WHITEPAPER

42Gears Support for Office 365

By 42Gears Team

Table of Contents

Introduction

Organizations need productivity tools, such as Microsoft Word, Excel, PowerPoint, Skype, Mail, and many other Microsoft applications, to perform day-to-day activities and complete everyday tasks efficiently. Organizations have long been using on-premise tools that call for high maintenance charges and significant support efforts, and pose challenges while scaling. However, many organizations are still supporting on-premise infrastructure due to security reasons or by choice.

Google and Microsoft have introduced cloud-based productivity tools (G-Suite and Office 365 respectively) to cope with problems related to on-premise setup. And an increasing number of organizations are migrating to cloud-based tools due to their cost-effectiveness and ease of management. Today, Microsoft's Office 365 is considered to be the most trusted cloud-based solution. With over 120 million business users, it has become the most adopted solution.

Benefits of Office 365

Office 365 (O365) offers effective productivity tools to businesses and enables team collaboration. Some of the many benefits of using O365 are:

- O365 offers a Single-Sign-On feature to end users. Users just need to log in once to any one application using their O365 login credentials and they automatically get logged in to other Office 365 applications.
- From the admin portal, IT professional can remotely configure email on the devices, manage permissions and updated versions of apps.
- Office 365 supports both on-premise as well as cloud-based infrastructure.

Deployment Architecture of Office 365

There are two kinds of authentication methods for Office 365 deployments:

- Cloud-based authentication
- Federated authentication

Depending upon the organization's infrastructure i.e. on-premise or cloud, they can opt for a suitable deployment method. Organizations working on cloud setup can opt for cloud

authentication method, whereas those working on on-premise setup have to federate their account using federated authentication method.

Cloud Authentication

This method is generally used by organizations that don't have an On-Premise Active Directory (AD) server and not ready to invest in a new on-premise infrastructure, or want to migrate to cloud infrastructure. In this method, the user accounts are managed in the cloud using Azure AD. User accounts can be created and managed from the Office 365 admin center or by using Windows PowerShell cmdlets.

In this method, organizations do not require on-premise servers. They just need to create user profiles in O365 Identity provider. When devices ask permission to access office tools, O365 Identity Provider will identify and authenticate the device users, verify if the devices are managed, and check if compliance policies are in place. Only post authentication, O365 Identity Provider will allow any device to access O365 tools and apps.

Federated Authentication

In this method, organizations must have an On-Premise Active Directory server setup. This on-premise server interacts with the O365 cloud server. The Office 365 server fetches user profiles or details from the Active Directory server stored on premise. Whenever device tries to access Office 365 tools and apps, it delegates the authentication to on-premise active directory. Once user is authenticated, access is allowed.

Why Do Organizations Need to Federate

Organization with in-house tools and apps on on-premise server: When organizations have in-house tools and apps on an on-premise server and don't want to store it on cloud, they federate the account. They need to connect the on-premise server to the O365 server to provide employees secure access to the required tools.

Organizations not using Azure AD MFA: Azure AD only supports Azure AD MFA. Organizations that wish to use any other Multi Factor Authentication (MFA) provider need to federate the account.

Certificate Based Authentication: Only Federated accounts can support client certificate based authentication.

Challenges of Office 365

Office 365 is, undoubtedly, a great tool for organizations to ensure team collaboration and empower employees with efficient office tools and apps that can be monitored/updated in real time. However, there are some challenges on this path.

- Office 365 is a cloud-based tool that requires access to the internet. Traditional on-premise tools, such as emails and apps, will not work when Office 365 is active.
- Presence of mobile devices, especially in BYOD scenarios, poses many challenges, such as corporate data protection, containerization and remote wipe.
- There are many office mobile apps that may pose security threats or be against to compliance policies.

42Gears Support for Office 365

In order to help organizations leverage Office 365 apps and tools, 42Gears UEM offers a viable support for O365 deployment. It simplifies configuration of Office 365 email and deployment of Office 365 applications on both employee-owned and corporate-owned mobile devices. Configuring Office 365 email is as simple as configuring a profile on the 42Gears UEM console and pushing it to a device/set of devices. Office 365 applications can be pushed by making use of the custom app store feature in the UEM console.

How to Manage Office 365 Emails and Apps on Mobile Devices with 42Gears

Defining and enforcing security policy framework across all emails and mobile apps are of utmost importance to IT professionals. 42Gears UEM provides a platform to configure business mail deployments securely on business approved devices, which enables employees to access business mails from their mobile devices without compromising data security.

Device Enrollment

Depending upon whether an organization is using Cloud Authentication or Federated Authentication, IT admins can configure 42Gears UEM to authenticate end users before they enroll their devices. This can either be SAML or OAuth-based authentication.

Certificate-based Authentication

Accessing corporate emails on personal devices offers a level of convenience and improves productivity. However, it may also pose many challenges, such as ensuring security over unsecured networks, deploying emails across multiple mobile devices and restricting them against unauthorized access. Certificate-based authentication helps corporates deal with such challenges. Certificates deployed on devices allow employees to access business mails on their devices. Failing to comply may restrict access to mails.

Mobile Email Management (MEM)

Allowing email access to only certificate-deployed devices doesn't secure emails completely. As corporate emails can be leaked via other email accounts, such as employees' personal accounts to other unauthorized mails, restricting these possibilities requires an extra level of security. This is what a Mobile Email Management (MEM) solution can help with.

The MEM feature in 42Gears UEM solution can restrict users to access emails through secondary applications except for the application that has security controls over emails. From the Office 365 Admin center, IT admins can disable email access for all mobile clients by default. When devices enroll into 42Gears UEM, employees will automatically get mail access to pre-approved email application on their devices.

Containerization and Data Loss Prevention (DLP) controls

By deploying Office 365 apps through 42Gears UEM, 42Gears enforces containerization of applications to prevent data loss. The containerization policy helps businesses prevent sharing O365 data to personal apps. 42Gears offers different containerization controls for different operating systems such as Apple iOS, Android and Windows.

- Apple iOS: 42Gears supports containerization for Apple managed apps to prevent data loss from work and personal apps. It prevents opening an attachment from a managed email account in an unmanaged application.

- Android: 42Gears offers containerization for Android devices, which enables Office 365 apps and email to be deployed inside an app container. It prevents data leakage between work and personal

apps, ensures O365 data is encrypted, managed and can be remotely wiped. Moreover, businesses can enforce advanced DLP features, such as restrictions on screen capture and copy/paste.

- Windows: 42Gears offers containerization for Windows devices to ensure emails are set up only on managed devices and can be wiped remotely.

Summary

Today, many organizations are adopting new productivity apps or redesigning the digital communication strategy to collaborate with and support their teams. Organizations investing in new apps or infrastructure must ensure that their UEM solution integrates well with the new infrastructure and apps in which they are investing. 42Gears' UEM solution can be easily integrated with the Office 365 suite of applications. It supports multiple device ownership scenarios, both on-premise and cloud infrastructure, and multiple platforms, such as Android, iOS and Windows.

Learn more about configuring user accounts and managing **Office 365** apps with **42Gears UEM** Solution. Watch Office 365 Webinar now.