Flexible Identity Federation

Quick start guide

version 1.0.1
## Publication history

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
<th>Revision</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015.09.23</td>
<td>initial release</td>
<td>1.0.0</td>
</tr>
<tr>
<td>2015.12.11</td>
<td>minor updates</td>
<td>1.0.1</td>
</tr>
</tbody>
</table>
Welcome

Your company has chosen **Flexible Identity Federation** to protect online corporate identities and corporate data from unauthorized access.

This guide provides:

- An overview of Flexible Identity Federation, related terminology and processes.
- Links to Flexible Identity Federation [Administration](#) and [User](#) guides.
## Contents

1  Service overview .......................................................................................................................... 5  
   1.1  What is Flexible Identity? .................................................................................................... 5  
   1.2  What is Flexible Identity Federation? .................................................................................. 6  
2  What is Identity Federation? .......................................................................................................... 7  
   2.1  Identity Federation mechanisms .......................................................................................... 7  
   2.2  Identity Federation protocols ............................................................................................... 7  
3  What is SAML? ............................................................................................................................... 8  
   3.1  Circle of trust ......................................................................................................................... 8  
   3.2  What is a SAML assertion? ..................................................................................................... 8  
   3.3  SP-Initiated ............................................................................................................................ 9  
   3.4  IdP-Initiated .......................................................................................................................... 10  
4  What is Flexible Identity Federation? .......................................................................................... 11  
   4.1  What is an Identity Bridge? ................................................................................................... 12  
5  Flexible Identity Federation architecture ....................................................................................... 13  
   5.1  What are Flexible Identity Federation Accounts? ............................................................ 13  
   5.2  Lightweight integration with AD Connect .......................................................................... 13  
   5.3  Standard architectures .......................................................................................................... 14  
   5.4  Non-standard architectures ................................................................................................. 16  
6  Users experience ............................................................................................................................ 17  
   6.1  Authentication to the PingOne Dock .................................................................................... 17  
   6.2  Federated SSO ...................................................................................................................... 17  
   6.3  Basic SSO ............................................................................................................................. 17  
   6.4  Flexible Identity Federation User portal ............................................................................. 18  
   6.5  Laptop browser ...................................................................................................................... 18  
   6.6  Mobile browser and application ......................................................................................... 19  
7  Users documentation ....................................................................................................................... 20  
8  Administrators experience ............................................................................................................. 21  
   8.1  What is Flexible Identity Federation Management portal? .............................................. 21  
   8.2  What are Flexible Identity Federation Management portal privileges? ........................ 22  
9  Administrators documentation links ............................................................................................ 23
1 Service overview

1.1 What is Flexible Identity?

Flexible Identity is an enterprise identity hub provided by Orange Business Services.

Flexible Identity:

- is a versatile identity federation and multifactor authentication service
- secures cloud application and VPN access
- leverages existing user stores
- is an affordable, flexible, identity-as-a-service solution
- is a fully managed service offering best-in-class SLA
Flexible Identity Federation

Flexible Identity is made up of the following service blocks:

1.2 What is Flexible Identity Federation?

All the applications that previously were integrated in the customer corporate network are now available in the cloud, making it easier for the customer to operate hardware machines, application software and IT department resources.

The cloud provides countless benefits: access to applications, data and resources from anywhere, at any time. Yet it also demands secure and simple access to applications that are outside your immediate control. Flexible Identity Federation is an Identity as a Service (identity federation solution in the cloud) that connects people to the cloud simply and securely.

Users from external or corporate networks can connect to Flexible Identity Federation and get access to their corporate resources (in the cloud or on the premises) through the User portal.
2 What is identity federation?

Identity federation allows users to have a single account to access applications without having to authenticate each time they connect to another system. This is what is called Single Sign-On (SSO). Federation eliminates the requirement to use and remember passwords by using a secured token that is accepted by the target application. But identity federation is not limited to SSO. This is a complete identity management solution.

2.1 Identity federation mechanisms

Identity federation enables enterprises to exchange identity information securely across Internet domains, providing secure SSO and identity management.

Single sign-on (SSO) is an authentication process that allows users to enter their credentials (for example login/password or One Time Password) once in order to access multiple applications. The process authenticates the users for all the applications for which they have been given rights and eliminates further prompts when they switch applications during a particular session.

Identity federation manages the user’s various identities, providing applications with the appropriate identity. Several identity federation protocols are available, such as Security Assertion Markup Language (SAML), OpenID, OAuth, and WS-Federation for Microsoft applications.

The application a user wants to access needs to be "identity federation aware" using one of the protocols mentioned previously. If not, the application will ask for the credentials which are usually used, generally a username and password that the user will have to store securely. However, the number of applications with different credentials to store and manage will become a burden for the day-to-day user experience. Flexible Identity Federation has considered this state of the art reality and proposes a solution for the time being until the day all applications are integrated with identity federation protocols.

2.2 Identity federation protocols

All identity federation protocols are to a certain extent based on the same principle. A user who accesses a resource needs to present a valid token to the application. This token will be retrieved from an identity provider and consumed by the application that will be considered as a service provider in SAML.

Each time a user accesses a resource, a new token must be generated and consumed by the application. This is done seamlessly in the identity federation protocol to provide Single Sign-On.

Standard identity protocols are: SAML, OpenID, OpenID Connect, WS-Trust, WS-Federation and OAuth.
3 What is SAML?

For now, PingOne is using SAML protocol to give users access to their applications. SAML 2.0 is a language created by OASIS, a global consortium that develops web service standards. It is based on XML language and made for authentication. It could be inserted into HTTP, SOAP, FTP and SMTP requests.

Two operational roles are defined in a SAML SSO transaction:

- **Identity Providers (IdP):** An identity provider is an online service or website that authenticates users by means of login/password, login/OTP, user certificate…

- **Service Providers (SP):** A service provider is an entity that provides Web Services/Applications. A service provider relies on one or multiple trusted identity providers for authentication.

For information, an IdP can also be an SP and have the two roles at the same time. For example, Google Apps can be set up as an IdP or an SP.

3.1 Circle of trust

A trust relationship is defined whereby the SP provides access to users from the IdP. The IdP continues to manage its users, and the SP trusts the IdP to authenticate them. The relationship between these two is known as a circle of trust. To set up this circle of trust, they need to exchange metadata. These metadata are XML files that contain all the SAML URL endpoints, the attributes needed by the SP and the certificates to digitally sign the SAML tokens.

Once the circle of trust is enabled, a user can access applications directly (SP-initiated mode) or from a web portal linked to the IdP (PingOne dock) in order to present a list of applications that has been authorized (IdP-initiated mode).

3.2 What is a SAML assertion?

A SAML assertion is an XML-based format token which exchanges authentication and authorization data between an identity provider and a service provider. You can refer to the Flexible Identity Federation Administration guide for more technical information (format, attributes …)
A user can access applications directly (SP-initiated mode) or from a web portal linked to the IdP in order to present a list of applications that have been authorized (IdP-initiated mode). The exchange of the SAML assertion is explained below for both modes.

### 3.3 SP-initiated

In this scenario, the SP sends an HTTP redirect message to the IdP containing an authentication request. The IdP returns a SAML response with an assertion (or SAML token) to the SP via HTTP POST.

**Processing Steps:**

1. A user requests access to a protected SP resource. The user is not logged on to the site.
2. The SP returns an HTTP redirect (code 302 or 303) containing a SAML request for authentication through the user’s browser to the IdP’s SSO service.
3. If the user is not already logged on to the IdP site or if re-authentication is required, the IdP asks for credentials (e.g. ID and password) and the user logs on.
4. Additional information about the user may be retrieved from the user data store for inclusion in the SAML response (these attributes are predetermined as part of the federation agreement between the IdP and the SP).
5. The IdP’s SSO service returns an HTML form to the browser with a SAML response containing the authentication assertion and any additional attributes. The browser automatically posts the HTML form back to the SP.

Note: the user accesses the SP with a specific URL (i.e. containing the customer domain name such as http://google.com/a/orange.com or orange.salesforce.com), so the SP knows that this user has to be authenticated via a specific IdP.
3.4 IdP-initiated

In this scenario, a user is logged on to the IdP and attempts to access a resource on a remote SP server. The SAML assertion is transported to the SP via HTTP POST.

Processing Steps:

1. A user has logged on to the IdP.
2. The user requests access to a protected SP resource. The user is not logged on to the SP site.
3. Optionally, the IdP retrieves attributes from the user data store.
4. The IdP’s SSO service returns an HTML form to the browser with a SAML response containing the authentication assertion and any additional attributes. The browser automatically posts the HTML form back to the SP.
4 What is Flexible Identity Federation?

Flexible Identity Federation is a security layer between users and the web application they access. It acts as an identity provider interface to publish user identities to authorized cloud applications, depending on user rights.

Flexible Identity Federation provides the following functionalities:

- Users are authenticated once when accessing their desktop, their VPN solution and any application irrespective of their location (internal or cloud apps).
- The user’s expected authentication level is adapted depending on their profile, the application they are accessing or the device they are using.
- It is integrated with the customer corporate directory.

Flexible Identity Federation is based on the PingOne Cloud Access Service (CAS) from the company Ping Identity. It is a fully managed service, implemented on Ping Datacenter and Amazon Web Service Cloud platforms in the US and Europe.

PingOne solution provides simple and secure access to applications. It enables Orange customers to give their employees single sign-on to any application. Furthermore, it centralizes control of applications to put them under the control of the IT department, while delivering the applications users want and need:

- Secure SSO: Employees, customers and partners can get single sign-on to any web application.
- Provisioning: One convenient place for customer IT administrators to create, update and delete accounts.
- PingOne dock: With a single company identity, employees can access cloud applications from a virtual desktop on any device.

Flexible Identity Federation can integrate Orange customer local identity management using the PingOne directory. This feature allows customers to store identities directly in PingOne (authentication/account) and therefore is suitable for any size of company, even the smallest ones with no existing identities directory.

Flexible Identity Federation can also be configured to leverage the existing customer directory (AD, LDAP…) using a lightweight synchronization agent “AD Connect”, the former PingOne identity bridge. It can also leverage the existing customer federation infrastructure using the 3rd party SAML option.

Flexible Identity Federation proposes an application catalog of more than 1700 applications to integrate preconfigured federated applications using SAML or WS Federation and also cloud applications already configured using a password vault. Federated and cloud applications with a standard username/password can also be configured manually on the PingOne administration portal.
To access federated and cloud applications, users simply authenticate once to the Flexible Identity Federation user portal, called the PingOne dock, dynamically displayed based on users’ access rights. Then in a single click, they can access all their authorized business applications.

Flexible Identity Federation transparently authenticates and logs the user into the application, which is launched in a new browser window:

- For federated applications, a federated exchange is created to get a valid token sent to the application (see What is SAML? for more detail).
- For cloud applications with a standard username/password, a browser plugin that has been previously installed transparently sends credentials to the application.

## 4.1 What is an identity bridge?

Identity bridges are used by PingOne to match your local user accounts from your identity repositories to your cloud user accounts.

Identity bridges can be:

- **PingOne AD Connect**: This identity bridge is useful if you want to use your on-premises Active Directory Forest/domain as an identity repository for your users. The users will use their corporate credentials to connect to the SaaS applications. It also enables (through IWA) silent authentication for users from your corporate network.

- **PingFederate (SAML)**: This identity bridge is useful if you want to use PingFederate as a SAML IDP. PingFederate allows you to use multiple identity bridges and develop complex context-based authentication. Users will have to authenticate on PingFederate before getting access to their SaaS applications.

- **Google Apps**: This identity bridge is useful if you want to use your existing Google Apps for Work account as your identity repository. Users will have to authenticate on your Google Apps environment before getting access to their SaaS applications.

- **3rd-party SAML**: This identity bridge is useful if you want to use a 3rd-party SAML as a SAML IDP for PingOne. Multiple SAML IDPs are available, such as Juniper SSL VPN, OpenAM, SafeNet/Gemalto SAS Cloud (Orange Flexible Identity Authentication). Users will have to authenticate on the 3rd-party SAML before getting access to their SaaS applications.

- **PingOne Directory**: This identity bridge is useful if you do not have an identity repository or do not want to use one of yours. With this identity bridge, PingOne creates a cloud identity repository dedicated to your PingOne environment. Users will have to authenticate on this identity repository before getting access to their SaaS applications.
5  Flexible Identity Federation architecture

5.1 What are Flexible Identity Federation accounts?

The Flexible Identity Federation service is based on a structure made of isolated nodes called Accounts. Only Orange Business Services is able to create accounts.

There are 2 account categories within the Flexible Identity Federation structure:

- **Service Provider Account**: root account dedicated to the Orange Business Services teams in charge of the service.
- **PingOne Account**: one or more accounts (depending on the complexity of your organization) created from your Administrator Account by Orange Business Services and dedicated to your users.

5.2 Lightweight integration with AD Connect

PingOne AD Connect light opens a secure channel for communications with PingOne servers using the 443 port. PingOne sends authentication requests through this channel. No incoming traffic from the Internet is necessary towards the AD Connect agent, allowing a secure and quick installation.

High availability (automatic failover and load balancing) is handled by the PingOne datacenters, and requires no configuration or management on your part. You just have to install multiple instances of AD Connect for authentication resiliency. You can also dedicate a specific AD Connect agent for provisioning only in order to split AD Connect features.
user accessing the Flexible Identity Federation portal or the service provider directly being redirected to Flexible Identity Federation

2 credential/identity validated by the corporate directory (no account replication in the cloud) using agent connections

3 authenticated user redirected to the cloud service

No DMZ, no load balancers needed. Just install several AD Connect agents somewhere in your corporate Windows domain to leverage Integrated Windows Authentication (IWA).

5.3 Standard architectures

Each account has its own identity bridge that acts as identity provider on cloud applications.

- For the time being, a trust relation is unique between service provider and identity provider (for example, one Google tenant can be configured with only one identity provider).
- Partners, employees, home workers are managed by the same identity bridge and work on the same service provider instance (same O365 tenant for example).

- Partners, employees, home workers are managed by different identity bridges and work on different service provider instances (different O365 tenant for example).
5.4 Non-standard architectures

- In one account, you cannot merge AD Connect and Ping One directory. Several Flexible Identity Federation accounts must be created.
- Several accounts cannot share the same service provider instance as the trust relation is unique.

For these reasons, some specific scenarios need to be addressed with the PingFederate identity bridge as an option of the Flexible Identity Federation solution.
6 User experience

6.1 Authentication to the PingOne dock

PingOne uses the identity bridge for authentication. When the user tries to sign in to the PingOne dock, they are redirected to the identity bridge for authentication. Once authenticated, they will be redirected to the PingOne dock.

6.2 Federated SSO

In PingOne, federated SSO uses the industry-standard SAML protocol to establish a secure connection, through an identity bridge, to user repositories. User credentials are authenticated through the identity bridge and a token is generated for the credentials with the user attributes. The tokens are then used for single sign-on (SSO) to the federated cloud applications. A secondary level of authentication can be added through the use of an authentication policy.

6.3 Basic SSO

To use this functionality, the user needs to install a plugin on their favorite web browser. They will be asked to create a primary key. This primary key will be used to encrypt their credentials. Their encrypted credentials will be stored in the PingOne cloud so they will be available from anywhere. As the user will be the only one to know their primary key, neither the Orange Business Services team nor the PingOne team can read their encrypted credentials.

The user needs to send their credentials when first connecting to the cloud application:

The PingOne plugin will then reuse their credentials each time the user tries to sign in to the cloud application through the PingOne dock.
If the user wants to switch from one web browser to another, (from a desktop browser to a mobile one for example), they will have to re-enter their primary key to access their stored credentials. Passwords stored can be modified directly in the PingOne dock.

This solution must be used if the cloud application does not allow a SAML authentication. Otherwise, it is advised to use SAML as the authentication method to access the cloud application.

6.4 Flexible Identity Federation user portal

The PingOne dock displays all the applications the users are entitled to access, based on group membership rules defined in PingOne. The PingOne dock logo and texts can be customized to fit the company brand policy.

Access to the portal is supported across all major browsers including Internet Explorer, Firefox, Chrome and Safari. Users can easily access the portal not just from their desktop, but also mobile devices such as tablets and smartphones.

6.5 Laptop browser
6.6  Mobile browser and application

The URL of your Flexible Identity Federation user portal is determined when completing the Service Request Form (aka SRF2). Of course, you can change it afterwards but you need to notify your employees (example of URL: https://desktop.pingone.com/acme).
7 User documentation

User guide
This guide gives instructions for using the PingOne dock and installing the PingOne plugin on your browser to enable Basic SSO.
8 Administrator experience

8.1 What is the Flexible Identity Federation management portal?

The Flexible Identity Federation management portal allows administrators to perform service management functions:

- Selecting and configuring the type of identity bridge,
- Managing local users in the case of the PingOne directory,
- Managing customer administrators (add, delete, role assignment),
- Managing cloud applications using the application catalog or standard application creation with SAML or Basic SSO plugin,
- Configuring strong authentication with the Flexible Identity Authentication solution
- Creating rules to authorize applications for users based on criteria such as group membership, source IP, level of authentication (step-up),
- Accessing a dashboard view for logs and reporting features. Scheduling a predefined report and being able to send it by mail or downloading it from the portal.

As Flexible Identity Federation administrator, there are two different ways to access the management portal:

- Management portal URL

Each administrator has been previously invited to register for the management portal by the main administrator. After authenticating against this portal (https://admin.pingone.com) and accepting agreements, you should be able to manage your Flexible Identity Federation account dedicated to your organization. In this case, each administrator may have a specific privilege on management portal features.
Using the AD Connect identity bridge, you can grant access to the management portal to one of your Active Directory group. Members of this group will have the opportunity to access the management portal through an icon in the PingOne dock. In this case, all group members will have the same privilege on the management portal features.

### 8.2 What are the Flexible Identity Federation management portal privileges?

The Flexible Identity Federation management portal allows administrators to perform service management functions.

Different kinds of privileges can be granted to administrators:

- **Global Administrator:** This role has full permissions to manage and configure all aspects of the account and the admin portal.

- **SaaS Administrator:** This role manages the Application Catalog and application connections, and has access only to these related pages.

- **Directory Administrator:** This role manages the AD Connect configuration and connection, and has access only to the Setup pages.

- **Service User Administrator:** This role manages the PingOne services a user can use, and has access only to the Users by Service, Reports, and Dashboard pages.
9 Administrator documentation links

Administration guide
This guide provides instructions to:

- Configure and install the identity bridge.
- Configure the application.
- Configure the authentication policy.
- Customize the service.