

Linking myOneLogin with Active Directory & LDAP

myOneLogin offers a complete identity services platform, including single sign-on, strong authentication, access control/authorization, federation and provisioning. Many organizations have a significant investment in directory-based user stores like Microsoft Active Directory. Integrating myOneLogin with internal directories lets you leverage those existing user stores while maintaining control over authentication within the enterprise network.

This technology brief describes options for integrating myOneLogin with LDAP-based directories, including Microsoft Active Directory, within an enterprise network.

Why integrate myOneLogin with internal directories?

Many enterprises have invested in internal directory services, such as Microsoft Active Directory or Sun ONE Directory Server. These directory servers use LDAP (Lightweight Directory Access Protocol) to provide standards-based integration with other programs, making integrated services a viable option.

myOneLogin can actually 'look up' user information in these internal directories rather than storing it within the myOneLogin service. Building integration between myOneLogin and the LDAP directory delivers:

- *A single location for managing users.* For example, when you hire a new employee, you only need to add them to the LDAP directory to give them a login for both internal and web applications.
- *A single login for employees.* Employees only need to remember one account and password to access all of their internal applications and, through myOneLogin, all web-based applications as well.
- *Roles-based access control.* myOneLogin can extract attributes and groups from internal directories and use them for access control/authorization and provisioning purposes.

This option describes a number of options for integrating myOneLogin with internal directories, offering varying levels of security and functionality.

Basic directory integration

The simplest integration method is to use a Web FORM login page to have myOneLogin access an internal directory. myOneLogin communicates with the FORM page using HTTPS. The FORM login page can check that the requesting IP address belongs to the myOneLogin service. The FORM login page, in turn, takes the credentials passed on from myOneLogin and validates them against the directory.

The myOneLogin service passes users' credentials to the FORM login page, which authenticates the user account and password against the internal directory. It then authenticates the additional factor (mobile credential, browser-based credential, one-time password) selected to provide strong authentication.

Solution Brief: Directory Integration

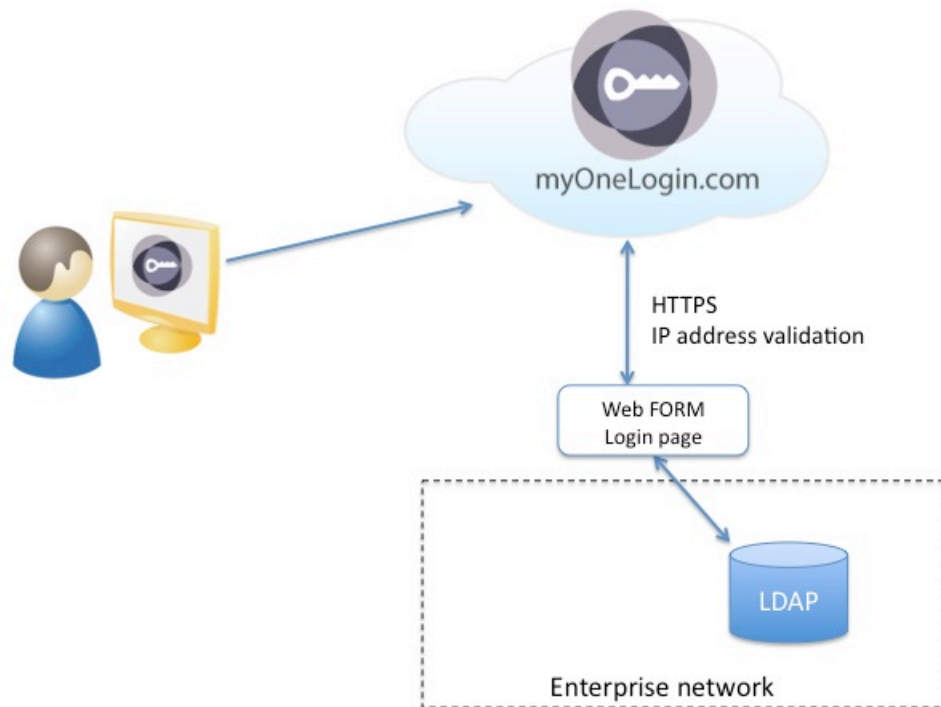


Figure 1: Using a Web FORM page for directory integration

myOneLogin Enterprise Connector (EC)

For organizations wanting more flexibility or greater capabilities, myOneLogin offers a lightweight utility for directory integration: myOneLogin Enterprise Connector, part of myOneLogin Enterprise Edition.

Enterprise Connector is a lightweight component, delivered either as a virtual appliance independent of operating system, or as a module to run on a Microsoft IIS server.

Enterprise Connector communicates with internal directories to authenticate users and, if necessary, pull user attributes from the directory. All communication between the directory, EC and the myOneLogin service are secured.

You can use the myOneLogin EC in two ways:

- As a direction integration service, EC is installed within the DMZ. It communicates with the myOneLogin cloud identity platform and validates user IDs and passwords against internal directory. myOneLogin Enterprise Connector can also extract attributes and roles from the directory for access control/authorization and provisioning purposes.
- As a full enterprise integration service, EC can fully authenticate users within your network, passing only SAML assertions to the myOneLogin service in the cloud. In this configuration, EC also enables integration with desktop authentication, corporate portals and SSL VPNs.

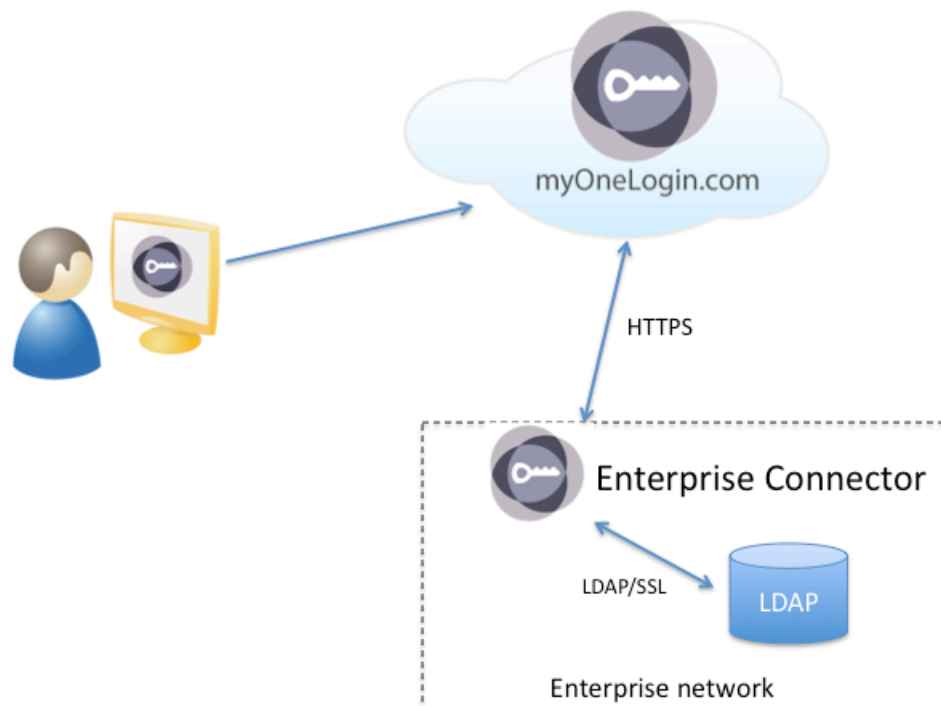
Solution Brief: Directory Integration

These options are described below.

Directory integration with EC

In the first, directory integration implementation, EC sits in the DMZ and communicates with the directory using LDAP over SSL.

When a user (either from inside or outside your network) connects to myOneLogin, the myOneLogin service communicates with EC over HTTPS to authenticate the user ID and password. The myOneLogin service verifies additional authentication factors.



Using myOneLogin EC for directory integration

Once authenticated, the user has one-click access to the applications on their myOneLogin portal.

The user may be connecting to myOneLogin from anywhere, either inside or outside the corporate network. The myOneLogin service enforces multi-factor authentication.

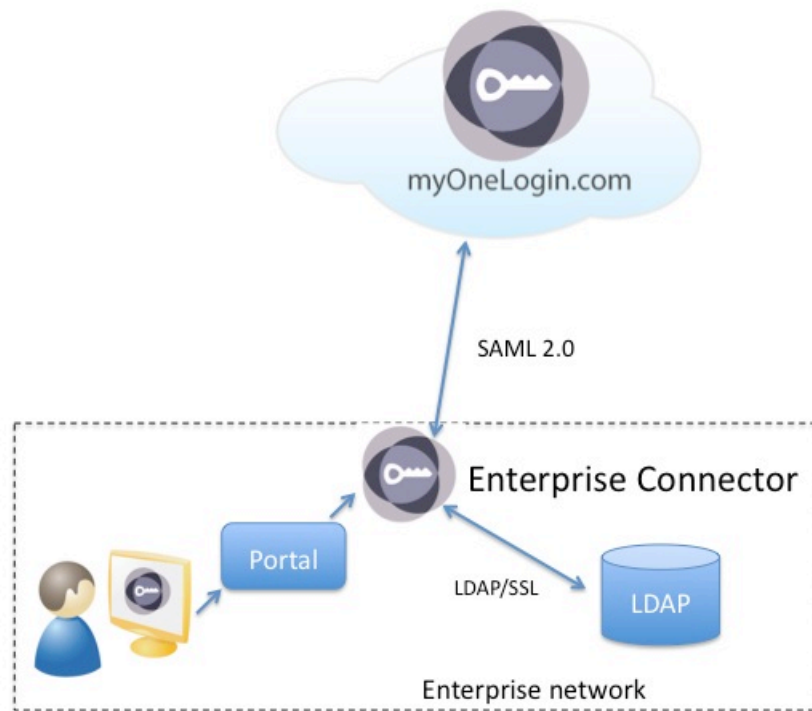
This is the simplest EC configuration to deploy, and serves the needs of many types of businesses by providing a single place to manage users. When you delete a user from the directory, for example, their myOneLogin authentication will automatically fail and users are instantly denied access to myOneLogin.

Solution Brief: Directory Integration

Full federation inside the network

myOneLogin EC can actually implement a federation server within your network, creating an in-network federation authority that communicates with the myOneLogin service using SAML 2.0 assertions.

The user authenticates with the Active Directory/LDAP server within the network, leveraging existing network security. If using Active Directory, users can transparently authenticate to AD using a Kerberos desktop login. When a user from within the corporate network accesses a SaaS application URL on an internal portal page, they are redirected to the EC, which authenticates the user with the LDAP directory and generates a SAML assertion to the myOneLogin service. The user credentials never leave the corporate network.



Using EC for in-network authentication and federation

Note that using this configuration, all user authentications happen in-network; the myOneLogin service does not enforce multiple authentication factors, but simply accepts the SAML assertion from the Enterprise Connector. Users can use this support from outside the network using an SSL VPN.

Next steps

If you are interested in directory integration options and documentation, contact Support@tricipher.com.