

CITRIX ADC - OIDC

Buypass Code

BUYPASS OPEN

Version: 1.0

Versionsdato: 18.09.2019

History of change

Version	Date	Status	Description
1.0	18.09.2019	First version	First version

Contributors

Company name	Name
Buypass AS	Georg Johansen

Table of content

- 1 Overview 4**
 - 1.1 Requirements 4
 - 1.2 Prerequisites..... 4
- 2 Integration..... 5**
 - 2.1 Step by step guide 5

1 Overview

1.1 Requirements

- Citrix ADC Advanced License with AAA feature. Minimum ADC version 11.

1.2 Prerequisites

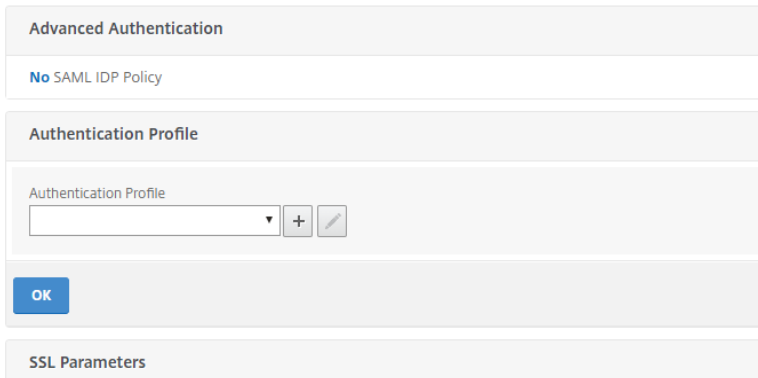
- Citrix Gateway virtual server configured and ready to add Buypass Code OpenID Connect authentication. This Gateway must be configured for browser based access e.g. Receiver for Web use.
- For use with Citrix Virtual Apps / Desktops it is required to have Citrix Federated Authentication Service (FAS) installed.
- OpenID Connect configuration acquired from Buypass.
- The user's mobile phone number is used for user account mapping in the local directory. The example in this document requires that the user's mobile phone number is stored in the AD attribute 'mobile'.

2 Integration

2.1 Step by step guide

1. Open the configuration page for the Gateway to be secured with OpenID Connect.

Choose Authentication Profile and create a new profile with the ADD (+) button.



Advanced Authentication

No SAML IDP Policy

Authentication Profile

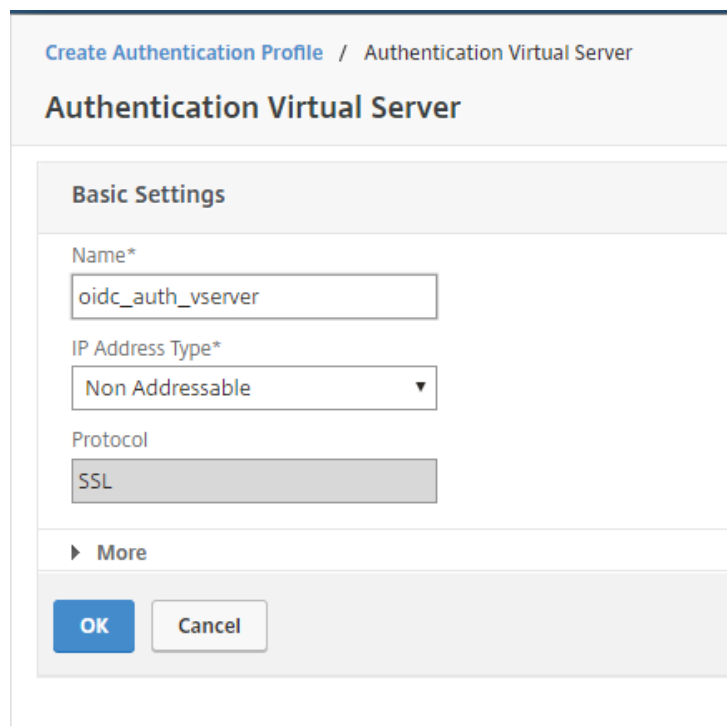
Authentication Profile

OK

SSL Parameters

2. Give the Authentication Profile a name. Press ADD (+) to create an Authentication Virtual Server.

Configure the Basic Settings. If the Authentication Virtual Server should not be reachable externally to the Citrix ADC the IP Address Type can be set to Non Addressable.



Create Authentication Profile / Authentication Virtual Server

Authentication Virtual Server

Basic Settings

Name*

oidc_auth_vserver

IP Address Type*

Non Addressable

Protocol

SSL

More

OK Cancel

3. Press No Authentication Policy.

Configure Authentication Profile / Authentication Virtual Server

Authentication Virtual Server

Basic Settings

Name **testoidc_auth_vserver**
Authentication Domain -

Advanced Authentication Policies

No Authentication Policy

No SAML IDP Policy

Done

4. Press ADD (+) on Select Policy to create an Authentication Policy.

Create Authentication Profile / Authentication Virtual Server / Policy Binding

Policy Binding

Select Policy*

Click to select > +

Binding Details

Priority*
100

Goto Expression*
NEXT

Select Next Factor

Click to select > +

Bind Close

5. Give the Authentication Policy a name. Choose Action Type to OAUTH. Set Expression to true.

The screenshot shows the 'Create Authentication Policy' configuration page. The breadcrumb navigation at the top reads: 'Create Authentication Profile / Authentication Virtual Server / Policy Binding / Create Authentication Policy'. The main title is 'Create Authentication Policy'. The form contains the following fields and controls:

- Name***: A text input field containing 'oidc_auth_policy'.
- Action Type***: A dropdown menu with 'OAUTH' selected.
- Action***: A dropdown menu with 'testoidc_oidc_action' selected, followed by a '+' button and an edit icon.
- Expression***: A section with three dropdown menus: 'Operators', 'Saved Policy Expressions', and 'Frequently Used Expressions'. Below these is a text input field containing 'true'.
- More**: A link with a right-pointing arrow.
- Buttons**: 'Create' (blue) and 'Close' (grey) buttons at the bottom.

Press ADD (+) on Action to create a new OAUTH Authentication Action.

6. Configure the OAUTH Server according to OpenID Connect configuration received from Buypass.

[Create Authentication Profile](#) / [Authentication Virtual Server](#) / [Policy Binding](#) / [Create Authentication Policy](#) / [Configure Authentication OAuth Server](#)

Configure Authentication OAuth Server

Name
testoidc_oidc_action

The status of the OAuth Server is INIT.

OAuth Implementation Type*
GENERIC

Client ID*
netscaler-demo

Client Secret*
ada6e2e31aebd941689528f5b004c5

Authorization Endpoint*
https://auth.code.bypass.no/auth/realms/bpcode/protocol/openid-connect/auth?client_id=netscaler-demo&response_type=code&scope=openid%20profile%20email

Token Endpoint*
https://auth.code.bypass.no/auth/realms/bpcode/protocol/openid-connect/token

ID Token Decrypt Endpoint
https://auth.code.bypass.no/auth/realms/bpcode/tokeninfo

Graph Endpoint

Cert Endpoint

Audience

User Name Field
preferred_username

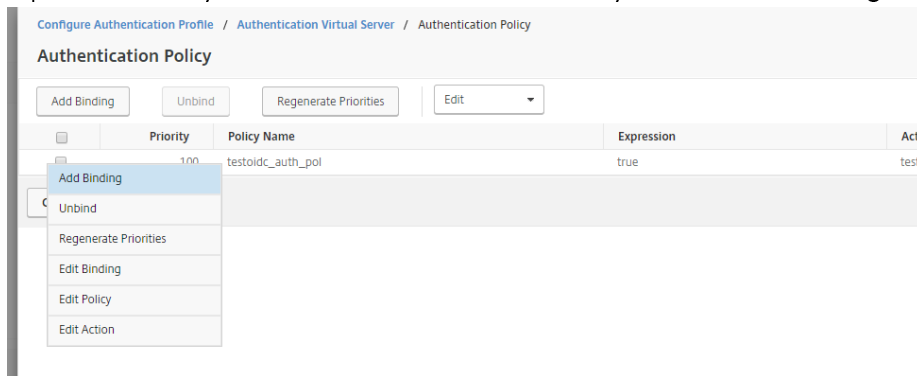
Skew Time (mins)
5

Issuer

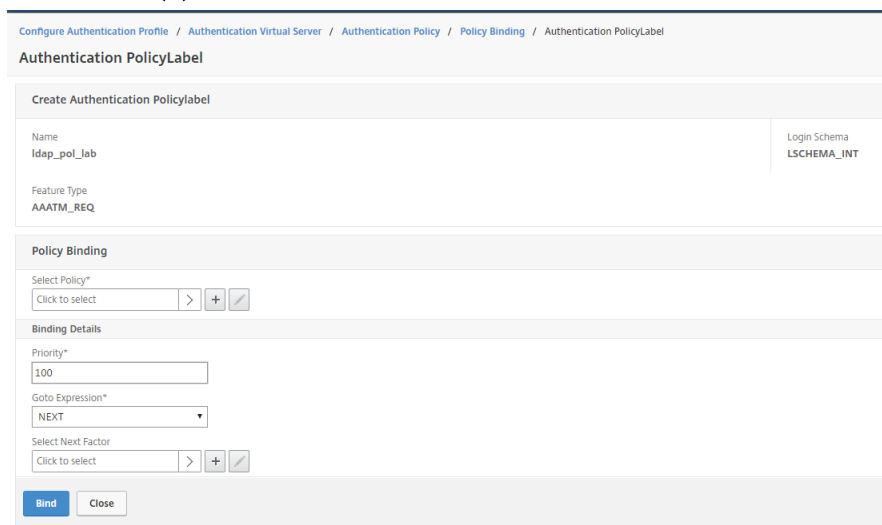
Refresh Interval
1440

Press Create and press Bind.

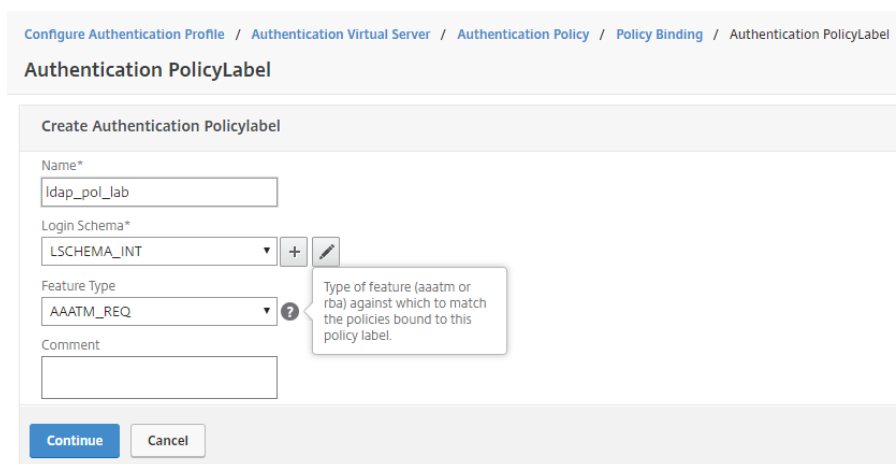
7. Add authorization of users through LDAP. This is achieved through Next Factor. Open the newly created Authentication Policy. Press Edit Binding.



Press ADD (+) on Select Next Factor to create the next Factor.



8. Give the Authentication PolicyLabel a name. Since the LDAP authorization will be performed without GUI, Login Schema can be kept as LSCHEMA_INT. Press Continue.



9. Press ADD (+) on Select Policy.

Configure Authentication Profile / Authentication Virtual Server / Authentication Policy / Policy Binding / Authentication PolicyLabel

Authentication PolicyLabel

Create Authentication Policylabel

Name ldap_pol_lab	Login Schema LSHEMA_INT
Feature Type AAATM_REQ	

Policy Binding

Select Policy*
Click to select > + ✎

Binding Details

Priority*
100

Goto Expression*
NEXT

Select Next Factor
Click to select > + ✎

Bind Close

10. Give the Authentication Policy a name. Choose Action Type LDAP. Set Expression to true. Press ADD (+) on Action to create an LDAP action.

Configure Authentication Profile / Authentication Virtual Server / Authentication Policy / Policy Binding / Authen

Configure Authentication Policy

Name
testoidc_ldapextract

Action Type
LDAP

Action*
testoidc_ldapactionextrac + ✎

Expression*
Operators Saved Policy Expressions Frequently Used Expressions
true

More

OK Close

11. Below is an example configuration for the LDAP server.

Configure Authentication Profile / Authentication Virtual Server / Authentication Policy / Policy Binding / Authentication PolicyLabel / Configure Authentication Policy / Configure Authentication LDAP Se

Configure Authentication LDAP Server

Name
testoidc_idapactionextrac

Server Name Server IP

Server Name*
192.168.171.110

Security Type
PLAINTEXT

Port
389

Server Type
AD

Time-out (seconds)
3

Authentication

Connection Settings

Base DN (location of users)*
DC=CTXLAB.DC=LOCAL

Administrator Bind DN*
adc_sa@ctxlab.local

Administrator Password*
.....

Confirm Administrator Password*
.....

Test Connection

Other Settings

Server Logon Name Attribute
---<< New >>---
mobile

Search Filter

Group Attribute

Sub Attribute Name

SSO Name Attribute
---<< New >>---
userPrincipalName

Default Authentication Group

User Required
 Referrals

Maximum Referral Level
1

Referral DNS Lookup
A-REC

Validate LDAP Server Certificate

LDAP Host Name

OTP Secret

The Authentication check-mark is not chosen since the LDAP action is only going to find the user account which has the matching mobile number attribute in AD. userPrincipalName is used for SSO attribute to e.g. Storefront. Press Bind, Create, OK and Done until you reach the Gateway GUI again.