Implementing conditional access and compliance policies for devices

1. **Understanding conditional access policies**

What is Conditional Access?

* Conditional Access is a tool in Azure that brings signals together for access decision making
* Signals help in decision making on whether to allow access or enforce certain policies

*The Dilemma of Modern Administration*

* Administrators today must allow users to be productive anywhere at anytime and from a massive selection of applications.
* Administrators are also expected to protect organizational data/assets all at the same time.

Signal examples = user and location, devices, application, real time risk, ip location info, Microsoft cloud app security,

Those signals need to “Verify every access attempt” using allow access, require MFA or block access depending on the signal.

Decisions = Block Access, Grant Access, Require MFA, Compliant Device, Require Hybrid Azure AD Joined, Require Approved App.

Apps and Data = are allowed once authenticated against the signals and verification

1. **Implement conditional Access Policies**

Endpoint.microsoft.com > Devices > Conditional Access

Or can be done in

portal.azure.com >aad> security > conditional Access Policies

Step 1.) Who is getting this policy assigned to them? (Exclusions will override inclusions)

Step 2.) Select the Cloud apps you wish to have included in the conditional access policy

Step 3.) Assign the conditions. Decide what is high medium or low risk. Usually, will exclude the location based on where you work. Client apps are browser-based apps which has legacy use for exchange. Device State needs to be hybrid azure ad joined or marked as compliant. If we created a compliance policy, we could have this conditional access policy deny you.

Step 4.) Grant Control User Access Enforcement to block or grant access. Then you can decide how many controls you would like to implement onto that policy.

Step 5.) Enable the policy.

NOTE: The Security Defaults must be disabled before enabling the conditional access Policy.

Portal.azure.com > AAD > Properties > Manage Security Defaults. This must be disabled and its because we are using conditional access policies. (This is already disabled in our environment)

1. **Understanding Device Compliance Policies**

What are Compliance Policies

* Compliance Policies help create the rules and settings that users and devices must meet to be compliant.
* When combined with Conditional Access, admins can block users and devices that don’t meet the rules.

Ways to use Compliance Policies

1. With Conditional Access – If devices do not comply, they do not get access to organizational resources
2. Without Conditional Access – If devices don’t comply, they don’t get restricted, but reports are generated for monitoring.

What are the Non-Compliant Settings?

* Pin or password configuration
* Device Encryption
* Jailbroken or rooted device
* Email profile
* Minimum OS version
* Maximum OS version
* Windows Health Attestation.

What is the Outcome of Non-Compliance?

* Remediated: the device OS enforces compliance. For Example, the user is forced to set a PIN or update the OS
* Quarantined: The Device OS doesn’t enforce compliance. For example, Android and Android Enterprise devices don’t force the user to encrypt the device. When the device isn’t compliant, the following actions take place:
  + -if a conditional access policy applies to the user, the device is blocked.
  + The company Portal app notifies the user about any compliance problems.

1. **Implementing and managing compliance policies**

Enpoint.microsoft.com > Devices > Conditional Access Policies >create policy

Then Define the compliance settings. Like Require bit locker, require secure boot to be enabled on this device, require code integrity (checks the tpm code)

Device properties – Minimum OS Version and max os version so could use that not to upgrade to windows 11.

System Security Settings

Password require complex password (redefine the password policy.

Set the actions for noncompliance whether that’s blocking or logging. Scope tags, assignments (who gets the compliance policy)

Notes on issue with the Configuration policy: Devices show conflicts and error with the antivrus protection policy under the system account (there is a conflict) error with NSW-Wi-Fi policy (checked omars account.

On Tyler’s account conflict with the Microsoft defender AV.

Also issue with real time protection and password length. (looks like windows defender is blocking the policy and windows defender needs to be updated to allow real time protection.

Note on issue with Compliance: real-time protection is not compliant.