**Intune with Cloud Attach**

**Architecture and Deployment**

*PLACEHOLDER FOR COVER PAGE*

*PLACEHOLDER FOR CONTENTS PAGE*

Topics to be covered in this document.

1. Introduction and Goals
2. System Scope and Context
3. Solution Strategy and Architecture Decision Records
4. Deployment view
5. Cross cutting concepts
6. FinOps
7. Infrastructure & Operations
8. Quality Assurance
9. General Architectural Concerns
10. Appendix
11. Introduction and Goals

This document outlines the deployment and architecture of Intune with Cloud Attach. The goal for this document is to provide a detailed overview of this solution, including the design and deployment. The proposed solution will leverage Intune for comprehensive device management capabilities along with Cloud Attach which allows configuration of policies for on-premises servers.

Intune with cloud attach provides a unified solution for Microsoft Defender for Servers (MDS) policies covering both cloud and on-premises servers. It provides a single console to manage the endpoint security on all devices. The scope of this solution is limited to server environments in terms of the infrastructure. Other components such as endpoints, network devices etc are excluded for this solution.

Using this solution, ensures improved device security, provides automated deployment and management across device types, and provides consistent user experience. It also helps in enforcing organisations’ s compliance policies to meet regulatory requirements with the help of centralised monitoring of devices.

* 1. Requirements Overview

This section provides a high-level overview of the functional and non-functional requirements for the Intune with Cloud Attach deployment. These requirements aim to ensure that the solution supports A&O’s business needs and objectives.

* Reduced costs – Lower IT infrastructure and tooling costs by leveraging a single cloud-based device management solution.
* Improved Efficiency – Streamline specific device and application management processes to improve the efficiency using Intune with cloud attach solution.
* Efforts estimation –
  + Prerequisites: 3-4 working days (obtaining privileges, scope of servers, configuring proxy rules for domains etc).
  + Enabling cloud attach: 5-6 working days (enabling configuration for tenant attach, Entra ID configurations, synchronisation, enabling features).
  + Onboarding servers in scope: 2-3 working days.
  + Validation: 2-3 working days (validation of servers reporting to Intune via cloud attach and if servers are receiving the configurations and policies).
  + (Optional) Troubleshooting (in case of any issues being reported): the effort will be dependent on the number of issues received.

Total: 12 -16 days.

* 1. Quality Goals

This section outlines the relevant quality goals for Intune with Cloud Attach deployment. This ensures that the end users have a positive experience, and organisation can maintain business continuity. Quality goals are linked to Microsoft’s WAF (Well Architected Framework) and ensure that the solution meets the requirements for reliability, security, operational excellence and performance efficiency.

|  |  |
| --- | --- |
| **Pillar** | **Description** |
| Reliability | Ensures a high uptime for Intune services e.g., deployment and conditional access. |
| Security | Protects the workload by adhering to industry standards and regulations (e.g., GDPR) for data protection and security. |
| Operational Excellence | Providing single pane of glass for device management. Reduce issues by using automation for routine tasks e.g., device enrolment, app deployment etc. Implement monitoring and logging to track system performance. |
| Performance Efficiency | Adjust the changes in demands placed on the workload through horizontal scaling and testing changes before deploying to production.  Ensure optimum use of compute, storage and other resources. |

|  |  |  |
| --- | --- | --- |
| **Pillar** | **Metric** | **Goal** |
| Reliability | Maintain high level of service availability for Intune. | Target 98-99% uptime |
| Security | Microsoft Defender for Cloud Security Score | 80 or above |
| Operational Excellence | Maintain a low mean time to resolve for critical incidents | Less than 1 hour |
| Performance Efficiency | Maintain low resource utilization for memory, storage etc. | 75% or below |

* 1. Stakeholders

This section provides an overview of the stakeholders i.e. all persons, roles or organisations that have varied interests in this implementation and architecture document for Intune with cloud attach. They may be directly involved in the deployment and management of the solution or indirectly affected. They could be consulted or approached for their inputs. The below list shows key stakeholders with respect to this document.

* Platform team
* Infosec team
* Operations team
* Any other relevant member, group or team as needed.
  1. Architecture Standard

It is essential to adhere to specific architecture standards to ensure a secure, efficient, and scalable implementation solution. These standards can be internal guidelines or frameworks or requirements, or industry standards, best practices and recommendations. For the implementation of this solution the standards that are referenced are shown in the table below.

|  |  |  |  |
| --- | --- | --- | --- |
| **Architecture Standard** | **Type of Standard** | **Description** | **Reference Link** |
| Azure Security Baseline | Microsoft Azure Standard | Provides recommendations for securing the cloud resources and aligning with other industry standards such as CIS, NIST etc. | <https://learn.microsoft.com/en-us/security/benchmark/azure/security-baselines-overview> |
| Microsoft Intune Best Practices | Microsoft Azure Standard | This provides guidance on Intune deployment and covers information on various other topics. | <https://learn.microsoft.com/en-us/mem/intune/fundamentals/deployment-guide-intune-setup>  [Deployment guide for Windows device management | Microsoft Learn](https://learn.microsoft.com/en-us/mem/intune/fundamentals/deployment-guide-platform-windows) |
| CIS Benchmarks | Industry Standard | This offers specific configuration related recommendations for various technologies including Microsoft Azure. | [CIS Microsoft Windows Server Benchmarks (cisecurity.org)](https://www.cisecurity.org/benchmark/microsoft_windows_server) |
|  |  |  |  |

1. System Scope and Context

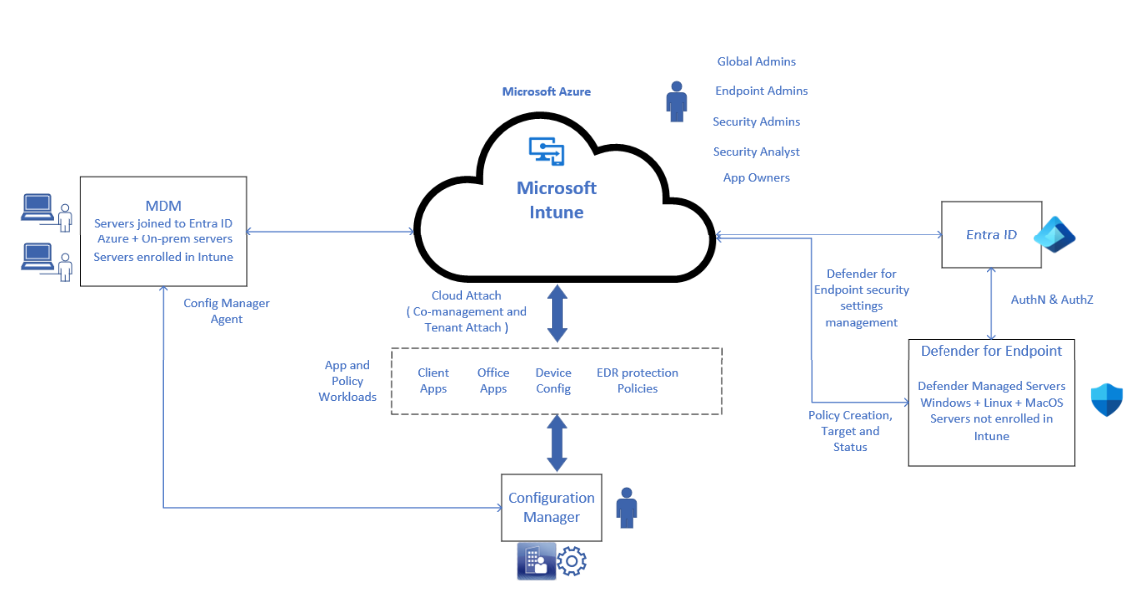
The current on-boarding are for the servers Windows 2012 r2 and above.

Note:

1. Windows Server 2008, 2008 R2, and 2012 – End of support and not supported by Intune (There are estimated to be around 30 servers, which will not be in scope of this project)

2. Windows Server 2012 R2 – Nearing end of support but supported by Intune currently. There should be plan in place to cover these servers once they are out of support.

A high-level system diagram that provides an overview of the system, components involved in the solution and the roles or users.



1. Solution Strategy and Architecture Decision Records

The solution strategy and architecture decision records play a critical role to ensure that the overall strategy and the key decisions taken for the implementation are documented. This section covers some of the key aspects and components involved and their justification with regard to the Intune with cloud attach solution.

Solution Strategy –

Microsoft Intune solution can be used as an on-premises platform with configuration manager, a cloud-based platform and lastly with co-management which acts as a bridge connecting on-premises to cloud.

Using co-management enterprises can transition to cloud using configuration manager with Intune.

There are two options for organisations that have management workloads with on-premises and cloud servers transitioning to Microsoft Intune. These are tenant attach and co-management.

* Tenant Attach
  + 1. Enables organisations to connect their on-premises configuration manager environment to the cloud and Intune tenant. This helps in a smooth transition of servers to the cloud-based management platform without any manual effort of enrolment.
    2. The main advantage of this option is that the administrators can have a unified and single place for all management tasks for the enrolled servers within the organisation.
    3. Using tenant attach admins can manage endpoint security for all the attached devices from Intune admin center.
* Co-management
  + 1. This option provides flexibility to gradually transition all device functions from configuration manager to Intune. This allows the organisation to specify and switch workloads and control the pace of the entire transition with less disruption. Co-management helps simplify device management functions.

After configuring both tenant attach and co-management organisation can view and manage all enrolled servers, both on-premises and cloud-based, from a single console.

**Co-Management Workloads:** Co-management supports the following workloads:

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

For this deployment, Endpoint protection is the only applicable workload in scope which includes the Defender suite of protection features:

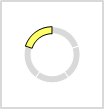
* Microsoft Defender Antivirus
* Microsoft Defender Application Guard
* Microsoft Defender SmartScreen
* Microsoft Defender for Endpoint (formally known as Windows Defender Advanced Threat Protection)
* Windows Defender Firewall
* Windows Encryption (also known as BitLocker)
* Windows Defender Exploit Guard
* Windows Defender Application Control
* Windows Defender Security Center

Key components:

* Microsoft Intune – Cloud-based mobile device management (MDM) solution that enables centralized management and control of devices and applications with security settings and policies.
* Microsoft Defender for Endpoint – A comprehensive endpoint security solution that provides threat detection and prevention capabilities and protects the enterprise devices.
* Configuration manager – Microsoft’s on-premises management platform which can be integrated with Intune for hybrid management across the enterprise. When the devices are managed with both Configuration manager and Microsoft Intune, this configuration is called co-management. It provides comprehensive tools for managing updates, configuration settings and monitor the device health.
* Cloud Attach – A process for connecting on-premises configuration manager environments to Intune, enabling hybrid management. For configuration manager, cloud attach typically involves using tenant attach to connect configuration manager to Intune.
* Entra ID – Microsoft’s cloud-based identity and access management service used for user authentication and authorization.

Key Architectural Decisions:

* Device Enrolment – Enforce device enrolment for all necessary IT devices with Azure AD or Intune which ensures that they are subject to consistent security policies and management controls. Device enrolment can be automated with Intune.
* Simplified Device Management – Intune with cloud attach ensures that the device management is streamlined. Cloud-based Intune controls can be used to manage the devices without the need of complex infrastructure. This results in decreased maintenance efforts, improved scalability and administration.
* Device Lifecycle Management – This solution would provide end to end lifecycle management for all devices under a single console. The entire lifecycle can be easily managed, from setting up the device with the required configurations to its retirement.
* Conditional Access – Using Intune with cloud attach conditional policies can be implemented based on device properties, usage etc. This allows for granular and dynamic access controls over the organizational data on all devices.
* Enhance Security – Cloud attaching configuration manager with Intune provides advanced security features e.g., conditional access, Microsoft Entra authentication, and threat detection. All the enrolled devices are protected against emerging threats with Intune and configuration manager’s robust endpoint protection.
* Unified Management – Cloud attaching configuration manager with Intune provides modern management features e.g., zero touch provisioning, app deployment, remote device management etc. This allows unified and efficient cloud management across platforms for different device types.



**Tier 1 Intune with Cloud Attach Deployment**

**Activities:**

* + 1. Enable Cloud Attach
    2. Onboarding and testing of severs into Intune
    3. Integration of Intune and MDE

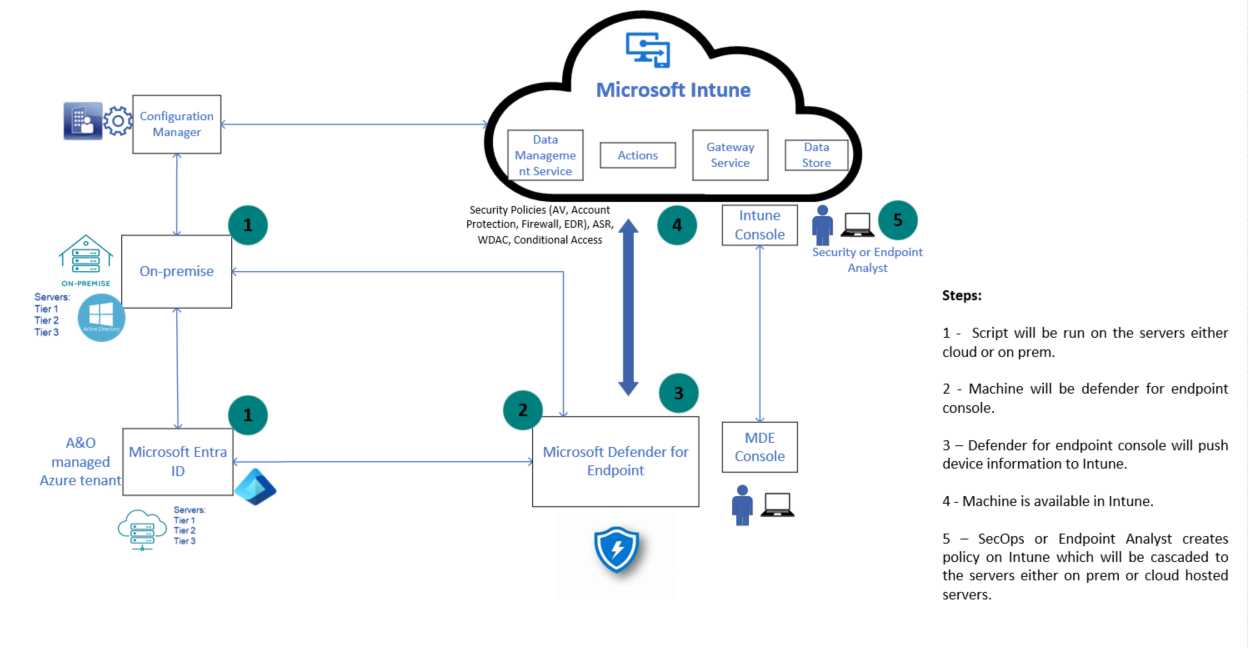
**Ideal outcome:**

* + 1. Cloud attach successfully enabled
    2. All servers successfully onboarded to Intune
    3. Integration with MDE is completed successfully

1. Deployment

A&O is currently using configuration manger version 2303 with an upgrade to 2309 planned in November 24. The deployment steps mentioned in this section are aligned to this version and above. Older and newer versions of configuration manager may have different configuration steps.

**Detailed step by step deployment diagram is shown below.**



* 1. Pilot Deployment Strategy

An initial set of servers that host non-critical applications will be selected for deployment. A&O has a ranking system for server criticality, consisting of the three tiers outlined in the table below.

|  |  |  |
| --- | --- | --- |
| Tier | Resilience | Example Servers/Services |
| Tier 1 Core IT services supporting fee-earning operations | Resilience significant and infrastructure in place to facilitate rapid recovery (cited at 2 geographical locations/load balanced) | Active Directory, Email, SharePoint, Mimecast |
| Tier 2 Non-core IT services supporting fee-earning operations | Less resilience | Templafy, Condeco, Wireless, Netbackup |
| Tier 3 Support services and non-critical services | Best endeavours | Collaborate, eDiscovery, ICM Bibles |

We will identify a group of servers within Tier 3 for the pilot deployment. This group of servers has the lowest business criticality, and the deployment will have the lowest impact on business services.

During the pilot deployment, any challenges and their solutions should be documented to assist with the later deployments in the rollout.

* 1. Deployment Roadmap Diagram

Following the pilot deployment, we will roll out the deployment of Intune with cloud attach to each Tier, in order of least criticality to most. This will allow us to incorporate lessons learned at each stage meaning the final deployment to Tier 1 servers should be the smoothest and will have least impact on the most critical business services.

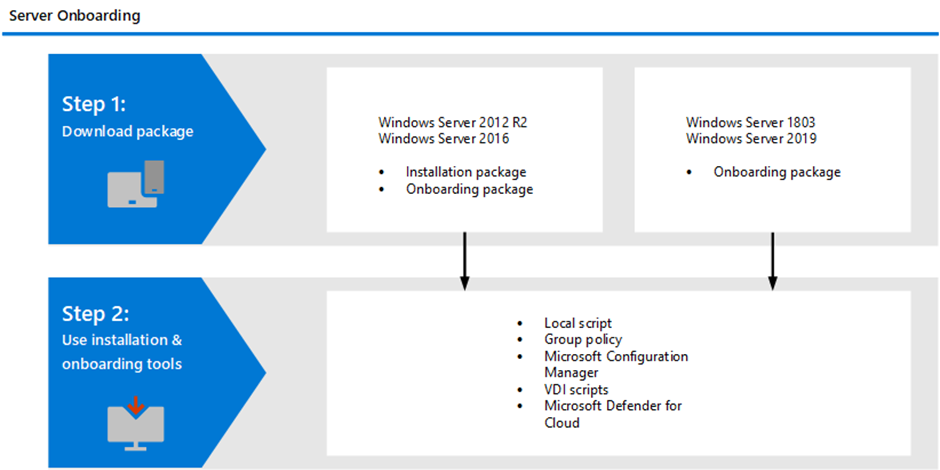
A screenshot of a document

Description automatically generated

**Deployment of Intune with Cloud Attach across server Tier 1, 2 and 3**

|  |  |  |
| --- | --- | --- |
| **Tier 3** | **Tier 2** | **Tier 1** |
| **Activities:**  1.Enable Cloud Attach  2.Onboarding and testing of severs into Intune  3.Integration of Intune and MDE  **Ideal outcome:**  1.Cloud attach successfully enabled  2.All servers successfully onboarded to Intune  3.Integration with MDE is completed successfully |  |  |

Deployment of the onboarding script can either be done via group policy in AD or can be done via configuration manager. The below image shows the steps for server onboarding.



* 1. Deployment Timeline

Below shown is an estimate for each collection type (Details on collection types in section <to insert>)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ​**Activity**​ | ​**Week Commencing**​ | **Week 1**​ | **Week 2**​ | **Week 3**​ | **Week 4**​ | **Week 5**​ |
| ​ | ​ | ​ | ​ | ​ |
| **Pre-requisites** |  | X |  |  |  |  |
| **Microsoft defender and Intune integration** | ​ |  | ​X | ​ | ​ | ​ |
| **​Enable Cloud Attach** | ​ |  | ​X | ​X | ​ | ​ |
| **Create collections** |  |  | X |  |  |  |
| **​ Deploy servers to Defender** | ​ | ​ |  | ​X | ​ X | ​ |
| **​Enrolment Validation** | ​ | ​ | ​ | ​ | ​ X | ​ |

* 1. Prerequisites

The below sections provide all the pre-requisites for the configuration of Configuration manager and Intune, for enabling cloud attach for on-boarding and management of on-premises and cloud servers via Intune console.

**Network:**

|  |  |  |
| --- | --- | --- |
| **Sno** | **Destination/URL** | **Description** |
| 1 | https://aka.ms/configmgrgateway  https://\*.manage.microsoft.com  https://dc.services.visualstudio.com | Helps validate internet endpoints and ensures availability of cloud service |
| 2 | http://crl3.digicert.com  http://crl4.digicert.com  http://ocsp.digicert.com  http://www.d-trust.net  http://root-c3-ca2-2009.ocsp.d-trust.net  http://crl.microsoft.com  http://oneocsp.microsoft.com  http://ocsp.msocsp.com  http://www.microsoft.com/pkiops | Allow URL if the environment has proxy rules for specific CRL & OCSP verification locations |

**Configuration manager:**

1. Configuration manager Version: Current Branch 2006 + Hotfix Rollup KB4575789
2. Configuration manager infrastructure with SSL Communication or E-HTTP Enabled Management Point
3. Configuration manager client version 5.00.9012.1056 and above. (This client version is available once the Configuration manager site has been upgraded to Current Branch 2006 + Hotfix Rollup KB4575789)

**Access and Permissions:**

1. Domain Administrator Account – Required for signing in Configuration manager when applying the onboarding change.
2. The user account performing device actions need to be a synced user object in Microsoft Entra ID (Hybrid Identity)
3. Intune admin

**Licensing:**

* Ensure that you have the Microsoft Intune Plan 2 license which is required for existing configuration manager devices to be enrolled into Intune.

**Other requirements:**

1. Server List with details including tiers and operating system.
2. Configuration manager collection name(s).
3. The geographic location of the Azure tenant and the service connection point should be the same.
4. At least one Intune role as the administrator or Endpoint Security Manager is required to be able to manage the security features in MDE and access the Microsoft Intune admin centre.
5. The administration service in Configuration manager should be set up and functional.
   1. Deployment Steps

There are four different use cases within the A&O estate with regards to enrolment of the servers. These different scenarios should be taken into consideration as part of this deployment. They are listed below.

**Use Cases**

1. Servers which are already enrolled in Defender should be onboarded to the Intune portal once communication is enabled and established.
2. Domain joined Cloud servers will be enrolled as well according to the deployment script.
3. Domain joined on-prem servers will need to be enrolled separately.
4. New Servers can be enrolled in Intune in several ways.

* The onboarding script can be deployed via configuration manager which can be deployed once configuration manager is deployed
* Pushed via GPO upon first logon to the domain
* hey can be done manually if required or pushed during server deployment.

Below are the detailed deployment steps for Intune with Cloud Attach to manage servers.  
Note: The below configuration steps are applicable only for servers. For e.g., Windows 10/11 will require different configuration steps.

1. **Microsoft Defender and Intune integration**

Intune and Defender for Endpoint work together to apply endpoint security policies on MDE onboarded devices. Devices will get a record in Intune to target them with policies. In case the devices are not onboarded in Intune or not fully registered in Entra ID, it will automatically generate a so-called synthetic object. This is nothing more than a representation of that MDE only device in Entra ID.

* 1. Defender Portal: Logon to security.microsoft.com 🡪 From the left-hand side under endpoint section ensure that slider of Microsoft Intune connector is switched on 🡪 In the same section under endpoint and enforcement scope make sure that the Windows server devices is chosen
  2. Intune Portal: Logon to intune.microsoft.com à Under home choose endpoint security à Under setup choose Microsoft Defender for endpoint and ensure that ‘Allow Microsoft Defender for Endpoint to enforce Endpoint Security Configurations’ is switched on à In the Same page ensure that ‘Connect Windows devices version 10.0.15063 and above to Microsoft Defender for Endpoint’ is switched on.

1. **Enable Cloud Attach**

The configuration manager administrator performs the steps outlined below to cloud attach the configuration manager to Intune. It connects the configuration manager hierarchy to Intune, which enables managed devices to be visible and managed from Intune.

* 1. Configuration Manager Portal: Go to Overview à cloud services à Cloud Attach à CoMgmtSettingsProd properties enable on configure upload tab à Upload all devices Managed by Microsoft Configuration manager.
  2. Configuration Manager Portal: Overview à cloud services à Cloud Attach à CoMgmtSettingsProd under the workloads tab move the slider of endpoint protection to the configuration manager type ‘Pilot Intune’ for the pilot set of servers. Once onboarded without any issues, it should be amended to type ‘Intune’.

Workload Configuration Types:

* **Configuration Manager**: Configuration Manager continues to manage this workload.
* **Pilot Intune:** Switch this workload only for the devices in the pilot collection. You can change the Pilot collections on the Staging tab of the co-management properties page.
* **Intune:** Switch this workload for all Windows devices enrolled in co-management.

Note - When pilot Intune is selected for Endpoint Protection and Device Configuration Policies, Intune will only deploy the policies and will not perform policy removal upon un-assignment. For policy removal from the device when the policy is unassigned, the workload must be switched to Intune.

* 1. Validation: Ensure that cloud attachment is available, and configuration manager is connecting with the Cloud part.

SCCM console à Administration à Cloud Services à Cloud management gateway and check that service status is marked as ready

1. **Create Device Collection**

Collections help to organize resources into manageable units. We create collections to match our needs, and to perform operations on multiple resources at one time. Microsoft provides a set of built-in collections and a capability to build custom collections.

Most management tasks rely on or require using one or more collections. Although we can use the built-in collection of All Systems, using it for management tasks is not a best practice and creating custom collections is more appropriate for specifically identify the devices or users for a task. For our need, we will create custom collections.

Built-in and custom collections appear in the User Collections and Device Collections nodes in the Assets and Compliance workspace in the Configuration Manager console.

Note: A collection can contain users or devices, but not both.

**Steps for device collections are outlined below.**

* 1. Download the 2 packages for the corresponding groups i.e. for 2012r2 and 2016, 2019 and 2022 Windows server OS versions.
  2. Identify Windows server OS machines and their tiers.
  3. Create six Collections (2 groups and 3 tiers) on configuration manager.

(For the scope of this project, we will create one collection for Endpoint Protection, but device collection should be created for each workload when they are consumed.)

It is recommended to follow a naming convention covering each workload to avoid any confusion during the setup, future upscaling, and operations.

* Co-Management - Compliance Policies
* Co-Management - Device Configuration
* Co-Management - Endpoint Protection
* Co-Management - Resource Access Policies
* Co-Management - Client Apps
* Co-Management - Office Click To Run Apps
* Co-Management - Windows Update Policies
  1. In the configuration manager console for each group that was created in the previous step right click on the created group under device collections, click on the Cloud sync tab and tick check box “Make this collection available to assign Endpoint security policies from Microsoft Intune admin center”.

Note: Ideally each tier should be done one at a time and a new collection and tier should be started after completion of the previous tier

**4. Deploy servers to Defender**

* 1. Place the machines under the correct group collection.

On legacy OS (2012 r2 and 2016),

* Deploy install with administrator privileges.

(Refer:<https://support.microsoft.com/en-au/topic/microsoft-defender-for-endpoint-update-for-edr-sensor-f8f69773-f17f-420f-91f4-a8e5167284ac>)

* + Install MD4WS.msi on these systems with administrator privileges.
  + Run onboarding script on required collections with administrator privileges.

For Windows Server 2019 and 2022

* Run Onboarding script with administrator privileges.
* The above step can be done via the pilot Intune slider in configuration manager to target a specific collection of machines

**5. Enrolment Validation**

Below are the steps to perform the validation for the devices enrolled. Please note it may take few minutes to hours for the servers to replicate in the defender and Intune portal.

* 1. Verify if all the servers in the collection are now visible in the Defender portal.
  2. Verify if all the servers in the collection are now visible in the Intune portal.
  3. Azure portal 🡪 Enterprise apps 🡪 All apps 🡪 New app created called ‘configmrserv.\*’ 🡪 Click – check audit logs to confirm if this was created recently.

**Applicability of the above configuration steps for each use case:**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Step** | | **Use Case 1 (Servers in Defender)** | | **Use Case 2 (Domain joined Cloud Servers)** | **Use Case 3 (Domain joined on-prem servers)** | | **Use Case 4 (New Servers)** |
| 1. Defender Intune Integration | | Yes | | Yes | Yes | | Yes |
| 2. Enable Cloud Attach | | No | | Yes | Yes | | Yes |
| 3. Create Collections | | No | | Yes | Yes | | No |
| 4. Deploy Servers | | No | | Yes | Yes | | No |
| 5. Intune Validation | | Yes | | Yes | Yes | | Yes |
| **Category** | **Endpoint Security Policy** | | **Description** | | | **Benefits** | | |
| Security Policies | Account Protection | | Account protection policies help you protect the identity and accounts of your users. The account protection policy is focused on settings for Windows Hello and Credential Guard, which is part of Windows identity and access management. | | | The management potential allows these features to be deployed across your full estate providing a unified security approach, ensuring device compliance is more complete. | | |
| Antivirus | | You can create and deploy Microsoft Defender Antivirus policies to manage antivirus settings on cloud attached devices. This includes different types of policies for real-time protections, scheduled scans etc. | | | Antivirus policy management with Intune allows granular controls of devices, unified management interface etc. | | |
| EDR | | You can leverage different features for EDR policies which includes endpoint security policies for devices managed by Configuration Manager. Other features of EDR include – real-time data synchronization, PowerShell scripts etc. | | | The real time data synchronisation allows you to query and present data from all registered devices instantly.  The integration allows for easier troubleshooting by running PowerShell scripts directly from the Intune admin centre | | |
| Firewall | | You can create and deploy firewall policies from the Intune admin centre to devices managed by Configuration Manager. Intune allows you to configure various Windows Firewall settings, such as enabling or disabling the firewall, configuring rules for inbound and outbound traffic, and setting up network profiles | | | The extended management potential allows standard firewall policies to be deployed across your full estate and managed from one central interface. | | |
| Additional Security Policies | Attack Surface Reduction (ASR) | | You can use attack surface reduction rules to reduce the attack surface of devices by minimizing the areas where your organization is most vulnerable to attacks.  You can target behaviours that malicious software typically uses to infect devices. Examples of these include using executable files and scripts. | | | The extended management potential allows ASR rules to be deployed across your full estate easily and from one central interface. | | |
| Conditional Access | | Conditional Access policies help you to enforce the organisation policies across all the devices. Conditional Access works with Intune device configuration and compliance policies. They also can ensure that only compliant devices can access corporate resources. This includes checking for device compliance with Intune policies. Other features include – enforcing MFA, application protection etc. | | | The extended management potential allows conditional access policies to be deployed across your full estate easily and from one central interface. | | |
| WDAC | | WDAC (Windows Defender Application Control) provides advanced application control policies, ensuring a robust defence against a wide range of cyber threats. By strictly following the application control policies, WDAC ensures that only approved and trusted software is allowed to run on devices. This approach reduces the risk of threats and infections. | | | In WDAC you can use templates to create policies allow list rules. You can also create custom rules within the policy that specifies the level at which the applications are identified and trusted. | | |

This above table highlights the important Intune security features that are available as part of this deployment project.

* 1. Troubleshooting

Below are some scenarios which may be encountered during the deployment stages:

1. Issue: The Configuration manager client is installed, and the device is registered successfully with Microsoft Entra ID. However, the device isn't automatically enrolled in Intune and no errors are seen.

* This issue usually occurs when auto-enrolment is misconfigured in your Intune tenant under Microsoft Entra ID > Mobility (MDM and MAM) > Microsoft Intune.
* Fix: Follow the steps in [Configure auto-enrollment of devices to Intune](https://learn.microsoft.com/en-us/mem/configmgr/comanage/tutorial-co-manage-clients#configure-auto-enrollment-of-devices-to-intune).

1. Issue: The Configuration manager client is installed. However, the device isn't registering with Microsoft Entra ID and no errors are seen. This issue usually occurs because the Configuration manager client agent settings aren’t configured to direct the clients to register.

* Fix: Verify that you follow the steps in [Configure Client Settings to direct clients register with Microsoft Entra ID.](https://learn.microsoft.com/en-us/mem/configmgr/comanage/tutorial-co-manage-clients#configure-client-settings-to-direct-clients-to-register-with-azure-ad)

1. Issue: There is a known bug in configuration manager that could prevent the workload CI from merging with the other co-management workloads. This can be identified by checking the CoManagementHandler.log. The following error can be observed in the log file: Failed to merge/resolve rules. Error 0x8000ffff

* Fix: To overcome this, the CoMgmtSettingsProd always need to be evaluated 1st before evaluating the specified non-compliant workload.

Therefore, the co-management workloads should be evaluated in the following sequence:

1. Select CoMgmtSettingsProd - Click Evaluate
2. Select <WorkloadName> - Click Evaluate
3. Select CoMgmtSettingsProd - Click Evaluate
4. Select <WorkloadName> - Click Evaluate
5. Select CoMgmtSettingsProd - Click Evaluate
6. Cross Cutting Concepts
   1. Policy

* **Business Impact Assessment (BIA)**
  1. Compliance

The Center for Internet Security (CIS) publishes benchmarks for Microsoft products and services including the Microsoft Azure, under which Intune falls. The Microsoft Intune for Microsoft Windows benchmarks and the Windows Server 2016 Benchmark will be relevant for determining compliance standards for this deployment.

* 1. Technical Controls
* **Cloud security**

During the and following the deployment of the tool, cloud security best practices will need to be followed. This should be done in line with the Global Cloud Security Policy.

* **Server Hardening**

During and following the deployment of the tool we should consider server hardening measures. Any actions taken in this regard should follow the Global Server Hardening Policy.

* **Authentication/Authorisation**

Authentication and authorisation should follow the same standards already outlined in several policies, including the Global Privileged Account and Identity Policy, The Global Guest User Access Policy, Global Information Security Access Control Policy and the Global Account Management and Password Policy.

* **Encryption**

The Global Encryption Policy lays out the expectations for how data at rest, data in transit and key management etc. should be handled.

1. FinOps

This section will detail the financial costings associated with implementing Intune with cloud attach. Cloud attach is a part of Intune and is available at no additional cost with any licence that allows the use of Intune.

There may be a cost associated with the deployment phase and BAU running of the tool. Please see below an estimate of the roles needed and time they will require to get the service running.

|  |  |  |  |
| --- | --- | --- | --- |
| **Resource** | **Amount** | **Description** | **Hours** |
|  |  |  |  |
|  |  |  |  |

1. Infrastructure & Operations

* **Service Level**

Intune with cloud attach is a Microsoft Azure product. Microsoft state their performance level for Azure products ranges from 99.9% to 99.99%.

* **Exceptions**

Exceptions will be dealt with by the \_\_\_\_ Team

* **Logging and Tracing**

Logging should be carried out in line with the requirements outlined in the Global Logging and Monitoring Policy. – Look at Intune monitoring logging etc.

* **Configurability**

Intune with cloud attach can be run either on default settings or with custom settings. To change the configuration, go to the Configuration manager console, go to Administration > Cloud services > Cloud Attach. Now select Configure Cloud Attach from the ribbon to open the wizard.

Responsibility for the configuration lies with the \_\_\_\_\_ team.

* **Patching**

Intune patches will be tested and rolled out in line with the Global Patch Management Policy.

* **Separation of Duties**

|  |  |
| --- | --- |
| **Roles** | **Responsibilities** |
| Global Administrator | Create Microsoft Entra applications from Configuration manager and review configuration changes. |
| Intune Administrator | Deploy and configure tenant configuration, user and device enrolment policies. Manage Intune subscriptions. Troubleshoot Intune issues.  Manages custom Intune roles. It's the only Intune role that can assign permissions to Administrators. |
| Security Administrator | Manage Intune security settings and compliance policies. Troubleshoot security risks. Review application and device deployments. |
| Endpoint Security Manager | Manages security and compliance features for the organisation, e.g., security baselines, device compliance, conditional access, and Microsoft Defender for Endpoint solution. |
| Application Owner | Manages the specific applications, view the device related information and configuration profiles. Review application specific deployments. |

* **Decommissioning – look at hardware policy.**

1. Quality Assurance

* **Testability – state success criteria. Devices registered, policy deployment.**
* **Testing Methodology:**
  + **Baseline MDE policy testing** –The purpose of this step is to develop and test the standard baseline MDE policies specific to non-critical servers within the organization. These policies are developed, refined and categorized for various areas such as AV, Firewall, Encryption and so on. The testing for these baseline policies will be done on select groups of devices in audit mode and verified if the policies are working as expected. Detailed sheet of drafted baseline policies can be referenced here.
  + **Application specific policy testing** – This step focuses on creating and tailoring application specific MDE policies and testing these policies on a single critical server that hosts the application. For this case we have selected iManage as the target application. Testing the policy enforcement for a single target application will help in validating the effectiveness of the MDE policies. In order to develop application specific policies, we need to consider the application-level dependencies and the relevant vulnerabilities that can potentially be exploited by an attacker. Detailed sheet of all iManage specific policies can be referenced here.
* **Test Cases**

The below table shows few of the test cases for the different categories of the MDE baseline policies and application specific policies.

|  |  |
| --- | --- |
| **Test Use Case** | **Expected Outcome** |
| Test if the real time monitoring defender for endpoint functionality for servers is set to ALLOW or enable by simulating using a sample malicious file on the test server. | MDE should detect and alert on any type of malicious activity based on the real time monitoring functionality. |
| An administrator should specify list of paths that should be ignored during a scan using the excluded paths option. | MDE should ignore each path in the list specified by the administrator during a system scan. |
| Configure MDE to scan all types of scripts present in the system. | Script scanning functionality in MDE should be set to ALLOW to protect against the risk of ransomware or other attacks. |
| Domain network firewall setting should be ON or TRUE for advanced security enforcement. | To ensure that the network is not vulnerable to attacks due to misconfiguration, domain network firewall setting should be set to TRUE. |

1. General Architectural Concerns

* **System resiliency**
* **Scalability**
* **Disaster Recovery**

Microsoft Intune falls under Microsoft 365 licences and Cloud PC Management services which guarantee a level of availability.

The Cloud PC Management Service has a regionally redundant architecture that is designed to be highly available, with a target uptime of 99.99%. If there's a Management Service outage, the service has the following target objectives:

RTO of < 6 hours.

RPO of <30 minutes for changes made in the management service.

Appendix

Important Links –

ASR : [Manage attack surface reduction settings with Microsoft Intune | Microsoft Learn](https://learn.microsoft.com/en-us/mem/intune/protect/endpoint-security-asr-policy)

Role permissions for Intune : [Microsoft Intune built-in roles reference | Microsoft Learn](https://learn.microsoft.com/en-us/mem/intune/fundamentals/role-based-access-control-reference)