Partner Identity Federation

Secure single sign-on to business applications from partner organizations

Sharing apps with your business partners doesn't have to be an all-or-nothing proposition. You don't need the hassles of managing external users in your network, or the concerns of enabling too much access. Get secure integration without the micro-management, with Centrify Identity Service.™

Growing businesses is all about leverage. In today's always-connected world, that means ensuring that partners have the technology they need to access the services you provide. Whether it's accessing parts databases, placing supply orders, or registering sales opportunities, partners need secure, managed access to your web-based applications — without complex and costly integration.

Once you decide to provide partners access to an application, you still have to find a way to ensure that only authorized partners get access. From the partner's perspective, their employees don't need yet another username and password to remember. You don't need the hassle of validating and creating every external user account yourself, and then supporting all of the password resets and manual provisioning requests you'll get as more partners sign up.

Following are some best practices for authenticating partners to your shared apps, while maintaining the security and integrity of your own resources.

VPN Access? No Way

You need to ensure your trusted partners can access your shared apps in order to meet mutual business objectives. But providing external access used to be an all-or-nothing proposition. You had to allow unknown users and their devices into your network over VPN, or block them entirely.

No Shared Passwords, Either

If you don't want to create new accounts for each external partner employee, you might be tempted to set up a few shared VPN accounts and passwords. Don't fall into this trap.

Shared passwords are a security risk, especially if you can't identify the users by name. VPN access, whether by individual or shared accounts, could enable external users to access more information on your network than you intended. Without granular endpoint management and app access policies in place, VPN access could expose your network to viruses or other threats found on unmanaged, unknown devices. Case in point: many recent data breaches have been traced back to malware delivered into a corporate network from compromised partner devices.

Maintain Separation of Responsibility

While you need to provide your partners with access, giving them user credentials in your internal identity store can become unmanageable, and introduces lots of risk:

- How can you be sure you have authorized only valid users?
- How do you ensure there are no stale accounts?
- How can you support password-reset requests?
- How can you protect against attacks from compromised accounts?
- How can you ensure user accounts and passwords are not shared within the partner organization?
- How can you ensure that each third party computer is a properly secured endpoint?

In order to be successful in sharing business apps with external partners, we recommend you maintain a clear separation of responsibility. Managing users unknown to your IT organization invites risk, as noted above. Instead, consider first how your organization will manage each partner's access to your environment. Then establish some criteria that the partner follows to manage their own users, according to industry best practices.

Enable Partner Identity Federation

Centrify Identity Service uses SAML to provide simple, cloud-based identity federation for your applications. Your partners can manage their own employee authentication, directories, and identity solutions, and then leverage federated trust with your Centrify environment to provide secure access to your shared applications. Have separate billing, shipping, and ordering apps that you don't want to share with

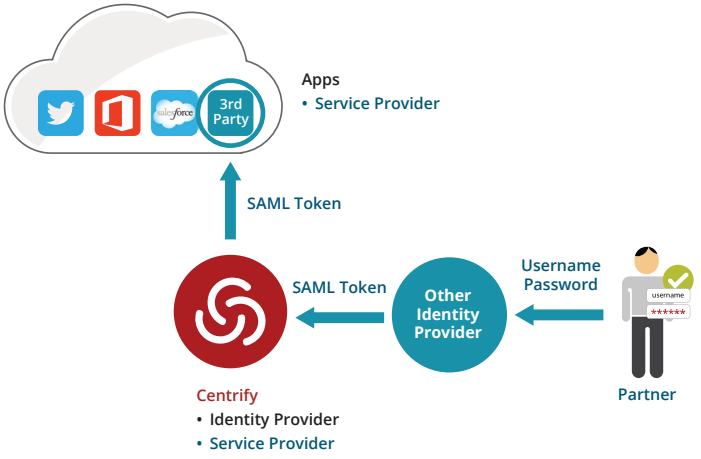
partners? No problem. Identity Service provides your employees with single sign-on across your internal applications. Centrify uses role-based access control to determine who gets access to which apps. You can assign each partner to a specific role within your Centrify tenant, with policies that determine application access.

Get Started with Your Partners

The first step for federating partners into your applications is requiring that each partner organization have its own identity provider in place. An identity provider creates, maintains and manages identity information, and uses technologies like SAML to authenticate its users from its user directory, into apps in the cloud, or on-premises. Centrify Identity Service is one identity provider. There are others from third party vendors as well. As long as your partners' identity provider supports SAML, partner identity federation will work. If your business partners do not currently use an identity provider, they can set up a Centrify tenant for free.

Why is it important for partners to have their own identity provider?

When your partner has an identity provider in place, you know that their users have been verified as part of their organization (through membership in Active Directory, for example). Your partner's identity provider can authenticate its users. So work with your partners to make sure they have their own Identity Provider in place before allowing their users into your environment. If your partner doesn't have an identity provider, they can set up a Identity Service cloud tenant in a few minutes.



Enable App Access to Your Partners

Now that you've ensured your partner is working with an Identity Provider, you can use your Centrify environment to host your shared apps. Setting up trust with partner is a simple process that can be done in a matter of minutes in the Identity Service cloud manager. This trust relationship uses SAML to enable access for external users based on role-based access, like any user in Centrify. Partner employees can then log in to their own Identity Provider with their existing credentials, and receive federated access to your applications.

Benefits

- Focus on your business, without hassling with complex authentication
- Avoid complex implementation and risky network changes
- Ilow partners to manage their own adds, moves, and changes
- Let partner employees use a single set of credentials for app single sign-on
- Integrate your application across partner identity providers

Centrify strengthens enterprise security by securing identities from cyberthreats. Centrify uniquely unifies identity for privileged and end users across cloud, mobile and data center. Centrify improves security, compliance, agility and productivity for over 5000 customers, including over half of the Fortune 50 and over 80 federal agencies. www.centrify.com.

SANTA CLARA, CALIFORNIA	+1 (669) 444 5200
EMEA	+44 (0) 1344 317950
ASIA PACIFIC	+61 1300 795 789
BRAZIL	+55 11 3958 4876
LATIN AMERICA	+1 305 900 5354
EMAIL	sales@centrify.com
WEB	www.centrify.com