

RSA Ready Citrix FAS SSO

Integrate RSA SecurID Access with Citrix XenApp and XenDesktop leveraging Citrix FAS

Peter Waranowski, RSA Partner Engineering
Last Modified: August 1st, 2018

Introduction

The Citrix Federated Authentication Service (FAS) is a privileged component designed to integrate with Active Directory Certificate Services. It dynamically issues certificates for users, allowing them to log on to an Active Directory environment as if they had a smartcard. This allows StoreFront to use a broader range of authentication options, such as RSA SecurID and SAML (Security Assertion Markup Language) assertions.

Without Citrix FAS, Citrix users authenticating with RSA SecurID or SAML must additionally present either Windows account credentials or a smartcard in order to access Citrix published resources.

Example use cases:

RSA SecurID Access SSO Agent with FAS

1. The user logs on to RSA SecurID Access SSO portal.
2. The user clicks on the Citrix NetScaler connector link and is SSOd using SAML on to NetScaler.
3. The user is then SSOd using FAS to StoreFront.

The user can now access Citrix published resources.

RSA SecurID Access SSO Agent without FAS

1. The user logs on to RSA SecurID Access SSO portal.
2. The user clicks on the Citrix NetScaler connector link and is SSOd on to NetScaler using SAML.
3. The user logs on to StoreFront using Windows account credentials or smartcard.

The user can now access Citrix published resources.

RSA SecurID Standard Agent with FAS

The user logs on to Citrix Receiver using RSA SecurID. In the background, FAS is used to SSO to StoreFront.

The user can now access Citrix published resources.

RSA SecurID Standard Agent without FAS

The user logs on to Citrix Receiver using RSA SecurID and Windows account credentials or smartcard. In the background, the Windows account credentials are used to logon to StoreFront.

The user can now access Citrix published resources.

Required Components:

Citrix NetScaler Gateway 11.0 (or newer)

Citrix StoreFront 3.6 (or newer)

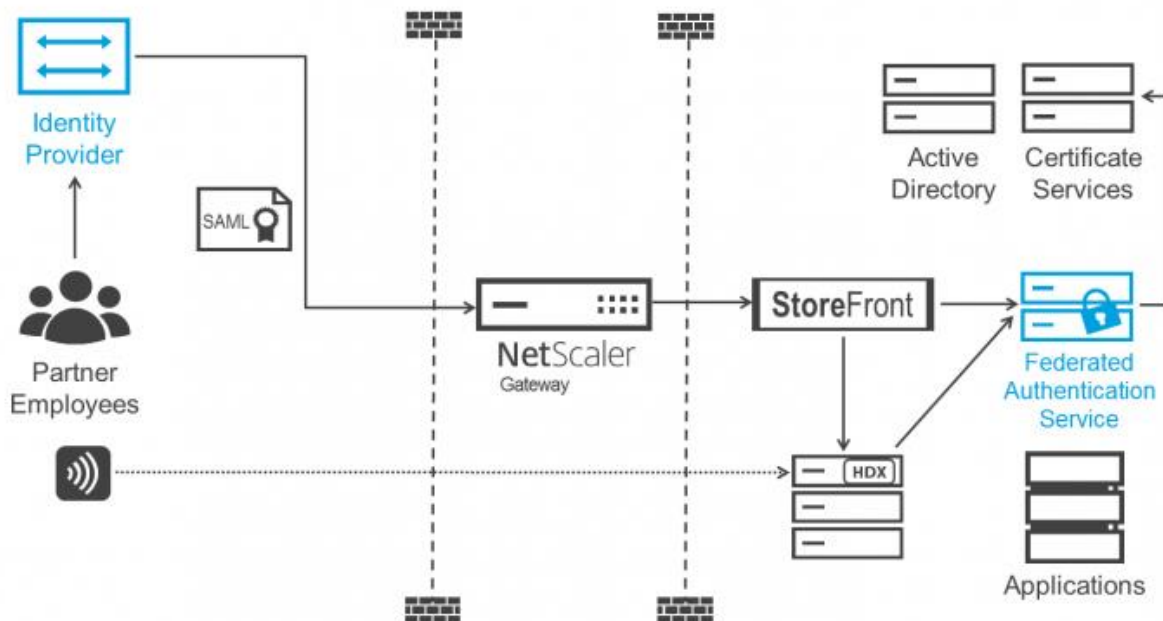
Citrix XenApp and/or XenDesktop 7.9 (or newer)

Citrix FAS (Federated Authentication Service)

Microsoft Active Directory DC

Microsoft Enterprise Certificate Authority

Note: It is recommended to first configure your Citrix deployment using AD username and password authentication prior to adding FAS and SAML or SecurID authentication.



Configuration

This document is not a step-by-step guide for configuring RSA SecurID Access with Citrix FAS. It is intended to be a supplement to existing Citrix and RSA documentation. It is expected that the reader has strong working knowledge of all components involved.

This section shows a basic configuration of Citrix NetScaler and Citrix StoreFront that is known to be compatible with RSA SecurID Standard and SSO Agents.

NetScaler

RSA SecurID Access uses Citrix NetScaler as its integration point. Follow the instructions in the appropriate RSA Ready implementation guide to configure the NetScaler Gateway authentication policy.

Authentication Policy

RSA SecurID SSO Agent -- Integrate RSA SecurID Access using a SAML authentication policy. Users must logon using a UPN formatted username. Refer to the RSA Ready implementation guide for instructions on how to integrate.

RSA SecurID Standard Agent -- Integrate with RSA SecurID using a RADIUS authentication policy. Users must logon using a UPN formatted username. This will require that SecurID users be configured with an alias that matches their AD UPNs. Refer to the RSA Ready implementation guide for instructions on how to integrate.

Session Policy

Network Configuration

The screenshot displays the Citrix StoreFront console interface. At the top, a table lists store details for 'vm2205':

Name	Authenticated	Subscription Enabled	Access
vm2205	Yes	Yes	Internal and external networks

Below this, the 'Manage Authentication Methods - vm2205' dialog is open, showing a list of authentication methods:

Method	Settings
<input checked="" type="checkbox"/> User name and password	[Settings icon]
<input type="checkbox"/> Domain pass-through <small>Can be enabled / disabled separately on Receiver for Web sites</small>	
<input type="checkbox"/> Smart card <small>Can be enabled / disabled separately on Receiver for Web sites</small>	
<input type="checkbox"/> HTTP Basic	
<input checked="" type="checkbox"/> Pass-through from NetScaler Gateway [Info icon]	[Settings icon]

A 'Configure Delegated Authentication' dialog is overlaid on top, with the following text and options:

Specify whether StoreFront fully delegates credential validation to NetScaler Gateway. This setting is applied when users log on with smart cards.

Fully delegate credential validation to NetScaler Gateway

[OK] [Cancel]

On the right side of the console, the 'Actions' pane for the 'vm2205' store is visible, listing various management tasks such as 'Create Store', 'Manage NetScaler Gateway', and 'Configure Remote Applications'.

Network Configuration

Configure NetScaler Gateway Session Profile

Name
2190

Unchecked Override Global check box indicates that the value is inherited from Global NetScaler Gateway Parameters.

Network Configuration Client Experience Security Published Applications Remote Desktop

Override Global

DNS Virtual Server
[Dropdown]

WINS Server IP
[Text Box]

Kill Connections*
OFF [Dropdown] ?

Advanced Settings

OK Close

Client Experience

Configure NetScaler Gateway Session Profile

Name
2190

Unchecked Override Global check box indicates that the value is inherited from Global NetScaler Gateway Parameters.

Network Configuration Client Experience Security Published Applications Remote Desktop

Accounting Policy
[Dropdown]

MAC Plugin Upgrade
Always [Dropdown]

Single Sign-on to Web Applications

Credential Index*
PRIMARY [Dropdown]

KCD Account
[Dropdown] [Add] [Edit]

Single Sign-on with Windows*
ON [Dropdown]

Client Cleanup Prompt*
ON [Dropdown]

Advanced Settings

OK Close

Security

Configure NetScaler Gateway Session Profile

Name
2190

Unchecked Override Global check box indicates that the value is inherited from Global NetScaler Gateway Parameters.

Network Configuration Client Experience **Security** Published Applications Remote Desktop

Override Global

Default Authorization Action*
ALLOW

Secure Browse*
ENABLED

Smartgroup

Advanced Settings

OK Close

Published Applications

Configure NetScaler Gateway Session Profile

Name
2190

Unchecked Override Global check box indicates that the value is inherited from Global NetScaler Gateway Parameters.

Network Configuration Client Experience Security **Published Applications** Remote Desktop


Override Global

ICA Proxy*
ON

Web Interface Address
m2209.pe.rsa.net/Citrix/vm2205Web

Web Interface Address Type*
IPV4

Web Interface Portal Mode*
NORMAL

Single Sign-on Domain 

Citrix Receiver Home Page

Account Services Address

OK Close

StoreFront

Enable FAS Plug-In

Run the following powershell script on the StoreFront server to enable the Federated Authentication Service plug-in.

```
Get-Module "Citrix.StoreFront.*" -ListAvailable | Import-Module
$StoreVirtualPath = "/Citrix/StoreName"
$store = Get-STFStoreService -VirtualPath $StoreVirtualPath
$auth = Get-STFAuthenticationService -StoreService $store
Set-STFClaimsFactoryNames -AuthenticationService $auth -ClaimsFactoryName
"FASClaimsFactory"
Set-STFStoreLaunchOptions -StoreService $store -VdaLogonDataProvider
"FASLogonDataProvider"
```

Configure Authentication Methods

Enable **Pass-through from NetScaler Gateway** and **Fully delegate credential validation to NetScaler Gateway** on the store on which you are enabling SSO.

The screenshot displays the Citrix StoreFront management console. A table lists the store 'vm2205' with columns for Name, Authenticated (Yes), Subscription Enabled (Yes), and Access (Internal and external networks). A 'Manage Authentication Methods' dialog box is open for the 'vm2205' store, showing a list of authentication methods: 'User name and password' (checked), 'Domain pass-through', 'Smart card', 'HTTP Basic', and 'Pass-through from NetScaler Gateway' (checked). A 'Configure Delegated Authentication' dialog box is also open, with the checkbox 'Fully delegate credential validation to NetScaler Gateway' checked. The background shows the console interface with a sidebar on the right containing 'Actions' and 'Stores' menus.

Set the StoreFront store to ignore password

Edit the following file:

```
C:\inetpub\wwwroot\Citrix\storeNameAuth\web.config
```

Change the following line from:

```
<citrixAGBasicAuthentication credentialValidationMode="password">
```

To:

```
<citrixAGBasicAuthentication credentialValidationMode="kerberos">
```

Citrix XenApp and/or XenDesktop

Set the XenApp / XenDesktop server to trust StoreFront.

To use the Federated Authentication Service, configure the XenApp or XenDesktop Delivery Controller to trust the StoreFront servers that can connect to it.

Run the following powershell script on the XenApp or XenDesktop systems:

```
Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $true
```

Citrix FAS (Federated Identity Service)

Install and configure the Federated Identity Service according the instructions at the following URL.

<http://docs.citrix.com/en-us/xenapp-and-xendesktop/7-9/secure/federated-authentication-service.html>

Microsoft Active Directory DC

No special consideration or configuration necessary.

Microsoft Enterprise Certificate Authority

The certificate authority must be installed as enterprise (rather than standalone) type or you will not be able to issue the Domain Controller and Domain Controller Authentication certificates to the DC. This is necessary in order for the end users to logon to the XenApp and/or XenDesktop server using FAS provisioned smartcards.