



F5 Secures and Simplifies Microsoft Office 365 Identity and Access Management

KEY BENEFITS

Secure anytime, anywhere

access to Office 365 through integrated, standards-based identity federation, single sign-on (SSO), and adaptive multi-factor authentication (MFA).

Simplify user access

to Office 365, increasing productivity while alleviating user password fatigue, eliminating insecure user credentials and mitigating password exposure.

Increase scalability while consolidating identity federation and access management infrastructure, saving time and cost.

Leverage existing, deployed MFA capabilities or built-in MFA, including one-time password (OTP) via email and certificate checks.

Transitioning to Microsoft Office 365

A staple of organizations worldwide, Microsoft Office has long been one of the most popular business productivity software suites. Cloud-based Office 365, Microsoft's subscription-based access to its well-known applications, has been adopted by organizations of all sizes to increase user productivity by enabling employees to work anytime, anywhere, from nearly any device. However, organizations often must overcome a few challenges to successfully deploy and gain the benefits of Microsoft Office 365.

Deployment and Identity Challenges

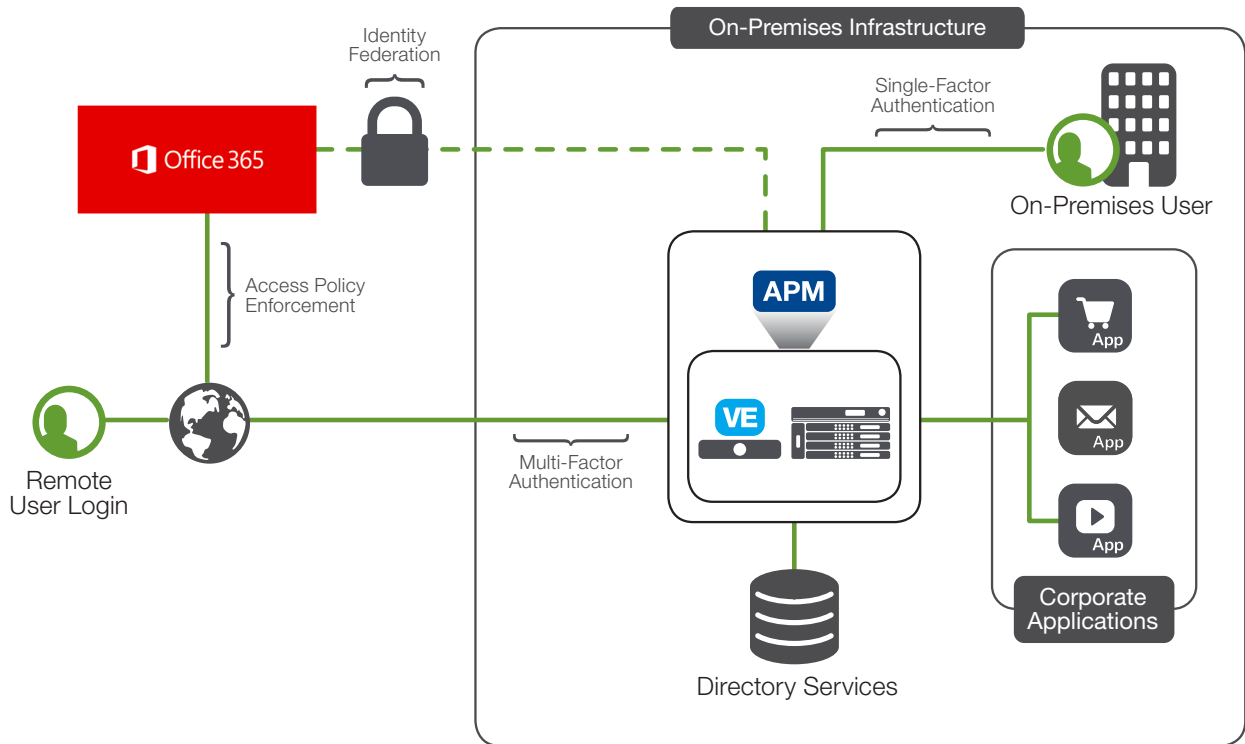
First, an organization must decide whether to stay the course with on-premises deployment, move directly into a cloud-based deployment, or architect a hybrid solution, maintaining some Office functionality on premises while offering Office 365 for anytime, anywhere user productivity.

An even bigger challenge, however, can be the federation of user identity and access management for enterprises using Office 365. Seamless, single sign-on (SSO) works well for users accessing Office 365 on premises, but organizations may require the enhanced security of multi-factor authentication when users are mobile or working remotely.

Office 365 offers three identity and access management models:

- **Cloud Identity Model**—User names and passwords are managed solely in the cloud with Office 365 creating a user identity, which is stored in and verified by Azure Active Directory.
- **Synchronized Identity Model**—An on-premises server manages user identity, while the user account and password hashes are synchronized to Office 365. Users enter the same password on premises as they would in the cloud, with their password verified by Azure Active Directory.
- **Federated Identity Model**—Performs similarly to the Synchronized Identity Model but uses an on-premises identity provider to verify the user password, which means that the password hash does not need to be synchronized to Azure Active Directory. This is the most secure method to access Office 365 because it provides more control over user credentials, which mitigates the threat of lost or stolen credentials, and it provides easier integration with existing or new MFA methods.

Identity Federation With Multi-Factor Authentication



Securing and Simplifying Identity and Access Management

By securing and simplifying user access to Microsoft Office 365 and the sensitive documents and data behind its applications, F5 helps organizations ensure user productivity, while mitigating potential threats to user credential security and theft of critical data.

The F5 solution blends identity federation, SSO, and flexible MFA driven by granular, context-based policies for Microsoft Office 365 (as well as other cloud-based and SaaS applications), securing access without increasing IT costs or the complexity of the user experience. In addition to supporting an array of industry standards for federating user identity, including SAML, the F5 solution enables different types of authentication mechanisms to communicate with each other, thus reducing “password fatigue” and eliminating insecure credentials. Finally, the F5 solution offers adaptive MFA, including certificate checks and context-aware, one-time passwords (OTP) via email.

By federating user identity, providing and supporting a variety of MFA options, and protecting user credentials, the F5 solution secures access to Office 365, enabling businesses to mitigate the risk of password exposure and data theft. Moreover, organizations already using F5 to authenticate and protect their existing Office deployments can leverage their existing authentication methods while migrating an on-premises deployment to Office 365.

Protecting Credentials Shared with Azure Active Directory

When deploying Office 365, some organizations using the Synchronized Identity Model have security concerns about replicating their user names and passwords in Azure Active Directory. Most businesses choose to deploy a Federated Identity model that allows users to authenticate against their local Active Directory without exposing passwords to the Azure cloud. But while the user names and passwords are sent through a secure tunnel to Office 365 for authentication, they are sent unencrypted. Should that SSL-secured tunnel be compromised or the Azure cloud be breached, all those user names and passwords would be exposed.

Fortunately, the F5 identity and access solution proxies ActiveSync traffic destined for Office 365, and encrypts user credentials before they leave the data center perimeter. When Microsoft requests an assertion from the federated identity provider, the F5 solution decrypts the user credentials before passing them along for authentication, ensuring that business-critical user names and passwords remain highly secure.

Helping Businesses Thrive

Cloud-based Office 365 helps businesses thrive, driving user productivity and facilitating growth. Secure, simple, and scalable, the F5 identity and access solution for Office 365 allows organizations to optimally leverage Microsoft's software suite, delivering consolidated SSO, contextual MFA, and additional security for ActiveSync traffic. The F5 solution, including BIG-IP® Access Policy Manager® (APM), blends identity federation, SSO, and flexible MFA driven by granular, context-based policies for Microsoft Office 365 (as well as other cloud-based and SaaS applications), securing access without increasing IT costs or the complexity of the user experience.

To learn more about F5 solutions for Office 365 migration and deployment, please visit <https://www.f5.com>, or contact your F5 representative or channel partner.

