Migrating mobile device management to Intune in the Azure portal

Microsoft employees use various operating systems across a wide range of corporate and personal device types for work. Microsoft Core Services Engineering and Operations (CSEO), formerly Microsoft IT, traditionally managed mobile devices and applications through a common set of tools in a hybrid environment of System Center Configuration Manager and Microsoft Intune. To accelerate modern management for Windows 10, we’ve recently started the transition to standalone mobile device management (MDM) using Microsoft Intune in the Azure portal.

Hybrid MDM uses Intune as the cloud delivery channel for policies, profiles, and applications to devices, and Configuration Manager on-premises infrastructure to administer content and manage the devices. The hybrid implementation uses the same on-premises infrastructure and administrative console to manage mobile devices with Intune, and PCs and servers with the Configuration Manager client. As we move toward a cloud-only future and modern management, we’re working to streamline our physical infrastructure and reduce the overall number of traditionally managed clients to provide a modern workplace that’s always updated, always protected, and easily scalable.

More personal devices are being used for work, and more of our identity services are moving to the cloud. The number of traditionally domain-joined PCs at Microsoft is beginning to trend down, and the number of devices managed through Intune is trending upward. Scalability and ease of management are a couple of key factors in our decision to migrate to Intune in the Azure portal as our modern service platform. Intune in the Azure portal provides many advanced features, such as:

- **An integrated enterprise mobility management platform.** Provides an integrated cloud platform and admin experience in Azure portal for Intune, Azure Active Directory (Azure AD) Premium, and Azure Information Protection.
- **Mobile device management.** Offers rich MDM and information protection capabilities.
- **Scale and agility.** Simplifies setup and the rapid delivery of new capabilities. We can deploy and manage mobile devices without worrying about scaling up the physical infrastructure.
- **Role-based access control.** Supports restricting access to administrative functions, based on assigned roles and scopes.
- **Programmatic access (API).** Supports Intune APIs in Microsoft Graph, and has SDK and PowerShell management options.
- **Web console.** Includes an HTML 5-based console built on web standards with support for most modern web browsers.
- **Advanced reporting.** Provides the ability to create customized reports.

A new process and tools offer an easier migration path

Previously, moving from hybrid MDM, using Configuration Manager and Intune, to Intune in the Azure portal required a one-time authority switch. This approach was challenging because it required IT to move the entire tenant at once and forced administrators to reconfigure all settings in Intune, including re-enrolling all devices. To provide an easier transition, Microsoft introduced a new migration process of moving from hybrid to standalone Intune in a phased manner without disrupting the end-user experience. The new process consists of three components: Microsoft Intune Data Importer, mixed authority, and an improved MDM authority switch.
Microsoft Intune Data Importer

Microsoft Intune Data Importer is a new administrator design tool that’s designed to automatically copy device management data created in Configuration Manager to an Intune environment. Importable objects include configuration items, certificate profiles, email profiles, VPN profiles, wireless network profiles, compliance policies, terms and conditions, and apps. The importer tool helps address one of the biggest challenges we were facing when looking at moving from hybrid to standalone— the need to recreate all profiles, policies, and apps.

Mixed authority

Using mixed authority, we can selectively migrate users from our existing hybrid MDM configuration to Intune in controlled phases. This means that now we can migrate some groups of users to the standalone implementation while continuing to use the hybrid MDM environment for the remaining users and devices. After a user is migrated, we can use Intune to create and deploy policies, initiate remote actions, and enroll new devices.

Note: Tenant-level policies, such as our iOS APNs certificate, will function for users and devices managed by either hybrid MDM or Intune, but will be editable only via the Configuration Manager console while we’re using mixed authority mode.

Improved MDM authority switch

After we’re satisfied with testing Intune in the Azure portal, we can initiate a tenant MDM authority switch through the Configuration Manager console to migrate the remaining users from the hybrid MDM environment. All the policies and apps that were migrated from the Configuration Manager console, as well as tenant-level policies, will be available for configuration in the Intune console. Most importantly, enrolled devices aren’t required to re-enroll— making the migration entirely transparent to users.

Migrating our hybrid environment to standalone

We strive to provide employees a consistent experience regardless of the device they use, how often they use it, or what platform it runs on. At Microsoft, we require any device that’s used for work to be enrolled in Intune or domain-joined in Active Directory or Azure AD. At Microsoft, we have approximately 300,000 domain-joined devices that we manage with System Center Configuration Manager, and approximately 125,000 devices that we manage using Intune, including:

- 40,000 iOS devices.
- 17,000 Android devices.
- 20,000 Windows Phone devices.
- 34,000 Windows 10 devices.
- 3,000 Mac devices.

Before we allow any device to access corporate resources such as email, SharePoint Online, Skype for Business, OneDrive for Business, or any applications or services built on Office 365, we need to make sure that:

- The device and its apps are up to date with the latest version of the operating system and any security updates.
- Work data on the device is secured through encryption and information protection technology.
- The identity of the person using the device is verified through multi-factor authentication.

We started our migration using a phased approach that’s allowing us to migrate and test subsets of users and devices while the remaining users and devices are still being managed by our hybrid MDM environment. We wanted to make sure that migration process would be transparent to our users.
Solution architecture

Assessing our hybrid environment

As part of our pre-migration assessment, we ran the Intune Data Importer tool, without performing the actual import, to collect data about objects we selected from our Configuration Manager hierarchy. Importing Configuration Manager data to Microsoft Intune saves us time by automating the process of recreating objects from Configuration Manager to Intune, plus it provides details about the objects we can import and information about the objects that can’t be imported. This step was useful in helping us identify which objects would need to be recreated in Intune rather than imported—helping us better plan our migration phases and more accurately estimate the time required to mitigate the objects that had errors.
### Table 1. Sample import statistics

<table>
<thead>
<tr>
<th>Import object type</th>
<th>Importable</th>
<th>Not importable</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>App</td>
<td>688</td>
<td>26</td>
<td>Most applications in our environment could be imported.</td>
</tr>
<tr>
<td>Certificate profile</td>
<td>22</td>
<td>5</td>
<td>A small number of configuration profiles needed to be recreated in Intune.</td>
</tr>
<tr>
<td>Configuration items</td>
<td>168</td>
<td>33</td>
<td>Most configuration items could be imported. We took this opportunity when looking at the ones that would need to be recreated to determine whether they were all still required or should be retired.</td>
</tr>
<tr>
<td>Deployment</td>
<td>395</td>
<td>576</td>
<td>Many deployment groups and collections couldn’t be imported because of complexities in how we create collection targeting and groups.</td>
</tr>
<tr>
<td>Policy</td>
<td>19</td>
<td>5</td>
<td>Some policies weren’t importable and had to be recreated in Intune.</td>
</tr>
<tr>
<td>VPN and wireless network profiles</td>
<td>13</td>
<td></td>
<td>Our wireless network and VPN profiles couldn’t be imported because of a mismatch in the way we had implemented our configuration schemas between Configuration Manager and Intune. Additionally, many organizations have many fewer connection profiles.</td>
</tr>
</tbody>
</table>

While analyzing the information about importable objects and errors, we took that opportunity to identify stale or obsolete objects—such as test apps, idle devices, or outdated policies—that might no longer be required. Beyond simply being an exercise in our migration process, this activity gave us an opportunity to critically look at our processes, and to streamline our environment—this is key toward our goal of implementing cloud-only, modern management at Microsoft.

### Preparing Intune

After assessing our environment, we began the task of preparing Intune for user migration. As a prerequisite, we needed to validate that we had Intune license assignments for all users. Because we were coming from a hybrid environment, we already had Network Device Enrollment Service and Exchange connectors installed. We also needed to ensure that all the required administrative access permissions for Configuration Manager and Intune were granted.

*Note: If you’re not already an Azure AD tenant admin, an Azure AD admin will need to make the Intune Data Importer tool a registered app in Azure AD and provide user access to the users who will be performing the migration.*

We decided which Intune roles, and their scope and assignments, we needed. Examples include app manager, policy manager, profile manager, and helpdesk operator. We then created Azure AD groups and made object assignments to these groups.

### Planning and testing our migration approach

We can configure a mixed MDM authority to change the MDM authority for specific users within the same tenant by selecting some users to be managed in Intune while all other devices continue to be managed with hybrid MDM. As part of planning and testing our approach, we created a small number of test accounts and enrolled those devices in hybrid MDM. We added those test accounts to a migration Active Directory security group. Because groups can be
Migrating mobile device management to Intune in the Azure portal

synced to Azure AD groups, deployments for the imported objects can be imported if the user collections in Configuration Manager are based on Active Directory groups. Deployments will appear as assignments in the Intune console. After we migrated the test migration group and validated the functionality of objects imported from Configuration Manager and those that were newly created, we excluded the migration collection from Configuration Manager. After the migration user collection was updated, Intune cloud user sync removed the users from Configuration Manager and Intune hybrid MDM, and the standalone Intune environment became their management authority.

Migrating users in controlled phases

After we finished pre-migration planning and testing, we began migrating small groups of users. As each group was migrated, and functionality was validated, we increased the number of targeted users in each phase.

<table>
<thead>
<tr>
<th>Pre-pilot validation</th>
<th>Pilot phase</th>
<th>Phase 1:</th>
<th>Phase 2:</th>
<th>Phase 3:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Migrated 100 users from our group</td>
<td>Migrate ~1,000 users from our organization</td>
<td>Migrate ~10,000 users from different groups with a priority placed on Android and iOS devices</td>
<td>Migrate remaining users at ~10,000 at a time in targeted groups</td>
<td>MDM switch from hybrid to standalone</td>
</tr>
</tbody>
</table>

Figure 2. Phased approach to migration

Performing test cases to validate end-to-end device manageability

Mixed authority made it possible for us to test that standalone functionality was working as expected, for each small subset of users, on the migration collection before we started migrating additional users. Our migration testing included:

- Installing apps from the company portal on migrated user devices for all platforms.
- Validating resource access certifications and profiles, including wireless network configurations and VPN.
- Ensuring conditional access works properly after the migration, for both existing and new users.
- Enrolling a new device for a migrated user.
- Navigating to the Intune web portal and reviewing the device and user reports.

As soon as we complete the migration of all the remaining users, we will initiate the MDM authority switch from Configuration Manager and Intune to Intune in the Azure portal.

Changing our MDM authority to Intune

Changing our MDM authority to Intune is the last phase, and final milestone, of our migration. After we ensured that all users and devices managed by hybrid MDM were successfully migrated to Intune, we completed the steps in the Configuration Manager console to delete our existing Intune subscription and change our tenant-level MDM authority.
Reporting

We rely on reporting for planning, analyzing business logic, and demonstrating service accountability through metrics. There are three options available for reporting, and we’re currently using all three options based on our business needs:

- We use the [Microsoft Azure](https://azure.microsoft.com) portal for overview and export details such as individual devices, apps, users, and policies. It’s very useful for reporting counts and amounts.
- We use [Intune API in Microsoft Graph](https://developer.microsoft.com) for real-time reporting to which we want to apply business and/or custom logic to extract custom variables.
- The [Intune Data Warehouse Power BI content pack](https://powerbi.microsoft.com) is useful for reporting historical or trending data for custom reporting needs. It’s refreshed at regular intervals, though it’s not considered real-time data, and is useful in helping us transform data into high-level views that can be consumed by a broader audience, including stakeholders.

Lessons learned

- Include all service and business stakeholders who are dependent on hybrid services in all your planning and pilot phases—for example, enterprise security; app; certificate; resources access; and wireless network, VPN, and helpdesk teams.
- Plan for training or brownbag sessions for Intune in the Azure portal prior to beginning your migration. It’s important that support personnel and administrators:
  - Know how to set up new users and policies.
  - Are familiar with the new portal.
  - Can access data.
  - Are able to troubleshoot helpdesk requests.
- Review all reporting consumers and prepare for new experience and tooling requirements. Any legacy reporting that used SQL won’t be available.
- Leave some support team members in the hybrid MDM environment until the last migration phase so they can support other hybrid users.
- Keep the migration duration short to minimize object changes, app updates, and policy changes, that have to be managed separately in the Configuration Manager console and in the Azure portal.
- After you plan the duration of your migration project, plan your tenant level settings accordingly. To avoid certificate renewals during the migration phases, check the validity of device-specific cert renewals—for example, the Apple Push Notification (APNs) certificate.
- During user migration phases, plan to take exported user and device data offline from Configuration Manager for validation purposes before each phase. It’s also important to recognize that tenant-level setting and configurations must be managed in Configuration Manager until everything is migrated. Intune roles, such as app manager, policy manager, profile manager, and helpdesk operator, can be assigned only for users who are migrated to Intune.
- When assessing your environment, it’s important to make sure that you understand the relationships with collection use and reuse. You will want to make sure that your Intune subscription collection and other collections’ “include” or “exclude” settings aren’t used by other Configuration Manager deployment collections.
- All tenant level settings must be managed in Configuration Manager until the switch to all users, by default, are managed by Intune.
- Automated processes in Configuration Manager might not have counterparts in Intune. For app publishing, we had to rebuild the automated processes we were using in Configuration Manager in Intune using Graph APIs. We recommend that reporting and engineering teams [learn Graph API](https://developer.microsoft.com) for an efficient way to manage Intune, build automation, access real-time data, and create custom reporting.
Next steps

If you’re thinking about deploying Microsoft Intune and aren’t sure which environment is best for you, read Choose between Microsoft Intune standalone and hybrid mobile device management with System Center Configuration Manager to help you decide. If you have hybrid MDM and have decided to migrate, download the Microsoft Intune Data Importer and see Start migrating from hybrid MDM to Intune standalone.

For more information

Microsoft IT Showcase

microsoft.com/itsshowcase

Migrate hybrid MDM users and devices to Intune standalone

Microsoft Intune Data Importer v1.1

Working with Intune in Microsoft Graph

Use the Intune Data Warehouse

Co-management for Windows 10 devices

Manage Windows 10 in your organization - transitioning to modern management

Intune PowerShell samples

© 2018 Microsoft Corporation. This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.