



[Previous - Export Data](#) | [Back to General Menu](#) | [Next - Virtual Sign-In](#)

## SAML 2.0 Single Sign-On



This new feature to authenticate users using the SAML protocols for SSO to simplify passwords management and increase security that will allow your students to login to Accudemia from your college portal rather than a separate webpage/URL should be relatively easy to setup in Accudemia. And here's how:

### Configuring Accudemia


1. Login to your school's <https://<mycollege>.accudemia.net> website using your domain in place of the <mycollege> and admin credentials provided.

A screenshot of a login form titled "A Demo College". Below the title is the instruction "Please enter your user information." There are two input fields: "User ID:" with a placeholder "--" and "Password:". Below the password field is a link that says "Forgot your password?". At the bottom right is a green button labeled "Log In".

2. Now to enable this option, you can access the setup under **Administration > Control Panel > User Accounts** section from the left-side navigation menu.

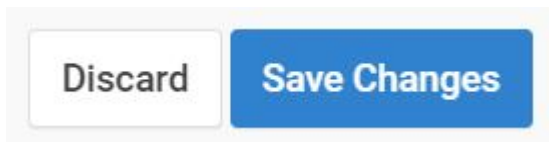
The screenshot shows the Accudemia Control Panel interface. At the top, there is a navigation bar with the 'Administration' menu highlighted, indicated by a red circle with the number 1. Below the navigation bar, the 'Control Panel' section is visible. On the left, there is a 'Jump To Section' sidebar with a search bar and a list of categories: Tracking Settings, GENERAL, WALK-INS, APPOINTMENTS, and RESTRICTIONS. The 'Tracking Settings' category is selected. In the main area, there are several tiles for different settings: General, Web Site Settings, Announcements, Email Templates, User Accounts, and Terminology. The 'User Accounts' tile is highlighted with a red box and a red circle with the number 3. A dropdown menu is open from the 'Administration' menu, showing options like User Accounts, User Groups, Sign in Stations, Surveys, Restrictions, Subject Areas, Centers & Rooms, Offtimes, Terms, Advanced, and Control Panel. The 'Control Panel' option is highlighted with a red box and a red circle with the number 2.

3. In the User Accounts page of your Accudemia website scroll down to the **SAML Single Sign-On** section. Here you'll enable SSO by checking the checkbox labeled "**Enable SAML SSO**".

 You'll need to set the **Identity Provider URL**, **Public Certificate**, and **Logout URL** to Accudemia so it knows where the users will be coming from and directed after they logout. Optionally there are other things you can do if needed too such as error page and alternate ID use (if uploaded into Accudemia specifically for SSO). Please make sure the certificate is type "PEM" [https://en.wikipedia.org/wiki/Privacy-Enhanced\\_Mail](https://en.wikipedia.org/wiki/Privacy-Enhanced_Mail) Here is an sample of this completed:

The screenshot shows the 'SAML SINGLE SIGN-ON' configuration page. On the left, there is a 'Jump To Section' sidebar with a list of categories: Account Information, Access Restrictions, Extended Profile, Communication, Accudemia Communities, and SAML Single Sign-On. The 'SAML Single Sign-On' category is selected. The main area contains the configuration form. The 'Enable SAML SSO' checkbox is checked and highlighted with a red box. Below it, there is a note: 'Turn on / off SAML single sign-on.' An 'IMPORTANT' note states: 'Once enabled, all requests to the Accudemia login page will be redirected to the IDP login URL. To use the standard login, please access https://your-account.accudemia.net/LoginForm.aspx directly.' There is a checkbox for 'Match user by alternate ID instead of the User ID' with a note: 'Check to look up for users using the Alternate ID instead of the default ID.' The 'Server URL' field is filled with 'https://caprizi.github.io/samling/samling.html' with a note: 'This is the URL of the Identity Provider. Accudemia will redirect anonymous users to this URL so that they login.' The 'Certificate Public Key' field is filled with a sample certificate: '-----BEGIN CERTIFICATE-----\nMIICPzCCAhACCQDuFX0Db5ijjDANBgkqhkiG9w0BAQsFADCBizELM\nALCA1UEBhMC\n' with a note: 'Get your identity provider's certificate and paste it here. Remember to maintain the BEGIN and END certificate delimiters.' The 'Logout URL' field is filled with 'https://www.engineerica.com' with a note: 'Users will be redirected to this URL when they logout from Accudemia.'

4. Once done completing this section please be sure to save this information at the top of the page by clicking on the **Save Changes** button.



Done! Now to test it go to your portal that you have setup for users and attempt to login using your credentials or a test user account.

## Configuring your IdP / SAML Server

To configure your Identity Provider (IdP), you need the Accudemia SAML Metadata. You can find it in:

```
"https://<your-domain>.accudemia.net/saml/metadata.aspx"
```

**NOTE:** Simply replace the <your-domain> with your domain given to you from Engineerica.

Once you have entered the metadata in your IdP, you will need to set it up to send the user ID or alternate ID in the NameID field, under the Subject tag. It's important to note that the NameID doesn't have to an attribute, but the tag that's defined under the Subject node/tag in the XML. If you look at the SAML authentication request, it should look like this:

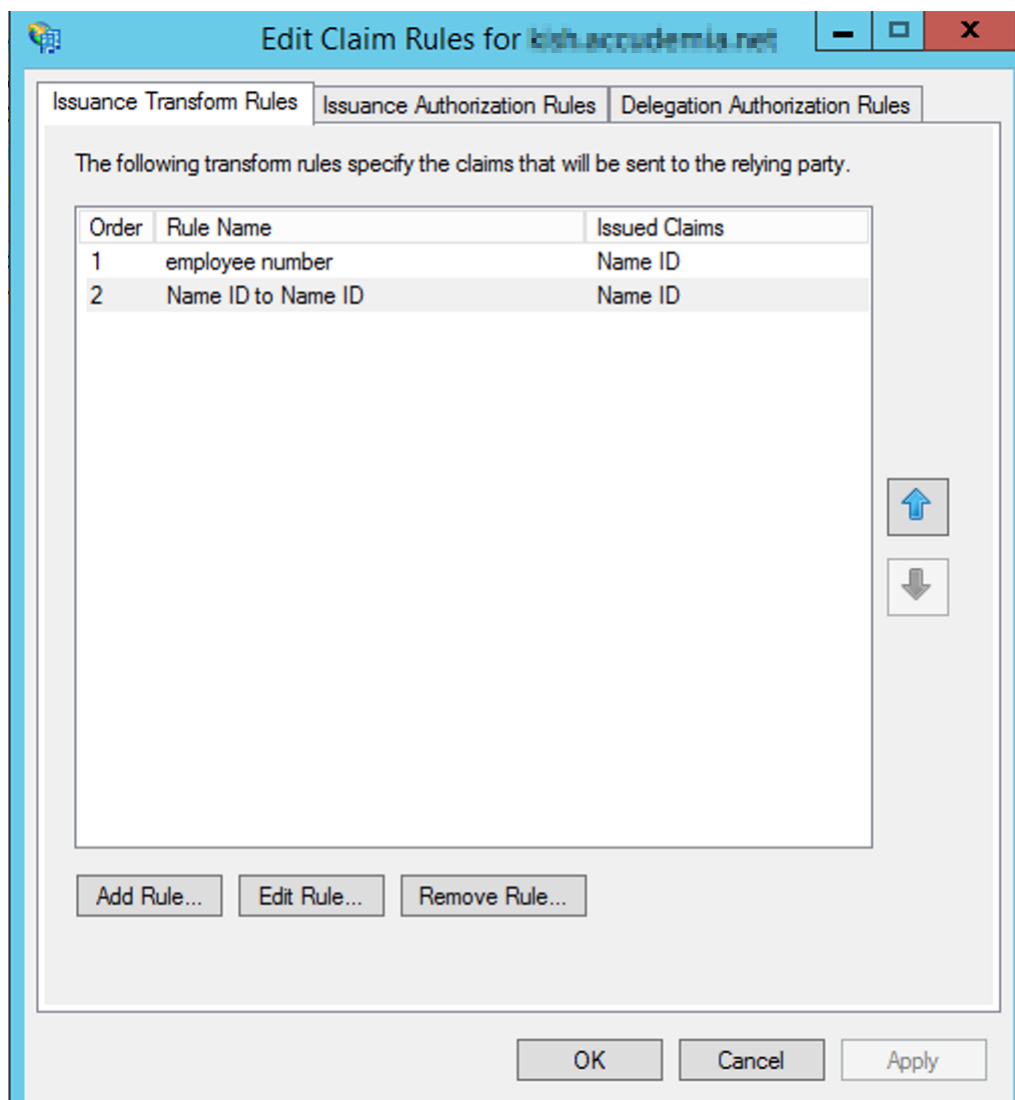
```
1. <saml:Subject>
2.   <saml:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-
   format:unspecified">111-11-1111</saml:NameID>
3.   ...
4. </saml:Subject>
```

## Configuring Active Directory Federation Services (ADFS)

In order to send the NameID in the Subject tag, you need to go to AD FS Management, navigate to Trust Relationships > Claims Provider Trusts, then right-click on your provider and select *Edit Claim Rules*:



Then click Add Rule and add the following rules:



First, to send the LDAP attribute as a claim, create a rule of type "Send LDAP Attributes as Claims". Set the attribute you want to use to authenticate from your AD. For example, the Employee Number:



Then, create a second rule. This time, select "Transform an Incoming Claim". in another rule transform the NameID to the Subject:



For more information you can also checkout this video:

[Configuring Claims Provider and Relying Party Trusts in Windows Server 2012](#)

For any questions regarding this new feature, please contact our support team at [support@accudemia.com](mailto:support@accudemia.com) or simply [Submit a Ticket](#) on this site.

From:

<http://www.attendance-tracking.com/docs/> - **Engineerica Documentation**

Permanent link:

<http://www.attendance-tracking.com/docs/doku.php/accudemia/7/it-staff/manual/sso>

Last update: **2022/02/18 14:01**

