MobileIron Access Cookbook

Access with Facebook Workplace and Pingone

07 February 2018

Contents

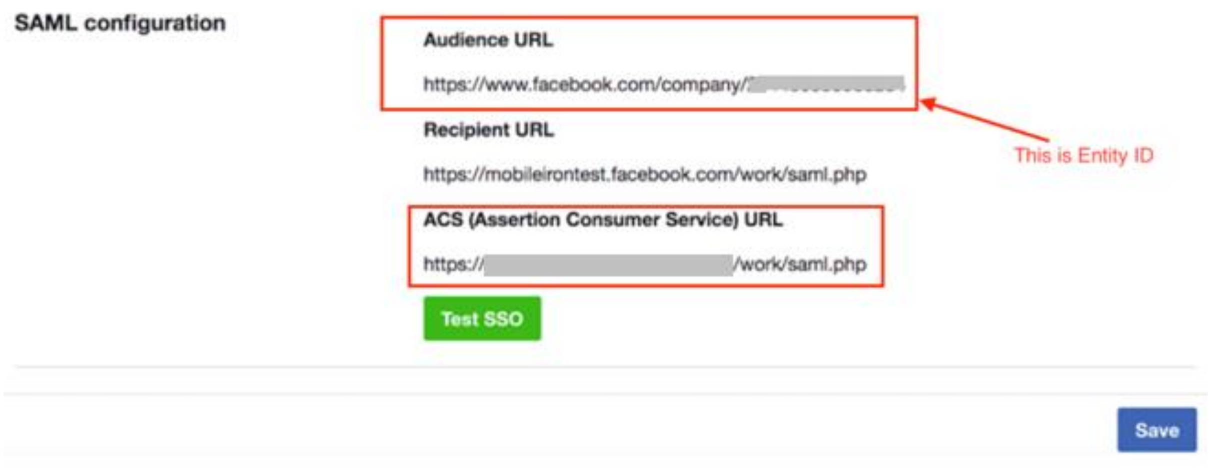
Overview

SAML provides single sign-on service for users accessing their services hosted in a cloud environment. Generally, a service provider such as Facebook Workplace is federated with an identity provider such as Pingone for authentication. The user gets authenticated by Pingone and obtains a SAML token for accessing applications in a cloud environment, such as Facebook Workplace.

This guide serves as step-by-step configuration manual for users using Pingone as an authentication provider with Facebook Workplace in a cloud environment.

Prerequisites

- Ensure that you have a working setup of the Facebook Workplace and Pingone pair without MobileIron Access.
- **Metadata files for Facebook Workplace**
  1. Login to Facebook Workplace with admin credentials.
  2. Click **Dashboard** > **Authentication**. Scroll down to SAML configuration and note the **Audience URL** and **ACS URL** as sown below:



SAML configuration

Audience URL

https://www.facebook.com/company/[redacted]

Recipient URL

https://mobileirontest.facebook.com/work/saml.php

This is Entity ID

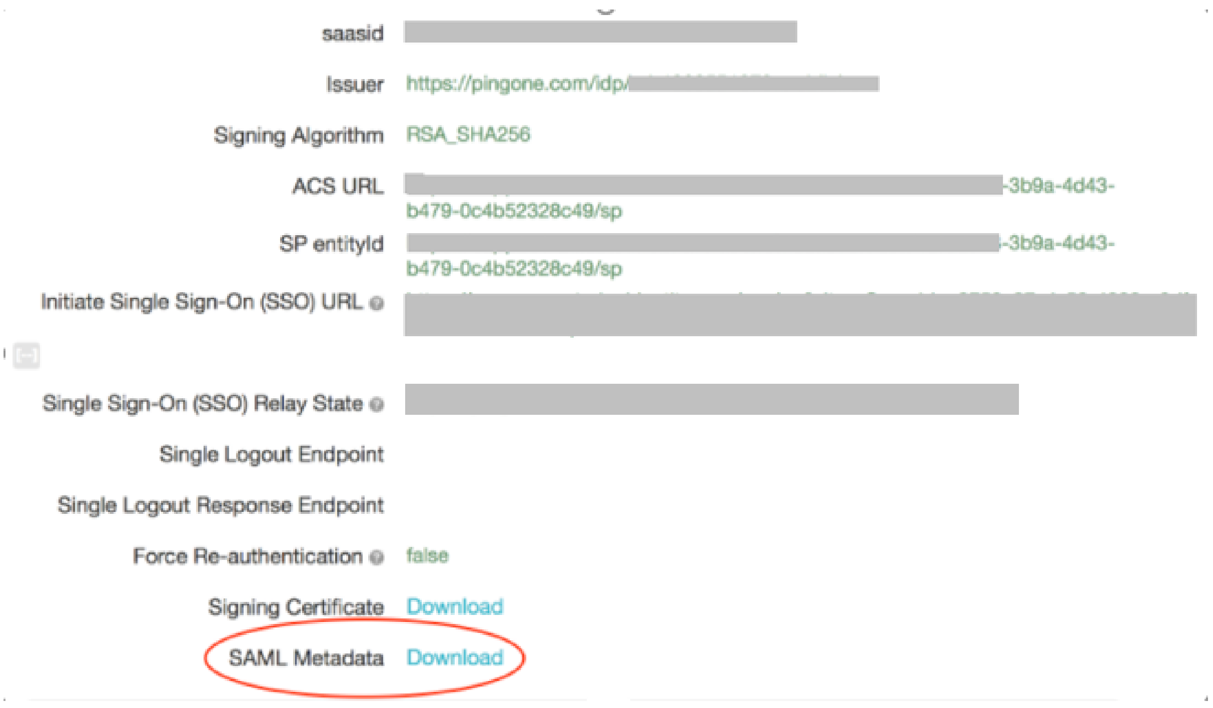
ACS (Assertion Consumer Service) URL

https://[redacted]/work/saml.php

- **Metadata files for Pingone**:

  1. Login to Pingone with admin credentials.
  2. Click **Applications** and select Facebook Workplace application.

3. Scroll down and download the metadata file for Pingone.



saasid	[redacted]
Issuer	https://pingone.com/idp/[redacted]
Signing Algorithm	RSA_SHA256
ACS URL	[redacted]-3b9a-4d43-b479-0c4b52328c49/sp
SP entityId	[redacted]-3b9a-4d43-b479-0c4b52328c49/sp
Initiate Single Sign-On (SSO) URL	[redacted]
Single Sign-On (SSO) Relay State	[redacted]
Single Logout Endpoint	
Single Logout Response Endpoint	
Force Re-authentication	false
Signing Certificate	Download
SAML Metadata	Download

Configuring Facebook Workplace and Pingone with MobileIron Access

You must perform the following tasks to configure Facebook Workplace and Pingone with MobileIron Access:

- Registering Sentry to Access
- Configuring Access to create a Federated Pair
- Configuring Facebook Workplace with MobileIron Access
- Configuring Pingone with MobileIron Access

Registering Sentry to Access

You must register Sentry to Access to fetch the latest configuration from Access.

Prerequisite

Verify that you have registered Sentry earlier. If so, then do not perform this step.

Procedure

1. **Clish** Sentry. In the configuration mode, execute the following command for registration.
   (config)#accs registration https:/<FQDN of Access server><Admin Username of Access Server>
2. Enter the **Tenant password** and complete the registration.
3. In **Access**, click the **Sentry** tab.
4. Select the appropriate Sentry instance, then click **Action** > **Assign**.
5. Click **OK**.
6. **Clish** Sentry and execute the following command in configuration mode to fetch the latest configuration from Access immediately:

   ```
   (config)# accs config-fetch update
   ```

   Note: All the published configuration changes are fetched by Sentry assigned to the profile in fifteen minutes. However, if you want to see the changes immediately, then perform Step 6.

Configuring Access to create a Federated Pair

You must configure Access to create a federated pair.

Prerequisites

Verify that you have configured Facebook Workpalce and Pingone natively.

Procedure

1. Log in to **Access**.
2. Click **Profile** > **Get Started**.
3. Enter the Access host information, and upload the **ACCESS SSL certificate** in p12 format. All the other fields are set to default. Click **Save**.
4. On the **Federated Pairs** tab, click **Add New Pair** and select **Facebook Workpalce** as the service provider.
5. Enter the following details:
    a. Name
    b. Description
    c. Upload the Access Signing Certificate or click **Advanced Options** to create a new certificate.
    d. Select **Add Metadata** and enter the **Entity ID** and **Assertion Consumer service URL**. See Prerequisites.
    e. (Optional) Select *Use Tunnel Certificates for SSO* to configure Cert SSO on MobileIron Core. See *Appendix* in the *MobileIron Access Guide* at https://support.mobileiron.com/docs/current/accs/
6. Click **Next**.
7. Select **Pingone** as the Identity provider. Click **Next**.
8. Select the Access signing Certificate or click **Advanced options** to create a new certificate.
9. Upload the IdP metadata file that you downloaded. See Prerequisites. Click **Done**.
10. Download the **ACCESS SP Metadata (Upload to IDP)** and the **ACCESS IDP Metadata (Upload to SP)** files from the federated pair page.
11. On the **Profile** tab, click **Publish** to publish the profile.

Configuring Facebook Workplace with MobileIron Access

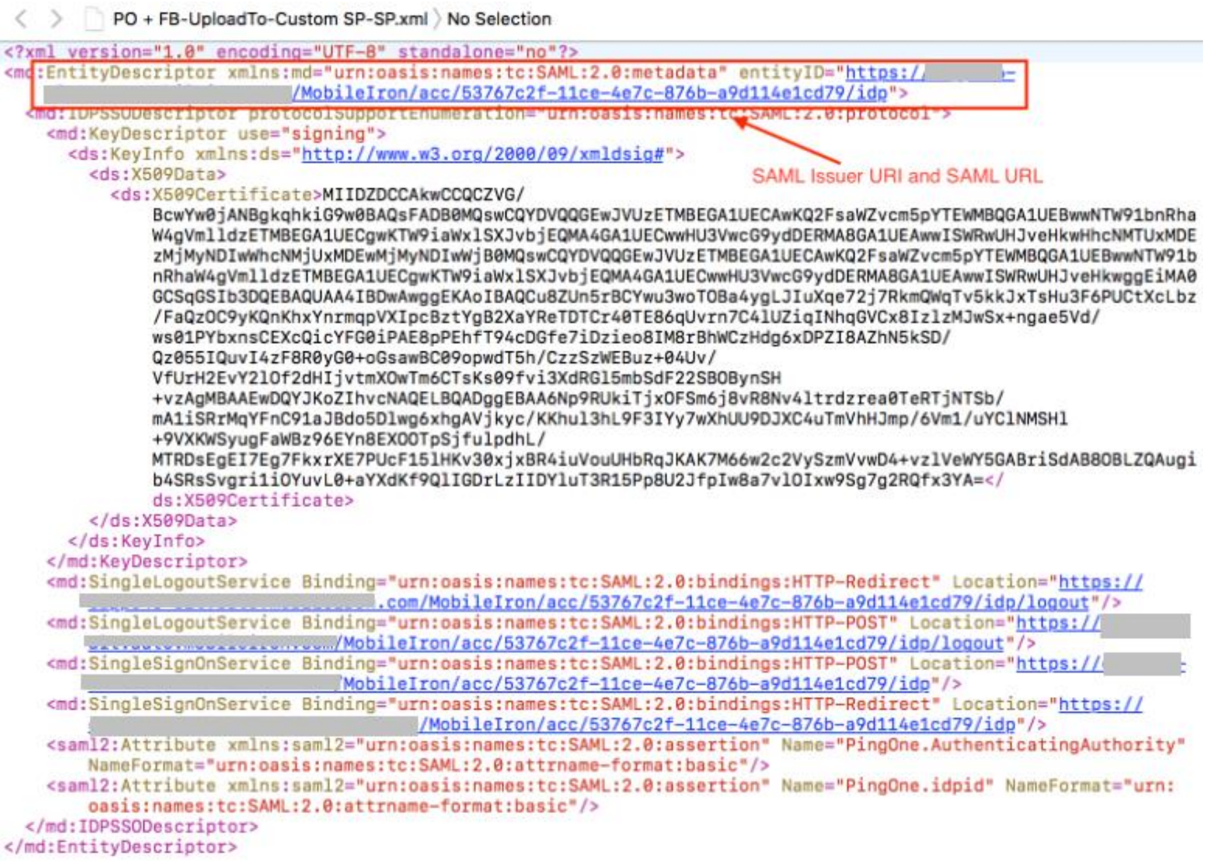
You must configure Facebook Workplace to use with Access.

Prerequisites

- Verify that you have created a federated pair with Facebook Workplace and Pingone.
- Verify that you have configured Facebook Workplace and Pingone natively.

Procedure

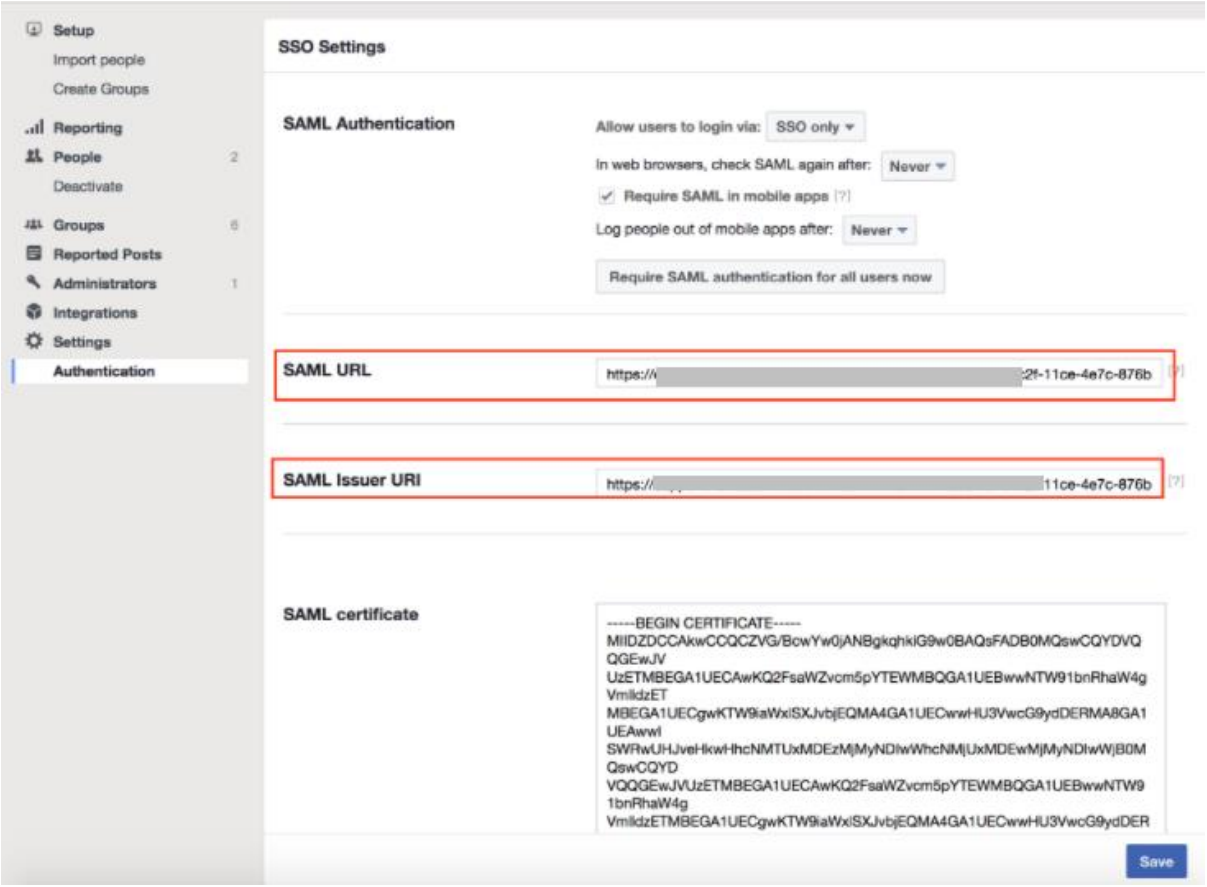
1. Login to the Facebook Workplace with admin credentials.
2. Click on **Dashboard** > **Authentication**.
3. Extract the **SAML Issuer** and **SAML URI** certificate information from Access IDP metadata (Upload to SP) downloaded in **Step 10** of Configuring Access to create a Federated Pair.



PO + FB-UploadTo-Custom SP-SP.xml 〉 No Selection

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" entityID="https://[redacted]-
  [redacted]/MobileIron/acc/53767c2f-11ce-4e7c-876b-a9d114e1cd79/idp">
  <md:IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <md:KeyDescriptor use="signing">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>MIIDZDCCAkwCCQCZVG/
              BcwYw0jANBgkqhkiG9w0BAQsFADB0MQswCQYDVQQGEwJVUzETMBEGA1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UEBwwNTW91bnRha
              W4gVmlldzETMBEGA1UECgwKTW9iaWxlSXJvbjEQMA4GA1UECwwHU3VwcG9ydDERMA8GA1UEAwwISWRwUHJveHkwHhcNMTUxMDE
              zMjMyNDIwWhcNMjUxMDEwMjMyNDIwWjB0MQswCQYDVQQGEwJVUzETMBEGA1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UEBwwNTW91b
              nRhaW4gVmlldzETMBEGA1UECgwKTW9iaWxlSXJvbjEQMA4GA1UECwwHU3VwcG9ydDERMA8GA1UEAwwISWRwUHJveHkwggEiMA0
              GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCu8ZUn5rBCYwu3woTOBa4ygLJIuXqe72j7RkmQWqTv5kkJxTsHu3F6PUCtXcLbz
              /FaQzOC9yKQnKhxYnrmqpVXIpcBztYgB2XaYReTDTCr40TE86qUvrn7C41UZiqINhqGVCx8IzlzMJwSx+ngae5Vd/
              ws01PYbxnsCEXcQicYFG0iPAE8pPEhfT94cDGfe7iDzieo8IM8rBhWCzHdg6xDPZI8AZhN5kSD/
              Qz055IQuvI4zF8R0yG0+oGsawBC09opwdT5h/CzzSzWEBuz+04Uv/
              VfUrH2EvY2lOf2dHIjvtmXOwTm6CTsKs09fvi3XdRGl5mbSdF22SBOBynSH
              +vzAgMBAAEwDQYJKoZIhvcNAQELBQADggEBAA6Np9RUkiTjxOFSm6j8vR8Nv4ltrdzrea0TeRTjNTSb/
              mA1iSRrMqYFnC91aJBdo5Dlwg6xhgAVjkyc/KKhul3hL9F3IYy7wXhUU9DJXC4uTmVhHJmp/6Vm1/uYClNMSHl
              +9VXKWSyugFaWBz96EYn8EXOOTpSjfulpdhL/
              MTRDsEgEI7Eg7FkxrXE7PUcF15lHKv30xjxBR4iuVouUHbRqJKAK7M66w2c2VySzmVvwD4+vzlVeWY5GABriSdAB8OBLZQAugi
              b4SRsSvgri1iOYuvL0+aYXdKf9QlIGDrLzIIDYluT3R15Pp8U2JfpIw8a7vlOIxw9Sg7g2RQfx3YA=</
              ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </md:KeyDescriptor>
    <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://
        [redacted].com/MobileIron/acc/53767c2f-11ce-4e7c-876b-a9d114e1cd79/idp/logout"/>
    <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://[redacted]
        [redacted]/MobileIron/acc/53767c2f-11ce-4e7c-876b-a9d114e1cd79/idp/logout"/>
    <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://[redacted]-
        [redacted]/MobileIron/acc/53767c2f-11ce-4e7c-876b-a9d114e1cd79/idp"/>
    <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://
        [redacted]/MobileIron/acc/53767c2f-11ce-4e7c-876b-a9d114e1cd79/idp"/>
    <saml2:Attribute xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion" Name="PingOne.AuthenticatingAuthority"
        NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"/>
    <saml2:Attribute xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion" Name="PingOne.idpid" NameFormat="urn:
        oasis:names:tc:SAML:2.0:attrname-format:basic"/>
  </md:IDPSSODescriptor>
</md:EntityDescriptor>
```

SAML Issuer URI and SAML URL



SSO Settings

SAML Authentication

Allow users to login via: SSO only ▾

In web browsers, check SAML again after: Never ▾

☑ Require SAML in mobile apps [?]

Log people out of mobile apps after: Never ▾

Require SAML authentication for all users now

SAML URL: https://[redacted]2f-11ce-4e7c-876b [?]

SAML Issuer URI: https://[redacted]11ce-4e7c-876b [?]

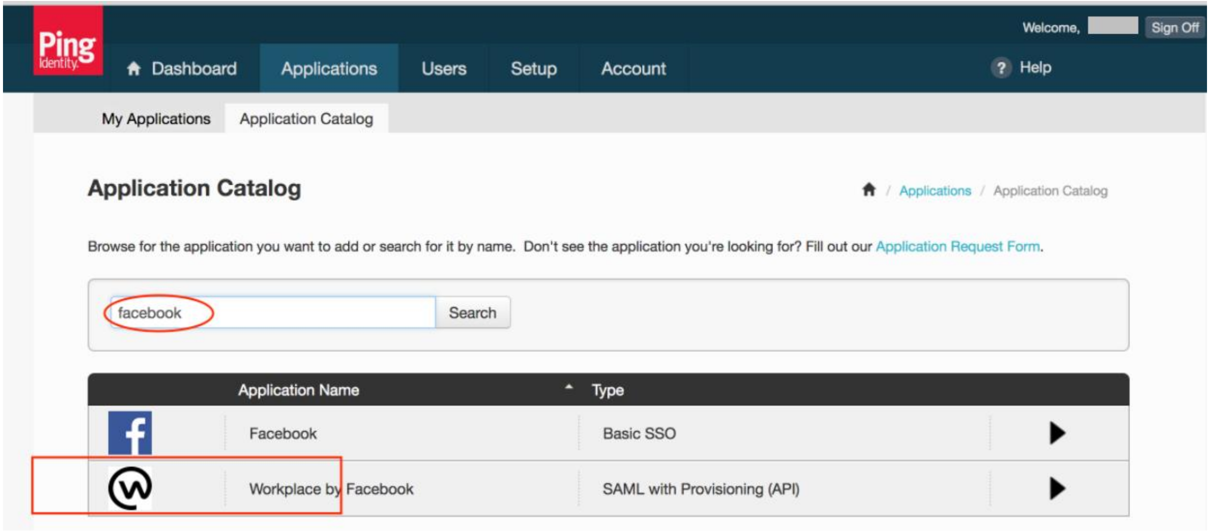
SAML certificate:

```
-----BEGIN CERTIFICATE-----
MIIDZDCCAkwCCQCZVG/BcwYw0jANBgkqhkiG9w0BAQsFADB0MQswCQYDVQ
QGEwJV
UzETMBEGA1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UEBwwNTW91bnRhaW4g
VmlldzET
MBEGA1UECgwKTW9iaWxlSXJvbjEQMA4GA1UECwwHU3VwcG9ydDERMA8GA1
UEAwwI
SWRwUHJveHkwHhcNMTUxMDEzMjMyNDIwWhcNMjUxMDEwMjMyNDIwWjB0M
QswCQYD
VQQGEwJVUzETMBEGA1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UEBwwNTW9
1bnRhaW4g
VmlldzETMBEGA1UECgwKTW9iaWxlSXJvbjEQMA4GA1UECwwHU3VwcG9ydDER
```

Configuring Pingone with MobileIron Access

You must configure the identity provider with the service provider metadata file. This builds the trust relationship with the service provider.

1. Login to Pingone with admin credentials.
2. Click **My Applications** and select **Facebook Workplace** SSO settings.

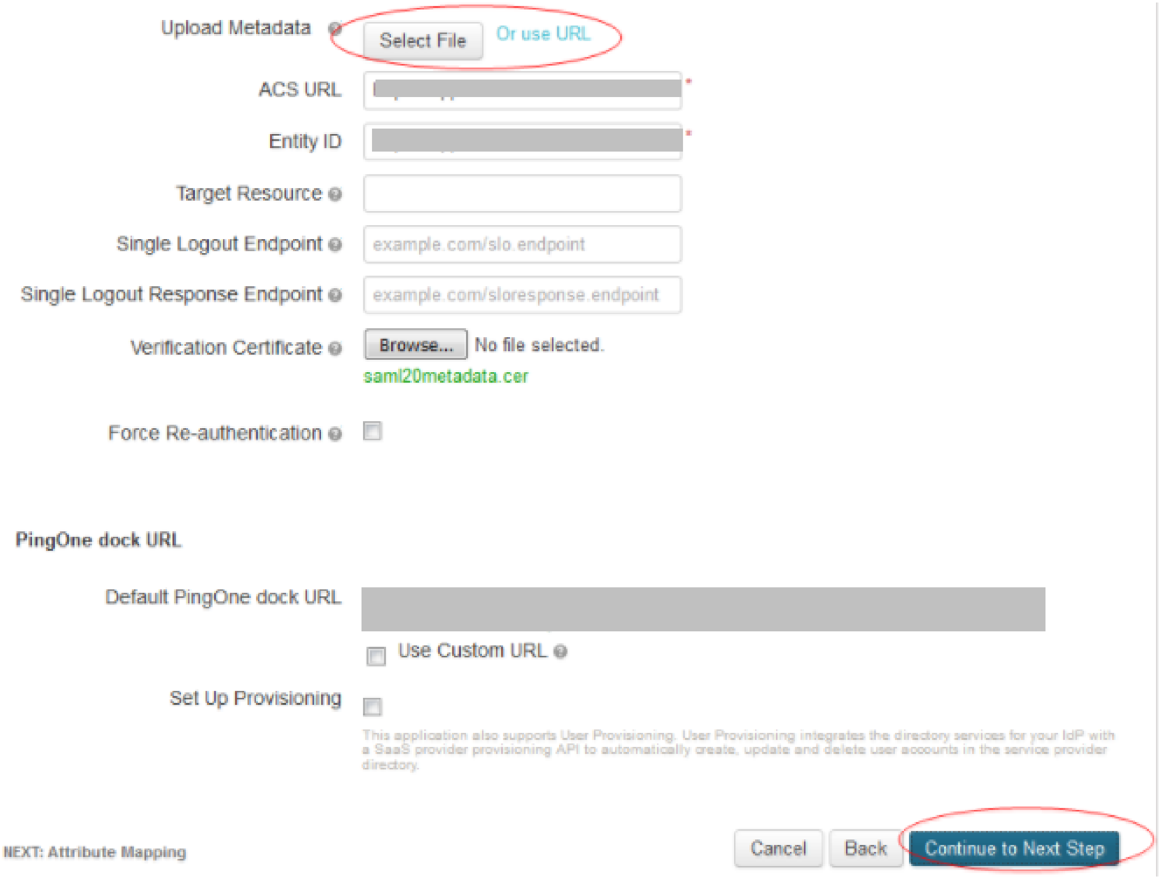


Application Catalog

Browse for the application you want to add or search for it by name. Don't see the application you're looking for? Fill out our Application Request Form.

Application Name	Type
Facebook	Basic SSO
Workplace by Facebook	SAML with Provisioning (API)

3. Click **Edit** > **Continue to Next Step**.
4. Upload the **Access SP Metadata (Upload to IDP)** metadata file in **Step 10** of Configuring Access to create a Federated Pair.



Upload Metadata: Select File Or use URL

ACS URL: [redacted] *

Entity ID: [redacted] *

Target Resource:

Single Logout Endpoint: example.com/slo.endpoint

Single Logout Response Endpoint: example.com/sloresponse.endpoint

Verification Certificate: Browse... No file selected.
saml20metadata.cer

Force Re-authentication: □

PingOne dock URL

Default PingOne dock URL: [redacted]

□ Use Custom URL

Set Up Provisioning: □

This application also supports User Provisioning. User Provisioning integrates the directory services for your IdP with a SaaS provider provisioning API to automatically create, update and delete user accounts in the service provider directory.

NEXT: Attribute Mapping

5. Click **Continue to Next Step** > **Save** > **Publish**.
6. Click **Finish**.

Verification

Facebook Workplace and Pingone is now configured with MobileIron Access. You must validate the new federation settings.

- Register a device to Core.
- Download Facebook Workplace application from App Store.
- Opening this application triggers the per-app-vpn.
- Verify that SAML SSO is working.