

SAML Authentication Security Enhancements

Download the PDF of this article.

In this Article

Related Articles

Overview

What's new

Security alerts are now displayed within your SAML settings to help identify configurations that should be reviewed as part of stricter validation.

You may see critical errors (red) in your SAML configuration when settings require attention. These alerts do not necessarily mean authentication is currently failing, but they should be reviewed to help ensure continued and secure access.

What you should do

If you are an Account Admin

Account admins can review SAML security issues across all users and forms on the instance from a single page in the Admin Dashboard.

1. Go to the **Admin Dashboard** and navigate to **Forms > Security Issues**, or go directly to:
<https://xxxxx.tfaforms.net/admin/forms/security-issues>
 - Replace "xxxxx" with your FormAssembly subdomain.
2. Review the list of flagged forms.
 - The table displays the **Form Name**, **Form ID**, **Form Owner**, and **Issues**. Hover over the listed issue to view more information about the issue identified for each flagged form.
3. Click **Review Config** to view the SAML configuration details.
4. Work with the form owner to make the necessary updates, or update the configuration directly if you have access to the form.
 - **Note:** To update the configuration directly, an admin must have the following permissions:
 - Allow administrator to access user's data
 - Can manage form identity providers
5. Save the configuration.

Forms with Security Issues

The following forms across your account have SAML authentication configurations with security issues such as expired certificates, deprecated certificates, or missing required fields. Each form is shown with its owner and Form ID so you can identify and follow up on non-compliant configurations.

FORM NAME	FORM ID	OWNER	ISSUES	ACTIONS
Simple SAML Authentication Test Form	389	Asuka Goya	⚠️ 2 issues	Review Config

The "Manage Identity Providers" permission (p_manage_idps) is required to modify these configurations as an admin. Without it, the SAML advanced configuration page will not be accessible.

Note: This page is only accessible to users with Admin permissions. Standard users should follow the steps in the "If you are a Standard User" section below to review their own forms.

If you are a Standard User (Form by Form Authentication)

- Go to the Forms with Security Issues page: <https://xxxxx.tfaforms.net/forms/security-issues>
 - Replace "xxxxx" with your FormAssembly subdomain name
- Review any forms flagged with issues.
- Click **Review Config** to view details and make any necessary updates.
- Save the configuration

Forms with Security Issues

The following forms have SAML authentication configurations with security issues such as expired certificates, deprecated certificates, or missing required fields. Review and fix each configuration to ensure secure access.

FORM NAME	ISSUES	ACTIONS
Application Form	⚠️ 1 issue	Review Config

Note: Consider transitioning to [shared SAML configurations](#). This allows certificates and security settings to be managed in a central location rather than updated individually for each form.

If you are using [User Login SSO](#) (Single Sign-On)

- Go to the **Admin Dashboard > Security**.
- Review any issues listed at the top of the page.
- Click **View Advanced Settings** to make any necessary updates.
- Save the configuration.

Test the SAML Configuration

You can test against the stricter validation rules and validate your setup by clicking **Test Configuration** on the SAML Configuration page.

Test SAML Configuration

Verify your SAML configuration is valid before enabling authentication for this form.

[Test Configuration](#)
