



Workplace by Facebook SAML-Proxy with ADFS

Jürgen Seitz; v1.0

Dec 2017

Table of Contents

INTRODUCTION	3
PREREQUISITES	3
SAML-Proxy Setup	4
SAML Proxy Step-by-Step configuration	5
ADFS Claim-Rule to selectively bypass the R-Proxy	10
ADFS Claim-Rule Step-by-Step configuration	10

INTRODUCTION

This “How-To” describes the steps to add a Netskope SAML-/R-Proxy to a SSO setup with ADFS and Workplace by Facebook. The use case here is to control access and content from unmanaged devices. In addition, this document explains how to selectively enforce R-Proxy based on AD group membership.

PREREQUISITES

Before inserting the Netskope R-Proxy configuration, there has to be a working ADFS SSO integration with Workplace. If you have to do this, please follow this instruction:

- SSO for Workplace: <https://tinyurl.com/ya9h9eyb>

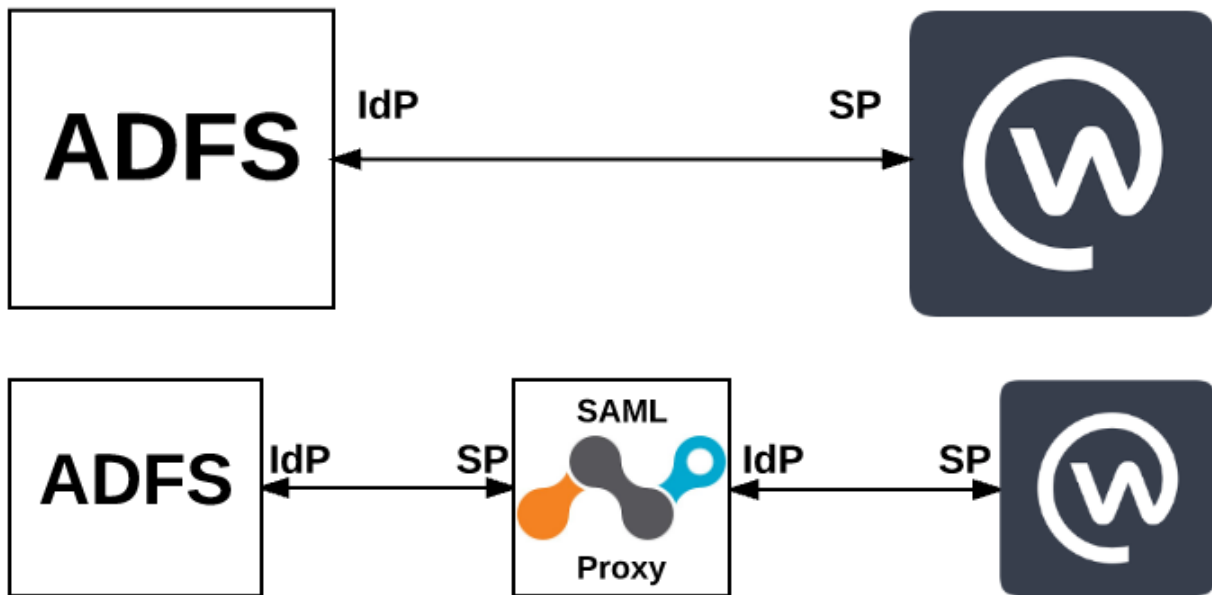
Important:

To prevent any loops while setting up Netskope R-Proxy:

- Be connected to the Netskope tenant via the desktop client to avoid having our SAML proxy rewrite POST URL to *.rproxy domain for the first verification call before saving the configuration on the application side
- Temporary add the Internet source IP being used to the IP Bypass list for the SAML proxy config to avoid SAML proxy from rewriting the URL. You will get your public IP quite easy with this link: <https://whatismyipaddress.com/>

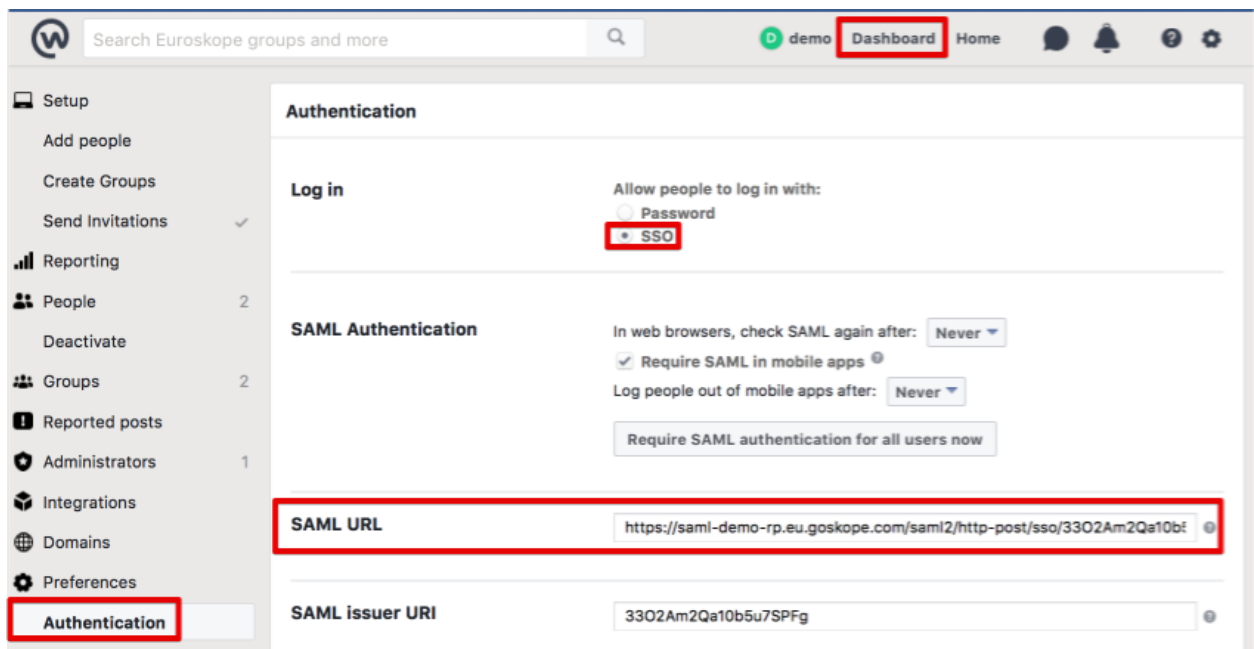
SAML-Proxy Setup

The integration of Netskope's SAML Proxy works in same way as we do for other applications like Box or Dropbox. The SAML Proxy will act as an IdP towards Workplace and as an SP against ADFS.

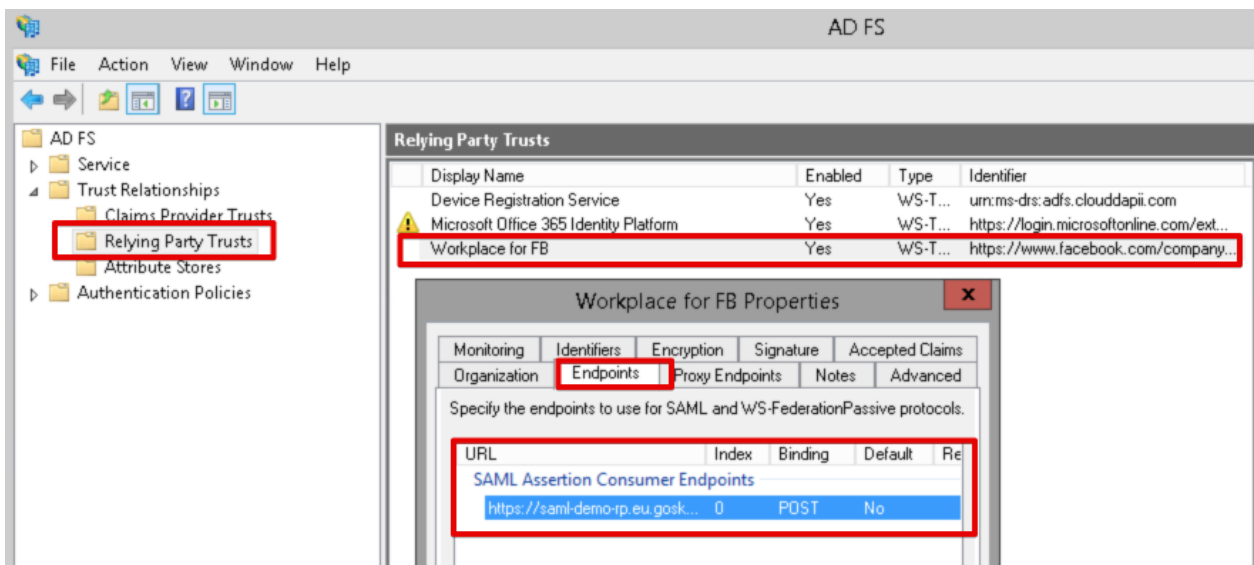


SAML Proxy Step-by-Step configuration

1. Go to Setting - Active Platform - Reverse Proxy – SAML in the Netskope tenant.
2. Add a new Account, select “Workplace for Facebook” and give it a name.
3. Copy the “SAML URL” from the Workplace SSO settings to the “IdP URL” in this setup screen.



4. Copy the “SAML Assertion Consumer Endpoint” from the ADFS setting to the “ACS URL” in the setup Screen.



- Copy the ADFS Server certificate to the field "IdP Certificate". The easiest way to do this is to copy the certificate from the Workplace SSO settings:

SAML certificate

```
-----BEGIN CERTIFICATE-----
MIIEPjCCAyagAwIBAgIDBF+nMA0GCSqGSIb3DQEBCwUAMIG8MQswCQYDVQ
QGEwJV
UzELMAkGA1UECBMCQ0ExEjAQBgNVBAcTCUxvcyBBbHRvczEWMBQGA1UE
ChMNTmV0
c2tvcGUgdGVzdDEpMCcGA1UECXMgZDIhMjRkNjRkMGVjMWU3NDg1Zjc3ND
Q0Zml1
ODA1NzUxIjAgBgNVBAMTGWNhLmRlbW8tcnAuZXUuZ29za29wZS5jb20xJTA
jBgkq
hkiG9w0BCQEFmNlcnRhZG1pbkBuZXRza29wZS5jb20wHhcNMTCwMTIzMT
c1NzA2
WhcNMjcwMTIxMTc1NzA2WjCBwTElMAkGA1UEBhMCVVMxCzAJBgNVBAGT
AkNBMRlw
-----
```

The certificate is valid for 9 years

- Now the setup screen looks like this:

Edit Account: EMEA-WP By FB With ADFS

App

Workplace by Facebook

Name

EMEA-WP by FB with ADFS

ACS URL

https://work-62227112.facebook.com/work/saml.php

IdP URL

https://adfs.clouddapii.com/adfs/ls

IdP Certificate

-----BEGIN CERTIFICATE-----
MIIC4jCCAcqAwIBAgIQTknDTCXOrqRBJZnQdk/51zANBgkqhkiG9w0BAQsFADAt
MSswKQYDVQQDEyJBREZTIFNpZ25pbmcgLSBhZGZzLmNsb3VhZGFwaWkuY29tMB4X
DTE3MDcyMzEzMzUwN1oXDTE4MDcyMzEzMzUwN1owLTERMCKGA1UEAxMiQURGUyBT
aWduZW50LmNlcnRhZG1pbkBuZXRza29wZS5jb20wHhcNMjcwMTIxMTc1NzA2WjCBwTElMAkGA1UEBhMCVVMxCzAJBgNVBAGT
AkNBMRlw

Alternate User Id Field

Save

- Save the settings.

- Click the magnifying glass icon in the SAML Proxy overview screen for this configuration to get the missing configuration items to finalize the setup:

Settings: EMEA-WP By FB With ADFS

Organization ID

33O2Am2Qa10b5u7SPFg

SAML Proxy IdP URL

https://saml-demo-rp.eu.goskope.com/saml2/http-post/sso/33O2Am2Q

SAML Proxy ACS URL

https://saml-demo-rp.eu.goskope.com/saml2/http-post/acs/33O2Am2Q

SAML Proxy Issuer Certificate

-----BEGIN CERTIFICATE-----
MIIEPjCCAyagAwIBAgIDBF+nMA0GCSqGSIb3DQEBCwUAMIG8MQ
swCQYDVQQGEwJV
UzELMAkGA1UECBMCQ0ExEjAQBgNVBACTCUxvcyBBbHRvczEW
MBQCA1UEChMNTmV0

Ok

- Copy the "Organization ID" to the Workplace SSO settings field "SAML issuer URL".
- Copy the "SAML Proxy IdP URL" to the Workplace SSO settings field "SAML URL".
- Copy the "SAML Proxy ACS URL" to the ADFS settings field "SAML Assertion Consumer Endpoint" (refer to step 4).
- Copy the "SAML Proxy Issuer Certificate" to the Workplace SSO settings field "SAML certificate".
- The Workplace SSO settings should now look like this:

SAML URL

https://saml-demo-rp.eu.goskope.com/saml2/http-post/sso/33O2Am2Qa10b5u7SPFg

SAML issuer URI

33O2Am2Qa10b5u7SPFg

SAML logout redirect

☐ Enable SAML logout redirection

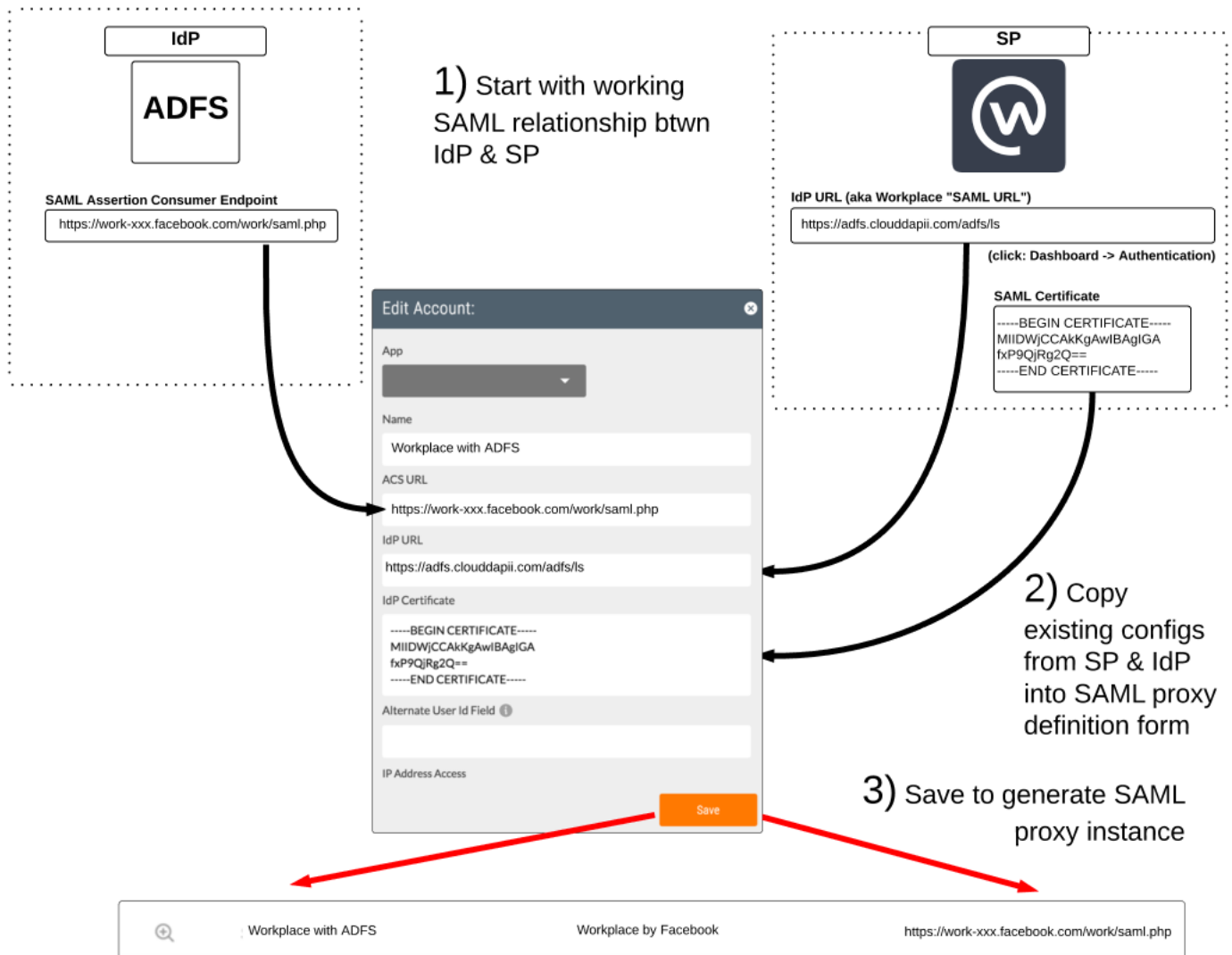
SAML certificate

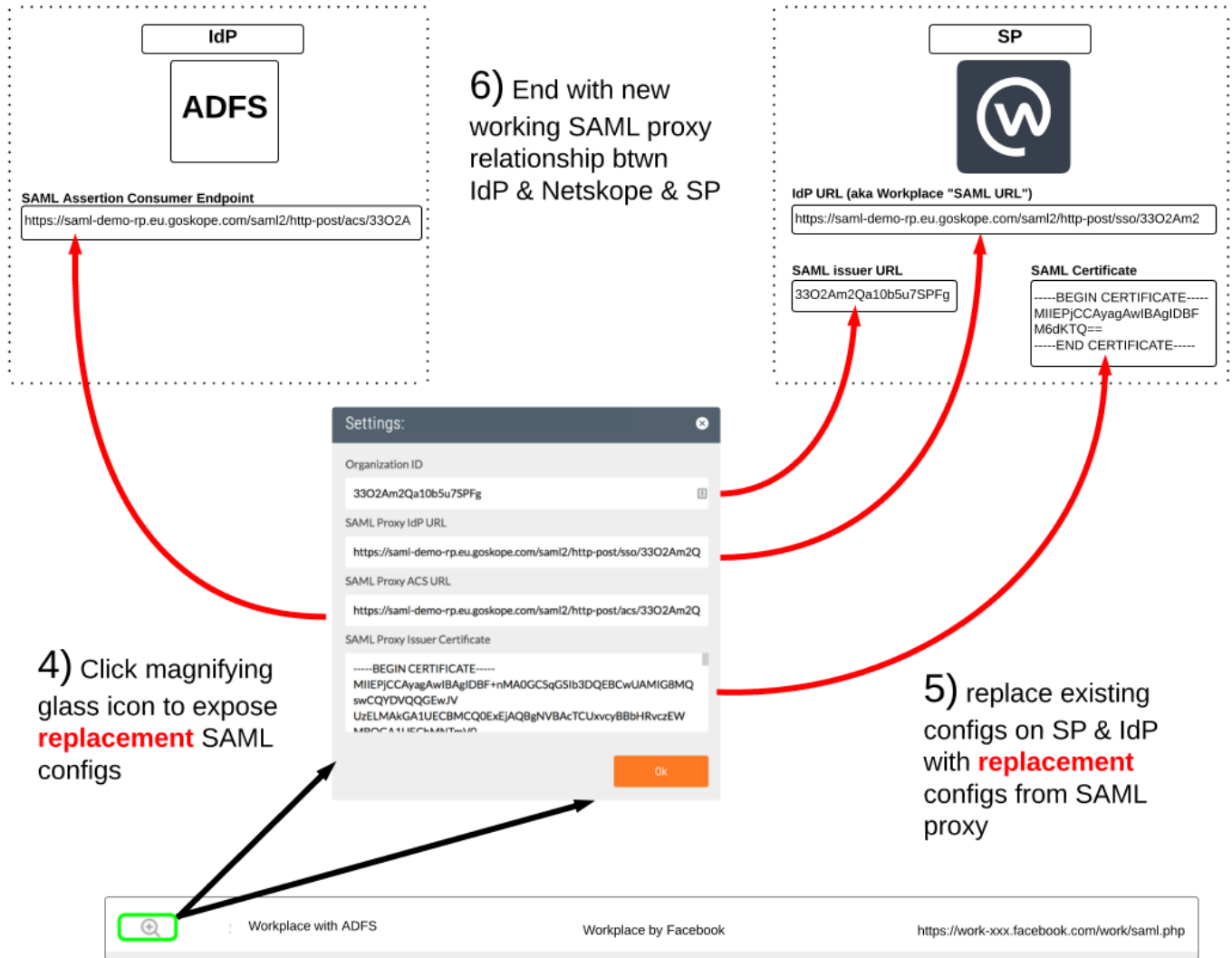
-----BEGIN CERTIFICATE-----
MIIEPjCCAyagAwIBAgIDBF+nMA0GCSqGSIb3DQEBCwUAMIG8MQswCQYDVQQGEwJV
UzELMAkGA1UECBMCQ0ExEjAQBgNVBACTCUxvcyBBbHRvczEWMBQCA1UEChMNTmV0
c2tvcGUgdGVzdDEpMCcGA1UECXMgZDIhMjRkNjRkMGVjMWU3NDg1Zjc3ND
Q0Zml1
QDA1NzUxIjAgBgNVBAMTGWNhLmRlW8tcnAuZXUuZ29za29wZS5jb20xJTA
jBgkq
hkiG9w0BCQEFmNlcRhZG1pbkBuZXRza29wZS5jb20wHhcNMTCwMTIzMT
c1NzA2
WhcNMjcwMTIxMTc1NzA2WjCBwTELMakGA1UEBhMCVVMxZzAJBgNVBAGT
AkNBMRlww

The certificate is valid for 9 years

14. Press the “Test SSO” button on the bottom of Workplace SSO screen and verify the configuration. If the authentication was successful, save the config. **Pleaser remembert** the “Important Note” under the section prerequisites.

Here is a graphical summary of the configuration step:



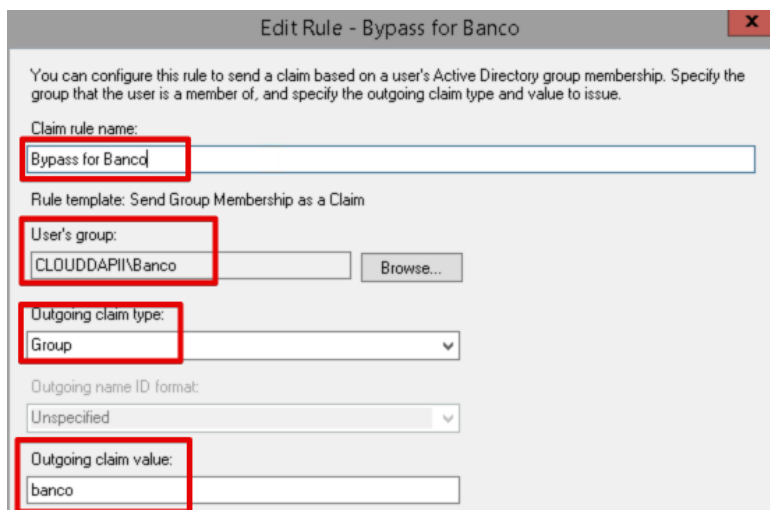


ADFS Claim-Rule to selectively bypass the R-Proxy

This example is a helpful extension to the SAML-/R-Proxy setup to bypass or block certain user groups or do a device classification to be used in policies. In this case we use the “SAML Assertion Key Value Pair” to bypass all users, which are not member of a certain user group, from the R-Proxy. An aligned use case may be, to launch R-Proxy first a for a pilot group and not for the whole company.

ADFS Claim-Rule Step-by-Step configuration

1. Right click on the “Relying Party Trusts” entry for Workplace in the ADFS configuration and click on “Edit Claim Rules”.
2. Add Rule ... and set a name.
3. Select a user group you would like to use as a selection criteria.
4. Set the “Outgoing claim type” to “Group”.
5. Define the “Outgoing claim value”.



The screenshot shows the 'Edit Rule - Bypass for Banco' dialog box. The title bar reads 'Edit Rule - Bypass for Banco'. The main text says: 'You can configure this rule to send a claim based on a user's Active Directory group membership. Specify the group that the user is a member of, and specify the outgoing claim type and value to issue.' The fields are as follows:

- Claim rule name:** 'Bypass for Banco' (highlighted with a red box)
- Rule template:** 'Send Group Membership as a Claim'
- User's group:** 'CLOUDDAPI\Banco' (highlighted with a red box, with a 'Browse...' button next to it)
- Outgoing claim type:** 'Group' (highlighted with a red box, shown in a dropdown menu)
- Outgoing name ID format:** 'Unspecified' (shown in a dropdown menu)
- Outgoing claim value:** 'banco' (highlighted with a red box)

6. Go to the SAML proxy setting for Workplace in the Netskope Tenant.

7. Scroll down to the section “Match SAML Assertion Key Value Pair” and modify the setting like in this sample:

Edit Account: EMEA-WP By FB With ADFS

☒ Match SAML Assertion Key Value Pair (Up to 3) ⓘ

Bypass ▼ if Not Match ▼ the following conditions:

Pair 1: ☐ Partial Match

Pair 2: ☐ Partial Match

Pair 3: ☐ Partial Match

Authentication Method: ⓘ

8. To get the right syntax of the “Key” value (<http://schemas.xmlsoap.org/claims/Group>) a SAML tracer (Firefox plugin: <https://github.com/UNINETT/SAML-tracer>) is helpful. Sign in to your SasS while the tracer is enabled. Select the last POST entry marked with “SAML” and switch to the “SAML” view in the body. Ctrl+F and search for your value from the claim rule. In this case “banco”. The “Attribute Name” above will be the correct “Key” value.

moz-extension://6ce45663-9dfd-9740-b126-fdadf94f7f03 - Trace Window

X Clear ± Autoscroll Filter resources

POST https://work-62227112.facebook.com/cookie/consent/?dpr=3

POST https://work-62227112.facebook.com/work/saml/begin_login/

GET https://saml-demo-rp.eu.goskope.com/saml2/http-post/sso/3302Am2Qa10b5u7SPFg/7?SAMLRequest=fZJPj9MwEMXv%2FRRR

POST https://adfs.clouddapil.com/adfs/ls

GET https://saml-demo-rp.eu.goskope.com/favicon.ico

GET https://adfs.clouddapil.com/favicon.ico

POST https://adfs.clouddapil.com/adfs/ls

POST https://adfs.clouddapil.com/adfs/ls

POST https://adfs.clouddapil.com/adfs/ls

POST https://work-62227112.facebook.com/rproxy.goskope.com/work/saml.php

GET https://work-62227112.facebook.com/rproxy.goskope.com/

GET https://facebook.com/security/hsts-pixel.gif?c=3.2.5

GET https://video-ort2-2.xx.fbcdn.net/rproxy.goskope.com/v/t42.1790-2/14634988_208453536234887_1485390993095131136_n.mp4?efg=eyJ

GET https://video-ort2-2.xx.fbcdn.net/rproxy.goskope.com/v/t42.1790-2/14625201_208453476234893_1809110215862255616_n.mp4?efg=eyJ

OPTIONS https://video-ort2-2.xx.fbcdn.net/rproxy.goskope.com/v/t42.1790-2/14634988_208453536234887_1485390993095131136_n.mp4?efg=eyJ

HTTP Parameters SAML

<AudienceRestriction>

<Audience>https://www.facebook.com/company/130140734340736</Audience>

</AudienceRestriction>

</Conditions>

<AttributeStatement>

<Attribute Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress">

<AttributeValue>demo@euroscope.com</AttributeValue>

</Attribute>

<Attribute Name="http://schemas.xmlsoap.org/claims/Group">

<AttributeValue>banco</AttributeValue>

</Attribute>

</AttributeStatement>

<AuthnStatement AuthnInstant="2017-12-08T13:57:48.680Z"

SessionIndex="_d5654d41-957d-4caf-bb45-0c3198e846e6"

>

<AuthnContext>

483 requests received (404 hidden)

X Search banco Highlight All Match Case Whole Words 1 of 1 match

9. Test your claim rule while signing in with a member of your selected group and verify that R-Proxy is enforced. All other users should be bypassed.