



## Key Business Benefits

- *Identity integration with partners*
- *Fast, simple implementation*
- *Low total cost of ownership*

## Key Features

- *Federation provider and consumer services*
- *Multi-protocol federation support*
- *Protocol/version translation*
- *Auto provisioning with partners*

## Identity Federation as a Service

Using federation standards like SAML, ADFS and OpenID, web application providers can share user identity with partners and customers:

- Giving users single sign-on across web properties
- Creating private clouds or services aggregating applications from partners
- Provisioning users already authenticated with trusted partners

Enterprises can use federation to give employees access to external web applications from within enterprise portals like Microsoft SharePoint or BEA WebLogic.

Implementing federation is quick and easy with myOneLogin's multi-protocol federation services in the cloud. Use simple Web Services calls to turn your application into a federation consumer and/or provider, avoiding the cost and complexity of internal development efforts.

### Federation as a service

Implementing federation standards within an application can be a complex and time-consuming task. You have to learn about the standards, pick the libraries, and develop the expertise. Many commercial implementations require you to buy, host and maintain software.

myOneLogin delivers identity federation as an on-demand service, easily called from web applications. There's no hardware or software to deploy, and it requires no in-depth expertise. With both producer and consumer federation services available, your application can participate in a variety of federation relationships.



## myOneLogin Federation

### Participate in partner communities and marketplaces

Broaden your market by participating in partner communities. For example, give your partner's users the ability to sign up and sign on to your application. Or enable OpenID access to your application, allowing users from sites like Google, Yahoo, AOL, and MySpace to access your application using their OpenIDs from those services.

Using myOneLogin Federation, you can support multiple partners and integrate with other identity management solutions. Federation also helps you work with organizations using enterprise identity management solutions.

### Translate between different federation standards

Do your partners use different federation standards? myOneLogin Federation supports multiple federation standards:

- SAML 1.1
- SAML 2.0
- WS-Federation
- OpenID
- Active Directory Federation Services (ADFS)

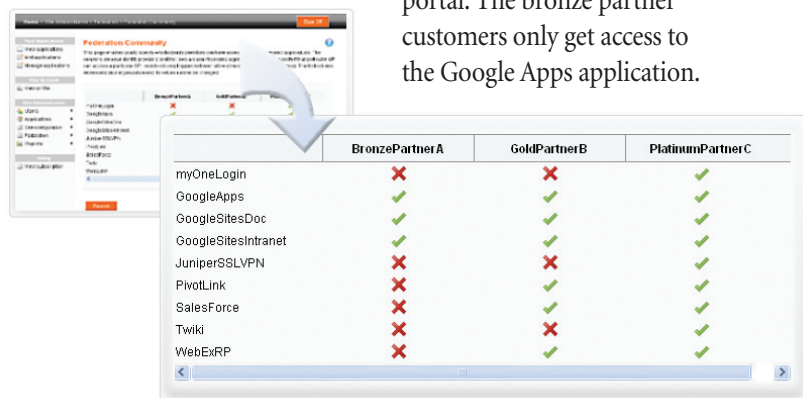
For example, your application can generate SAML 2.0 assertions, yet accept SAML 1.1 assertions from a partner. The myOneLogin service acts as a federation 'hub' for your business, connecting you seamlessly with applications and partners.

### Create and manage federation communities

Perhaps the trickiest part of federation is managing the trust relationships with partners and vendors. For example, you might provide identity assertions for one partner but not allow another partner's identity assertions to your applications.

myOneLogin helps you manage those relationships in an automated way. The myOneLogin administrative interface includes a graphical representation of your federation relationships.

In the example below, an enterprise allows its platinum partner federated access to all of its applications. The gold partners' users get access to all applications except the SSL VPN and internal Twiki portal. The bronze partner customers only get access to the Google Apps application.



	BronzePartnerA	GoldPartnerB	PlatinumPartnerC
myOneLogin	✗	✗	✓
GoogleApps	✓	✓	✓
GoogleSitesDoc	✓	✓	✓
GoogleSitesIntranet	✓	✓	✓
JuniperSSLVPN	✗	✗	✓
PivotLink	✗	✓	✓
SalesForce	✗	✓	✓
Twiki	✗	✗	✓
WebEXRP	✗	✓	✓

### Share provisioning information with partners

Use federation to enable trusted partners to provision users in your service and, in the other direction, to help provision your users with partners.

For example, a trusted partner could supply the information you need to provision a new user as part of a federation assertion. Your application can use this information to create the user's account in your service.

### Part of myOneLogin Identity Services

myOneLogin Federation is part of myOneLogin Identity Services, which also includes strong authentication using patented multifactor authentication technologies. By combining federation with strong authentication, you can provide users with a single highly secure login, protected from phishing and password theft.

myOneLogin Identity Services offer:

- Easy accessibility through Web Services calls provided by TriCipher
- Integration with internal Active Directory or LDAP directories
- Self-provisioning processes for faster deployment

### Trust in TriCipher

myOneLogin Identity Services are provided by TriCipher™, experts in Internet identity services.

myOneLogin Identity Services is hosted in a SAS 70 Type II-certified data center that employs advanced security and protection technologies. The service uses a secure, multi-tenant architecture in which you will have your own, dedicated domain with complete data isolation. Authentication technology and factors are managed by the patented TriCipher Armored Credential Systems, which has a U.S. government Federation Information Processing Standard (FIPS) 140-2 Level 2 rating.



**TriCipher Headquarters:**  
750 University Avenue, Suite 260  
Los Gatos, CA 95032  
Phone: +1.650.372.1300  
Fax: +1.650.376.8301  
www.myOneLogin.com

**TriCipher Worldwide Sales:**  
Email: sales@tricipher.com  
Phone: +1.650.376.8326  
Fax: +1.650.376.8301