Securing Access to the Office 365 Cloud with Two Factor Authentication

Published: February 2012

For the latest information, visit www.whymicrosoft.com

Microsoft

Microsoft Office 365

Table of Contents

Executive Summary

Microsoft designed the Office 365 productivity suite specifically for customers' secure access over the Internet and for the customer's choice of a partial or all-at-once transition to the cloud. Office 365 provides the flexibility to temporarily or permanently maintain a hybrid environment so you can move to the cloud gradually, or maintain some users on-premises indefinitely. Many organizations using Office 365 in a hybrid cloud and on-premises environment choose to secure user access to Office 365 with two factor authentication. In doing so, users can also have convenient, Single Sign On (SSO) to both Office 365 services and on-premise applications. Considerations in implementing two factor authentication for Office 365 include using Active Directory and Active Directory Federation Services technologies.

Whether you are learning about Office 365 or about to adopt the solution in your organization, this paper will help you to select your approach to user authentication, will guide you through basic planning and deployment steps, and point out additional resources.

Office 365 User Identities

Customers use Office 365's authentication capability to access the service from inside or from outside the corporate environment or organization. Office 365 customers have the option to implement single factor or two-factor authentication. Single factor authentication is a combination of username and password. Two-factor authentication uses both a first factor, something you know such as a password; and a second, different type of factor, which is something you have such as a token, to reduce the risk of unauthorized access to your applications and data.

With Office 365, your authentication possibilities vary depending on how you establish user identities. The Office 365 administrator has three options for identifying users to Office 365:

1. Microsoft Online IDs exclusively
2. Microsoft Online IDs with Active Directory Synchronization
3. Federated Microsoft Online IDs with Active Directory Synchronization

When an organization chooses Microsoft Online IDs exclusively, users create Office 365 accounts which they use to sign in to all their Office 365 services via a single username and password. We recommend that users create and use passwords that expire within 90 days, are at least 7 characters long, and include numbers or symbols, to help protect their Office 365 service from unauthorized access. See "Office 365 Password Policy" in the Resources section of this paper for the full considerations. Smaller companies and other organizations which don't use Active Directory, or don't use it extensively, elect this option. When Office 365 customers elect to use Microsoft Online IDs exclusively, Microsoft manages their password policy in the cloud. This includes password reset services.

Organizations which have Active Directory on-premises yet do not have a business need for two-factor user authentication to Office 365 services, may want to create users and groups on-premises. These customers may choose to establish Office 365 identities as Microsoft Online IDs with Active Directory Synchronization. This approach leverages their existing user and group administration processes, and Active Directory Synchronization enables them to extend user administration processes to the cloud.

The third option for creating Office 365 user identities is our focus. When customers choose to implement federated identities plus active directory synchronization, they can enable access to their Office 365 application with two factor authentication, and users have the convenience of Single Sign On to on-premises applications and to Office 365 with the same identities. As a system requirement, organizations that have Active Directory in place and have business needs for two factor authentication to Office 365 will assure they have on-premises Active Directory Federation Services (ADFS), a service of Microsoft Windows Server 2008, in place to enable use of federated identities. This approach to identity management uses ADFS to authenticate users on Office 365 using their corporate ID and password. In these organizations the customer administers Office 365 identities on-premises. The organization can then implement a second authentication factor in addition to passwords, purchased from a third party, to increase security. RSA Security may provide the second authentication factor via its well-known solution, RSA SecurID.

This table summarizes the three alternatives for establishing Office 365 user identities.

Table 1: Office 365 Identity Options

Microsoft Online IDs	Microsoft Online IDs plus Directory Synchronization	Federated Identities plus Directory Synchronization
Appropriate for • Small organizations without Active Directory on premises	Appropriate for • Mid-sized and large organizations with Active Directory on premises	Appropriate for • Larger, enterprise organizations with Active Directory on premises
Advantages • Requires no on-premise servers	Advantages • Administer users and groups on-premises • Active Directory synchronization enables Active Directory to be the primary system for managing users and continuing to use existing processes.	Advantages • You can implement strong, two factor user authentication • You enable hybrid scenarios • You have Single Sign On to cloud and on-premises applications using corporate credentials • Your administrator creates and manages IDs on-premises, and controls password policy there
Considerations • Two factor authentication is not available • No Single Sign On (SSO) for on-premises applications • Involves 2 sets of credentials, on-premises and cloud, with different password policies • Office 365 IDs are created and managed in the cloud	Considerations • Two factor authentication is not available • No SSO for on-premises applications • There are different password policies on-premises and in the cloud • Organizations need an additional server for active directory synchronization	Considerations • Additional servers would be required to enable identity federation (ADFS) and Directory Synchronization (DirSync) • Single Sign On • Identities are created and administered on-premises and synchronized to the cloud

How Organizations Use Two Factor Authentication Today

Today, many of us use two factor authentications in reaching online resources at work, at school, or at home. Where personal data or financial information is concerned, and also when industry regulations demand it, many businesses and some schools provide employees, customers or business partners with a second factor to access applications. Two factor authentication is simply more secure than providing a username and password combination only. For example, for online banking, institutions may provide a username and password login as a first factor, and a special code as a second factor. In paying bills or checking balances online, many people use both of these factors to demonstrate to their network that they are who they claim to be. Then the user is authenticated: logged on.

In each of these scenarios, an organization chose the security level that 2 factor authentication provides, and used RSA Security's SecurID technology:

- A United States county government uses a hardware token to comply with the US Federal Bureau of Investigation's criminal justice regulations for security of public safety information.
- A small, United Kingdom-based preparatory school provides two factor authentication via hardware tokens so that educators can access sensitive, student records via the Web when working from home. In doing so, the school also addresses emerging, local compliance considerations.
- An online, for-profit, gaming company provides hardware tokens to clients to protect clients' fee transactions over the Web.

User Authentication to Office 365

When customers elect to move to the cloud with Office 365 using only Microsoft Online IDs, Microsoft employs and manages best practices for users' single factor authentication. For example, Office 365 captures password history so that users do not fall back to using previous passwords. Additionally, by default, Office 365 requires that users create passwords which expire within 90 days, are at least six characters long, and include numbers or symbols, and Office 365 sets a password expiration period. See "Office 365 Password Policy"in the Resources section of this paper for additional details and safeguards regarding password history, lockout, and use of strong passwords. Microsoft has also designed Office 365 so that local administrators can implement the same policies in hybrid, on-premises and cloud implementations which include Active Directory Federation Services.

Customers may choose to set a higher standard for authentication by using the security which two factors provide. As of this writing, Microsoft recommends that Office 365 customers electing this option acquire RSA Security's token-based security service. RSA Security, a division of EMC Corporation, has been a security innovator and security industry leader for twenty five years. Its RSA SecurID customer case studies draw from a group of 30,000 customers worldwide, and include a wide range of applications and industries. Historically, enterprises have depended on the company's token-based security.

This approach to strong authentication for Office 365:

- Leverages a trusted technology that many customers already have in-place, are experienced with, and are using it in a range of applications,
- Is available from an industry leader in security with proven technology.

As part of the SecurID service, the token displays a 6 digit code that changes every 60 seconds. The organization must acquire and provide a token for each Office 365 user. In companies already using SecurID, many Office 365 users may already have a token which they carry with them to receive a secure code. The user inputs their username and password followed by that code to prove their identity and access Office 365.

Hardware Token Delivery of 2nd Factor

Next, Microsoft encrypts the connections users establish over the Web to the Office 365 service using industry-standard, 128-bit Secure Sockets Layer/Transport Layer Security (SSL/TLS) encryption. Microsoft also protects the connection by SSL/TLS encryption if the organization has elected a different identity and authentication method, and the user signs in using a single factor only.

Planning for Two Factor Authentication to Office 365 with SSO

Organizations not already using SSO or Active Directory Federation Services 2.0 on-premises, implement single sign-on using ADFS 2.0. After deploying ADFS 2.0, customers can also implement two factor authentications with RSA SecurID. These organizations, often enterprises, benefit from the security which two-factor authentication to Office 365 provides, and have convenient, single sign on access to services and applications in a hybrid environment. With this approach the customer administers Office 365 identities on-premises. On-premises Active Directory Federation Services, a service of Microsoft Windows Server 2008, authenticates users via their corporate ID and password, and the organization employs RSA SecurID for second factor authentication to Office 365.

When planning this implementation, consider whether users:

- have a currently supported operating system
- are inside or outside the corporate network
- Employ rich clients or web browsers.

Also consider whether your authentication provider interoperates with other services your organization uses. The following table outlines the implementation scenarios which Office 365 supports.

Table 2: Two Factor Authentication with Single Sign on for Office 365

Scenario	Supported/Unsupported	Notes

Scenario	Supported/Unsupported	Notes
- Domain joined PC	- Supported for Lync and SharePoint - Supported for Outlook Web Access	- Allows users to log onto the corporate Active Directory from either inside or outside the corporate network. - The existing infrastructure supports domain-joined PCs, yet you must configure Office 365 for federated identities using SSO.
- Non-domain joined PC with web application	- Limited Support - See the Deploying Two-Factor Authentication for Office 365 section of this paper	- Requires two-factor authentication when users sign into web applications from a non-domain joined computer, such as a home PC or Internet kiosk.

Deploying Two Factor Authentication for Office 365

So, if your organization is ready to get started, what do you need to do? It's likely that users will need to access Office 365 from locations outside of the corporate network, such as from a home PC or an Internet kiosk. In terms of current technology available, an organization has these two options for enforcing two-factor authentication with single sign-on for users accessing Office 365 web applications outside the corporate network:

1. Integrate the Active Directory Federation Services 2.0 proxy logon page with the strong authentication provider, RSA SecurID, by customizing the:
   - Organization's Active Directory Federation Services 2.0 proxy logon web page to introduce the extra fields needed to gather information for two-factor authentication.
   - Page to interact with two-factor authentication servers or services to authenticate users.
2. Use the Microsoft Forefront Unified Access Gateway SP1 server.
   - See the Future Possibilities section of this paper for the current recommendation for a sustainable approach to two factor authentication.
   - Use a Microsoft Forefront Unified Access Gateway SP1 server to support a wide range of two-factor authentication providers, and to support direct access to an expanded set of scenarios that involve two-factor authentication.
   - For more information, see Deploying Forefront UAG with AD FS 2.0.

For more details, download this resource to learn about deploying authentication services for Office 365:
Identity and Provisioning Service Description Office 365 Dedicated Plans Oct 2011.
You might also see the blog post: Office 365 with Federated Authentication, Identities in Active Directory.
See this post for specific guidance on configuring advanced options for ADFS 2.0 and Office 365.

Future Possibilities

From a technical standpoint, there are a wide variety of feasible; two factor authentication methods for Office 365. In fact, Microsoft technology enables two factor authentication with Microsoft Forefront Access Gateway and a choice of any of the authentication protocols which Forefront Access Gateway supports, including RSA SecurID, LDAP authentication, SSL client, certificate authentication, RADIUS, TACACS and WINHTTP authentication. Beyond this, it is technically feasible to authenticate users to Office 365 via either smart cards or biometrics.

Microsoft knows that technical capability is one thing and recommending a sustainable solution for an educational institution or a business of any size is much different. That is an important and much greater commitment. As business partners and customers test, verify and gain experience with how these technologies interoperate and work within organizations, Microsoft may begin to recommend both RSA SecurID and other two factor authentication technologies to Office 365 customers. Until that time may come, Microsoft recommends RSA SecurID for two factor authentication to Office 365.

Resources

- Office 365 Password Policy
- Identity Service Description
- Identity and Provisioning Service Description Office 365 Dedicated Plans Oct 2011
- Office 365 with Federated Authentication, Identities in Active Directory
- Configuring Advanced Options for ADFS 2.0 and Office 365
- Deploying Forefront UAG with ADFS 2.0.
- Office 365 Community
- RSA Announces More Secure User Access to Microsoft Cloud Services and Applications
- RSA SecurID Customer Case Studies
- RSA Security Innovation
- RSA Security History