Recast

Scenario 4 StoreFront via ADC SAML integration

Last Modified on 04.20.26

This scenario describes the integration of Application Workspace with Citrix StoreFront for external application access through Citrix ADC.

> Implementing this integration requires Citrix ADC knowledge. We recommend you contact your Citrix ADC administrator to learn more about it before implementation. The scenario may vary according to the Citrix implementation.

In this scenario:

- Citrix Federated Authentication Services (FAS) is deployed and configured.

Prerequisites

- Application Workspace 3.2 or later
- A Citrix ADC 12.1.xx or later configured with a virtual server for the StoreFront
- Citrix XenApp/XenDesktop 7.9 or late
- Citrix StoreFront connector must be configured
- Citrix StoreFront must be configured for Citrix ADC (Gateway)
- Citrix Federated Authentication Service must be deployed and configured
- SAML identity provider must be configured on the Application Workspace Server
- The public certificate of the Application Workspace SAML identity provider must be exported as base 64

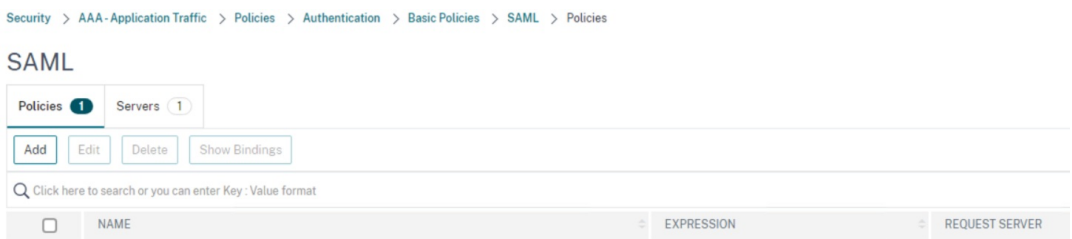
For enhanced integration, see Configure the Citrix StoreFront connector.

> 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.

ADC Configuration

The configuration steps described here are done in the web interface of the Citrix ADC.

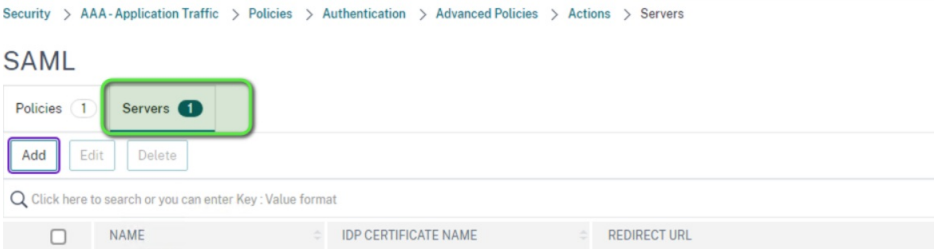
1. In Citrix ADC, navigate to **Traffic Management** > **SSL** > **Certificates** > **Server Certificates** and click **Install**.
2. Import the Application Workspace SAML identity provider public certificate into ADC.
3. Navigate to **Security** > **AAA – Application Traffic** > **Policies** > **Authentication** > **Basic Policies** > **SAML** > **Policies** tab.



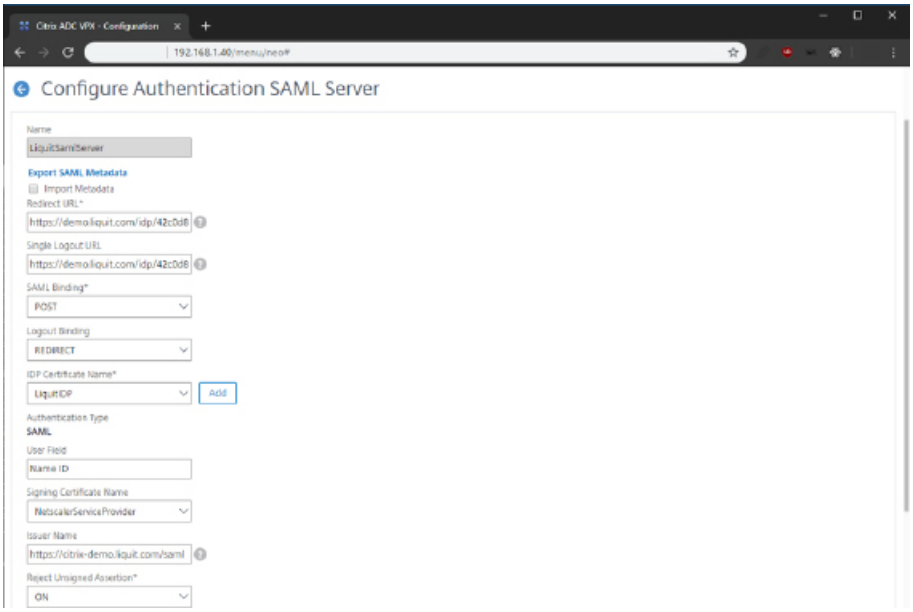
4. Add a new policy with the following parameters:
    - **Name:** RECASTSOFTWARE_IDP_POLICY

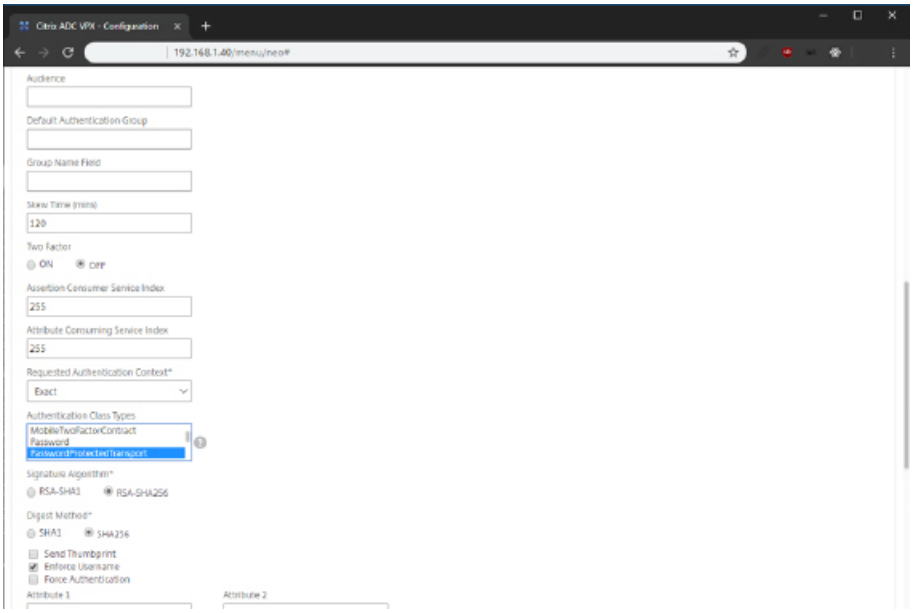
- **Expression**: ns_true

5. On the **Servers** tab, click on **Add**.



6. Configure the following parameters:
    - **Name**: RECASTSOFTWARE_IDP_SERVER
    - **Redirect URL**: https://workspace.recastsoftware.com/idp/{guid}/saml2/sso (the entity ID can be found on the Application Workspace SAML identity provider details page, followed by "sso")
    - **Single Logout URL**: https://workspace.recastsoftware.com/idp/{guid}/saml2/slo (the entity ID can be found on the Application Workspace SAML identity provider details page, followed by "slo")
    - **SAML Binding**: POST
    - **Logout Binding**: REDIRECT
    - **IdP Certificate Name**: The Application Workspace identity provider certificate that was imported
    - **Authentication Type**: SAML
    - **User Field**: Name ID
    - **Signing Certificate Name**: The Citrix ADC certificate that will be used to sign SAML requests
    - **Issuer Name**: This can be anything, for example: https://{Virtual server dns name}/saml
    - **Reject Unsigned Assertion**: ON
    - **Authentication Class Types**: Select "PasswordProtectedTransport"
    - **Signature Algorithm**: RSA-SHA256
    - **Digest Method**: SHA256





After creating the SAML Server, the metadata can be exported and used for registering the StoreFront SAML Service Provider in the Application Workspace.

If ADC version 12.1+ is being used, then the popup window that will be shown will contain a URL in the address bar that can be directly used by Application Workspace for importing the SAML metadata.

The newly created SAML policy can now be configured as the primary authentication policy on the virtual server for StoreFront.

Register the StoreFront SAML Service Provider in the Application Workspace

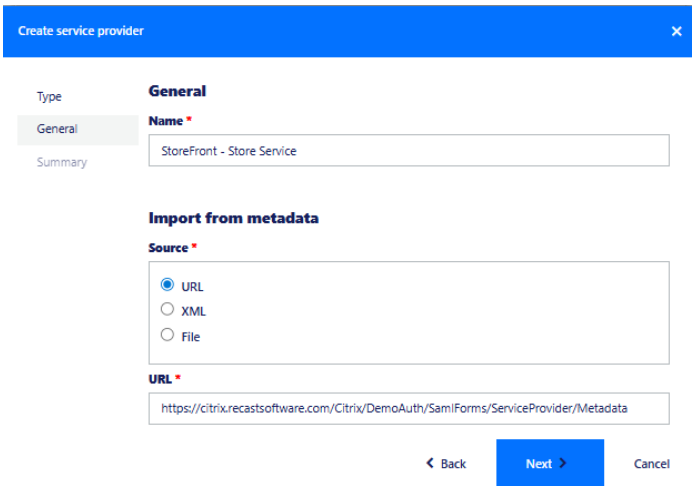
1. In the Application Workspace, navigate to **Manage** > **Authentication** > **Identity Providers** and open the desired SAML identity provider.

2. Navigate to the **Service Providers** screen and click **Create service provider**.

3. In **Type**, select *Import Service provider from Metadata*.

Recast

4. In **General**, provide a name to identify the new service provider later. For example, "ADC – Store Service". Specify the import method that is appropriate for your environment and provide the metadata source.



5. In **Summary**, leave the **Modify Service Provider after creation** checkbox selected. The service provider entry will be created and populated with the information found in the metadata.

6. Configure the name identifier on the server provider as follows:
    - **Name Identifier**: Persistent
    - **User attribute**: User principal name