Ping Identity

The Identity Security Company™

SOLUTION BRIEF

Pick Your Identity Bridge

Options for connecting users and resources across the hybrid cloud

Executive Overview

Enterprises are increasing their use of software as a service (SaaS) for two principal reasons: ease of deployment and cost savings. SaaS offers an attractive alternative to the high risk, high investment "big bang" approach to on-premises IT deployments by providing an elastic architecture, reduced IT resource utilization and an externally hosted topography. SaaS offerings also eliminate capital expenditure (CAPEX) by leveraging a subscription-based pricing model; costs scale up or down as utilization changes.

Identity management as a service (IDaaS) applications provide similar advantages. Many enterprises are migrating to IDaaS to take advantage of single sign-on (SSO) and the seamless management of user identities in SaaS applications. As enterprises leverage IDaaS across the hybrid cloud, they will likely require an identity bridge to overcome the "impedance mismatch" between on-premises, SaaS and partner topographies. The identity bridge[1] is important for both "to the cloud" and "from the cloud" application access. On-premises identity systems that leverage Kerberos and LDAP don't make the leap to SaaS applications. External identities, like those of your partners or customers, won't be able to readily connect from their environments to on-premises resources.

PingOne® from Ping Identity® solves these connectivity challenges. This IDaaS offering delivers SSO to SaaS and on-premises environments via a single turnkey solution. PingOne provides SSO to both SAML-enabled and password-based applications. Ping Identity offers two identity bridges — PingFederate® and AD Connect — to allow connectivity to the PingOne IDaaS from the on-premises enterprise.[2] They will be described in detail in this paper.

The purpose of this document is to:

- Define the three identity management disciplines required to provide SSO.
- Describe the attributes and capabilities of the two identity bridges — PingFederate and AD Connect.
- Provide guidance for the selection of an identity bridge for use with PingOne.

1 For a broader discussion of identity bridges, read Gartner's Hype Cycle for Identity and Access Management Technologies, 2013 (subscription required).

2 Organizations can also leverage a third-party federation product—like Microsoft Active Directory Federation Services—to connect to PingOne.

Table of Contents

The Magic of Three

SSO requires three crucial identity management processes. Without these processes, SSO isn't possible.[3]

- **Provisioning.** The provisioning process creates the user account — including associated attributes and access rights — inside the application. The provisioning process may occur at "admin time" in advance — or at runtime when the user attempts to access the application for the first time. Admin time provisioning to a SaaS application is frequently achieved via directory synchronization services. The runtime method is commonly referenced as just-in-time (JIT) provisioning.
- **User Authentication.** The user must prove their identity by providing credentials to the SSO system. After a successful authentication, the user receives a session token. A variety of authentication methods exist, including password and hardware one-time password (OTP) devices. In the case of federation, the session token is typically a SAML credential.
- **Token Issuance.** The session token is presented to relying applications as proof of authentication. Common token types include the previously mentioned SAML, OAuth (particularly for native applications on mobile devices), the venerable web access management (WAM) HTTP cookie for on-premises application access, and Kerberos tickets. Without a token, users must authenticate for each transaction, which isn't really SSO at all.

Ping Identity Bridges

Ping Identity provides two identity bridges for access to PingOne. The AD Connect identity bridge is an unobtrusive, lightweight component. It easily connects to Active Directory and provides a single outbound federation identity provider and provisioning (via directory synchronization services) connection to PingOne. From there, PingOne takes care of the SSO part. PingFederate is a standalone identity bridge that can be used by itself and in conjunction with PingOne.

Provisioning

Before SSO is possible, the organization must define its users in the SaaS applications. The workforce identity "to the cloud" provisioning problem of managing employee identities in SaaS applications — without recreating on-premises identity management investments — is paramount. In addition, many organizations wish to solve the "from the cloud" provisioning problem — granting partner SSO to on-premises applications. Both use cases require provisioning user identities into the application's identity store.

To the Cloud (Employees)

Both PingFederate and AD Connect can provision user identities into SaaS applications via directory synchronization. AD Connect delivers a simplified approach; it monitors Active Directory and synchronizes a subset of user attributes from a single user object. The organization need not reinvent identity management to extend its reach to SaaS applications. The PingOne IDaaS finishes the job of provisioning users into SaaS applications. The result is a low-touch, rapidly installed and simply configured synchronization process (Figure 1).

3 Some might argue that SSO is possible without the provisioning process if user access to the application is anonymous. But anonymous access to enterprise applications is extremely rare as it precludes the application's ability to restrict access to specific resources and audit user activity.

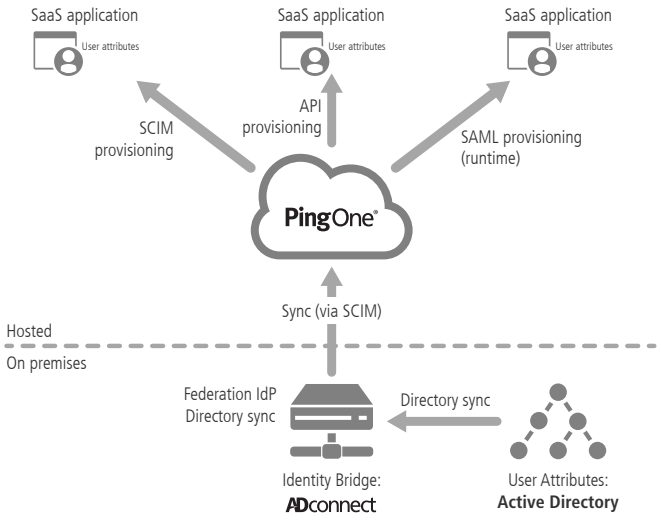


Figure 1. Provisioning via AD Connect

Compared to AD Connect, PingFederate has additional provisioning capabilities and supports additional user directories. It can also correlate user attributes from multiple, heterogeneous identity stores and then synchronize the composite user identity to PingOne (Figure 2). As with AD Connect, PingOne finishes the process and manages user identities within the SaaS applications.

In addition to using PingOne as the provisioning engine, organizations can also use a combination of PingFederate and PingOne to provision user identities in applications (not shown). The use of PingFederate as the provisioning engine may be applicable for specific partner applications, while using PingOne for a broader set of SaaS applications.

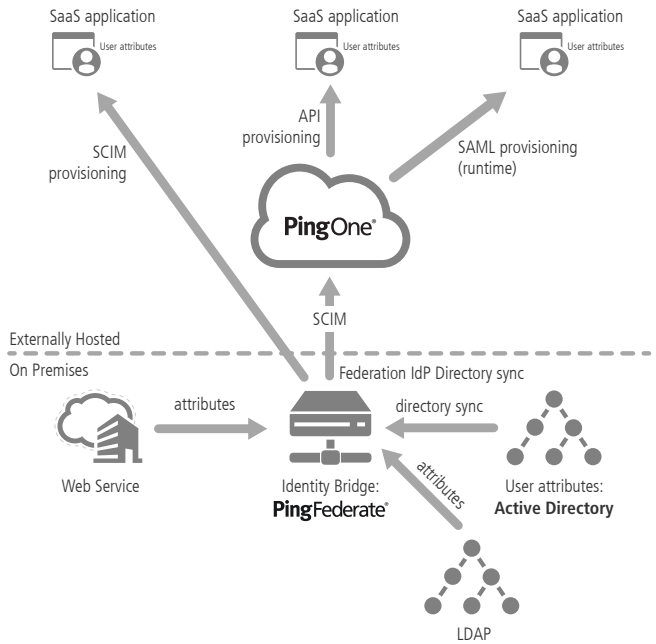


Figure 2. User provisioning to the cloud via a PingFederate identity bridge (not all options shown)

From the Cloud (Partners)

Organizations can use PingFederate to provision external identities into an on-premises identity store like Active Directory. PingFederate leverages JIT provisioning by extracting the user attributes from the SAML assertion, then creating the user in the identity store. This is useful for providing access to on-premises applications requiring Active Directory identities (Figure 3).

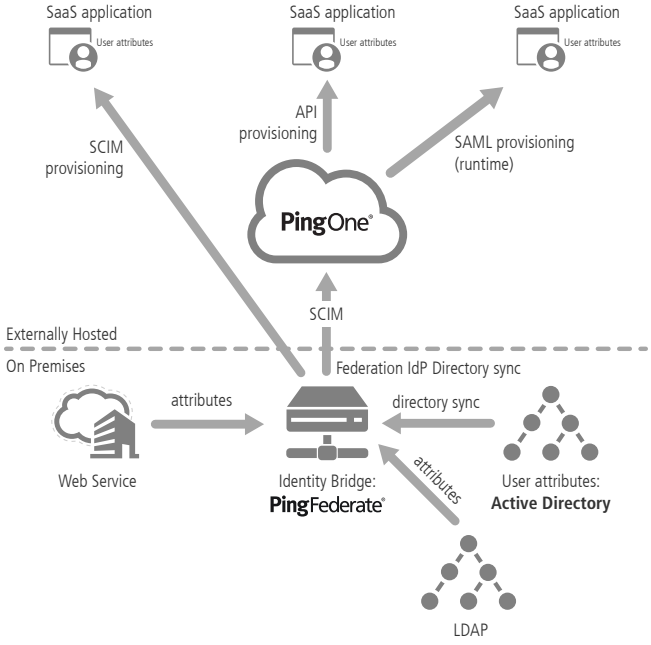
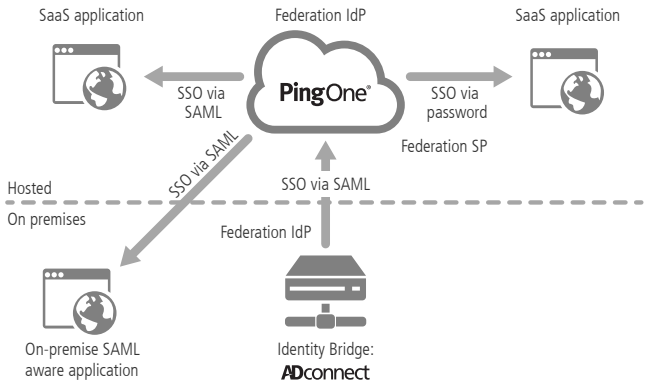


Figure 3. From the cloud, SSO via PingOne and PingFederate

User Authentication

User authentication is a crucial identity management service. Enterprises must match authentication methods to the identity assurance requirements of their environment. Without it, organizations have insufficient confidence that users at the other end of the transaction are legit. In many cases, Active Directory authentication (either Kerberos/IWA or a forms-based password) meets identity assurance requirements. Active Directory authentication can also provide "desktop to SaaS" SSO by leveraging the user's initial workstation logon. The AD Connect identity bridge best aligns to this use case (Figure 4).

Figure 4. User authentication options for an AD Connect identity bridge



For organizations that want to use other authentication methods besides those provided by Active Directory, PingFederate supports additional methods, including an X.509 certificate and one-time password. It also can be extended to support multiple authentication types (Figure 5).

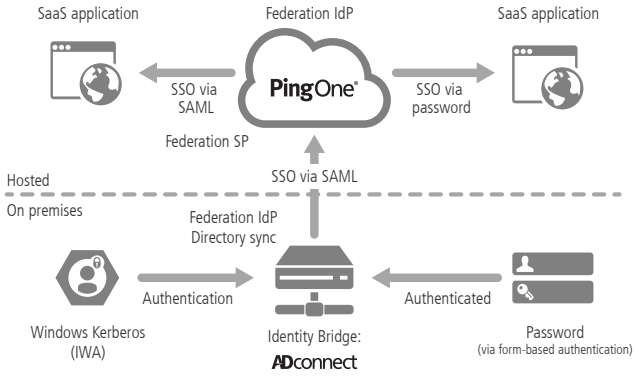


Figure 5. User authentication options for a PingFederate identity bridge (not all authentication methods are shown)

Table 1 summarizes the authentication methods for each of the Ping identity bridges.

	ADconnect	PingFederate®
Kerberos (IWA)	Yes	Yes
Windows password (forms-based authentication)	Yes	Yes
LDAP password	No	Yes
One-time password devices	No	Yes
X.509 certificate (smart card optional)	No[4]	Yes
WAM cookies	No	Yes
Custom authentication	No	Yes

Table 1. Ping identity bridge user authentication options

Token Issuance

The last of the three identity management processes for SSO is token issuance. The token provides SSO at runtime. Regardless of the identity bridge, the PingOne IDaaS provides SSO to SaaS applications and SAML-based on-premises applications (Figure 6). Several benefits exist for using PingOne for SSO. PingOne provides a single administration point for all SSO connections, whether on premises or externally-hosted.

On-Premises SSO

PingOne may also preclude the need for an on-premises federation identity provider as it issues SAML assertions (Figure 6).

4 While AD Connect cannot perform X.509 certificate logon directly, it can leverage the Kerberos tickets from a smart card authentication originating from an Active Directory-joined workstation. The result is strong authentication, natively supported by the network operating system.

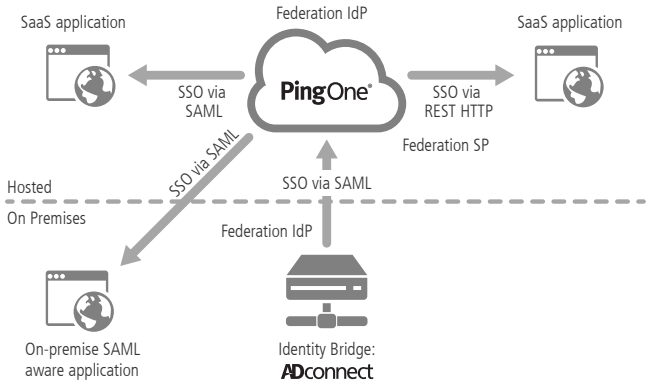


Figure 6. PingOne SSO for on-premises SAML aware applications (Active Directory interaction not shown)

Due to an extensive list of integration kits and token services, PingFederate delivers a rich set of heterogeneous on-premises SSO capabilities (Figure 7).

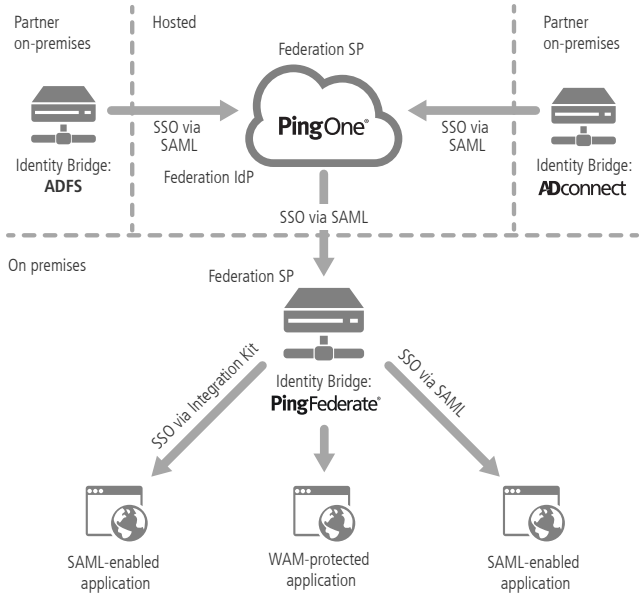


Figure 7. "From the cloud" provisioning via the PingFederate identity bridge

Of course, PingOne can provide SAML-based SSO to on-premises applications (see Figure 6). If SSO for non-SAML SSO is required for on-premises applications, then PingFederate may be the best choice for the identity bridge (see Figure 7).

Conclusion

The PingOne IDaaS delivers SSO to SaaS and on-premises applications. Identity bridges can easily extend the enterprise's existing identity management processes to PingOne. The AD Connect identity bridge is best suited for enterprises that:

- Leverage Kerberos or Active Directory passwords as the initial user authentication.
- Store user attributes in a well-formed Active Directory.
- Desire SSO for SaaS-based applications or SAML-based on-premises applications.

The PingFederate identity bridge is the right choice for enterprises that:

- Store user attributes across multiple identity stores.
- Authenticate users with stronger authentication methods besides Kerberos and AD password.
- Wish to leverage PingFederate's SSO capabilities for on-premises applications.

About Ping Identity | The Identity Security Company

Ping Identity is The Identity Security Company. Ping Identity believes secure professional and personal identities underlie human progress in a connected world. Our identity and access management platform gives enterprise customers and employees one-click access to any application from any device. Over 1,200 companies, including half of the Fortune 100, rely on our award-winning products to make the digital world a better experience for hundreds of millions of people. Visit pingidentity.com for more information.

.