Microsoft

Microsoft 365 Mobility and Security

Exam Ref MS-101

Brian Svidergol
Bob Clements

FREE SAMPLE CHAPTER

SHARE WITH OTHERS

Microsoft

Exam Ref MS-101 Microsoft 365 Mobility and Security

Brian Svidergol
Bob Clements

Exam Ref MS-101 Microsoft 365 Mobility and Security

Published with the authorization of Microsoft Corporation by:
Pearson Education, Inc.

ISBN-978-0-13-557489-8
ISBN-0-13-557489-7

Library of Congress Control Number: 2019941779

ScoutAutomatedPrintCode

Editor-in-Chief	Brett Bartow
Executive Editor	Loretta Yates
Sponsoring Editor	Charvi Arora
Development Editor	Troy Mott
Managing Editor	Sandra Schroeder
Senior Project Editor	Tracey Croom
Editorial Production	Backstop Media
Copy Editor	Liv Bainbridge
Indexer	MAP Systems
Proofreader	Jana Gardner
Technical Editor	Santos Martinez
Cover Designer	Twist Creative, Seattle

Contents at a glance

Contents

Acknowledgments

Brian Svidergol I would like to acknowledge my wife Lindsay, my son Jack, and my daughter Leah – thanks for being supportive of my endeavors. And thanks for providing me good times and great memories that enable me to maintain a high level of motivation. I love you! I would also like to thank the people working hard on the backend of the project – Loretta Yates (executive editor), Santos Martinez (technical reviewer), Charvi Arora (assistant sponsoring editor), and Troy Mott. I would like to dedicate this book to all the IT professionals taking the time to explore, learn, experiment, and test their skills with certification exams. Keep up the good work and good luck!

Bob Clements I would like to acknowledge my amazing family for all their love, support, and laughter. To my wife Diane, who enables me to work on fun projects like these. To my daughter Abigail, who surprises me every day with her kindness and creativity. And to my son Samuel, who consistently finds ways to make me laugh out loud. Thank you! I would like to dedicate this book to my wife Diane. Your encouragement and support are invaluable. Thank you for all that you do!

About the Authors

BRIAN SVIDERGOL designs and builds infrastructure, cloud, and hybrid solutions. He holds many industry certifications including the Microsoft Certified Solutions Expert (MCSE) – Cloud Platform and Infrastructure. Brian is the author of several books covering everything from on-premises infrastructure technologies to hybrid cloud environments. He has extensive real-world experience from startup organizations to large Fortune 500 companies on design, implementation, and migration projects.

BOB CLEMENTS specializes in enterprise device management. He holds industry certifications around client manageability and administration for Windows, Mac, and Linux. Bob has an extensive background in designing, implementing, and supporting device management solutions for private and public sector companies. In his free time he enjoys spending time with his family, writing, and exploring new technologies.

Introduction

The MS-101 exam focuses on common tasks and concepts that an administrator needs to understand to deploy and manage infrastructure in Microsoft Azure. Managing Azure subscriptions and resources is a key topic on the exam, which includes configure cost center quotas, tagging, subscription level policies, as well as resource organization using resource groups. Another topic covered is implementing and managing storage; which includes creating and configuring storage accounts, implementing Azure backup, as well as configuring Azure files and understanding the services for importing and exporting data to Azure. A significant portion of the exam is focused on deploying and managing virtual machines, which includes configuring of networking, storage and monitoring, automated deployments and managing VM backups. Configuring, managing, and monitoring virtual networks is part of the exam, as-is configuring load balancing. This book covers the creation and managing of virtual networks, DNS, connectivity between virtual networks, and configuring network security groups. The final topic is managing identities, which includes topics on managing Azure Active Directory (AD) when creating users, groups, and devices. You will also find the configuring of hybrid identity using Azure AD Connect, multi-factor authentication, as well as configuring services such as identity protection and self-service password resets.

This book is geared toward Azure administrators who manage cloud services that span storage, security, networking and compute. It explains how to configure and deploy services across a broad range of related Azure services to help you prepare for the exam.

This book covers every major topic area found on the exam, but it does not cover every exam question. Only the Microsoft exam team has access to the exam questions, and Microsoft regularly adds new questions to the exam, making it impossible to cover specific questions. You should consider this book a supplement to your relevant real-world experience and other study materials. If you encounter a topic in this book that you do not feel completely comfortable with, use the "Need more review?" links you'll find in the text to find more information and take the time to research and study the topic. Great information is available on MSDN, TechNet, and in blogs and forums.

Organization of this book

This book is organized by the "Skills measured" list published for the exam. The "Skills measured" list is available for each exam on the Microsoft Learning website: *https://aka.ms/examlist*. Each chapter in this book corresponds to a major topic area in the list, and the technical tasks in each topic area determine a chapter's organization. If an exam covers six major topic areas, for example, the book will contain six chapters.

Important: How to use this book to study for the exam

Certification exams validate your on-the-job experience and product knowledge. To gauge your readiness to take an exam, use this Exam Ref to help you check your understanding of the skills tested by the exam. Determine the topics you know well and the areas in which you need more experience. To help you refresh your skills in specific areas, we have also provided "Need more review?" pointers, which direct you to more in-depth information outside the book.

The Exam Ref is not a substitute for hands-on experience. This book is *not* designed to teach you new skills.

We recommend that you round out your exam preparation by using a combination of available study materials and courses. Learn more about available classroom training and find free online courses and live events at *https://microsoft.com/learn*. Microsoft Official Practice Tests are available for many exams at *https://aka.ms/practicetests*.

This book is organized by the "Skills measured" list published for the exam. The "Skills measured" list for each exam is available on the Microsoft Learn website: *http://aka.ms/examlist*.

Note that this Exam Ref is based on this publicly available information and the author's experience. To safeguard the integrity of the exam, authors do not have access to the exam questions.

CHAPTER 1

Implement modern device services

In this chapter we are working with cloud-based services within Microsoft 365 that are designed to deploy, secure, and manage devices in the enterprise. Throughout this book we will be working with various Microsoft technologies such as Azure, Microsoft Intune, Office 365, and System Center Configuration Manager (ConfigMgr). Along the way there will be several walkthroughs and examples that illustrate how to manage these tools. For these demonstrations we do recommend that you follow along in your own lab. Here are a few links to help get you started:

> ***IMPORTANT***
>
> ***Have you read page xvii?***
>
> It contains valuable information regarding the skills you need to pass the exam.

- **Enterprise Mobility + Security 90-day trial (includes Azure Active Directory Premium P2)** *https://www.microsoft.com/cloud-platform/enterprise-mobility-security-trial*
- **Office 365 Business Premium 30-day trial**: *https://products.office.com/business/office-365-business-premium*
- **System Center Configuration Manager Current Branch 90-day technical preview** *https://www.microsoft.com/evalcenter/evaluate-system-center-configuration-manager-and-endpoint-protection-technical-preview*

Skills in this chapter:

- Implement Mobile Device Management
- Manage device compliance
- Plan for devices and apps
- Plan Windows 10 deployment

Skill 1.1: Implement Mobile Device Management

There are a variety of mobile device management (MDM) solutions available in the market for managing corporate devices and applications. Microsoft Intune is an MDM solution designed around modern device management and built within the Microsoft 365 umbrella.

Without a functional MDM solution, the devices that are meant to provide value and productivity to your workforce, can also introduce security threats, IT support inefficiencies, and an overall inconsistent user experience.

When considering how to manage devices in the enterprise, you need to consider answers to questions such as: is on-premises data protected when accessed from an unmanaged device? Are users able to work in a consistent and effective manner when moving between devices? Can you support a bring-your-own-device (BYOD) program? MDM helps solve these problems by providing a centrally managed service that delivers a secure and productive experience to your organization. In this skill section we will review the process for implementing MDM, including planning considerations, configuration of the MDM, and device enrollment.

This section covers the following topics:

- Plan for MDM
- Configure MDM integration with Azure AD
- Set an MDM authority
- Set device enrollment limit for users

Plan for MDM

In this section we will cover planning considerations for MDM. For the exam you will need to be familiar with the different MDM services that are available from Microsoft, what those services support, and which service to choose if given a scenario with specific requirements. Other considerations that we will cover include prerequisites for your environment, such as network security and capacity planning, as well as pre-existing Group Policy Objects that may overlap with future MDM policies.

The planning stage for MDM is all about knowing what your options are, what the needs of the organization are, and how these two points intersect.

Choose an MDM solution

Microsoft offers a combination of MDM solutions to their customers. These offerings have changed over the years, with heavy investments into cloud services and integration with Azure. The introduction of Windows 10 has also influenced the way you manage devices with a set of native MDM protocols within the operating system, eliminating the need to install another agent on your endpoints. Knowing which solution to choose depends on your organization's deployment goals and objectives. Here is a breakdown of these cloud-based services and some examples on why you might choose one over the other:

- **Microsoft Intune** This solution works best for customers that require modern management capabilities for Windows 10 devices, but also need to limit their on-premises server infrastructure. Microsoft Intune is a cloud-based management solution that does not require additional server infrastructure. Platform support for Intune includes

management capabilities for Windows 10 and macOS. You also have access to features like Autopilot, which can help reduce traditional operating system deployment requirements.

- **Co-management between Microsoft Intune and ConfigMgr** This solution bridges Microsoft Intune and ConfigMgr, enabling customers to co-manage devices based on their requirements. ConfigMgr is an on-premises management solution that includes additional platform support, such as Windows Server. It also includes a unique set of technologies, such as task sequences and image deployment. Environments with co-management can take workloads for their Windows 10 devices and mobile devices and move them to the cloud, while still supporting traditional infrastructure.
- **MDM for Office 365** This MDM solution works best for customers that rely heavily on Office 365 and have a requirement to manage iOS and Android mobile devices. MDM for Office 365 is a cloud-based management solution that does not require additional server infrastructure, but has the smallest footprint when it comes to MDM capabilities.

There is a fourth solution that is not listed here, and that is Microsoft Intune Hybrid. This configuration was an earlier capability that enabled integration between ConfigMgr and Intune in order to maximize platform support and enable administrators to manage devices from a single pane of glass. With the rapid release of new capabilities in Intune, Microsoft reworked how these products were integrated. Intune Hybrid has now been deprecated and will be reaching the end of its support in September 2019.

MORE INFO **TRANSITION FROM HYBRID MDM**

For more information about the transition from hybrid MDM to co-management, visit: *https://techcommunity.microsoft.com/t5/Intune-Customer-Success/Move-from-Hybrid-Mobile-Device-Management-to-Intune-on-Azure/ba-p/280150*. ConfigMgr plays an important role in bridging traditional device management with cloud-based MDM, and co-management is the technology that makes this happen. This is not to be confused with Intune Hybrid. Co-management is a feature available in the ConfigMgr management console starting with ConfigMgr 1710 and supports Windows 10 1709 and later. Setup will require a licensed Intune account to initiate the connection. Once enabled, an administrator can decide which workloads remain managed by ConfigMgr and which workloads move to Intune. For example, Windows Update policies is a workload that can be moved to Intune.

Table 1-1 breaks down each MDM solution in additional detail, along with the list of supported operating systems. From an exam perspective, plan for questions that describe a company's requirements for MDM. You should be familiar with the capabilities and supported operating systems for each solution.

TABLE 1-1 Available MDM solutions and capabilities

Management Platform	Capabilities	Supported Operating Systems
Microsoft Intune	All the capabilities of MDM for Office 365 Mobile device inventory and reporting Certificate management Application management Conditional Access Manage Windows 10 devices	iOS, Android, Surface Hub, Windows 10 Mobile, Windows 10, Windows Holographic for Business
MDM for Office 365	Secure access to Office 365 email and documents, security policies to enforce settings such as PIN lock, selective wipe of company data	iOS, Android, Windows mobile

EXAM TIP

The MS-101 exam is focused on Microsoft 365 mobility and security. This covers modern cloud-based technologies and solutions that help customers move to the cloud. As you prepare for the exam keep an eye on new features and capabilities, such as co-management and how it fits in with modern MDM management. In Skill 1.3 we cover co-management in detail.

Plan your infrastructure

Cloud-based MDM services can help reduce or eliminate the need for on-premises server infrastructure, but there are other infrastructure components to consider, such as external network communication and bandwidth requirements.

Devices that are enrolled in MDM for Office 365 or Microsoft Intune will require regular communication with these cloud services. Communication is standardized across HTTP (80) and HTTPS (443). Microsoft maintains a published list of domains and IP addresses that should be reviewed and implemented into your existing firewall exceptions to ensure that devices can reach the corresponding cloud service. For the exam, you are not expected to memorize this list, but you should know what ports the service communicates over.

Moving from an on-premises management solution to the cloud will impact Internet bandwidth. Your organization's Internet connection must be scaled accordingly to accommodate the increase in traffic. For example, depending on the policies you define, a device enrolled with Intune will check in daily for policy changes, updates, and malware definitions. Other activities like software updates or software distribution can have a substantial impact if they are not accounted for. At a minimum, Microsoft recommends that managed devices remain connected to the Internet for at least one hour each day. The following technologies can be implemented to help reduce network bandwidth impact:

- **Proxy server** A caching proxy server can be used to cache certain types of content, reducing the impact of redundant downloads from multiple devices. For example, a Windows 10 feature update can be multiple gigabytes in size. Caching this content can dramatically reduce Internet bandwidth usage.

- **Delivery Optimization** Delivery Optimization is a cloud-managed solution that helps reduce bandwidth consumption by leveraging peer-caching technology, sharing package contents between devices on a per-deployment basis. This technology is available for Windows 10 devices. Because it is a cloud-managed service, devices must have access to the Internet to leverage its capabilities.

MORE INFO **INTUNE NETWORK REQUIREMENTS AND DELIVERY OPTIMIZATION**

To learn more about the types of Intune communication, frequency and network requirements, visit: *https://docs.microsoft.com/en-us/intune/network-bandwidth-use*. To learn more about Delivery Optimization and the available configurations, visit: *https://docs.microsoft.com/en-us/windows/deployment/update/waas-delivery-optimization*.

Plan your device policies

This section covers the planning considerations for device policies when implementing MDM for Office 365 or Microsoft Intune. In a traditional Active Directory domain, Group Policy serves multiple roles. Administrative templates in Group Policy enable you to define various custom configuration changes for the operating system and your business applications. Enrolling devices in MDM will present two challenges to plan for:

1. **Policy conflicts** Once a device is enrolled in MDM, you create and assign a series of new policies to manage the device. Some of these policies may overlap with configurations that exist in Group Policy, or possibly other management tools, such as ConfigMgr. One example could be Windows Update settings, because these options can be configured in Group Policy, ConfigMgr, and MDM. Considering this challenge as part of the planning phase can save countless hours troubleshooting policy conflicts following enrollment.
2. **Unified management** The policies available in MDM for Office 365 and Microsoft Intune continue to evolve, providing additional controls for device management. There are, however, policy settings that are not yet available. In these situations, consider the impact of eliminating the policy setting altogether, or continuing to support traditional on-premises controls until they can be fully managed by MDM or are no longer needed.

Now that you know some of the challenges with policy management, let's look at two possible solutions that can help you address these challenges as you plan for MDM. First, in Windows 10 1803 Microsoft introduced a new Intune policy called ControlPolicyConflict. When applied, this MDM policy ensures that when a conflict occurs between MDM and Group Policy, the MDM policy will always win. Figure 1-1 shows the Intune portal with the custom policy setting defined for ControlPolicyConflict. You can create this policy by following these steps:

1. Sign-in to the Microsoft Azure portal at *https://portal.azure.com/*.
2. Click **All services**.
3. Search for **Intune** and select it.
4. Under Manage, click **Device configuration**.

5. On the Device Configuration blade, under Manage, click **Profiles**.
6. Click **Create profile**.
7. On the Create Profile blade, fill in the following:
   A. **Name** ControlPolicyConflict
   B. **Platform** Windows 10 and later
   C. **Profile type** Custom
8. On the Custom OMA-URI Settings blade, click **Add**.
9. On the Add Row blade, fill in the following and click **OK**.
   D. **Name** ControlPolicyConflict
   E. **OMA-URI** ./Device/Vendor/MSFT/Policy/Config/ControlPolicyConflict/MDMWinsOverGP
   F. **Data type** Integer
   G. **Value** 1
10. On the Custom OMA-URI Settings blade, click **OK**.
11. On the Create profile blade, click **Create**.

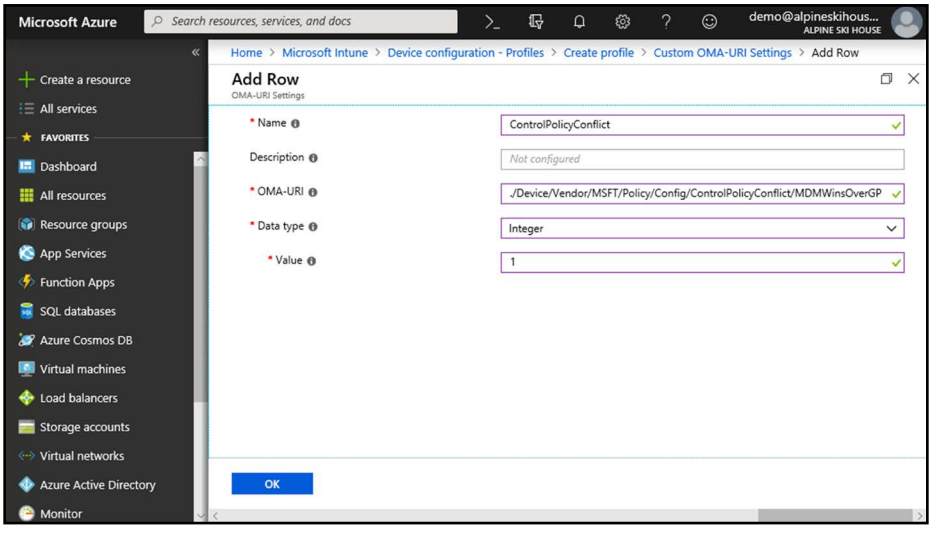


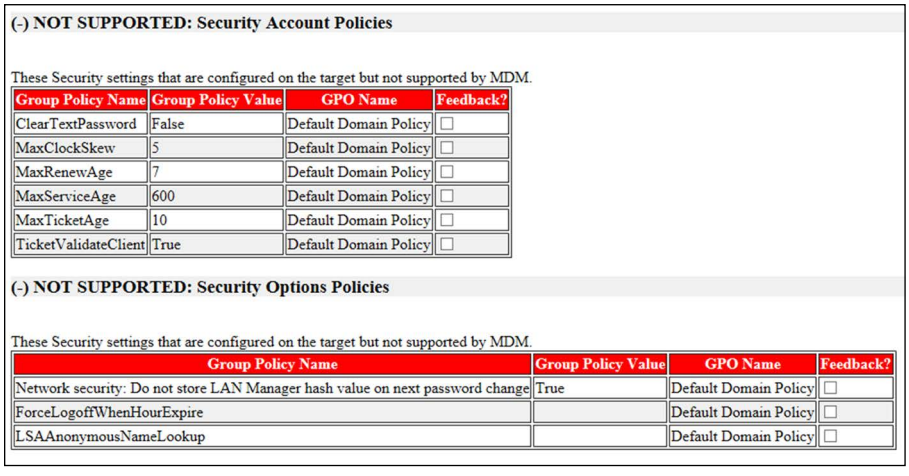
FIGURE 1-1 Custom Intune policy for ControlPolicyConflict

The second solution helps you identify Group Policy settings in your domain that are not supported by MDM. This solution is the MDM Migration Analysis Tool (MMAT). When executed, MMAT will scan the policies in your domain and compare them against a list of supported MDM policies. Once complete, the tool will generate an XML and HTML report that can assist administrators in determining potential conflicts.

In Figure 1-2 you can see an example of the HTML report generated by MMAT. In this example the tool has identified settings in the default domain policy that are not compatible

with MDM and will need to be addressed. The following requirements need to be met before running MMAT in your environment:

1. The latest version of the Remote Server Administration Tools (RSAT) must be installed on the system you will be running MMAT from.
2. Execution is supported on Windows 7, Windows 8, Windows 8.1, and Windows 10.
3. The Invoke-MdmMigrationAnalysisTool.ps1 script needs to be executed from an elevated PowerShell window.
4. The PowerShell execution policy needs to be temporarily bypassed to run the script.



(-) NOT SUPPORTED: Security Account Policies

These Security settings that are configured on the target but not supported by MDM.

Group Policy Name	Group Policy Value	GPO Name	Feedback?
ClearTextPassword	False	Default Domain Policy	☐
MaxClockSkew	5	Default Domain Policy	☐
MaxRenewAge	7	Default Domain Policy	☐
MaxServiceAge	600	Default Domain Policy	☐
MaxTicketAge	10	Default Domain Policy	☐
TicketValidateClient	True	Default Domain Policy	☐

(-) NOT SUPPORTED: Security Options Policies

These Security settings that are configured on the target but not supported by MDM.

Group Policy Name	Group Policy Value	GPO Name	Feedback?
Network security: Do not store LAN Manager hash value on next password change	True	Default Domain Policy	☐
ForceLogoffWhenHourExpire		Default Domain Policy	☐
LSAAnonymousNameLookup		Default Domain Policy	☐

FIGURE 1-2 MDM Migration Analysis Tool (MMAT) results

MORE INFO **MMAT DOCUMENTATION**

At the time of this writing MMAT is still in active development and available on GitHub. For more information about the tool, including where to download it, prerequisites and runtime instructions, visit: *https://github.com/WindowsDeviceManagement/MMAT*.

Configure MDM integration with Azure AD

This section covers how to configure MDM integration with Azure Active Directory (Azure AD). This integration enables you to enroll Windows 10 devices, and is not associated with other platforms, such as iOS and Android. Microsoft has developed a series of protocols in the Windows 10 operating system that are designed to communicate with Azure AD and cloud-based MDM solutions. Furthermore, they have developed an open framework for third-party MDM providers to integrate their solutions with Azure AD. With these components interlinked, administrators can integrate MDM, whether it be Intune or a third-party solution, with Azure AD in an efficient manner. The outcome provides a consistent experience for administrators and end-users.

Plan for MDM integration

Organizations that are starting to take steps toward cloud-based modern management are going to have some new challenges to undertake. In many cases the first obstacle will be an existing on-premises Active Directory domain, with several business applications and processes that have interlinking dependencies. Over the next three sections we will look at steps to help address these early obstacles.

The integration between MDM and Azure AD has a few key prerequisites that you should be familiar with before implementation.

- **Active MDM subscription with a supported provider** During the configuration of MDM, you can select which MDM provider you are going to configure. Intune is there by default and will require a supported subscription to enable. You also have the option to select a third-party MDM provider from the Azure AD app gallery.
- **Configure MDM settings** Once you have obtained a subscription for Intune or an alternative MDM provider, you can start configuring you MDM enrollment settings. These settings include the URLs for MDM terms of use, MDM discovery, MDM compliance, and the scope of devices that will use automatic enrollment.
- **Automatic device enrollment** At a minimum you will need an active Azure AD Premium P1 subscription in order to enable automatic device enrollment. This is an important prerequisite, as most organizations are going to want to leverage automatic enrollment for some portion of their organization. For information about Azure AD pricing, you can visit *https://azure.microsoft.com/en-us/pricing/details/active-directory/*.
- **Configure devices for automatic hybrid domain join with Azure AD and enrollment with Intune** For modern management of devices in MDM, they need to be domain joined with Azure AD. If you have an on-premises Active Directory environment, you can accomplish this by configuring the hybrid Azure AD domain join.

Now that we have reviewed some of the planning considerations prior to configuring MDM integration, let's explore the Azure portal and see where these configurations are located.

1. Sign-in to the Microsoft Azure portal at *https://portal.azure.com/*.
2. Click **All Services**.
3. Search for **Azure Active Directory** and select it.
4. Locate **Mobility (MDM and MAM)** and select it.
5. On the Mobility (MDM and MAM) blade, click **Add Application**. Figure 1-3 shows an example of the third-party MDM applications that are available in the Azure AD app gallery at the time of this writing. Notice there is an option available for an on-premises MDM. This option enables administrators to setup and MDM provider that is not hosted on an Azure tenant.

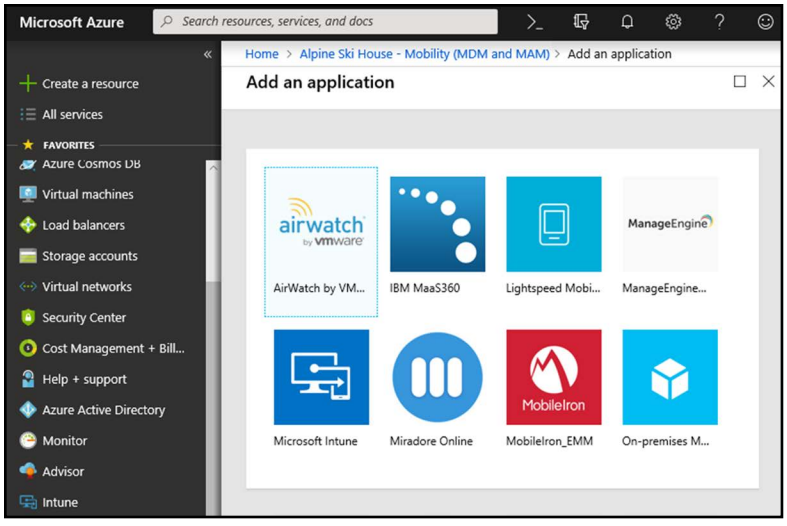


FIGURE 1-3 Azure AD App Gallery for MDM applications

6. Return to the Mobility (MDM and MAM) blade by clicking the navigation link above the **Add An Application** blade.
7. On the Mobility (MDM and MAM) blade, click the **Microsoft Intune** application. If your subscription includes an active Azure AD Premium license then you will reach the MDM and MAM configuration page, as shown in Figure 1-4. Otherwise, you will be presented with the option to sign up for a premium subscription.

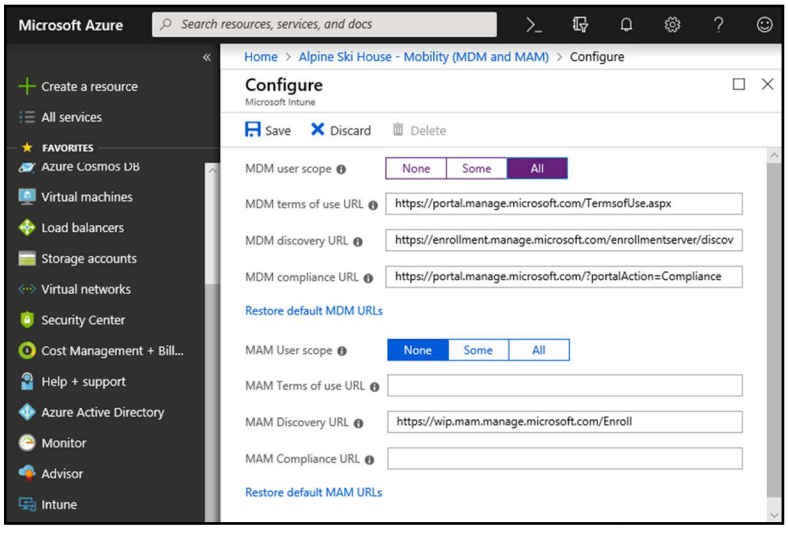


FIGURE 1-4 Azure AD MDM and MAM configuration page

From the configuration page you can define the following MDM settings.

- **MDM user scope** The user scope setting defines the list of users that will be enabled for automatic MDM enrollment. This setting is dependent on the device being joined to Azure AD. You have the option to enable this setting for all users or specify multiple groups.
- **MDM terms of use URL** The terms of use URL is used during manual device enrollment and displays your organization's terms of use to users before a device can be enrolled. The default URL is configured for Microsoft Intune.
- **MDM discovery URL** The discovery URL is used for device enrollment to the MDM. The default URL is configured for Microsoft Intune.
- **MDM compliance URL** The compliance URL is used when a device is found to be non-compliant. This URL displays the compliance issue to the user for further action. The default URL is configured for Microsoft Intune.

At this stage the settings we have reviewed deal primarily with setting up your MDM provider in Azure AD and modifying automatic enrollment for Azure AD joined devices. In the next section we will look at how to setup automatic enrollment using Group Policy or ConfigMgr, but before introducing those options you need to understand some basics about hybrid Azure AD join.

Administrators that manage an on-premises Active Directory domain can leverage configurations in Group Policy or ConfigMgr to enable hybrid Azure AD join and MDM enrollment. Hybrid Azure AD join is a foundational technology for migrating to the cloud. Organizations that have an on-premises domain will use this as a stepping stone to meet future goals and objectives. Before configuring hybrid Azure AD join or device enrollment, there are a few prerequisites to be aware of. For this exam you should be familiar with the following:

- **Azure AD Connect** Azure AD Connect is an application that synchronizes users, groups and computer objects in your on-premises domain with Azure AD.
- **Registration URLs** For hybrid Azure AD join to work, devices in your organization will require communication with Microsoft Azure. The following URLs must be accessible by the devices on your network that will be enrolling:
  - *https://enterpriseregistration.windows.net*
  - *https://login.microsoftonline.com*
  - *https://device.login.microsoftonline.com*

MORE INFO **HYBRID AZURE AD JOIN IN-DEPTH**

For more information about planning your hybrid Azure AD join implementation, visit: *https://docs.microsoft.com/azure/active-directory/devices/hybrid-azuread-join-plan*.

Setup MDM integration using Group Policy

Earlier in this chapter we discussed policy management between Group Policy and MDM. In that scenario we covered two methods for identifying and preventing Group Policy conflicts

when MDM is introduced into an environment. Here we review two Group Policy settings that will assist you in configuring devices for MDM enrollment.

The first policy setting enables administrators to configure automatic hybrid Azure AD join for domain joined devices. This setting is supported on Windows 10 1607 and later. Use the following steps to locate and enable this setting.

> ***NOTE*** **GROUP POLICY PREREQUISITES**
>
> **In these examples use the group policy templates for Windows 10 1803. Earlier versions of the templates may not support these settings. You will also need the Group Policy management console installed on your device before proceeding.**

1. Open the **Group Policy Management Editor**.
2. Create a new Group Policy Object (GPO) and name it "Azure AD Join."
3. Right-click the new GPO and select **Edit**.
4. Under Computer Configuration, expand **Policies**.
5. Expand Administrative Templates.
6. Expand Windows Components.
7. Locate and select **Device Registration**.
8. Locate and edit the policy: Register Domain Joined Computers As Devices.
9. Select the radio button next to **Enabled**, as shown in Figure 1-5.

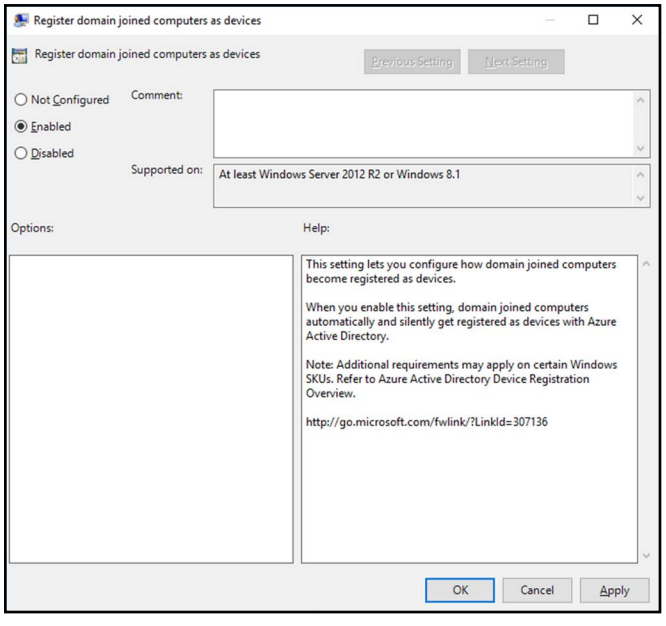


FIGURE 1-5 Group Policy preference editor

10. Click **OK**.

Once configured, you can link this GPO to a domain, site, or Organizational Unit (OU) to enforce hybrid Azure AD join. With the previous prerequisites complete, the targeted devices will join Azure AD. The following setting controls automatic enrollment into MDM. This setting is supported on Windows 10 1709 and later. Use the following steps to locate and enable this setting.

1. Open the **Group Policy Management Editor**.
2. Create a new Group Policy Object (GPO) and call it "Intune MDM Enrollment."
3. Right-click the new GPO and select **Edit**.
4. Under Computer Configuration, expand **Policies**.
5. Expand **Administrative Templates**.
6. Expand **Windows Components**.
7. Locate and select **MDM**.
8. Locate and edit the policy: Enable Automatic MDM Enrollment Using Default Azure AD Credentials.
9. Select the radio button next to Enabled, as shown in Figure 1-6.

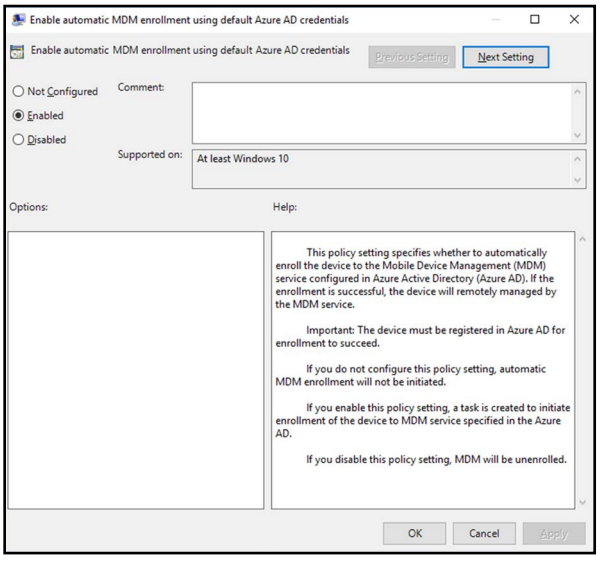


FIGURE 1-6 Group Policy preference editor

10. Click **OK**.

After applying this GPO, supported Windows 10 devices will begin enrolling into the MDM provider that you previously configured at the start of the chapter. For Intune, these devices should start appearing in the Devices blade of the Intune Azure portal.

EXAM TIP

Windows 10 is an evolving operating system. Every six months a new feature update is released unlocking new capabilities. You should be familiar with when major features are introduced. For example, automatic MDM enrollment with Azure AD was not available in the Windows 10 operating system until Windows 10 1709.

Setup MDM integration using ConfigMgr

The policy settings described in the previous section can also be applied with ConfigMgr. The effect on the managed device is often the same, but ConfigMgr offers some additional flexibility for administrators. For example, if you want to test these settings on a small ring of devices, you can explicitly target those devices in ConfigMgr, as opposed to creating a new OU.

ConfigMgr is now releasing major product updates every four months. The features introduced with these updates will account for new features found in the Windows 10 operating system. For example, when MDM automatic enrollment was introduced with Windows 10 1709, support was introduced with ConfigMgr 1710

Here you will see how to enable the comparable settings for hybrid Azure AD join and MDM enrollment with ConfigMgr. This walkthrough assumes you already have a current version of ConfigMgr running in your environment. First, let's examine enabling hybrid Azure AD join.

NOTE **CONFIGMGR VERSION**

These examples use ConfigMgr 1806. Earlier versions of ConfigMgr may not have these options available.

1. Click Start, search for **Configuration Manager Console** and select it.
2. In the Configuration Manager Console, click the **Administration Workspace**.
3. Under Overview, click **Client Settings**.
4. In the ribbon, click **Create Custom Client Device Settings**.
5. On the Create Custom Client Device Settings window, enter **Azure AD join**.
6. Select the **Cloud Services** checkbox and click Cloud Services in the navigation pane.
7. Under Device Settings, choose **Yes** from the dropdown next To **Automatically Register New Windows 10 Domain Joined Devices With Azure Active Directory**, as shown in Figure 1-7.

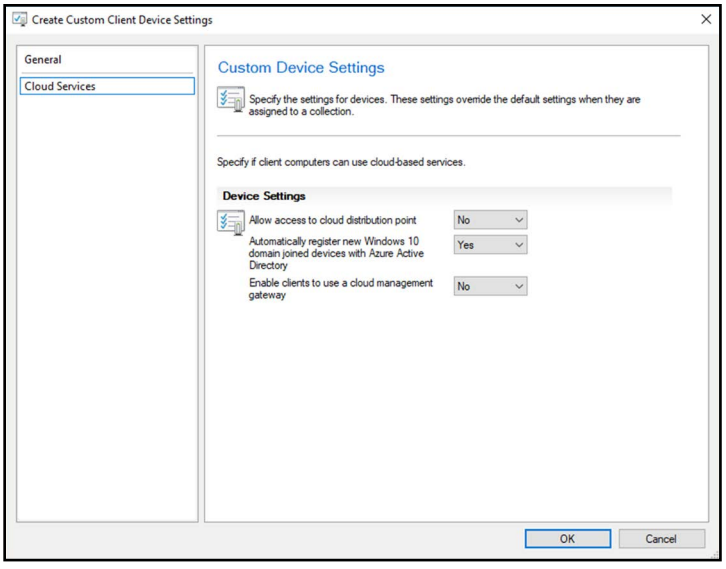


FIGURE 1-7 ConfigMgr custom client device settings

8. Click **OK**.

Before deploying these custom client device settings, be aware that you may need to increase the priority value in comparison to other device settings that are deployed. This will ensure these settings take priority over any conflicting deployments. Next, you can create a device collection with the devices you need to target, followed by a deployment for the custom client device settings.

Automatic MDM enrollment with ConfigMgr is the last configuration setting we will be reviewing in this section. This setting is controlled in the properties for Co-Management, a feature that was first introduced in the 1710 release of ConfigMgr. Because of this, you will need to have Co-Management enabled before you can configure this setting. We will go into more detail on Co-Management in Chapter 3, "Plan for devices and apps." For now, let's examine how automatic MDM enrollment is managed in ConfigMgr.

1. Click Start, search for **Configuration Manager Console** and select it.
2. Click the **Administration Workspace**.
3. Under Overview, expand **Cloud Services**.
4. Click **Co-Management**.
5. Right-click the Co-Management policy and select **Properties** (requires prior configuration of Co-Management).
6. On the Properties window, on the Enablement tab, review the available options in the dropdown for Automatic enrollment in Intune. The following options are available:
   - **None** Selecting this option will disable automatic enrollment. This option is preferred if you are not ready to enable automatic enrollment or you are managing it through another solution, such as Group Policy.

- **Pilot** Selecting this option will enable automatic enrollment for the devices contained in a pilot collection, which you define on the Staging tab of the properties window. This option is preferred if you need to enable automatic enrollment on a select list of devices. If you choose this option, be sure to have your pilot collection created and ready for targeting.
- **All** Selecting this option will enable automatic enrollment for all supported devices managed by ConfigMgr.

7. Select Pilot from the dropdown list. Refer to Figure 1-8 for an example of this setting configuration.

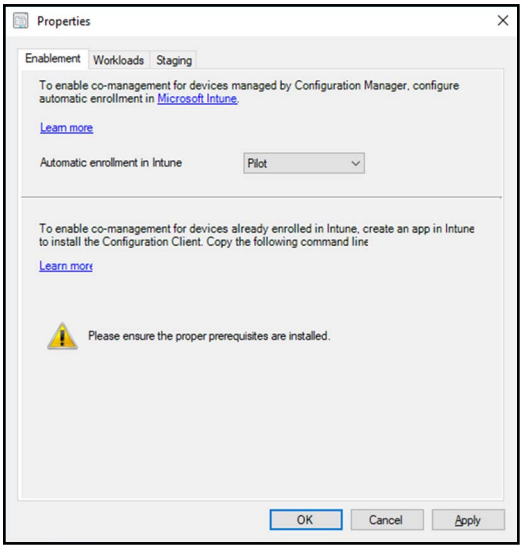


FIGURE 1-8 ConfigMgr Co-management properties

8. Click the **Staging** tab.
9. Under Pilot Collection, click **Browse** and select a device collection that you want to enable automatic enrollment for. This device collection should be closely monitored and only contain devices that you need to enroll.
10. Click **OK**.

EXAM TIP

MDM integration settings in ConfigMgr are not configured from the same location in the management console. Be prepared for questions that test your knowledge of the interface. For example, you are provided with a list of six steps to enable automatic MDM enrollment for Windows 10. You are asked to select the three steps required to accomplish the task and put them in the correct order. Client device settings and Co-Management are both listed as available options and you need to know which interface is the correct one.

Set an MDM authority

For the exam you will need to understand what role the MDM authority plays relative to your overall goals and objectives for device management. As the MDM administrator, you can't enroll any devices until the MDM authority is configured, which highlights this as an important prerequisite. In its simplest form, the MDM authority that you assign determines which interface you will be administering devices from. Microsoft has a few configuration options available, and we will be reviewing each of these in greater detail.

Choose the MDM authority

Previously we discussed the steps for configuring MDM integration. Among those steps we discussed the need for Azure AD join and automatic enrollment, but before you can enable device enrollment you must assign an MDM authority. This is both a technical requirement, associating devices with the solution, but also a literal requirement in that the Intune portal requires an MDM authority defined before you can access other controls in the portal.

When it comes to choosing an MDM authority, the decision is centered around the products you are using in your environment and what subscription model you have chosen. For example, if you have a pre-existing subscription, such as Office 365, then you will have access to MDM for Office 365. At the time of this writing, there are three configuration options for assigning an MDM authority. Table 1-2 shows the breakdown of these options.

TABLE 1-2 Available MDM authorities

MDM Authority	Capabilities	Key Points
Microsoft Intune	Standalone cloud-based MDM No on-premises server requirements Support for all Intune management capabilities	Requires an Intune or EMS subscription Support for Windows 10, Mac OS X, iOS and Android No server management Migration support from on-premises to the cloud using Co-management
Microsoft Intune Hybrid	Integration with on-premises ConfigMgr environment Supports a limited set of Intune capabilities Extended capabilities through ConfigMgr Single pane of glass for managing modern and legacy operating systems	Requires an Intune or EMS subscription Solution is deprecated as of August 2018, support ending September 2019 Limited set of Intune capabilities New capabilities tied to support with ConfigMgr
MDM for Office 365	Cloud-based MDM Integration with Intune Support for a limited set of Intune capabilities	Requires an Office 365 subscription Limited set of Intune capabilities Support for iOS and Android Configured from the Office 365 Admin Center

As mentioned in Table 1-2, at the time of this writing, the Microsoft Intune Hybrid solution is still available to customers. Support, however, will be ending in September 2019. Customers that are using the hybrid MDM solution today will need to start working on a retirement strategy.

Set the MDM authority

Next, we will walk through setting the MDM authority for standalone Intune and MDM for Office 365. While Intune Hybrid is still supported, do not expect to see any exam questions related to setup. The next two sections will include screenshots for the most important elements of the interface, but it is recommended that you follow along in your own lab. These exams will test your knowledge of the management interface.

STANDALONE INTUNE

In this first section we are working with standalone Intune. For this example, we are working in an environment where the MDM authority has not been configured yet.

1. Sign-in to the Microsoft Azure portal at *https://portal.azure.com/*.
2. Click **All Services**.
3. Search for **Intune** and select it.
4. Under manage, click **Device Enrollment**. Review the Device enrollment blade in Figure 1-9. Notice that the MDM authority field is blank, and the account status is active. Without an MDM authority assigned, the Choose MDM Authority blade will open automatically.

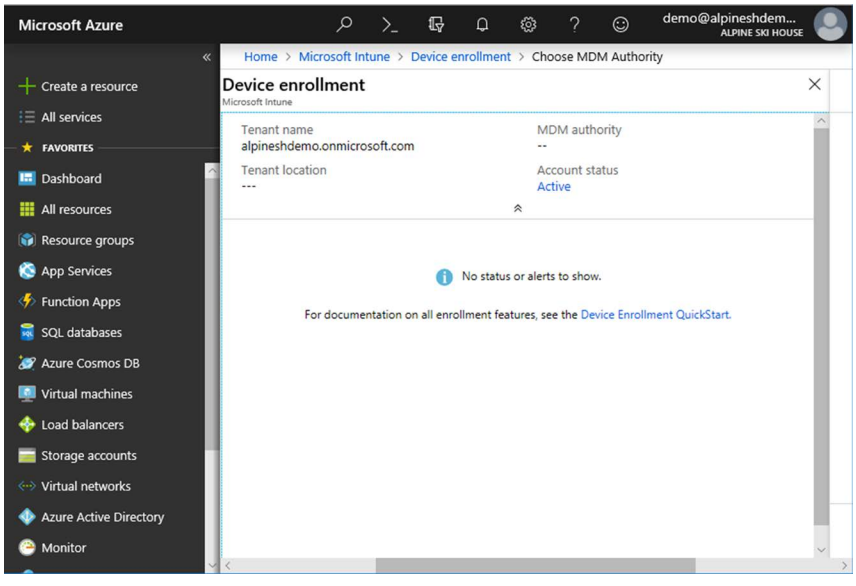


FIGURE 1-9 Device enrollment blade

5. On the Choose MDM Authority blade, select the radio button next to Intune MDM Authority, as shown in Figure 1-10.

NOTE **CONFIGURATION MANAGER MDM AUTHORITY**

On the Choose MDM Authority blade, review the option for Configuration Manager MDM Authority. This is referencing the Intune Hybrid configuration, which is covered in the next section. For now, know that if you select this option in your environment, the Intune portal will direct you to the ConfigMgr console.

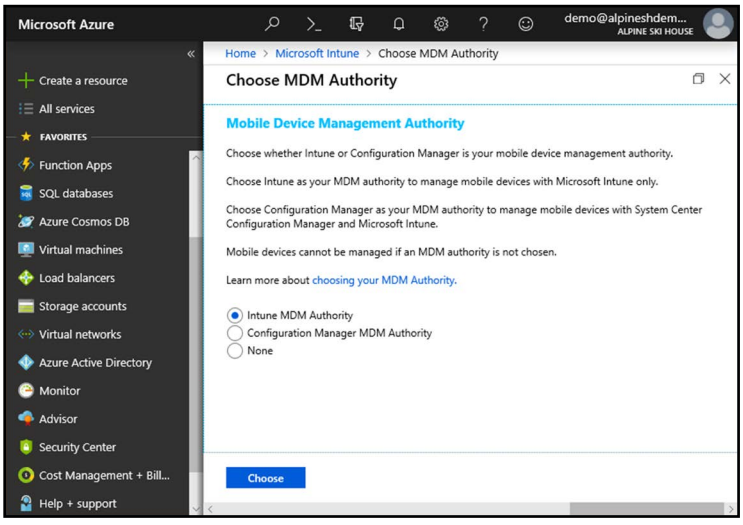


FIGURE 1-10 Choose MDM Authority blade

6. Click **Choose** to complete the configuration.
7. Review the Azure portal notifications to confirm that the MDM Authority was successfully chosen (see Figure 1-11).

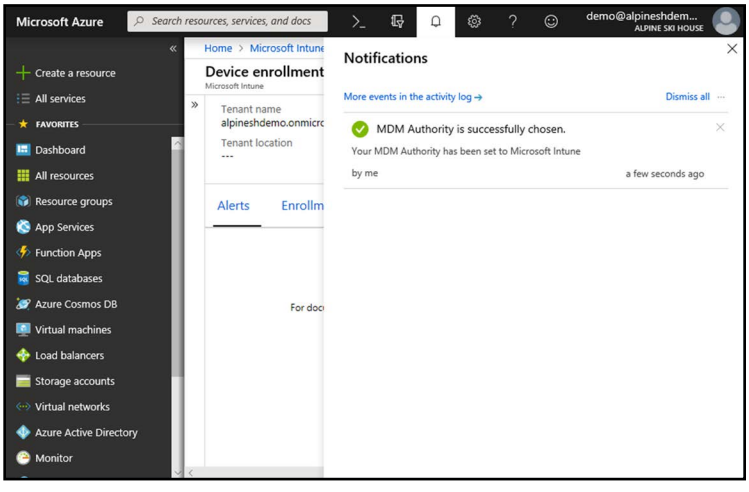


FIGURE 1-11 Azure Portal Notifications

MDM FOR OFFICE 365

1. Unlike standalone Intune, the MDM for Office 365 configuration change is done through the Microsoft 365 admin center. Sign-in to the Microsoft 365 admin center at *https://admin.microsoft.com/*.
2. On the Home page, type **mobile device management** in the search field and select it from the list of available options.
3. On the Set up Mobile Device Management for Office 365 page, review the list of available features, as shown in Figure 1-12. Click **Let's Get Started**. This will start the setup process and can take a few hours to complete.

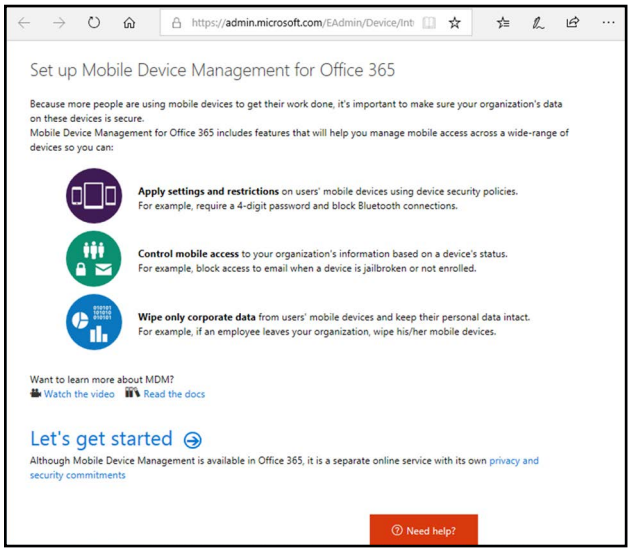


FIGURE 1-12 Set up MDM for Office 365

4. Once setup is complete, click **Manage Devices** or navigate to *https://admin.microsoft.com/adminportal/home#/MifoDevices*. All device management tasks will take place from the Microsoft 365 admin center.
5. To verify your MDM authority is set, sign-in to the Microsoft Azure portal at *https://portal.azure.com/*.
6. Click **All Services**.
7. Search for **Intune** and select it.
8. Under Manage, click **Device Enrollment**. Note that the MDM authority now shows Office 365.

Change the MDM authority

There are two scenarios where an administrator can change their MDM authority. These include the following.

- **Intune Hybrid** In this scenario an administrator can change the MDM authority from standalone Intune to ConfigMgr, or from ConfigMgr to standalone Intune. Both of these actions are completed in the ConfigMgr management console.
- **Office 365** In this scenario an administrator can change the MDM authority from Office 365 to standalone Intune. This action is completed in the Azure portal.

INTUNE HYBRID

For this example, we are going to walk through changing the MDM authority from ConfigMgr to standalone Intune. This walk through assumes that your environment already has ConfigMgr set as the MDM authority and an active Intune subscription is configured in the ConfigMgr management console.

> ***NOTE*** **CONFIGMGR VERSION**
>
> **In this example we will be using ConfigMgr 1806. Earlier versions of ConfigMgr may not have these options available.**

1. Click Start, search for **Configuration Manager Console** and select it.
2. Click the **Administration Workspace**.
3. Under Overview, expand **Cloud Services**.
4. Click **Microsoft Intune Subscriptions**.
5. Select the **Microsoft Intune** subscription. From the ribbon, click **Delete**.
6. On the Remove Microsoft Intune Subscription Wizard, review the available options (see Figure 1-13). Note that you have the option to remove the Intune subscription or change the MDM authority. Select the radio button next to **Change MDM Authority to Microsoft Intune** and click **Next**.

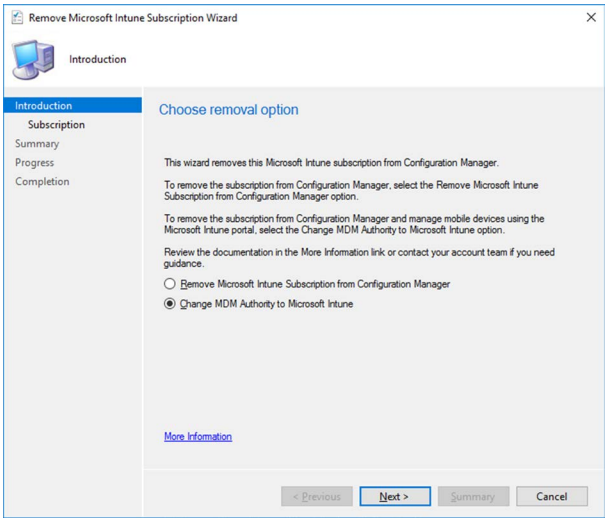


FIGURE 1-13 Remove Microsoft Intune Subscription Wizard

7. Review the warning presented before changing the MDM authority, as shown in Figure 1-14. This change will shift management from the ConfigMgr console to the Intune portal, and existing applications or policies will need to be recreated in Intune. Click **Yes**.

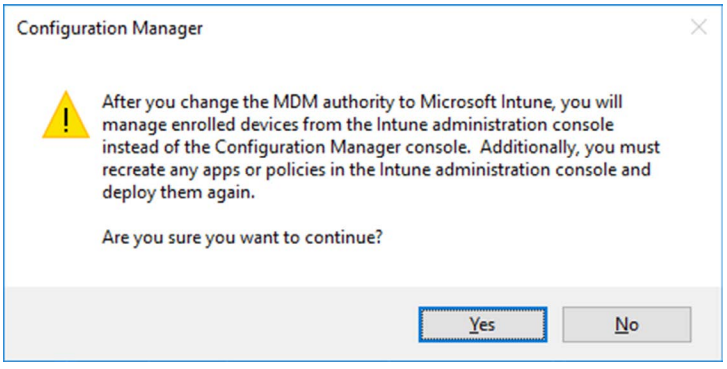


FIGURE 1-14 Change MDM Authority Warning

8. On the Subscription page, enter your credentials to sign-in to Microsoft Intune and click **Next**.
9. On the Summary page, review the requested changes and click **Next**.
10. On the Completion page, click **Close**.
11. To verify your MDM authority has changed, sign-in to the Microsoft Azure portal at *https://portal.azure.com/*.
12. Click **All Services**.
13. Search for **Intune** and select it.
14. Under Manage, click **Device Enrollment**. Note that the MDM authority now shows Intune.

OFFICE 365

For this example, we are going to walkthrough changing the MDM authority from Office 365 to standalone Intune. This walkthrough assumes that your environment already has MDM for Office 365 set as the MDM authority and that you have an active Intune subscription.

1. Sign-in to the Microsoft Azure portal at *https://portal.azure.com/*.
2. Click **All Services**.
3. Search for **Intune** and select it.
4. Under manage, click **Device Enrollment**. With Office 365 set as the MDM authority, you will automatically be taken to the Add MDM Authority blade, as shown in Figure 1-15.

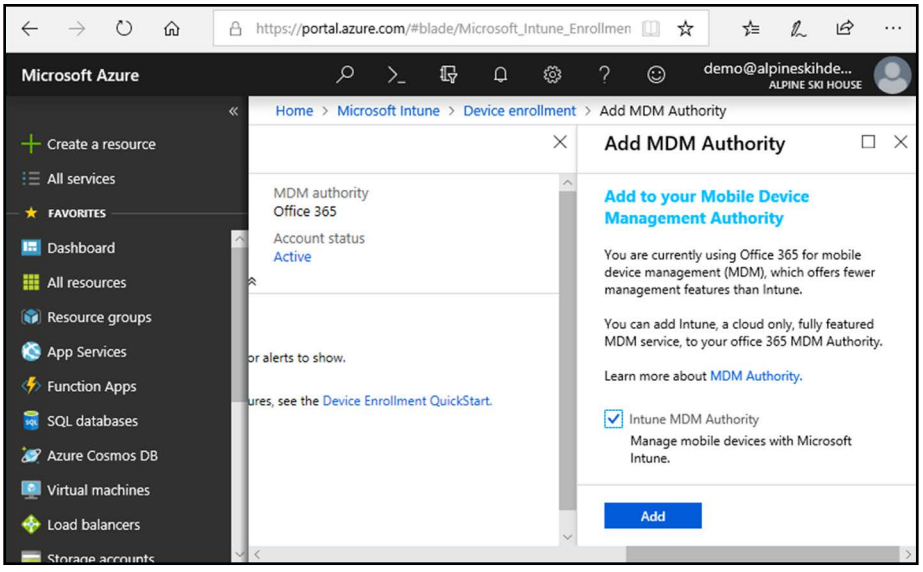


FIGURE 1-15 Add MDM Authority blade

5. Check the box for **Intune MDM Authority** and click **Add**.
6. Review the Azure portal notifications to confirm the MDM Authority was successfully changed to Intune (see Figure 1-16).

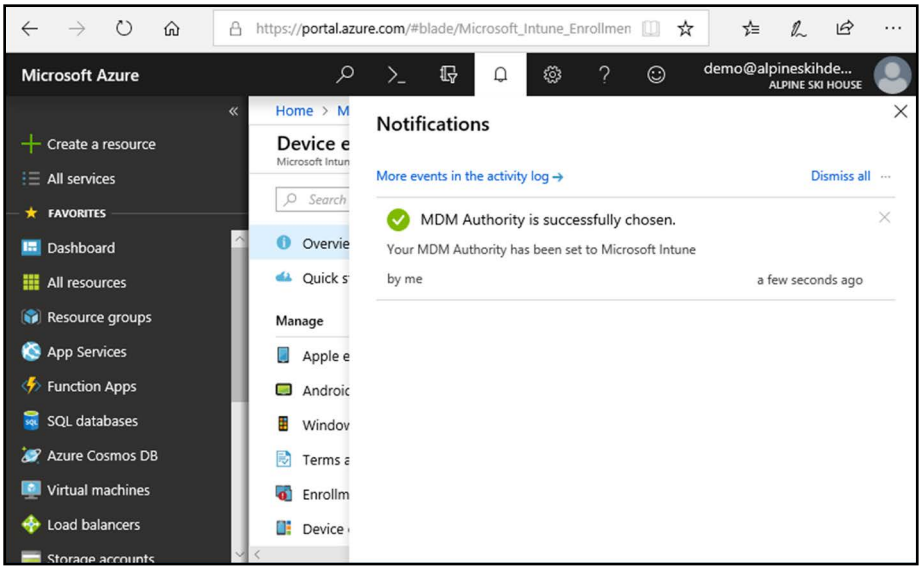


FIGURE 1-16 Azure Portal Notifications

Set device enrollment limit for users

This section covers the controls given to administrators to limit the number and type of devices a user can enroll. Why would you need to setup device enrollment restrictions for MDM? Limiting the number of devices assigned to a user can help with license constraints and organization. Restricting devices that are running an older operating system is a requirement for many organizations due to security and compliance. Blocking personally-owned devices may be a scenario you need to consider if your organization is not ready to support Bring Your Own Device (BYOD). These are a few of the examples that we'll be reviewing.

Plan for device enrollment restrictions

We have covered three MDM solutions in this chapter, and each of them has some basic ability to restrict device enrollment. Hybrid Intune and MDM for Office 365, however, cannot leverage the same enrollment restrictions available in standalone Intune. There are additional capabilities available beyond limiting the number of devices a user can enroll. For this section we will focus on the controls in the standalone Intune solution. Table 1-3 describes each of the restriction types and what their capabilities are.

TABLE 1-3 Device Enrollment Restrictions

Restrictions	Restriction Type	Description
Maximum number of enrolled devices	Limit restriction	Restrict the number of devices a user can enroll, ranging from 1 to 15.
Allow or block based on device platforms	Type restriction	Restrict device enrollment by device platform, including Android, Android work profile, iOS, Mac OS, and Windows (MDM).
Allow or block based on platform operating system	Type restriction	Restrict device enrollment by operating system, providing a minimum and maximum version number.
Allow or block personally owned devices	Type restriction	Restrict device enrollment by corporate-owned, requiring additional steps to define a device as corporate-owned.

NOTE **PERSONALLY OWNED DEVICES**

The ability to allow and block personally owned devices is dependent on other factors in your MDM configuration. For Windows (MDM), if the device was previously enrolled through a bulk provisioning package, ConfigMgr Co-Management or Windows Autopilot, it will be allowed to enroll.

Set device enrollment restrictions

With a high-level understanding of the possible enrollment restrictions, let's examine the interface and explore the controls. Device enrollment restrictions are available in the Azure portal under the Microsoft Intune service.

DEVICE LIMIT RESTRICTION

In this walk-through, we will implement a restriction to limit the number of devices a user can enroll with.

1. The first enrollment restriction covered focuses on limiting the number of devices a user can enroll. Sign-in to the Microsoft Azure portal at https://portal.azure.com/.
2. Click **All Services**.
3. Search for **Intune** and select it.
4. Under Manage, click **Device Enrollment**.
5. On the Device Enrollment blade, under Manage, click **Enrollment Restrictions**.
6. On the Device Enrollment – Enrollment Restrictions blade, review the items under Device Type Restrictions and Device Limit Restrictions. Refer to Figure 1-17 for an example. Take note that there is a default enrollment restriction for each restriction. Both can be modified, but not deleted.

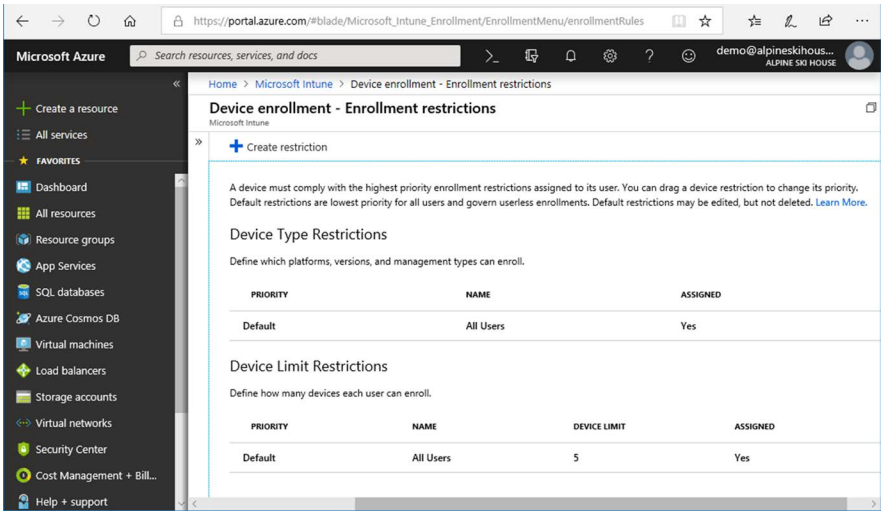


FIGURE 1-17 Device enrollment – Enrollment Restrictions

7. Click **Create Restriction**.

8. On the Create Restriction blade, fill in the following:
   A. **Name** Custom device limit
   B. **Restriction Type** Device Limit Restriction
   C. **Specify The Maximum Number Of Devices A User Can Enroll** 3
9. Click **Create**.
10. Review the Azure portal notifications to confirm that the new enrollment restriction was created successfully.

At this stage you will have a new custom device restriction created and available on the Device Enrollment – Enrollment Restrictions blade. Here we worked with limit restrictions. Assigning a limit prevents users from enrolling more than the defined value. The default restriction allows users to enroll up to five devices. Attempting to enroll more than five will result in a notification. Now let's take a look at Device Type Restrictions.

DEVICE TYPE RESTRICTIONS

The second enrollment restriction we will work with is based on limiting enrollment by the type of device.

1. Sign-in to the Microsoft Azure portal at *https://portal.azure.com/*.
2. Click **All Services**.
3. Search for **Intune** and select it.
4. Under Manage, click **Device Enrollment**.
5. On the Device Enrollment blade, under Manage, click **Enrollment Restrictions**.
6. On the Device Enrollment – Enrollment Restrictions blade, click **Create Restriction**.
7. On the Create restriction blade, fill in the following:
   A. **Name** Custom type limit
   B. **Restriction Type** Device Type Restriction
8. Click **Select Platforms**.
9. On the Select Platforms blade, select the following options, as shown in Figure 1-18:
   A. **Android** Block
   B. **Android Work Profile** Block
   C. **iOS** Allow
   D. **macOS** Block
   E. **Windows (MDM)** Allow

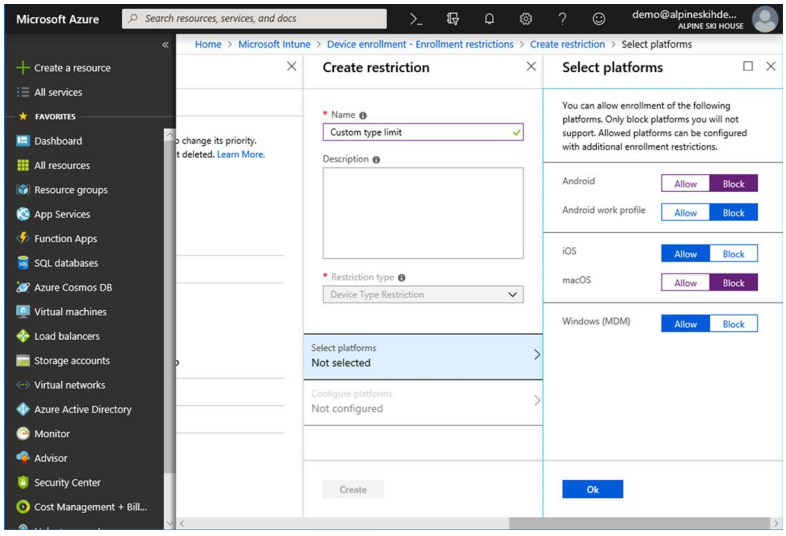


FIGURE 1-18 Create Restriction – Select Platforms

10. Click **OK**.
11. On the Create Restrictions blade, click **Configure Platforms**.
12. On the Configure Platforms blade, fill in the following, as shown in Figure 1-19:
    - **A. iOS Min Version** 12.0
    - **B. iOS Personally Owned** Block
    - **C. Windows (MDM) Min Version** 10.0.17134.345
    - **D. Windows (MDM) Personally Owned** Block

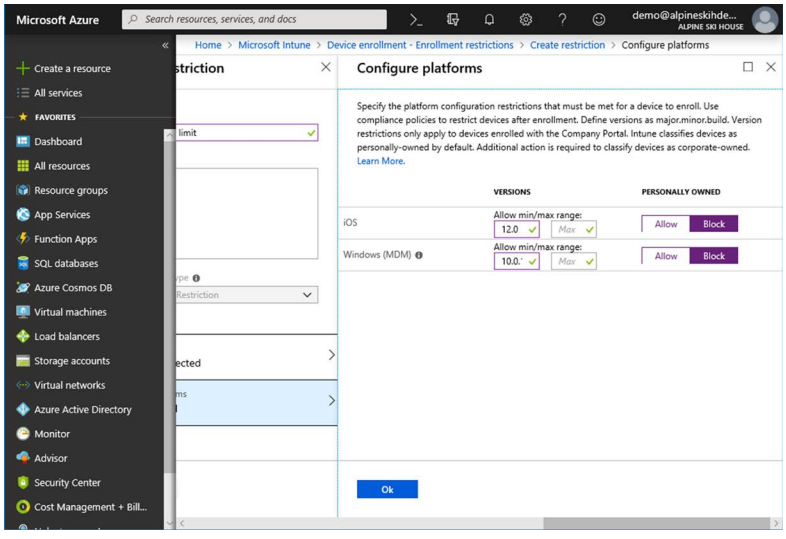


FIGURE 1-19 Create Restriction – Configure Platforms

13. Click **OK**.
14. Click **Create**.
15. Review the Azure portal notifications to confirm that the new enrollment restriction was created successfully.

With these steps complete, you should now have a custom device type restriction available on the Device Enrollment – Enrollment Restrictions blade. In this example we worked with platform restrictions. Platform restrictions provide a granular set of controls for approving specific device types and operating system versions. With an enrollment plan that supports BYOD, controlling the minimum and maximum operating system version can prevent known vulnerabilities or pre-release versions from entering your environment.

ASSIGNMENT

Let's examine the process for assigning enrollment restrictions. First, you need to understand the priority system. The priority value, shown on the Device Enrollment – Enrollment Restrictions blade, is for users that are members of multiple groups, but may have different enrollment restrictions assigned. You can change the priority value in the portal by dragging a device restriction up or down the list.

> ***REAL WORLD*** **DEVICE RESTRICTION PRIORITIES**
>
> **Ethan Rincon is a member of two Azure AD groups, IT and All Employees. The IT group has device enrollment restrictions that allow members to enroll all device types. This device restriction has a priority of 1. The All Employees group has device enrollment restrictions that only allow members to enroll Windows (MDM) devices. This device restriction has a priority of 2. In this situation Ethan will receive the IT device restrictions due to the higher priority.**

Enrollment restrictions are assigned to Azure AD groups. The following walkthrough assumes you already have an Azure AD group created with the users you need to target.

1. Sign-in to the Microsoft Azure portal at *https://portal.azure.com/.*
2. Click **All Services**.
3. Search for **Intune** and select it.
4. Under Manage, click **Device Enrollment**.
5. On the Device Enrollment blade, under Manage, click **Enrollment Restrictions**.
6. On the Device Enrollment – Enrollment Restrictions blade, select the custom device limit restriction that was previously created.
7. On the Custom Device Limit blade, click **Assignments**.
8. On the Custom Device Limit – Assignments blade, click **Select Groups**.
9. Select an Azure AD group that you want to target and click **Select**, as shown in Figure 1-20.

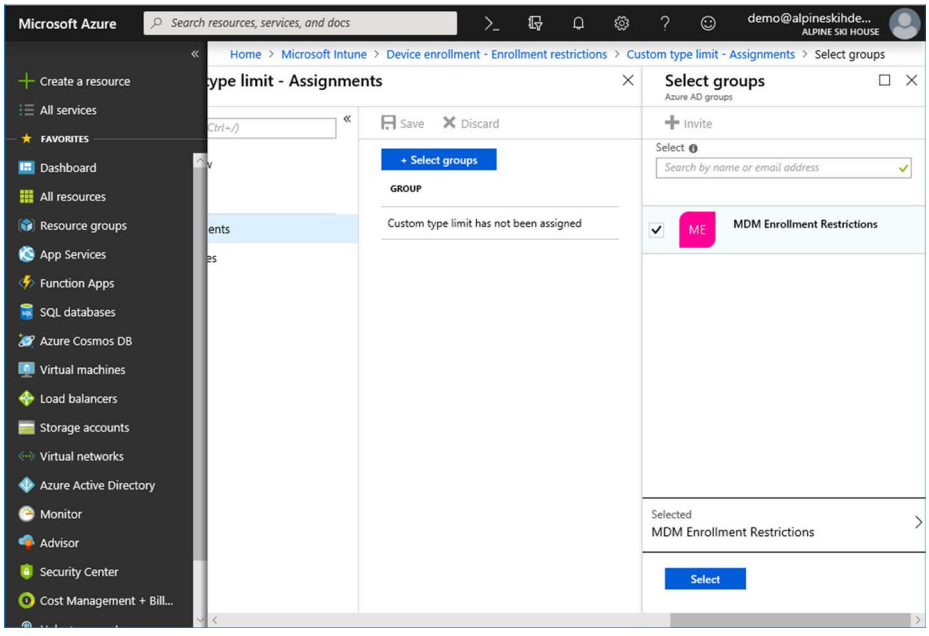


FIGURE 1-20 Enrollment Restriction Assignment

1. On the Custom Device Limit – Assignments blade, click **Save**.
2. Review the Azure portal notifications to confirm the device enrollment restriction was successfully assigned.

Once you have completed these steps you should have the device restrictions available in the portal and assigned to an Azure AD group of your choosing.

Skill 1.2: Manage device compliance

Device compliance is the practice of ensuring that the devices accessing your environment meet a distinct set of requirements, often defined by the IT and cybersecurity teams in your organization. For the purpose of this exam, device compliance is also referred to as a feature in Microsoft Intune. This feature is provided to aid administrators in defining their compliance requirements and using them to delegate access to data and services. As an administrator, it is your job to understand the use cases for device compliance and how to implement them.

The compliance policies that you define make up the connective tissue for several other actions in the platform. For example, the compliance status of a device can be leveraged as a determining factor for granting access to Exchange Online. This is accomplished using conditional access policies, another key feature covered in this chapter. Conditional access policies are a different type of policy, managed within Azure Active Directory (Azure AD), for allowing and denying access to data and services.

This section covers the following topics:

- Plan for device compliance
- Design Conditional Access Policies
- Create Conditional Access Policies
- Configure device compliance policy
- Manage Conditional Access Policies

Plan for device compliance

This skill section covers planning considerations for device compliance. This includes topics such as prerequisites before implementation, compliance workflows, and possible use cases for your organization. Later in this chapter you will work with conditional access policies, and one of the dependencies for conditional access is the compliance status of the end user device. The MS-101 exam will present scenarios dealing with Intune enrollment, device compliance, and conditional access. As you prepare, take time to work with these technologies in the Azure portal and see what the dependencies are.

Understand the prerequisites for device compliance

Before you get started with creating device compliance policies, there are some technical prerequisites to plan for. Throughout this book you will see some trending prerequisites for each of the cloud technologies, particularly around the required subscriptions. Keep an eye on these for the exam and take some extra time to understand which features are included with the various subscription models.

These are the prerequisites for device compliance:

- **Subscriptions** Device compliance is a technology with dependencies on Azure AD and Microsoft Intune. The device must be enrolled in Intune to receive a compliance policy, and the compliance flag is written to Azure AD for other features, such as conditional access. At a minimum you need a standalone Intune subscription and an Azure AD Premium P1 subscription. The higher tiered subscriptions, such as Azure AD premium P2, do not include additional capabilities focused on device compliance.
- **Platform support** Device compliance policies support a wide range of platforms. For clarification, the term platform is referring to the operating system, not the physical hardware. Platform support is an important prerequisite if you are planning to manage devices that are not supported. At the time of this writing the following platforms are supported:
  - Android
  - Android Enterprise
  - iOS
  - macOS

- Windows Phone 8.1
- Windows 8.1
- Windows 10

- **Enrollment** Devices cannot report compliance until they are enrolled in Microsoft Intune.

MORE INFO **CHOOSING A SUBSCRIPTION**

For more information about the different editions of Azure AD and their corresponding subscription tier, visit: *https://azure.microsoft.com/en-us/pricing/details/active-directory/*. For more information about the subscriptions pertaining to Microsoft Intune, visit: *https://www.microsoft.com/en-us/cloud-platform/microsoft-intune-pricing*.

Understand the process flow for device compliance

Device compliance and conditional access are both policy-based technologies. You configure the policy to address your needs, and then assign that policy to the desired resources in Microsoft Intune. Devices will evaluate the policy and report back whether they meet the requirements or not. The compliance state is then written to the device object in Azure AD as a custom attribute. The state of that attribute will determine if the device is approved to access data and services. This is where conditional access enters the picture, which is covered in more detail later in this chapter.

Refer to Figure 1-21 for a diagram that illustrates the device compliance flow. In this example we are using the default configuration for device compliance. As an administrator, you have a few options to change this flow to meet your needs.

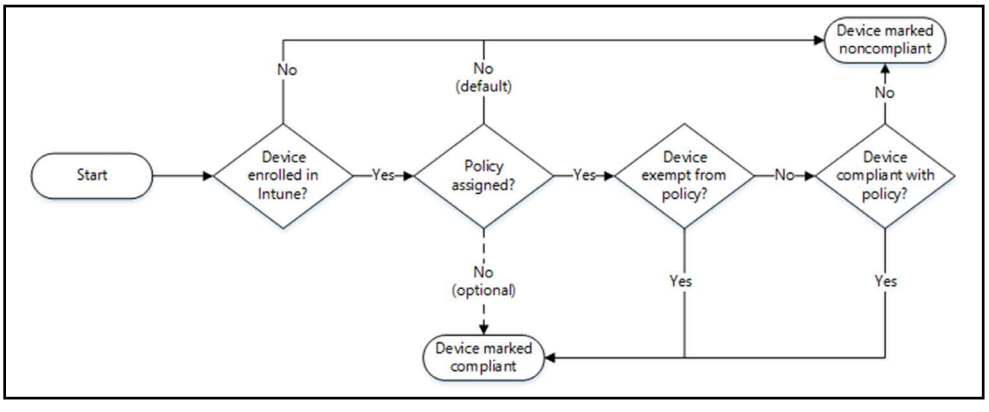


FIGURE 1-21 Device Compliance Process Flow

These next few items address controls that an administrator has available to alter the device compliance flow.

- **Intune enrollment** Devices that are not enrolled in Intune cannot receive device compliance policies. This rule also applies to devices that are Azure AD joined. This was covered earlier in the prerequisites section. In this context it can also be used to prevent compliance policies from applying to unmanaged devices.
- **Policy assignment** In the compliance policy settings for Microsoft Intune, you have the option to mark devices as compliant if they do not have a policy assigned. By default, all devices without an assigned policy are marked as noncompliant. But you do have the option to change this behavior, making all devices compliant by default. This is represented by the dashed line between the policy assigned and the device marked compliant in the illustration, also marked as optional.
- **Device exemption** Device exemption is another control you can configure. This is accomplished in the policy settings by defining which device platforms the compliance policy is scoped for. If your compliance policy includes all platforms except iOS, then iOS devices will be exempt from running that policy.

EXAM TIP

As you prepare for this exam, spend time looking at each of the device compliance options in the Intune portal. In this last section we reviewed the default behavior for devices that have no policy assigned. You may see questions that test your knowledge about the default behavior for device compliance policy, or where to change that behavior under certain circumstances.

Determine use cases for device compliance

In this section we are going to look at some potential use cases for device compliance. First, understand that compliance policies contain a series of rules that you define. These rules determine whether a device is compliant or not. Compliance policies can help to remediate certain conditions, but in most cases the device will be quarantined, and remediation will be left up to the user. For example, you have a device compliance policy that has a security rule that requires a password before unlocking a device. If a device is noncompliant with this policy, the user will be prompted to set a password on their noncompliant device.

Users with devices that are marked as noncompliant will receive notifications about the conflicting rules. As an administrator, you can also create a conditional access policy to block these devices until they are remediated. Refer to Table 1-4 for a series of compliance policies and corresponding use cases.

TABLE 1-4 Device Compliance Use Cases

Platform	Setting(S)	Example Use Case
Windows 10	Minimum OS version Valid operating system builds	Windows 10 devices that are not running the latest cumulative update are marked as noncompliant. Windows 10 devices running the latest release of 1709 are still valid while upgrades are rolling out.
macOS	Require system integrity protection	macOS devices that do not have system integrity protection enabled are marked as noncompliant.
Android	Rooted devices Encryption of data storage on device	Android devices that are rooted are marked as noncompliant. Android devices that do not have data storage encryption enabled are marked as noncompliant
iOS	Jailbroken devices Minimum OS version Restricted apps	iOS devices that are jailbroken are marked as noncompliant. iOS devices that are not running the latest major release of iOS are marked as noncompliant. iOS devices that have the Dropbox app installed are marked as noncompliant.

Design conditional access policies

In this skill section you will review the design aspects of conditional access policies. It is worth pointing out that a majority of this chapter is dedicated to conditional access: designing, creating, and managing policies. As you prepare for these skills plan to spend time working in the Azure portal and following along to review the interface and controls for conditional access.

This chapter began by covering what device compliance means from a cloud management perspective. Now you will see how device compliance is used to establish access requirements for data and services in your organization.

Design for the protection of data and services using conditional access policies

There are a variety of policy settings available for conditional access, and a mixture of configurations that you can implement. Let's first look at the Conditional Access Policies blade in the Azure portal. This will help set the stage for conditional access policies and introduce you to some key terms. Refer to Figure 1-22 for an example of the Policy Creation blade, as we drill down and take a closer look at each of the available options.

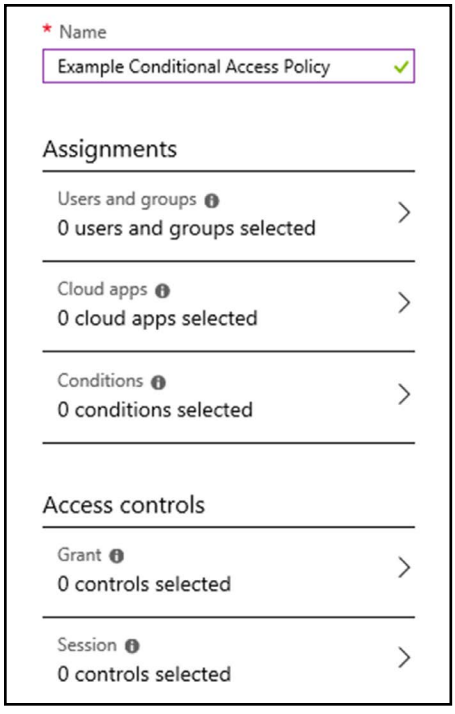


FIGURE 1-22 Conditional Access Policy Creation

- **Assignments** Assignments define the scope, criteria and conditions of the policy you are deploying. On the Policy Creation blade you are presented with three categories under assignments. These three categories include:
- **Users And Groups** They define who will receive the policy. You can either include or exclude users and groups. Although the creation screen will not prevent you from proceeding, all conditional access policies require a user and group assignment before it is applied. For includes you can select all users or specific users and groups. For example, if you have a group that only contains your marketing team you can select that as an option. For excludes you can select all guest users (defined by the userType attribute), specific directory roles such as "Application developer," or specific users and groups.
- **Cloud Apps** They define the services that users will access for productivity. You have the choice to include or exclude a pre-defined list of supported cloud apps. For includes you can select all cloud apps or specific apps, such as Microsoft Teams. For excludes you can select specific apps.
- **Conditions** They define when a policy is applied. Refer to Table 1-5 for a breakdown of each condition, the available options, and some example use cases.

TABLE 1-5 Conditional Access Options

Condition	Description	Options	Example Use Case
Sign-in risk	Azure AD determines a user's sign-in risk based on a configurable policy under Azure AD Identity Protection.	High, medium, low, or no risk	Enforce a MFA policy for users that are flagged with a medium sign-in risk.
Device platforms	Azure AD retrieves the operating system of joined device, but the information is not verified. This should be combined with a Microsoft Intune enrollment and device compliance policy.	Android, iOS, Windows Phone, Windows, macOS	Enforce an app restriction policy on iOS and Android devices only.
Locations	Locations are used to define trusted network locations. Trusted network locations are configured in Azure AD under Named Locations.	Trusted locations	Block access to Exchange online from the San Francisco office with an IP subnet of 10.20.11.0/22
Client apps (preview)	Set conditional restrictions based on specific client apps.	Browsers, mobile apps and desktop clients	Restrict access to mobile apps unless the device is marked as compliant.
Device state (preview)	Exclude corporate or trusted devices from conditional access restrictions	Hybrid Azure AD joined devices, devices marked as compliant	Enforce restrictions to Office 365 Exchange Online for noncompliant devices.

- **Access controls** They define additional requirements for granting or denying access, along with session controls for limiting the experience within cloud apps. The following options are available from the access controls section:
- **Grant** It enables you to block access based on the conditions that you defined under the assignments section. Alternatively, you can choose to grant access and enforce additional requirements. For example, you can require MFA or only grant access to devices that are marked as compliant through device compliance policies.
- **Session** This control enables you to limit the experience within certain cloud apps. At the time of this writing, Exchange Online and SharePoint Online are the only cloud apps that support app enforced restrictions. Enabling this feature adds real-time monitoring and control capabilities to these apps.

Now that you have spent some time exploring the interface, let's look at how a conditional access policy is constructed. The policy is made up of two parts: the condition and the access control. You can also look at these in the following context: *when this happens* (condition), *then do this* (access control). For the exam you should be familiar with this formula and how it corresponds to conditional access restrictions. Refer to Table 1-6 for a few examples on how conditional access policies are assembled.

TABLE 1-6 Conditions and access controls

When This Happens (Condition)	Then Do This (Access Control)
Windows and macOS device owners are accessing SharePoint Online from an untrusted network. Additional security requirements are needed.	Grant access to SharePoint Online for Windows and macOS devices. Require multi-factor authentication and a compliant device when accessed from an untrusted network.
The sales team is accessing Exchange Online from their iOS and Android devices. These devices need to be compliant before access is granted.	Grant access to Exchange Online for the sales group. Require all sales team device owners to be enrolled in Intune and marked as compliant.
All users are accessing Microsoft Teams from trusted and untrusted networks. Users that are on an untrusted network need additional security requirements.	Grant access to Microsoft Teams for all users. Require multi-factor authentication when accessed from an untrusted network.
BYOD devices are accessing Exchange Online from their browser. Access needs to be restricted to approved apps.	Grant access to Exchange Online for all users. Restrict access to trusted client apps only.

The following list covers prerequisites that you need to be familiar with. Some of these are firm requirements and others are strategic questions to help prepare you for designing policies.

- **Subscriptions** The basic capabilities of conditional access are available with an Azure AD premium subscription. There are additional capabilities, however, that will not be available until you upgrade your subscription. These include the following:
  - **Azure AD Premium P1** The P1 subscription provides you with the basic capabilities of conditional access policies.
  - **Azure AD Premium P2** The P2 subscription enables identity protection, which is a requirement if you want to leverage sign-in risk. Sign-in risk is a capability that determines if a user sign-in is malicious and measures the risk level. This can be leveraged as part of your policy conditions.
  - **Microsoft Intune** Intune can be purchased standalone or through an EMS E3 or E5 subscription. Policy definitions that require a compliant device are dependent on the device being enrolled in Intune.

MORE INFO **SUBSCRIPTION DETAILS**

For more information about Azure AD subscriptions, visit: *https://azure.microsoft.com/pricing/details/active-directory/*. For more information about Microsoft Intune subscriptions, visit: *https://www.microsoft.com/cloud-platform/microsoft-intune-pricing*.

- **Permissions** Before you can start creating and managing conditional access policies, you will need the appropriate permissions assigned to your account. Conditional Access Administrator is a pre-defined role that that enables the necessary privileges.

- **Requirements to be delivered** What requirements do you have for device compliance and conditional access? This is something you should start defining from the beginning. Determine if your goal is something straightforward, such as enforcing multi-factor authentication for users. Or something more advanced, such as restricting access to SharePoint Online from Windows devices when they are connected to an untrusted network.
- **Device management** What kind of device management solution are you using today? The full capabilities of conditional access do have dependencies on Microsoft Intune, but if you are using ConfigMgr, you can enable co-management and start leveraging conditional access policies sooner.
- **Device platforms** What types of devices and operating systems do you need to support? Conditional access policies support a variety of operating systems. At the time of this writing, the only current outliers are devices running Linux. Consider the devices in your environment and what type of restrictions you need to enforce.
- **Email requirements** What are your access requirements around email? Email is often used as one of the first services for enforcing conditional access restrictions. If you have a goal to enable access restrictions for Exchange Online, then selecting the cloud app from the default list of assignments is straightforward, and something we will look at later in this chapter. If you have a goal to enable access restrictions for an on-premises Exchange server, you will need to plan for additional prerequisites, such as installing and configuring the on-premises Exchange connector.

NOTE **PREVIEW FEATURES**

New features are introduced on a monthly basis to the Azure portal. Some features are not fully production ready and will be introduced in a preview format, enabling you and other customers to try them and provide feedback to the developers. Elements in the portal that are in a preview state will be marked with "preview" following the name of the feature. For example, "Device state (preview)" is one of the features discussed in this skill section. At the time of this writing, there are features in a preview state and these may change over time. Keep these in mind and be sure to stay up to date on these features as you prepare for the exam.

Design device-based and app-based conditional access policies

First, understand that a conditional access policy can contain any mixture of options, including device-based and app-based restrictions. The distinction between device-based and app-based restrictions is relative to the controls that you select and how you structure your policies. That said, device-based and app-based policies can have different requirements and can operate independently of each other if you choose.

Let's look at a few examples:

- **Device-based** This first policy focuses on device-based controls. In this example the policy requires multi-factor authentication on untrusted networks for iOS devices.

The policy is assigned to all users. In this example we have not defined any app-based restrictions, keeping the focus on the platform and network.

- **App-based** This second policy focuses on app-based controls. In this example the policy requires approved client apps when accessing Exchange Online. This policy is assigned to all users. In this example we have not defined any device-based restrictions, keeping the focus on application controls.
- **Mixed** This third policy includes a mixture of controls. In this example the policy requires all platforms to be enrolled in Intune and marked compliant before they can access Exchange Online from approved client apps. In this example we are specifying device-based restrictions and app-based restrictions to accomplish the desired result.

At this stage you should have a good understanding of the differences between device-based and app-based policies. Next, let's examine the individual controls related to each policy type. The following items are focused on device-based policy requirements:

- **Azure AD joined** This requirement is available as both a condition and an access control item. When you are defining a condition, you have the option to exclude devices that are Azure AD joined. This is available through the device state blade and can be used in a scenario where you are locking down access, but want to ignore Azure AD joined devices. Alternatively, when you are defining the controls for granting access, you have the option to require Azure AD joined devices. This is available through the grant blade for access control and can be used as one of many required controls before enabling access to cloud apps.
- **Device compliance** This requirement is available as both a condition and an access control item, similar to the Azure AD join requirement mentioned above. Devices must be enrolled in Microsoft Intune and be marked as compliant for this requirement to work. When you are defining a condition, you have the option to exclude devices that are marked as compliant. This is available through the device state blade and can be used in a scenario where you are locking down access but want to ignore enrolled devices that are compliant. Alternatively, when you are defining the controls for granting access, you have the option to require enrolled and compliant devices. This is available through the grant blade for access control and can be used as one of many required controls before enabling access to cloud apps.
- **Device enrollment** This requirement is not directly defined through a conditional access policy but is a prerequisite for identifying device compliance.
- **Device platforms** This requirement is available as a condition item. When you are defining a condition, you have the option to include or exclude the following operating systems: Android, iOS, Windows Phone, Windows, and macOS. This is available through the device platforms blade and can be used in a scenario where you are restricting access to a cloud app and want to exclude certain platforms.

Next, let's examine app-based requirements. We introduced session controls earlier in this skill section, which enable you to limit the experience within cloud apps. Two of the requirements we are going to cover are enabled using session controls. The following items are focused on app-based policy requirements.

- **Use app enforced restrictions** This requirement is available as an access control item. When you are defining access controls, you have the option to enable app enforced restrictions. This is defined on the session blade and could be used in a scenario where you need to provide limited access to Office 365 Exchange Online or SharePoint Online for noncompliant devices.
- **Use Conditional Access App Control** This requirement is available as an access control item. When you are defining access controls, you have the option to enable conditional access app control. This is defined on the session blade and could be used in a scenario where you need to monitor and control application access in real time. Access and session policies can then be configured through the Cloud App Security portal, enabling granular control over user access.
- **Available policies** Include access, activity, app discovery, app permission, cloud discovery anomaly detection, files, and session policies. Some of these are designed for monitoring and alerting, others have automated actions that can be enabled.
- **Require approved client app** This requirement is available as an access control item. When you are defining access controls, you have the option to enable the requirement for approved client apps. This is defined on the grant blade and can be used in a scenario where you need to ensure services are only accessed from approved client applications.

MORE INFO **APPROVED CLIENT APPS**

Enabling the requirement for approved client apps will prevent users from accessing services from native or third-party apps that Microsoft has not approved. For a list of approved client apps, visit: *https://docs.microsoft.com/azure/active-directory/conditional-access/technical-reference#approved-client-app-requirement.*

Create Azure AD Conditional Access policies

In this skill section we examine conditional access policies and how to create them. We leverage the design elements and controls that were reviewed in the previous skill section to assist with the creation process. At the time of this writing PowerShell support for conditional access policies is not available, so our walkthrough will be focused on the Azure portal. As with any policy, the controls you choose to enable will depend greatly on the needs of your organization and the goal you wish to achieve.

From an exam perspective, expect to see questions or scenarios that test your knowledge of the conditional access controls and what their capabilities are. We covered some of these fundamentals in the previous skill section, but now we will create the policies and assign them, so you can experience the end-to-end process. Over the next few sections we cover some of the more common conditional access use cases, which will provide you with the fundamentals you need. As always, try to follow along with the step-by-step instructions in your own lab.

Navigate and prepare for conditional access policies

Before creating conditional access policies, be aware that the restrictions you enforce can impact the productivity of your organization if assigned incorrectly. As a word of caution, always assign new policies to a dedicated test user or group and make it a priority to initially exclude admin accounts. Admin accounts can be re-introduced once you have tested the policy. This will prevent undesirable behavior, such as blocking Exchange Online for your senior management. Also, make sure you have the necessary subscription(s) active in your tenant.

To start off, let's take a look at the Conditional Access – Policies blade in the Azure portal. There are a number of controls here that are leveraged prior to policy creation. Depending on your objective, you may need to configure some of these options.

1. Sign-in to the Microsoft Azure portal at *https://portal.azure.com/*.
2. Click **All Services**.
3. Search for **Azure Active Directory** and select it.
4. Under Security, select **Conditional Access**. In Figure 1-23 you can see an example of the Conditional Access blade in the Azure portal.

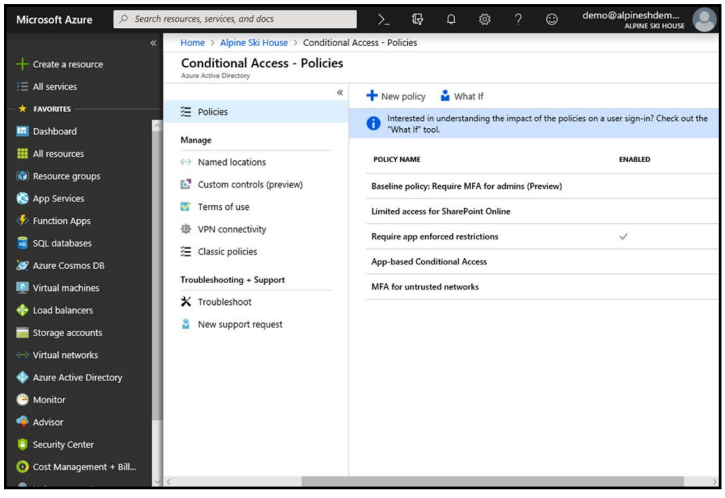


FIGURE 1-23 Conditional Access Policies blade

Let's look at the available options on the Conditional Access blade:

- **Policies** The policies blade is where you will create and manage conditional access policies. In Figure 1-23 the Policies blade is selected. You can see on the right that we have a few policies already defined and one of them is enabled.
- **Named Locations** The Named Locations blade enables administrators to configure network and region-based locations. Network locations are defined by an IP range. Regional locations are defined through a dropdown list of known countries and regions. Named locations that you define can later be used in your conditional access policies.

- **Custom Controls (preview)** The Custom Controls blade enables administrators to declare external services with additional authentication and validation steps. The administrator creates the control and provides the data input using the JSON format, interlinking conditional access and the third-party provider. At the time of this writing, the following providers offer integration with conditional access:

  Duo Security, Entrust Datacard, Ping Identity, RSA, and Trusona.

- **Terms Of Use** The Terms of Use blade enables administrators to upload a terms of use document, which can later be used by conditional access. Once uploaded, the terms of use are listed as another access control that you can require users to comply with before accessing data and services.
- **VPN Connectivity** The VPN Connectivity blade enables administrators to create and manage VPN certificates for Always On VPN. Once created, a conditional access policy can be configured to grant access to the VPN server cloud app.
- **Classic Policies** The class policies blade enables administrators to review and mange classic policies that were created using older versions of the Azure portal. This blade will list any existing classic policies and allow you to disable them as you migrate over to the new policy design.

Create conditional access policies

Now that you have some experience navigating the conditional access controls, let's examine an example scenario and configure a policy. This scenario includes a basic example of what controls you have as an administrator and how they apply in a real world scenario.

SCENARIO: REQUIRE MULTI-FACTOR AUTHENTICATION

As an example, let's say you have a requirement to enable multi-factor authentication and restrict access for cloud services to approved client apps only. The following conditions must be met:

- Applies to all users.
- Applies to iOS and Android platforms.
- Applies to Office 365 Exchange Online.
- Sign-in risk is medium or high.
- Location is untrusted networks.
- Devices are marked as compliant.

We are going to create a conditional access policy that meets these requirements. For each of these scenarios, consider any prerequisites that you may have to address before proceeding. For example, remember that sign-in risk does require an Azure AD premium P2 subscription and you will need to enable Azure AD Identity Protection for your tenant.

1. Sign-in to the Microsoft Azure portal at *https://portal.azure.com/.*

2. Click **All Services**.
3. Search for **Azure Active Directory** and select it.
4. Under Security, select **Conditional Access**.
5. On the Policies blade, click **New Policy**.
6. On the New blade, name the policy "ASH CA Policy."
7. Under Assignments, click **Users And Groups**.
8. On the Users and groups blade, on the Include tab, select the radio button next to **All Users** and click **Done**. Refer to Figure 1-24 for an example of this configuration.

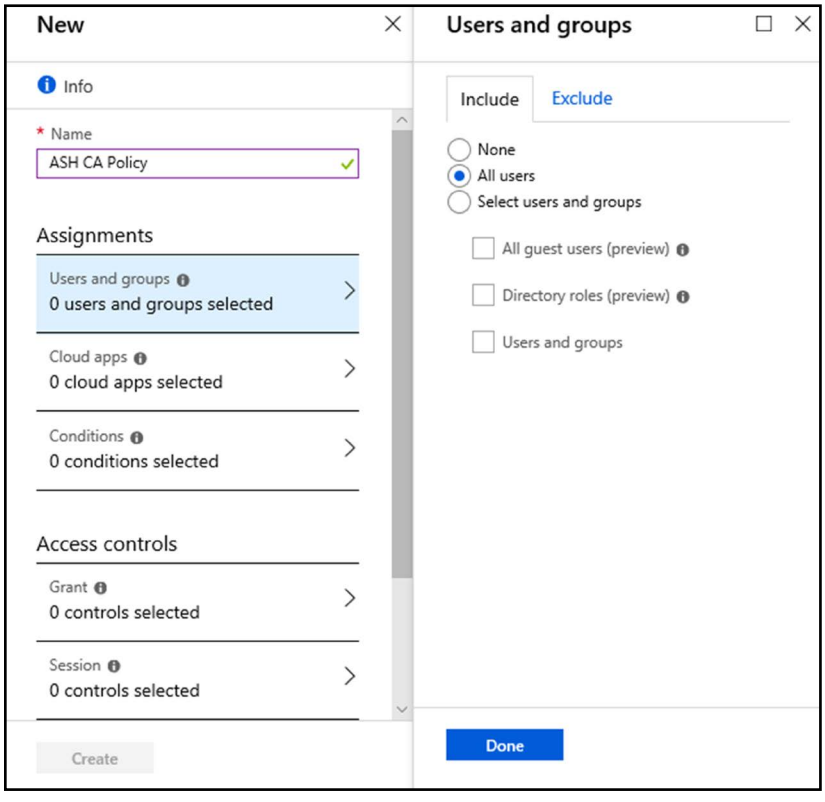


FIGURE 1-24 Conditional Access Users and Groups

9. Under Assignments, click **Cloud Apps**.
10. On the Cloud Apps blade, on the Include tab, select the radio button next to **Select Apps** and click **Select**.
11. On the Select blade, search for **Office 365 Exchange Online** and select it. Click **Select**. Refer to Figure 1-25 for an example of this configuration.

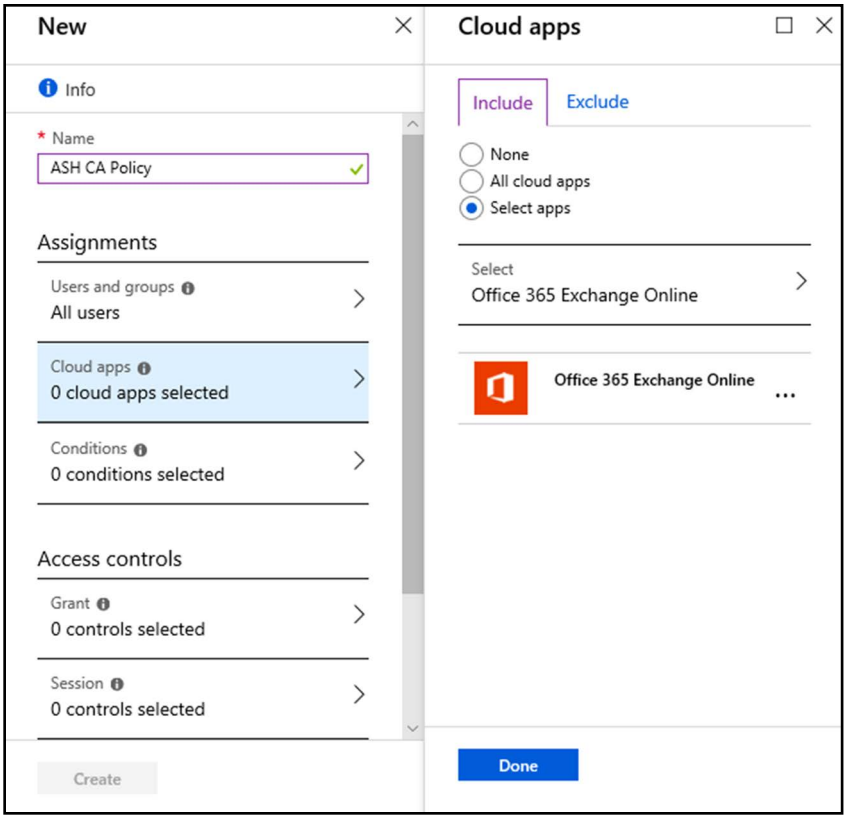


FIGURE 1-25 Conditional Access Cloud Apps

12. Click **Done**.
13. Under Assignments, click **Conditions**.
14. On the Conditions blade, click **Sign-In Risk**.
15. Under Configure, click **Yes** to configure this condition.
16. Check the boxes for **High** and **Medium** and click **Select**. Refer to Figure 1-26 for an example of this configuration.

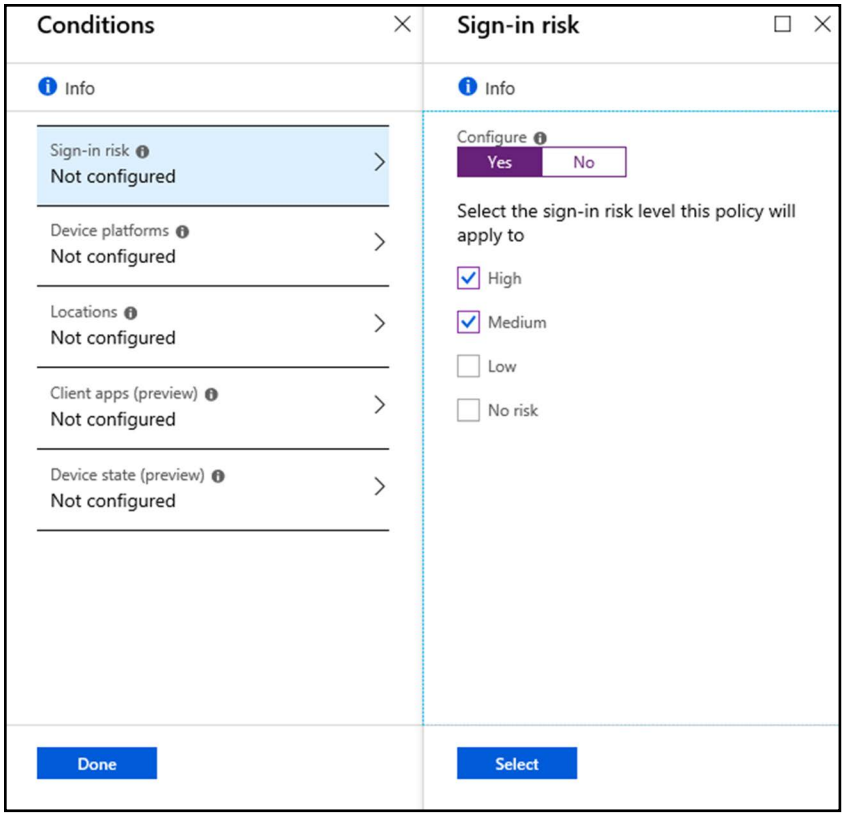


FIGURE 1-26 Conditional Access Sign-in Risk

17. On the Conditions blade, click **Device Platforms**.
18. Under Configure, click **Yes** to configure this condition.
19. On the Include tab, select the radio button next to **Select Device Platforms**.
20. Check the box next to **Android** and **iOS** and click **Done**. Refer to Figure 1-27 for an example of this configuration.

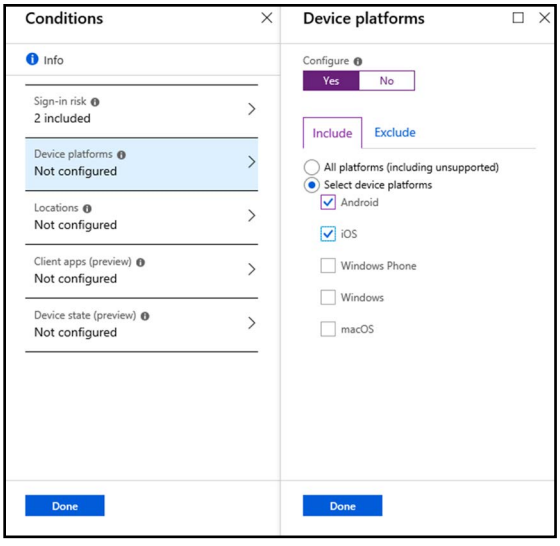


FIGURE 1-27 Conditional Access Device Platforms

21. On the Conditions blade, click **Locations**.
22. Under Configure, click **Yes** to configure this condition.
23. On the Exclude tab, select the radio button next to **All Trusted Locations** and click **Done**. Refer to Figure 1-28 for an example of this configuration. With this configuration we are including any location (default option on the include tab) and excluding all trusted networks. Once applied this policy will only affect users when connected from untrusted networks.

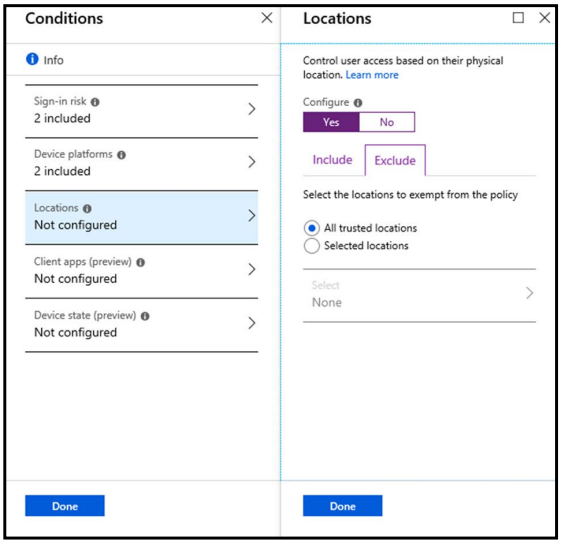


FIGURE 1-28 Conditional Access Locations

24. On the Conditions blade, click **Done**.
25. Under Access controls, click **Grant**.
26. On the Grant blade, select the radio button next to **Grant access**, check the box next to the following items and click **Done**. Refer to Figure 1-29 for an example of this configuration.
    - Require Multi-Factor Authentication
    - Require Device To Be Marked As Compliant
    - Require Approved Client App

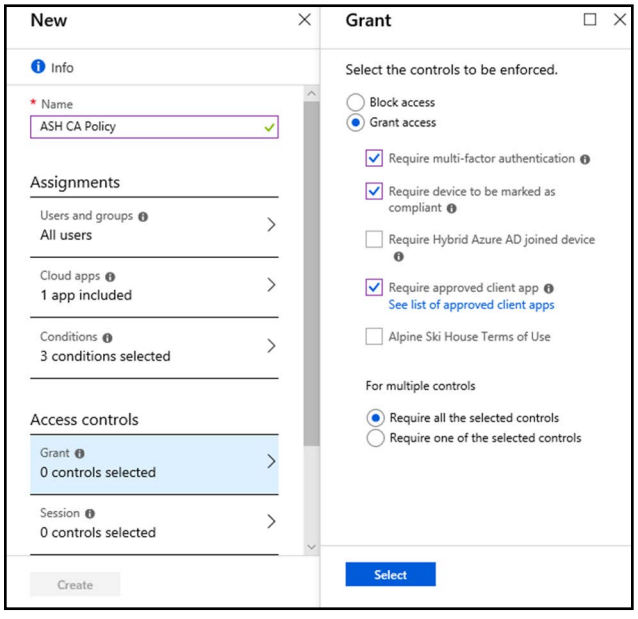


FIGURE 1-29 Conditional Access Grant

27. On the New blade, under Enable Policy, select **On**.
28. Click **Create**.
29. Review the Azure portal notifications to confirm that the conditional access policy was successfully created.
30. On the Policies blade, review the list of policies to confirm that the policy is present, and a check mark is present to indicate the policy is enabled.

After completing the above configuration, you should have a conditional access policy enabled that addresses both the device-based and app-based requirements outlined in this scenario. The goal for this scenario was to introduce you to the Conditional Access blades and build up your comfort level with navigating the various controls. Next, we will look at the What If tool to help assess which policies get applied to a user when certain criteria is defined.

Configure device compliance policy

This skill section covers the creation process for device compliance policies in Microsoft Intune. The examples cover common use cases for device compliance. Like conditional access policies, there are a variety of options and configurations for administrators to work with. This includes the ability to connect with third-party vendor solutions to further enhance the native capabilities. Also, as we navigate through the portal, remember that conditional access policies can leverage compliance status for restricting access to data and services.

Navigate and configure device compliance settings

When you access the Device Compliance blade for the first time, the first thing you might notice is the number of options available in comparison with the conditional access interface. The core functions are split into three groups: manage, monitor, and setup. Like we did with conditional access, let's take a look through these groups and identify the purpose for each.

1. Sign-in to the Microsoft Azure portal at *https://portal.azure.com/*.
2. Click **All Services**.
3. Search for **Intune** and select it.
4. Under Manage, select **Device Compliance**. In Figure 1-30 you can see an example of the Device Compliance blade in the Azure portal.

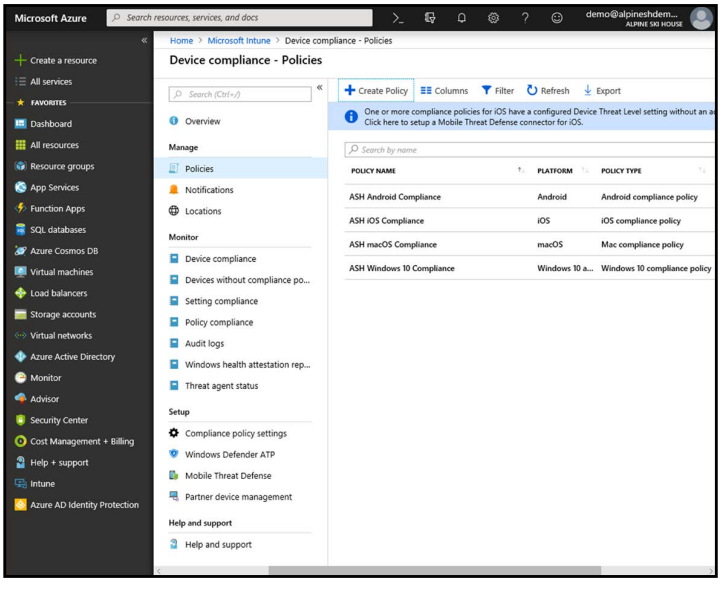


FIGURE 1-30 Device Compliance – Policies

Device compliance includes several built-in reports for administrators to review and export as needed. This includes an overview dashboard, providing a high-level look at overall compli-

ance and areas of interest. Later in this section we will look at monitoring in more detail. For now, refer to Table 1-7 for a breakdown of each section.

TABLE 1-7 Device compliance blade

OPTION	CATEGORY	DESCRIPTION
Overview	Overview	This blade offers a compliance dashboard with summarization data for: ■ Device compliance status ■ Devices without compliance policy ■ Policy compliance ■ Setting compliance ■ Device protections status ■ Threat agent status
Policies	Manage	This blade is used for creating and managing device compliance policies.
Notifications	Manage	This blade is used for creating and managing notification templates that are used for compliance policies.
Locations	Manage	This blade is use for creating and managing locations for location-based compliance policy settings.
Device compliance	Monitor	This blade offers a report with all managed devices and their device compliance status.
Devices without compliance policy	Monitor	This blade offers a report with all managed devices that do not have a compliance policy assigned.
Setting compliance	Monitor	This blade offers a report with per-setting compliance information.
Policy compliance	Monitor	This blade offers a report that summarizes policy compliance by device count, including compliant, noncompliant and errors.
Audit logs	Monitor	This blade offers a report that shows recent administrative actions for compliances policies completed in the portal.
Windows health attestation report	Monitor	This blade offers a report that shows detailed information for health attestation, including the status for BitLocker, code integrity, secure boot, and more.
Threat agent status	Monitor	This blade offers multiple reports show detailed information for anti-virus enforcement, pending reboots, critical failures, and more.
Compliance policy settings	Setup	This blade is used for managing how the compliance service treats devices, such as compliance state when no policies are assigned.
Windows Defender ATP	Setup	This blade is used for integrating Windows Defender ATP with Microsoft Intune, enabling risk association for device compliance.
Mobile Threat Defense	Setup	This blade is used for creating and managing connection points with third-party vendors, enabling additional risk association visibility for device compliance.
Partner device management	Setup	This blade is used for creating and managing a connection with JAMF, a third-party MDM provider specializing in macOS and iOS devices.

When you first begin working with device compliance, there are some configurations that you should review. From the Conditional access blade, click **Compliance Policy Settings** under Setup. There are three controls on this blade that should be considered before you begin creating policies.

- **Mark Devices with No Compliance Policy Assigned As** Compliant | Not Compliant
  - The default configuration for this setting is not compliant. In many cases this will be the desired setting because you want to have some understanding of the device state before granting it access to services. Consider a scenario where you assign a conditional access policy that requires devices to be compliant in order to access Exchange Online.
- **Enhanced Jailbreak Detection** Enabled | Disabled
  - The default configuration for this setting is Disabled. Enabling this feature requires iOS devices to evaluate and report their jailbreak status more frequently in conjunction with leveraging location services. This will impact the battery life of the device while enabled.
- **Compliance Status Validity Period (Days)** 1 – 120
  - The default configuration for this setting is 30 days. This value determines the frequency in which devices must report back their device compliance status to Intune. If a device does not report compliance within the required timeframe they will be marked as noncompliant.

Create device compliance policies

Keep in mind that each compliance policy that you create is associated to a specific device platform, unlike conditional access policies, which enable you to select multiple platforms. Each platform has its own set of options. Some will be similar across platforms, but others will not. For example, macOS has a rule for requiring system integrity protection, which is exclusive to this platform. Based on this you should design your policies on a per-platform basis.

In the following example you are going to create a device compliance policy for Alpine Ski House. This goal is to cover common compliance rules and get you working with the technology.

SCENARIO: WINDOWS 10 DEVICE COMPLIANCE

For this example, you are the MDM administrator for Alpine Ski House. You have a requirement to create and assign a device compliance policy for the Windows 10 platform. This compliance policy will be focused on the security posture of the device and will be re-enforced using a conditional access policy for all cloud services. The following requirements must be met:

- BitLocker is required.
- Secure Boot is required.
- Minimum OS version is 10.0.17134.
- Encryption is required.

- Firewall is required.
- Antivirus is required.
- AntiSpyware is required.
- Windows Defender ATP machine risk is low.

Now that you have a list of requirements defined, follow these steps to create your device compliance policy:

1. Sign-in to the Microsoft Azure portal at *https://portal.azure.com/*.
2. Click **All Services**.
3. Search for **Intune** and select it.
4. Under Manage, select **Device Compliance**.
5. On the Device compliance blade, under Manage, click **Policies**.
6. On the Policies blade, click **Create Policy**.
7. On the Create Policy blade, name the policy "Windows 10 Security Compliance."
8. Under Platform, select **Windows 10 And Later**.
9. On the Windows 10 compliance policy blade, click **Device Health**.
10. On the Device Health blade, set the following options and click **OK**. Refer to Figure 1-31 for an example of this configuration.
    - Set **Require Bitlocker** to **Require**.
    - Set **Require Secure Boot To Be Enabled On The Device** to **Require**.

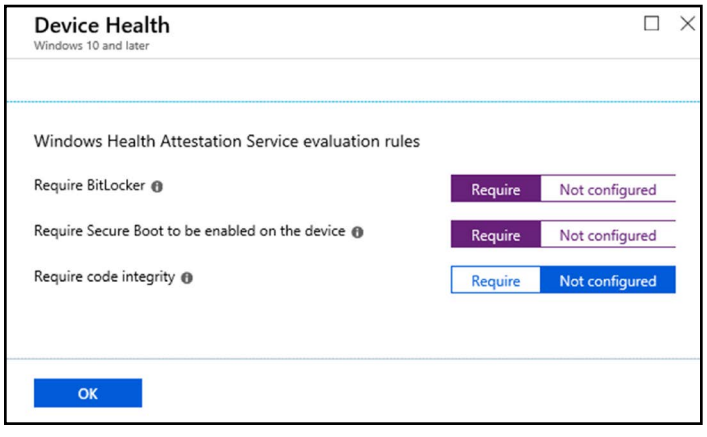


FIGURE 1-31 Device Compliance - Device Health

11. On the Windows 10 Compliance Policy blade, click **Device Properties**.
12. On the Device Properties blade, set the following option and click **OK**. Refer to Figure 1-32 for an example of this configuration.
    - Set **Minimum OS version** to **10.0.17134**.

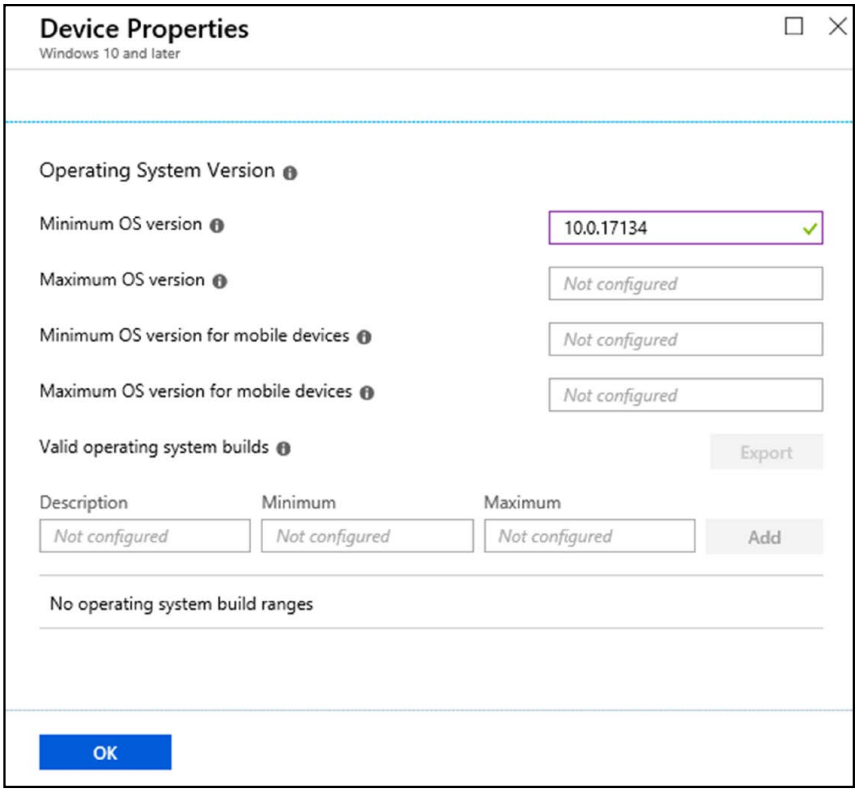


FIGURE 1-32 Device Compliance – Device Properties

13. On the Windows 10 compliance policy blade, click **System Security**.
14. On the System Security blade, set the following options and click **OK**. Refer to Figure 1-33 for an example of this configuration.
    - Set **Encryption Of data Storage On Device** to **Require**.
    - Set **Firewall** to **Require**.
    - Set **Antivirus** to **Require**.
    - Set **AntiSpyware** to **Require**.

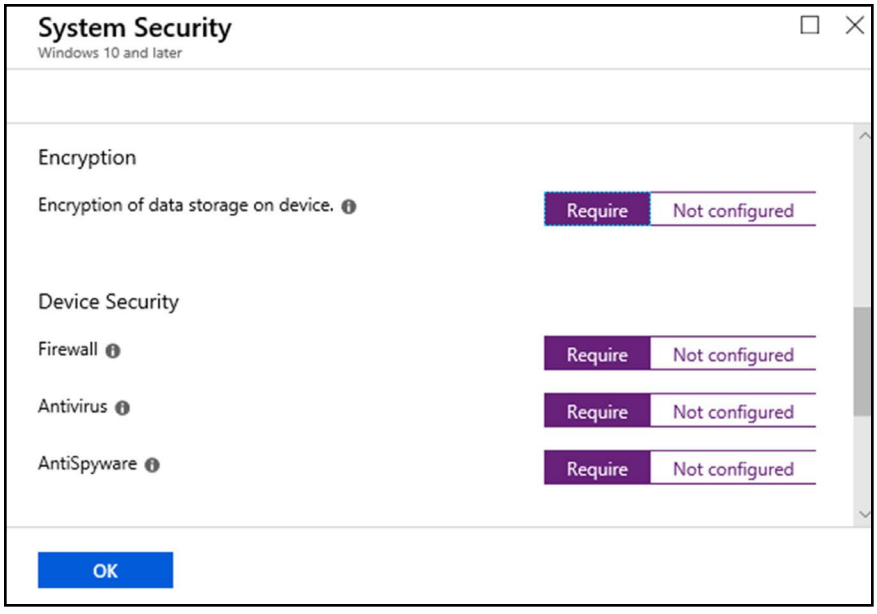


FIGURE 1-33 Device Compliance – System Security

15. On the Windows 10 compliance policy blade, click **Windows Defender ATP**.
16. On the Windows Defender ATP blade, set the following option and click **OK**. Refer to Figure 1-34 for an example of this configuration.
    - Set **Require The Device To Be At Or Under The Machine Risk Score** to **Low**.

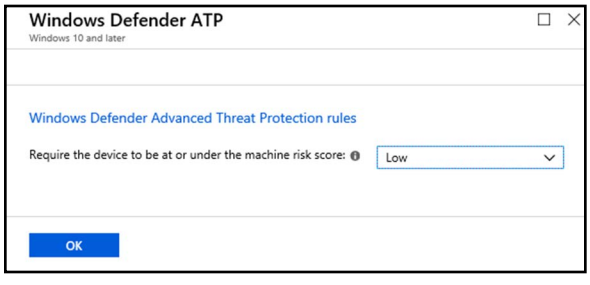


FIGURE 1-34 Device Compliance – Windows Defender ATP

17. On the Windows 10 Compliance Policy blade, click **OK**.
18. On the Create Policy blade, click **Create**.
19. Review the Azure portal notifications to confirm that the compliance policy was successfully created.

Once you complete these steps, you should have a compliance policy containing rules that pertain to Windows 10 device security. The next step is to assign this policy to your target audience and trigger an evaluation. For these steps it is assumed that you already have an existing AD group that contains Windows 10 devices.

1. On the Windows 10 Security Compliance blade, under Manage, click **Assignments**.
2. On the Assignments blade, click **Select Groups To Include**.
3. On the Select groups to include blade, select the group **Windows 10 Devices** and click **Select**.
4. On the Assignments blade, click **Save**.
5. Review the Azure portal notifications to confirm that the assignment was successfully saved.
6. On the Assignments blade, click **Evaluate** to force all group members to evaluate the compliance policy.

Manage conditional access policies

In this skill section we introduce two new tools in the Azure portal designed to help you manage their conditional access policies. The first tool is the What If tool. An administrator can define a user and specific criteria to determine which policies are getting assigned. The second tool is the Azure AD Sign-ins report. This report provides a record of user activity with the capability to drill down and view conditional access events. Over the next few sections these tools are examined in detail along with some examples of the interface.

Manage conditional access policies using the What If tool

As you begin designing the structure for your conditional access policies, you may find some policies start to overlap with others. For example, you might have a policy applied that enforces multi-factor authentication for all users. Then you introduce a new policy that does not enforce multi-factor authentication for a specific group of users with the condition that they are connected to a trusted network. The What If tool can help highlight exactly what policies are getting applied to each per-user. The What If tool is also a great solution for evaluating new policies before you enforce them across your organization, and should be considered as a first step in your rollout process.

The What If tool is available on the Conditional Access blade. Refer to the following steps to access the tool:

1. Sign-in to the Microsoft Azure portal at *https://portal.azure.com/*.
2. Click **All Services**.
3. Search for **Azure Active Directory** and select it.
4. Under Security, select **Conditional Access**.
5. On the Policies blade, click **What If** in the menu bar. In Figure 1-35 you can see an example of the What If tool in the Azure portal and what criteria is available.

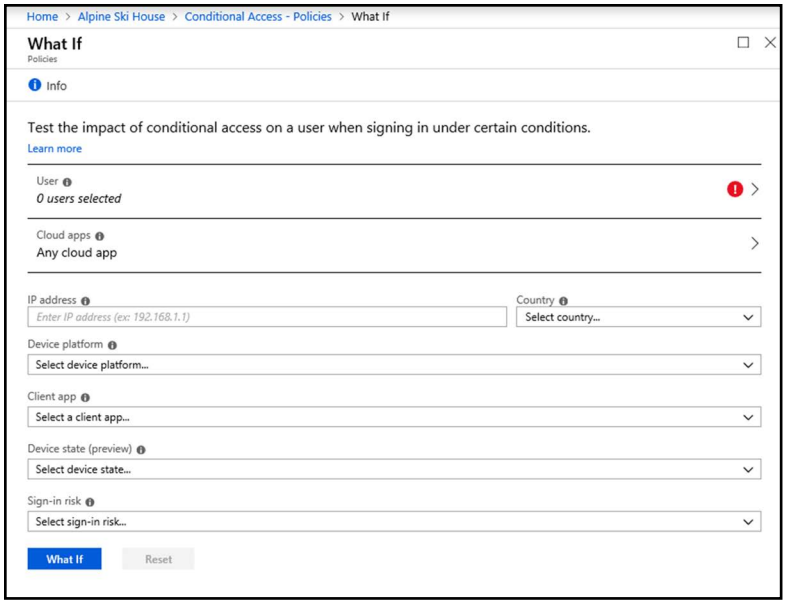


FIGURE 1-35 What If Options

The following list covers the available criteria on the What If blade. Each of these options should look familiar, as they directly correspond to the controls that were defined when creating the conditional access policy.

- **User** This option enables you to select a single user account for analysis. You cannot select multiple users or groups. This is the only required option to run the What If tool.
- **Cloud Apps** This option enables you to select one or multiple cloud apps. Any Cloud Apps is the default option. If you are troubleshooting a policy issue with a specific cloud app, you should select that app here.
- **IP Address** This option enables you to enter an IP address for location-based queries. Typically, this is the IP address of the user's device. If you select this option, you must also specify a country.
- **Country** This option enables you to select a specific country for location-based queries. Again, if you select a country you also must provide an IP address.
- **Device Platform** This option enables you to select a specific device platform. This is helpful for troubleshooting policies that only apply to specific device platforms.
- **Client App** This option enables you to select a specific client app. This is helpful for troubleshooting policies that apply to a combination of client app types.
- **Device State (preview)** This option enables you to select Hybrid Azure AD join or device compliance. This is helpful for troubleshooting policies that have a device state requirement.
- **Sign-In Risk** This option enables you to select a specific risk level. This is helpful for troubleshooting policies that have a sign-in risk level defined.

When you first start using the What If tool, you can begin by selecting any user in your tenant and clicking the What If button. This should provide you with some basic results regardless of whether the user has a conditional access policy assigned. In the following example the What If tool is used against a user account in our Alpine Ski House tenant. After running the tool you will be presented with the evaluation results at the bottom of the page. This includes two tabs. The first tab is for policies that will apply to the selected user account, and the second tab is for policies that will not apply.

In Figure 1-36 we have an example of the first tab. Take note of the Grant Controls column. This column will specify which access controls are being applied by the associated policy. You can use this information to determine where policies overlap, and drill down further by modifying the query criteria that we reviewed above. For example, set cloud apps to Exchange Online and rerun the tool to see if the same controls are being applied.

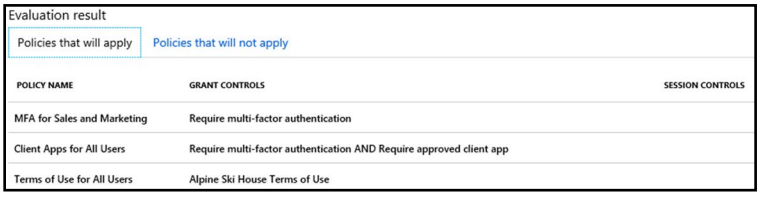


FIGURE 1-36 What If – Policies That Will Apply

Figure 1-37 shows an example of the second tab. Take note of the column: **Reasons Why This Policy Will Not Apply**, which is particularly helpful for identifying gaps in your policy design. For example, in this scenario we are reviewing the MFA policy for All Users, which should apply to iOS and Android devices. When running the tool, you selected iOS for the device platform, with the expectation that this policy would show applied. However, based on this evaluation, the tool has identified that this policy is not being applied due to the device platform, which is iOS in this case. With this information you now know that this policy needs to be reviewed to confirm that correct device platforms are selected.

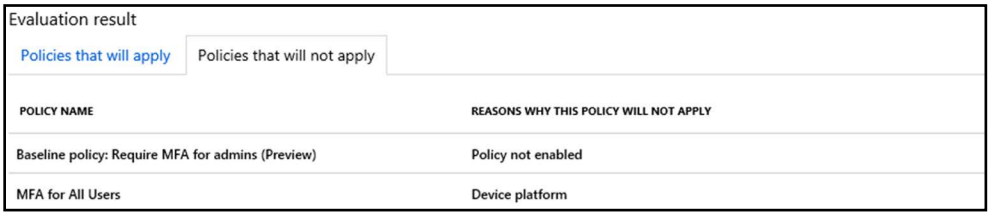


FIGURE 1-37 What If – Policies That Will Not Apply

Manage conditional access policies using the Sign-ins report

Let's now examine the Azure AD Sign-ins report. This report is helpful for tracking and troubleshooting various events related to user activity with Azure AD. For conditional access, it pro-

vides a drill down view of each user event. Unlike the What If tool, these are actual events that have occurred in your environment, compared to a view that shows what will happen.

Refer to the following steps for accessing the Azure AD Sign-ins report. In this example we have some activity recorded in the report to help demonstrate what kind of data to expect.

1. Sign-in to the Microsoft Azure portal at *https://portal.azure.com/*.
2. Click **All Services**.
3. Search for **Azure Active Directory** and select it.
4. Under Monitoring, select **Sign-ins**. In Figure 1-38 you can see an example of the Sign-ins report that we will be working with in this example.
5. On the Sign-ins report, select an event that you would like to see more detail for. In this example, we have defined the following search criteria to help narrow down the results:
   - **User** Adam
   - **Application** Microsoft Office 365 Portal
   - **Status** Failure
   - **Date** Last 24 hours

NOTE **SEARCH CRITERIA**

As shown in Figure 1-38, all search criteria is case sensitive and supports the 'starts with' operator. For context, if you were to enter 'Office 365' for the application it would only return results that start with Office 365, such as Office 365 Exchange Online.

On the details pane there are five tabs. Each tab contains additional information about the selected event. Refer to the following list for a breakdown of each tab:

- **Basic Info** This tab contains basic details about the selected sign-in event. Some of this is visible in the main report but there are key items like Location, Sign-In Error Code, Failure Reason, and Client App.
- **Device Info** This tab contains details about the browser and device used during the sign-in event, including whether the device is enrolled in Intune and what the compliance status is.
- **MFA Info** This tab contains details that pertain to multi-factor authentication. This includes whether an MFA request was required, if the request was completed, the authentication method, and details about that method. For example, if the method was text message, the details would include the last two digits of the phone number.
- **Conditional Access** This tab contains details about the active conditional access policies, what the grant controls are, and the results of applying those policies during the sign-in event.

Index

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W