CampusPress (Edublogs)

The following is an overview of the steps required to configure the CampusPress (Edublogs) Web application for single sign-on (SSO) via SAML.

1 **Prepare CampusPress (Edublogs) for single sign-on (see** CampusPress (Edublogs) requirements for SSO**).**

2 **In the Centrify Admin Portal, add the application and configure application settings.**

Once the application settings are configured, complete the user account mapping and assign the application to one or more roles. For details, see Configuring CampusPress (Edublogs) in Admin Portal.

3 **Configure the CampusPress (Edublogs) application for single sign-on.**

You will need to copy some settings from Application Settings in Centrify Admin Portal and paste them into fields on the CampusPress (Edublogs) website. For details, see Configuring CampusPress (Edublogs) on its web site

After you have finished configuring the application settings in the Admin Portal and the CampusPress (Edublogs) application, users are ready to launch the application from the Centrify user portal.

Preparing for Configuration

CampusPress (Edublogs) requirements for SSO

Before you configure the CampusPress (Edublogs) web application for SSO, you need the following:

- An active CampusPress (Edublogs) account with administrator rights for your organization.
- A signed certificate.

  You can either download one from Admin Portal or use your organization's trusted certificate.

Setting up the certificates for SSO

To establish a trusted connection between the web application and the Centrify Directory Service, you need to have the same signing certificate in both the application and the application settings in Admin Portal.

If you use your own certificate, you upload the signing certificate and its private key in a .pfx or .p12 file to the application settings in Admin Portal. You also upload the public key certificate in a .cer or .pem file to the web application.

What you need to know about CampusPress (Edublogs)

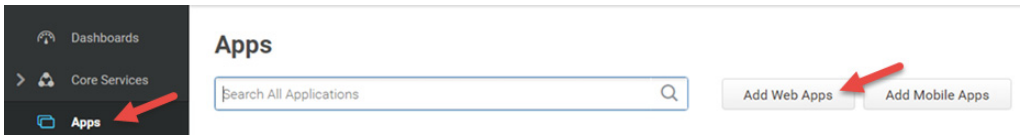
Each SAML application is different. The following table lists features and functionality specific to CampusPress (Edublogs).

Capability	Supported?	Support details
Web browser client	Yes	
Mobile client	No	
SAML 2.0	Yes	
SP-initiated SSO	Yes	
IdP-initiated SSO	No	
Force user login via SSO only	No	
Separate administrator login after SSO is enabled	No	
User or Administrator lockout risk	No	Username-password login remains available after configuration.
Automatic user provisioning	No	
Multiple User Types	Yes	SSO works the same way for all admin and non-admin user types.
Self-service password	Yes	Users can reset their own passwords. Resetting another user's password requires administrator rights.
Access restriction using a corporate IP range	Yes	You can specify an IP Range in the Admin Portal Policy page to restrict access to the application.

Configuring CampusPress (Edublogs) in Admin Portal

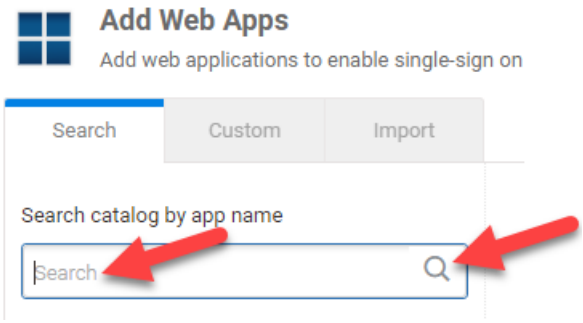
To add and configure the CampusPress (Edublogs) application in Admin Portal:

1 In Admin Portal, click **Apps**, then click **Add Web Apps**.



The Add Web Apps screen appears.

2 On the Search tab, enter the partial or full application name in the Search field and click the search icon.



3 Next to the application, click **Add**.

4 In the Add Web App screen, click **Yes** to confirm.

Admin Portal adds the application.

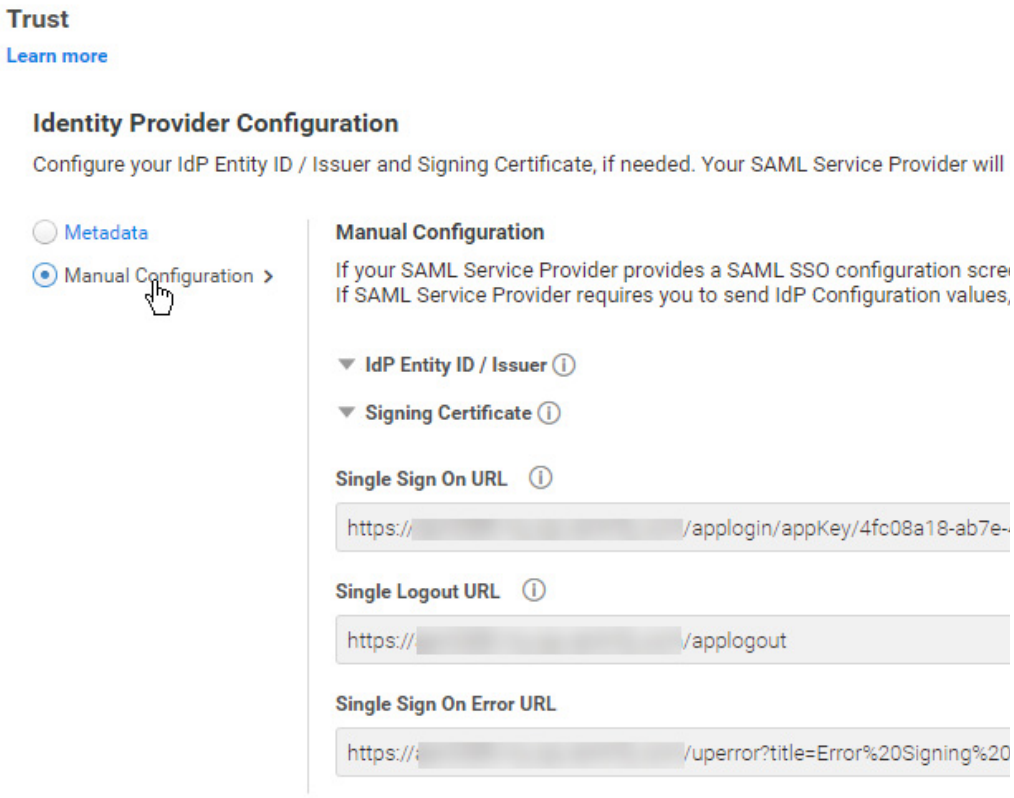
5 Click **Close** to exit the Application Catalog.

The application that you just added opens to the Settings page.

6 Click the **Trust** page to begin configuring the application.

The UI is evolving in order to simplify application configuration. For example, many of the settings previously found on the Application Settings page are now on the Trust page.

You might have to select **Manual Configuration** to expose those settings, as shown in the following example.



Any previously configured applications retain their configuration and do not require reconfiguration. If you are configuring an application for the first time, refer to the Trust page for any settings previously found on the Application Settings page.

In addition, the description of how to choose and download a signing certificate in this document might differ slightly from your experience. See Choose a certificate file for the latest information.

7 Configure the following:

Field	Set it to	What you do
Your SAML Assertion Consumer URL	The URL assigned by CampusPress (Edublogs).	Sign in to your CampusPress (Edublogs) Admin account and go to **MySites -> Network Admin -> Settings -> Single Sign-On -> General**. Then copy **Your SAML Assertion Consumer URL** and paste it here.
Your Entity ID	The Entity ID assigned by CampusPress (Edublogs).	Sign in to your CampusPress (Edublogs) Admin account and go to **MySites -> Network Admin -> Settings -> Single Sign-On -> General**. Then copy **Your Entity ID** and paste it here.

8 Copy your **URL to IdP Metadata**. You will need this URL when Configuring CampusPress (Edublogs) on its web site.

9 Click **Download Signing Certificate**. Open the downloaded file in a text editor.

10 (Optional) On the **Settings** page, click **Enable Derived Credentials for this app on enrolled devices (opens in built-in browser)** to use derived credentials on enrolled mobile devices to authenticate with this application.

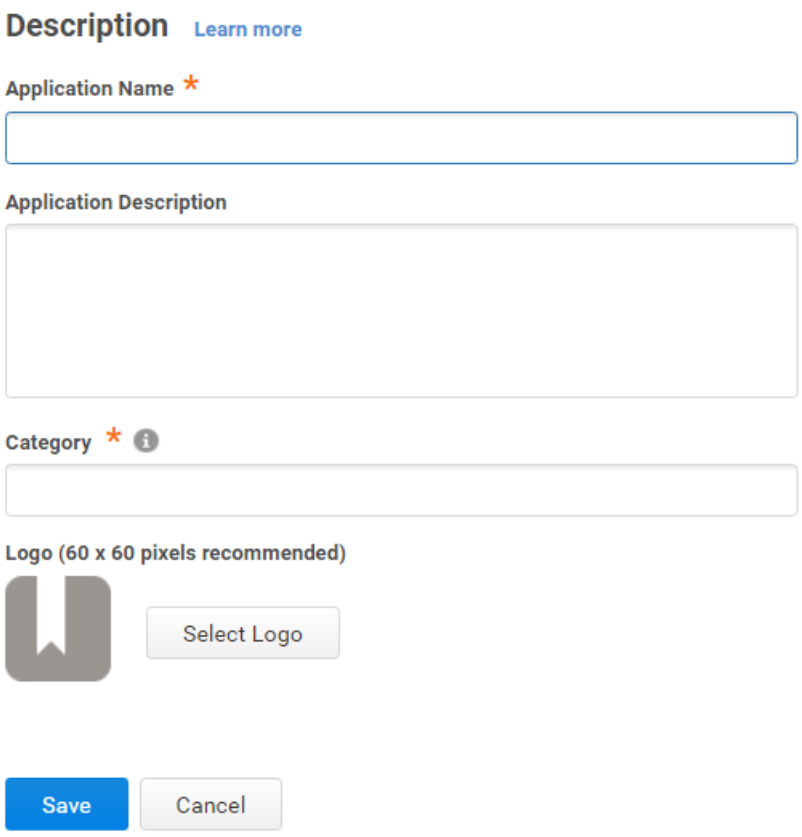
For more information, see *Derived Credentials*.

11 On the **Settings** page, specify the following settings:

Option	Description
Category	Specifies the default grouping for the application in the user portal. Users have the option to create a tag that overrides the default grouping in the user portal.
Application ID	Configure the Application ID field if you are deploying a mobile application that uses the Centrify mobile SDK, for example mobile applications that are deployed into a Samsung KNOX version 1 container. The Centrify Directory Service uses the Application ID to provide single sign-on to mobile applications. Note the following: • The Application ID has to be the same as the text string that is specified as the target in the code of the mobile application written using the mobile SDK. If you change the name of the web application that corresponds to the mobile application, you need to enter the original application name in the Application ID field. • There can only be one SAML application deployed with the name used by the mobile application. The Application ID is case-sensitive and can be any combination of letters, numbers, spaces, and special characters up to 256 characters.

Option	Description
Show in User app list	Specifies whether this web application displays in the user portal. By default, this option is selected.
On enrolled mobile devices, open this application in the built-in browser (required for derived credentials)	Allows the use of derived credentials on enrolled mobile devices to authenticate with this application. For more information, see *Derived Credentials*.

12 (Optional) On the **Settings** page, you can change the name, description, and logo for the application. For some applications, the name cannot be modified.



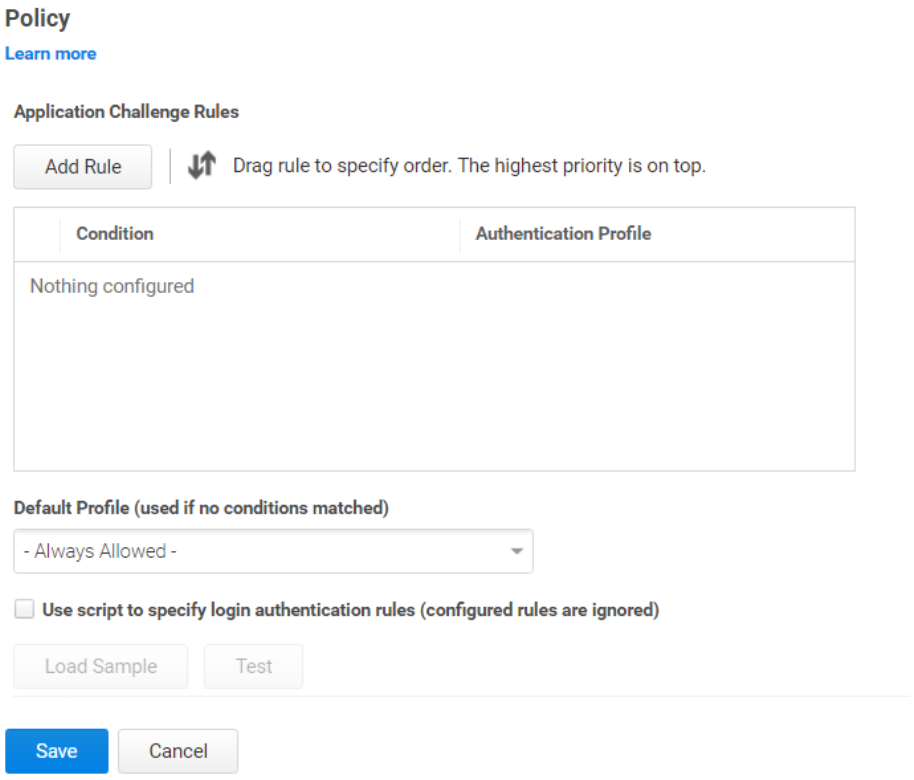
The Category field specifies the default grouping for the application in the user portal. Users have the option to create a tag that overrides the default grouping in the user portal.

13 On the **User Access** page, select the role(s) that represent the users and groups that have access to the application.

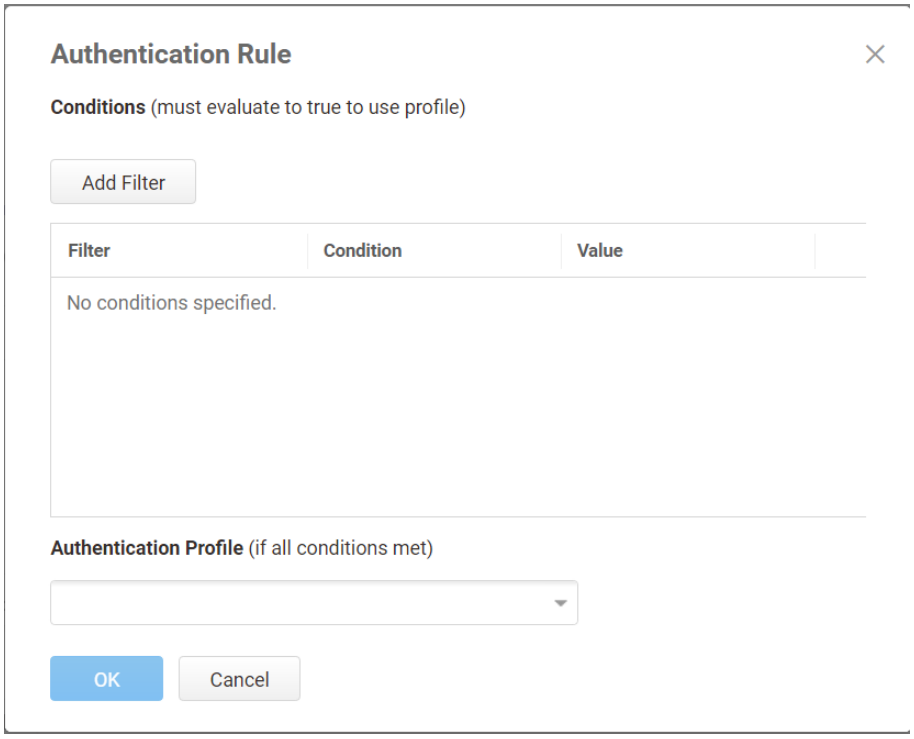
When assigning an application to a role, select either **Automatic Install** or **Optional Install**:

- Select **Automatic Install** for applications that you want to appear automatically for users.
- If you select **Optional Install**, the application doesn't automatically appear in the user portal and users have the option to add the application.

14 (Optional) On the **Policy** page, specify additional authentication controls for this application.



a Click **Add Rule**.
The Authentication Rule window displays.



b Click **Add Filter** on the Authentication Rule window.

c Define the filter and condition using the drop-down boxes.
For example, you can create a rule that requires a specific authentication method when users access the Centrify Directory Service from an IP address that is outside of your corporate IP range. Supported filters are:

Filter	Description
IP Address	The authentication factor is the computer's IP address when the user logs in. This option requires that you have configured the IP address range in Settings, Network, Corporate IP Range.
Identity Cookie	The authentication factor is the cookie that is embedded in the current browser by the directory service after the user has successfully logged in.
Day of Week	The authentication factor is the specific days of the week (Sunday through Saturday) when the user logs in.
Date	The authentication factor is a date before or after which the user logs in that triggers the specified authentication requirement.
Date Range	The authentication factor is a specific date range.
Time Range	The authentication factor is a specific time range in hours and minutes.
Device OS	The authentication factor is the device operating system.
Browser	The authentication factor is the browser used for opening the Centrify Identity Services user portal.

Filter	Description
Country	The authentication factor is the country based on the IP address of the user computer.
Risk Level	The authentication factor is the risk level of the user logging on to user portal. For example, a user attempting to log in to Centrify Identity Services from an unfamiliar location can be prompted to enter a password and text message (SMS) confirmation code because the external firewall condition correlates with a medium risk level. This Risk Level filter, requires additional licenses. If you do not see this filter, contact Centrify Identity Services support. The supported risk levels are: • Non Detected -- No abnormal activities are detected. • Low -- Some aspects of the requested identity activity are abnormal. Remediation action or simple warning notification can be raised depending on the policy setup. • Medium -- Many aspects of the requested identity activity are abnormal. Remediation action or simple warning notification can be raised depending on the policy setup. • High -- Strong indicators that the requested identity activity is anomaly and the user's identity has been compromised. Immediate remediation action, such as MFA, should be enforced. • Unknown -- Not enough user behavior activities (frequency of system use by the user and length of time user has been in the system) have been collected.
Managed Devices	The authentication factor is the designation of the device as "managed" or not. A device is considered "managed" if it is managed by Centrify Identity Services, or if it has a trusted certificate authority (CA has been uploaded to tenant).
For the Day/Date/Time related conditions, you can choose between the user's local time and Universal Time Coordinated (UTC) time.	

d Click the **Add** button associated with the filter and condition.

e Select the profile you want applied if all filters/conditions are met in the **Authentication Profile** drop-down.
The authentication profile is where you define the authentication methods. If you have not created the necessary authentication profile, select the **Add New Profile** option. See Creating authentication profiles.

f Click **OK.**

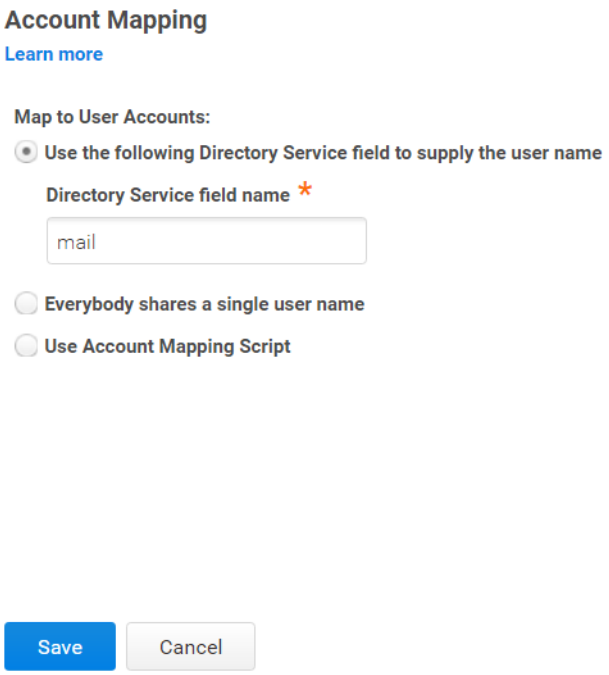
g (Optional) In the **Default Profile (used if no conditions matched)** drop-down, you can select a default profile to be applied if a user does not match any of the configured conditions.
If you have no authentication rules configured and you select **Not Allowed** in the **Default Profile** dropdown, users will not be able to log in to the service.

h Click **Save**.
If you have more than one authentication rule, you can prioritize them on the **Policy** page. You can also include JavaScript code to identify specific circumstances when you want to block an application or you want to require

additional authentication methods. For details, see Application access policies with JavaScript.

Note If you left the Apps section of Admin Portal to specify additional authentication control, you will need to return to the Apps section before continuing by clicking **Apps** at the top of the page in Admin Portal.

15 On the **Account Mapping** page, configure how the login information is mapped to the application's user accounts.



The options are as follows:

- **Use the following Directory Service field to supply the user name**: Use this option if the user accounts are based on user attributes. For example, specify an Active Directory field such as *mail* or *userPrincipalName* or a similar field from the Centrify Directory.
- **Everybody shares a single user name**: Use this option if you want to share access to an account but not share the user name and password. For example, some people share an application developer account.
- **Use Account Mapping Script**: You can customize the user account mapping here by supplying a custom JavaScript script. For example, you could use the following line as a script:

```
LoginUser.Username = LoginUser.Get('mail')+'.ad';
```

The above script instructs the Centrify Directory Service to set the login user name to the user's mail attribute value in Active Directory and add '.ad' to the end. So, if the user's mail attribute value is Adele.Darwin@acme.com then the Centrify Directory Service uses Adele.Darwin@acme.com.ad. For more information about writing a script to map user accounts, see the SAML application scripting.

16 (Optional) On the **SAML Response** page, you can edit the script that generates the SAML assertion, if needed. In most cases, you don't need to edit this script. For more information, see the SAML application scripting.

17 (Optional) On the **Changelog** page, you can see recent changes that have been made to the application settings, by date, user, and the type of change that was made.

18 (Optional) Click **Workflow** to set up a request and approval work flow for this application.

The Workflow feature is a premium feature and is available only in the Centrify Identity Services App+ Edition. See Configuring Workflow for more information.

19 Click **Save**.

Configuring CampusPress (Edublogs) on its web site

To configure the CampusPress (Edublogs) application on its web site:

1 In your web browser, go to the following URL and sign in:
`https://<your_subdomain>.campuspress.com`

2 Go to **My Sites > Network Admin > Settings > Single Sign On > Identity Provider**.

3 Copy the **URL to IdP Metadata** from the Application Settings page in Admin Portal and paste it in the **URL to IdP Metadata** field.

4 Click **Fetch Metadata**.

The fields in the **Enter IdP Info Manually** section are updated with the information from the Metadata URL.

5 Click **Update Options**.

6 Go to the **Service Provider** tab.

7 In the **Authentication** section, locate **NameID Policy** and select the **emailAddress** option.

8 Under **Attributes**, configure the following:

Field	Set it to
Attribute to be used as a username	userPrincipalName
Attribute to be used as a First Name	givenName
Attribute to be used as a Last Name	sn
Attribute to be used as E-mail	mail
Attribute to be used as Groups	memberOf

9 (Optional) Configure Groups using information provided by CampusPress (Edublogs) If you want to use a particular group for all SSO users signing in from Centrify, you must configure the attribute value for "memberOf" in Admin Portal. To do this, follow these steps:

a In Admin Portal, go to the CampusPress (Edublogs) SAML application **Advanced** page.

b Locate the line of script:
`setAttribute('memberOf', "");`

c Replace the empty string with your group value configured in CampusPress (Edublogs).

d Click **Save**.

10 Click **Update Options**.

11 Go to **My Sites > Network Admin > Settings > General Settings**.

12 Make sure the option **Enable SAML authentication** is checked.

13 For **Set SAML authentication button text**, enter "`Single Sign-On via Centrify.`"

14 Click **Update Options**.

15 (Optional) To configure the CampusPress (Edublogs) application for automatic provisioning, see CampusPress (Edublogs) provisioning.

CampusPress (Edublogs) provisioning

SCIM (System for Cross-domain Identity Management) is an open standard for automating the exchange of user identity information between identity domains, or IT systems. It can be used to automatically provision and deprovision accounts for users in external systems such as your custom SAML app. For more information about SCIM, see www.simplecloud.info.

If your application supports SCIM, you can set it up to enable provisioning by entering the Access Token and SCIM URL.

For more information about provisioning your app, see Setting up generic SCIM provisioning.

For more information about CampusPress (Edublogs)

Contact CampusPress (Edublogs) for more information about configuring CampusPress (Edublogs) for SSO.

• • • • • •