Breaking the Last Barriers to Microsoft Intune Integration

Scale your mobile app program faster with a no-code approach that simplifies security integration and streamlines backend connectivity.

BlueCedar

Business is on the move

The future of business doesn't have a street address. It doesn't even have a URL. It takes place at the edge, which is wherever employees and consumers are, on whatever devices or appliances they hold in their hands.

That future contains a world of possibilities—but for established businesses trying to make the leap from more traditional models, more than a few roadblocks stand in the way. Mobile app development teams are under pressure to create innovative mobile apps that delight and satisfy employees and consumers everywhere they go. At the same time, IT teams are scrambling to keep devices and data secure, even as the threat landscape grows larger and more sophisticated.

Inevitably, these aims collide, posing a challenge: How can companies launch and scale enterprise mobile apps that are easy to use, yet still provide rigorous protection for corporate data?

Enter the Microsoft Intune platform

In 2011, Microsoft launched Intune, its cloud-based service that focuses on mobile device management (MDM) and mobile application management (MAM). Its goal was to facilitate mobile device management and mobile application management from a single console. Today, Intune is better than ever before, giving IT admins app-level controls over corporate data on corporate-issued and bring-your-own (BYO) devices. Key for these security controls is the protection enabled by the Intune app SDKs and the integration with Azure Active Directory, which provide robust authentication services.

The growth of Intune coincides with Microsoft's renewed attention to Office 365. Thanks to the software giant's strategic efforts over the last two years, Office 365 has become the most widely-used enterprise cloud service based on sheer enrollment.

For companies invested in Office 365, the ability to use Intune-enabled apps at scale—whether built in-house or from ISVs—is essential to fostering greater corporate productivity.

When Office 365 is used within the Intune app ecosystem, it allows safe sharing of corporate data between apps, so users can complete complex workflows entirely on their mobile devices. App-level security controls keep everyone happy—users don't have to sacrifice privacy and IT doesn't have to compromise on security.

1 out of 5

corporate employees use an Office 365 cloud service[1]

[1] McAfee, Office 365 Adoption Rate, Stats, and Usage, 2019

Microsoft Intune and the rise of mobile apps for business

Launching innovative apps is on every company's roadmap, whether they develop them internally or customize third-party apps. But for companies whose core business lies outside of information technology, it can be difficult to keep up with changing end-user demands and emerging technologies around mobile apps.

And development is only half the battle. The big issue that keeps DevOps teams up at night is security. We've all seen the headlines and know that the risk of a cybersecurity breach is high. As more workers access corporate data around the clock, from unenrolled devices, keeping that data secure will continue to be a massive challenge.

> **Yet mobile apps aren't a nice-to-have; they're a business imperative.**

Mobile apps engage and connect workers everywhere they go

Companies use mobile apps to support a workforce that is widely distributed and on the go. It only makes sense to help employees do more in the moment, wherever they are, without requiring a desktop computer or a secured device in another location. Business happens everywhere—whether it's serving customers onsite, accessing data while on the go, or inputting information about the sales process right after an important meeting. If employees can't interact with data in a secure way from anywhere, companies risk falling behind more technically savvy competitors.

Custom mobile apps serve a wide range of needs, helping the business:

- Facilitate secure communication through chat and text
  - » Enable sales growth via quoting and deal tracking apps
  - » Foster rapid decision making by providing branch and remote employees with fast access to critical data
- Improve collaboration and project outcomes among distributed employees
- Help professional services organizations manage and track hours for large-scale projects
- Streamline the delivery of HR services, such as employee on-boarding and benefits administration

That's why Microsoft developed Intune

Microsoft understands that organizations need a cohesive way to manage their mobile app programs for a diverse digital ecosystem that includes enrolled and unenrolled devices.

The promise of Intune is significant.

Intune offers a method for encrypting and controlling data at the app level, with access and authentication to Microsoft's identify services. It provides organizations with a single source of app management, whether the device is under MDM controls or not. Workers using Office 365 apps on their personal mobile devices know that they'll never have to sacrifice privacy. Since IT can set policies that allow company data to be only shared between Office 365 and other Intune-enabled apps, there is no mixing of corporate and personal data and so no reason for IT to need device-level controls.

The problem? Integration isn't simple.

Manually integrating Intune into apps onto the Intune platform and enabling secure backend connectivity to assets that live behind the firewall (and not on Azure) has proven to be a challenge—one that has prevented many organizations from realizing the benefits of Intune.

The last barriers to Intune adoption

IT organizations trying to solve security concerns and enable ease-of-use often discover that integration on the Intune platform can be a lengthy, complicated process. The challenge plays out on two levels:

App Integration

First, there's the initial process of integration with the Microsoft Intune platform, embedding Microsoft Azure ADAL, and securing the mobile app.

- ✕ **Initial integration takes weeks of developer time.** This costly process often delays the launch of new apps.
- ✕ **Ongoing updates continually drain resources.** Every time an app is updated, which happens multiple times a year, it has to be secured all over again.

Secure Backend Connectivity

Second, there's the ongoing issue of giving authorized users on unenrolled devices access to firewalled data. Today, every time a user on an unenrolled device wants to access a backend system, they must manually start a device-level VPN and authenticate to the gateway. This has the effect of routing all data, including personal data, through the corporate network.

- ✕ **There's nothing simple or seamless about it.**
- ✕ **It defeats the original purpose of a mobile app.** Instead of helping end users accomplish something faster and more effectively, it makes them more frustrated and more likely to try solutions that aren't secure.

The no-code solution for a resource-intensive process

Solving these issues isn't easy. The current shortage of technical talent makes it difficult to build internal teams, and using outsourced teams has its own drawbacks. Many companies would rather avoid growing their development teams or relying too heavily on outside contractors.

There's another option for quickly and easily embedding Intune app protection and Microsoft Azure ADAL in mobile apps—one that doesn't require weeks of developer effort and a big budget.

Blue Cedar is the leading mobile app security integration platform that secures and accelerates mobile app deployment for enterprises and government organizations around the world. App developers and leading security service providers view Blue Cedar as the trusted bridge that allows them to quickly and easily add custom security services into their apps.

The Blue Cedar Accelerator for Microsoft is a no-code solution that embed Microsoft Intune and Microsoft Azure ADAL in mobile apps. With it, you can enable app-level protection policies, without requiring device enrollment, and a single sign-on (SSO) experience across all Intune-enabled apps on the device. It provides a frictionless method for rapidly securing mobile apps and enabling enterprise-level controls, while saving substantial development hours and reducing IT costs.

A straightforward solution for a complicated process

Blue Cedar makes integrating Microsoft Intune into mobile apps simple. Our integration technology provides visibility from the application to the network layer, enabling reliable API interception across tens of thousands of native APIs. This deep visibility is what makes the Blue Cedar solution so effective, and how it relieves the two big challenges that currently plague many mobile app development teams.

Solved: App Integration

With Blue Cedar, you can embed Microsoft Intune App Protection Policies and Microsoft Azure ADAL authentication with one click. No weeks-long process, no expensive outsourcing required, and a much lower risk of manual coding errors.

Solved: Secure Backend Connectivity

Blue Cedar also allows you to embed a VPN into your mobile apps without coding, so your apps can connect seamlessly to protected networks or backend services. End users on unenrolled devices no longer need to configure a VPN, go through a lengthy authorization processes, or resign themselves to allowing their personal data to be controlled by their employers.

Blue Cedar gives your business an edge

10x
cost savings

3x
faster time
to value

Reduces
coding errors

Why choose Blue Cedar?

Trusted by enterprises across highly regulated industries, such as healthcare, legal services, and government, Blue Cedar provides a valuable shortcut, while still providing world-class security. It eliminates the costly, lengthy, error-prone manual coding required to integrate security into your mobile apps, so your business can keep moving forward.

- **It makes it easier and faster to secure apps.** Security integration times shrink from weeks to hours, and does not affect your internal teams. You don't need to train anyone or learn new vendor SDKs.

- **It makes connectivity issues a thing of the past.** Users on both managed and unmanaged devices can log in and authenticate easily, via an in-app VPN. The frustration and long wait times that come with end-user VPN configuration become a thing of the past. Blue Cedar integration makes employees more likely to use your apps, instead of using clumsy workarounds that put corporate data at risk.

- **It improves the end user experience.** Better productivity starts with a single sign-on experience that authenticates to cloud or on-premises Active Directory (AD)—while enforcing app protection policies. It's compatible with Microsoft 365 and other Microsoft Intune-protected mobile apps.

- **It works the way you do.** Blue Cedar is compatible with any development framework or database you use for building apps on iOS and Android. It offers visibility up to the network layer, so that you can add Microsoft app-level security and SSO functionality to any app—no code required.

The catalyst for an app-first world

For many companies, Blue Cedar is the trusted bridge that allows them to add custom security services into their apps for a range of needs, from secure communications to human resources services and more. As the edge continues to expand, Blue Cedar ensures that your mobile apps can be there to meet it—fully secured, and ready to help you take advantage of new business opportunities.

Read our data sheet on the Blue Cedar Accelerator for Microsoft

GET DATA SHEET

+1 (415) 329-0401 • 325 Pacifc Avenue, San Francisco California 94111 • www.bluecedar.com

BlueCedar