Rimo3

Microsoft Intune

THE JOURNEY TO FULLY CLOUD NATIVE
WINDOWS ENDPOINT MANAGEMENT

JAMES GRAHAM, PHD, FIELD CTO

Foreword

In this whitepaper we discuss the business value of migrating your Windows Endpoint Management to Cloud Native [1] and the routes to get there.

This is a goal that many organizations have right now. However, the journey for some can be quite a challenge, particularly for those with complex application estates.

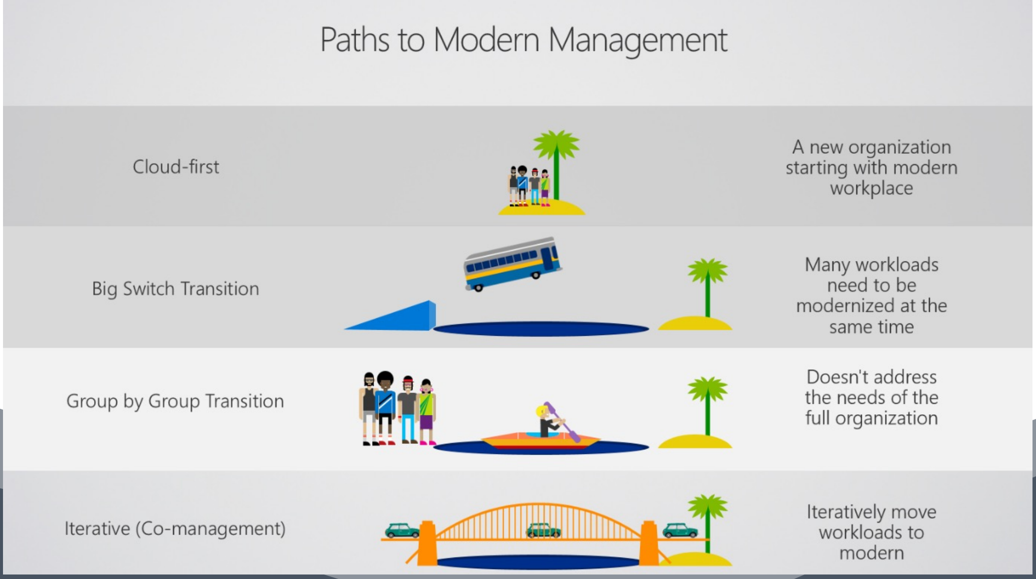
Microsoft has provided options to support organizations on this journey, which we will discuss in this whitepaper. However, what I have found when speaking to organizations over the past five years is that their complex application estates are keeping them anchored to Configuration Manager, and the options that have been provided will get them most of the way to Cloud Native but do not solve the application problem.

I wanted to write this whitepaper to give organizations an understanding of how they can get all the way to Cloud Native for their Windows Endpoint estate without having to leave the applications behind.

What is Cloud Native....4
The Business Value....7
Configuration Manager to Microsoft Intune....9
CMG....10
Tenant Attach....11
Co-management....13
Compliance Policies....15
Windows Update Policies....15
Resource Access Policies....16
Endpoint Protection....16
Device Configuration....16
Office Click-to-Run apps....17
Client apps....17
Summary....17
Solving the Application Problem with Rimo3....18
Import, Discover, Test, Conversion, and Export....18
Rimo3 Discovery....19
Discovery data results....20
Custom Operating System Image Support (Azure)....21
Rimo3 Intelligent Smoke Test....22
Unattended Intelligent Smoke Test Automated Sequence....23
Rimo3 Multi-session Intelligent Smoke Test....23
Rimo3 Automated Modern Packaging....23
Rimo3 automated Intune export....24
Rimo3 automated MSIX conversion....24
Post Packaging Automated Intelligent Smoke Test....25
Rimo3 Integrations 25
Application Export/Deployment....25
Partner Opportunity....26
Closing 28
Bibliography....29

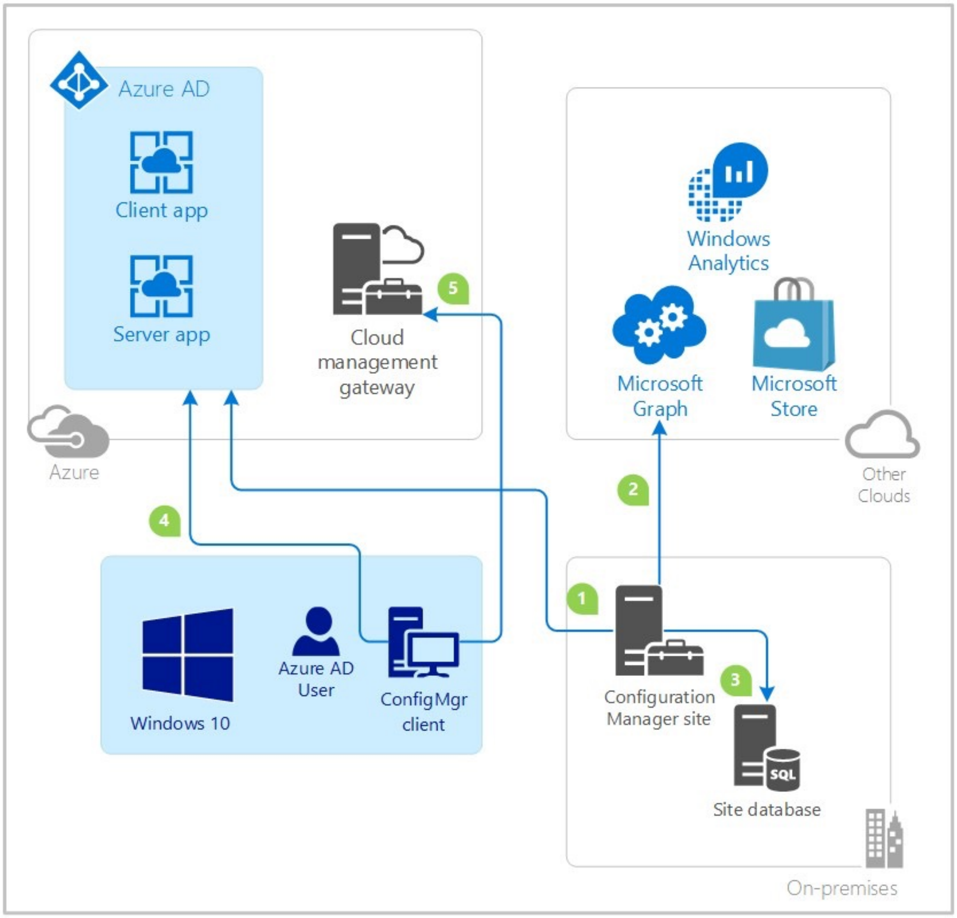
What is Cloud Native

The concept of Cloud Native from a Windows perspective is not necessarily a new concept, in fact, this was something that I was discussing with customers when I first joined Microsoft back in 2017. Back then Windows Autopilot [2] was still a relatively new concept and certain industries would find this approach unfathomable given their complexity and reliance on their custom image approach. Microsoft Intune from a Windows management perspective was also in need of enhancements, especially when compared to Group Policy, which is what many customers were reliant on at the time. Therefore, this leap from traditional on-premises Windows management to Cloud Native was too big an ask on many organizations who were still struggling with the concept of Windows as a Service [3] on Windows 10.


Paths to Modern Management
Cloud-first
A new organization starting with modern workplace
Big Switch Transition
Many workloads need to be modernized at the same time
Group by Group Transition
Doesn't address the needs of the full organization
Iterative (Co-management)
Iteratively move workloads to modern

To help customers bridge this chasm Microsoft released co-management [4], thus providing organizations with a palatable migration path to Microsoft Intune. However, for some, this was still a big ask given that Windows endpoints would need to be enrolled into Microsoft Intune to be able to take advantage of the features provided therein. Co-management provided organizations with the ability to shift workloads from Configuration Manager to Microsoft Intune at their own pace, and at the same time provide routes for organizations to achieve this for both existing devices and new devices.

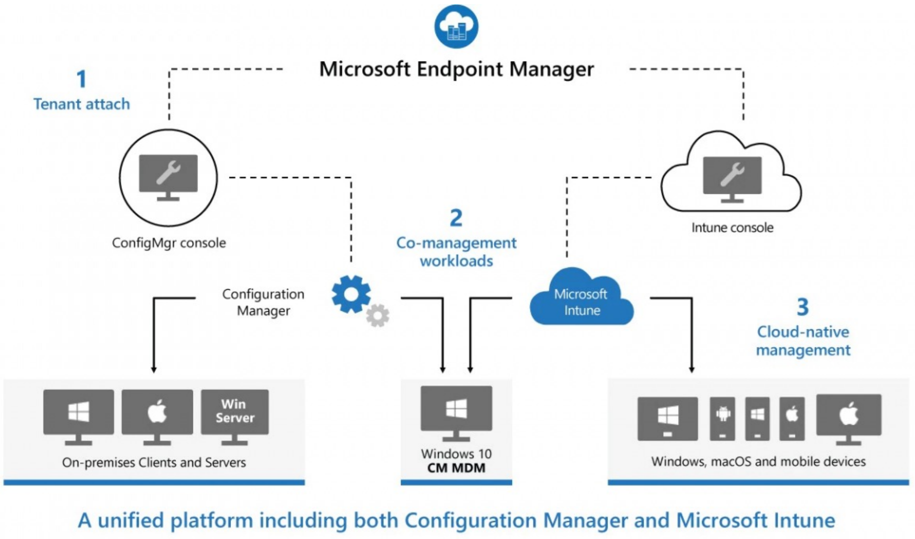
Alongside Co-management, Microsoft also provided a route to manage Configuration Manager clients from the internet with the Cloud Management Gateway (CMG) [5]. The CMG provided organizations with the ability to manage remote users without the need for them to be on the CORP network, which would include remote devices receiving policy and checking in, and being able to distribute applications via the CMG, which would act as both a Management Point and a Distribution Point (optional).



I recall at a Microsoft Event; I demonstrated the ability for an organization to deploy an end user device with Windows Autopilot from an internet connection and bootstrap the Configuration Manager Client. The client would then connect to the CMG to onboard and gain policy from an on-premises Configuration Manager server and receive policy and deploy an application from Software Centre, without ever touching CORP network. Then co-management organizations can choose which workloads are managed by Intune or Configuration Manager. Thus, providing organizations with the ability to leverage Cloud Native Windows management without the need to worry about migrating all their applications over to Microsoft Intune. Not quite as straightforward as Brad Andersons' #Just4Clicks slogan in 2018 [6], but I wanted to provide a practical use case that would resonate.

In 2020, Microsoft announced the rebranding of Unified Endpoint Management to Microsoft Endpoint Manager, which to this day is still a bit confusing. Essentially, Microsoft Endpoint Manager was the bringing together of Microsoft Intune and Configuration Management under the same marketing banner. What changed? Well, nothing really changed fundamentally, aside from a new URL to access Intune and the launching of a new acronym, MECM (Microsoft Endpoint Configuration Manager). However, within this rebranding launch, was a very exciting feature – Tenant Attach [7].

Tenant attach was essentially the ability to surface Configuration Manager clients into the Intune console, thus finally unifying the experience. One of the main advantages was the ability to include those on-premises managed Windows endpoints in your Endpoint Analytics insights [8]. Alongside this feature, Microsoft also catered for a helpdesk persona by allowing certain actions, previously only being possible via the Configuration Manager console, available in Intune. Unfortunately, Microsoft has never gone on to expand this capability into further personas.


Microsoft Endpoint Manager
1
Tenant attach
ConfigMgr console
2
Co-management workloads
Intune console
Configuration Manager
Microsoft Intune
3
Cloud-native management
Win Server
On-premises Clients and Servers
Windows 10
CM MDM
Windows, macOS and mobile devices
A unified platform including both Configuration Manager and Microsoft Intune

In this section I've touched on the 3 ways Microsoft provides help to a customer on their journey to Cloud Native:

1. Cloud Management Gateway [5].
2. Co-Management [4].
3. Tenant Attach [9].

To be clear, none of the above options will solve the application challenges and fully remove the reliance on Configuration Manager for those organizations with complex application estates.

The Business Value

There are many benefits for an organization to achieve Cloud Native for Windows Endpoint Management:

- Cost savings across hosting and running a Configuration Manager Infrastructure.
- Operational efficiencies by unifying endpoint management within a single portal.
- Security improvements by having better RBAC and MFA controls to harden access to a Cloud Management portal.
- End user experience improvements and efficiencies by providing better self-service options.

What is quite interesting is that Microsoft has funded four Forrester Total Economic Impact studies for Endpoint Management:

- TEI of Intune Suite [10].
- TEI of Microsoft Endpoint Management [11].
- TEI of Modernizing Endpoints [12].
- TEI of Microsoft Managed Desktop [13].

You can also include the TEI for Microsoft 365 E3, as that also covers Endpoint Management data points [14].

The challenge for me with the above studies is that they all assume that an organization will be using the combination of both Microsoft Intune and Configuration Manager to manage the Windows estate, rather than showing the value of the organization decommissioning the Configuration Manager infrastructure. One could assume there is a political reason for this, with Microsoft not wanting to show any signs that they would be deprecating Configuration Manager – based on previous fallout when many in the EUC industry felt Microsoft was headed in this direction, which led to many “ConfigMgr is not dead” posts from Product Managers.

Microsoft Managed Desktop (MMD) was the closest Microsoft came to pushing customers towards Cloud Native. The biggest challenge for customers looking to adopt MMD and for Microsoft selling MMD was migrating the complex applications to Intune. Whilst this approach was ok for a subset of users who perhaps only used Office and some SaaS apps to do their job, it was not enough to make it a wall-to-wall proposition that many folks in field roles needed it to be to hit aggressive sales targets. Eventually Microsoft conceded and supported co-management with MMD, but ultimately it was too late to save MMD which is now back at the engineering drawing board, and what remains in its place is Windows Autopatch [15].

Based on the above though, we can look at the TEI of MMD [13] to review the quantified benefits of migrating to Cloud Native, based on 5,000 user devices:

- Savings of $4.2 million by consolidating endpoint management and security infrastructure.
- Fifty percent fewer IT FTE hours required to maintain IT infrastructure.
- Ninety percent less time required to set up end users.
- Thirty-five percent reduction in help desk calls related to device issues.
- Savings of over $313,000 in time required to provision and deploy user devices.

Going one level down, the study [13] made the following cost assumptions:

- On average, $30 per user per year in license and infrastructure costs for endpoint management and security infrastructure.
- In the previous environment, two FTEs maintained the platform. In the new environment, one FTE is needed, resulting in a savings of one FTE ($130,000 annually).

The actual CapEx and OpEx savings to fully decommission Configuration Manager will vary for each organization, and Microsoft has not commissioned a study to perform this actual comparison. However, for an organization that owns and manages this infrastructure, clients will see significant benefits proportional to the size and complexity of the estate, and savings can be made against CapEx depreciation on the hardware hosting the infrastructure and OpEx for the ongoing support and maintenance of the environment.

Organizations should consider the costs of migrating the application estate to Microsoft Intune. These costs are traditionally driven by lengthy people heavy project services that will potentially outstrip the cost savings achieved by decommissioning a Configuration Manager infrastructure. Therefore, customers should be considering automated and AI powered approaches to migrating their complex application estates to Microsoft Intune, thus reducing the project timeframes and the spend on costly FTE hours.

In addition to the business benefits, the tangible technical goals that can be achieved through a Cloud Native Windows estate are as follows [1]:

- The ability to ship devices directly to the end user.
- Automatically configure applications and settings on devices using an internet connection.
- The ability for end users to reset their devices and redeploy applications without losing data.
- Allow your end users to be productive from anywhere, while protecting and securing user and organization data.

Configuration Manager to Microsoft Intune

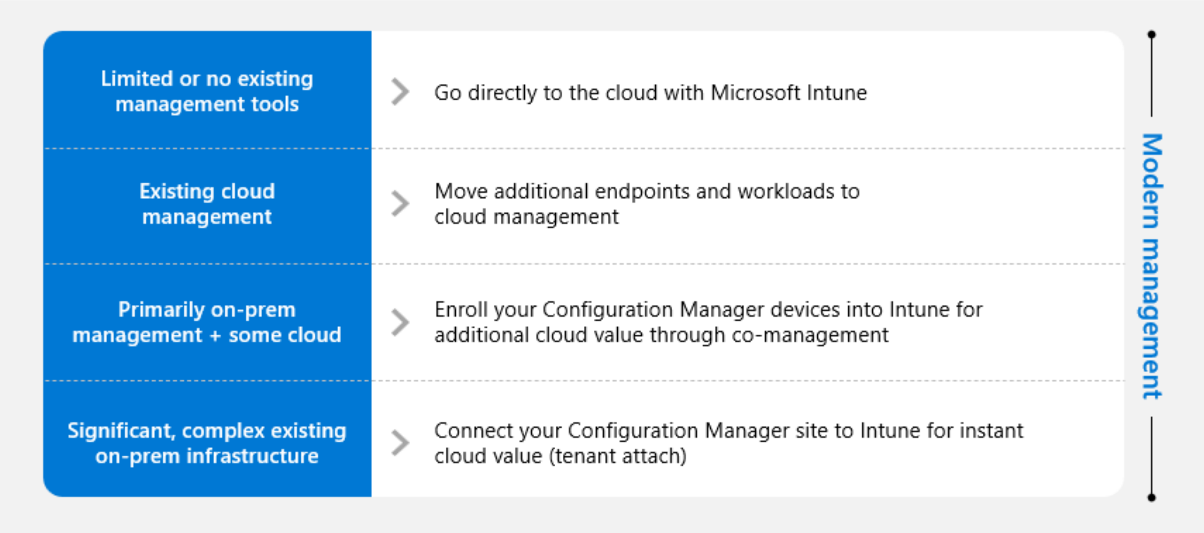
One key element of migrating to Cloud Native is the Cloud Identity. This whitepaper is focused on the Windows Endpoint; however, any organization looking at this move must consider that Cloud Identity with Azure Active Directory is a key prerequisite to achieving Cloud Native [16].

There is no prescribed ordering of activities on the journey to achieving Cloud Native. For example, the paths are well summarised in one of my favourite blogs by Danny Guillory (Microsoft) in his “The Big 3” blog [7]. In this blog, Danny’s preferred approach is:

1. CMG.
2. Tenant Attach.
3. Co-management.

The ordering of these should be tied to your business or operational strategic goals. To give credit to Danny’s blog; this was written during the Covid-19 period where organizations were prioritising enabling remote work. Therefore, at the time, I would agree that the CMG is a logical first step given that it would enable the remote management of Configuration Manager clients without having to enforce this traffic through the VPN.

Microsoft themselves recommend an approach based on the current environment, as per Figure 4, taken from the Microsoft Endpoint Management and Security Build Intent Workshop content.

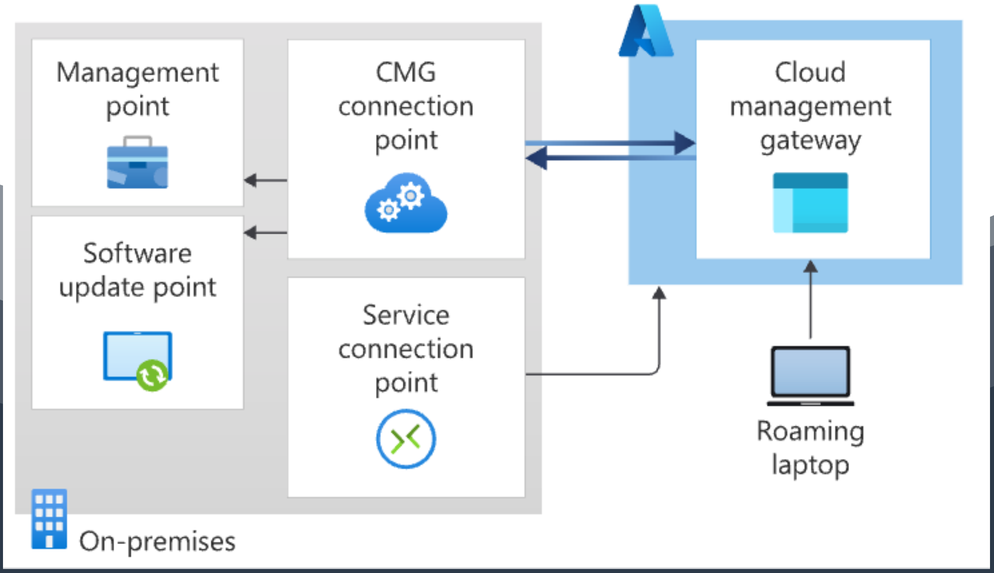


Limited or no existing management tools	Go directly to the cloud with Microsoft Intune
Existing cloud management	Move additional endpoints and workloads to cloud management
Primarily on-prem management + some cloud	Enroll your Configuration Manager devices into Intune for additional cloud value through co-management
Significant, complex existing on-prem infrastructure	Connect your Configuration Manager site to Intune for instant cloud value (tenant attach)

Modern management

CMG

The CMG provides a simple way to manage Configuration Manager clients over the internet. You deploy the CMG as a cloud service in Microsoft Azure. Then, without more on-premises infrastructure, you can manage clients that roam on the internet or are in branch offices across the WAN. You also don’t need to expose your on-premises infrastructure to the internet [17].



By deploying the CMG, you can extend the reach of Configuration Manager without the additional cost of extending the physical infrastructure. If you optionally choose to leverage the CMG as a Cloud Distribution Point for your applications, you will need to consider the storage and data egress charges that will apply against the Azure Resource.

You can also deploy internet facing Azure AD joined devices using Windows Autopilot and bootstrap the Configuration Manager Client to be able to co-manage the devices [18]. If access to on-premises resources is still required, then this can still be achieved without the need for a hybrid joining the device [19].

Tenant Attach

I will start by explaining what tenant attach entails and what it enables. Tenant attach is the process of connecting your Configuration Manager environment directly to Microsoft Intune. The process is fully focused on the infrastructure and does not affect or make any changes to the Windows Endpoints themselves. I feel it’s always important to be clear on that point.

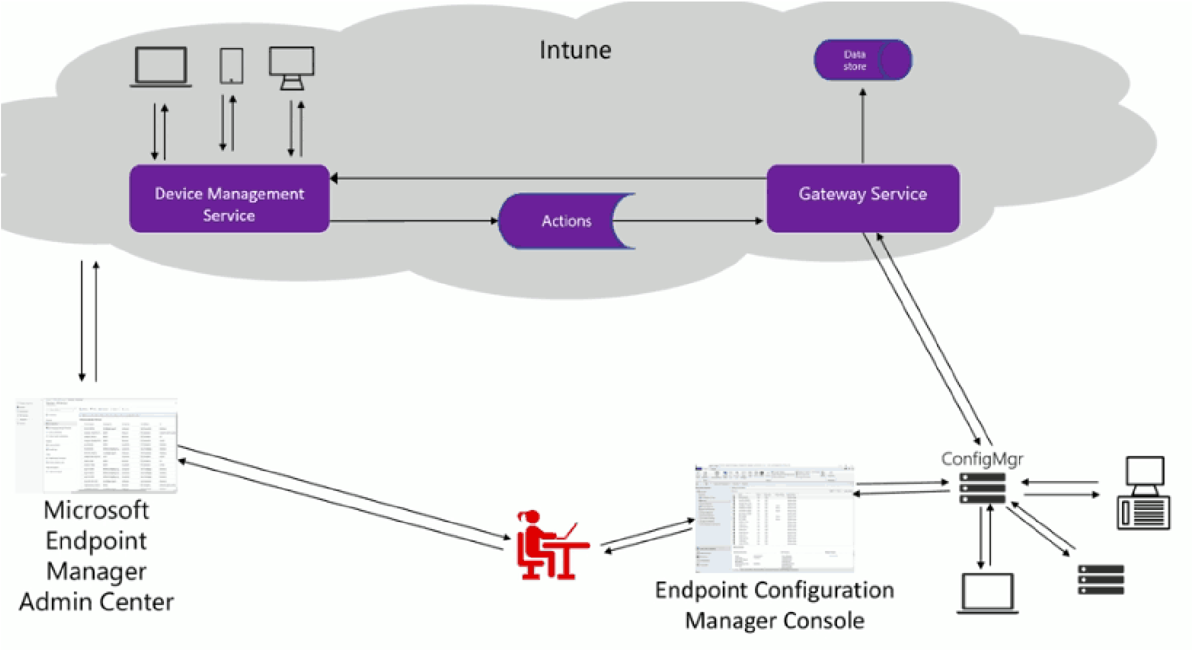
The process is triggered from within the Configuration Manager Admin Console and requires a Global Administrator when preforming the initial setup, this is mainly required because the onboarding creates a third-party app and a first-party service principal in the Azure AD tenant. Further prerequisites can be found here [20].

Once enabled, Tenant attempts to transform Microsoft Intune into the main console in the Cloud for managing Windows Endpoints. The architecture allows the Configuration Manager site to synchronize data about the device and the user to Microsoft Intune. Organizations can then query and present data from an on-premises environment, in Microsoft Intune, in real time, without active synchronization. Therefore, this does entail additional data collection from Microsoft and requires reviewing prior to enabling [21].

In terms of the features that tenant attach enables for Configuration Manager devices via Intune, some of these include:

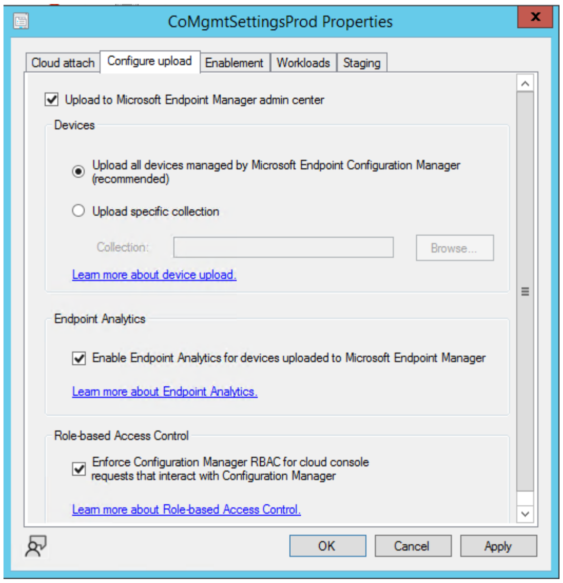
Run PowerShell scripts.

- Install applications.
- Query devices with CMPivot.
- Display a timeline of events from a device.
- Read the Bitlocker Recovery Key.
- View the status of Software Updates.
- Endpoint Security Policies.


Intune
Data store
Device Management Service
Actions
Gateway Service
Microsoft Endpoint Manager Admin Center
ConfigMgr
Endpoint Configuration Manager Console

Another key feature of tenant attach is the ability to enroll Configuration Manager devices into Endpoint Analytics. Thus, having visibility of the type of insights you would typically receive for your Cloud Managed devices, such as:

- Startup performance.
- Restart frequency.
- Application reliability.



☑ Upload to Microsoft Endpoint Manager admin center

Devices

● Upload all devices managed by Microsoft Endpoint Configuration Manager (recommended)

○ Upload specific collection

Collection:

Learn more about device upload.

Endpoint Analytics

☑ Enable Endpoint Analytics for devices uploaded to Microsoft Endpoint Manager

Learn more about Endpoint Analytics.

Role-based Access Control

☑ Enforce Configuration Manager RBAC for cloud console requests that interact with Configuration Manager

Learn more about Role-based Access Control.

Therefore, tenant attach can provide some immediate value for those organizations with limited Microsoft Intune management of their Windows Endpoints, and a great starting point on the journey to Cloud Native. The challenge for organizations in this scenario will be accepting the additional data collection required by Microsoft; however, this is a concept that comes hand in hand when moving to Cloud Native and organizations will need to accept and overcome.

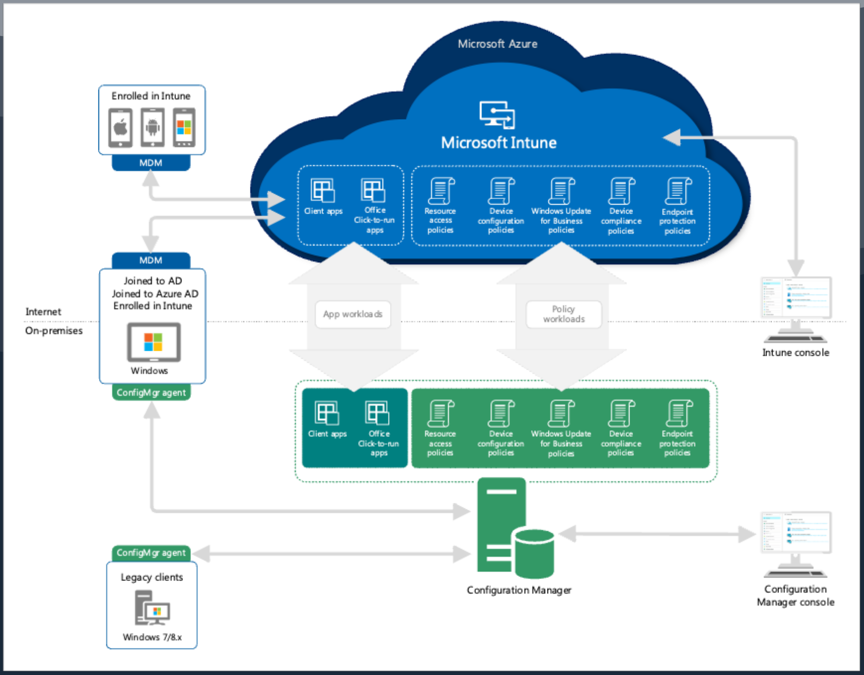
Co-Management

Organizations that are serious about getting to Cloud Native will likely be either considering co-management or have it enabled in their environment.

We need to be clear that we are not confusing co-management with co-existence. Co-existence is a term used when an organization manages devices with Configuration Manager and a third-party MDM service and comes with its own set of challenges [22].

Co-management requires the enrolment of Windows Endpoints into Intune, and these endpoints can be either Azure AD Joined or Hybrid Azure AD Joined. Azure AD Joined devices will typically be your new devices that are internet facing and deployed via Windows Autopilot, whilst Hybrid Azure AD Joined devices will cater for existing devices being enrolled into Intune.

In co-management, Configuration Manager is still the management authority for all workloads until being switched to workloads over to Microsoft Intune. This is the main advantage to co-management; it allows organizations to switch workloads over to Intune at their own pace. Also, as these devices are enrolled in Intune, a device administrator can perform device actions from within the Intune administration portal.

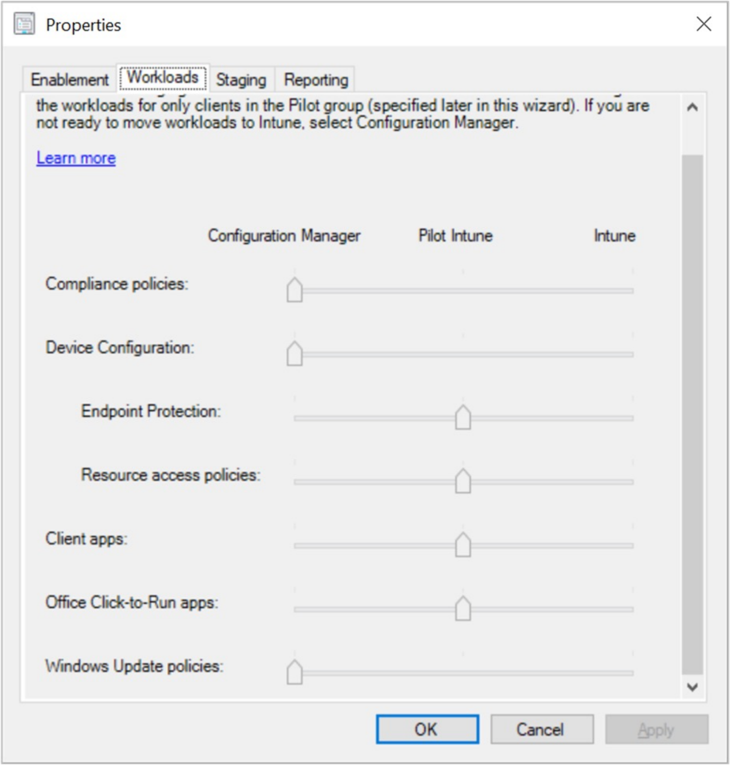


In terms of immediate value that organizations can gain from enabling co-management [23]:

- Conditional Access with device compliance.
- Intune-based remote actions, e.g., restart, remote control, or factory reset.
- Centralised visibility of device health.
- Link users, devices, and apps with Azure AD.
- Modern provisioning with Windows Autopilot.
- Remote Actions.

Co-management supports the following workloads and provides organizations with the ability to switch them individually over to Intune to manage [24]:

- Compliance policies.
- Windows Update policies.
- Resource access policies.
- Endpoint protection.
- Device configuration.
- Office Click-to-Run apps.
- Client apps.



the workloads for only clients in the Pilot group (specified later in this wizard). If you are not ready to move workloads to Intune, select Configuration Manager.

Learn more

	Configuration Manager	Pilot Intune	Intune
Compliance policies:	●		
Device Configuration:	●		
Endpoint Protection:		●	
Resource access policies:		●	
Client apps:		●	
Office Click-to-Run apps:		●	
Windows Update policies:	●		

Compliance Policies

Compliance policies define the rules and settings that a device must comply with to be considered compliant by conditional access policies. Also, compliance policies are used to monitor and remediate compliance issues with devices independently of conditional access. You can add an evaluation of custom configuration baselines as a compliance policy assessment rule.

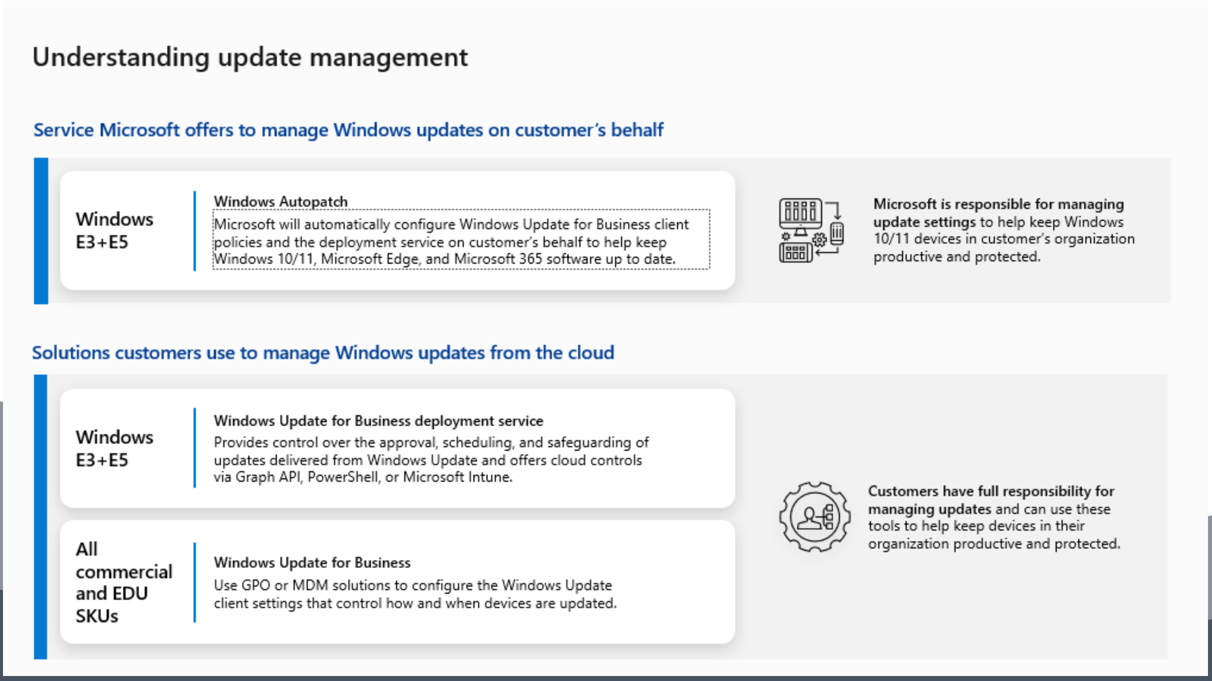
Compliance policies for devices are strategically tied to a Zero Trust strategy. When it comes to Zero Trust, device signals are important to verify that an end user is attempting to access a resource from a trusted endpoint. What a trusted endpoint is defined as will vary for each organization and compliance policies allow organizations to apply this definition.

From my experience this is typically the first workload that an organization will shift to Intune. This is normally down to the fact that an organization will have Cloud Identity in place and be using Conditional Access to manage access to corporate Cloud Resources, so device compliance is the logical first step to enrich this solution.

Windows Update Policies

Windows Update for Business (WUfB) allows an organization to configure and deploy Windows Update policies via Intune. These policies can consist of update deferral policies for Windows monthly updates and/or Windows Feature updates and are typically defined by update rings with increasing deferral time frames.

Organizations can also leverage Windows Autopatch [15] by shifting the Windows Update policies workload over to Intune.



Understanding update management

Service Microsoft offers to manage Windows updates on customer's behalf

Windows E3+E5

Windows Autopatch

Microsoft will automatically configure Windows Update for Business client policies and the deployment service on customer's behalf to help keep Windows 10/11, Microsoft Edge, and Microsoft 365 software up to date.

Microsoft is responsible for managing update settings to help keep Windows 10/11 devices in customer's organization productive and protected.

Solutions customers use to manage Windows updates from the cloud

Windows E3+E5

Windows Update for Business deployment service

Provides control over the approval, scheduling, and safeguarding of updates delivered from Windows Update and offers cloud controls via Graph API, PowerShell, or Microsoft Intune.

All commercial and EDU SKUs

Windows Update for Business

Use GPO or MDM solutions to configure the Windows Update client settings that control how and when devices are updated.

Customers have full responsibility for managing updates and can use these tools to help keep devices in their organization productive and protected.

Resource Access Policies

Resource access policies configure VPN, Wi-Fi, email, and certificate settings on devices.

Please note, these policies in Configuration Manager are being deprecated and will no longer be tested and supported from version 2203 [25]. Therefore, it is now recommended to use Microsoft Intune to deploy resource access profiles and starting in version 2211 this slider will be disabled.

Endpoint Protection

The Endpoint Protection workload includes the Defender suite of protection features, and I highly recommend configuring and deploying these policies, alongside Windows Security Baseline, with Microsoft Intune. The following protection features are included:

- Microsoft Defender Antivirus.
- Microsoft Defender Application Guard.
- Microsoft Defender SmartScreen.
- Microsoft Defender for Endpoint.
- Windows Defender Firewall.
- Windows Encryption (also known as BitLocker).
- Windows Defender Exploit Guard.
- Windows Defender Application Control.
- Windows Defender Security Centre.

Microsoft notes that they have built in protections during a transition of this workload from Configuration Manager to Intune. When an organization switches this workload, the Configuration Manager policies stay on the device until the Intune policies overwrite them. This behaviour ensures that the device still has protection policies during the transition [26].

Device Configuration

The device configuration workload includes settings that you manage for devices in your organization. This slider also acts as a master slider for the Resource Access and Endpoint Protection workloads, so essentially when this slider is moved over to Intune, these sliders are moved over also.

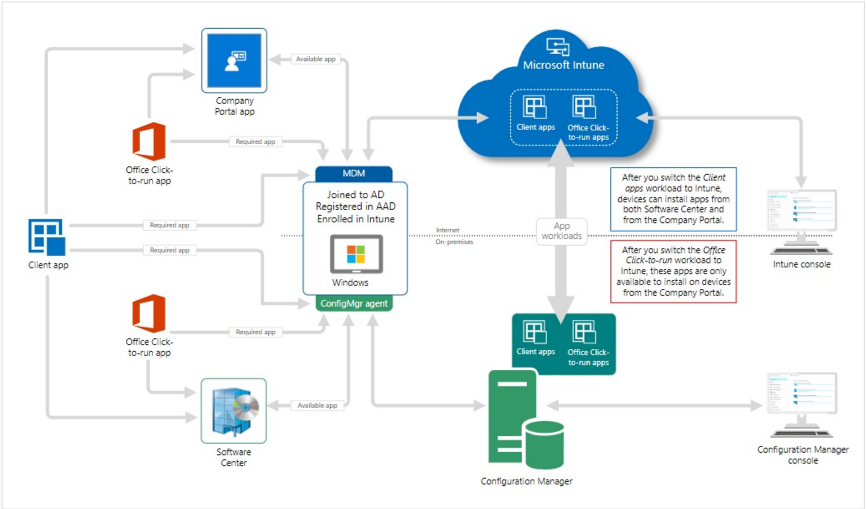
This workload includes the device configuration profiles with settings catalog that are configured and deployed with Intune. If there are gaps between what is not available in Intune when compared to Configuration Manager there is an option to cater for this by specifying an exception on a Configuration Manager configuration baseline.

Office Click-to-Run apps

This workload manages Microsoft 365 Apps on co-managed devices. After moving this workload, Microsoft 365 apps assigned from Microsoft Intune will show up in the Company Portal on the device.

Client apps

This workload can be misleading in terms of assuming this will ensure that apps are only deployed via Intune when the slider is shifted to Intune. What happens is that the Company Portal will now show both the apps delivered via Intune and the apps delivered via Configuration Manager. Therefore, it provides a single destination for a user to find and install their assigned apps, rather than having to go to both the Company Portal and Software Centre.



After you switch the *Client apps* workload to Intune, devices can install apps from both Software Center and from the Company Portal.

After you switch the *Office Click-to-run* workload to Intune, these apps are only available to install on devices from the Company Portal.

Summary

In this section we have covered the various routes that Microsoft has made available to organizations when moving from Configuration Manager to Microsoft Intune. We only discussed the tooling and mechanisms available to transition, rather than going further into the deeper steps required when looking at a migration away from Group Policy to Intune Settings Catalog as an example.

What is missing from this migration path is how an organization can migrate their application estate from Configuration Manager to Microsoft Intune. Many organizations have spent a large amount of time and effort building logic and intelligence into their Configuration Manager applications; modernizing these applications and migrating into Intune is far from a trivial task.

In the next section we look at how Rimo3 can solve the application problem for organizations.

Solving the Application Problem with Rimo3

Rimo3 offers a comprehensive, cloud hosted solution for modernizing and maintaining your Windows™ application estate, from migration to ongoing maintenance. The Rimo3 platform automates the entire modernization process, eliminating the need for scripting or complex configuration. It integrates with industry-leading solutions and uses your unique infrastructure configuration for testing, modernization, and migration.

Rimo3 Cloud platform is an intelligent and scalable solution that automates packaging, testing, modernization, and migration of Windows applications to modern environments. It simplifies migrations and day-to-day workspace maintenance [27].

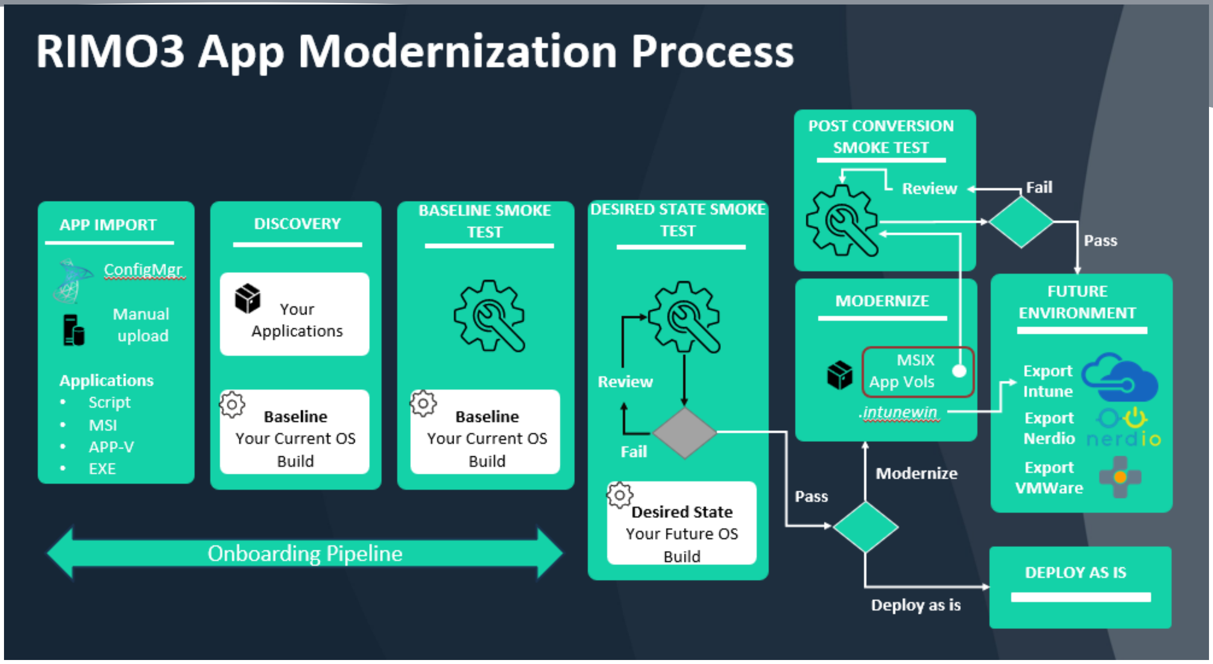
Import, Discover, Test, Conversion, and Export

Rimo3 automatically imports enterprise metadata from storage repositories like Configuration Manager, eliminating the need for custom scripting and manual package transfers. After import, applications are discovered and analyzed for their suitability for migration and capturing package customizations.

Automated testing determines application readiness against custom images, and detailed reports highlighting the readiness for Windows 10 and Windows 11 target images.

Rimo3 then automates the testing phase to determine application suitability for modern package formats like MSIX and VMware App Volumes and automatically converts applications to modern formats. Applications suitable for modern package formats are automatically captured and converted using best practices and vendor-supported tooling.

The Rimo3 platform also automatically retests the newly created packages against the target environment. To complete the migration process, Rimo3 facilitates automatic export of the entire application estate to modern management planes like Microsoft Intune and Nerdio Manager for Enterprise [28], enabling efficient management of modern workspaces.



RIMO3 App Modernization Process

APP IMPORT

ConfigMgr

Manual upload

Applications
- Script
- MSI
- APP-V
- EXE

DISCOVERY

Your Applications

Baseline
Your Current OS Build

BASELINE SMOKE TEST

Baseline
Your Current OS Build

DESIRED STATE SMOKE TEST

Review

Fail

Desired State
Your Future OS Build

POST CONVERSION SMOKE TEST

Review

Fail

Pass

MODERNIZE

MSIX
App Vols

.intunewin

Modernize

Pass

FUTURE ENVIRONMENT

Export Intune

Export Nerdio

Export VMWare

DEPLOY AS IS

Deploy as is

Onboarding Pipeline

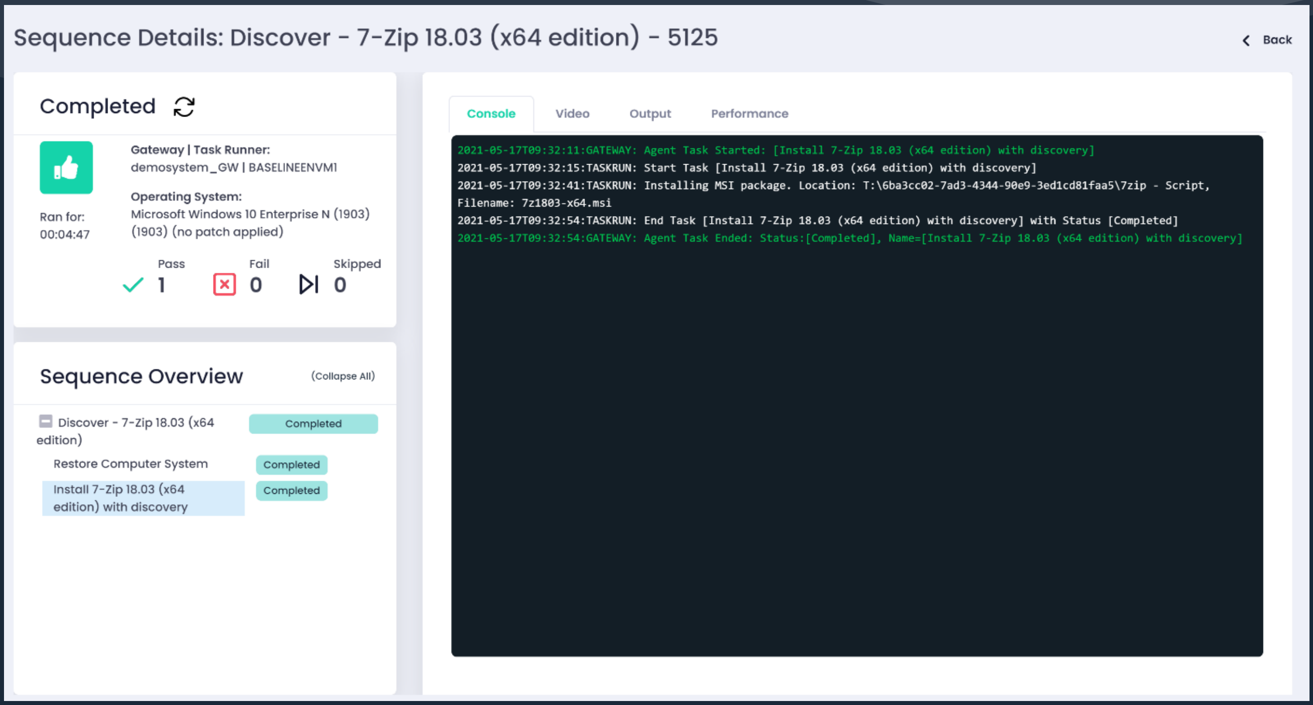
Rimo3 Discovery

Rimo3 allows the importing of existing packages and applications configured as silent installs from Microsoft Configuration Manager into its Cloud based environment.

Rimo3 will then perform an in-depth automated Discovery process on the applications to identify the application behaviors and all elements that are laid down to the Operating System when the application is installed.

An activity run as part of onboarding applications to automatically identify application executables and determine which should be tested as part of the Intelligent Smoke Test. The Rimo3 Discovery process is automatically executed during the out of the box Microsoft Configuration Manager import integration.

The Rimo3 automated discovery process will ingest the packages from Microsoft Configuration Manager and go through an automated process of installing them on a Rimo3 Task Runner against your current Operating System image to enable us to gather the package intelligence.



Sequence Details: Discover - 7-Zip 18.03 (x64 edition) - 5125

Completed

Gateway | Task Runner: demosystem_GW | BASELINEENVM1

Operating System: Microsoft Windows 10 Enterprise N (1903) (1903) (no patch applied)

Ran for: 00:04:47

Pass ✓ 1 | Fail ☒ 0 | Skipped 0

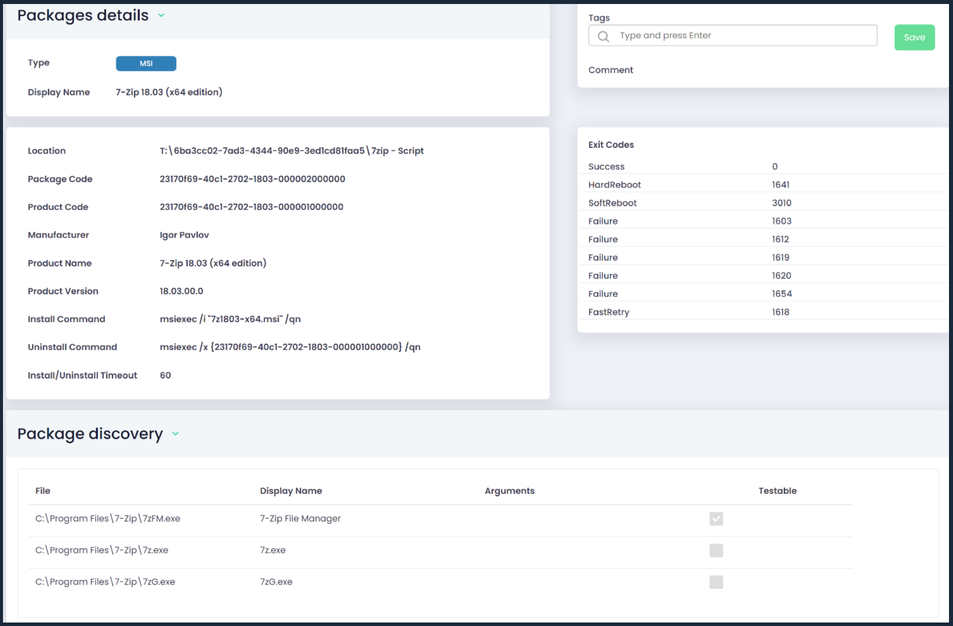
```
2021-05-17T09:32:11:GATEWAY: Agent Task Started: [Install 7-Zip 18.03 (x64 edition) with discovery]
2021-05-17T09:32:15:TASKRUN: Start Task [Install 7-Zip 18.03 (x64 edition) with discovery]
2021-05-17T09:32:41:TASKRUN: Installing MSI package. Location: T:\6ba3cc02-7ad3-4344-90e9-3ed1cd81faa5\7zip - Script,
Filename: 7z1803-x64.msi
2021-05-17T09:32:54:TASKRUN: End Task [Install 7-Zip 18.03 (x64 edition) with discovery] with Status [Completed]
2021-05-17T09:32:54:GATEWAY: Agent Task Ended: Status:[Completed], Name=[Install 7-Zip 18.03 (x64 edition) with discovery]
```

Sequence Overview

Discover - 7-Zip 18.03 (x64 edition)	Completed
Restore Computer System	Completed
Install 7-Zip 18.03 (x64 edition) with discovery	Completed

Discovery data results

The Rimo3 Discovery Process will identify all the key components of the packages, including the package installation/uninstallation behavior. Rimo3 then uses this intelligence to feed the Intelligent Smoke Test process.



Packages details

Type	MSI
Display Name	7-Zip 18.03 (x64 edition)

Location	T:\6ba3cc02-7ad3-4344-90e9-3ed1cd81faa5\7zip - Script
Package Code	23170f69-40c1-2702-1803-000002000000
Product Code	23170f69-40c1-2702-1803-000001000000
Manufacturer	Igor Pavlov
Product Name	7-Zip 18.03 (x64 edition)
Product Version	18.03.00.0
Install Command	msiexec /i "7z1803-x64.msi" /qn
Uninstall Command	msiexec /x {23170f69-40c1-2702-1803-000001000000} /qn
Install/Uninstall Timeout	60

Exit Codes

Success	0
HardReboot	1641
SoftReboot	3010
Failure	1603
Failure	1612
Failure	1619
Failure	1620
Failure	1654
FastRetry	1618

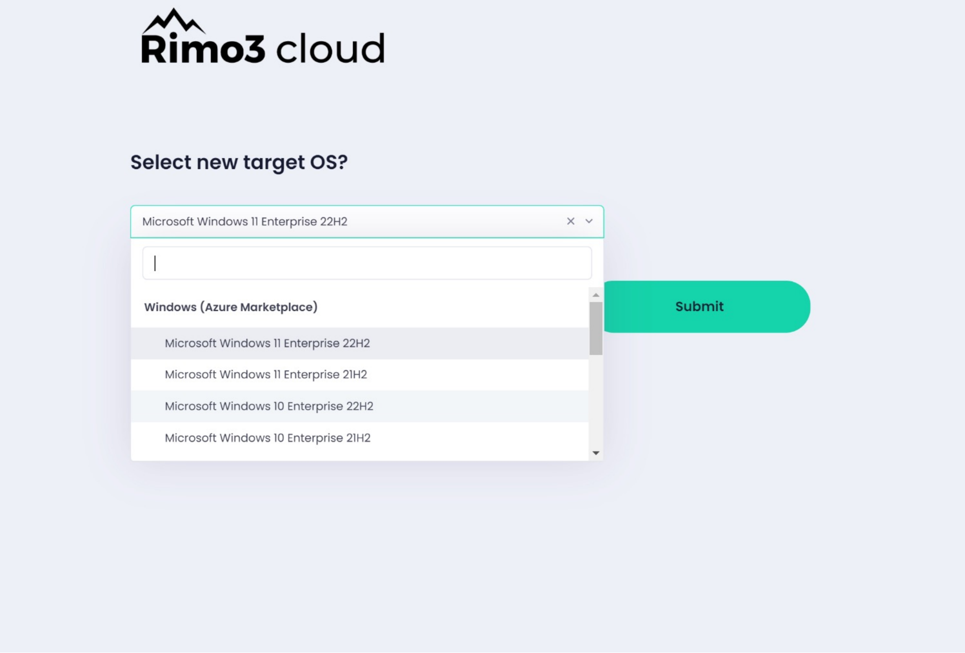
Package discovery

File	Display Name	Arguments	Testable
C:\Program Files\7-Zip\7zFM.exe	7-Zip File Manager		☑
C:\Program Files\7-Zip\7z.exe	7z.exe		□
C:\Program Files\7-Zip\7zG.exe	7zG.exe		□

Custom Operating System Image Support (Azure)

Custom OS Image Support enables custom images to be used for testing in Rimo3 Cloud tenants that have been linked to a customer's Azure Subscription. The feature allows organizations to configure additional Operating Systems that reference Managed Images in Azure to be used when provisioning Task Runners. Customer images can include core applications and dependencies such as Office and C++ Runtimes that other applications may depend on.

Rimo3 also supports Microsoft Azure Marketplace Image Gallery for ease of use. However, the use of a custom image is preferred as it will represent the environment to provide contextual relevance when testing applications.



Rimo3 cloud

Select new target OS?

Microsoft Windows 11 Enterprise 22H2

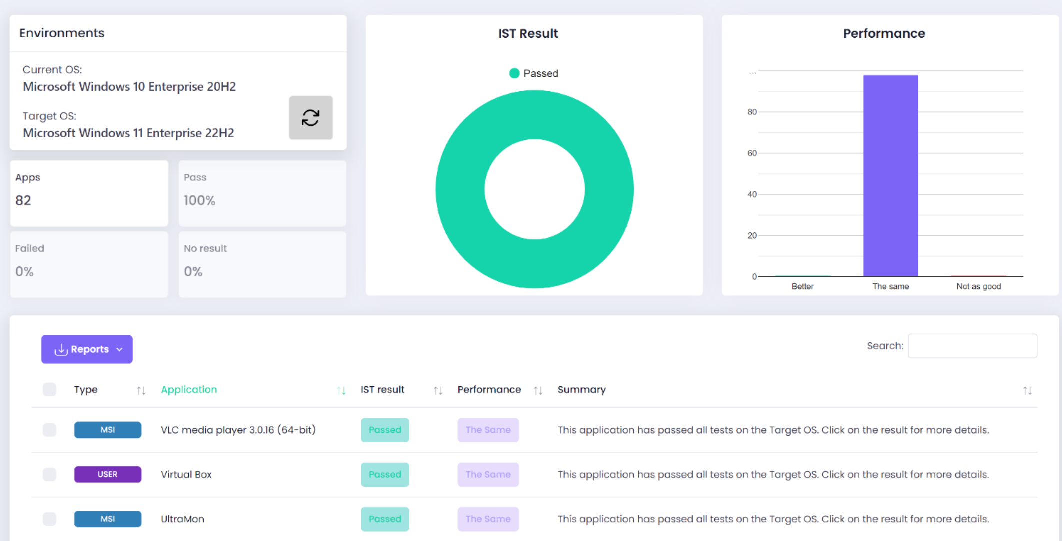
Windows (Azure Marketplace)

- Microsoft Windows 11 Enterprise 22H2
- Microsoft Windows 11 Enterprise 21H2
- Microsoft Windows 10 Enterprise 22H2
- Microsoft Windows 10 Enterprise 21H2

Rimo3 Intelligent Smoke Test

The Intelligent Smoke Test is Rimo3's revolutionary automated testing capability; designed to test any application for compatibility with Windows without requiring a predefined script or needing to know what the application is or does. The entire Intelligent smoke test is 100% unattended.

Rimo3's Intelligent Smoke Test dashboard will provide documental proof that the package installs and runs successfully in the desired environment. For applications that fail the process, the Rimo3 platform provides detailed log files, video, and screenshot evidence to support remediation.



Environments

Current OS:
Microsoft Windows 10 Enterprise 20H2

Target OS:
Microsoft Windows 11 Enterprise 22H2

Apps: 82
Pass: 100%
Failed: 0%
No result: 0%

	Type	Application	IST result	Performance	Summary
□	MSI	VLC media player 3.0.16 (64-bit)	Passed	The Same	This application has passed all tests on the Target OS. Click on the result for more details.
□	USER	Virtual Box	Passed	The Same	This application has passed all tests on the Target OS. Click on the result for more details.
□	MSI	UltraMon	Passed	The Same	This application has passed all tests on the Target OS. Click on the result for more details.

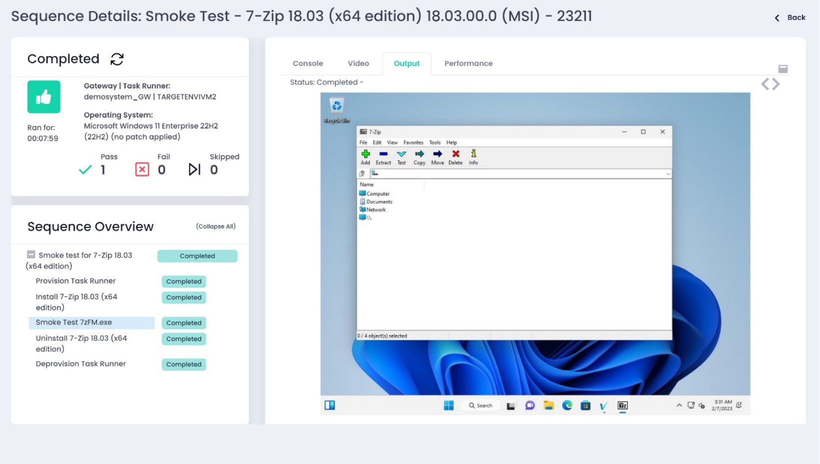
Unattended Intelligent Smoke Test Automated Sequence

The Rimo3 platform automates the provisioning of a Task Runner Virtual Machine (VM), that is running the customers Operating System Image.

The application is then installed and the Rimo3 platform then runs our Patented Intelligent Smoke Test process to run the application and monitor for any errors. During this time, we capture video of the full process and where necessary, take screenshots.

In addition, we also log performance counters to measure impact on the task runner VM.

Finally, Rimo3 confirms the uninstall behavior and deprovisions the Task Runner.



Sequence Details: Smoke Test - 7-Zip 18.03 (x64 edition) 18.03.00.0 (MSI) - 23211

Completed

Gateway | Task Runner: demosystem_GW | TARGETENVIVM2

Operating System: Microsoft Windows 11 Enterprise 22H2 (22H2) (no patch applied)

Ran for: 00:07:59

Pass	Fail	Skipped
1	0	0

Sequence Overview

Smoke test for 7-Zip 18.03 (x64 edition)	Completed
Provision Task Runner	Completed
Install 7-Zip 18.03 (x64 edition)	Completed
Smoke Test 7zFM.exe	Completed
Uninstall 7-Zip 18.03 (x64 edition)	Completed
Deprovision Task Runner	Completed

Status: Completed -

Rimo3 Multi-session Intelligent Smoke Test

Building on the existing Intelligent Smoke Test (IST) the Multi-session smoke test launches applications concurrently in different user sessions on a multi-session capable version of Windows to provide the same revolutionary insights into the application's behaviour in each session as the existing IST.

Rimo3 Automated Modern Packaging

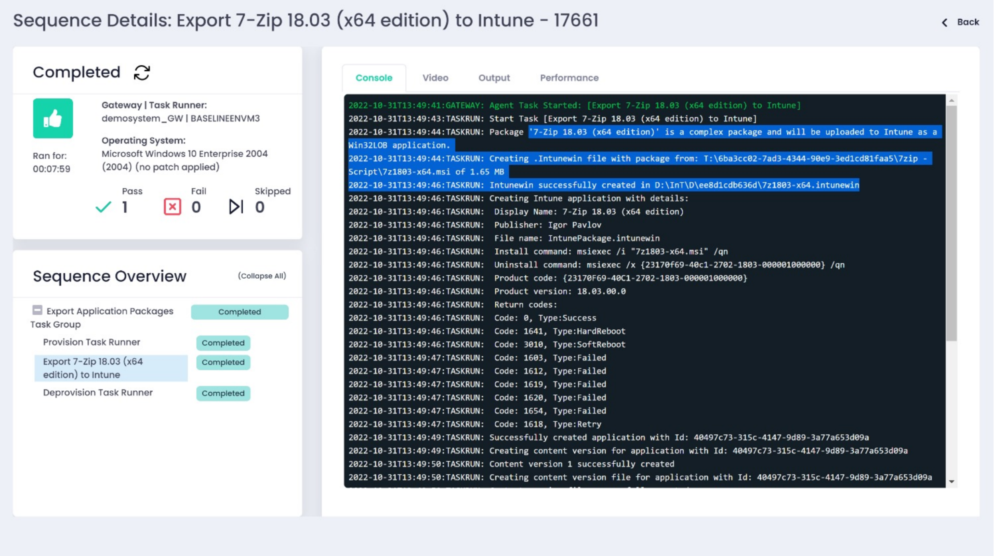
Rimo3 supports unattended packaging for the following application package types:

- Microsoft MSIX (includes global trusted root certificate as part of conversion)
- VMware App Volumes
- Microsoft Intune
    - Windows Universal line-of-business apps (MSIX).
    - MSI line-of-business apps [28] [29].
    - Windows app (Win32) (.intunewin format).

Rimo3 automated Intune export

The Rimo3 platform enables the export of applications directly into Intune.

Successfully exported applications will land in the Intune applications blade and will be in a state that is ready to be assigned.



Sequence Details: Export 7-Zip 18.03 (x64 edition) to Intune - 17661

Completed

Gateway | Task Runner: demosystem_GW | BASELINEENVM3

Operating System: Microsoft Windows 10 Enterprise 2004 (2004) (no patch applied)

Ran for: 00:07:59

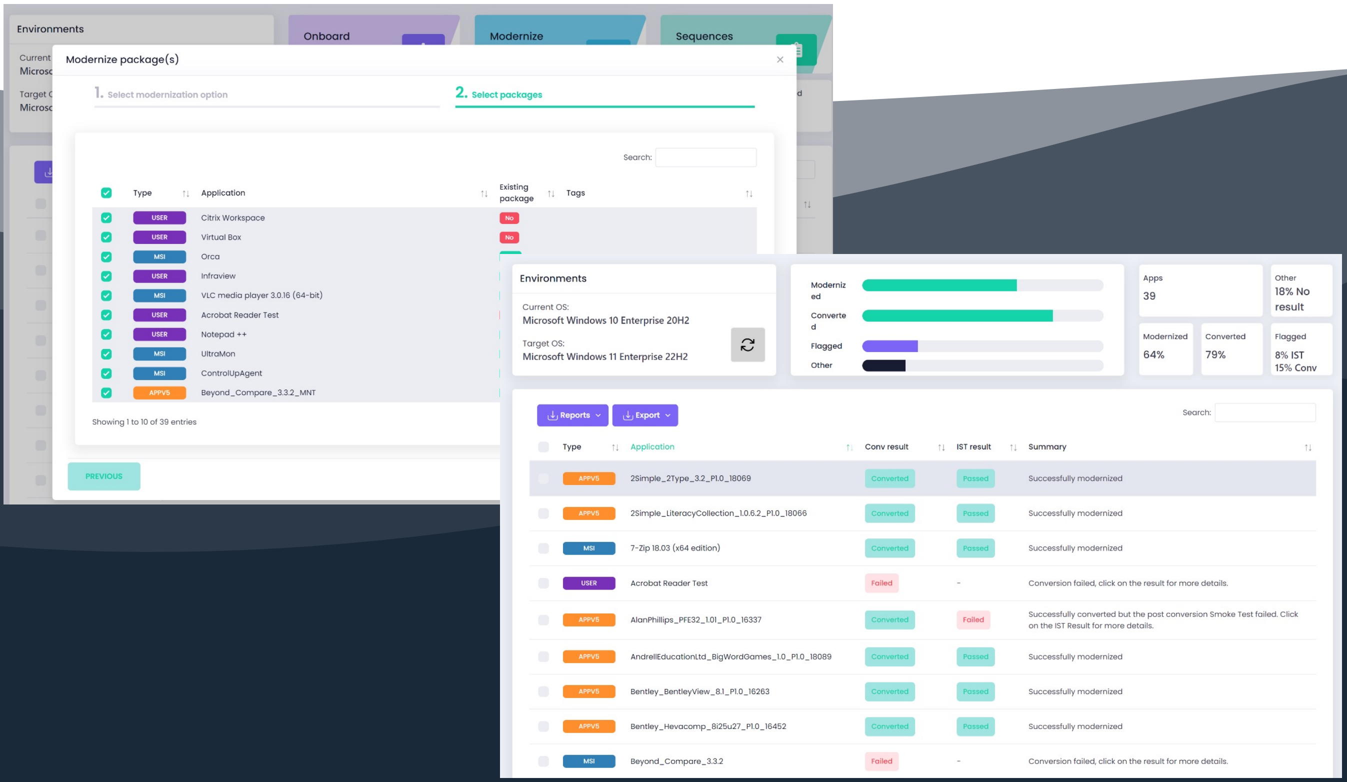
Pass	Fail	Skipped
✓ 1	☒ 0	0

Sequence Overview

Export Application Packages Task Group	Completed
Provision Task Runner	Completed
Export 7-Zip 18.03 (x64 edition) to Intune	Completed
Deprovision Task Runner	Completed

```
2022-10-31T13:49:41:GATEWAY: Agent Task Started: [Export 7-Zip 18.03 (x64 edition) to Intune]
2022-10-31T13:49:43:TASKRUN: Start Task [Export 7-Zip 18.03 (x64 edition) to Intune]
2022-10-31T13:49:44:TASKRUN: Package '7-Zip 18.03 (x64 edition)' is a complex package and will be uploaded to Intune as a
Win32LOB application.
2022-10-31T13:49:44:TASKRUN: Creating .Intunewin file with package from: T:\6ba3cc02-7ad3-4344-90e9-3ed1cd81faa5\7zip -
Script\7z1803-x64.msi of 1.65 MB
2022-10-31T13:49:46:TASKRUN: Intunewin successfully created in D:\InT\D\ee8d1cdb636d\7z1803-x64.intunewin
2022-10-31T13:49:46:TASKRUN: Creating Intune application with details:
2022-10-31T13:49:46:TASKRUN:  Display Name: 7-Zip 18.03 (x64 edition)
2022-10-31T13:49:46:TASKRUN:  Publisher: Igor Pavlov
2022-10-31T13:49:46:TASKRUN:  File name: IntunePackage.intunewin
2022-10-31T13:49:46:TASKRUN:  Install command: msiexec /i "7z1803-x64.msi" /qn
2022-10-31T13:49:46:TASKRUN:  Uninstall command: msiexec /x {23170f69-40c1-2702-1803-000001000000} /qn
2022-10-31T13:49:46:TASKRUN:  Product code: {23170F69-40C1-2702-1803-000001000000}
2022-10-31T13:49:46:TASKRUN:  Product version: 18.03.00.0
2022-10-31T13:49:46:TASKRUN:  Return codes:
2022-10-31T13:49:46:TASKRUN:  Code: 0, Type:Success
2022-10-31T13:49:46:TASKRUN:  Code: 1641, Type:HardReboot
2022-10-31T13:49:46:TASKRUN:  Code: 3010, Type:SoftReboot
2022-10-31T13:49:47:TASKRUN:  Code: 1603, Type:Failed
2022-10-31T13:49:47:TASKRUN:  Code: 1612, Type:Failed
2022-10-31T13:49:47:TASKRUN:  Code: 1619, Type:Failed
2022-10-31T13:49:47:TASKRUN:  Code: 1620, Type:Failed
2022-10-31T13:49:47:TASKRUN:  Code: 1654, Type:Failed
2022-10-31T13:49:47:TASKRUN:  Code: 1618, Type:Retry
2022-10-31T13:49:49:TASKRUN: Successfully created application with Id: 40497c73-315c-4147-9d89-3a77a653d09a
2022-10-31T13:49:49:TASKRUN: Creating content version for application with Id: 40497c73-315c-4147-9d89-3a77a653d09a
2022-10-31T13:49:50:TASKRUN: Content version 1 successfully created
2022-10-31T13:49:50:TASKRUN: Creating content version file for application with Id: 40497c73-315c-4147-9d89-3a77a653d09a
```

Rimo3 automated MSIX conversion



Modernize package(s)

☑	Type	Application	Existing package	Tags
☑	USER	Citrix Workspace	No	
☑	USER	Virtual Box	No	
☑	MSI	Orca		
☑	USER	Infraview		
☑	MSI	VLC media player 3.0.16 (64-bit)		
☑	USER	Acrobat Reader Test		
☑	USER	Notepad ++		
☑	MSI	UltraMon		
☑	MSI	ControlUpAgent		
☑	APPV5	Beyond_Compare_3.3.2_MNT		

Showing 1 to 10 of 39 entries

Environments

Current OS: Microsoft Windows 10 Enterprise 20H2

Target OS: Microsoft Windows 11 Enterprise 22H2

Apps	Other
39	18% No result

Modernized	Converted	Flagged
64%	79%	8% IST 15% Conv

☐	Type	Application	Conv result	IST result	Summary
☐	APPV5	2Simple_2Type_3.2_P1.0_18069	Converted	Passed	Successfully modernized
☐	APPV5	2Simple_LiteracyCollection_1.0.6.2_P1.0_18066	Converted	Passed	Successfully modernized
☐	MSI	7-Zip 18.03 (x64 edition)	Converted	Passed	Successfully modernized
☐	USER	Acrobat Reader Test	Failed	-	Conversion failed, click on the result for more details.
☐	APPV5	AlanPhillips_PFE32_1.01_P1.0_16337	Converted	Failed	Successfully converted but the post conversion Smoke Test failed. Click on the IST Result for more details.
☐	APPV5	AndrellEducationLtd_BigWordGames_1.0_P1.0_18089	Converted	Passed	Successfully modernized
☐	APPV5	Bentley_BentleyView_8.1_P1.0_16263	Converted	Passed	Successfully modernized
☐	APPV5	Bentley_Hevacomp_8i25u27_P1.0_16452	Converted	Passed	Successfully modernized
☐	MSI	Beyond_Compare_3.3.2	Failed	-	Conversion failed, click on the result for more details.

Post Packaging Automated Intelligent Smoke Test

The post packaging Intelligent Smoke Test validates the modern package against a specified Operating Environment.

Rimo3 Integrations

- Microsoft Configuration Manager Import

  The feature will import Applications from ConfigMgr with a Deployment Type of Windows Installer (MSI), AppV5 as well as Script Installers. This process is unattended.

- Microsoft Intune Export

  Applications that have been successfully onboarded into Rimo3 can be exported to Intune with the desired package format from supported package types.

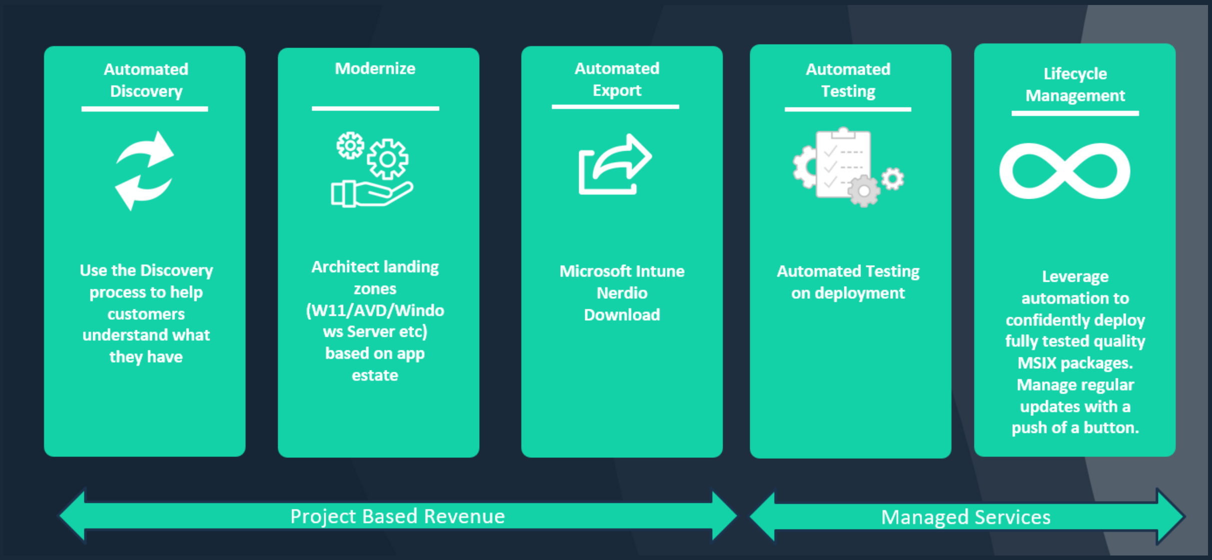
Application Export/Deployment

Finally, Rimo3 supports the export of applications, either modernized or in their existing format to:

- Microsoft Intune (.intunewin wrapped or MSIX).
- Nerdio Manager for Enterprise [28] (MSIX only).
- Local download.

Partner Opportunity

With Rimo3 Services, partners can enrich their offerings to help customers on their journey to Cloud Native for Windows Endpoints.



Automated Discovery

Use the Discovery process to help customers understand what they have

Modernize

Architect landing zones (W11/AVD/Windows Server etc) based on app estate

Automated Export

Microsoft Intune Nerdio Download

Automated Testing

Automated Testing on deployment

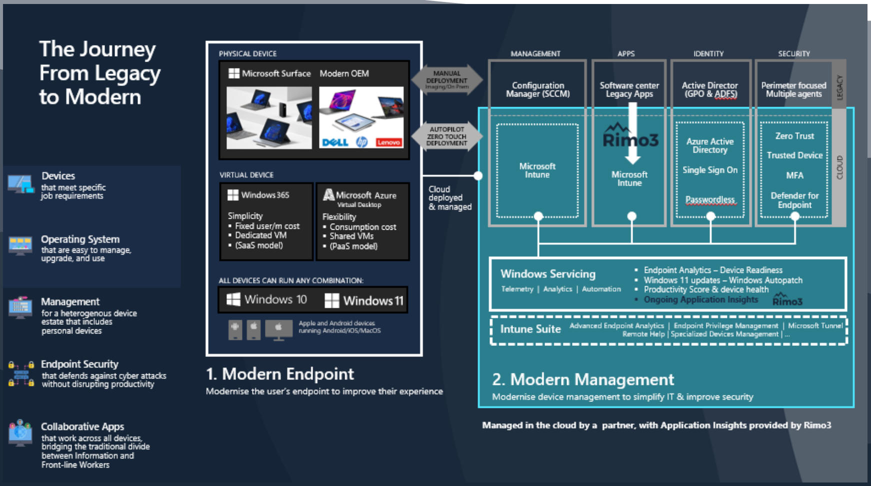
Lifecycle Management

Leverage automation to confidently deploy fully tested quality MSIX packages. Manage regular updates with a push of a button.

Project Based Revenue

Managed Services

From a Professional Services perspective, Rimo3 can support the acceleration of the migration of the applications from Configuration Manager to a Microsoft Intune. During that process, Rimo3 automates the testing of the applications against the target Operating System image, Windows 11 as an example. Services Partners can wrap around this process by providing the management of the overall transformation and the consultancy engagement to provide the expertise around the applications pre and post-migration. So rather than leaving the applications as an item, not in scope of a transformation or throwing costly bodies at the problem, a Services Partner is able to fully transform the customer to a fully Cloud Native Windows Endpoint environment.



The Journey From Legacy to Modern

Devices that meet specific job requirements

Operating System that are easy to manage, upgrade, and use

Management for a heterogenous device estate that includes personal devices

Endpoint Security that defends against cyber attacks without disrupting productivity

Collaborative Apps that work across all devices, bridging the traditional divide between Information and Front-line Workers

PHYSICAL DEVICE

Microsoft Surface | Modern OEM

VIRTUAL DEVICE

Windows 365

Simplicity
- Fixed user/m cost
- Dedicated VM
- (SaaS model)

Microsoft Azure Virtual Desktop

Flexibility
- Consumption cost
- Shared VMs
- (PaaS model)

ALL DEVICES CAN RUN ANY COMBINATION:

Windows 10 | Windows 11

Apple and Android devices running Android/iOS/MacOS

MANUAL DEPLOYMENT Imaging/On Prem

AUTOPILOT ZERO TOUCH DEPLOYMENT

Cloud deployed & managed

1. Modern Endpoint

Modernise the user's endpoint to improve their experience

MANAGEMENT	APPS	IDENTITY	SECURITY	
Configuration Manager (SCCM)	Software center Legacy Apps	Active Director (GPO & ADFS)	Perimeter focused Multiple agents	LEGACY
Microsoft Intune	Rimo3 Microsoft Intune	Azure Active Directory Single Sign On Passwordless	Zero Trust Trusted Device MFA Defender for Endpoint	CLOUD

Windows Servicing

Telemetry | Analytics | Automation

- Endpoint Analytics – Device Readiness
- Windows 11 updates – Windows Autopatch
- Productivity Score & device health
- Ongoing Application Insights Rimo3

Intune Suite Advanced Endpoint Analytics | Endpoint Privilege Management | Microsoft Tunnel Remote Help | Specialized Devices Management | ...

2. Modern Management

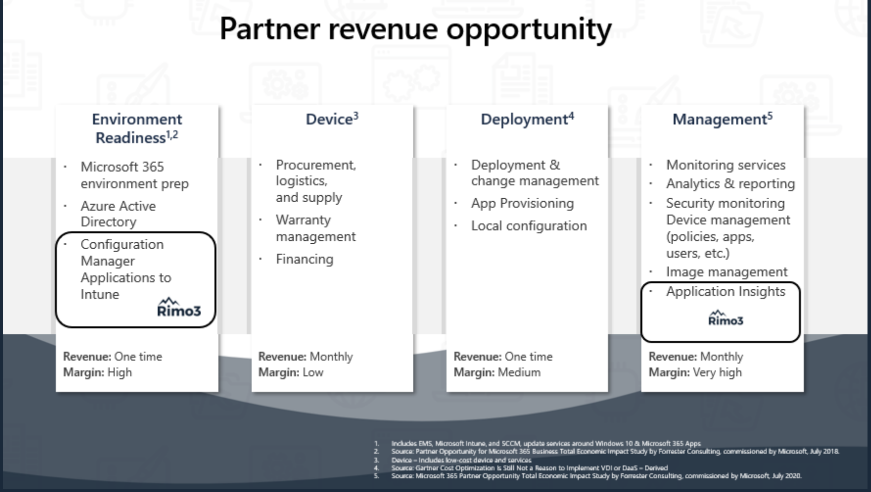
Modernise device management to simplify IT & improve security

Managed in the cloud by a partner, with Application Insights provided by Rimo3

Once the customer has gone through the transformation, they can then be onboarded to a Modern Desktop Managed Service, with a partner providing the ongoing management of elements such as:

- Device lifecycle.
- Image management.
- Intune Policy Management.
- Endpoint Security management and monitoring.
- Joiners, movers, and leavers.
- Analytics and reporting.

With Rimo3 providing the ongoing preproduction Application Insights to identify potential application outages caused by changes to the production environment.



Partner revenue opportunity

Environment Readiness[1,2]	Device[3]	Deployment[4]	Management[5]
· Microsoft 365 environment prep · Azure Active Directory · Configuration Manager Applications to Intune Rimo3	· Procurement, logistics, and supply · Warranty management · Financing	· Deployment & change management · App Provisioning · Local configuration	· Monitoring services · Analytics & reporting · Security monitoring Device management (policies, apps, users, etc.) · Image management · Application Insights Rimo3
Revenue: One time **Margin:** High	**Revenue:** Monthly **Margin:** Low	**Revenue:** One time **Margin:** Medium	**Revenue:** Monthly **Margin:** Very high

[1] Includes EMS, Microsoft Intune, and SCCM, update services around Windows 10 & Microsoft 365 Apps
[2] Source: Partner Opportunity for Microsoft 365 Business Total Economic Impact Study by Forrester Consulting, commissioned by Microsoft, July 2018.
[3] Device – Includes low-cost device and services
[4] Source: Gartner Cost Optimization Is Still Not a Reason to Implement VDI or DaaS – Derived
[5] Source: Microsoft 365 Partner Opportunity Total Economic Impact Study by Forrester Consulting, commissioned by Microsoft, July 2020.

Therefore, Services Providers can provide an end-to-end modern offering to support the customer journey to Cloud Native Windows Endpoints.

Closing

Over the past 6 years Microsoft has been providing organizations with paths to Cloud Native Windows management.

However, for organizations to fully achieve Cloud Native they still must tackle the one thing that, in my experience, holds most organizations back – the applications. So far, Microsoft has not provided a clear path beyond meeting their customers where they are. Many customers are essentially stuck in this co-management limbo where they have moved their workloads to Intune but are still reliant on delivering their applications via Configuration Manager.

To compound this problem, many organizations are experiencing a reduction on their operation budgets and headcounts. This is making it extremely challenging to build a business case for tackling this problem which is perceived as an expensive manual effort to Discover, Modernize, Migrate and Test a complex application estate.

At Rimo3 we pride ourselves on being the world's first fully automated package modernization solution for application migrations from Configuration Manager to Intune. Thus, helping organizations maintain critical packaging configuration and installation logic, automate migrations of legacy Configuration Manager packages to Intune, and accelerate the move to a modern workspace [9].

[1] Microsoft, “Learn more about cloud-native endpoints,” https://learn.microsoft.com/en-us/mem/solutions/cloud-native-endpoints/cloud-native-endpoints-overview, 2023.

[2] Microsoft, “Overview of Windows Autopilot,” https://learn.microsoft.com/en-us/mem/autopilot/windows-autopilot, 2023.

[3] Microsoft, “Overview of Windows as a service,” https://learn.microsoft.com/en-us/windows/deployment/update/waas-overview, 2023.

[4] Microsoft, “What is co-management?,” https://learn.microsoft.com/en-us/mem/configmgr/comanage/overview, 2023.

[5] Microsoft, “Cloud Management Gateway Overview,” https://learn.microsoft.com/en-us/mem/configmgr/core/clients/manage/cmg/overview, 2022.

[6] Microsoft, “Co-Management is Instant and Easy With #Just4Clicks,” https://techcommunity.microsoft.com/t5/microsoft-intune-blog/co-management-is-instant-and-easy-with-just4clicks/ba-p/250539, 2018.

[7] D. Guillory, “Cloud Attach Your Future - Part II - "The Big 3",” https://techcommunity.microsoft.com/t5/configuration-manager-blog/cloud-attach-your-future-part-ii-quot-the-big-3-quot/ba-p/1750664, 2020.

[8] Microsoft, “Enroll Configuration Manager devices into Endpoint analytics,” https://learn.microsoft.com/en-us/mem/analytics/enroll-configmgr, 2023.

[9] Microsoft, “Tenant Attach Documentation,” https://learn.microsoft.com/en-us/mem/configmgr/tenant-attach/, 2023.

[10] Forrester, “New Technology: The Projected Total Economic Impact of the Microsoft Intune Suite,” 2023.

[11] Forrester, “The Total Economic Impact of Microsoft Endpoint Manager,” 2021.

[12] Forrester, “The Total Economic Impact of Modernizing Endpoints,” 2021.

[13] Forrester, “The Total Economic Impact of Microsoft Managed Desktop,” 2020.

[14] Forrester, “The Total Economic Impact of Microsoft 365 E3,” 2022.

[15] Microsoft, “What is Windows Autopatch?,” https://learn.microsoft.com/en-us/windows/deployment/windows-autopatch/overview/windows-autopatch-overview, 2023.

[16] Microsoft, “Azure AD Joined Devices,” https://learn.microsoft.com/en-us/azure/active-directory/devices/concept-azure-ad-join, 2023.

[17] Microsoft, “CMG Overview,” https://learn.microsoft.com/en-us/mem/configmgr/core/clients/manage/cmg/overview, 2022.

[18] Microsoft, “Co-management with Autopilot,” https://learn.microsoft.com/en-us/mem/configmgr/comanage/autopilot-enrollment, 2023.

[19] Microsoft, “Cloud-native endpoints and on-premises resources,” https://learn.microsoft.com/en-us/mem/solutions/cloud-native-endpoints/cloud-native-endpoints-on-premises, 2023.

[20] Microsoft, “Tenant Attach Prerequisites,” https://learn.microsoft.com/en-us/mem/configmgr/tenant-attach/prerequisites, 2023.

[21] Microsoft, “Tenant attach data collection,” https://learn.microsoft.com/en-us/mem/configmgr/tenant-attach/data-collection, 2023.

[22] Microsoft, “Third-party MDM coexistance with Configuration Manager,” https://learn.microsoft.com/en-us/mem/configmgr/comanage/coexistence, 2022.

[23] Microsoft , “Co-management Benefits,” https://learn.microsoft.com/en-us/mem/configmgr/comanage/overview#benefits, 2023.

[24] C. B. a. P. Larsen, in Mastering Microsoft Endpoint Manager, 2021.

[25] Microsoft, “Frequently asked questions about resource access deprecation,” in https://learn.microsoft.com/en-us/mem/configmgr/protect/plan-design/resource-access-deprecation-faq, 2023.

[26] Microsoft, “Co-management Workloads - Endpoint Protection,” in https://learn.microsoft.com/en-us/mem/configmgr/comanage/workloads#endpoint-protection, 2023.

[27] Rimo3, in https://www.rimo3.com/, 2023.

[28] Nerdio, “Nerdio Manager for Enterprise,” in https://getnerdio.com/nerdio-manager-for-enterprise/, 2023.