

Azure Active Directory **Conditional Access** Deployment Plan

**How to use this guide**

This step-by-step guide walks through the implementation of Conditional Access in a five-step process. The links below take you to each of those steps.



**1**

**[Include](#_Stakeholders_and_Sign-off)**

[Stakeholders](#_Stakeholders_and_Sign-off)

**2**

**[Plan](#_Planning_Your_Implementation)**

[Your project](#_Planning_Your_Implementation)

**3**

**[Design](#_Design)**

[Policies and integration](#_Design)

**5**

**[Manage](#_Operational_Doc_1)**

[Your implementation](#_Operational_Doc_1)



**4**

**[Implement](#_Implementing_Your_Solution)**

[Your design](#_Implementing_Your_Solution)

**Note:**

Throughout this document, you will see items marked as

* **Microsoft Recommends**

These are general recommendations, and you should only implement if they apply to your specific enterprise needs.

Table of Contents

Contents

[Business Value of Conditional Access 2](#_Toc513650641)

[Planning Your Implementation 3](#_Toc513650642)

[Stakeholders and Sign-off 3](#_Toc513650643)

[Licensing 4](#_Toc513650644)

[How to draft Conditional Access policies 4](#_Toc513650645)

[Types of policies 5](#_Toc513650646)

[Recommended Policies 6](#_Toc513650647)

[Design 7](#_Toc513650648)

[MFA when not at work 7](#_Toc513650649)

[MFA for admins 7](#_Toc513650650)

[MFA for risky sign-ins 9](#_Toc513650651)

[Require a compliant device 9](#_Toc513650652)

[Password change for risky users 12](#_Toc513650653)

[Implementing Your Solution 13](#_Toc513650654)

[Phase 1: Implementation Steps 13](#_Toc513650655)

[Phase 2: Testing 16](#_Toc513650656)

[Phase 3: Moving to production 16](#_Toc513650657)

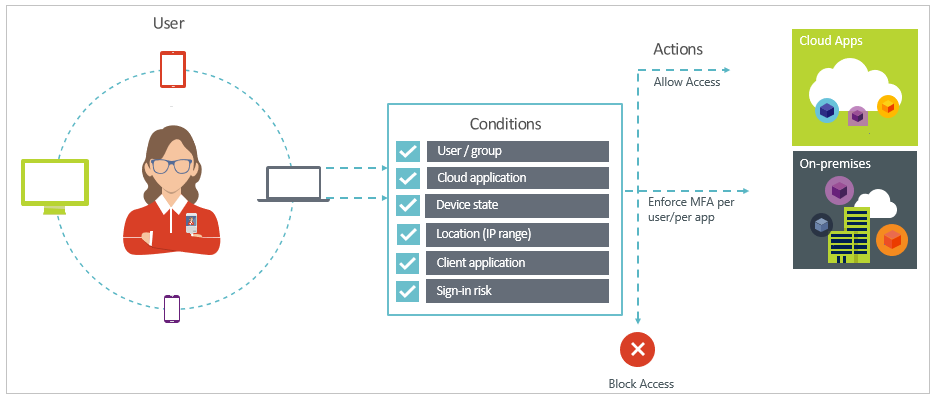
[Phase 4: Rollback Steps 16](#_Toc513650658)

[Managing your solution 18](#_Toc513650659)

[Required Roles 18](#_Toc513650660)

# Business Value of Conditional Access

In a mobile-first, cloud-first world, users can access your organization's resources from anywhere using a variety of devices and apps. As a result, only focusing on who can access a resource is no longer sufficient. You need to be able to control who has access, where the user is, which device is being used, and much more. Azure AD Conditional Access (CA) provides this control by allowing you to specify the conditions a user must meet for access to an application, such as multiple factors of authentication (MFA).



|  |  |
| --- | --- |
|  |  |
| |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | \\MAGNUM\Projects\Microsoft\Cloud Power FY12\Design\ICONS_PNG\Increase.png | **INCREASE PRODUCTIVITY**  Conditional Access (CA) policies allow you to control when users are prompted for MFA, when access is blocked, or when they are required to use a trusted device. For example, you can set a policy so that users must MFA for access to an application only when outside the corporate network. This keeps users more productive than a policy requiring MFA every single time. Furthermore, Azure AD Conditional Access not only allows you to specify policies on a per-user basis, as with ADFS, but also to create app specific policies. | | \\MAGNUM\Projects\Microsoft\Cloud Power FY12\Design\ICONS_PNG\Confidentiality.png | **MANAGE RISK**  Enabling Conditional Access policies provides you with cloud-scale identity protection, risk-based access control capabilities, and native multi-factor authentication support. Coupling Conditional Access with identity protection, which uses adaptive machine learning to detect anomalies and suspicious events, allows you to target when access to an application is blocked or gated. | | C:\Users\mitchellg\Desktop\Simple_Licensing.png | **ADDRESS COMPLIANCE AND GOVERNANCE**  Auditing access requests and approvals for the application, as well as understanding overall application usage becomes easier with Azure Active Directory, which supports native audit logs for every application access request performed. Auditing includes requester identity, requested date, business justification, approval status, and approver identity. This data is also available from an API, which will enable importation of this data into a Security Incident and Event Monitoring (SIEM) system of choice. | | \\MAGNUM\Projects\Microsoft\Cloud Power FY12\Design\ICONS_PNG\Within_Your_Reach.png | **MANAGE COST**  Moving access policies to Azure AD reduces the reliance on custom or on-premises solutions such as ADFS for CA, reducing the cost of running that infrastructure. | |  | |  |

# Planning Your Implementation

## Stakeholders and Sign-off

Use the following table to identify stakeholders in your organization that are involved in this deployment.

* Action:
  + SO = Sign-off on this project
  + R = Review this project and provide input
  + I = Informed of this project

|  |  |  |
| --- | --- | --- |
| Name | Area | Action |
| <Enter name and email> | **IT Support Manager**  *A representative from the IT support organization who can provide input on the supportability of this change from a helpdesk perspective.* | <Input Action Required (SO,R,I)> |
| <Enter name and email> | **Identity Architect or Azure AD Global Administrator**  *A representative from the identity management team who owns defining how this change aligns with the core identity management infrastructure in the customer’s organization.* | <Input Action Required (SO,R,I)> |
| <Enter name and email> | **Business Owner**  *A representative colleague who can provide input on the user experience and usefulness of this change from an end-user’s perspective and owns the overall business aspect of the application, which may include managing access.* | <Input Action Required (SO,R,I)> |
| <Enter name and email> | **Security Owner**  *A representative from the security team that can sign off that the plan will meet the security requirements of your organization.* | <Input Action Required (SO,R,I)> |

## Licensing

The following table describes some of the license requirements that may be relevant. For a full list of license requirements, click [here](https://azure.microsoft.com/en-us/pricing/details/active-directory/).

* [Conditional Access](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-conditional-access-azure-portal) (P1 Required)
* [Identity Protection](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-identityprotection) (P2 Required)

**Note:** all users covered under a policy must be covered by the appropriate licenses

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Free | BASIC | PREMIUM P1 | PREMIUM P2 |
| CA based on location | Not available | | Available | |
| CA based on device state (Allow access from managed devices) | Not available | | Available | |
| CA to require MFA (Require MFA when not at work) | Not available | | Available | |
| Identity protection | Not available | | Not available | Available |

If you have an existing Enterprise Mobility and Security (EMS) subscription with Microsoft, you already have Azure AD Premium.

* EMS E3 includes P1
* EMS E5 includes P2.

If you have an existing Enterprise Agreement or Server and Cloud Enrollment, you may already have Azure Premium. Check the details of your agreement.

## How to draft Conditional Access policies

Use the following documentation to familiarize yourself with how Conditional Access works:

* 10,000 foot overview of CA: [Conditional Access in Azure Active Directory](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-conditional-access-azure-portal).
* Conditional Access capabilities:[Access controls in Azure Active Directory Conditional Access](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-conditional-access-controls).
* Real-world use cases: [Conditions in Azure Active Directory Conditional Access](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-conditional-access-conditions).

Now that you know the ingredients (conditions and controls), you should learn how to draft policies. You don’t need to be a CA expert to complete this task.

To do this, use the following pattern:

cid:image001.png@01D3D5D9.74D56D00

|  |  |
| --- | --- |
| **When this happens** | **Then do this** |
| An access attempt is made:   * To a cloud app\* * By users and groups\*\* * Using   + Condition1 (e.g. outside Corp network)   + Condition2 (e.g. sign-in risk) | Block access to the application |
| An access attempt is made:   * To a cloud app * By users and groups * Using   + Condition1 (e.g. outside Corp network)   + Condition2 (e.g. sign-in risk) | Grant access with (AND):   * Requirement 1 (e.g. MFA) * Requirement 2 (e.g. Device compliance) |
| An access attempt is made:   * To a cloud app * By users and groups * Using   + Condition1 (e.g. outside Corp network)   + Condition2 (e.g. sign-in risk) | Grant access with (OR):   * Requirement 1 (e.g. MFA) * Requirement 2 (e.g. Device compliance) |

|  |  |
| --- | --- |
| \*To a **cloud app** can be:   * A single cloud app * A list of cloud apps * A wildcard (all cloud apps) * A descriptive label (all HR apps) | \*\*By **users and groups** can be:   * A single user or group * A list of users and groups * A list of roles * A wildcard (all users and groups) * A descriptive label (all administrators) |

## Types of policies

With Conditional Access, you can control how authorized users can access your resources. A few key options you have at your disposal are:

* **What if a legitimate user tries to access a cloud app from a network location you don’t trust?**
  + With **location-based policies**, you can define whether and how your users can access your resources from inside and outside your organization’s network. For example, you can require that they always MFA from outside your corporate network.
* **What if a legitimate user tries to access a cloud app with a device that is not managed by your organization?**
  + Using device-based Conditional Access, you can tie requirements to the device that is used by a user to access your resources.
* **What if a user with compromised credentials tries to sign in?**

Leverage Identity Protection’s capability to analyze the risk of the user and restrict access

## Recommended Policies

**If you have P1 Licenses:**

|  |  |
| --- | --- |
| **When this happens** | **Then do this** |
| An access attempt is made:   * To **all cloud apps** * By **Global Administrators** | [Require MFA (for admin)](#_MFA_for_admins) |
| An access attempt is made:   * To a **specific app** * By **All Users and Groups** | [Require MFA when not at work](#_MFA_when_not) |
| An access attempt is made:   * To a **specific app** * By **All Users and Groups** | [Require a compliant device or an approved app](#_Device_Compliance_when) |

**If you have P2 Licenses:**

|  |  |
| --- | --- |
| **When this happens** | **Then do this** |
| An access attempt is made:   * To **all cloud apps** * By **all users and groups**   + Condition: **Sign in Risk is Medium or High** | [MFA for risky sign-ins](#_MFA_for_risky) |
| An access attempt is made:   * To **all cloud apps** * By **All Users and Groups**   + Condition: **High sign in risk due to leaked credentials** | [Require MFA + Password change if credentials are leaked](#_Password_change_for) |
| An access attempt is made:   * To **all cloud apps** * By **Global Administrators** | [Require MFA (for admins)](#_MFA_for_admins) |

## Design

This section articulates the design considerations and information you need to collect to roll out your Conditional Access policy. Each sub-section focuses on designing one of the recommended CA policies articulated above. Add / remove sub-sections based on the polices that you plan to implement.

### MFA when not at work

Azure AD enables single sign on to devices, apps, and services from anywhere on the internet. Using a location based Conditional Access policy, you can control access to your cloud apps based on the network location (either a named location such as a country or a specific IP range) of a user. You can require MFA when a user is outside the corporate network by defining the Internet facing IP ranges for your trusted corporate network. Use the table below to identify the trusted locations for your corporate network.

**Notes:**

* When defining named locations, ensure that IP ranges you trust are marked as trusted.
* Trusted IP ranges can be split into multiple named locations so that it is easy to manage (e.g. office locations).
* These locations represent the public IP ranges for the corporate network.

Use the table below to design your policy. It will be used when configuring your policy. Default values have been provided. Change them as appropriate for you.

|  |  |
| --- | --- |
| **Field** | **Value** |
| Policy Name | MFA when not at work |
| Users and Groups | <Insert users and groups> |
| Cloud Apps | <Insert applications or All Cloud Applications> |
| Grant | Require Multi Factor Authentication |

**Conditions**

|  |  |
| --- | --- |
| **Location Name** | **IP Ranges** |
| <Insert Location Name 1> | <Insert IP Ranges> |
| <Insert Location Name 2> | <Insert IP Ranges> |
| <Insert Location Name 3> | <Insert IP Ranges> |

For more information, see [Location conditions in Azure Active Directory Conditional Access](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-conditional-access-locations).

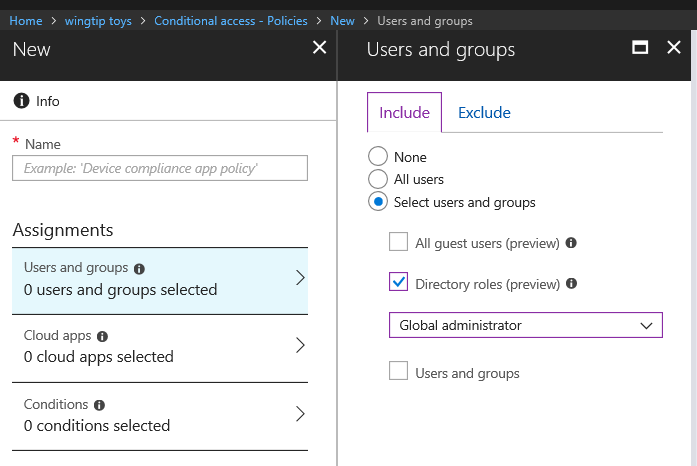
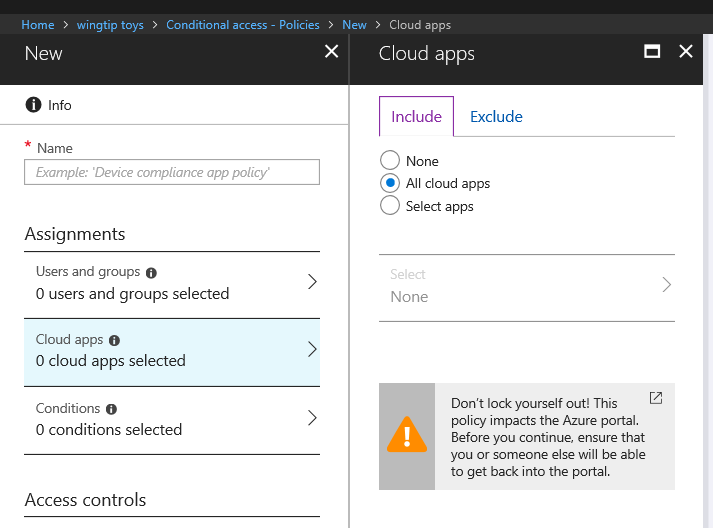
### MFA for admins

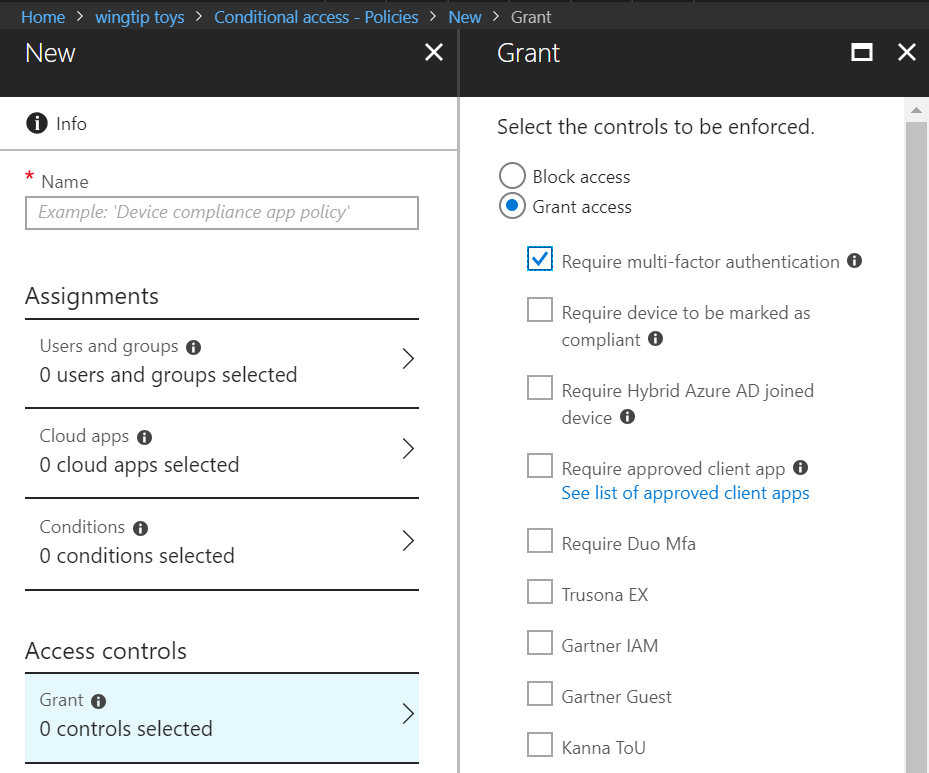
Administrators are frequently the target of attacks as their privileged accounts can perform actions in the Azure portal that others cannot. Requiring MFA for admins is a simple policy that helps to secure these high privilege accounts. **When rolling out MFA for admins, ensure that at least one admin is excluded from the policy until there is another admin that has successfully registered for MFA and signed in. You do not want to lock all admins out of the azure portal.**

* **Microsoft recommends** requiring MFA for global admins (at a minimum), for **all cloud applications**

Use the table below to design your policy. It will be used when configuring your policy. Default values have been provided. Change them as appropriate for you.

|  |  |
| --- | --- |
| **Field** | **Value** |
| Policy Name | MFA for Admins |
| Users and Groups | Global Administrator  <Add additional roles as appropriate> |
| Cloud Apps | All Cloud Applications |
| Grant | Multi Factor Authentication |





### 

### MFA for risky sign-ins

Azure AD Identity Protection (IP) “sign-in risk” indicates the likelihood (high, medium, or low) that a sign-in attempt was not performed by the legitimate owner of a user account. IP calculates the sign-in risk level in real time, as users try to access their applications. You can use the calculated sign-in risk level as a condition in a Conditional Access policy.

Use the table below to design your policy. It will be used when configuring your policy. Default values have been provided. Change them as appropriate for you.

|  |  |
| --- | --- |
| **Field** | **Value** |
| Policy Name | MFA for Risky Sign-Ins |
| Users and Groups | <Insert users and groups> |
| Cloud Apps | All Cloud applications |

**Conditions / Grants**

|  |  |
| --- | --- |
| **Condition** | **Grant** |
| No Sign-In Risk | <Recommendation: Don’t include no sign-in risk> |
| Low Sign-In Risk | <Recommendation: Don’t include low risk in your policy unless this is a high priority app> |
| Medium Sing-In Risk | <Recommendation: Require MFA> |
| High Sign-In Risk | <Recommendation: Require MFA or Block Access> |

Learn More: [Azure Active Directory Identity Protection](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-identityprotection)

* **Microsoft recommends** applying this CA policy to **all your cloud applications**

### Require a compliant device or an approved app

Enterprise Mobility + Security offers a comprehensive set of technologies that can help address the challenges and concerns of the BYOD scenario. The technologies we will cover in this document include:

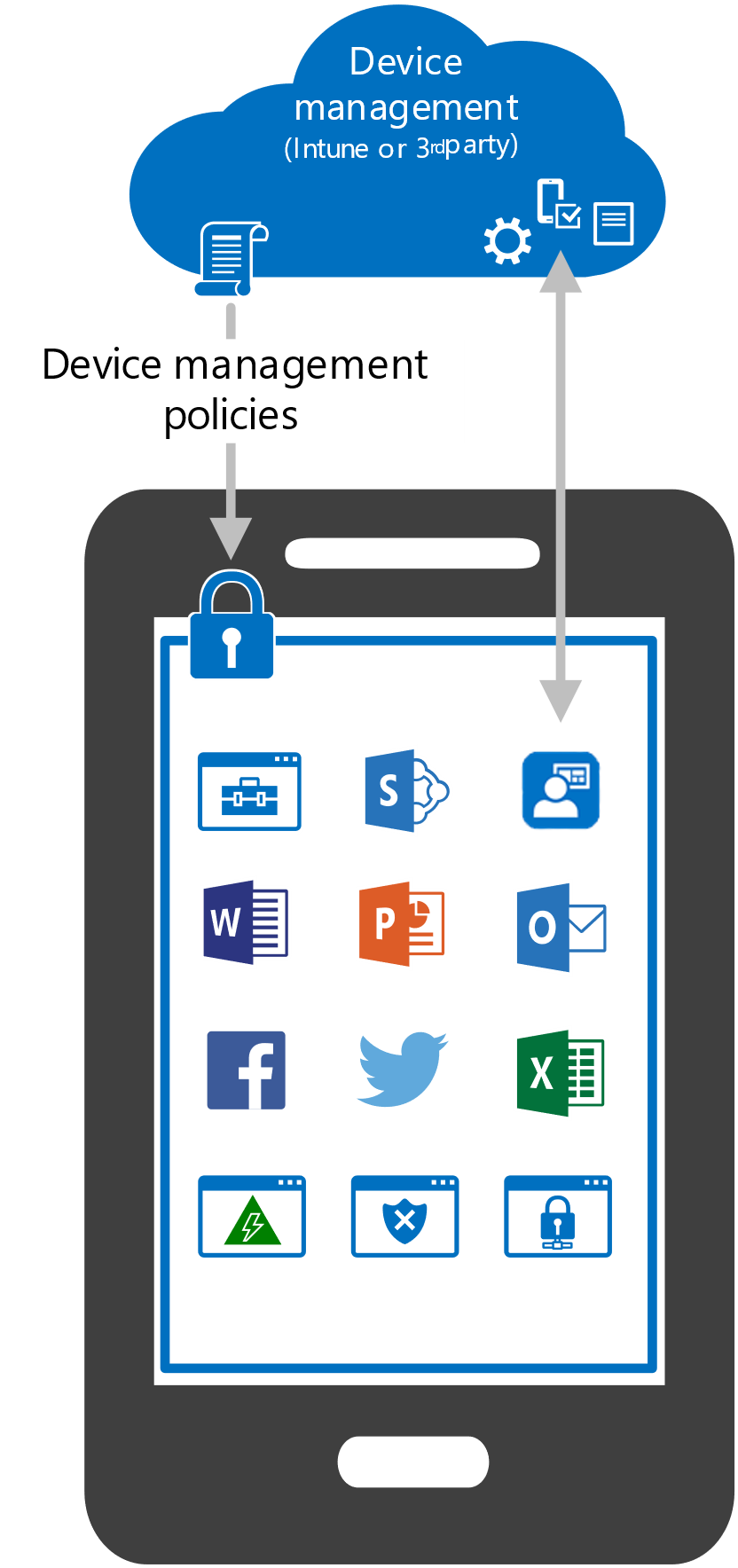
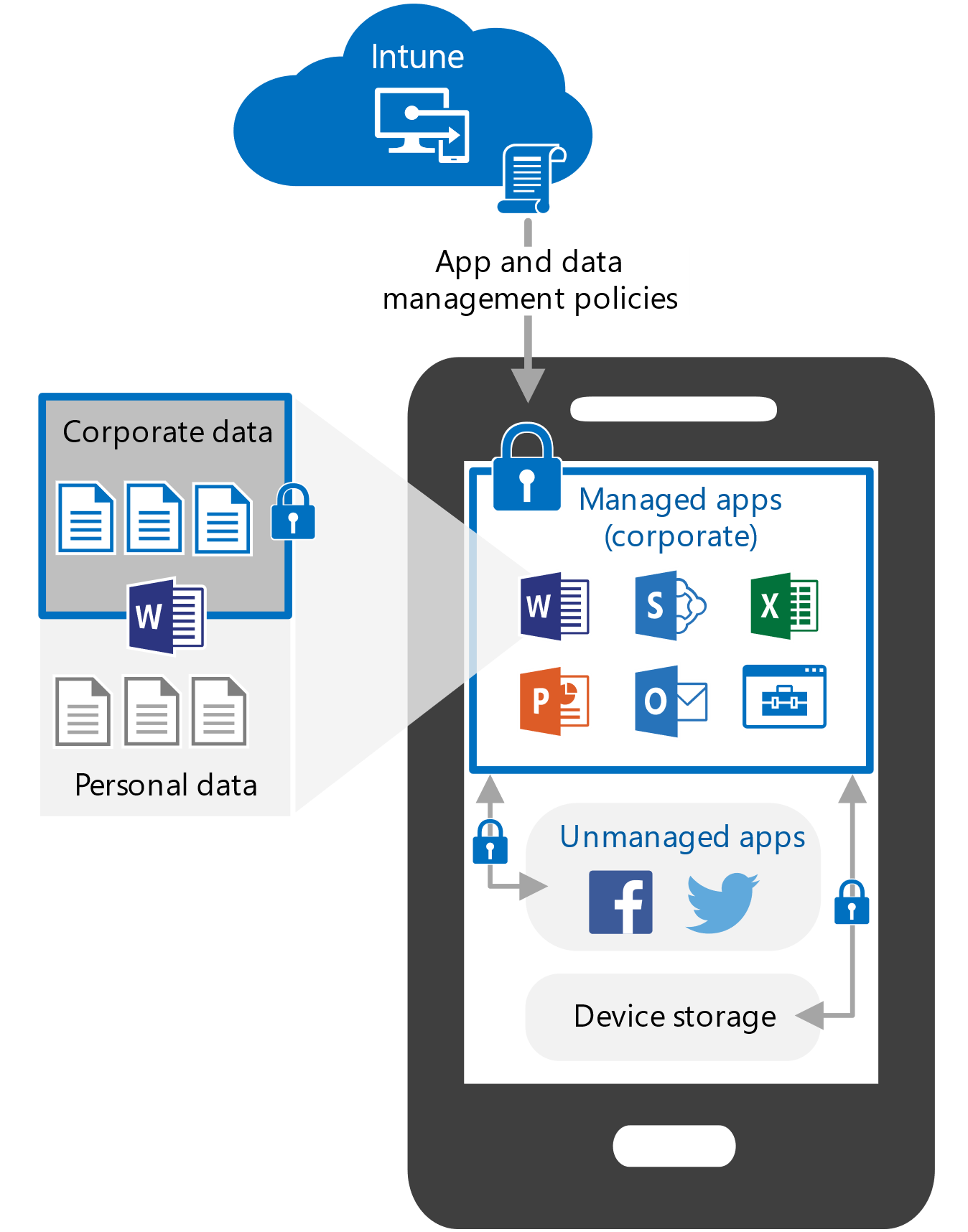
* Microsoft Intune for mobile device management (MDM) and Intune App Protection
* Azure Active Directory (Azure AD) for identity management

One of the first decisions you need to make for bring your own devices (BYOD) scenarios is whether you need to manage the entire device or just the data on it.

Managing the entire device means that it is under the control of Intune or a third party mobile device management (MDM) solution. Intune allows for both Mobile Device Management (MDM) as well as Intune App Protection. It offers extensive protection to the device and the applications running on the device. Some enterprises require their employees to enroll their devices with MDM, but with Intune, this device management is optional, depending on your organization's security and user experience requirements. Employees are often hesitant to enroll a personal device because they fear that IT groups can “control” or “see and delete” personal information when, with Intune, this statement is false.

Below is a table that represents some common considerations about BYOD and key features of Intune that address them to help you decide whether to manage BYOD devices with MDM, Intune App Protection, or both. You can learn more in the device management [Planning Guide](https://docs.microsoft.com/en-us/intune/planning-guide).

|  |  |  |
| --- | --- | --- |
| Consideration | MDM | Intune App Protection |
| User onboarding experience | User generally needs to **accept that device will be remotely managed** by IT (varies by OS). | User gets **FYI about data protections** upon first launch of a protected app. |
| Access pin | Admins can create and enforce PINs to sign into the **device**. | Admins can create and enforce PINs to get corporate data in mobile **apps**. |
| Data encryption | Admins can create and enforce policies for **full device encryption.** | Admins can create and enforce policies for **application data encryption.** |
| Hardware setup | Admins can create and enforce policies around various hardware features such as camera, cellular radios, Wi-Fi, radios, and so on. | N/A |
| Wi-Fi, VPN, email, and certificate profiles | Admins can deploy profiles to devices that configure Wi-Fi, VPN, email, and certificates to meet company requirements.  Admins can also create and deploy custom profiles. | N/A |
| App provisioning | Intune can distribute Store apps and line-of-business apps directly to the device.  You can tag the apps as “available” (the user must install the app) or as “required” (the app will be installed automatically). | Apps are not distributed to devices by Intune. The admin creates an app policy to target a set of apps. After the end user downloads the app and logs on with their corporate credentials, the app policy is immediately applied to the app. |
| App inventory | Can inventory all apps on device. | Cannot inventory apps on device. |
| Data removal | Remove corporate data and settings with “selective wipe”.  Run a complete factory reset if necessary.  Learn more about [selective wipe](https://docs.microsoft.com/en-us/intune/devices-wipe) and [factory reset](https://docs.microsoft.com/en-us/intune/device-factory-reset) for MDM. | Remove corporate data from Intune-managed app with “selective wipe”. [Learn more about selective wipe for app protection.](https://docs.microsoft.com/en-us/intune/apps-selective-wipe) |
| MDM conflict | N/A | Can co-exist with any Microsoft or non-Microsoft MDM solution. |

*Device management* *App and data management*

Learn more about [device management and app management lifecycles](https://docs.microsoft.com/en-us/intune/introduction-device-app-lifecycles).

Learn more about which apps are protected by [Intune App Management](https://www.microsoft.com/cloud-platform/microsoft-intune-apps)

**Ways to ensure corporate data is not leaked**

As a complimentary solution to enforcing Conditional Access on devices and applications, you can add additional security controls by creating app protection policies to control which applications can be used to access corporate data.

|  |  |  |
| --- | --- | --- |
| Concern | Device Management Mitigations | Intune App Management Mitigations |
| Lost or stolen device | Remove all device data  Require Device PIN | Remove all app data |
| Compromised device or app | Device encryption | App data encryption |
| Accidental data sharing or saving to unsecured locations | Restrict device data backups  Restrict save-as  Disable printing | Restrict cut/copy/paste  Restrict save-as |

## 

For both, corporate and personal devices, you should define whether your users should be able to access your resources from within and outside your organization’s network. In addition to this, you should define whether a trusted device is required for an access attempt.

* **Microsoft Recommends:**
  + To grant access, require device to be marked compliant or an approved application

Now that you have seen how you can use Intune and Azure AD to protect corporate data on employee-owned devices, decide if you are going to use Intune as a device management solution with app management, or if you are going to focus solely on app management. With either option, you can use the identity and security features available with Azure AD. Use the Intune [Planning Guide](https://docs.microsoft.com/en-us/intune/planning-guide) to map out your next level of planning.

**Use the table below to design your policy. It will be used when configuring your policy. Default values have been provided. Change them as appropriate for you.**

|  |  |
| --- | --- |
| **Field** | **Value** |
| Policy Name | Compliant Device or Application |
| Users and Groups | <Insert users and groups> |
| Cloud Apps | All Cloud applications |
| Grant | Require device to be marked as compliant  Require approved client application |
| Multiple Controls | Require one of the selected controls |

### Password change for risky users

While ensuring that users’ credentials are not stolen is a top priority, there needs to be a plan when credentials are compromised. Microsoft identity protection can automatically detect when users’ credentials are leaked. Coupling Identity Protection with Conditional Access enables you to require that all users with compromised credentials have to change their password or are not allowed to access the application. Changing the password ensures that the leaked password is no longer valid.

|  |  |
| --- | --- |
| **Option 1 – Password Change** | **Option 2 – Block Access** |
| When a user attempts to sign into an application with compromised credentials, require that the user MFA into the app and update his / her password  **Note:** Enabling this requires that you have setup password writeback | When a user attempts to sign into an application with compromised credentials, block the user from getting access |

* **Microsoft Recommends:** Microsoft recommends requiring password change to ensure that the password is updated. This policy should be applied across all applications / users and groups in a tenant.

Learn More in the user risk security policy section: <https://docs.microsoft.com/en-us/azure/active-directory/active-directory-identityprotection#users-flagged-for-risk>

# Implementing Your Solution

The foundation of proper planning is the basis upon which you can deploy an application successfully with Azure Active Directory. It provides intelligent security and integration that simplifies onboarding while reducing the time for successful deployments. This combination ensures that your application is integrated with ease while mitigating down time for your end users.

Use the following phases to plan for and deploy your solution in your organization:

[Phase 1: Configuring your solution](#_Phase_1:_Implementation)

[Phase 2: Testing](#_Phase_2:_Testing)

[Phase 3: Rollback Steps](#_Phase_3:_Moving)

[Phase 4: Moving to Production](#_Phase_4:_Rollback)

## Phase 1: Implementation Steps

Use this section to help with your implementation. Based on the policies that you selected in the design section, identify the users, groups, conditions, and controls that apply to each policy.

*Identify a set of users and groups to validate the implementation*

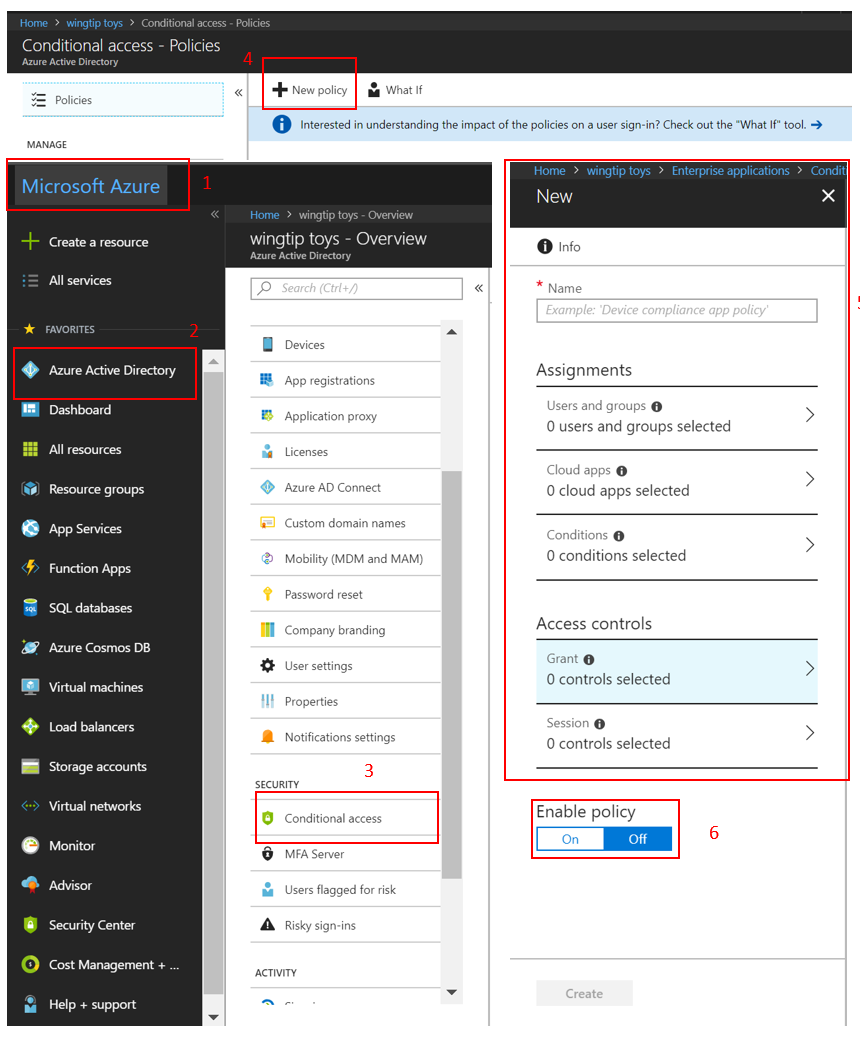
Microsoft recommends starting with a set of pilot users and groups before rolling out a Conditional Access policy to the entire set of users and groups that the policy covers. In this table, identify the test users that will verify that the policy is working.

|  |  |
| --- | --- |
| **Policy Name** | **Test Users and Groups** |
| <Insert Policy Name> | <Insert users and groups to test the policy> |
| <Insert Policy Name> | <Insert users and groups to test the policy> |

*Configuring your policy*

Once you’re ready to create your policy:

1. Go to **portal.azure.com**
2. Navigate to **Azure Active Directory**
3. Click on **Conditional Access** on the left navigation
4. Click on **New Policy**
5. Configure the **Users, Apps, Conditions, and Controls**
6. Set **Enable Policy** to on



## Phase 2: Testing

Use the following table to identify test cases that you would like to verify before rolling out your application to the rest of the organization. We’ve created a set of default use cases for you to get started with. Add and remove test cases based on the policies that you would like to implement. Leverage the [Whatif](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-conditional-access-whatif) tool to verify the scenarios below.

**Note:** Make sure to open a new browser session for all tests

* **Microsoft recommends** using the Whatif tool to verify that policies are working as expected

The following table outlines example test cases. Adjust the scenarios and expected results based on how your CA policies are configured.

|  |  |  |  |
| --- | --- | --- | --- |
| Policy | Scenario | Expected Results | Actual Results |
| MFA when not at work | Authorized user signs into the app while **on** a trusted location / work | User is **not** prompted to MFA | <Input actual result> |
| MFA when not at work | Authorized user signs into the app while **not on** a trusted location / work | User **is** prompted to MFA and can sign in successfully | <Input actual result> |
| MFA for Admins | Global Administrator signs into <Insert App Name> | Admin **is** prompted to MFA | <Input actual result> |
| Risky Sign-Ins | User signs into <Insert app name> using a [Tor browser](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-identityprotection-playbook) | Admin **is** prompted to MFA | <Input actual result> |
| Device Management | Authorized user attempts to sign in from an authorized device | Access Granted | <Input actual result> |
| Device Management | Authorized user attempts to sign in from an unauthorized device | Access blocked | <Input actual result> |
| Password Change for risky users | Authorized user attempts to sign in with compromised credentials (high risk sign in) | User is prompted to change password or access is blocked based on your policy | <Input actual result> |

## Phase 3: Moving to production

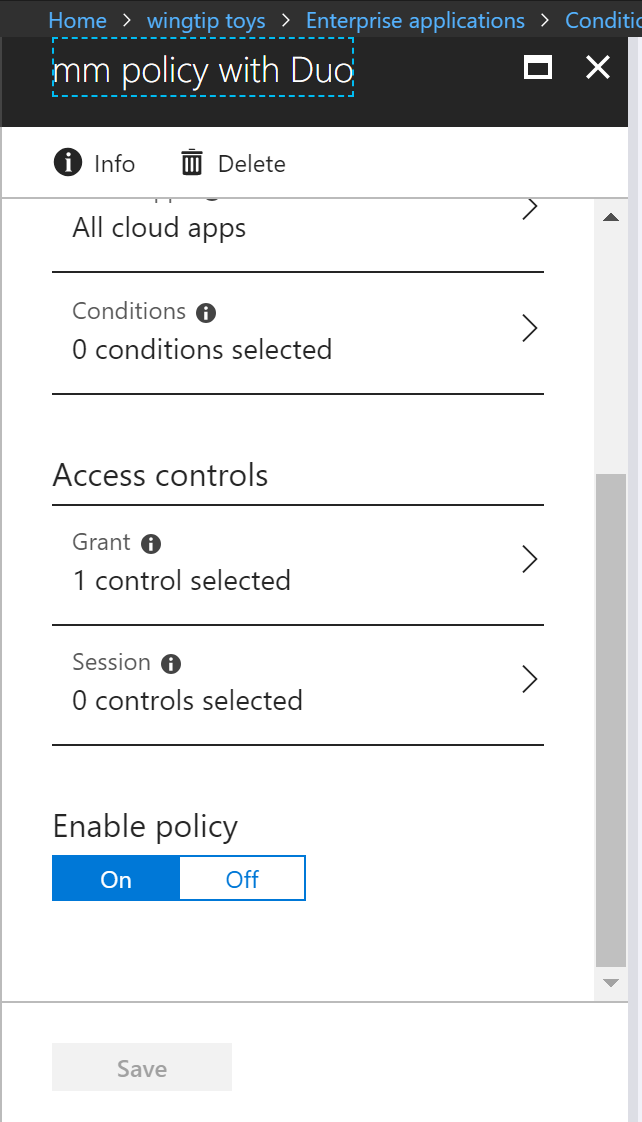
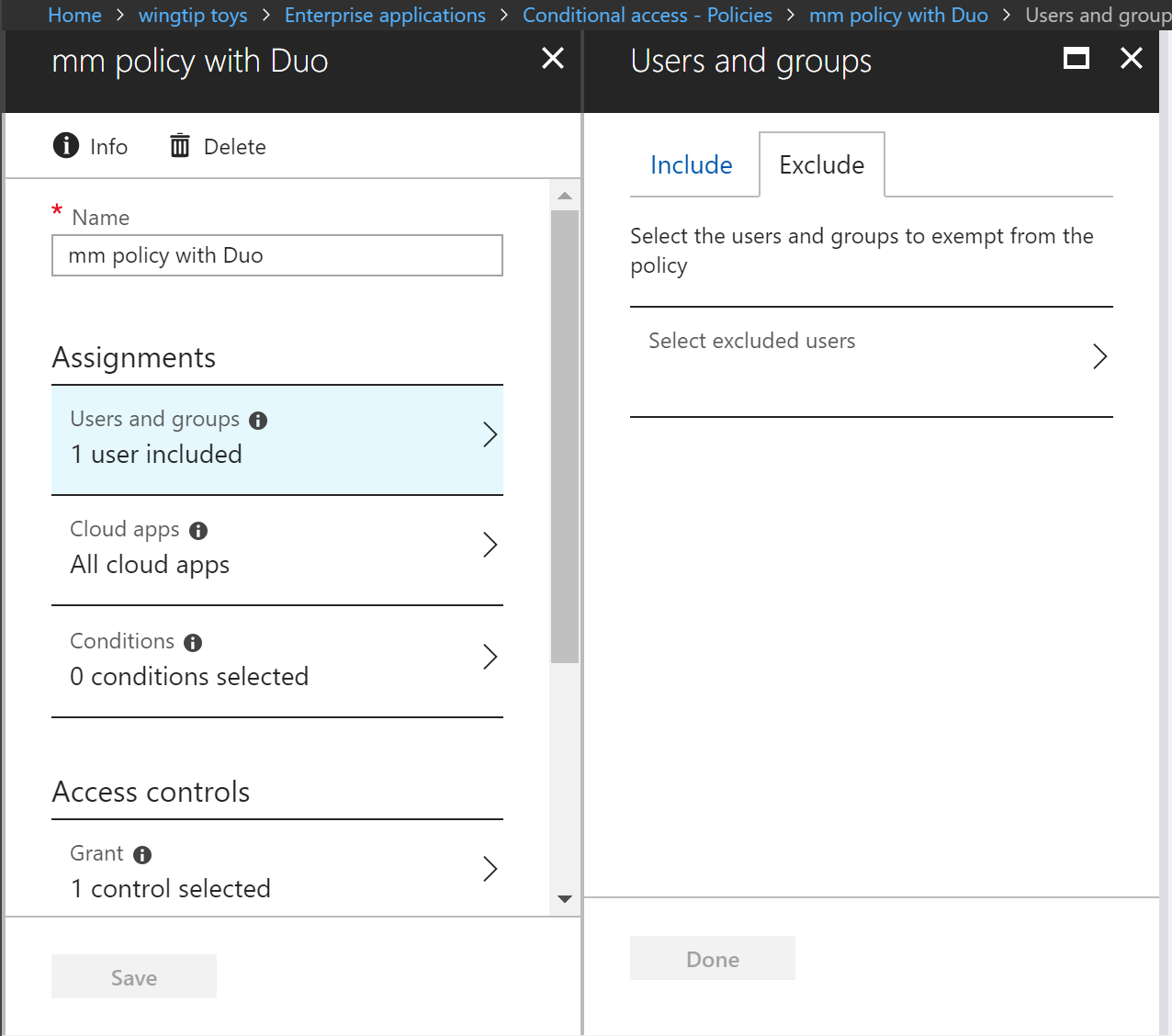
1. Provide Internal Change Communication to end users.
2. Apply a policy to a small set of users and verify it behaves as expected.
3. When you expand a policy to include more users, continue to exclude one administrator from the policy. This ensures that administrators still have access and can update a policy if a change is required.

**Best practices for deploying to production:** <https://docs.microsoft.com/azure/active-directory/active-directory-conditional-access-best-practices#how-should-you-deploy-a-new-policy>

## Phase 4: Rollback Steps

Use the following options to roll back a Conditional Access policy

|  |  |  |
| --- | --- | --- |
| **Disable the policy** | **Exclude a user / group from a policy** | **Delete the policy** |
| Disabling a policy ensures it does not apply when a user tries to sign in  You can always come back and enable the policy when you’d like to use it | If a user is unable to access his / her application, you can choose to exclude the user from the policy  Note: This option should be used sparingly, only in situations where the user is trusted. The user should be brought back into the policy as soon as possible | If the policy is not needed anymore, you can always choose to delete the policy |

# Managing your solution

## Required Roles

Azure AD roles enable you to delegate the ability to configure and view Conditional Access policies based on your role. The following roles can read and or write Conditional Access policies

* Global Admin (can read / write)
* Conditional Access Admin (can read / write)
* Security Admin (can read / write)
* Security Reader(can only review the policies)
  + This role is often assigned to those in help desk so that they can troubleshoot

Identify who in your organization needs permission to manage Conditional Access policies and what role would be appropriate for them.

* **Microsoft recommends** limiting the number of users that have global admin rights. Provide users with the role that is most limited, while still meeting the needs of the user

In the table below, identify who in your organization will have the permissions necessary to manage Conditional Access policies

|  |  |
| --- | --- |
| Person | Role |
| <Insert Name / email address> | <Insert Role> |
| <Insert Name / email address> | <Insert Role> |
| <Insert Name / email address> | <Insert Role> |
| <Insert Name / email address> | <Insert Role> |

Learn More About [Azure AD Administrative Roles](https://docs.microsoft.com/azure/active-directory/active-directory-assign-admin-roles-azure-portal)

**IMPORTANT NOTICES**

© 2018 Microsoft Corporation.  All rights reserved.  This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it.   
Some examples are for illustration only and are fictitious. No real association is intended or inferred.   
   
This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes. You may modify this document for your internal, reference purposes

**Confidentiality Statement**

This document may provide certain information that is and must be kept confidential. To ensure the protection of such information you should not disclose any part of this plan summary to anyone who does not have a legitimate reason for using it.