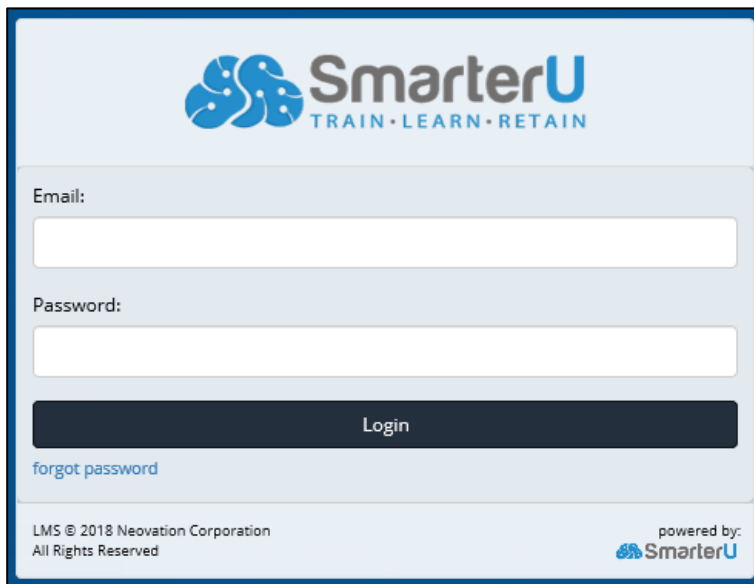


# Configuring SmarterU for Single Sign-On

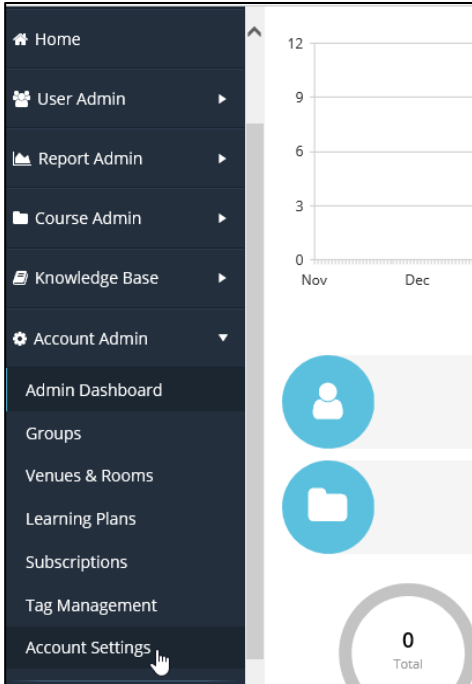
Configuring SmarterU for SSO enables administrators to manage their users using Citrix Gateway service. Users can securely log on to SmarterU using their enterprise credentials.

To configure SmarterU for SSO through SAML, follow the steps below:

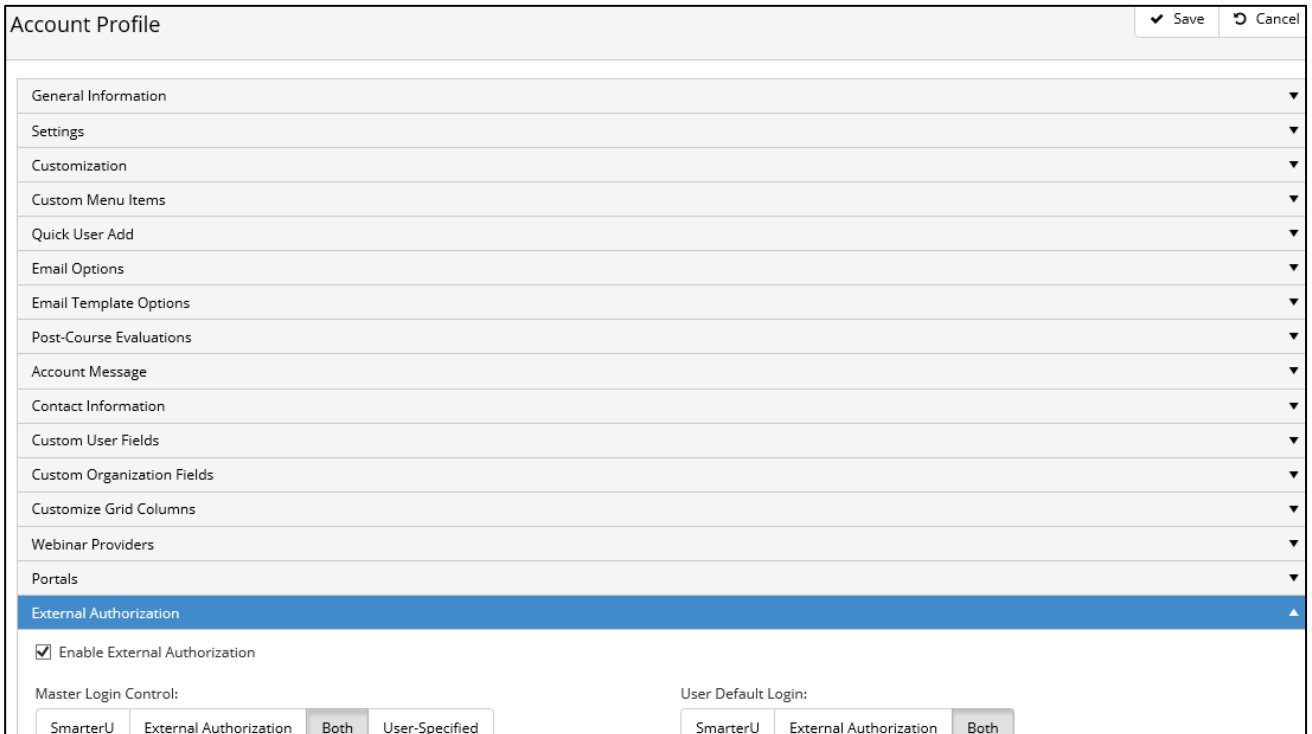
1. In a browser, type the URL, `http://<companyname>.smarteru.com/remote-login/login.cfm` and press **Enter**.
2. Type the credentials and click **Login**.

The image shows a login form for SmarterU. At the top, there is the SmarterU logo with the tagline "TRAIN · LEARN · RETAIN". Below the logo, there are two input fields: "Email:" and "Password:". A dark blue "Login" button is positioned below the password field. A link for "forgot password" is located below the login button. At the bottom left, it says "LMS © 2018 Neovation Corporation All Rights Reserved". At the bottom right, it says "powered by: SmarterU" with the SmarterU logo.

3. On the Home page, under Account Admin, click **Account Settings**.



4. In the Account Profile page, click **External Authorization**.



5. In the External Authorization section, specify the following details:

- i. **Enable External Authorization:** Select to enable authorization.
- ii. **Master Login:** Select **Both**.
- iii. **User Default Login:** Select **Both**.
- iv. **Login URL:** Enter the IdP URL, SAML 2.0 endpoint, for example, <https://example.com/saml/login>
- v. **Customize Login Button Text:** Enter the text for Login button. This is used to log in with SSO.
- vi. **Customize Portal Login Button Text:** Enter the text for Portal Login button. This is used to log in to the default application.
- vii. **Enable SAML:** Select to enable SAML 2.0.
- viii. **IDP Metadata:** Enter the IDP metadata.
- ix. **Identifier Attribute/Claim:** From the drop-down list, select **Name ID**.
- x. **Identifier Type:** Click **Email**.

The SAML configuration is saved.