Recast

Configure the Application Workspace identity provider

Last Modified on 2026-09-28

Authentication via SAML to either the Citrix StoreFront or through the Citrix ADC requires an identity provider configured in the Application Workspace.

> Access Manager license
> The SAML identity provider is available only with a valid Access Manager license. We recommend you contact Recast Sales if the option is not available in your Application Workspace System.

Certificate

The SAML identity provider needs a signing certificate that will be used to sign the SAML messages.

1. In the Application Workspace navigate to **Manage** > **System** > **Certificates**.
2. Click ✚ **Create** in the table toolbar.
3. In the **Create certificate** dialog box that opens:
    - In **Type** select *Self signed*
    - In **Overview** write *Signing certificate for SAML IDP*
    - In **Self signed** write
        - **Common name**: SAML-IDP-SIGNING
        - **Days valid**: 1825 (5 years for example)
        - **Key size**: 2048

Identity provider

1. In the Application Workspace navigate to **Manage** > **Authentication** > **Identity Providers**.
2. Click ✚ **Create** in the table toolbar.
3. In the **Create identity provider** dialog box that opens:
    - In **Type** select *SAML 2.0*
    - In **Overview** fill in:
        - **Name**: SAML Identity Provider
        - **Description**: Identity Provider used for SAML federation
    - In **Summary**, leave **Modify identity provider after creation** selected.
4. Navigate to the **Settings** screen and configure the following:

- **Certificate used for signing SAML messages**: select the SAML-IDP-SIGNING created previously, or another appropriate certificate.
- Enable **Allow requesting metadata**
- In the **Single sign in** section enable **Allow post requests**
- In the **Single logout** section enable **Allow redirect requests**

For security purposes, we recommend you have the options **Require signing** enabled.

For more information, see SAML 2.0.