

## Configure SAML authentication and authorization on the Remote Spark gateway

Remote Spark gateway supports user authentication and authorization through SAML 2.0 ([https://en.wikipedia.org/wiki/SAML\\_2.0](https://en.wikipedia.org/wiki/SAML_2.0)).

To support SAML, the gateway needs the following configurations:

- Servers.json file, which contains the list of servers and / or remote applications (see gateway manual for details)
- Users.json file, which contains the user(s) and the servers he/she is able to access. In this file, the name attribute is the email of the user set on the IDP server. For example,

```
{
  "users": [
    {
      "name": "remotesparktest@gmail.com", ← the email of the user existing on IDP
      "password": "password",
      "servers": [
        "Win7_RDP", ← The server name(s) existing in the Servers.json
        "Win10_RDP"
        "Ubuntu_xRDP"
      ],
      "isDomainUser": false
    },
    ... ..
  ]
}
```

- SAML Identity Provider (IdP) XML Metadata, which is a file generated by the IDP server. This XML based file contains configuration and integration details for SAML2.0 Single Sign-on (SSO).
- SAML Service Provider (SP) XML Metadata, which is a file created with the gateway information.
- In the gateway config file (gateway.conf), add the following mandatory section at the bottom:

```
... ..
# SAML configuration
samIdpMetadataFile=[full path to the IDP metadata xml file]
samSpMetadataFile=[full path to the SP metadata xml file]
```

For example, in the gateway.conf, add the two lines below:

```
samIdpMetadataFile=C:\\SparkGateway\\ssocircle_idp.xml
samSpMetadataFile=C:\\SparkGateway\\sparkgateway_sp.xml
```

In addition to the configuration on the gateway, when a new Service Provider Metadata is imported against a given user, make sure the attribute "EmailAddress" to be sent in the SAML assertion. (See the sample below).

A step-by-step instruction of configuring SAML on the gateway using a public IDP provided by SSOcircle.

1. Build a new user on IDP and log in.
  - 1) Go to <https://idp.ssocircle.com/sso/UI/Login> to load the page below. Click “New User” button to create a new user.

The screenshot shows the SSOcircle login interface. At the top left is the SSOcircle logo. On the left side, there are navigation links: Home, Login, and Logout. In the center, there is a green circular icon with a checkmark and the text 'SSOCIRCLE'. To the right of this icon, the text reads: 'Microsoft Office365 SAML Authentication Bypass. Are you sure your SP is not vulnerable? Click here to get more information.' Below this, there is a login form with the label 'user name / password'. It includes input fields for 'User Name:' and 'Password:', and buttons for 'Log In' and 'New User'. Below the login form, there are several alternative login options, each with a small icon and a button: 'Certificate Log In', 'OTP Log In', 'Swekey Log In', 'Swekey&Pin Log In', 'Yubikey Log In', 'Yubikey & Pin Log In', and 'MSISDN Log In'.

- 2) In the next page, input “User Name”, “Password”, “First Name”, “Last Name”, “Full Name” and “Email Address”, and click “Register” button to create a new user on IDP.

The screenshot shows the SSOcircle self-registration page. At the top left is the SSOcircle logo. On the left side, there are navigation links: Home, Login, and Logout. On the right side, the text 'Self Registration' is displayed. Below this, there is a registration form with the following fields, each marked with an asterisk to indicate it is required: '\* User Name [a-zA-Z.-]:', '\* Password - at least 8 characters:', '\* Confirm Password:', '\* First Name:', '\* Last Name:', '\* Full Name:', and '\* Email Address:'. Below the fields, there is a legend: '\* Indicates required field'. At the bottom of the form, there are three buttons: 'Register', 'Cancel', and 'Reset Form'.

- 3) Log in with the newly created user with the name and password. A user profile page shows up as:

User Profile	
Attribute	Value
User ID	samlbadger
Google Apps Email	No longer available
OpenID 1.0 Identifier	<a href="http://samlbadger.ssocircle.com">http://samlbadger.ssocircle.com</a>
Client Certificate	Not Enrolled
Given name	<input type="text" value="saml"/>
Surname	<input type="text" value="badger"/>
Email	<input type="text" value="remotesparktest@gmail.com"/>
ePass OTP token number	not assigned
Yubikey ID	<input type="text" value="not assigned"/>
Yubikey PIN	<input type="text" value="*****"/>
Swekey ID <a href="#">detect</a>	<input type="text" value="not assigned"/>
Swekey PIN	<input type="text" value="*****"/>
MSISDN identification	<input type="text" value="not active"/>
Password (length > 8)	<input type="text"/>
Retype Password	<input type="text"/>
<input type="button" value="Submit"/>	

2. Create the Service Provider (SP) XML metadata, if you do not have one already. If you have SP metadata XML file already, go to step 3.

- 1) In above user profile page, click the “Manage Metadata” button on the left side menu bar. The existing SP entity shows up, if there is any, like:

Manage your Service Provider Metadata	
SAML Service Provider Entity	Expiration
<input type="checkbox"/> sparkgateway	2018-02-08 21:30:50 GMT
<input type="button" value="Remove Metadata"/>	
<a href="#">Add new Service Provider</a>	
<a href="#">SSOCircle Public IDP Metadata</a>	
<a href="#">SSOCircle Public IDP Metadata (deprecated)</a>	

- 2) If the existing one has expired, remove it by pressing “Remove Metadata” button.

- 3) Click “[Add new Service Provider](#)” link to load the page which imports SP metadata, as:

here'. Below this is a large empty text area for pasting metadata." data-bbox="231 144 811 463"/>

- 4) Press the link “you can build it [here](#)”. The template of SP metadata is shown in a new page as:

## Build your own Metadata

Some Service Provider software does not support SAML Metadata out-of-the-box.

Although Metadata might include more complex data, a sample minimal Metadata for a service provider is shown below. Enter the data specific for your SP and click the button. Then copy the generated Metadata and paste it into the SSOCircle [Service Provider Import Page](#).

But remember that the entityID must be a unique identifier for your SP. With approaching 10.000 service providers in the SSOCircle of Trust many names are already used especially IDs similar to `http://localhost:8080`.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?><EntityDescriptor
entityID="%YOUR SP ENTITY ID%" xmlns="urn:oasis:names:tc:SAML:2.0:metadata">
<SPSSODescriptor AuthnRequestsSigned="false" WantAssertionsSigned="true"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
<NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-
format:unspecified</NameIDFormat><AssertionConsumerService index="0"
isDefault="true" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="%YOUR SP ASSERTION CONSUMER URL%"/></SPSSODescriptor>
</EntityDescriptor>
```

Enter your data here, and click the button below

entityID:

ACS URL:

- 5) Input entity ID with “sparkgateway” and ACS URL with “[http://\[gateway\\_host\\_name\]/samlcallback](http://[gateway_host_name]/samlcallback)”. The entity ID is the identification of the service provider; and the ACS URL is the saml callback URL. After clicking the “insert” button, you will see the updated SP metadata in the text area in red, with the information of entity ID and callback url inserted.

For example, it can look like:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?><EntityDescriptor
entityID="sparkgateway"
xmlns="urn:oasis:names:tc:SAML:2.0:metadata"><SPSSODescriptor
AuthnRequestsSigned="false" WantAssertionsSigned="true"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol"><NameIDFormat
>urn:oasis:names:tc:SAML:1.1:nameid-
format:unspecified</NameIDFormat><AssertionConsumerService index="0"
isDefault="true" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="http://sparkgateway1/samlcallback"/></SPSSODescriptor></EntityDescriptor
>
```

- 6) Copy the content and save it as a local XML file, such as “c:\SparkGateway\sparkgateway\_sp.xml”. This is the SP XML metadata file of the gateway.

### 3. Add new Service Provider (SP).

- 1) Click the “Manage Metadata” button on the left side menu bar. The existing SP entity shows up, if it is added, like:

SAML Service Provider Entity	Expiration
<input type="checkbox"/> sparkgateway	2018-02-08 21:30:50 GMT

[Remove Metadata](#)

[Add new Service Provider](#)

[SSOCircle Public IDP Metadata](#)

[SSOCircle Public IDP Metadata \(deprecated\)](#)

- 2) Click “[Add new Service Provider](#)” link to load the page which imports SP metadata, as:

here'. Below this note is a large empty text area for pasting XML metadata." data-bbox="231 128 812 444"/>

- 3) Input the host name of the gateway in the FQDN field.
- 4) Check the “EmailAddress” checkbox to include the “EmailAddress” attribute in the SAML assertion response.
- 5) Paste the SP XML Metadata in the text area. This is the XML content generated in above step 2-(5).
- 6) Finally, click “Submit” to add this Service Provider (sparkgateway) to the user.

4. Get the public IDP XML metadata.

- 1) Click the “Manage Metadata” button on the left side menu bar. The existing SP entity shows up, if it is added, like:



- 2) Right click the link “SSOCircle Public IDP Metadata” and select “Save link as ...” to save the XML in local, such as “c:\SparkGateway\ssocircle\_idp.xml”. This is the IDP XML metadata file.

- Specify the IDP XML Metadata file and SP XML Metadata file on the gateway. Edit the gateway.conf by adding the following two lines at the end:

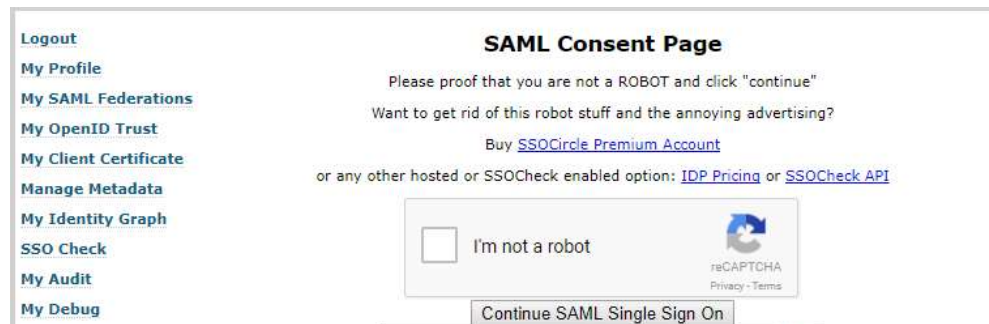
```
samlIdpMetadataFile=C:\\ SparkGateway\\ssocircle_idp.xml
```

```
samlSpMetadataFile=C:\\ SparkGateway\\sparkgateway_sp.xml
```

- Start gateway, and load the login page [http://\[your\\_gateway\\_hostname\]/login.html](http://[your_gateway_hostname]/login.html) in a browser.



- Click the red icon “SAML” to do user authentication and authorization on the SSOcircle public IDP.
  - If you have logged in the SSOCircle web page as above, you should see:



Click “I’m not a robot”, and then “Continue SAML Single Sign On” button to get the user’s email and password from the IDP. The user’s email will be filled in the user name field as below:

### Spark View 5.0.0

Spark Gateway:

Domain\user name:

Password:




80 is default port of Spark Gateway if it's not specified (ip:port).  
[What's new](#)  
 Copyright © Remote Spark Corp. 2011 - 2017 [www.remotespark.com](http://www.remotespark.com)

Click “Sign in” button, you will see the icons of all servers which were assigned in the users.json file.

- 2) If you have not logged in SSOCircle web page, after clicking the red icon “SAML”, you should be redirect to the IDP login page as:



The screenshot shows the SSOCircle login interface. At the top left, there are links for Home, Login, and Logout. The main heading is "Microsoft Office365 SAML Authentication Bypass" with a red warning icon. Below this is a "user name / password" section with input fields for "User Name" and "Password", and buttons for "Log In" and "New User". A list of authentication methods is provided, each with a small icon and a button: Certificate Log In, OTP Log In, Swekey Log In, Swekey&Pin Log In, Yubikey Log In, Yubikey & Pin Log In, and MSISDN Log In.

After logging in and checking “I’m not a robot” as above step, you can also see the icons of your servers.