JUMP Session:
SAML 2.0 partnership with IBM Connections Cloud

Presenters:

Paul Henry

Advisory Engineer,

Connections Cloud L2

Kevin Joyce

Connections Cloud L2

Panellists:

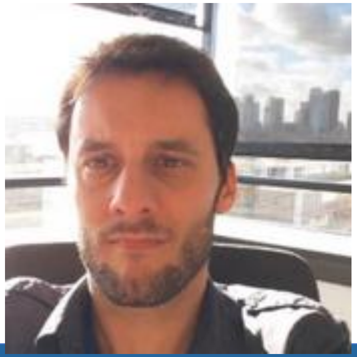
Hardik Thakkar

BSS Developer

Baptiste Strauss

Advisory Engineer,

Connections Cloud L2



Agenda

- What is SAML?
- The SAML assertion
- SAML flow; SP-initiated VS Idp-initiated
- Connection Cloud Login types
- Configuring SAML Partnership via new “Self Serve” feature (October update)
- Updating SAML Partnership
- Application passwords
- SSO for Plugins/Mobile applications
- SAML Partnership Request process
- Troubleshooting/Common exceptions
- Observations
- Documentation
- Q&A

What is SAML 2.0?

Security Assertion Markup Language 2.0 (SAML 2.0):

- …is a version of the SAML standard for exchanging authentication and authorization data between security domains.
- …is an XML-based protocol that uses security tokens containing assertions to pass information about a principal (e.g end-user) between a SAML authority (e.g IDP) and a SAML consumer (e.g SP).
- …enables web-based, cross-domain single sign-on (SSO), which helps reduce the administrative overhead of distributing multiple authentication tokens to the user.
- …uses single-use, digital "tokens“ (aka assertions) to exchange authentication and authorization data between an identity provider and the service provider that have an established trust relationship.

Source: *https://en.wikipedia.org/wiki/SAML_2.0*

SAML for Web browser SSO involves three parties:

- The end-user
- An identity provider (IDP) e.g AD FS, MS Azure, IBM Cloud Identity
- A Service Provider (SP) e.g IBM Connections Cloud

Benefits:

- You (the customer) control the type of authentication and authentication options.
- Users can use their familiar, on-premises credentials to access the cloud service.
- While users are logged on to the on-premises identity provider, they can access a cloud service without being re-prompted for credentials.

The SAML Assertion

The IdP stores information about the user in a database like Active Directory.

The user authenticates with the IDP upon login. The IDP creates a SAML Assertion which contains:

- identity of the user
- the time of authentication
- method of authentication

The SAML Assertion is sent to the Service Provider (SP).

The SP uses the assertion to continuously verify a user's identity. As long as the token has not expired and has a valid signature, the user is allowed in.
Once the SP detects the token is expired, the service provider is then aware that the user needs to repeat the process again to authenticate with the IDP.

Hybrid SP-initiated VS Idp-initiated

Note: Connections Cloud only supports IDP initiated authentication.

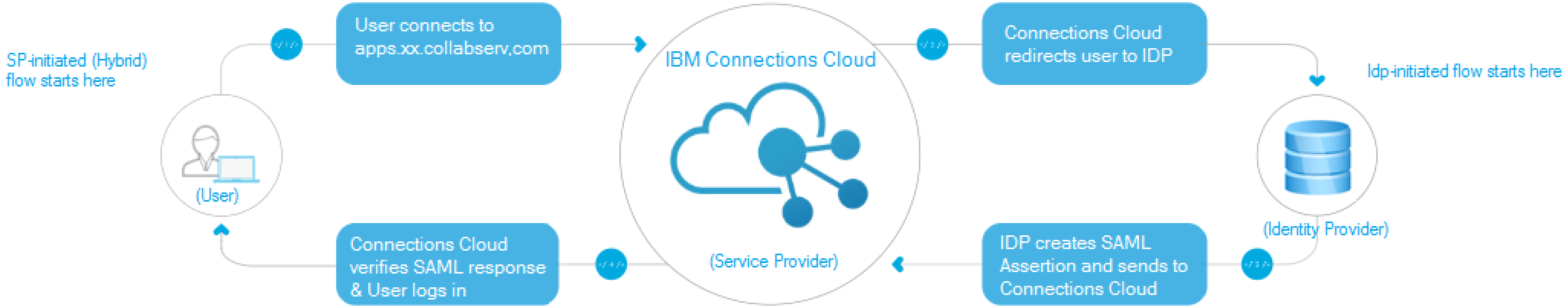
An IdP-initiated flow;

- the user first navigates to the IdP for authentication
- the Idp then sends the SAML assertion to the SP (Connections Cloud)

Hyrbrid SP-initiated flow;

- the user first navigates to Connections Cloud (SP)
- the user is then redirected to the IdP for authentication
- the Idp then sends the SAML assertion to the SP (Connections Cloud)

The service provider retrieves & validates the authentication response and the user is granted access.


SP-initiated (Hybrid) flow starts here
User connects to apps.xx.collabserv.com
IBM Connections Cloud
Connections Cloud redirects user to IDP
Idp-initiated flow starts here
(User)
(Identity Provider)
(Service Provider)
Connections Cloud verifies SAML response & User logs in
IDP creates SAML Assertion and sends to Connections Cloud

Preparation Checklist

In preparation of requesting SAML Partnership with Connections Cloud, you should:

❑ Choose the version of SAML that you want to use (SAML 1.1 or SAML 2.0)
Note: the new Self Serve tool only supports SAML 2.0

❑ Decide the login type you want to use (Federated, UserChoice, or AdminChoice)

❑ Understand the differences between the IdP-initiated flow Vs the SP-initiated hybrid flow model that Connections Cloud supports and decide which you want to choose.

❑ Implement SAML on your web server (Idp)

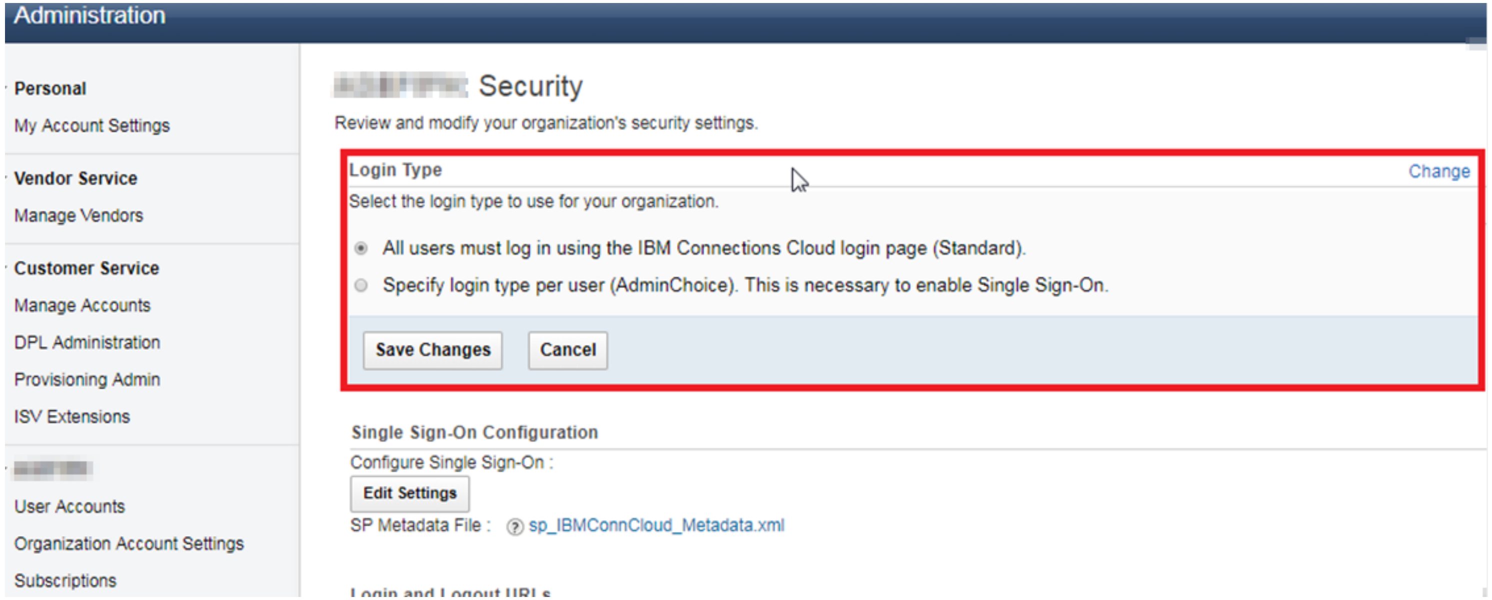
❑ If you are setting up federated identity for users of mobile apps or for IBM® Connections Desktop Plug-ins, create a second endpoint that accepts basic authorization. The mobile apps and Desktop Plug-ins work with the SP-initiated flow model only.

❑ Integrate your directory server with your SAML service.

❑ Test your Idp setup using a dummy service provider

❑ Know that IBM Connections Cloud servers are set to GMT and synchronize with NTP for clock updates. If the Idp server is on a different TZ or has time differential, it may result in the SAML assertions being rejected (for NotBefore timestamp in assertion). To prevent this, apply a skew time of a few minutes in your Identity Provider to handle clock synchronization mismatches or network latency.

Connections Cloud Login type



Administration

Personal
My Account Settings

Vendor Service
Manage Vendors

Customer Service
Manage Accounts
DPL Administration
Provisioning Admin
ISV Extensions

[redacted]
User Accounts
Organization Account Settings
Subscriptions

[redacted] Security

Review and modify your organization's security settings.

Login Type — Change

Select the login type to use for your organization.

● All users must log in using the IBM Connections Cloud login page (Standard).

○ Specify login type per user (AdminChoice). This is necessary to enable Single Sign-On.

Single Sign-On Configuration

Configure Single Sign-On :

SP Metadata File : ⓘ sp_IBMConnCloud_Metadata.xml

Login and Logout URLs

From the Security page, Administrator can choose

Standard (non-federated)
Default option.
Users must log in with their email address and password to use the cloud-based services.

AdminChoice
Enables administrator to edit user login types individually from User Accounts Page.

IMPORTANT:

- The option to change Org Login Type will be enabled by Support when you request the activation of the Self Serve feature
- Customer Admins can only change Login Type when the current setting is Standard.
- When Standard is set, the customer admin can change the login type to AdminChoice.
- If you want the org Login Type changed to anything else (e.g FEDERATED or USERCHOICE) open a case with Support and we will do it for you.

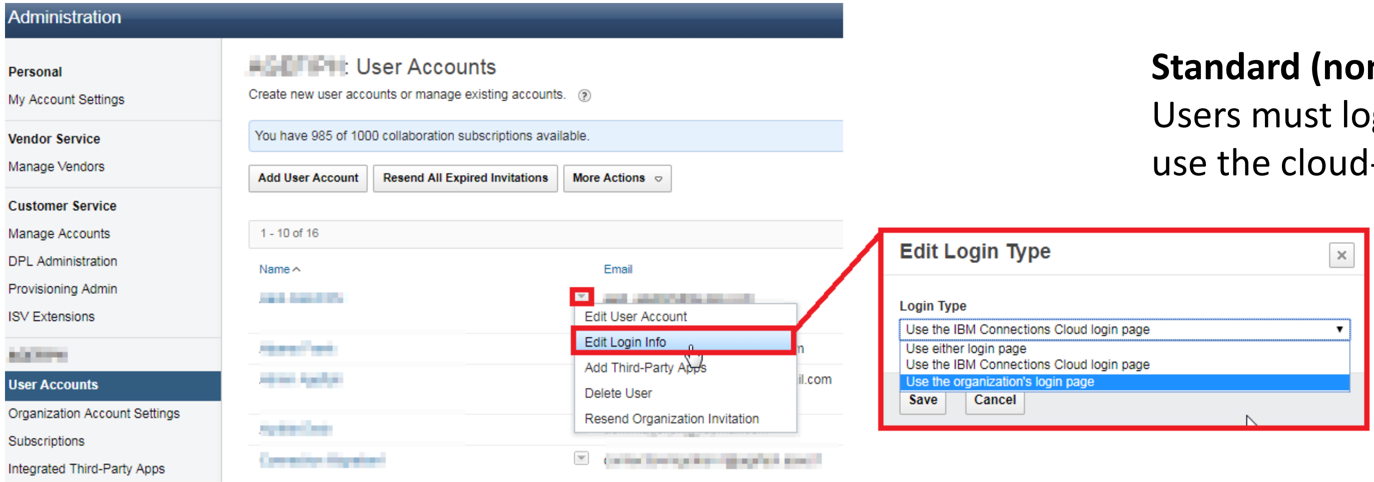
Connections Cloud Login type

If Admin Choice was selected in the Security page, an administrator can edit individual user’s login types in the User Accounts page:

UserChoice
Users have the option of authenticating with your organization before accessing the cloud-based services, or using their Connections Cloud user name and password to log on to Connections Cloud.

Federated
Users will be directed to use the organisation IDP login page.

Standard (non-Fed)
Users must log in with their email address and password to use the cloud-based services.



[redacted]: User Accounts

Create new user accounts or manage existing accounts.

You have 985 of 1000 collaboration subscriptions available.

1 - 10 of 16

Edit Login Type

Login Type: Use the IBM Connections Cloud login page

Configuring SAML 2.0 Partnership – SP side

You can now configure SAML 2.0 Partnership with Connections Cloud via our new "Self Serve" tool. Self Serve is:

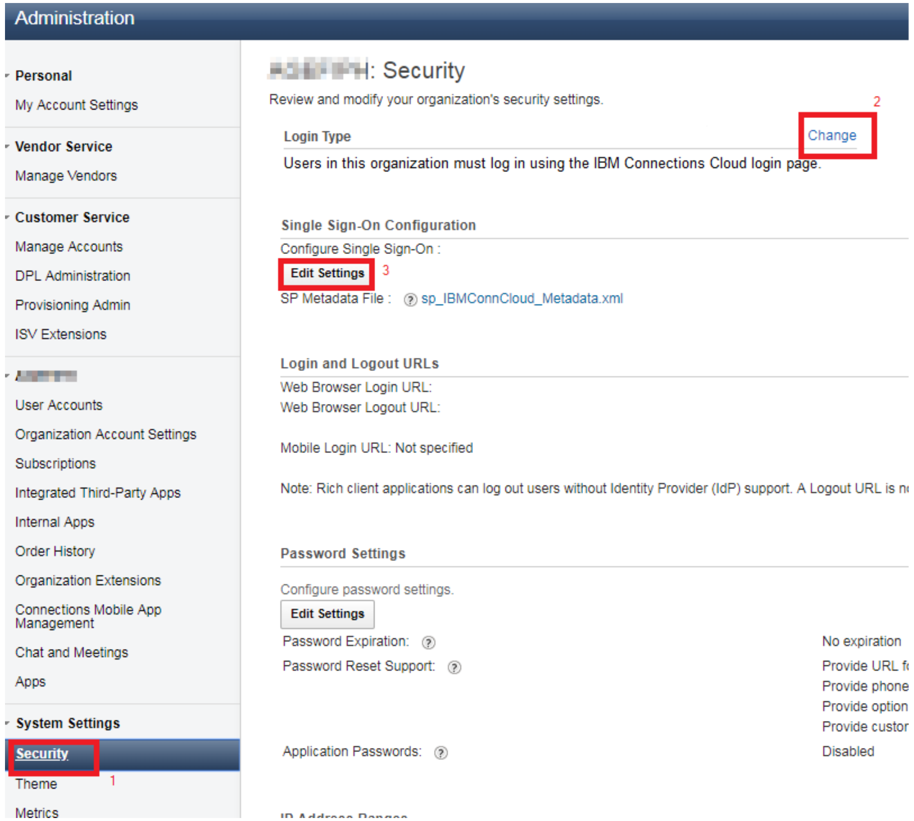
- the "Single Sign-on Configuration" section in Security page
- it facilitates config of SAML 2.0 partnership (not 1.0)
- available since Oct Deployment
- enabled by Support upon customer request

To use Self Serve, once enabled:

(1) In the Security UI,
(2) Change Org login type to AdminChoice
(3) Click on Edit Settings under "single Sign-on configuration"
(4) Click on Set Up SAML Partnership

Notes:

- Self Serve will *only* appear when you have set Admin Choice for Login Type
- 'Set Up SAML Partnership' option will only appear if you have not already submitted SAML Partnership details.
- If you have already applied SAML partnership details, you will only then have an option to Update the certificate of the partnership



[redacted]: Security

Review and modify your organization's security settings.

Login Type

Users in this organization must log in using the IBM Connections Cloud login page.

Single Sign-On Configuration

Configure Single Sign-On :

SP Metadata File : sp_IBMConnCloud_Metadata.xml

Login and Logout URLs

Web Browser Login URL:
Web Browser Logout URL:

Mobile Login URL: Not specified

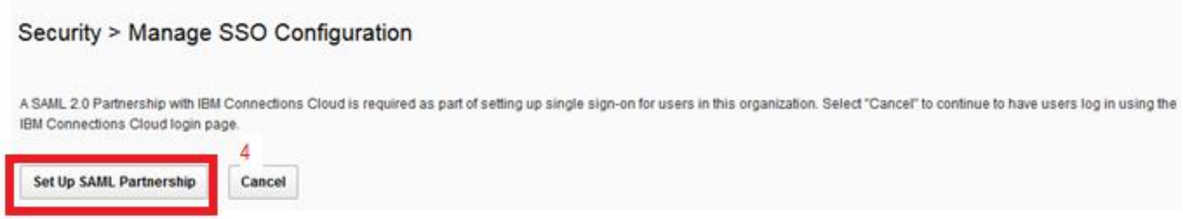
Note: Rich client applications can log out users without Identity Provider (IdP) support. A Logout URL is n

Password Settings

Configure password settings.

Password Expiration: No expiration
Password Reset Support: Provide URL f
Provide phone
Provide option
Provide custor
Application Passwords: Disabled

IP Address Ranges



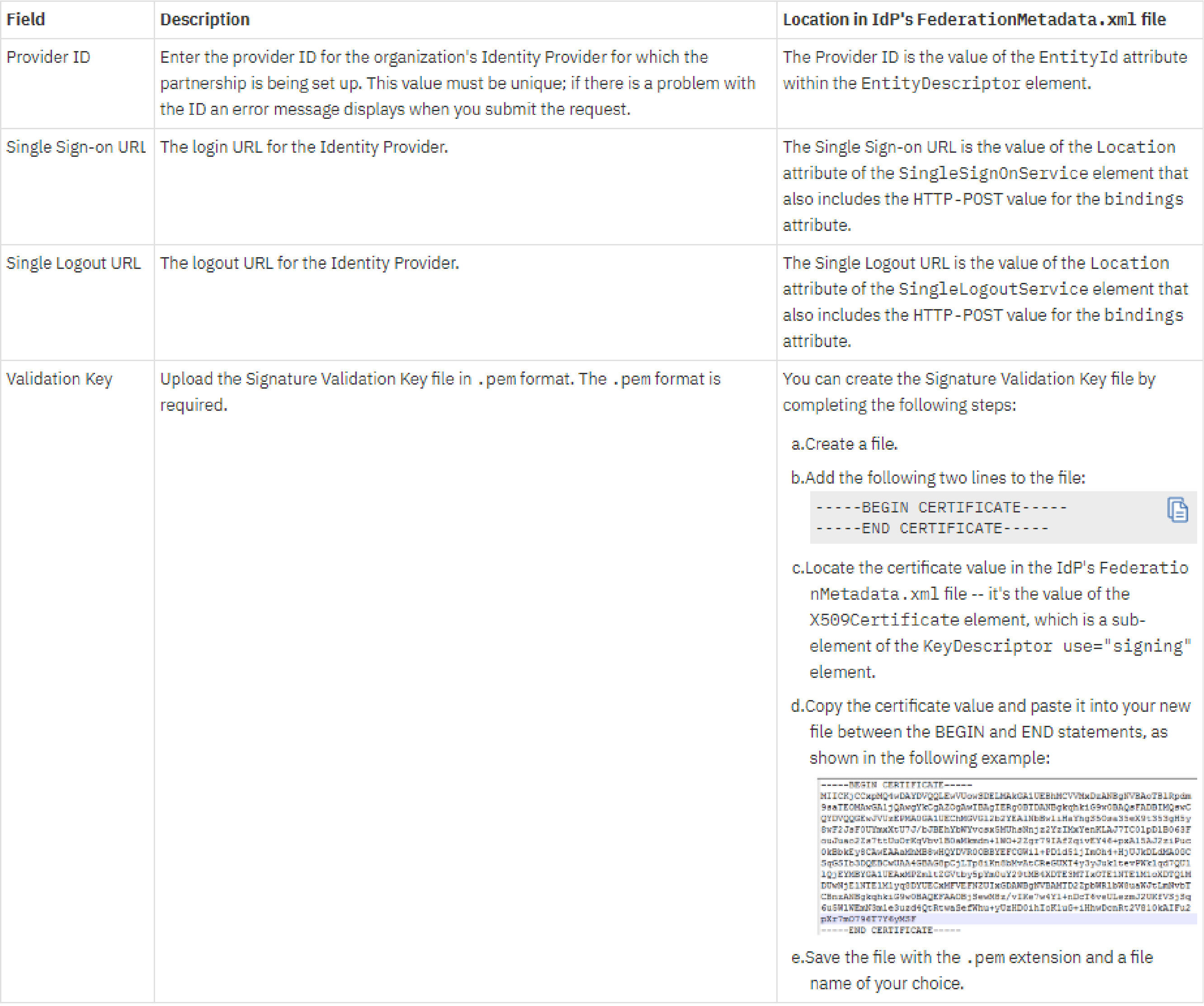
Security > Manage SSO Configuration

A SAML 2.0 Partnership with IBM Connections Cloud is required as part of setting up single sign-on for users in this organization. Select "Cancel" to continue to have users log in using the IBM Connections Cloud login page.

Configuring SAML Partnership – SP side

To apply your IDP settings to Connections Cloud, you simply copy/paste four fields from your IDP metadata into the Self Serve tool – see table

IMPORTANT:
Care is needed when applying this info.
Once you submitted your details, they cannot be undone.
If details need to be changed, engage in Support to delete the SAML Partnership to facilitate re-entering the config again.

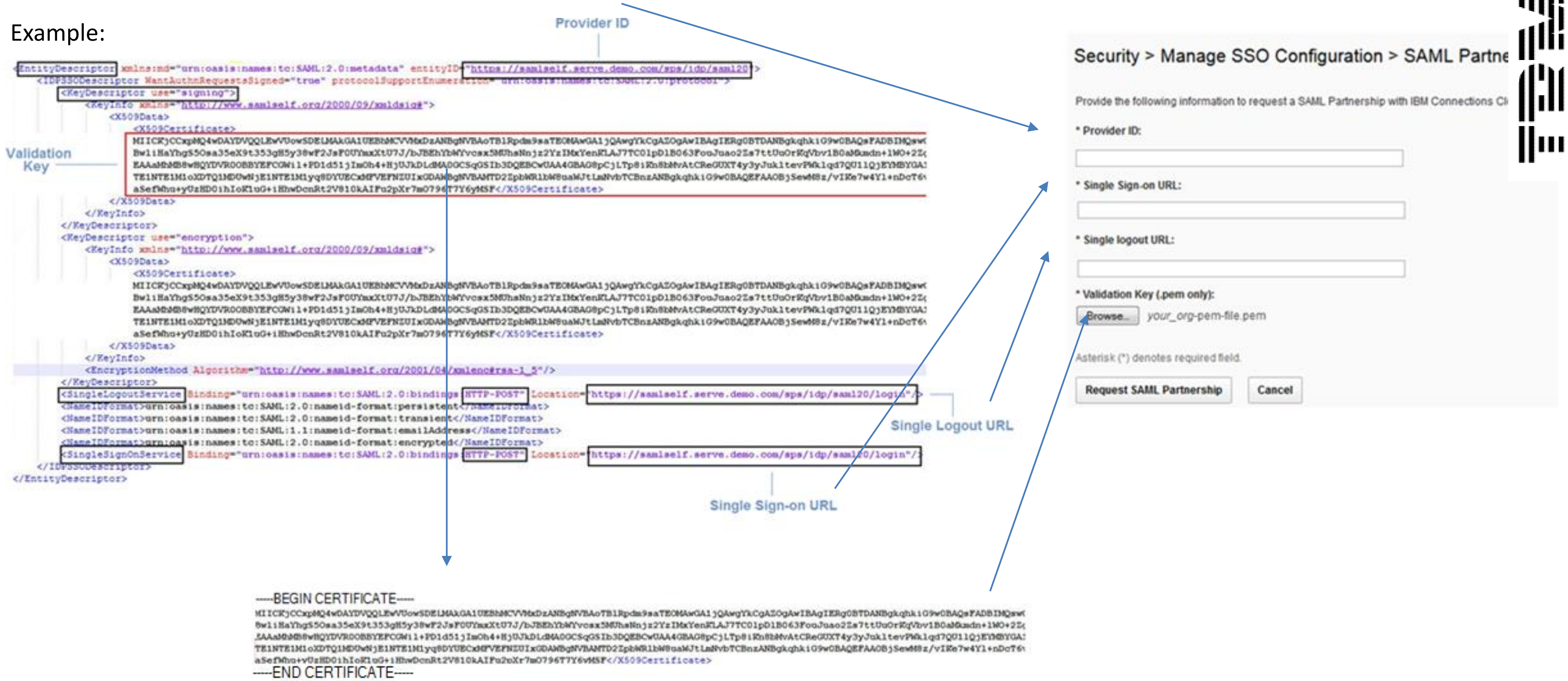


Field	Description	Location in IdP's `FederationMetadata.xml` file
Provider ID	Enter the provider ID for the organization's Identity Provider for which the partnership is being set up. This value must be unique; if there is a problem with the ID an error message displays when you submit the request.	The Provider ID is the value of the `EntityId` attribute within the `EntityDescriptor` element.
Single Sign-on URL	The login URL for the Identity Provider.	The Single Sign-on URL is the value of the `Location` attribute of the `SingleSignOnService` element that also includes the `HTTP-POST` value for the `bindings` attribute.
Single Logout URL	The logout URL for the Identity Provider.	The Single Logout URL is the value of the `Location` attribute of the `SingleLogoutService` element that also includes the `HTTP-POST` value for the `bindings` attribute.

Validation Key	Upload the Signature Validation Key file in `.pem` format. The `.pem` format is required.	You can create the Signature Validation Key file by completing the following steps:
		a.Create a file.
		b.Add the following two lines to the file:
		`-----BEGIN CERTIFICATE-----`
		`-----END CERTIFICATE-----`
		c.Locate the certificate value in the IdP's `FederationMetadata.xml` file -- it's the value of the `X509Certificate` element, which is a sub-element of the `KeyDescriptor use="signing"` element.
		d.Copy the certificate value and paste it into your new file between the BEGIN and END statements, as shown in the following example:
		`-----BEGIN CERTIFICATE-----`
		`MIICKjCCApMQ4wDAYDVQQLEwVUow3DELMAkGA1UEBhMCVVMxDzANBgNVBAoTB1Rpdm`
		`9saTEOMAwGA1jQAwgYkCgAZOgAwIBAgIERg0BTDANBgkqhkiG9w0BAQsFADBIMQswC`
		`QYDVQQGEwJVUzEPMA0GA1UEChMGVGl2b2YEA1NbBwliHaYhg35Oma35eX9t353gH5y`
		`8wF2JsF0UYmxXtU7J/bJBEhYbWYvcsx6HUhsNnjz2YzIMxYenKLAJ7IC01pD1B063F`
		`ouJuac2Zs7ttUuOrKqVbv1B0aMkmdn+1MO+2Zgr79IAf2qivEY46+pxA15AJ2ziPuc`
		`0kBbkEy8CAwEAAaMhMB8wHQYDVR0OBBYEFCOM1l+PD1d51jImOh4+HjUJkDLdMA0GC`
		`5qGSIb3DQEBCwUAA4GBAG0pCjLTp01Kn0bMvAtCReGUXT4y3yJuk1tevPWk1qdTQUl`
		`1QjEYMBYGA1UEAxMPZmlt2GVtbySpYa0uY29tMB4XDTE3MTIxOTE1NTE1MloXDTQ1M`
		`DUwNjE1NTE1MlyqSDYUECxMFVEFNZUIxGDANBgNVBAMTD2ZpbWR1bW0usWJtLmNvbT`
		`CBnzANBgkqhkiG9w0BAQKFAAOBjSewNBz/vIKe7w4Y1+nDcI6veULezmJ2UKfV5j5q`
		`6uSW1NEmN3mle3uzd4QtRcwaSefWhu+yUzHD0ihIoK1uG+iHhwDcmRt2V810kAIFu2`
		`pXr7mO796T7Y6yM5F`
		`-----END CERTIFICATE-----`
		e.Save the file with the `.pem` extension and a file name of your choice.

Configuring SAML Partnership – SP side

Example:



```
<EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" entityID="https://samlself.serve.demo.com/sps/idp/saml20">
    <IDPSSODescriptor WantAuthnRequestsSigned="true" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
        <KeyDescriptor use="signing">
            <KeyInfo xmlns="http://www.samlself.org/2000/09/xmldsig#">
                <X509Data>
                    <X509Certificate>
                    MIICKjCCxpMQ4wDAYDVQQLEwVUowSDELMAkGA1UEBhMCVVMxDzANBgNVBAoTBlRpdm9saTEOMAwGA1jQAwgYkCgAZOgAwIBAgIERg0BTDANBgkqhkiG9w0BAQsFADBIMQsw(
                    Bw1iHaYhgS5Osa35eX9t353gH5y38wF2JsF0UYmxXtU7J/bJBEhYbWYvcsx5MUhsNnjz2YzIMxYenKLAJ7TC01pD1B063FouJuao2Zs7ttUuOrKqVbv1B0aMkmdn+1WO+2Z(
                    EAAaMhMB8wHQYDVR0OBBYEFCGWi1+PD1d51jImOh4+HjUJkDLdMA0GCSqGSIb3DQEBCwUAA4GBAG8pCjLTp8iKn8bMvAtCReGUXT4y3yJukltevPWk1qd7QU11QjEYMBYGA:
                    TE1NTE1M1oXDTQ1MDUwNjE1NTE1M1yq8DYUECxMFVEFNZUIxGDAWBgNVBAMTD2ZpbWR1bW8uaWJtLmNvbTCBnzANBgkqhkiG9w0BAQEFAAOBjSewM8z/vIKe7w4Y1+nDcT6\
                    aSefWhu+yUzHD0ihIoK1uG+iHhwDcnRt2V810kAIFu2pXr7m0796T7Y6yMSF</X509Certificate>
                </X509Data>
            </KeyInfo>
        </KeyDescriptor>
        <KeyDescriptor use="encryption">
            <KeyInfo xmlns="http://www.samlself.org/2000/09/xmldsig#">
                <X509Data>
                    <X509Certificate>
                    MIICKjCCxpMQ4wDAYDVQQLEwVUowSDELMAkGA1UEBhMCVVMxDzANBgNVBAoTBlRpdm9saTEOMAwGA1jQAwgYkCgAZOgAwIBAgIERg0BTDANBgkqhkiG9w0BAQsFADBIMQsw(
                    Bw1iHaYhgS5Osa35eX9t353gH5y38wF2JsF0UYmxXtU7J/bJBEhYbWYvcsx5MUhsNnjz2YzIMxYenKLAJ7TC01pD1B063FouJuao2Zs7ttUuOrKqVbv1B0aMkmdn+1WO+2Z(
                    EAAaMhMB8wHQYDVR0OBBYEFCGWi1+PD1d51jImOh4+HjUJkDLdMA0GCSqGSIb3DQEBCwUAA4GBAG8pCjLTp8iKn8bMvAtCReGUXT4y3yJukltevPWk1qd7QU11QjEYMBYGA:
                    TE1NTE1M1oXDTQ1MDUwNjE1NTE1M1yq8DYUECxMFVEFNZUIxGDAWBgNVBAMTD2ZpbWR1bW8uaWJtLmNvbTCBnzANBgkqhkiG9w0BAQEFAAOBjSewM8z/vIKe7w4Y1+nDcT6\
                    aSefWhu+yUzHD0ihIoK1uG+iHhwDcnRt2V810kAIFu2pXr7m0796T7Y6yMSF</X509Certificate>
                </X509Data>
            </KeyInfo>
            <EncryptionMethod Algorithm="http://www.samlself.org/2001/04/xmlenc#rsa-1_5"/>
        </KeyDescriptor>
        <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://samlself.serve.demo.com/sps/idp/saml20/login"/>
        <NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:persistent</NameIDFormat>
        <NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</NameIDFormat>
        <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</NameIDFormat>
        <NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:encrypted</NameIDFormat>
        <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://samlself.serve.demo.com/sps/idp/saml20/login"/>
    </IDPSSODescriptor>
</EntityDescriptor>
```

```
-----BEGIN CERTIFICATE-----
MIICKjCCxpMQ4wDAYDVQQLEwVUowSDELMAkGA1UEBhMCVVMxDzANBgNVBAoTBlRpdm9saTEOMAwGA1jQAwgYkCgAZOgAwIBAgIERg0BTDANBgkqhkiG9w0BAQsFADBIMQsw(
Bw1iHaYhgS5Osa35eX9t353gH5y38wF2JsF0UYmxXtU7J/bJBEhYbWYvcsx5MUhsNnjz2YzIMxYenKLAJ7TC01pD1B063FouJuao2Zs7ttUuOrKqVbv1B0aMkmdn+1WO+2Z(
EAAaMhMB8wHQYDVR0OBBYEFCGWi1+PD1d51jImOh4+HjUJkDLdMA0GCSqGSIb3DQEBCwUAA4GBAG8pCjLTp8iKn8bMvAtCReGUXT4y3yJukltevPWk1qd7QU11QjEYMBYGA:
TE1NTE1M1oXDTQ1MDUwNjE1NTE1M1yq8DYUECxMFVEFNZUIxGDAWBgNVBAMTD2ZpbWR1bW8uaWJtLmNvbTCBnzANBgkqhkiG9w0BAQEFAAOBjSewM8z/vIKe7w4Y1+nDcT6\
aSefWhu+vUzHD0ihIoK1uG+iHhwDcnRt2V810kAIFu2uXr7m0796T7Y6vMSF</X509Certificate>
-----END CERTIFICATE-----
```

Security > Manage SSO Configuration > SAML Partne

Provide the following information to request a SAML Partnership with IBM Connections Cl

* Provider ID:

* Single Sign-on URL:

* Single logout URL:

* Validation Key (.pem only):

your_org-pem-file.pem

Asterisk (*) denotes required field.

Configuring SAML Partnership – Idp side

Download the SP metadata from Connections Cloud

1. Go to the “Security” UI
2. Download the SP metadata

Finally, follow your IDP documented process to complete the partnership, including;

(depending on your IDP solution)

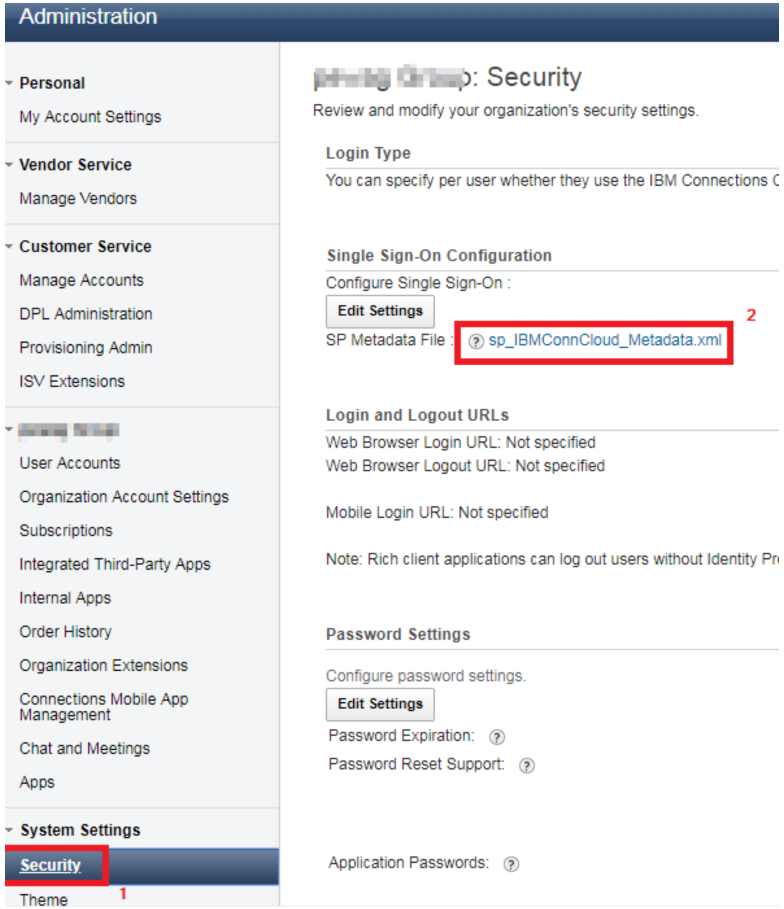
- Apply the SP metadata to your IDP config

  And/OR

- Specify the"Reply URL" to Connections Cloud

  Example:

  https://apps.xx.collabserv.com/sps/sp/saml/v2_0



[redacted]: Security

Review and modify your organization's security settings.

Login Type

You can specify per user whether they use the IBM Connections C

Single Sign-On Configuration

Configure Single Sign-On :

Edit Settings

SP Metadata File : sp_IBMConnCloud_Metadata.xml

Login and Logout URLs

Web Browser Login URL: Not specified

Web Browser Logout URL: Not specified

Mobile Login URL: Not specified

Note: Rich client applications can log out users without Identity Pr

Password Settings

Configure password settings.

Edit Settings

Password Expiration:

Password Reset Support:

Application Passwords:

Updating SAML Partnership

If your SAML signature validation key is expiring/modified on the IDP side, you need to apply the new keyfile to Connections Cloud to maintain the partnership.

If the certificate has expired, there will be a warning message in the Security > Manage SSO Configuration > SAML Partnership

Open a case with Support for assistance in the updating process.

You can update your SAML Partnership via Self Serve by submitting the new file yourself (Note: Support must enable the Self Serve feature first).
To use Self Serve for updating the keyfile, all the following conditions must be met:

- The SubjectDN of the new key matches that of the original keyfile applied to the partnership
- The new key must not expire in 15 days.
- The key must be in .pem format

If any of the conditions are not met, provide us with your new keyfile and we will apply it to the Partnership.
This will result in a short outage as we move from the old to the new certificate – accordingly, close collaboration between Support and customer is required to minimise disruption.

ADFS ROLLOVER WARNING:
If you use AD FS as the IdP, be aware that AD FS can auto roll over of renewed keys.
We would suggest you disable this feature to ensure it doesn't automatically renew the signing keys and rolls them over without IBM applying the renewed keys – this would mean the partnership is broken due to IdP having newer and IBM having older keys. This would result in an outage for your company's federated log-ins until the mismatch of keys is resolved.

Application Passwords

Application passwords are a way for mobile apps to bypass the regular Connections Cloud log in process. Typically, you would avail of this feature if you wanted control over mobile authentication but your IDP does not provide for either of the supported methods of mobile authentication (simple form or HTTP basic).

Application passwords provide an additional layer of password strength. This is due in part to their length (16 characters) and because they are generated using a strong random number generator.

Once enabled, its a one time password.

Administrators can enable/disable the use of application passwords at any time (via the security page) for all users.

Users can then enable, and subsequently revoke & generate new application passwords, at any time via their Account Settings page.

Mobile SSO

The two supported options for Mobile SSO:

(a) IdP supports **HTTP Basic** authentication

(b) IdP's log-in uses **simple form** authentication

-> Requires only the UserName and Password parameters. REF: http://www-01.ibm.com/support/docview.wss?uid=swg27048415

The Mobile SSO flow is referred to as “SP-initiated hybrid for mobile apps and for IBM plug-ins"

- The app issues a request to Connections Cloud asking for the login endpoint
- Connections Cloud looks up the email address and then responds with the login URL of the organization’s mobile authentication mechanism.
- The app performs the authentication request
- If the request is successful, a SAML assertion is returned to the app.
- The app sends the SAML assertion to the Connections Cloud endpoint via HTTP POST.
- If the user has a valid account, access is granted.

This flow model applies to the following apps and IBM plug-ins:

IBM Connections Cloud mobile apps (IBM Connections Social, IBM Connections Chat, IBM Connections Meetings, and IBM Verse)
IBM Connections Desktop Plug-ins for Microsoft Windows
IBM Connections for Mac
IBM Connections Plug-ins for IBM Notes
IBM Connections Plug-in for Microsoft Outlook

Mobile SSO…continued

Important Notes:

- Mobile SSO and Application Password for FEDERATED users do not mix!

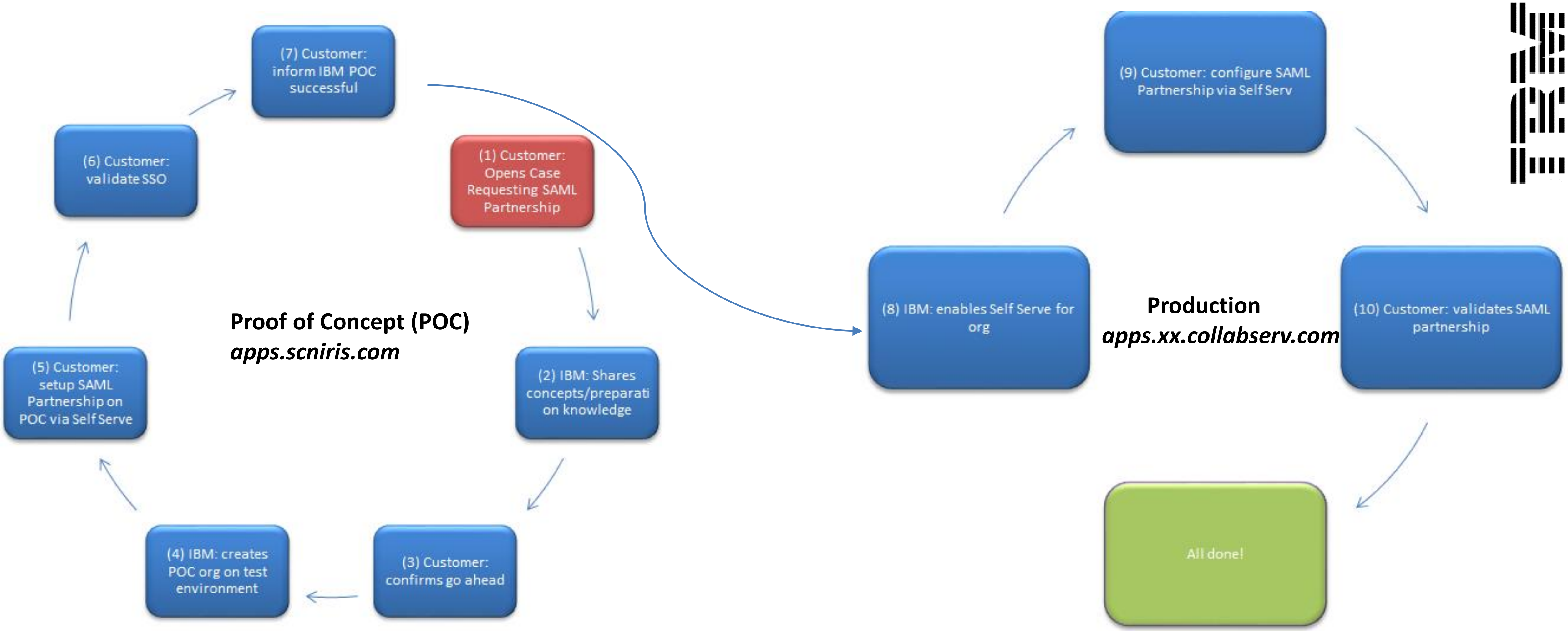
  Once the mobile Login URL has been applied via the Organisation settings page, the application passwords for FEDERATED users will immediately stop working.

  The app will try to submit the credentials to mobile app url, which will have no knowledge of application password's authentication.

  As so, user-education is advised to inform users to use IDP password instead of application password.

- For users with log-in type other than 'FEDERATED', the SSO will not apply i.e. they have to either use their cloud managed regular or application password for mobile app authentication.

SAML Partnership Request process



(1) Customer: Opens Case Requesting SAML Partnership

(2) IBM: Shares concepts/preparati on knowledge

(3) Customer: confirms go ahead

(4) IBM: creates POC org on test environment

(5) Customer: setup SAML Partnership on POC via Self Serve

(6) Customer: validate SSO

(7) Customer: inform IBM POC successful

Proof of Concept (POC)
apps.scniris.com

(8) IBM: enables Self Serve for org

(9) Customer: configure SAML Partnership via Self Serv

(10) Customer: validates SAML partnership

All done!

Production
apps.xx.collabserv.com

Observations

TIME/PROBLEMS

How long does it take to establish SAML Partnership with Connections Cloud?
Time/effort is minimal in Connections Cloud side.
The majority of time is consumed on the customer end configuring and validating the SAML Partnership.

The vast majority of problems hit during SAML Partnership are related to issues or (mis)understanding on the IDP side.
The configuration on the Connections Cloud side (SP) is minimal i.e. extract specific values from IDP exported metadata and apply to Connections Cloud Self Serve.

We strongly urge customers to gain a good understanding of the IDP configuration/requirements prior to engaging with Support to establish SAML Partnership. This will reduce risk of delays and problems in completing the Partnership.

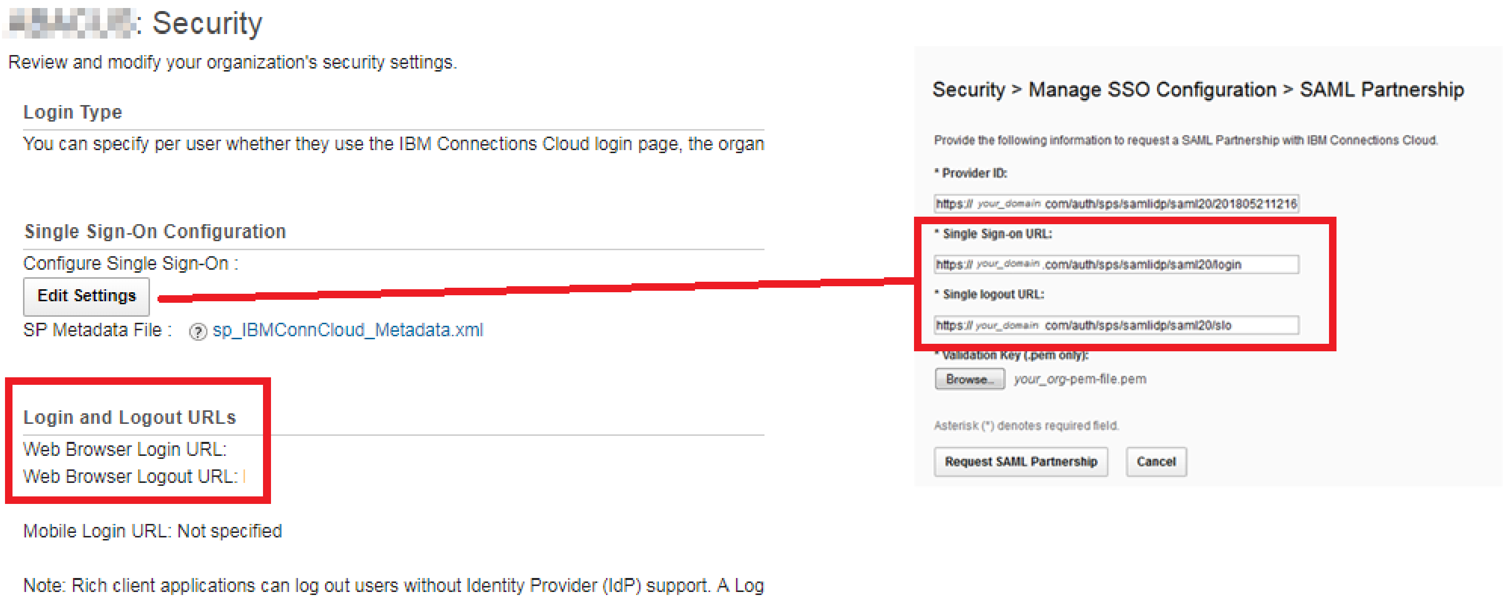
Observations

Confusion: Web Login/LogOut URLs Vs SAML Partnership Sign-on & Sign-Out URLs

Security Page: Login URL & Logout URL
These are *only* needed for Hybrid SP-initiated login flow i.e. where your users connect to Connections Cloud first, only to be redirected to your IDP for login, and subsequently logout when the user's session is cleared/expires.

Vs

SAML Partnership Page:
Single Sign-on URL & Single Sign-out URL
These values specified to configure the SAML Partnership (can be found in IDP metada. REF Slide 10)



[redacted]: Security

Review and modify your organization's security settings.

Login Type

You can specify per user whether they use the IBM Connections Cloud login page, the organ

Single Sign-On Configuration

Configure Single Sign-On :

SP Metadata File : sp_IBMConnCloud_Metadata.xml

Login and Logout URLs

Web Browser Login URL:

Web Browser Logout URL:

Mobile Login URL: Not specified

Note: Rich client applications can log out users without Identity Provider (IdP) support. A Log

Security > Manage SSO Configuration > SAML Partnership

Provide the following information to request a SAML Partnership with IBM Connections Cloud.

* Provider ID: https:// your_domain com/auth/sps/samlidp/saml20/201805211216

* Single Sign-on URL: https:// your_domain .com/auth/sps/samlidp/saml20/login

* Single logout URL: https:// your_domain com/auth/sps/samlidp/saml20/slo

* Validation Key (.pem only): your_org-pem-file.pem

Asterisk (*) denotes required field.

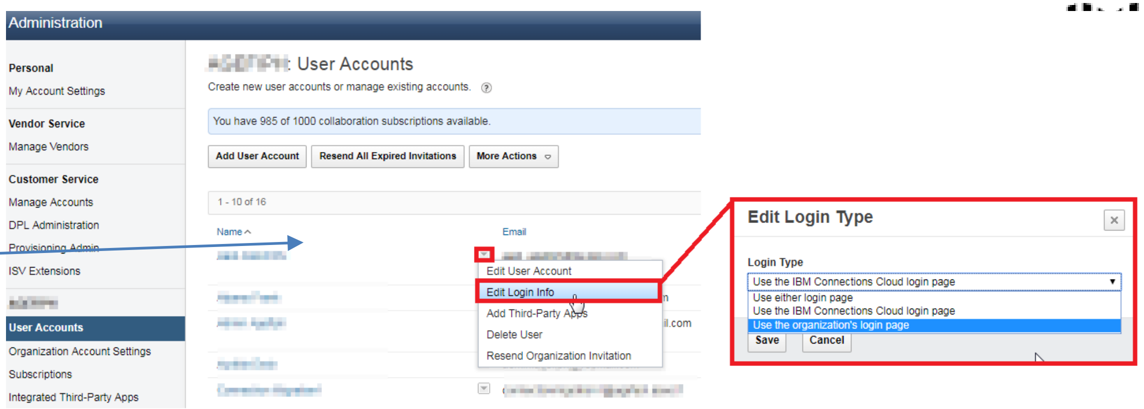
IMPORTANT: to validate SAML Partnership is working in POC phase, Web Login/Logout URLs are not required.

However, if you are planning to use Sp-initiated, you should validate Web Login/Logout URLs

Troubleshooting

If issues encountered during the Partnership setup, complete the following checklist:

- Can you login using IDP initiated flow?
- Is the user set to FEDERATED in Connections Cloud?



Administration

Personal
My Account Settings

Vendor Service
Manage Vendors

Customer Service
Manage Accounts
DPL Administration
Provisioning Admin
ISV Extensions

[redacted]
User Accounts
Organization Account Settings
Subscriptions
Integrated Third-Party Apps

[redacted]: User Accounts

Create new user accounts or manage existing accounts.

You have 985 of 1000 collaboration subscriptions available.

Add User Account | Resend All Expired Invitations | More Actions

1 - 10 of 16

Name	Email
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

Edit User Account
Edit Login Info
Add Third-Party Apps
Delete User
Resend Organization Invitation

Edit Login Type

Login Type: Use the IBM Connections Cloud login page

Use either login page
Use the IBM Connections Cloud login page
Use the organization's login page

Save | Cancel

- Review the IDP configuration to ensure:
  - The Connections Cloud SAML Partnership config (Self Serve) exactly match what is in the IDP metadata
  - The SP metadata been imported into the IDP config?

- Is there an authentication exception? If so, cross check the exception against these common IDP issues:

Error	Resolution
FBTSML225E Token exchange failed. com.tivoli.am.fim.trustserver.sts.STSModuleException: +null at …	This typically means that a FEDERATED user is PENDING in the service. To resolve this issue, the customer admin should force_activate the user using the integration server (https://www.ibm.com/support/knowledgecenter/en/SSL3JX/admin/IntegrationServer/llis_userprovchgfile_c.html) Or change the login type of the user to be Non-FED or mod-FED to allow the user to login thus activating the account - then change the user back to be FED.
FBTSML241E The incoming HTTP message is not valid.	Most likely cause of this is that the IdP made a GET request to our SAML endpoint instead of a POST.
FBTSML200E Unexpected exception: java.lang.NullPointerException at com.tivoli.am.fim.saml20.protocol.actions.sso.SAML20ExchangeTokenAtSPAction.getPartner(SAML20ExchangeTokenAtSPAction.java:754)	This mostly is the case when the IdP is ADFS. If it is not configured to send email address, Connections Cloud fails to validate the SAML assertion with the NullPointerException. First, for the users who are facing the issue, check if the AD record does have an email address associated. Next, check if the RP rule are set as below. 1) Make sure that Relying party trust has a claim rule with following mapping (LDAP attribute) -> (Outgoing Claim Type) E-Mail-Addresses -> E-Mail Address 2) Then add another rule and choose 'Transform an Incoming Claim' as the claim rule template. In this, give some name to the rule. Make sure that Incoming claim type = E-Mail Address Outgoing claim type = Name ID Outgoing Name ID format = Email
FBTSTS001E The given SAML assertion is not valid yet	The SAML assertion that is passed to Connections Cloud has a constraint on its validity i.e. not valid before a timestamp. Example, the given timestamp is faster than the Connections Cloud clock. Hence, we reject it saying it is not yet valid. If only one customer is impacted, it is very likely that your IdP clock is not synchronized with NTP service or somehow your IdP clock is faster than Connections Cloud. Check the 'NotBefore' skew in your IdP setting. We recommend a skew of 3-4 minutes to take care of possible clock synchronization issues between SP & IdP.

Error	Resolution

FBTSML234E No principal was found for alias <username>
FBTSML200E Unexpected exception:
com.tivoli.am.fim.saml.exception.SAMLException: FBTSML234E
No principal was found for alias abc@xyz.com
and partner provider
https://apps.scniris.com/sps/sp/saml/v2_0|https://aak0435.my-dev.centrify.com/a737c964-7880-421c-9575-201be7158a71. at
	the IdP is sending Connections Cloud the subject in SAML assertion having NameID Format as "**persistent**".
	<saml:Subject>
	    <saml:NameID Format="**urn:oasis:names:tc:SAML:2.0:nameid-format:persistent"**
	        SPNameQualifier="https://apps.collabservnext.com"
	        >furuie@mailinator.com</saml:NameID>
	    <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
	      <saml:SubjectConfirmationData NotOnOrAfter="2015-10-01T02:38:48Z"
	            Recipient="https://apps.collabservnext.com/sps/sp/saml/v2_0/login"
	            />
	    </saml:SubjectConfirmation>
	  </saml:Subject>
	
	And, we expect it to be emailAddress.
	For example:
	 <saml:Subject>
	    <saml:NameID Format="**urn:oasis:names:tc:SAML:2.0:nameid-format:email**">abc@xyz.com</saml:NameID>
	    <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
	     ....
	    </saml:SubjectConfirmation>
	  </saml:Subject>
	The IdP should fix their side's configuration for our partnership and then the issue will be gone.

2016-06-02T02:13:14Z FBTSML225E Token exchange failed. com.tivoli.am.fim.trustserver.sts.STSModuleException: **FBTSTS019E The audience in the assertion does not match the Service Provider's URI.** at com.tivoli.am.fim.trustserver.sts.modules.Saml20STSTokenModule.validateConditions(Saml20STSTokenModule.java:2740) at	The IdP's SAML assertion doesn't have the right value for audience restriction. For example, we expect: <saml:AudienceRestriction> <saml:Audience>**https://apps.xx.collabserv.com/sps/sp/saml/v2_0**</saml:Audience> </saml:AudienceRestriction>
FBTSML236E The assertion issued by <IDP-Entity-ID> could not be validated or decrypted.	Two likely causes a) The pair of certificates (signing & encryption) at IdP have been changed and there's a mismatch with public keys in the Connections Cloud side's partnership. In case of AD FS as the IdP, there's a feature called 'auto-rollover'. That feature renews certificates, keeps them along with old certificates for a short duration. And at some point, automatically rolls over the new certificate. If AD FS admin is unaware of this and/or if the rollover is not gracefully handled by informing Connections Cloud Security team, the above error will be seen. In short, when this error is seen, check for a change in your IdP metadata, mainly around the SAML signing keys. b) The partnership is either incorrect or missing in Connections Cloud. Common issue upon first time setup for the partnership is the details entered into the Self Serve tool were incorrect. Doublecheck the value for Provider ID (in Self Serve) match what is specified EntityId attribute within the EntityDescriptor element on the IDP metadata

Error	Resolution
FBTSTS006E No audience has been found in the given assertion.	In the SAML assertion, IdP is expected to specify audience as per our shared SP metadata: *<saml:AudienceRestriction>* *<saml:Audience>https://apps.xx.collabserv.com/sps/sp/saml/v2_0</saml:Audience>* *</saml:AudienceRestriction>* If this element is missing from the SAML assertion, Connections Cloud will throw error: **FBTSTS006E** The IdP side should fix this part in their configuration.
FBTSML237E The SAML message could not be decrypted. com.tivoli.am.fim.liberty.schemas.misc.LibertySchemaException: ++java.lang.RuntimeException: javax.crypto.BadPaddingException: Decryption error at com.tivoli.am.fim.liberty.schemas.util.MiscUtils.decryptXML(MiscUtils.java:929)	The error indicates that Customer not encrypting their assertion with our public encryption key. Customer should import SP Connections Cloud metadata to configure SAML partnership correctly at their end.
Your Organization's login page is unknown Your organization uses a different login page. Contact your organization for details on how to access this page. If you need assistance, email support	This is a failed attempt to follow SP-initiated flow when there is no Web Login URL specified. FEDERATED user has connected to Connections Cloud (and expects to be redirected to customer IDP for login) but the Web Browser Login URL is missing

If problem persists, engage with IBM Support and provide:

- The email address of the impacted user
- Are all users impacted or just one?
- Screenshot of the authentication exception (if there is one).

Summary/Documentation

Review/understand the following information:

Concepts: https://www.ibm.com/support/knowledgecenter/SSL3JX/admin/SAMLFederatedIdentity/fim_concepts.htm
Prepare/Checklist: https://www.ibm.com/support/knowledgecenter/SSL3JX/admin/SAMLFederatedIdentity/fim_preparing.html
Enabling: https://www.ibm.com/support/knowledgecenter/SSL3JX/admin/SAMLFederatedIdentity/fim_enabling.html

Open a case with Support whom will assist in validating a proof of concept SAML Partnership in a pre-production environment.
Support will guide you through POC, and subsequently production, configuration of SAML partnership using the following steps:

Change login: https://www.ibm.com/support/knowledgecenter/SSL3JX/admin/SAMLFederatedIdentity/saml_part_nonfed_enable_sso.html
Config (self Serve): https://www.ibm.com/support/knowledgecenter/SSL3JX/admin/SAMLFederatedIdentity/saml_part_config_sso.html
Updating your IDP: https://www.ibm.com/support/knowledgecenter/SSL3JX/admin/SAMLFederatedIdentity/saml_part_add_to_org.html
Updating certificate: https://www.ibm.com/support/knowledgecenter/SSL3JX/admin/SAMLFederatedIdentity/saml_part_update.html

Questions ???