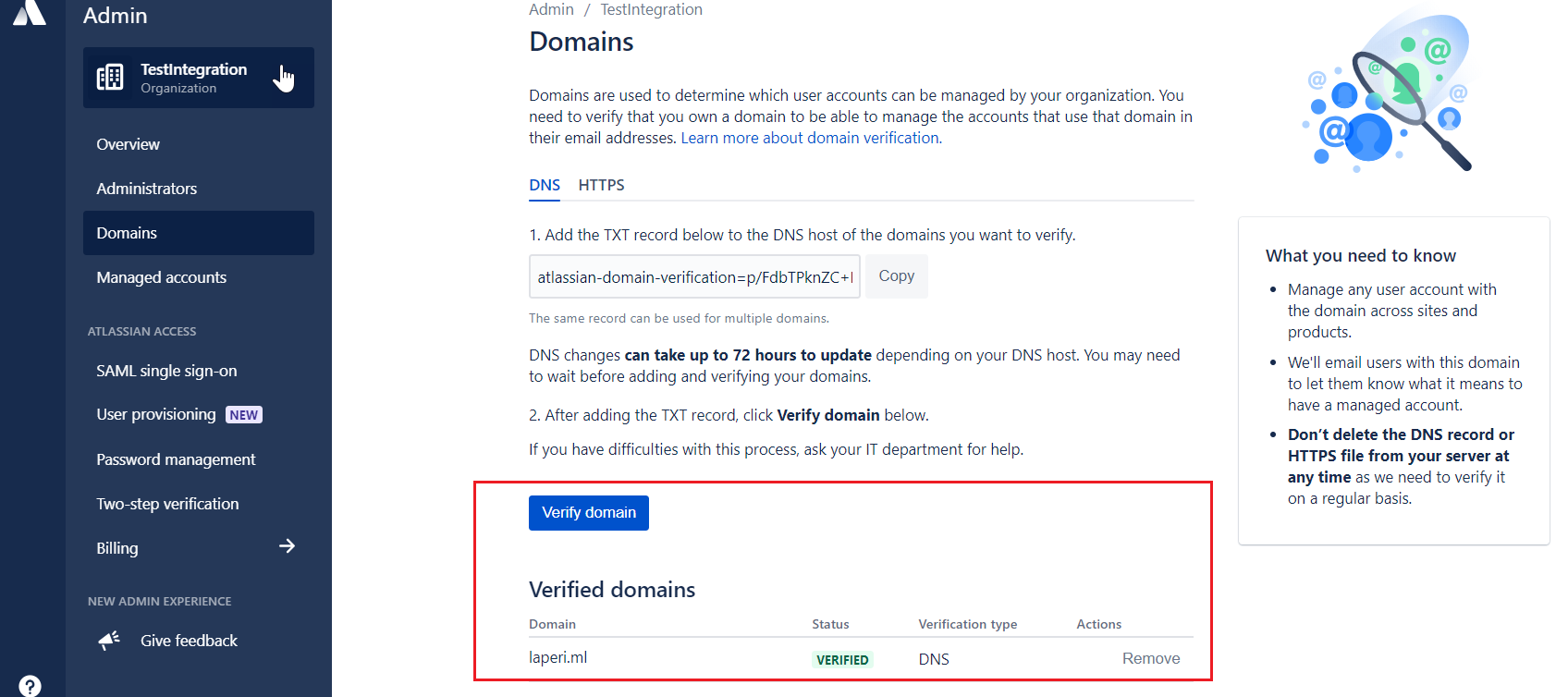
1. Select the option for adding a new record and paste the txt record to the Value field (that may also be named Answer or Description).



1. DNS record may have the following fields:

* **Record type:** Enter 'TXT'.
* **Name/Host/Alias:** Leave the default (@ or blank).
* **Time to live (TTL):** Enter '86400'.
* **Target:** Paste the TXT record token which was copied from the Atlassian account.

1. Save the record.
2. In your Atlassian administration area click **Verify domain.**
3. It may take up to 72 hours to know whether domain verification has succeeded, but usually you'll find out much sooner. Check the **Domains** page for the verification status.



1. After verification is successful, Atlassian will periodically checks the DNS host for the txt record.
2. If someone deletes or updates the txt record with incorrect information, Atlassian will send you an email letting you know that you have a certain amount of time to update the txt record. If you don't, your domain will lose its verification status. If this happens, any Atlassian Access security policies in place for that domain, including SAML single sign-on, won't be effective.
3. All the Atlassian accounts with email addresses from verified domains become *managed* by your organization.

## 2.3. Subscribe to Atlassian Access

* Atlassian Access enables visibility and security across all Atlassian accounts and products at your company.
* Subscription to Atlassian Access applies security policies over all those managed accounts. Users with those accounts will be subject to the policies you've set, no matter which Atlassian products they log in to.
* To subscribe to Atlassian Access:

1. From [admin.atlassian.com](http://admin.atlassian.com/?_ga=2.80386768.697316951.1548681761-2080300696.1547698915&_gac=1.18201675.1548061956.Cj0KCQiA-JXiBRCpARIsAGqF8wU5cccOVrxn0doYOh6EbkhbkrmtWehNFWixYtuQ1USAv97Nvbzt_aAaAtK0EALw_wcB), navigate to your organization.
2. From the **Overview** page, click **Learn more**.
3. Choose **Try it free for 30 days**to begin your Atlassian Access subscription.

### 2.3.1 Atlassian Access security features

* To apply security policies to your managed accounts, you have a few options after you subscribe to Atlassian Access.
* Atlassian Access includes two features for connecting your identity provider: **SAML single sign-on** and **user provisioning**.

#### 2.3.1.1 SAML single sign-on

SSO allows a user to authenticate with one set of login credentials and access multiple products during their session.

With SSO, following are the benefits:

* If [self-signup is enabled](https://confluence.atlassian.com/cloud/configure-site-access-744721636.html), an Atlassian account for them is created when that user logs in for the first time with SSO.
* Security policies can be set from identity provider (Okta) that will apply when users log in to Atlassian products(Confluence/Jira).

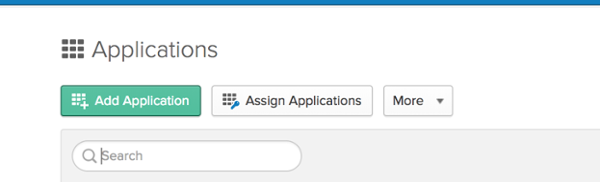
#### 2.3.1.2 User Provisioning

User provisioning integrates an external user directory with Atlassian Cloud products (Confluence/Jira).

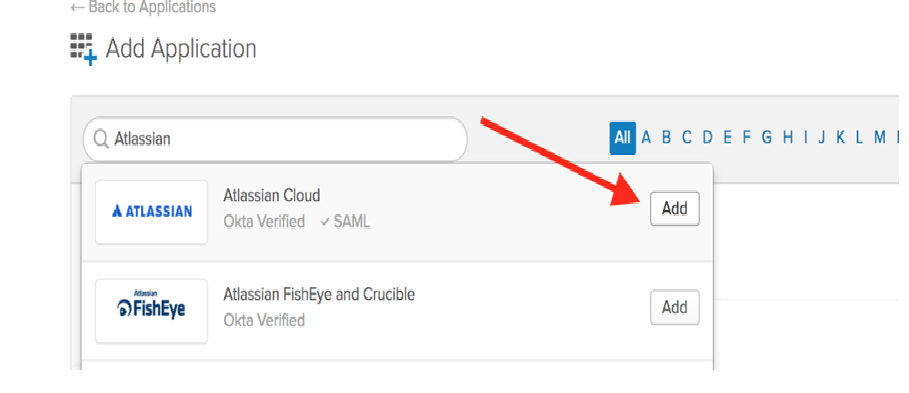
With user provisioning, following are the benefits:

* Automatically update the users and groups in your Atlassian organization when you make updates in identity provider, saves time.
* When you deactivate a user in identity provider, that use will automatically be deactivated in Atlassian organization, giving more security.
* New users automatically have access to your products as soon as they’re activated, making onboarding new employees easier.

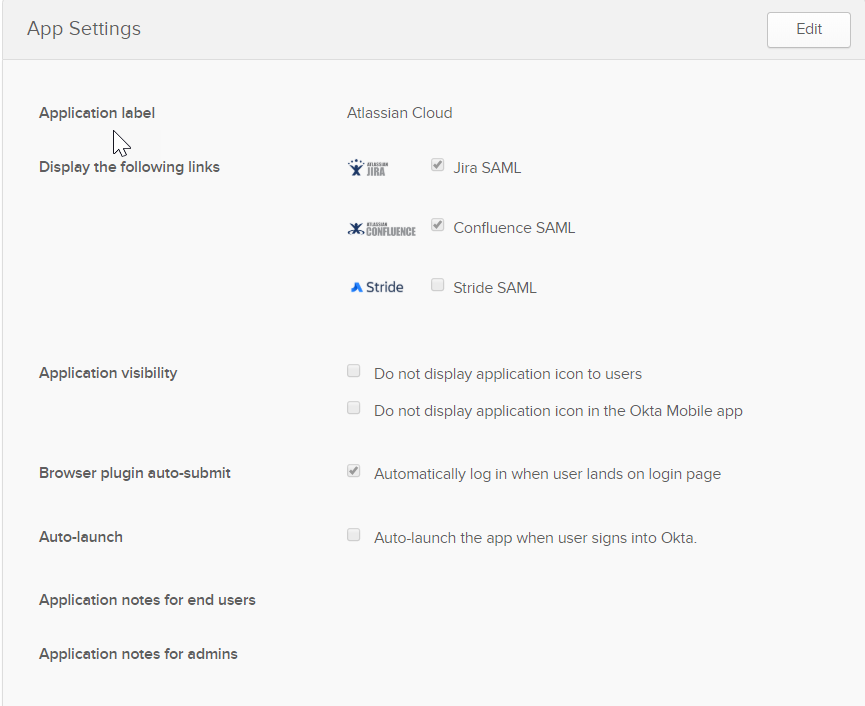
# Setup Okta for SAML single sign-on

**Step 1:** Log into your Okta account to add Atlassian Cloud application. To do this, go to **Applications🡪Add Applications** as shown in the image below.

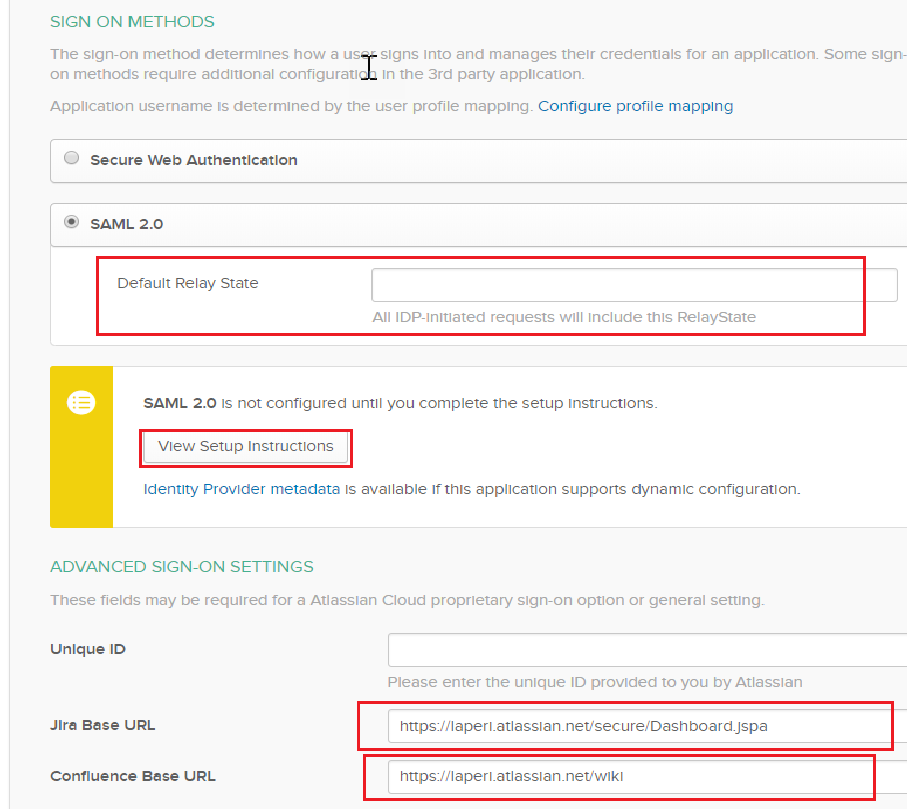
**Step 2:** Search for the Atlassian Cloud application and hit **Add**.



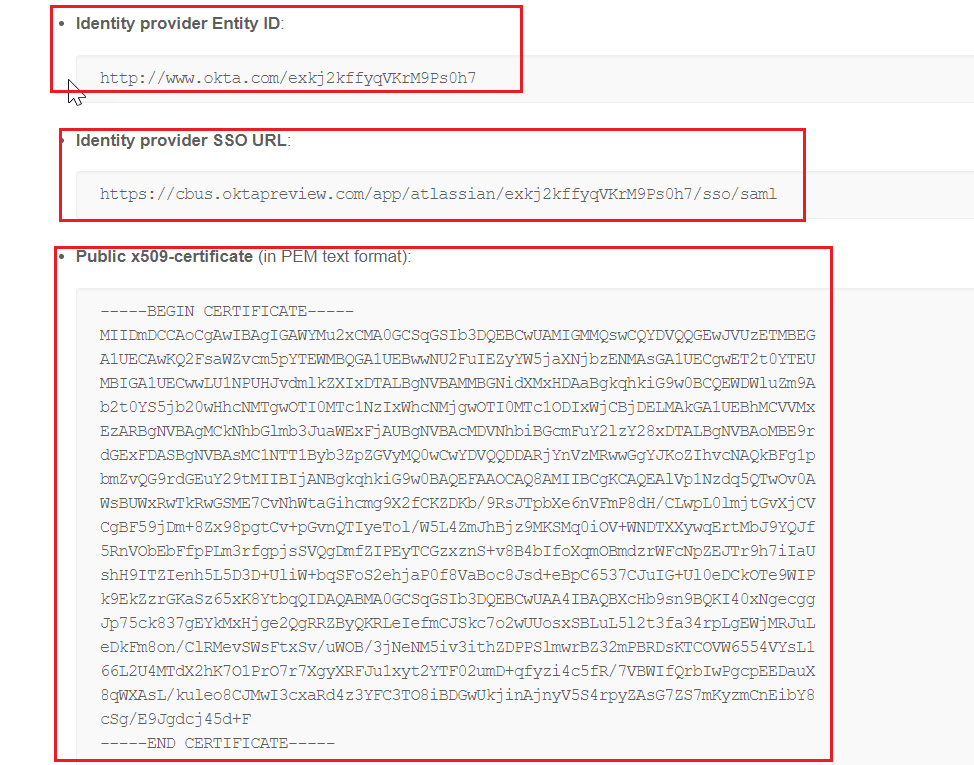
**Step 3:** Label the application appropriately, select the appropriate applications to enable SAML for, and hit **Next**.



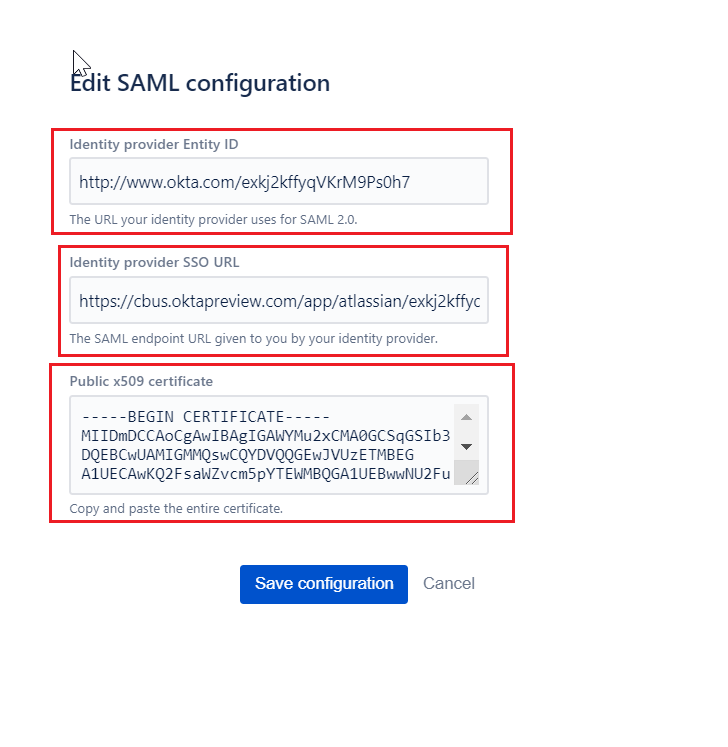
**Step 4:** In the **Sign-on Options**, choose **SAML 2.0.** Leave the **Default Relay State empty**, enter the **JIRA** and **Confluence Base URLs,** set the **Application Username Format** to **Email**, and click on **View Setup Instructions.**

****

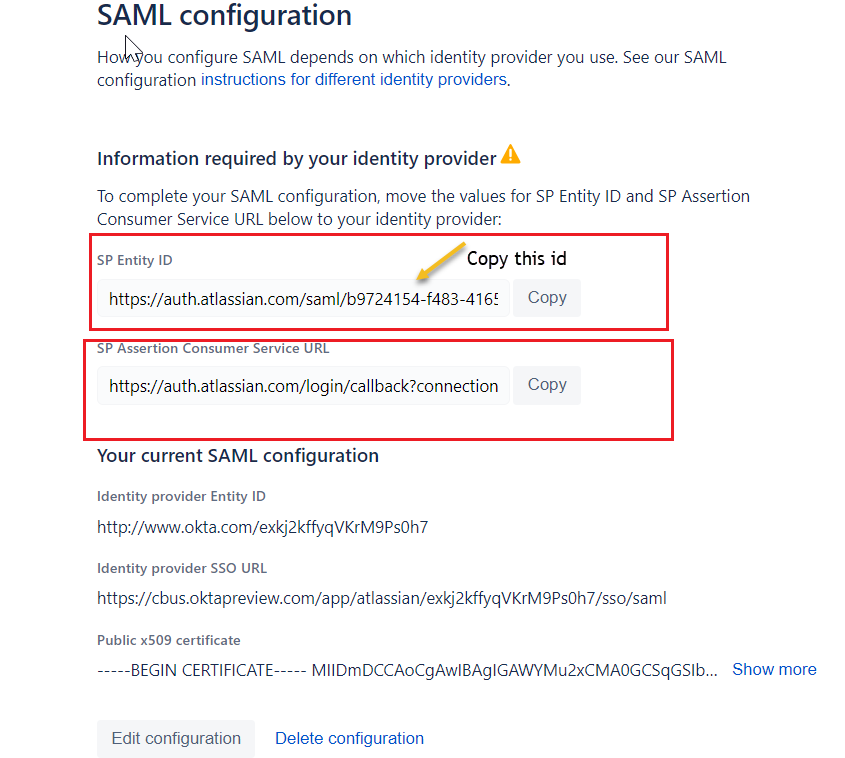
**Step 5:** Scroll to somewhere near the bottom of the Instructions page where you will see this:



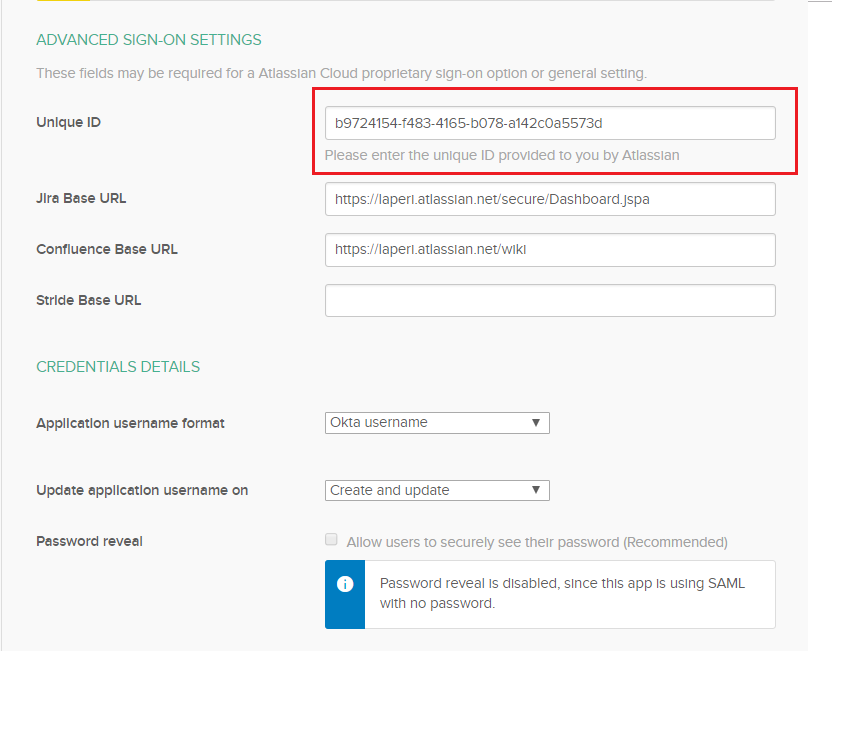
**Step 6:** Navigate back to [https://admin.atlassian.com](https://admin.atlassian.com/?__hstc=72543820.2ae543163ba30762bdb270cf4407f1cb.1548076770042.1548736517696.1548742662468.3&__hssc=72543820.1.1548742662468&__hsfp=358185139) , click on the SAML single Sign On tab, and input the information from the Okta Setup Instructions into the Atlassian screen:



**Step 7:** Hit **Save Configuration** in the Atlassian screen, and you should now see the SP Entity ID revealed. Copy the string **after** the [https://auth.atlassian.com/saml/](https://auth.atlassian.com/saml/?__hstc=72543820.2ae543163ba30762bdb270cf4407f1cb.1548076770042.1548736517696.1548742662468.3&__hssc=72543820.1.1548742662468&__hsfp=358185139) string.



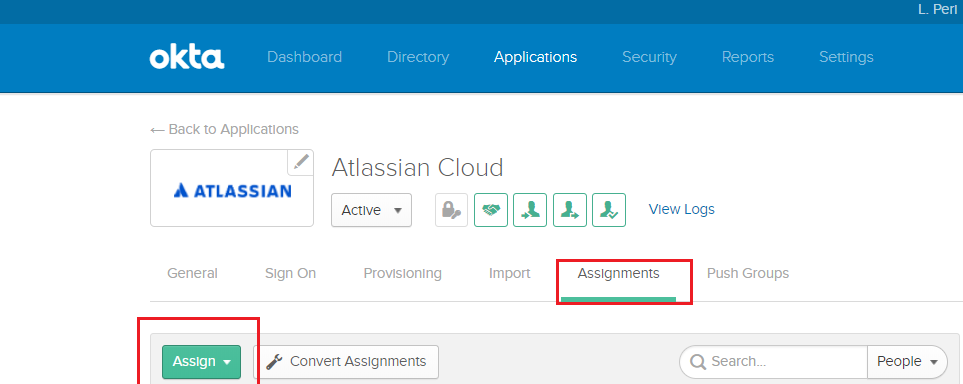
**Step 8**: Navigate back to **Okta**, into the Application configuration and paste the **Entity I**D copied earlier into the **Unique ID** field.



**Step 9:** Hit Done, and your application should be created.

## 3.1 User Assignment

* Navigate to the **Assignments** tab under the Atlassian Cloud application and click on **Assign to** **People.**



* Check the list of users you wish to be added to the application. You can also filter this by Okta groups.
* Hit Next, Confirm Assignments (check the usernames are correct).

## 3.2 Test the SAML Integration

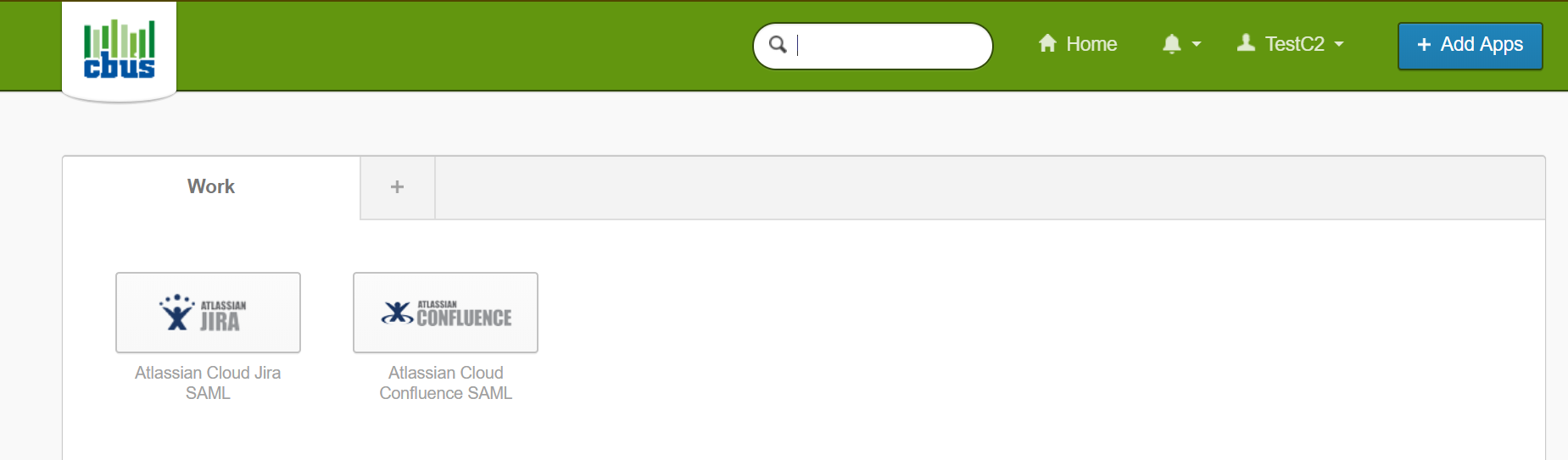
Assign the Atlassian Cloud app with SAML enabled in Okta to a test user with an email address which is domain verified in Atlassian.

**Test IDP flow:**

* Open a new incognito browser window and go to your Okta organization.
* Enter your test user's Okta credentials
* Clicking on Jira/Confluence chiclet will log you in to your Jira/Confluence site as your test user.

**Test SP flow:**

* Open a new incognito browser window and go to your Jira/Confluence tenant.
* Enter the email address of the test user you set up in Step 3, above.
* You will be redirected to Okta; entering the test user's Okta credentials will log you in to your Jira/Confluence site as your test user.
* See Troubleshooting SAML section if your testing fails.
* Once testing passes, you are ready to switch all your users to start using the new app.



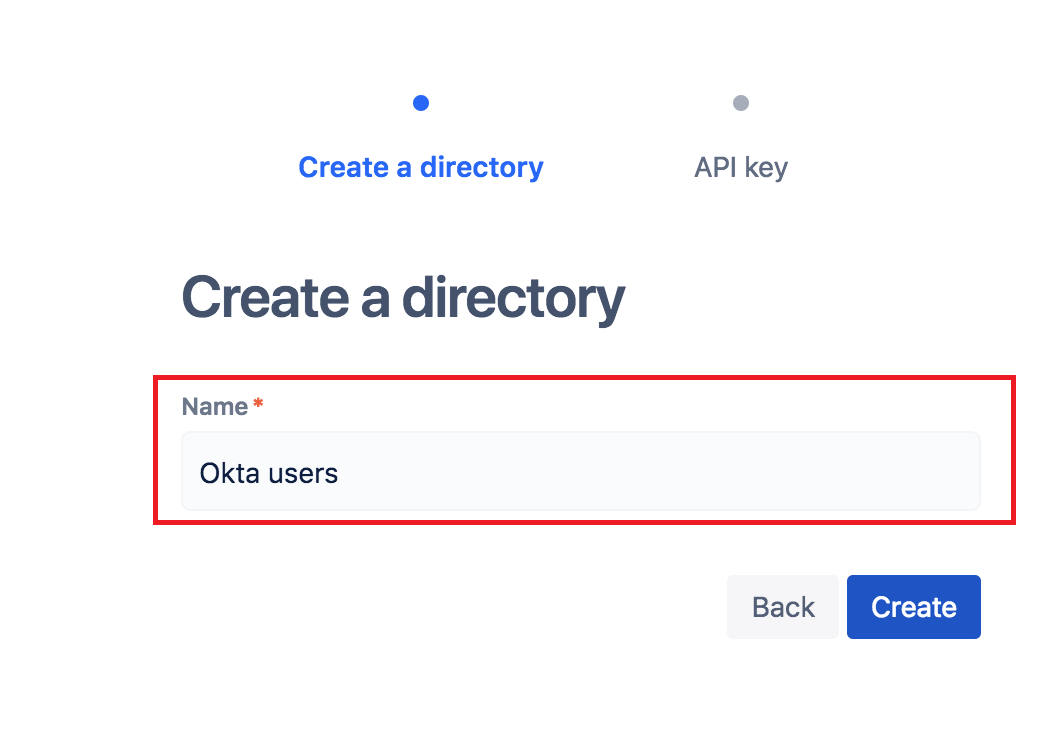
# Configure User-Provisioning with Okta

## 4.1 Create a SCIM Token in Atlassian Cloud

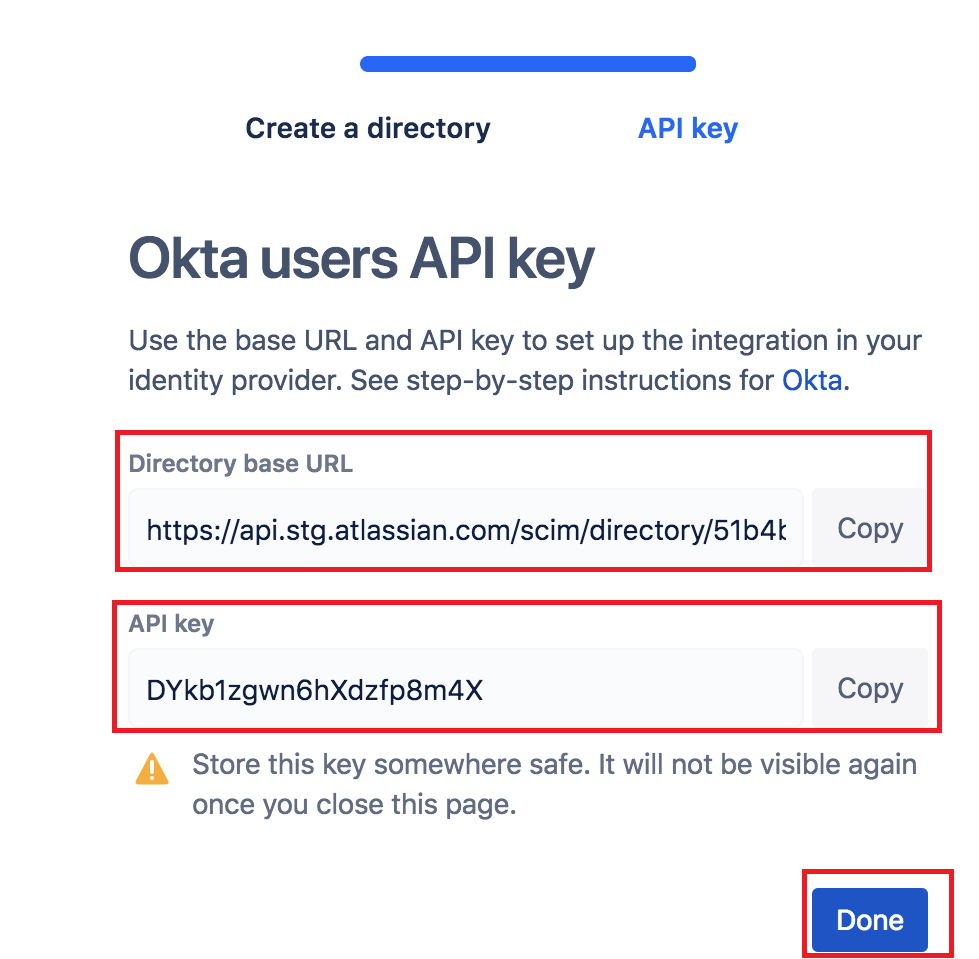
**Step 1:** Log in to [admin.atlassian.com](http://admin.atlassian.com/) and choose your **organization**.

**Step 2**: Choose **User provisioning** on the left, then click **Create directory**.

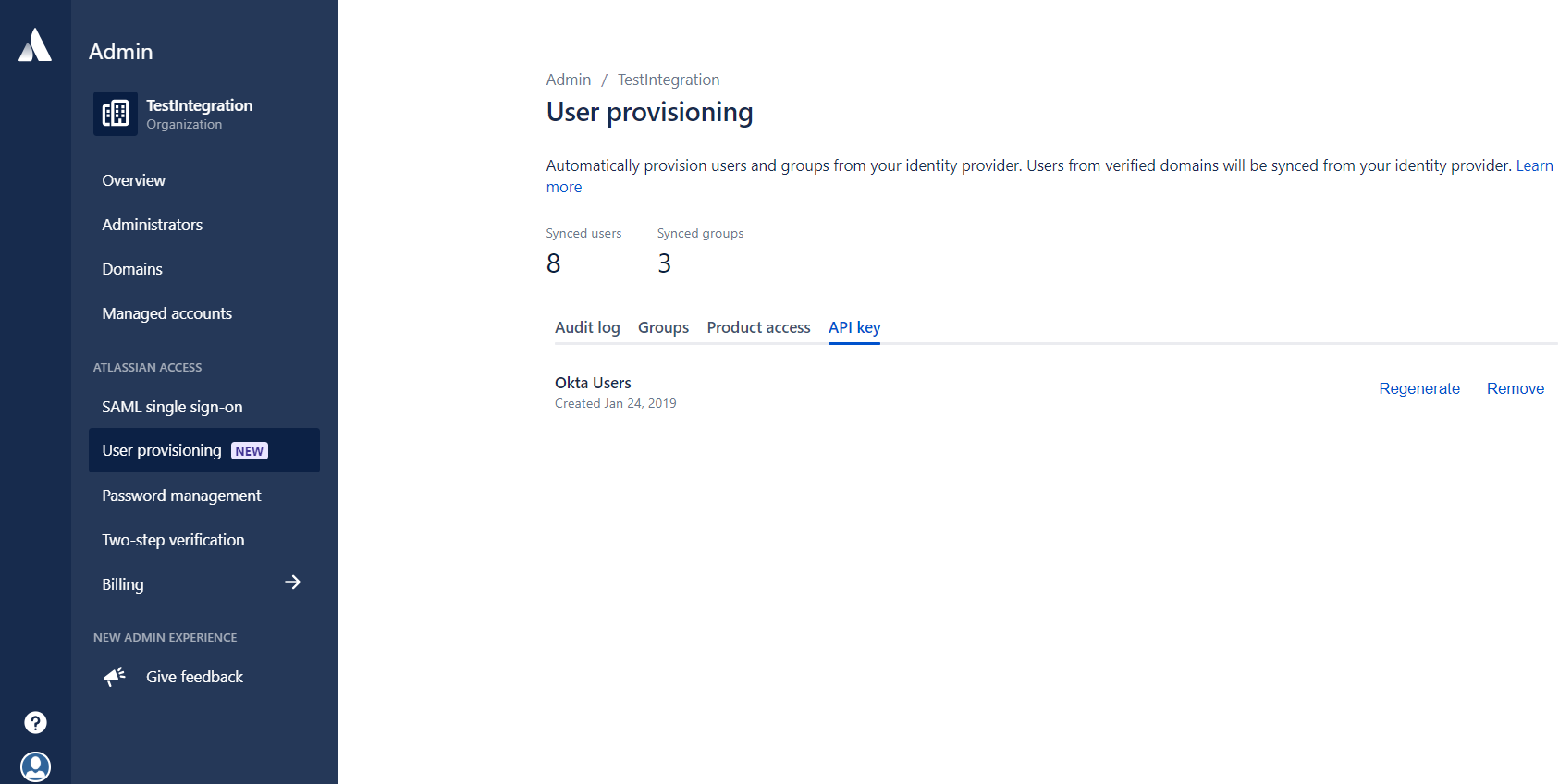
**Step 3:** Enter a name to identify the user directory, for example **Okta users**, then click **Create**.



**Step 4:** Copy the values for **Directory base URL** and **API key**. You'll need those for when you configure the Okta application later.

****

**Step 5:** Now add Jira or Confluence sites to your organization. You need to do this so that provisioned users can be granted access to the products.   
On the **'User provisioning'** page, click **Add a site**, select the site you want to add (**laperi.atlassian.net**), and follow the on-screen instructions.



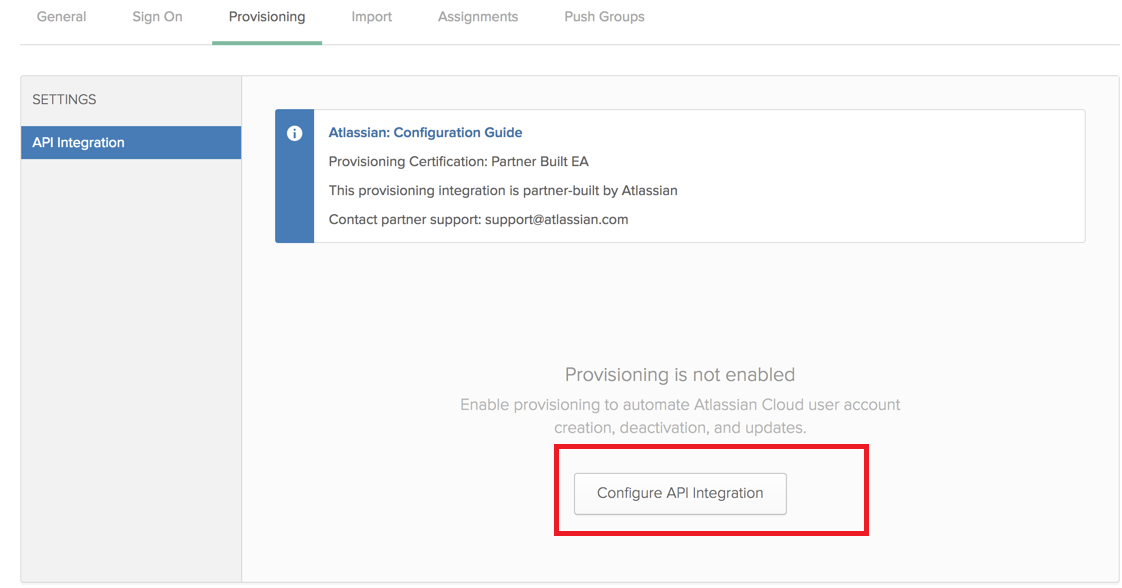
## 4.2 Configure Atlassian Cloud Application in Okta

**Note:** For this step you'll need the Directory base URL and Bearer token that you created in the 'Create a SCIM token in Atlassian Cloud' section above.

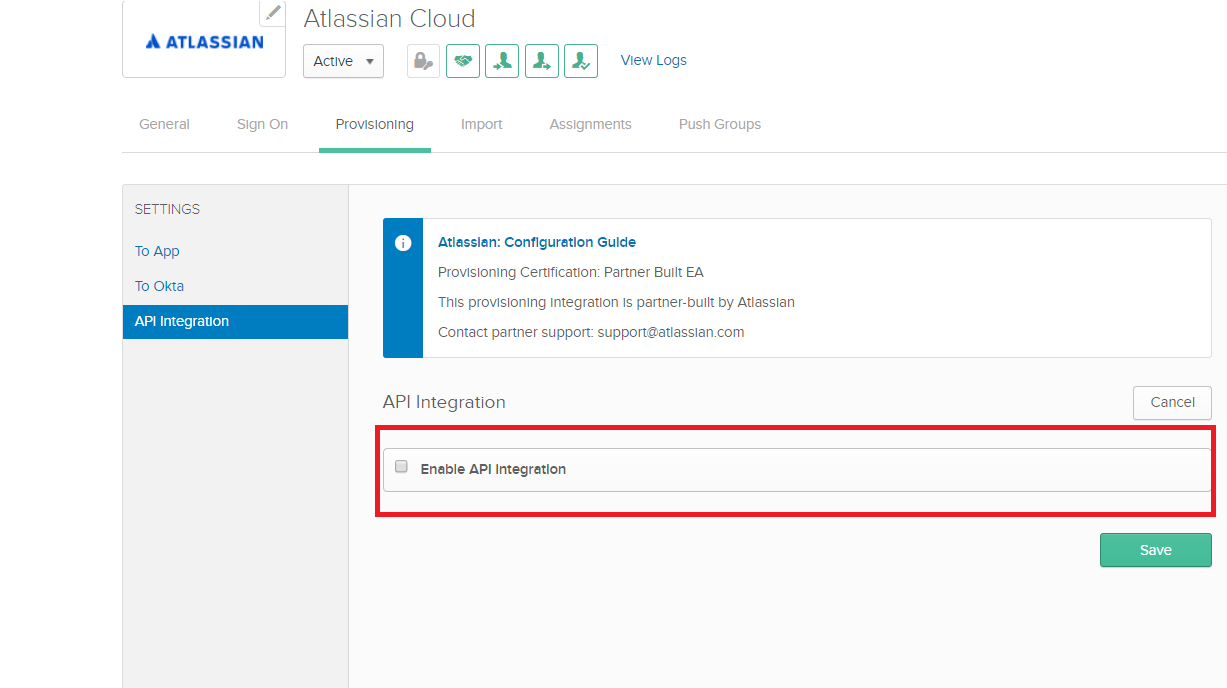
### 4.2.1 Enable SCIM API integration for user provisioning

**Step 1:** Log in to Okta and add the Atlassian Cloud application.

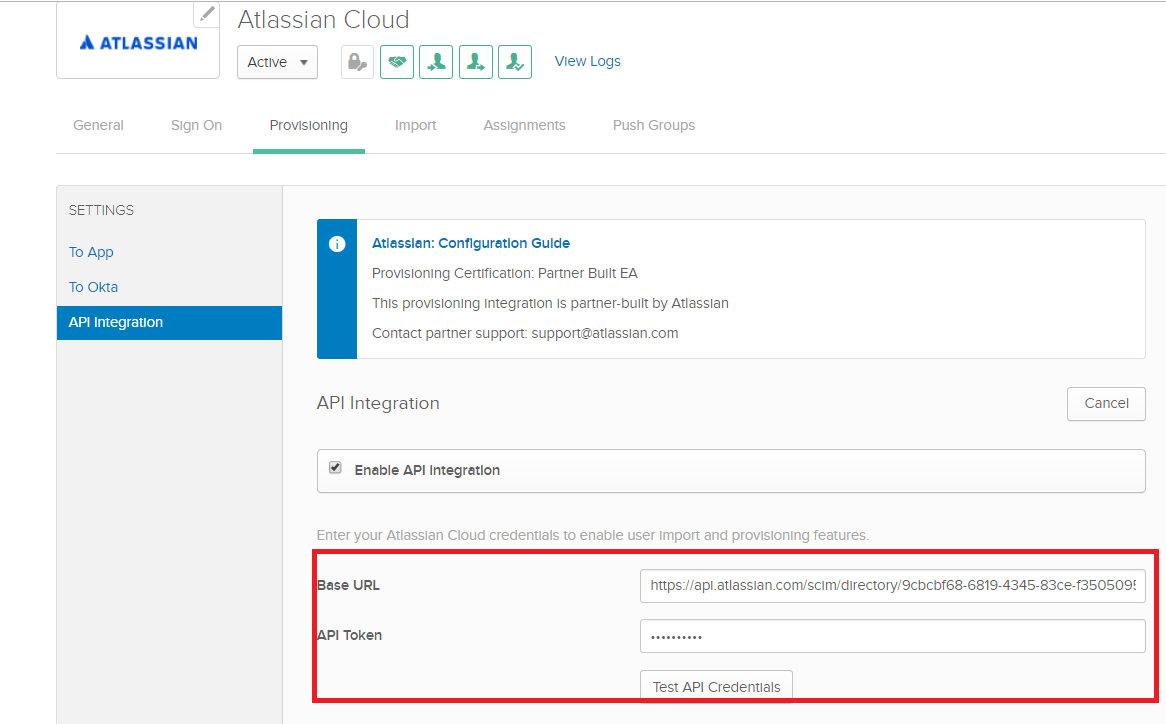
**Step 2**: In the Atlassian Cloud application, click on the **Provisioning** tab and then click **Configure API integration.**



**Step 3:** Select **Enable API integration.**

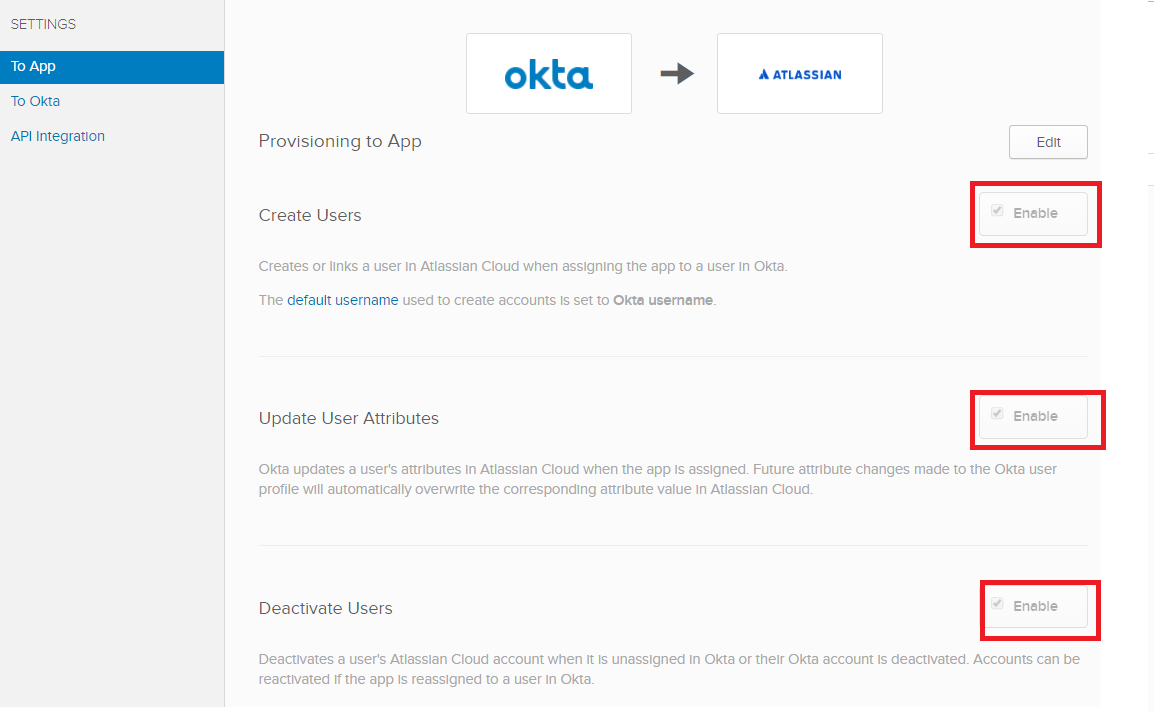


**Step 4:** Enter the **Directory base URL** and **API key** you created in your Atlassian organization.



**Step 5:** Click **Test API Credentials**. If the test passes, click **Save**.

**Step 6:** CIick on **To App** under Settings. Click **Edit** and select **Enable** for the options for **Create Users**, **Update User attributes**, **Deactivate Users**.



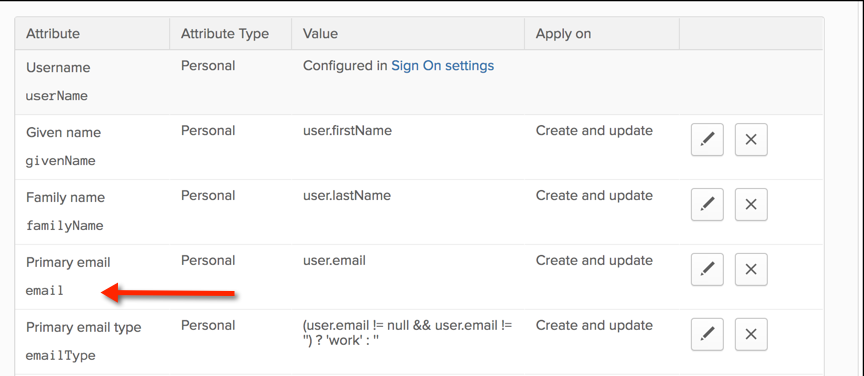
**Step 7:** Click **Save** to apply the integration settings.

### 4.2.2 Make sure the email address attribute is the same for SAML SSO and user provisioning

User provisioning uses an email address to identify a user in Atlassian Cloud and then create a new Atlassian account or link to an existing Atlassian account. As a result, if the email address attribute for a user is inconsistent between the SAML SSO setting and the SCIM user provisioning setting in the Okta app, the user could end up with duplicate Atlassian accounts.

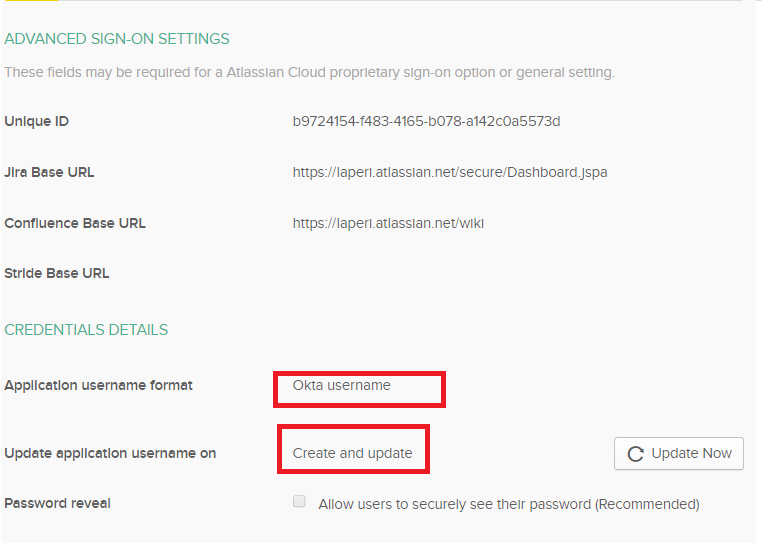
To avoid duplicate accounts, make sure the email address attribute that maps user account is the same for SAML SSO and SCIM user provisioning.

**Step 1:** From the **User** **provisioning** tab in Okta, note the field that maps to **the Primary email attribute**. The default is email, as shown in the screenshot.



**Step 2:** Click the **Sign** **on** tab. From the Credentials details section, look for the Application username format setting. Okta passes this field from a user's account as the SSO email address when creating or linking an Atlassian account.

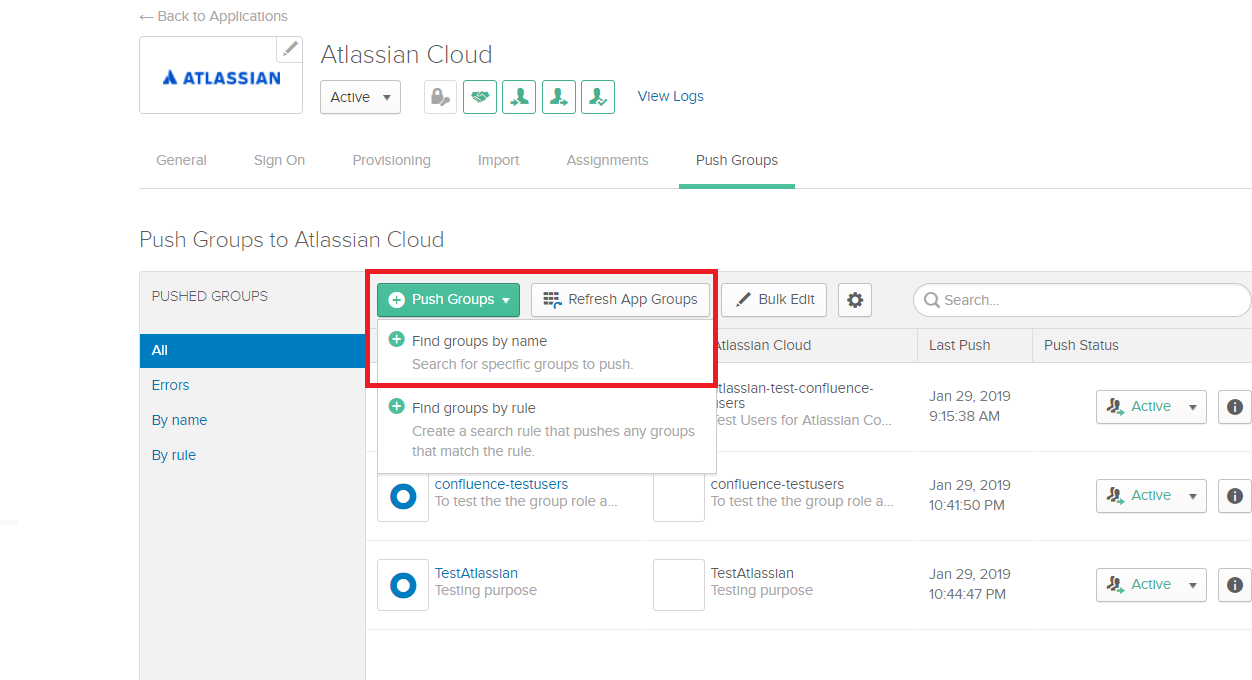
* Make sure **Application username format** is set to the same attribute specified as Primary email in the previous step.
* Make sure that **Update application username** on is set **to Create and update**. Click **Save** to apply your changes.



## 4.3 Push groups to Atlassian Cloud

This section describes how to configure group-based management.

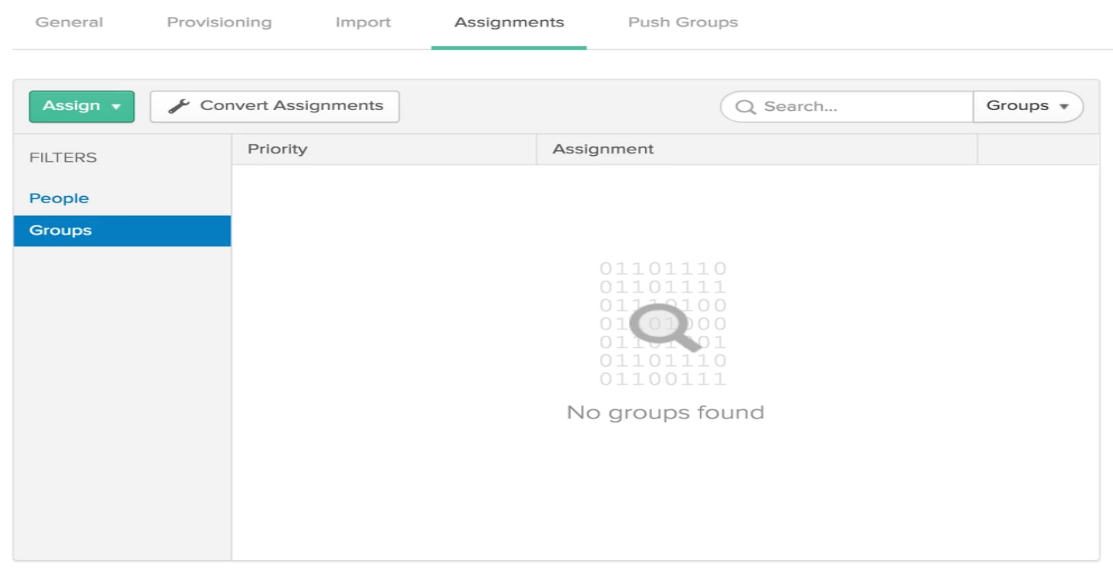
**Step 1:** In Okta, click on the **Push Groups** tab and then **By name**. Select the group name (e.g. atlassian-test-jira-users or atlassian-test-confluence-users) and click **Save**.



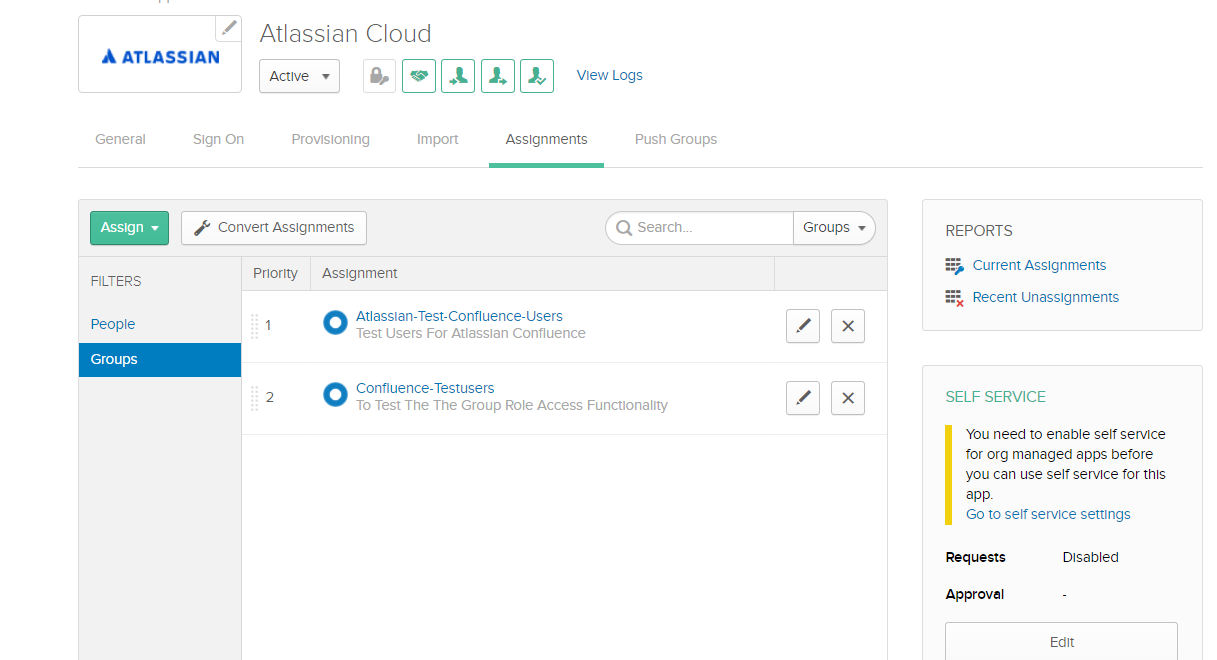
**Note:** Pushing a group does not synchronize any users. This will only push the group to Atlassian Cloud.

## 4.4 Assign users to the Atlassian Cloud application in Okta

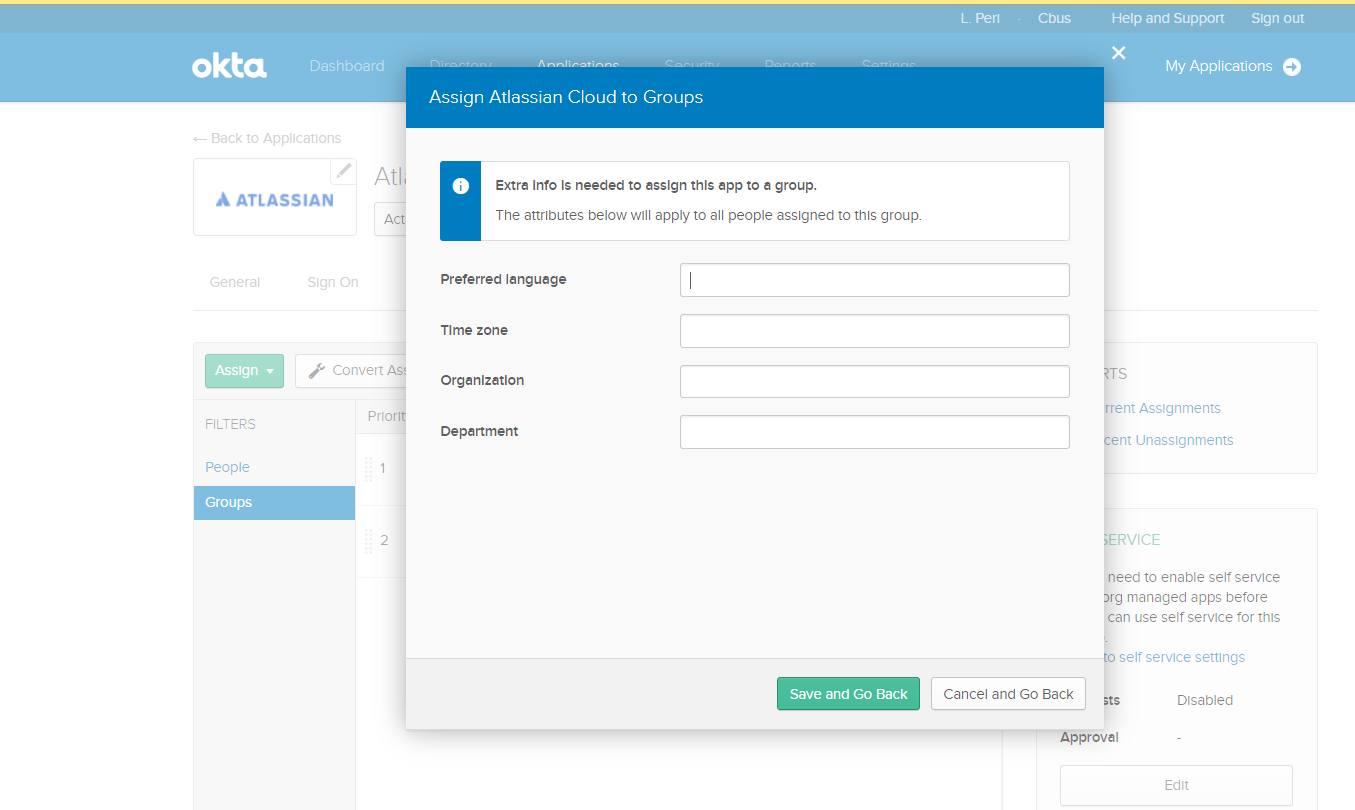
**Step 1:** In Okta, click the **Assignments** tab of the Atlassian Cloud application.



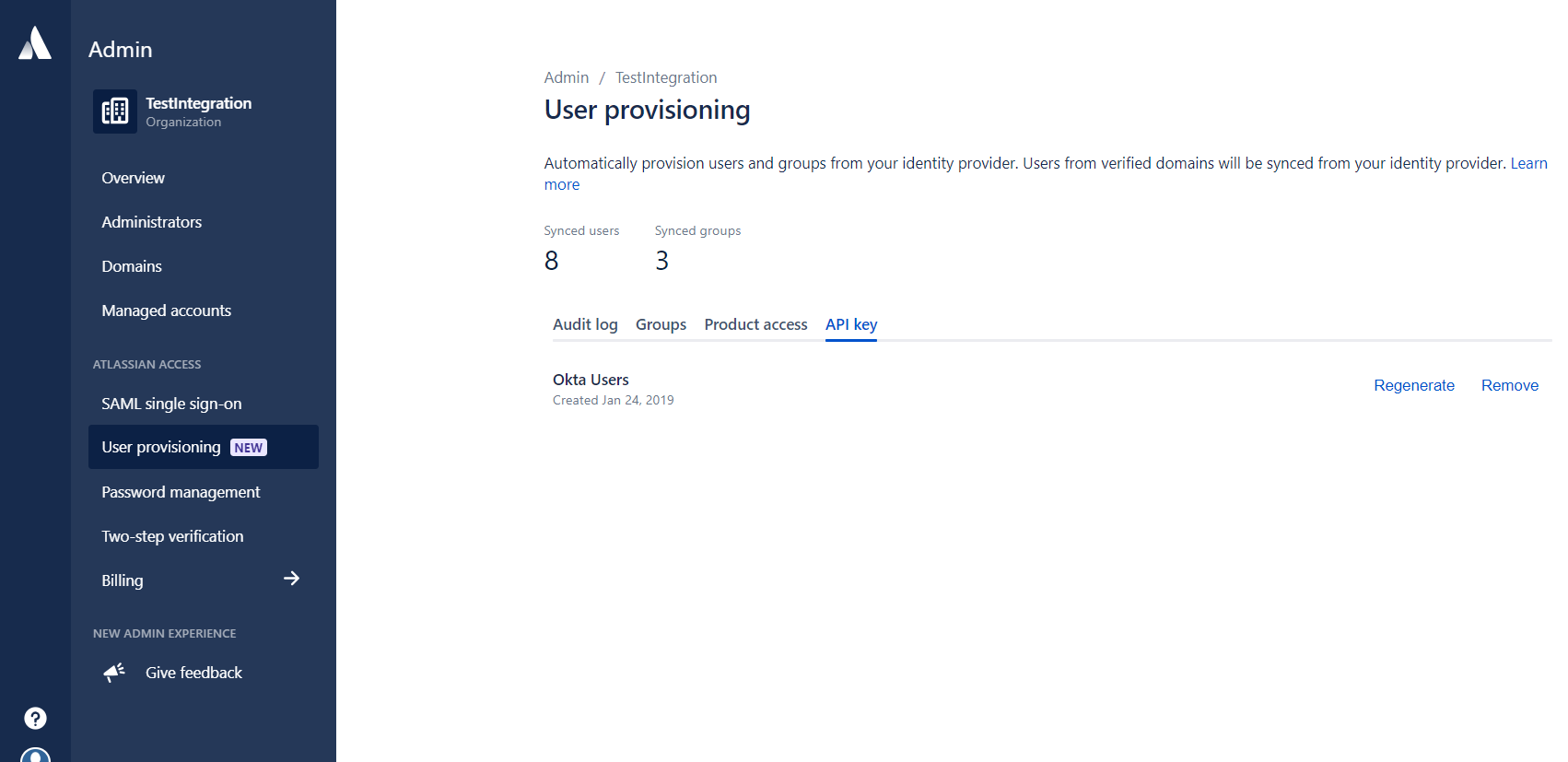
**Step 2:** Click **Assign**, then **Groups**. Select the group you'd like to assign.



**Step 3:** You'll see this dialog to set default values. These default values will be used only if the user profile does not have them set. All these fields are optional and can be left blank. When you are done with this step, click **Save and Go Back.**



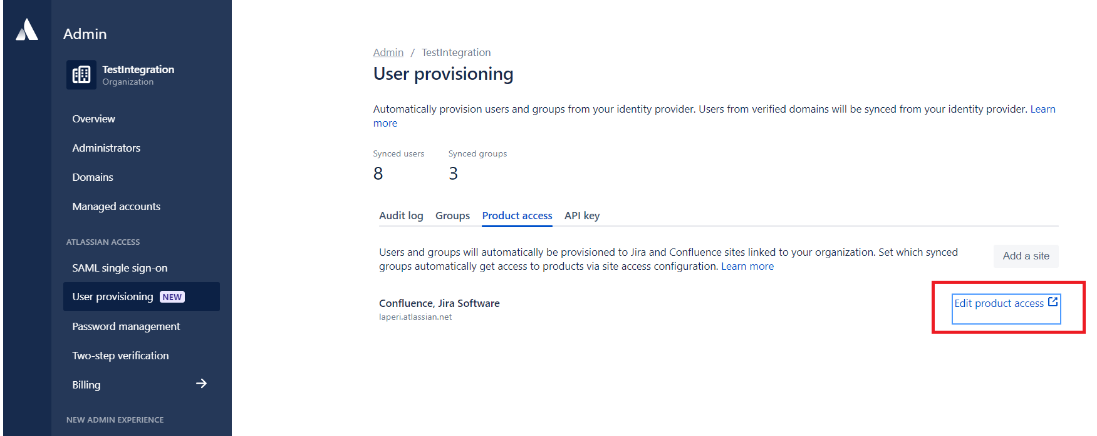
**Step 4:** Verify that users are synchronized with Atlassian Cloud. You can check either the Okta logs or the User provisioning page in the Atlassian Cloud admin area.

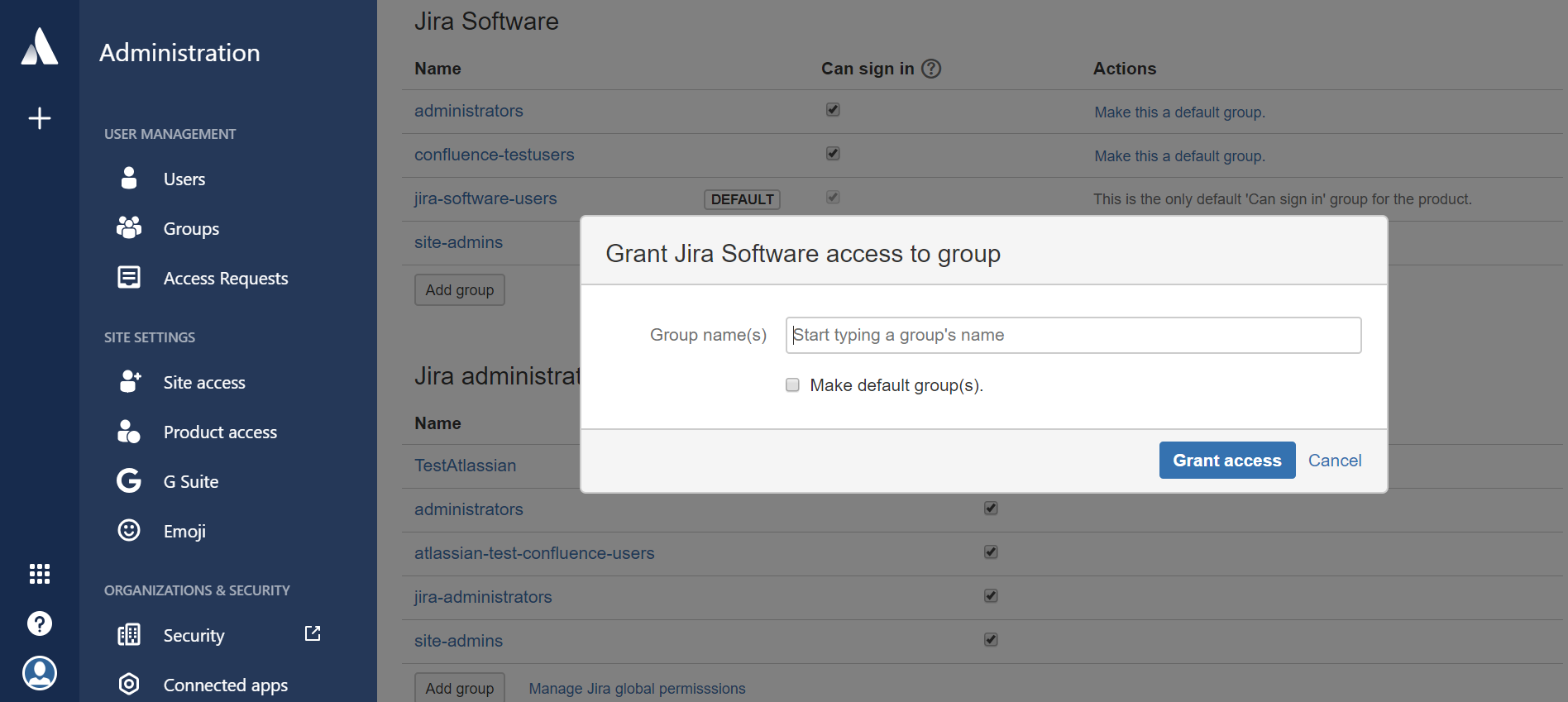


## 4.5 Configure product access for the provisioned groups and users

**Step 1:** To set up the product access any new provisioned users get granted, let's grant the product access the groups have.

In the Atlassian product site (laperi.atlassian.net) you added in 'Create a SCIM token in Atlassian Cloud' above, go to Product access in the admin area, and find the Confluence section. Click Add group and enter the name of the synchronized group. Click Grant access to confirm the change.





**Step 2:** Confirm that the group is configured for product access:

