Centrify®

Eight Great Reasons to Use Centrify with Office 365

If you've made the move to Office 365 or are considering it, congratulations! Office 365 is changing the game in cloud-hosted enterprise office and collaboration. Office 365 is delivered from the cloud, and supports both native and cloud-hosted versions of its applications. It runs on multiple operating systems and mobile platforms, too. But, with all this versatility comes complexity — especially when it comes to managing user identity and access.

So we're bringing you eight great reasons to use Centrify with Office 365. Centrify Identity Service is an Identity-as-a-Service (IDaaS) solution that federates user identity from Active Directory, LDAP directories, or the Centrify Cloud Directory. By federating identity from a central directory, you can give your users single sign-on to Office 365, while making the rollout much simpler for your IT department. Centrify also manages access to thousands of other Software as a Service (SaaS) applications from any device.

1 **Single Sign-on** means only having to remember one password.

Single sign-on (SSO) means you don't have to enter a different username and password for each application or service you use. Even in well-integrated IT environments, nearly 30 percent of corporate end users we surveyed are entering an average of 11 or more usernames and passwords a day to various cloud and on-premises applications.[1] They are accessing apps from their handheld devices, from web browsers, or from rich native apps — and they're doing so from locations both inside and outside the corporate network.

Office 365 is a cloud-based implementation of a complex set of tools that were traditionally deployed on-premises, including Microsoft Office (Word, Excel, PowerPoint), Outlook, SharePoint, and Lync. With Office 365, these same apps are available from the cloud as Software as a Service (SaaS), and also as apps on mobile clients for Windows, iOS and Android operating systems. Managing how users sign on to Office 365 from all of these different devices and locations is more complicated than filling in a username and password.

For single sign-on, Microsoft recommends federating identity from Active Directory into Office 365 using Active Directory Federation Services (AD FS), and then synchronizing user identities with directory synchronization (DirSync or Azure Active Directory Synchronization) to Azure Active Directory. These recommendations work well for Office 365, but can be complicated to implement and are not yet fully scalable to support third party SaaS applications.

[1] http://www.centrify.com/downloads/public/Centrify-Password-Survey-Summary.pdf

If you need SSO to Office 365 and other cloud or on-premises applications, consider an Identity-as-a-Service (IDaaS) provider like Centrify. Centrify Identity Service is a complete provisioning and single sign-on solution delivered via the Centrify Cloud. With Centrify, you can deploy browser-based apps, native mobile apps and custom apps for Office 365 — and thousands of other applications. Centrify lets you control and simplify the application sign on experience for your end users, by using industry standards such as WS-Federation and SAML.

With a single username and password, sign on to Office 365 and thousands of popular cloud apps — using your existing on-premises or cloud-based identity data.

2 **Quick deployment** means you get to have a life.

Migrating into Office 365 doesn't have to become a multi-week marathon. You can provide single sign-on to Office 365 in just a few minutes — instead of a few weeks — for all of your users. When you sign up for Centrify Identity Service, the Centrify Cloud connector is the only thing you need to install on a domain-joined server in your network, and that takes about five minutes. Cloud Connector proxies your Active Directory or LDAP directory data to Office 365 without replicating your identity data into the cloud.

If you don't have or want an on-premises directory service, you can use the Centrify Cloud Directory. And if you're using only the Cloud Directory, you don't even have to install the Cloud Connector. Instead, use the Bulk User Import wizard to import

a spreadsheet containing all your user accounts. Once all accounts are in the Centrify Cloud Directory, your users' identities will be federated to Office 365.

Also, there's no need to modify firewall policies or download public certificates. Centrify reduces the time to roll out Office 365 into a few hours, rather than a few weeks.

3 No on-premises federation servers means you can spend your budget on cooler stuff.

If you want to keep your Active Directory on-premises, Microsoft recommends you deploy Microsoft Active Directory Federation Services (AD FS) with high-availability clustered servers, both inside the firewall and in the DMZ, to achieve identity federation and single sign-on to Office 365. Centrify's Identity Service runs in the Microsoft Azure cloud computing platform, and eliminates the need to install clustered federation servers on-premises. Centrify is certified by Microsoft as a "Works with Office 365" partner, and is recommended by Microsoft for organizations where more complex identity federation infrastructure is not feasible or desirable.

4 User provisioning and deprovisioning means easy come, and easy go.

It's easy to on-board users automatically into Office 365 using Centrify Identity Service. You can pre-assign roles with users and groups in your directory service (Active Directory, LDAP, or Cloud Directory) for provisioning. When users log into Office 365 from the web client or Outlook client on their computer or phone for the first time, their account is available and accessible. If an employee changes job roles (for example, from engineering to sales), reassigning them to a different group in your directory service triggers a change to their software entitlements for Office 365. If an employee leaves your organization, removing them from your directory service automatically disables access to their Office 365 account. Easy come and easy go.

5 Role-based licensing and entitlement means the more you share, the more you have.

You can share license components more granularly across your user base with Centrify's role-based license management. And you can optimize your IT spend by splitting up or sharing Enterprise licenses across different users or groups, and reassign unused components.

For example, let's say you are deploying a combination of E1, E3, or E4 licenses. Each license type has different components it supports, like the Office suite (Word, PowerPoint, Excel, and more). And it may have other components like online conferencing. If you need to allocate an E4 license feature to an E1 license holder, you can do that with Centrify's granular license management. You have fewer high-end licenses to purchase, and more flexibility in how you allocate users with the tools they need.

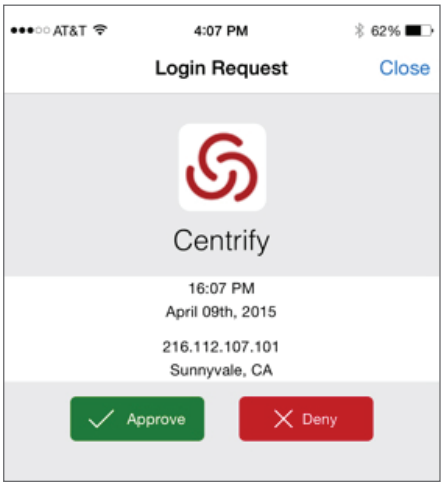
6 Mobile Access and Management: because people also do their jobs from their smart phones and tablets.

Mobile devices are here, and folks are using them get their work done, using your organization's data in Office 365. You want to encourage productivity, but what happens if a device is lost or stolen? Centrify integrates user identity and mobility policy management to provide secure, managed application access from any device. You can enforce and update mobile security settings, lock or remotely wipe devices, and provide secure access to email, VPN and Wi-Fi networks. Your end users can enroll their own mobile devices — to get automatic access to their Office 365 account. They can lock the Centrify Mobile App with a passcode or fingerprint, preventing unauthorized users from accessing your sensitive data. You can push apps, policy, certificates and more — and pull them all back when devices are lost or stolen, or when an employee leaves the company.

7 Multifactor Authentication and Policy means you can control application access — without being "overly controlling."

Most cloud and on-premises applications support access via username and password. But for some applications, you may want to require stronger authentication. Centrify combines multifactor authentication (MFA) with application access policy in order to secure your organization's data — even if the application itself doesn't support MFA. And Centrify makes MFA easy to use and minimally disruptive for end users.

You may want to require stronger authentication for Office 365 in certain situations. For example, you could create a policy requiring additional authentication when a user attempts to log in to their Office 365 account on



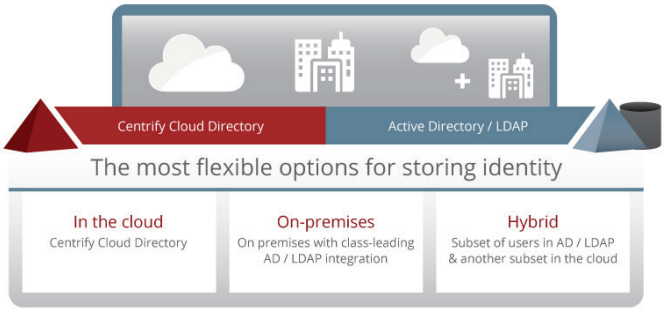
an unmanaged device, when they're outside the corporate IP address range, or when their IP address indicates they may be in a different country.

Setting up MFA and application access policy is easy. From the Centrify Identity Service Admin Portal, you click on the Office 365 app tile, and go to the Policy menu to see the options. You can check a box to require strong authentication, and load sample policy scripts that you can customize for your own environment.

But MFA can be a hassle for end users, especially if they are required to listen to a robot on a phone, or type in a complicated authentication code on their device (while walking across the street and not paying attention to oncoming traffic). The Centrify mobile authenticator is easy and safe to use on smartphones, tablets and smartwatches. There is no code to type in — just tap "Approve" or "Deny."

8 Hybrid Directory means freedom to have it your way.

Centrify lets you store your identity data where you want it. You can federate identity from on-premises Active Directory or LDAP, without replicating your identity data into the cloud. While other Identity as a Service providers claim a single source of "truth" from Active Directory, they're actually replicating your Active Directory into their Cloud. Many Centrify customers have told us that they'd prefer to keep their directory data on-premises. And they don't want to expose their identity data by storing copies in multiple places. That's why Centrify Identity Service was built to proxy authentication information for on-premises directories, and never to replicate directories into the cloud. Centrify eliminates directory replication, thus avoiding problems caused by directories becoming out-of-sync.



At the same time, Centrify Cloud Directory is available for organizations that don't have or don't want to maintain on-premises directory services.

Our Hybrid Directory gives you choice in deployment options, combining the best of both worlds — on-premises and cloud. For example, you can store your regular full time employees' identity in existing Active Directory, employees from a recent acquisition in a separate Active Directory forest, customers in LDAP, and contractors or partners in separate Centrify Cloud Directories.

Conclusion

OK. So we've given you eight great (and true) reasons to use Centrify with Office 365. But you don't have to take our word for it. Give it a try yourself. Start a free, full-featured 30-day trial today, or register for our free Express version, which supports up to three applications.

Centrify

Centrify strengthens enterprise security by managing and securing user identities from cyber threats. As organizations expand IT resources and teams beyond their premises, identity is becoming the new security perimeter. With our platform of integrated software and cloud-based services, Centrify uniquely secures and unifies identity for both privileged and end users across today's hybrid IT world of cloud, mobile and data center. The result is stronger security and compliance, improved business agility and enhanced user productivity through single sign-on. Over 5000 customers, including half of the Fortune 50 and over 80 federal agencies, leverage Centrify to secure their identity management. Learn more at 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