ca technologies

CA Advanced Authentication Integration for Office 365

How Do I Keep My Corporate Data Secure in the Cloud?

Over the next year or so, we will see the shift from on-premises Exchange to cloud-based Exchange Online/Office 365 reach the tipping point at which the cloud version becomes the majority[1]

Businesses are moving away from the traditional implementation of Microsoft® Office and migrating to the new, cloud-based Office 365™, which offers increased accessibility and significant cost savings. However, the cloud also introduces significant risk, as Office 365 requires that businesses store their Excel® PowerPoint® and Word files—many of which contain sensitive data— within their cloud environment.

This risk is further compounded by the authentication mechanism used to access this environment—passwords, which can be easily stolen and compromised. For Web application attacks, Verizon found that "63% of confirmed data breaches involved weak, default or stolen passwords."[2] As a result, many organizations are seeking a stronger authentication mechanism to secure access to their Office 365 environments.

Businesses require a solution that provides the following key capabilities:

- **Multiple device support**. Mobile devices and mobile applications have become the strategic initiative for all digital organizations looking to drive business forward. And this consumerization of IT has also extended to the workplace. Spurred by executives and remote employees seeking to work more productively, bring your own device (BYOD) initiatives are increasingly underway at companies of every size. Therefore, any strong mechanism adopted for Office 365 must support and deliver the same user experience across multiple devices and platforms.
- **User experience**. Today, an app's UX has come to embody the characteristics of a product or service that are important to the individual. While UX is primary concern and goal for business-to-consumer apps, it's also critical for employee-based use cases because it significantly improves adoption and reduces training and support costs. This is also true for any enhanced security associated with user authentication; it should be as frictionless and easy-to use as possible.
- **Flexibility**. As organizations seek to deploy strong authentication for their Office 365 solution, they need to ensure that it will support active and passive profiles, which is required to support client and browser-based access to the cloud environment. In addition, the business may want to only impose strong authentication for remote workers, but allow office-based workers who are logged into the network to login without any additional credentials.

The Solution from CA Technologies

Capabilities and benefits

- Mitigate risk—reduces risk of inappropriate access to Office 365 by blocking high-risk logins and requiring step-up authentication for suspicious activity
- Increase security—supports multifactor authentication (MFA) and/or contextual risk-based authentication for Office 365
- Gain flexibility—enables different authentication processes for network and remote users, as well as provides passive and active profile support
- Deliver exceptional user experiences—offers increased security without burdening your users with additional requirements

The Office 365 Integration from CA is an add-on services offering that allows you to integrate your Office 365 environment with your on-premises CA Advanced Authentication components. This offering can support any of the out-of-the-box authentication mechanisms, including CA AuthID, CA Mobile OTP, knowledge-based security questions, OATH tokens, out-of-band OTP, and risk-based adaptive authentication. In addition, you can alter the authentication mechanism with the solution, based on contextual criteria. For example, a user already logged into the network may be allowed to log into Office 365 without any additional login credentials, however, a remote user may be subject to a risk analysis and be required to perform a step-up authentication when login is deemed risky.

What it does

This service offering is a Packaged Work Product that integrates CA Advanced Authentication with Microsoft Office 365 and supports Web-based Office suite, Microsoft Office (2013 and 2016) apps on Windows®, OS X and mobile devices (iOS and Android).

Specifically, the service works for the following:

- Microsoft Office apps on Windows and OS X
  - Excel
  - OneDrive® (portal)
  - OneNote®
  - Outlook®
  - PowerPoint
  - Skype® for Business
  - Word
- Microsoft Office Native apps on iOS and Android
  - Excel
  - PowerPoint
  - Skype for Business
  - Word

The solution module can support both active and passive profiles. The WS-Federation Passive Requestor Profile works with passive requestors, primarily when the user logs in through Web browsers to Office 365. The passive profile enhances the login workflow(s) with CA Advanced Authentication and enables single sign-on between multiple productivity clients within the Microsoft Office 365 suite. The WS-Federation Active Requestor Profile is leveraged when the user launches the productivity client on their device and logs in using the client. Once authenticated via Advanced Authentication, users are seamlessly authenticated via single-sign-on between multiple Simple Object Access Protocol (SOAP)-enabled desktop clients provided by the Office 365 suite.

In addition, the user interface/branding for the authentication challenge pages can be customized as per customer requirement.

How it integrates

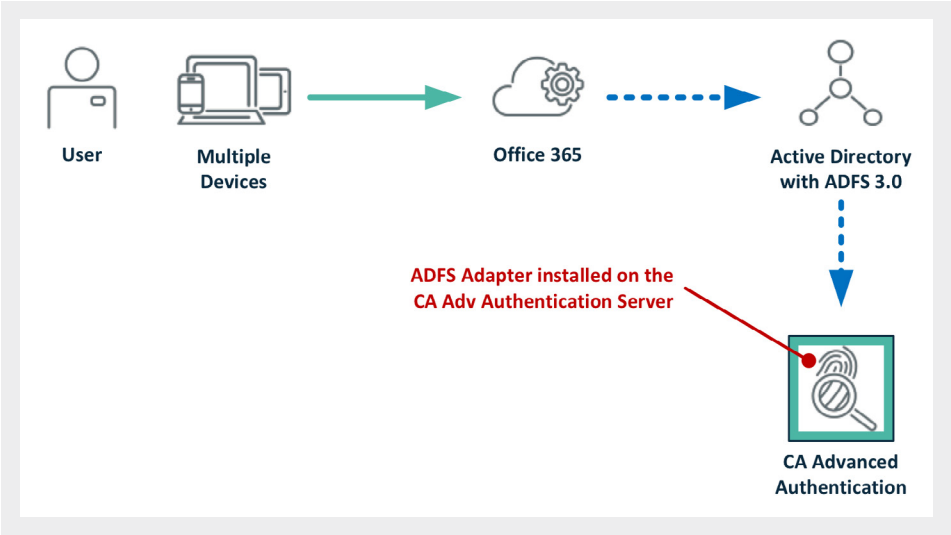


Figure A.

Office 365 is integrated with CA Advanced Authentication through the Active Directory Federation Services (ADFS) adapter that can be installed on CA Advanced Authentication servers.

Technical prerequisites:

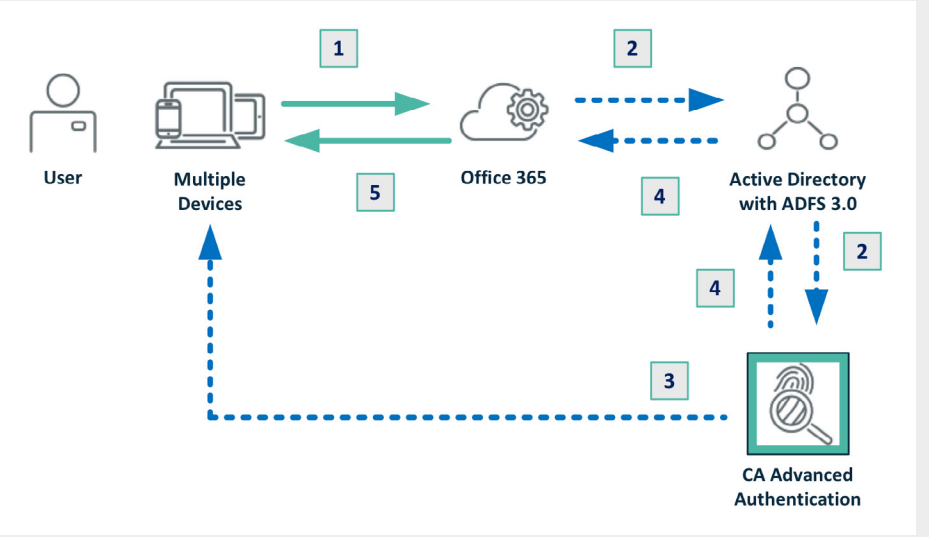
- Microsoft Office 365 subscription plans/licenses
- ADFS 3.0 (on Windows 2012 R2)
- Microsoft Active Directory (should be configured with the same domain name as Microsoft Office 365)
- Office 365 Tenant account configuration with domain
- Users created/synchronized with Azure Active Directory for this domain
- Public registered domain
- SSL certificate for the domain

The solution module supports Office 2013 or higher and leverages "modern authentication," a capability that was built into Microsoft Office to allow third-party authentication solutions to be integrated. Office 2016 supports modern authentication by default, but Office 2013 requires some configuration to support this feature. The solution module integrates with CA Advanced Authentication 7.x or higher.

How it works

Figure B.

Generic authentication process.



Process steps:

1. The user accesses the Office 365 Portal and provide User ID (UPN).
2. After successful UPN validation, Office 365 will redirect the user to CA Advanced Authentication, Authentication Flow Manager (AFM) through ADFS based on the configured claims.
3. AFM will authenticate the user as per configuration (MFA, risk analysis with step-up, etc.).
4. After successful authentication, the request is redirected to office 365 thru ADFS based on the relying party configuration.
5. Office 365 generates a JSON Web Token (JWT) token, which is sent to the device. The user will have access to all the office 365 applications as per the user permissions on the apps.

When using the Office clients, the process is very similar. When the user opens the Office client, it will automatically detect that CA Advanced Authentication is being used to authenticate the user. It will prompt the user for their Office 365 User ID (UPN) and forwards information to CA Advanced Authentication, which uses this as part of the authentication process. The authentication flow within CA Advanced Authentication will vary based on the type of credential being used. After successful authentication, the solution generates a Security Assertion Markup Language (SAML) token. After receiving the SAML token, Office 365 generates a JWT token, which is sent to the device. Each Office client can leverage this token to authenticate the user and grant them access to the respective cloud-based application.

Connect with CA Technologies at ca.com

CA Technologies (NASDAQ: CA) creates software that fuels transformation for companies and enables them to seize the opportunities of the application economy. Software is at the heart of every business, in every industry. From planning to development to management and security, CA is working with companies worldwide to change the way we live, transact and communicate—across mobile, private and public cloud, distributed and mainframe environments. Learn more at **ca.com**.

1 Verizon, "2016 Data Breach Investigations Report," April 2016

2 J. Peter Bruzzese, "Office 365's Corporate Takeover is Imminent," InfoWorld, April 20, 2016