Identity and Authentication in the cloud: Office 2013 and Office 365

For IT Pros and end users

Authentication is user centered—not computer centered

We've made a fundamental shift from an Office that only knows about an individual on a single device, to an Office that knows about an individual across all of his or her devices and services. This shift enables content, resources, most-recently-used lists, settings, links to communities, and personalization to roam seamlessly with users as they move from desktop, to tablet, to smartphone, or to a shared or public computer. For the IT admin, user audit trails and compliance are also separated by identity.

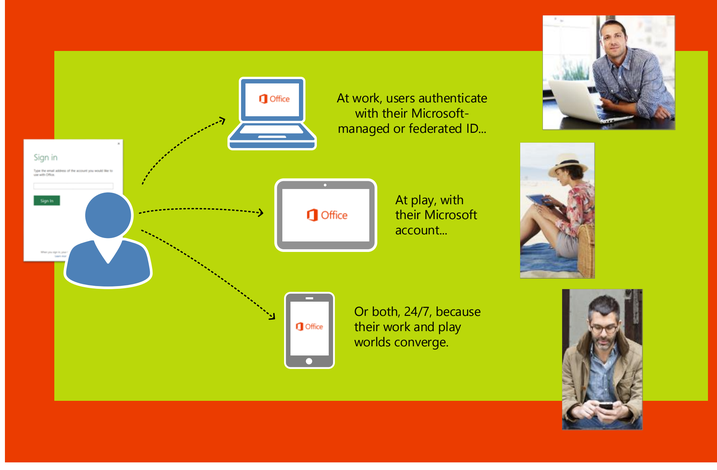
In this new environment, users sign in to the Office 365 client by using one of these identities:

- **Their business, organization, or school ID.** There are two flavors:

  An ID that your org assigned to users. This is for Office use, where Microsoft hosted enterprise and smaller organization user IDs are stored in the cloud. These identities are separate from on-premises identities, and are directly managed in the cloud.

  A federated, user ID. Also for Office use, where enterprise user IDs are stored and managed on premises. For businesses or organizations using Active Directory.

- **Microsoft Account (formerly known as a Windows Live ID).** A Microsoft account is the combination of an email address and a password used to sign in to services like Hotmail, Skype, OneDrive for Business, Windows Phone, Xbox LIVE, or Outlook.com. Typically, users use this identity to sign in to Office for non-business purposes.



You already know the on premises story

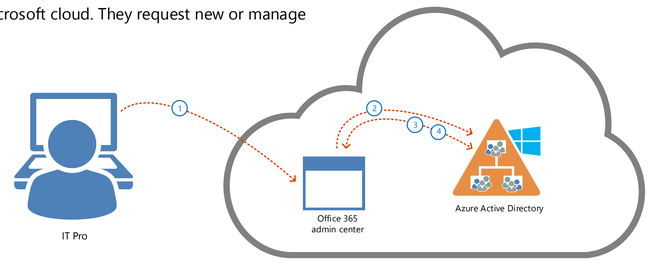
On premises is what you have done, day in and day out, 24/7, since your beeper days. What about the new world of cloud and hybrid?

Scenario 1: All in the Microsoft cloud

The IT Pro identity provisioning experience

You are in charge. If yours is a smaller business, use Microsoft cloud Identity Services to establish, manage, and authenticate your users. User accounts are cloud-managed by using a web portal and Microsoft Azure Active Directory in the Microsoft cloud. No servers are required. Microsoft manages all that for you. When identity and authentication are handled completely in the cloud without affinity to any on-premises Active Directory store, IT admins can still provision or de-provision IDs and user access to services through the portal or PowerShell cmdlets.

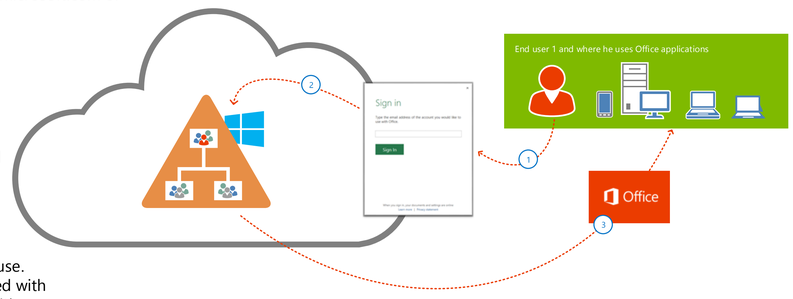
1. IT Pros connect to the web access Office 365 admin center in the Microsoft cloud. They request new or manage existing organization IDs.
2. These requests are passed on to your Azure Active Directory.
3. If this is a change request, the change is made and reflected back to the Office 365 admin center. If this is a new ID request, a request for a new ID is issued to the ID provisioning platform.
4. New IDs and changes to existing IDs are reflected back to the Office 365 admin center.



...and the end user authentication experience

After you've set up users in the Office 365 admin center in the Microsoft cloud, they can sign in from any device. And Office Pro Plus can be installed on up to five of their devices.

1. After you've provisioned a user (see the diagram above), they sign in to Office using one of the following identities:
   - their work identity (for example, mike@contoso.onmicrosoft.com or mike@contoso.com)
   - their personal (for example, mike@outlook.com)
   - their organization (for example, mike@charity.org)
2. Microsoft figures out where they want to authenticate and which files and Office settings they want to use depending on the identity they have chosen. That identity is associated with a Azure Active Directory, and their email identity and associated password are passed to the correct Azure AD server for authentication.
3. Their request is tested and then granted and the Office applications are streamed to their device and ready to use. Their OneDrive for Business saved documents associated with that identity are available to view, edit, and save back either locally to their device or back to OneDrive for Business.

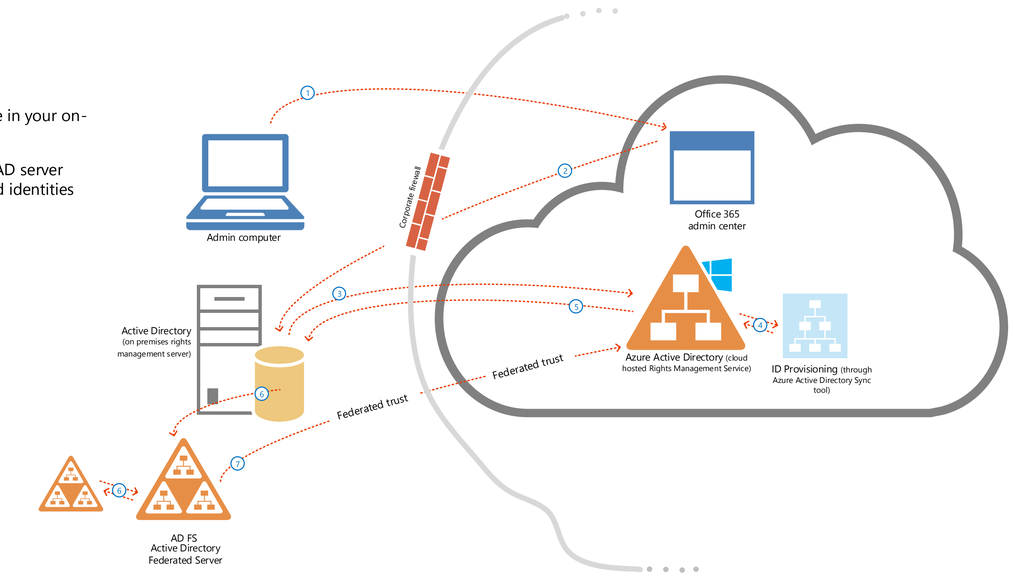


Scenario 2: Hybrid cloud and on-premises

The IT Pro identity provisioning experience

The Microsoft cloud Microsoft Azure Active Directory Sync tool keeps your on-premises and in-the-cloud corporate user identities synchronized.

1. Install the Azure Active Directory Sync tool. This tool helps to keep Azure Active Directory up to date with the latest changes you make in your on-premises directory.
2. 3. Create new users in your on-premises Active Directory. The Azure Active Directory Sync tool will periodically check your on-premises AD server for any new identities you have created. Then it provisions these identities into Azure Active Directory, links the on-premises and cloud identities to one another, and makes them visible to you through the Office 365 admin center.
4. 5. As changes are made to the identity in the on-premises AD, those changes are synchronized up to the Azure Active Directory and made available to you through the Office 365 admin center.
6. 7. If your users include federated users, those users log in with your Active Directory Federated Server (AD FS). AD FS generates a security token and that token is passed to Azure AD. The token is verified and validated and the users is then authorized for Office 365.



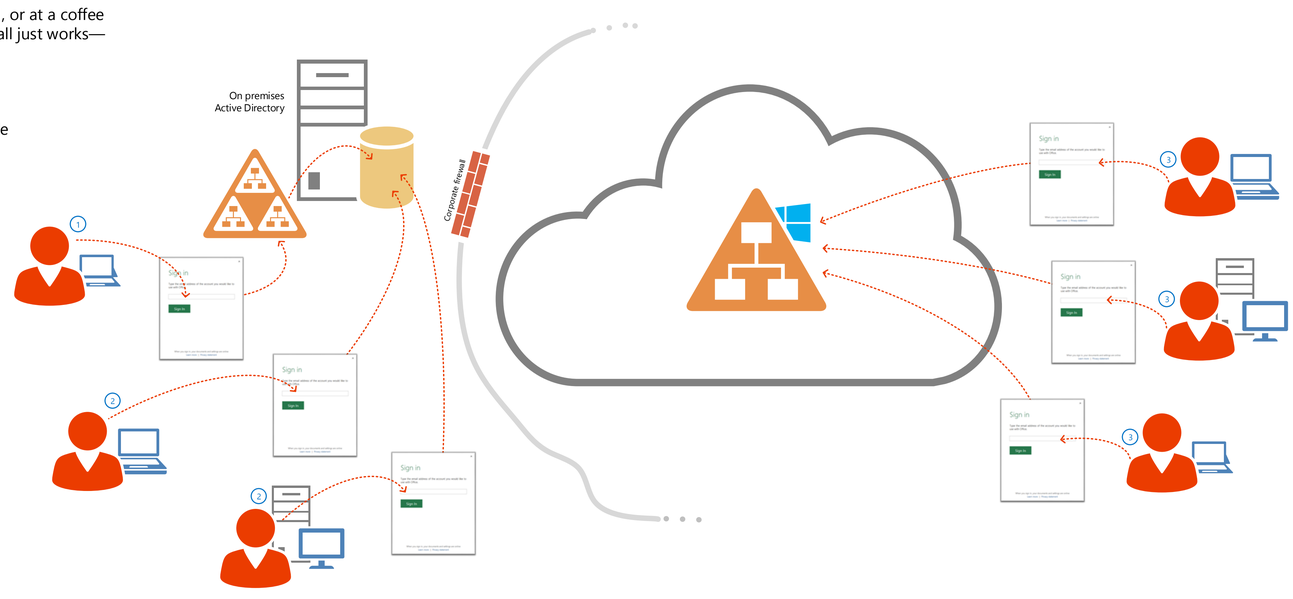
...and the end user authentication experience

For the end user, the authentication experience is the same—whether they are behind your corporate firewall, or at a coffee shop, home, or a hotel on the other side of the planet. They don't need to care where their request goes—it all just works—always, and wherever they are.

1. 2. If users are behind the corporate firewall and have already logged into their corporate network, when they try to access Office 365, they don't need to log in again! The user is silently re-authenticated by Active Directory Federated Services (AD FS). After re-authentication, they are able to use Office applications and access their local or OneDrive Office documents.

—and—

3. Roaming users signing in from outside of the corporate firewall will be prompted by AD FS for their corporate credentials. AD FS then authenticates these credentials against the on-premises AD. Their sign in information goes directory to your company's Azure Active Directory service in the Microsoft cloud.



Office

Microsoft