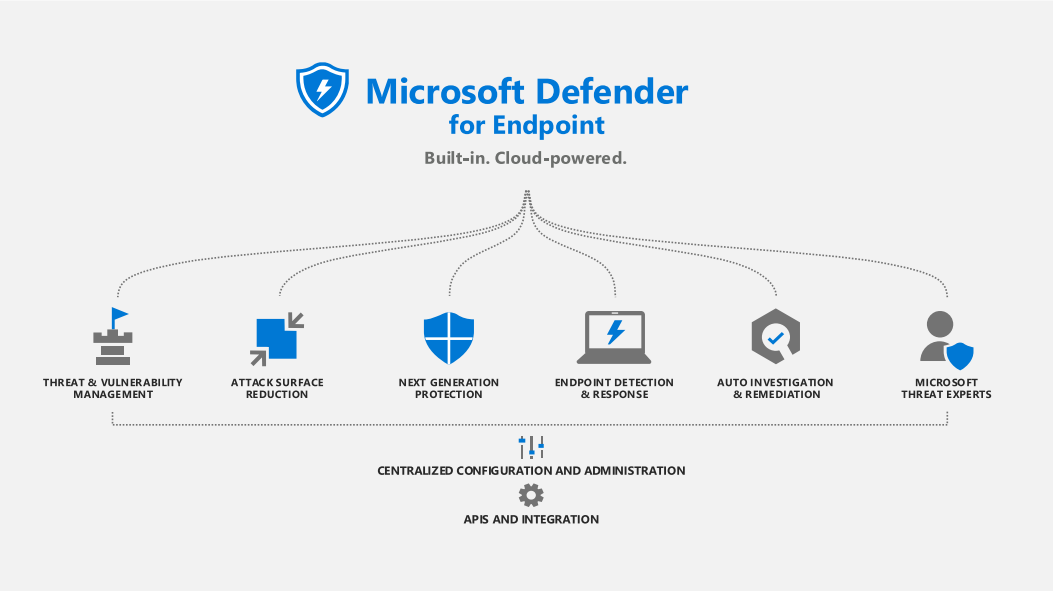
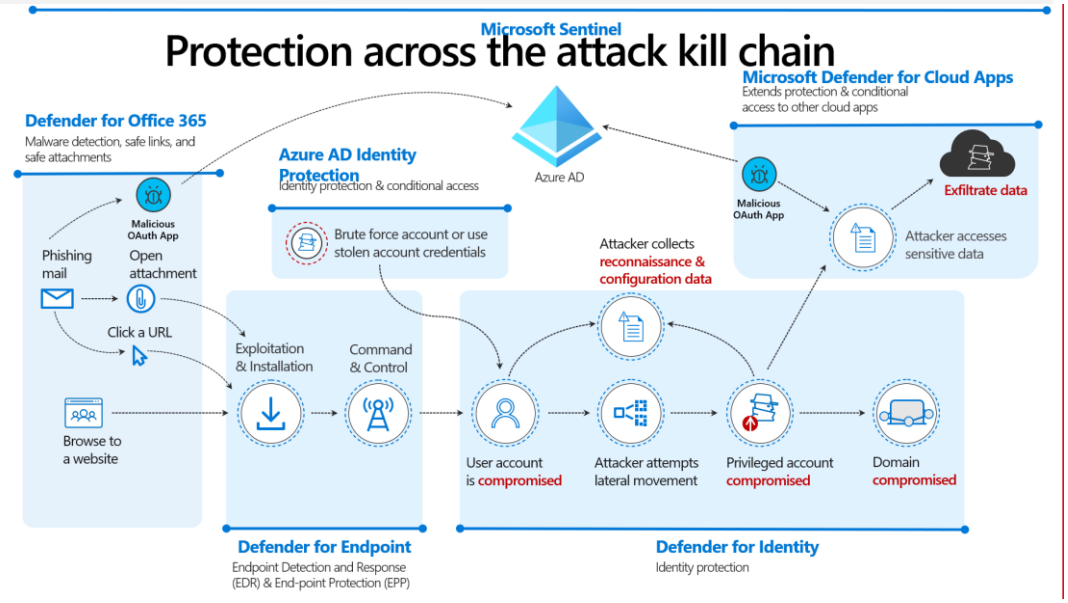
FIRST - M365 DEFENDER XDR

Attendees will get an opportunity to try their hands at configuration, detection and security analysis using MS tools such as the Defender XDR products and Azure Sentinel.
The workshop is aimed at security analysts and technical staff looking to learn or get more out of the security consoles provided within the Microsoft E5 suite.
“Best Practices” for configuration of Defender for Endpoints, Defender for Office and Cloud App Security will be covered, as well as analysis and mitigation of real attack scenarios.
The workshop will be held by Kent Husvik, Kjetil Nordlund and Richard Skjærstad from Microsoft Norway, assisted by personnel.





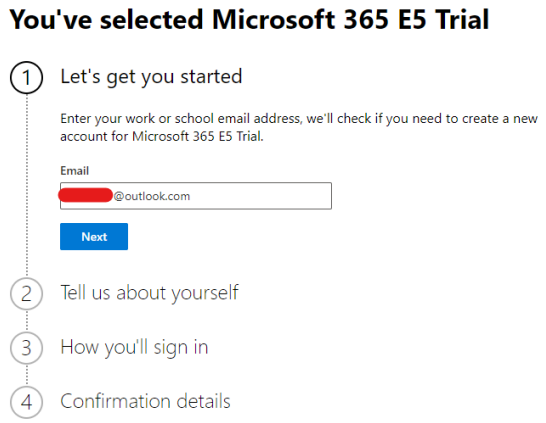
CONTENTS

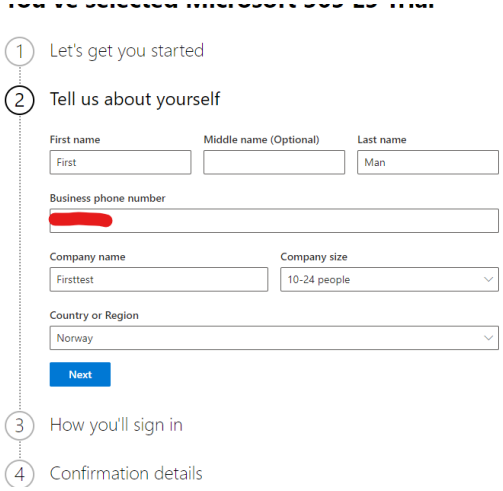
PRE WORKSHOP - PREPERATIONS

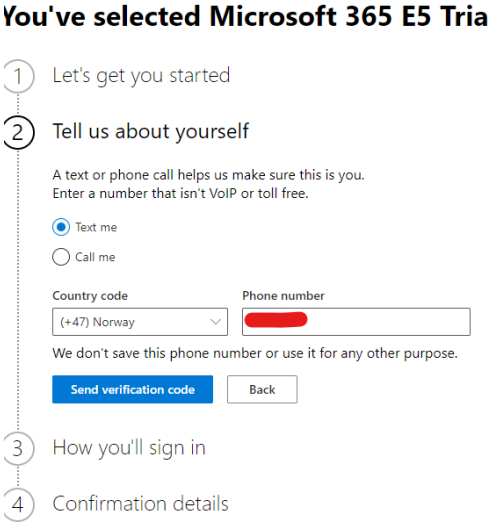
Create a New Email account, like Outlook.com or any other that you like.

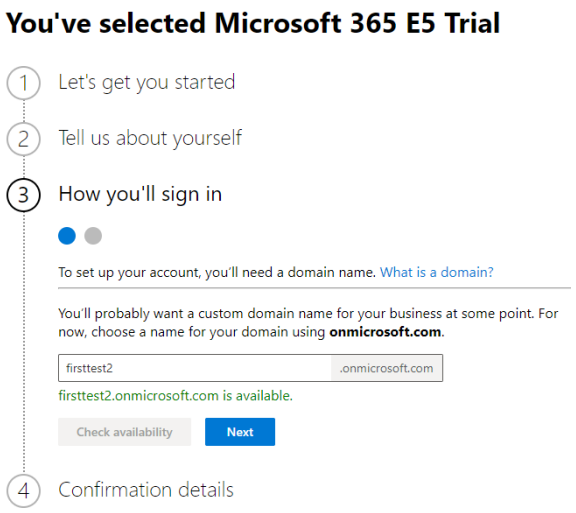
Create a M365 E5 Trial and connect it to the newly created Email account

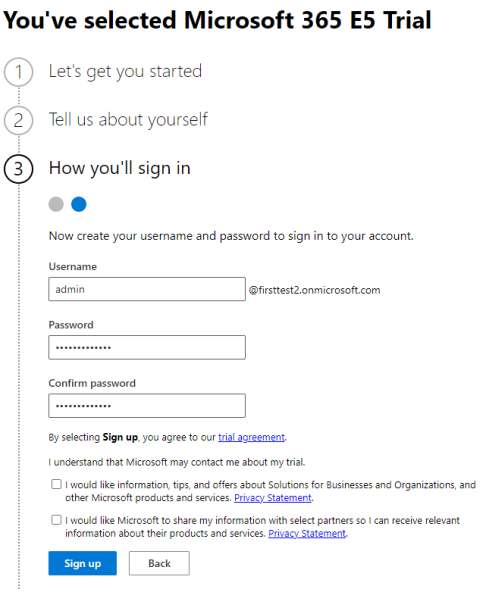
Use the newly created email account in the registration form

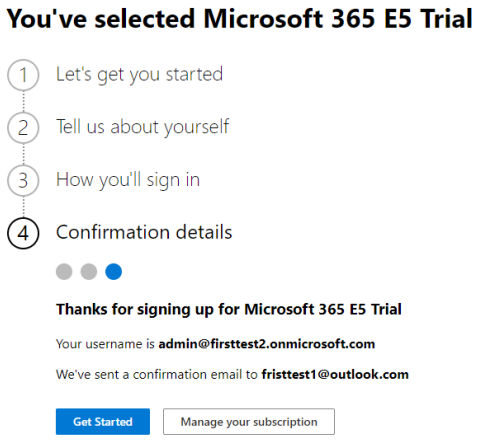






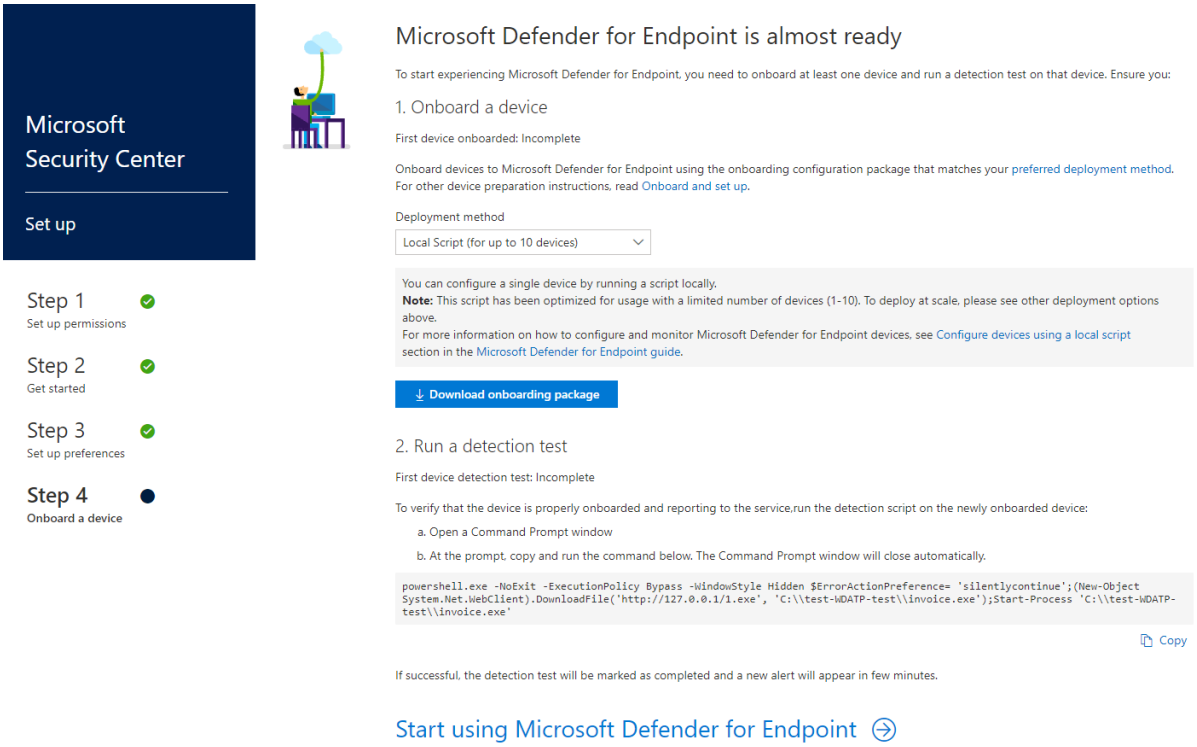






Complete the wizard.

Click on Get Started complete the steps required on Data storage location. If any service error message are being displayed, wait a few minutes on the backend provisioning and try again.



DATA STORAGE LOCATION

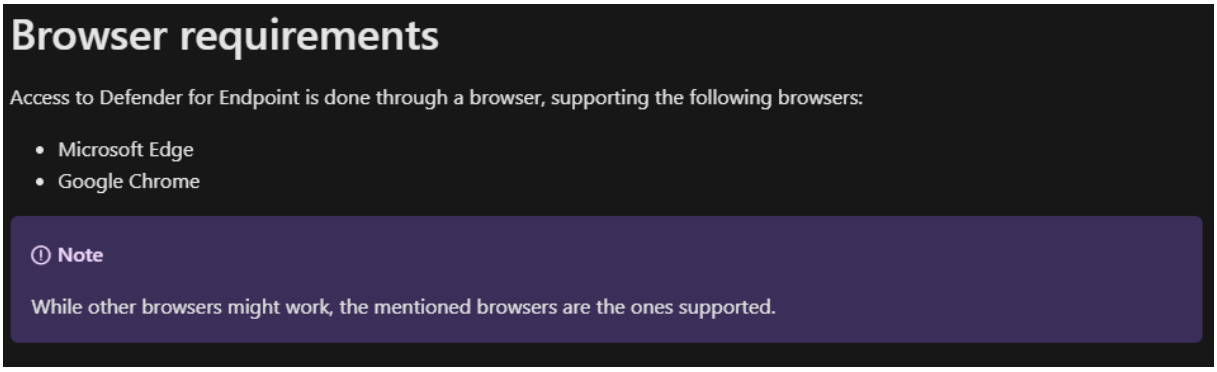
Defender for Endpoint operates in the Microsoft Azure datacenters in the European Union, the United Kingdom, or in the United States. Customer data collected by the service may be stored in: (a) the geo-location of the tenant as identified during provisioning or, (b) if Defender for Endpoint uses another Microsoft online service to process such data, the geolocation as defined by the data storage rules of that other online service.

SETTINGS AND PREVIEW FEATURES

SECURITY CONSOLE WELCOME WIZARD

Navigate in a supported browser to Security.microsoft.com and complete the wizard.

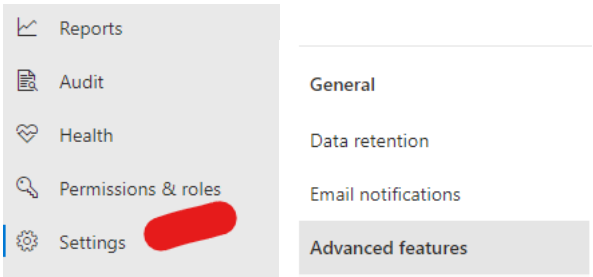
Minimum requirements for Microsoft Defender for Endpoint | Microsoft Docs



Turn on Preview features and other features:

Turn on the preview experience setting to be among the first to try upcoming features.

1. In the navigation pane, select **Settings** > **Endpoints** > **Advanced features** > **Preview features**.



2. Toggle the setting between **On** and **Off** and select **Save preferences**.
3. Reload the console and find your way back to **Settings** > **Endpoints** > **Advanced features**
4. Activate all features Except “Restrict correlation to within scoped device groups”

On

Automated Investigation
Enables the automation capabilities for investigation and response.

On

Live Response
Allows users with appropriate RBAC permissions to investigate devices that they are authorized to access, using a remote shell connection.

On

Live Response for Servers
Allows users with Live Response privileges to connect remotely to servers (Windows Server or Linux devices) that they are authorized to access.

On

Live Response unsigned script execution
Enables using unsigned PowerShell scripts in Live Response.

On

Enable EDR in block mode
When turned on, Microsoft Defender for Endpoint leverages behavioral blocking and containment capabilities by blocking malicious artifacts or behaviors observed through post-breach endpoint detection and response (EDR) capabilities. This feature does not change how Microsoft Defender for Endpoint performs detection, alert generation, and incident correlation. To get the best protection, make sure to apply security baselines in Intune. See EDR in block mode for more details.

On

Automatically resolve alerts
Resolves an alert if Automated investigation finds no threats or has successfully remediated all malicious artifacts.

On

Allow or block file
Make sure that Windows Defender Antivirus is turned on and the cloud-based protection feature is enabled in your organization to use the allow or block file feature.

On

Custom network indicators
Configures devices to allow or block connections to IP addresses, domains, or URLs in your custom indicator lists. To use this feature, devices must be running Windows 10 version 1709 or later. They should also have network protection in block mode and version 4.18.1906.3 or later of the antimalware platform (see KB 4052623). Note that network protection leverages reputation services that process requests in locations that might be outside of the location you have selected for your Microsoft Defender for Endpoint data.

On

Tamper protection
Keep tamper protection turned on to prevent unwanted changes to your security solution and its essential features.

ⓘ MAPS (Cloud-delivered Protection) is required. Learn more.

On

Show user details
Enables displaying user details: picture, name, title, department, stored in Azure Active Directory.

On

Skype for business integration
Enables 1-click communication with users.

Pending

Microsoft Defender for Identity integration
Retrieves enriched user and device data from Microsoft Defender for Identity and forwards Microsoft Defender for Endpoint signals, resulting in better visibility, additional detections, and efficient investigations across both services. Forwarded data is stored and processed in the same location as your MDI data.

ⓘ Feature has not been fully enabled. Enable integration on the Advanced Threat Analytics portal.

Pending

Office 365 Threat Intelligence connection 1
Connects to Office 365 Threat Intelligence to enable security investigations across Office 365 mailboxes and Windows devices.
For more information, see the Office 365 Threat Intelligence overview.

On

Microsoft Cloud App Security
Forwards Microsoft Defender for Endpoint signals to Cloud App Security, giving administrators deeper visibility into both sanctioned cloud apps and shadow IT. It also gives them the ability to block unauthorized applications when the custom network indicators setting is turned on. Forwarded data is stored and processed in the same location as your Cloud App Security data. This feature is available with an E5 license for Enterprise Mobility + Security on devices running Windows 10 version 1709 (OS Build 16299.1085 with KB4493441), Windows 10 version 1803 (OS Build 17134.704 with KB4493464), Windows 10 version 1809 (OS Build 17763.379 with KB4489899) or later Windows 10 versions.

On

Microsoft Secure Score
Forwards Microsoft Defender for Endpoint signals, giving Microsoft Secure Score visibility into the device security posture. Forwarded data is stored and processed in the same location as the your Microsoft Secure Score data.

On

Web content filtering
Block access to websites containing unwanted content and track web activity across all domains. To specify the web content categories you want to block, create a web content filtering policy. Ensure you have network protection in block mode when deploying the Microsoft Defender for Endpoint security baseline.

On

Download quarantined files
Backup quarantined files in a secure and compliant location so they can be downloaded directly from quarantine.

On

Share endpoint alerts with Microsoft Compliance Center
Forwards endpoint security alerts and their triage status to Microsoft Compliance Center, allowing you to enhance insider risk management policies with alerts and remediate internal risks before they cause harm. Forwarded data is processed and stored in the same location as your Office 365 data.

On

Microsoft Intune connection
Connects to Microsoft Intune to enable sharing of device information and enhanced policy enforcement.
Intune provides additional information about managed devices for secure score. It can use risk information to enforce conditional access and other security policies.

On

Device discovery
Allows onboarded devices to discover unmanaged devices in your network and assess vulnerabilities and risks. For more information, see Device discovery settings to configure discovery settings.

On

Preview features
Allow access to preview features. Turn on to be among the first to try upcoming features.
See the Microsoft Defender for Endpoint preview features section in the Microsoft Defender for Endpoint guide.

Microsoft Threat Experts - Targeted Attack Notifications
Microsoft Threat Experts is a managed threat hunting service that provides expert level monitoring and analysis for critical threats facing their organization.

ENROLL EVALUATION LAB

[Microsoft Defender for Endpoint evaluation lab | Microsoft Docs]

Welcome to the Microsoft Defender for Endpoint Evaluation lab

Learn about the Microsoft Defender for Endpoint platform capabilities through a virtual evaluation lab that's ready to go, complete with onboarded test devices. See it in action as it detects and prevents the most sophisticated attacks.

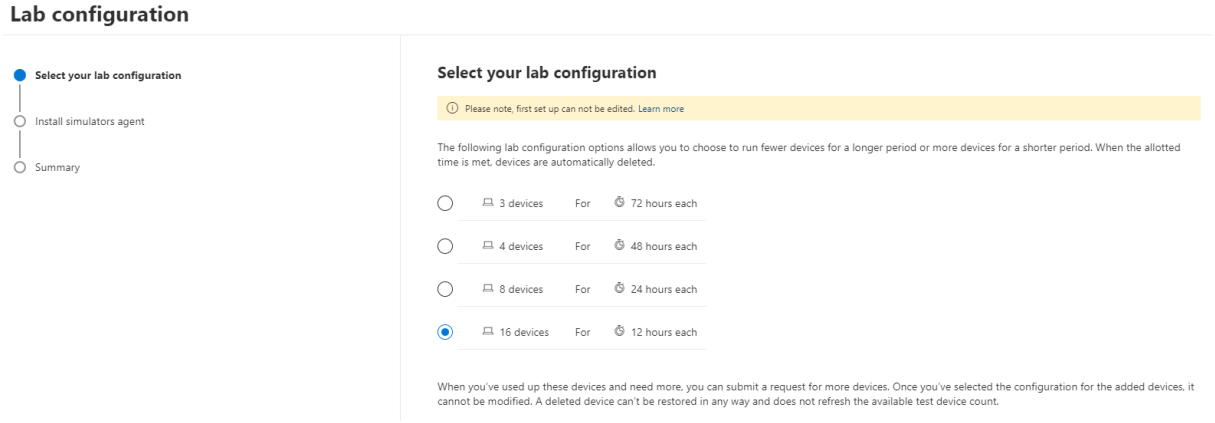
Learn more

Setup lab

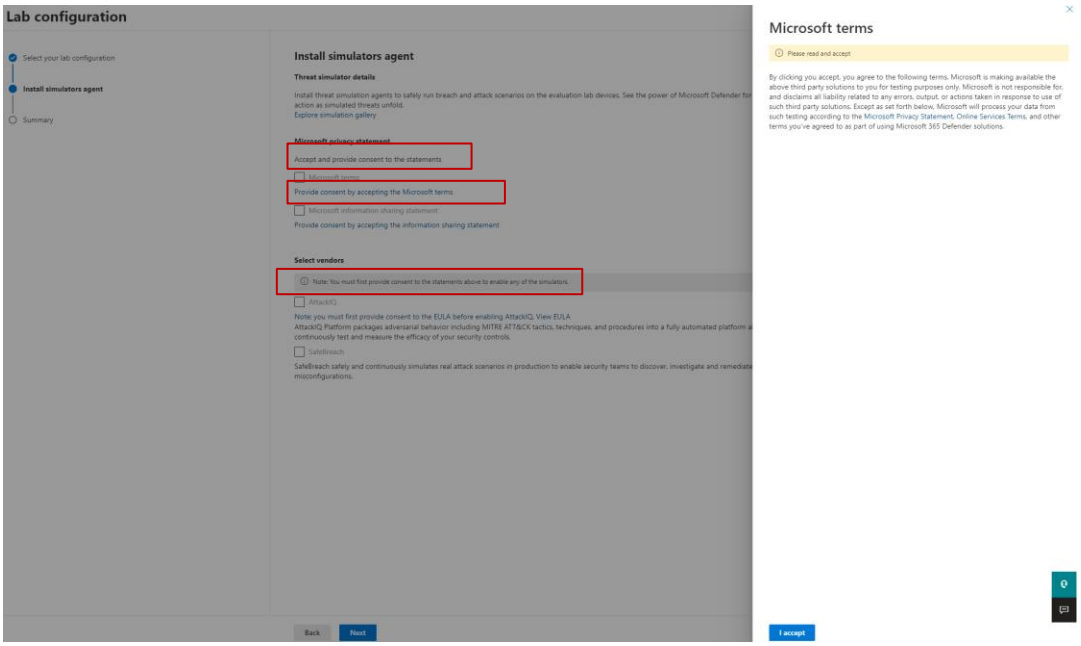
The Microsoft Defender for Endpoint evaluation lab is designed to eliminate the complexities of device and environment configuration so that you can focus on evaluating the capabilities of the platform, running simulations, and seeing the prevention, detection, and remediation features in action.

In the security.microsoft.com portal go to; Endpoints > Evaluation and learning > Evaluation lab

1. Click on Setup lab
2. Select the setup of your choice. This can only be done once and cannot be changed.
   I recommend 16 devices for 12 hours.

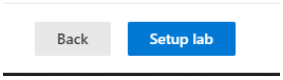


3. Accept and provide the Microsoft terms and Eula for AttackIQ and SafeBreach (click on the links to accept)

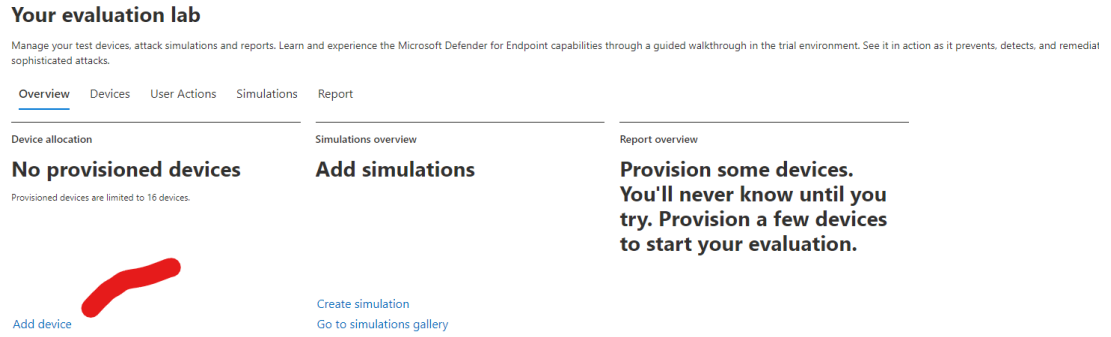


Choose both “AttackIQ” and “SafeBreach” and fill in your trial email and name

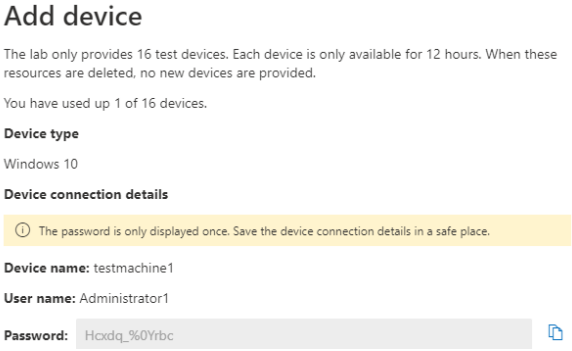
4. Click on the Setup lab



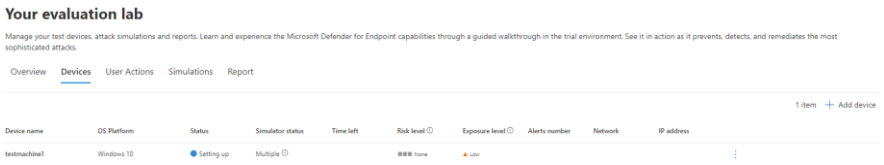
5. Click on Add device and select the default Windows 10 machine with Java, Office, Python, Sysinternals.



6. Remember to Copy and paste the Username and Password for the machine.

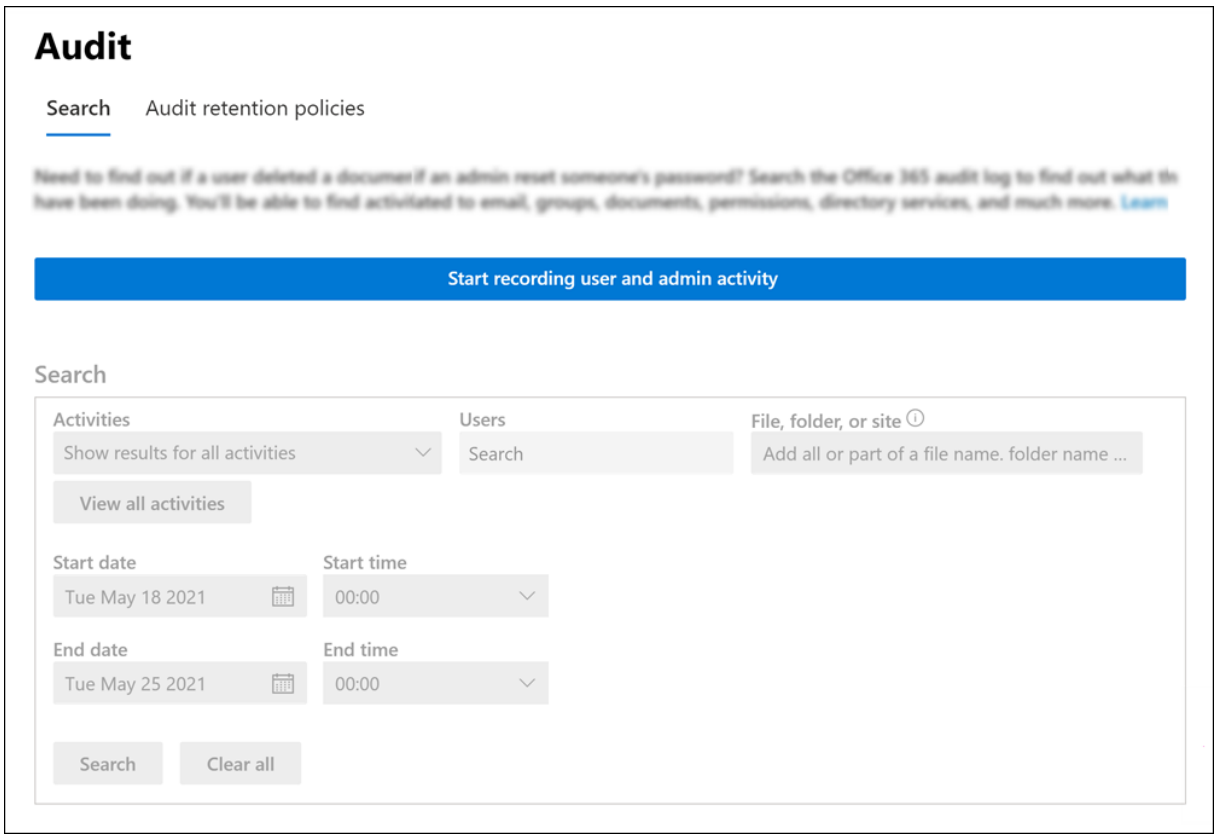


7. The device will now be provisioned in the back ground. When done Create one more machine.



TURN ON AUDITING

1. If auditing is not turned on for your organization, you can turn it on in the Microsoft 365 compliance center or by using Exchange Online PowerShell. It may take several hours after you turn on auditing before you can return results when you search the audit log.
2. Use the compliance center to turn on auditing
3. Go to compliance.microsoft.com and sign in.
4. In the left navigation pane of the Microsoft 365 compliance center, click **Audit**.
5. If auditing is not turned on for your organization, a banner is displayed prompting you start recording user and admin activity.



6.
7. Click the **Start recording user and admin activity** banner.
8. It may take up to 60 minutes for the change to take effect.

TEST USERS AND GROUPS

Create at least three regular users in your Azure AD tenant in addition to your Global Administrator user created when activated the tenant.

Create at least three Azure AD groups in your Azure AD tenant.

TURN OFF "SECURITY DEFAULTS"

To be able to test Conditional Access policies, the default enabled "Security Defaults" need to be turned off first.

Disabling Security Defaults: Azure Active Directory security defaults | Microsoft Docs

To disable security defaults in your directory:

1. Sign in to the Azure portal as a security administrator, Conditional Access administrator, or global administrator.
2. Browse to **Azure Active Directory** > **Properties**.
3. Select **Manage security defaults**.
4. Set the **Enable security defaults** toggle to **No**.

ENABLE BASIC CONDITIONAL ACCESS POLICIES

To maintain the security level in your Azure AD tenant, create one Conditional Access policy enforcing MFA for all your users.

NB! Make sure your Global Admin users (and other test users) is enrolled with MFA information before you activate MFA requirement for all users.

https://mysignins.microsoft.com/security-info

Follow these steps to create a Conditional access policy requiring MFA for all users:
Conditional Access - Require MFA for all users - Azure Active Directory | Microsoft Docs

In addition, create one Conditional Access policy to block use of all Legacy authentication protocols in your tenant.

AZURE ACTIVE DIRECTORY IDENTITY PROTECTION

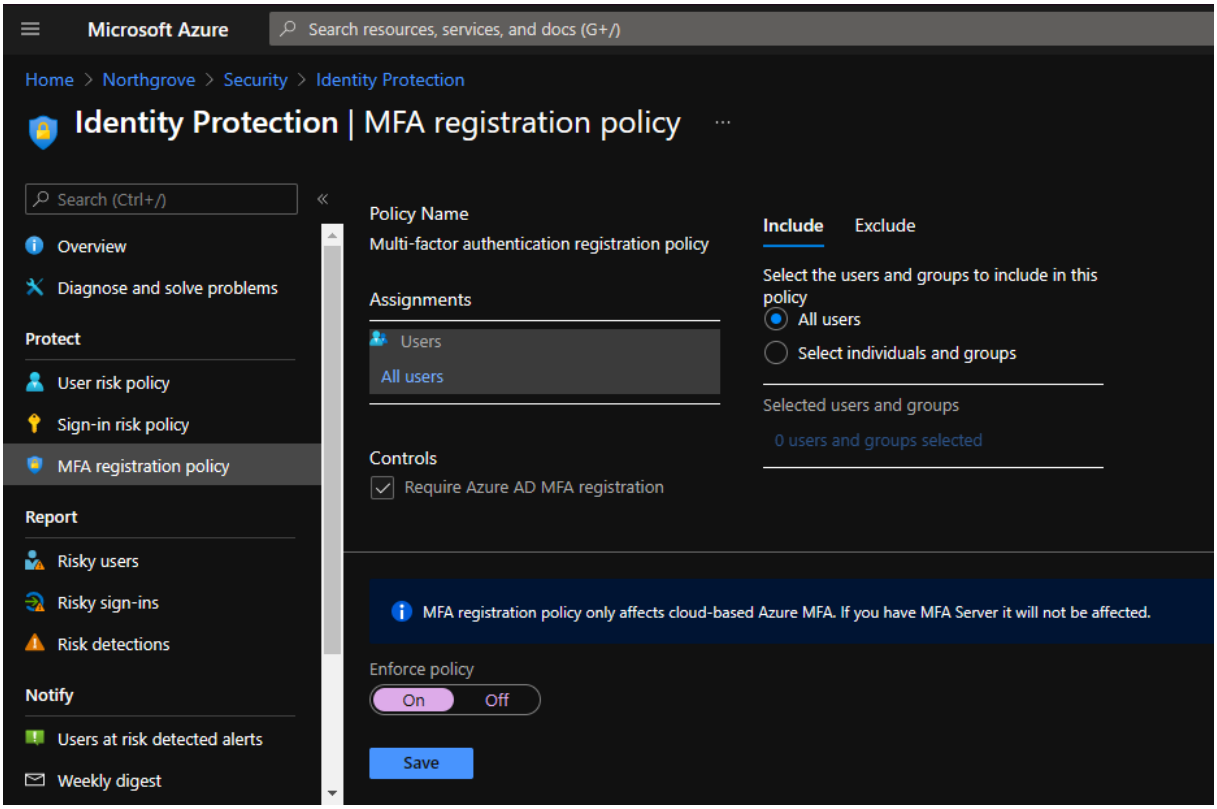
SETUP AND CONFIGURATION

Configure Azure AD Identity protection risk policies - Azure AD Identity Protection policies | Microsoft Docs

Configuration is done in the Azure Portal -> https://portal.azure.com -> Azure Active Directory -> Security -> Identity Protection

Deep link: Identity Protection - Microsoft Azure

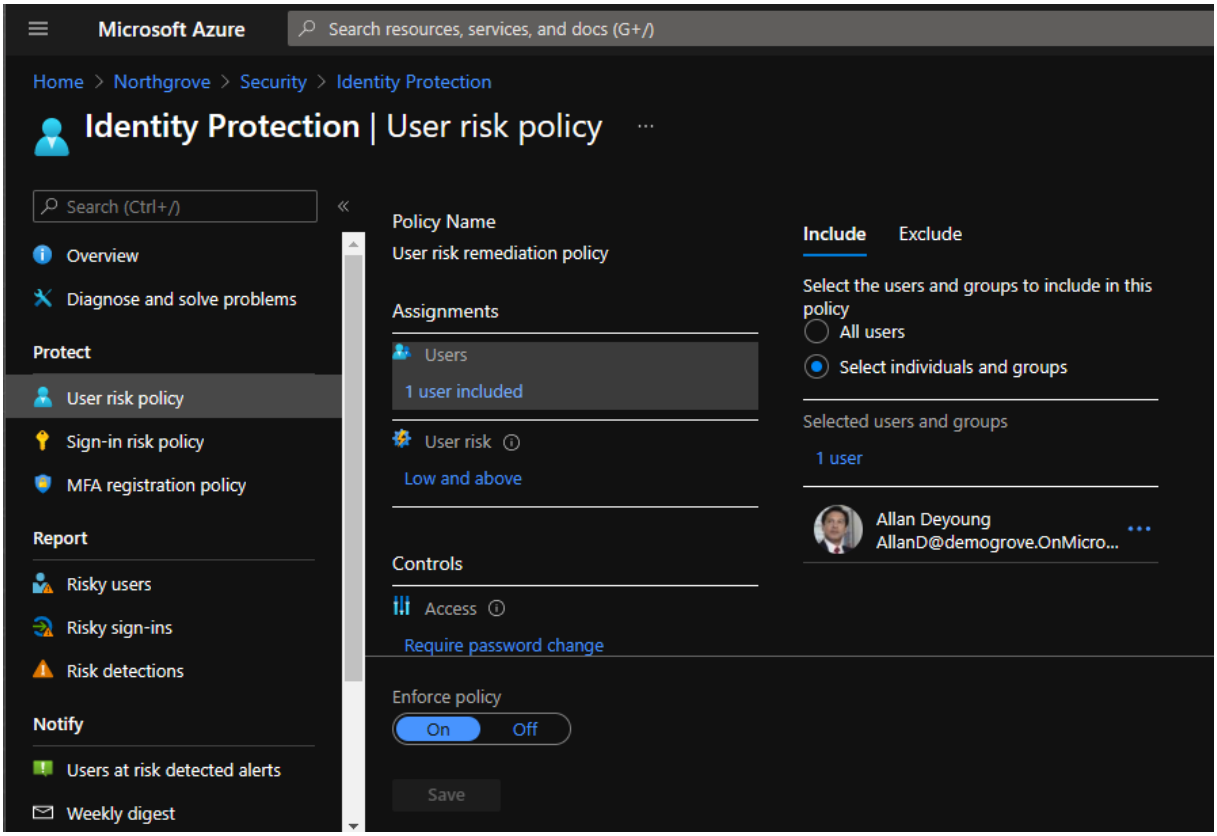
Create an MFA registration Policy:



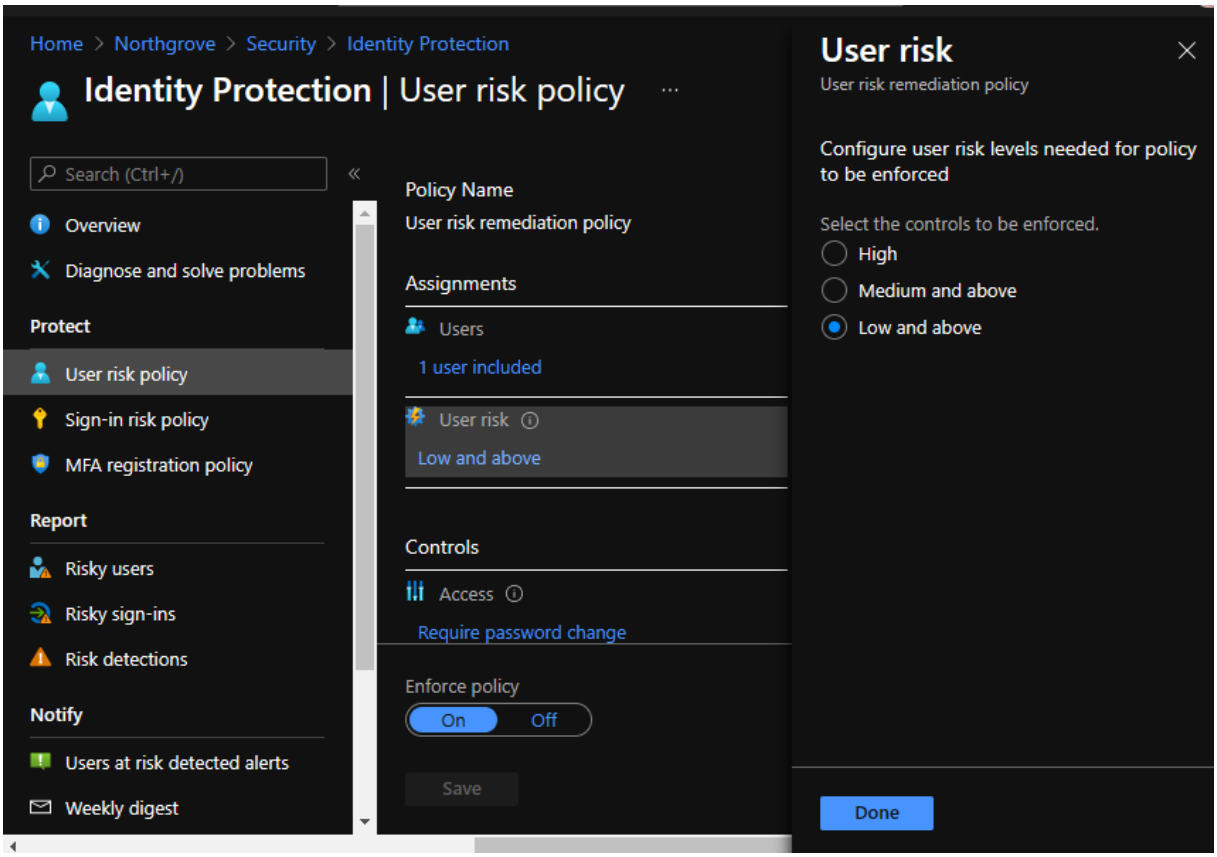
Assignments: All users
Controls: Require Azure AD MFA registration
Enforce policy: On
[save]

This policy will enforce all users in the tenant to register for MFA. An MFA registration wizard will appear during login. The users have the option to postpone the MFA registration up to 14 days.

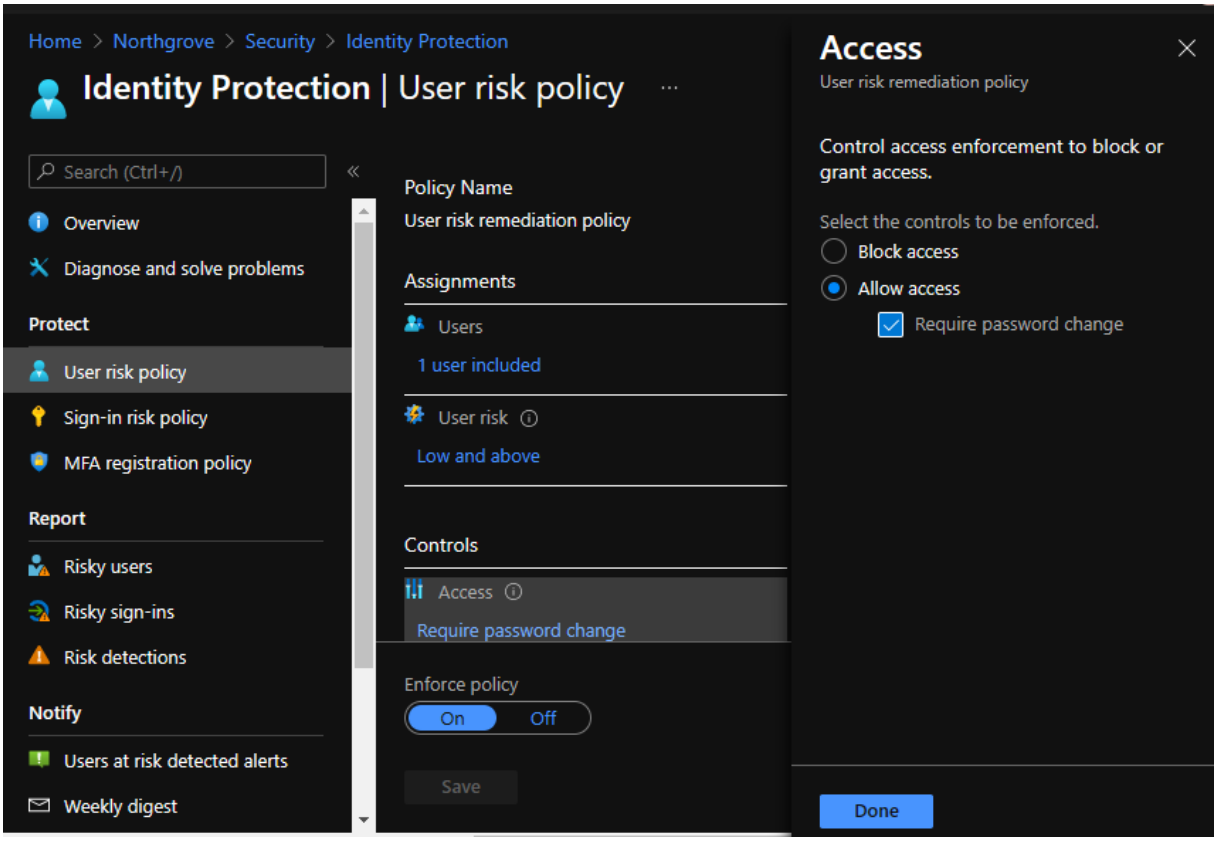
Create a risky user policy:



Assignments: Assign this policy only to *"testUser1"*

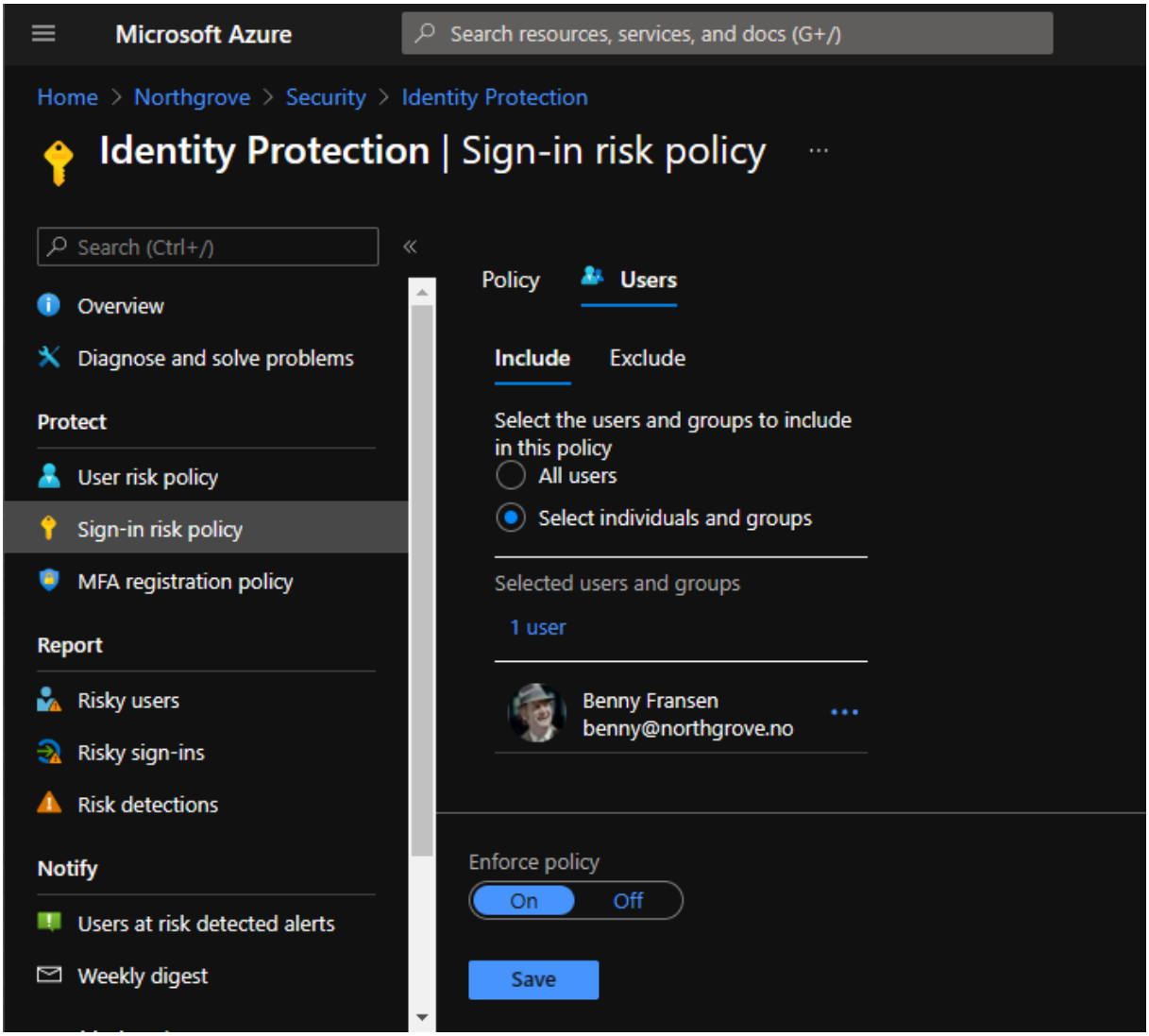


User risk: choose *"Low and above"*

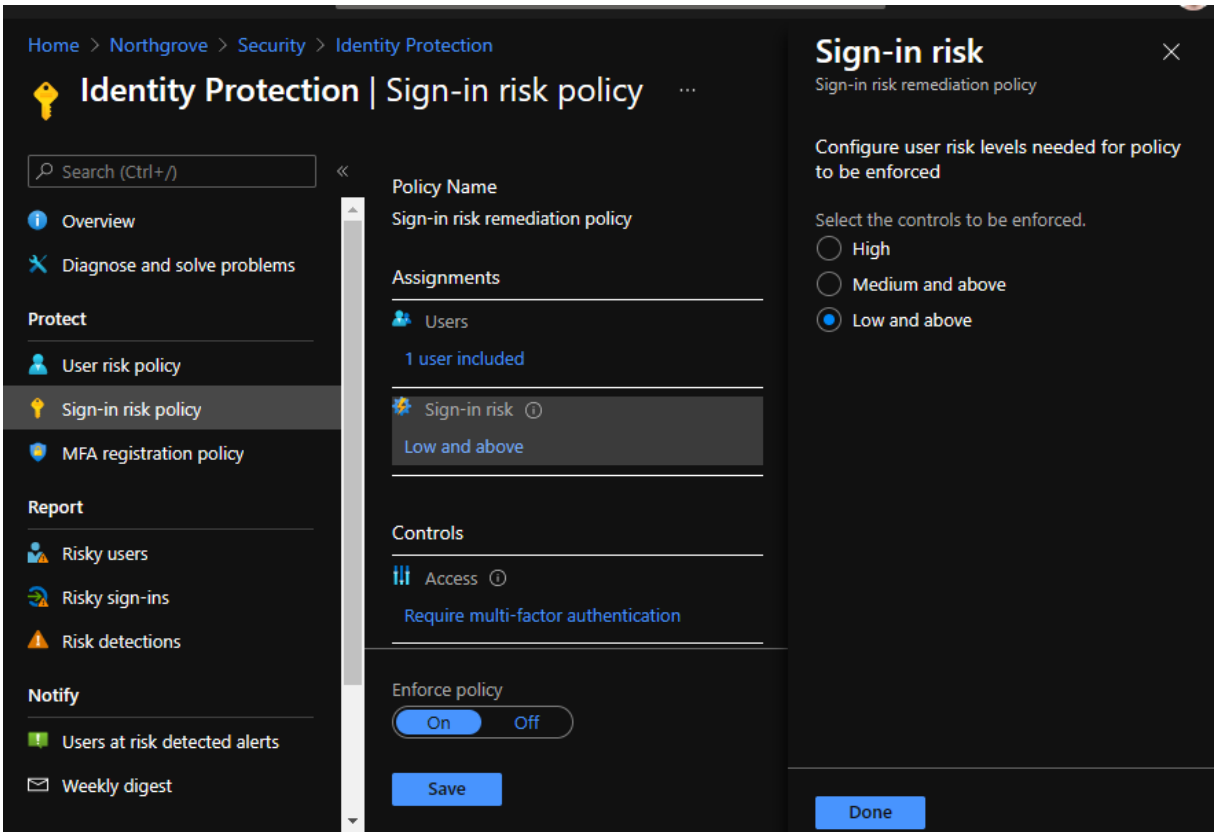


Controls: *Allow access + require password change*

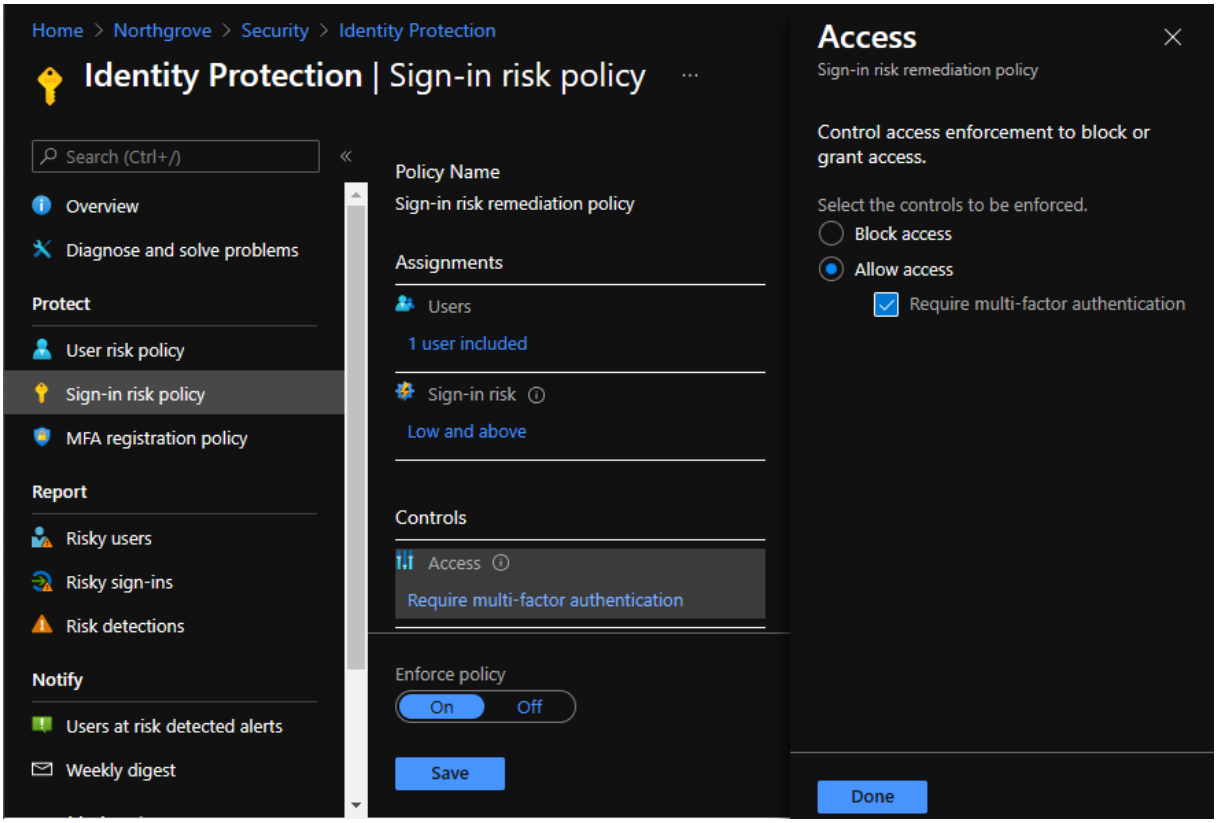
Create a risky sing-in policy



Assignments: Assign this policy only to *"testUser1" and "testuser2"*



Sign-in risk: choose *"Low and above"*



Controls: Allow access + require multi-factor authentication

RISK BASED CONDITIONAL ACCESS

Configuration of Conditional Access is done in the https://portal.azure.com -> Azure Active Directory -> Security -> Conditional Access

Deep link: Conditional Access - Microsoft Azure

Create a new Conditional Access policy with the following configuration:

Name	Block risky users
Users and groups	Choose your “testuser1”, “testuser2” and “testuser3”
Cloud Apps -> Selected Apps	“Office 365 Exchange online”
Conditions -> User risk	“yes” + “low” and “medium” and “high”
Grant	“Block access”
Enable policy	“On”

This policy will block users with any level of user risk from accessing Office 365 Exchange Online

TEST SCENARIO – IDENTITY PROTECTION

1. Anonymous login detection
    - On your test client, download and install the TOR browser - Tor Project | Download
    - Start the TOR browser, and connect to the TOR network
    - Login with your test account “testuser1” to https://portal.azure.com
    - Sign-in is interrupted with a “risky signin detected”. Cancel the sign-in
        - (if no Suspiciouse activity detected warning sign shows up, interrupt the sign-in, restart the TOR-browser and try sign-in again)
    - Close the TOR browser.
    - Re-open the TOR browser and create a new connection to the TOR network.
    - Login with your test account “testuser2” to https://portal.auzure.com
    - Sign-in is interrupted with a “risky singin detected”. Complete the MFA verification process and complete the login to portal.azure.com

    Expected result:

    - You ***should*** get one sign-in risk entry in Azure AD identity protection console for “testuser1”.
    - You ***should not*** get any sign-in risk entry in the Azure AD identity protection console for “testuser2”.

2. Block risky sign-in with Conditional Access
    - Start the TOR browser, and connect to the TOR network
    - Login with your test account “testuser3” to https://portal.azure.com
    - Sign-in is interrupted with a “risky signin detected”. Cancel the sign-in
        - (if no Suspiciouse activity detected warning sign shows up, interrupt the sign-in, restart the TOR-browser and try sign-in again)
    - Start a regular browser and login to portal.office.com with “testuser3”
    - Try accessing the outlook app in portal.office.com

Expected result:

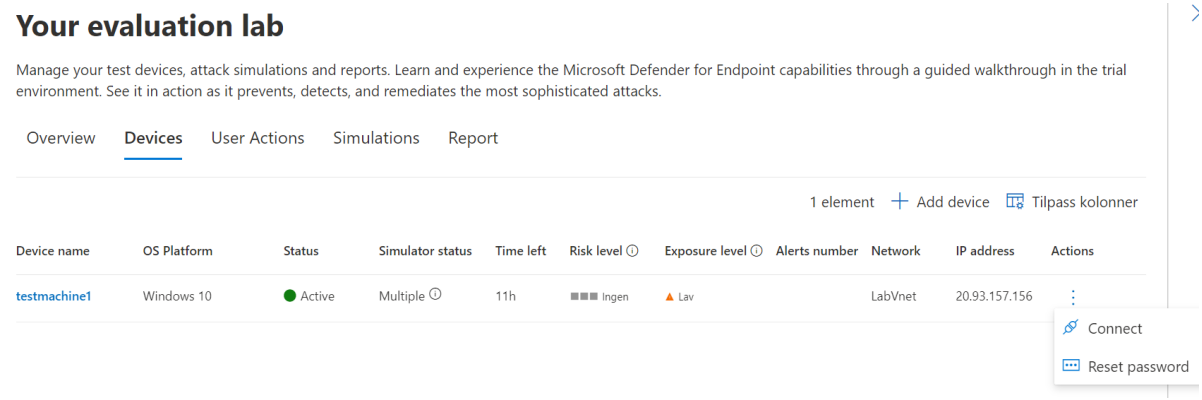
- User is blocked by Conditional access to access the outlook app

DEFENDER FOR ENDPOINT

SETUP AND CONFIGURATION

Pre-requisite for testing Defender for Endpoint is that you activated the Evaluation Lab or that you have a Newly installed Virtual machine or physical machine (Local, ESXI, Hyper-V etc.).

If using an Evaluation LAB machine, open Remote Desktop and Log in to the device with the Provided Username and Password. To be able to Add the machine to Azure AD and Endpoint Manager we need to disable NLA – NB! **Only needed for VM in Azure or Evaluation LAB.**



DISABLE NETWORK LEVEL AUTENTICATION (NLA) – NOT RECOMMENDED IN PRODUCTION

Run this powershell script in and administrator elevated powershell prompt:

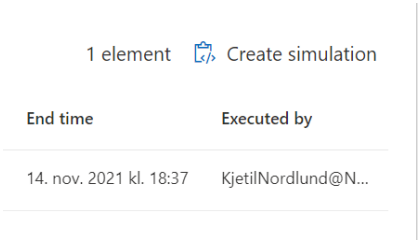
```
Write-Output 'Configuring registry to disable Network Level Authentication (NLA).'
$path = 'HKLM:\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp'
Set-ItemProperty -Path $path -Name SecurityLayer -Type DWord -Value 0
Set-ItemProperty -Path $path -Name UserAuthentication -Type DWord -Value 0
Set-ItemProperty -Path $path -Name fAllowSecProtocolNegotiation -Type DWord -Value 0
Write-Output 'Restart the VM for the change to take effect.'
```

Reboot the machine

RUN A EVALUATION LAB TEST SCENARIO

In the evaluation lab page select the “Simulations” pane

Click “Create simulation”



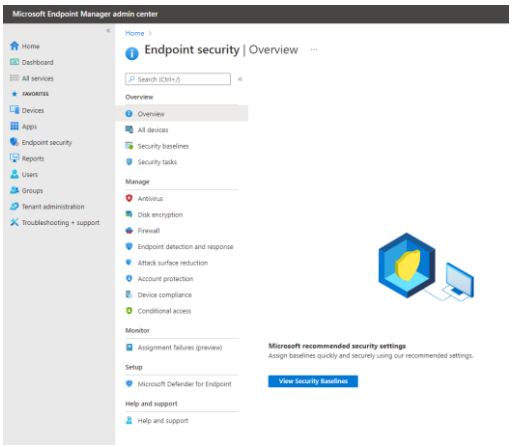
Choose:

AttackIQ and Persistence methods as the simulation, and run it on your lab machine

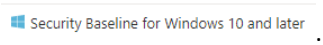
Click “Create simulation”

INTUNE INTEGRATION AND CONFIGURATION POLICIES

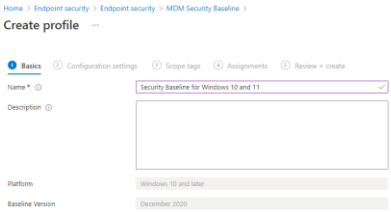
Open the Endpoint manager console with the URL – https://endpoint.microsoft.com



SECURITY BASELINES

1. Navigate to Endpoint Security, click on Security Baselines - > Click 

.
2. Click on Create profile.
3. Provide a Name and Click Next

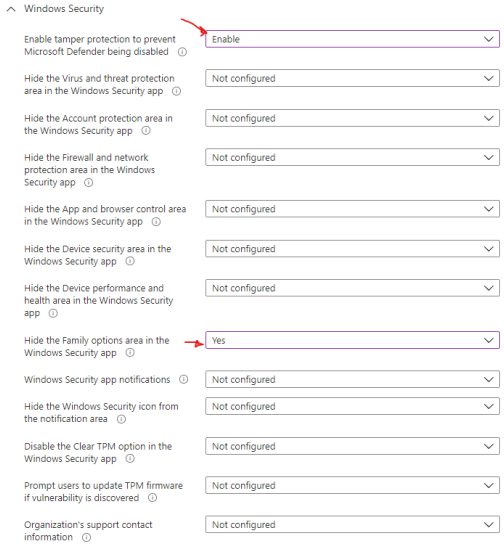


4. Click Next on configuration settings
5. Click Next on Scope tags
6. Click Next on Assignments
7. Click Create.

SECURITY POLICIES

1. Navigate to Endpoint Security, click on Antivirus
2. Click Create Policy
3. In the Dropdown box select Windows 10 and later
4. Windows Security Experience and Click Create
5. Provide a Name and Click Next

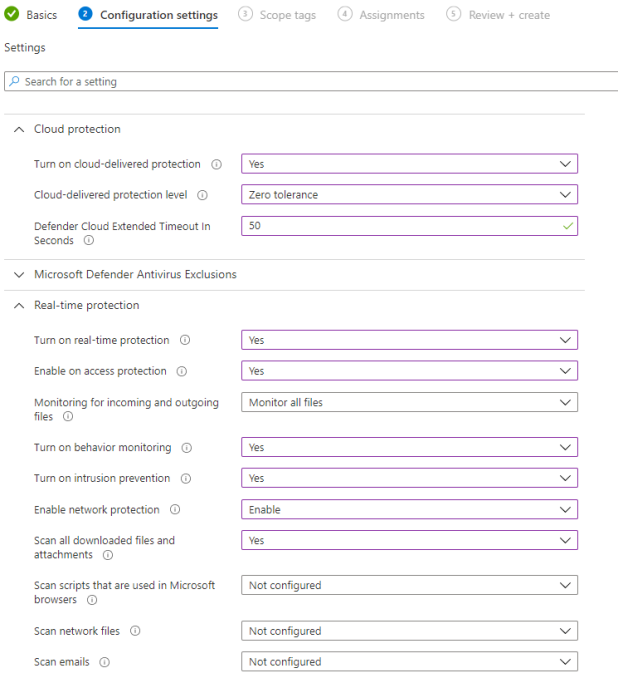
6. Make Sure the following is enabled (Tamper Protection and Hide Family Options)

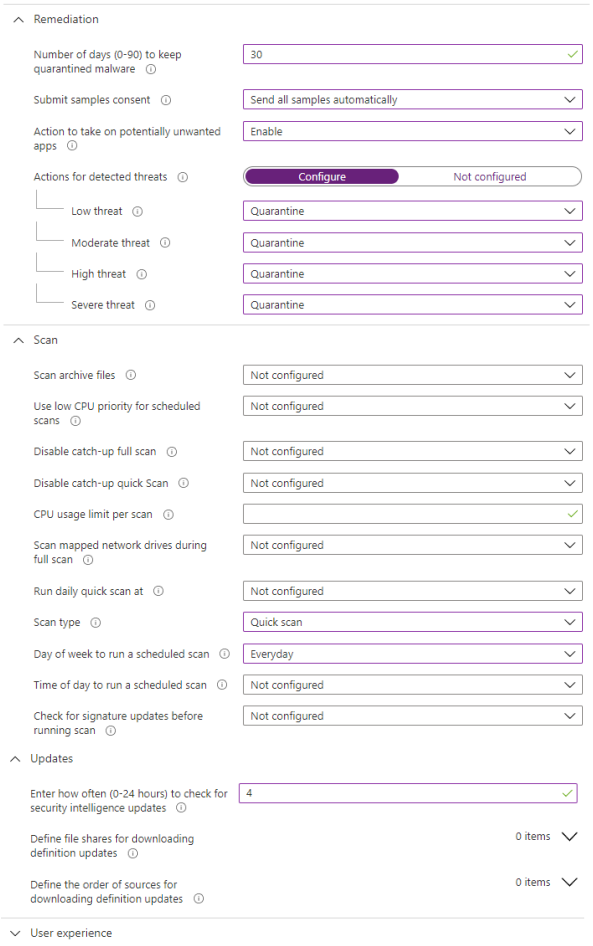


7. Click Next on Configuration settings
8. Click Next on Scope tags
9. Click Next on Assignments
10. Click Create

Back in the Console

1. Click Create Policy
2. In the Dropdown box select Windows 10 and later
3. Microsoft Defender Antivirus and Click Create
4. Provide a Name and Click Next
5. Make sure the following is enabled.





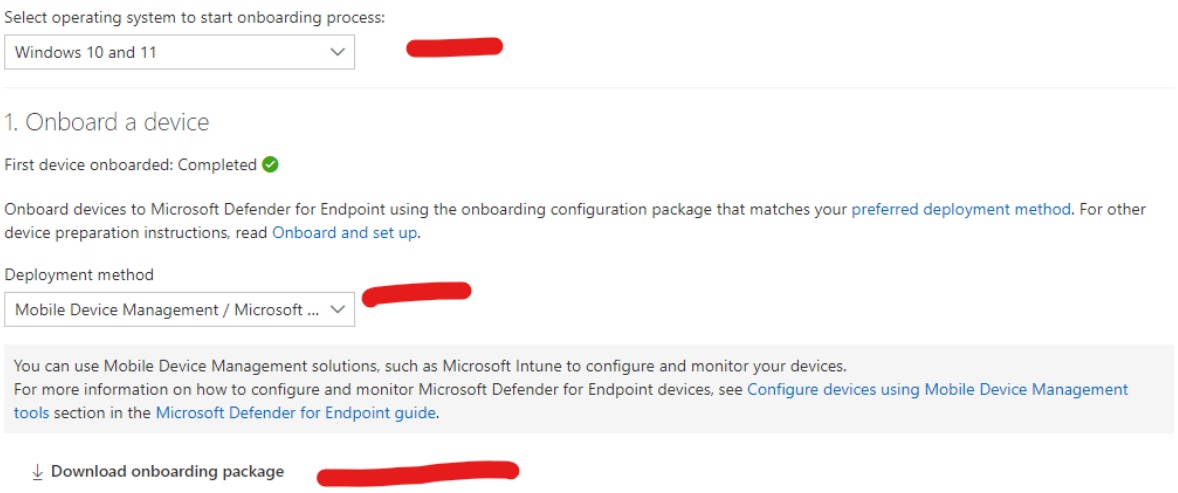
6. Click Next on Configuration settings
7. Click Next on Scope tags
8. Click Next on Assignments
9. Click Create

ENDPOINT DETECTION AND RESPONSE

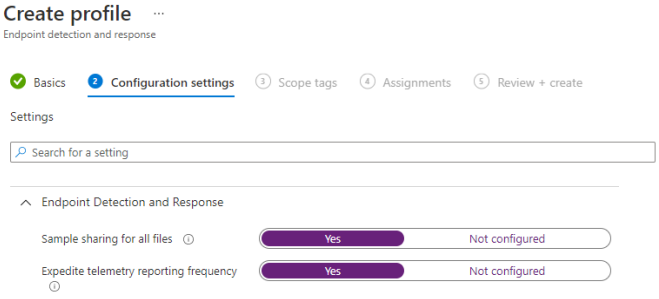
Before starting on this policy we may need to download a config file from Defender For Endpoint.

In Security.microsoft.com – Click on Settings -> Endpoints -> Onboarding.

Select the following to download the config file. Extract the Zip file.



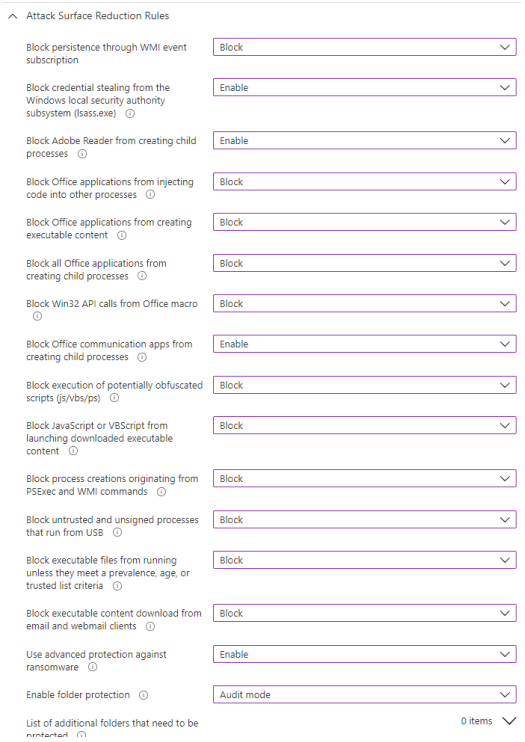
1. Navigate to Endpoint Security, click on Endpoint Detection and Response
2. Click Create Policy
3. In the Dropdown box select Windows 10 and later
4. Select Endpoint Detection and Response Click Create
5. Provide a Name and Click Next
6. Select the following and click Next



7.
8. Click Next on Configuration settings
9. Click Next on Scope tags
10. Click Next on Assignments
11. Click Create

ATTACK SURFACE REDUCTION

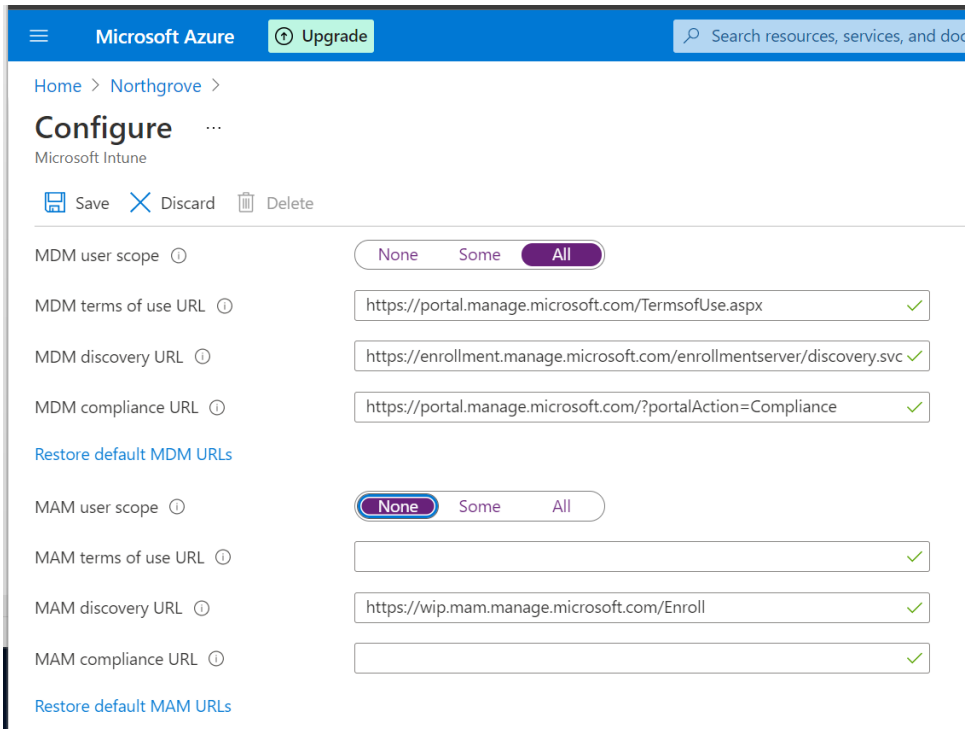
1. Navigate to Endpoint Security, click on Attack Surface Reduction
2. Click Create Policy
3. In the Dropdown box select Windows 10 and later
4. Select Attack Surface Reduction Click Create
5. Provide a Name and Click Next
6. Select the following and click Next



7. Click Next on Configuration settings
8. Click Next on Scope tags
9. Click Next on Assignments
10. Click Create

ENROLL YOUR TESTMACHINE TO INTUNE

Configure autoenrollment in Azure AD: Azure Active Directory > Mobility (MDM and MAM) > Microsoft Intune

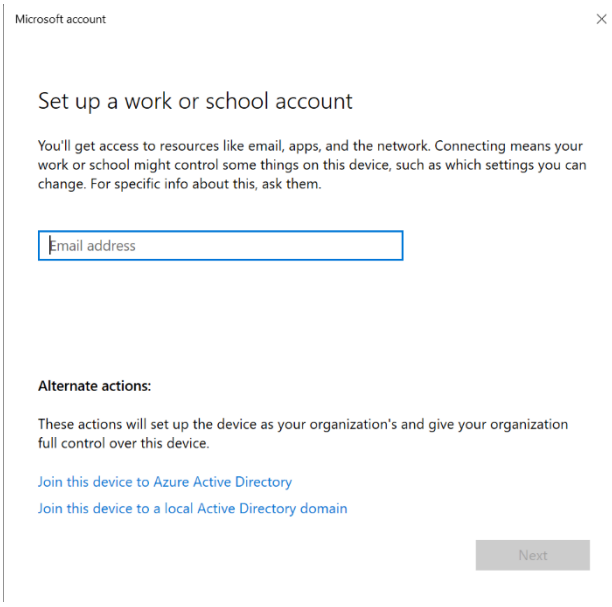


Set ”MDM user scope” to all. Click Save

Login to your testmachine with “Administrator1” and the provided password.

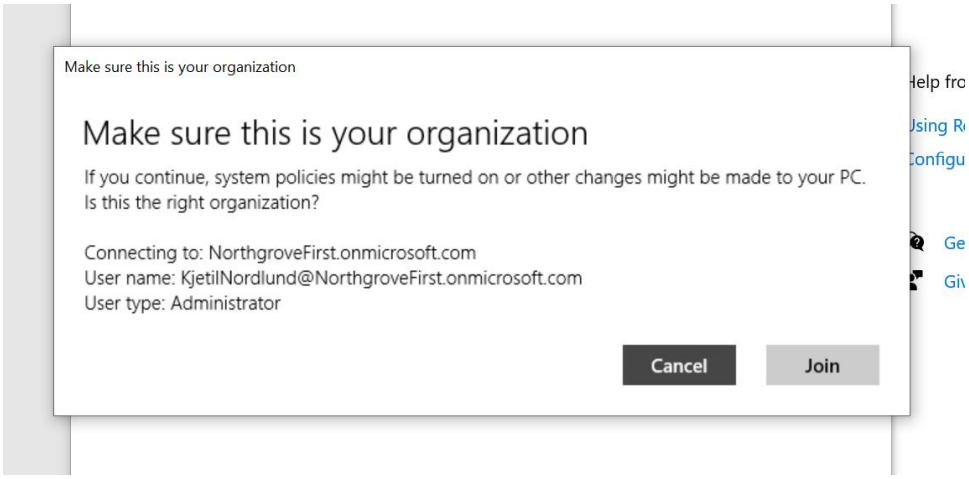
Go to: Start -> Settings -> Accounts -> Access Work or School

Click “Connect”



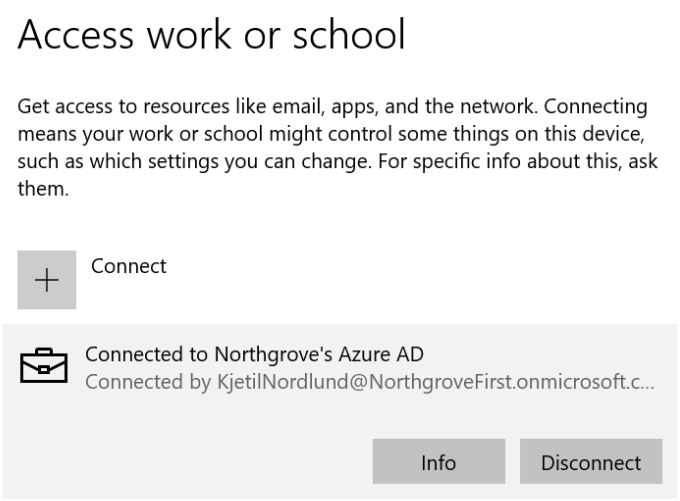
make sure to click on ”join this device to Azure Active Directory”

Enter the email address to your first Azure AD account, and login



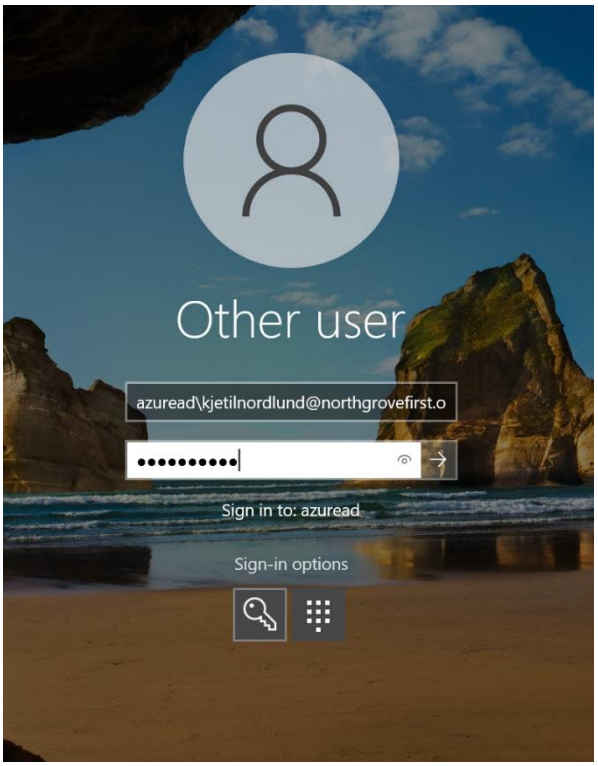
Click join

Click done



Verify that your computer is connected to your environment (both Azure AD and Intune)

Restart your computer



Login to the computer with your first Azure AD account
To be able to login you must type **azuread** in front of your email address

Wait for intune configuration profiles to be delivered

TEST SCENARIO

[Enable attack surface reduction rules | Microsoft Docs]

[https://demo.wd.microsoft.com/] - contains several test scenarios for Defender and ASR

https://aka.ms/ioavtest

Procdump. - [Sysinternals Utilities - Windows Sysinternals | Microsoft Docs]
(cmd.exe and run - procdump lsass.exe)

Mimikatz or similar tools.

Review the report for detections and what's blocked in security.microsoft.com console for ASR rules.

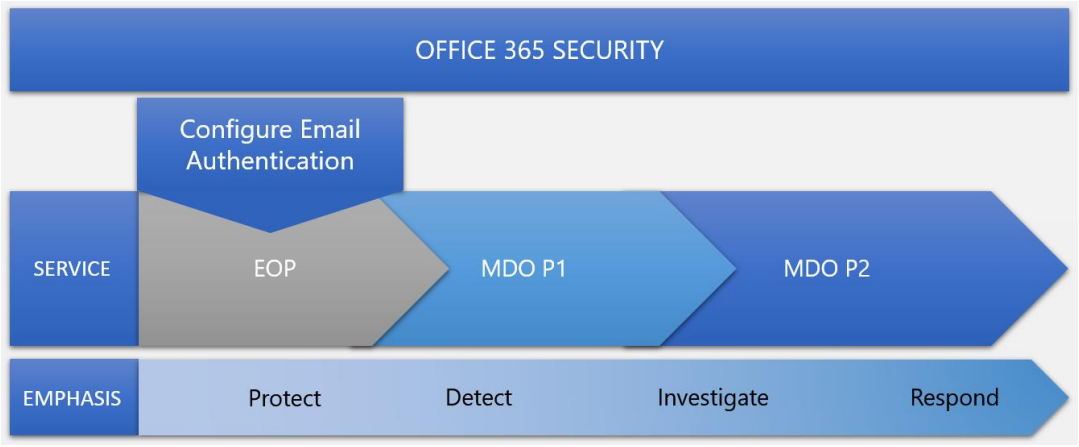
DEFENDER FOR OFFICE 365

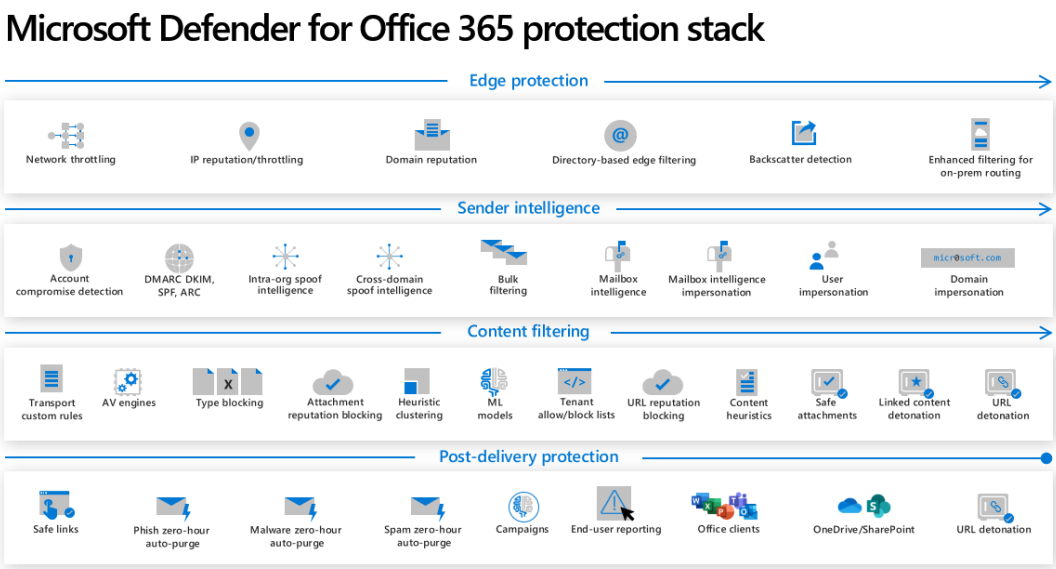
WHAT IS DEFENDER FOR OFFICE 365 SECURITY

Every Office 365 subscription comes with security capabilities. The goals and actions that you can take depend on the focus of these different subscriptions. In Office 365 security, there are three main security services (or products) tied to your subscription type:

1. Exchange Online Protection (EOP)
2. Microsoft Defender for Office 365 Plan 1 (Defender for Office P1)
3. Microsoft Defender for Office 365 Plan 2 (Defender for Office P2)

[Microsoft Defender for Office 365]





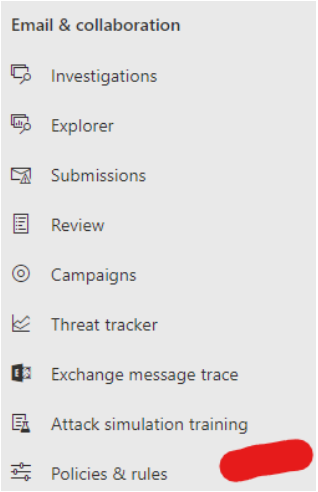
SETUP AND CONFIGURATION

Review architecture requirements

Security policies can be configured as,

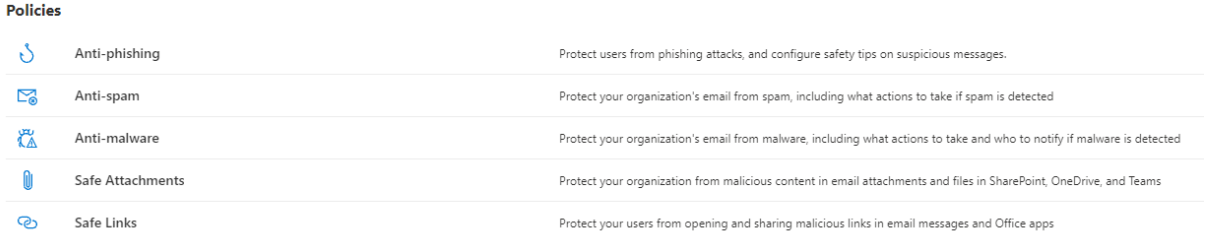
1. Assign preset security policies automatically Preset Security Policy **standard** or **strict.**
   If no need to customize the setup, this will keep the customer at recommended settings, however most customers need some kind of customization.
2. Configure baseline protection manually Custom
   - Anti-malware protection in EOP
   - Anti-phishing protection in EOP and Defender for Office 365
   - Anti-spam protection in EOP
   - Protection from malicious URLs and files
     - Safe Links
     - Safe Attachments

In Security.microsoft.com console navigate to Policies & Rules in the Email and Collaboration.



Click on **Threat policies**

We are going to focus on **Anti-phishing** policies **Safe Attachments**, **Safe Links**.

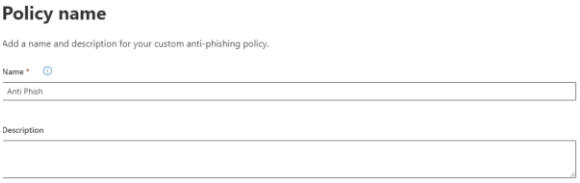


ANTI-PHISHING

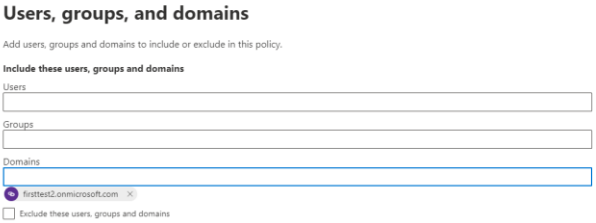
Refer to the recommended settings to determine Default, Standard og Strict settings
anti-phishing policies Default, Standard, Strict

1. Click on Anti-phishing and + Create create a new Policy

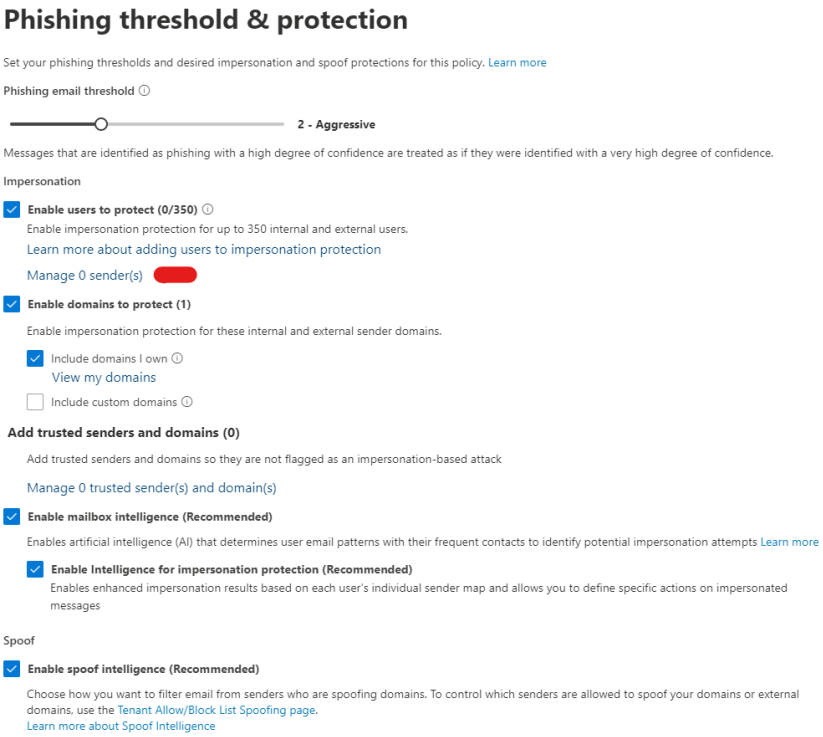
2. Give the policy a Name



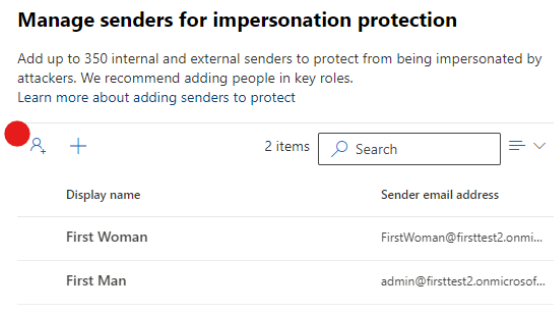
3. Add your tenant domain(s)



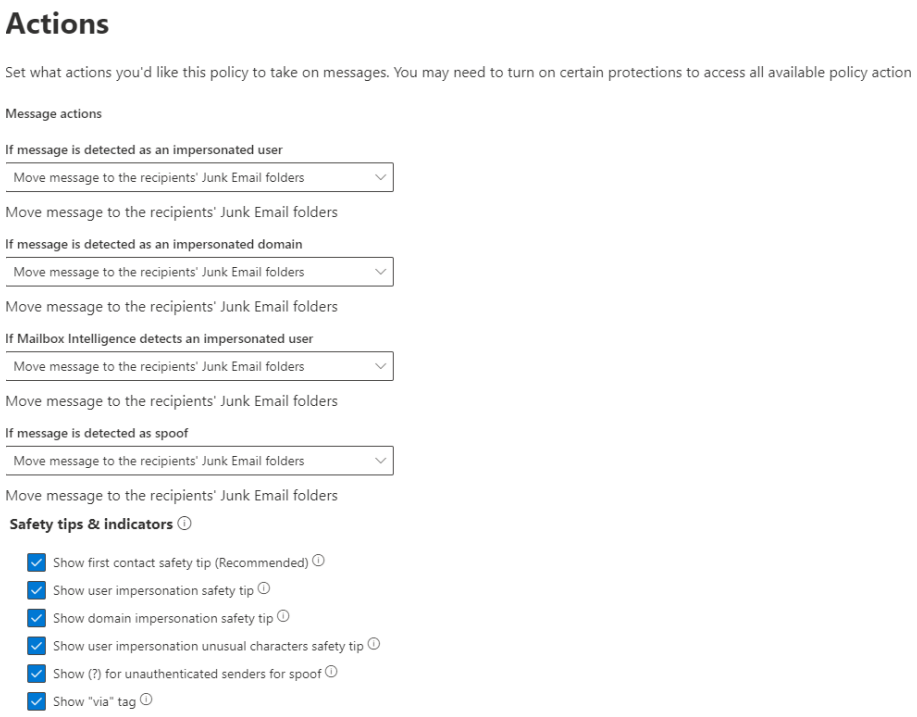
4. Move the Phishing email threshold slider to 2-Aggressive



5.
6. Click on manage 0 sende(s)



7.



8.

TEST SCENARIO

Create a new or use and existing Email account for Impersonation test.

Email address need impersonate a user in your tenant.
Example: - User1@kents-events.com - User1@firsttest2.onmicrosoft.com will trigger the impersonation protection settings in Anti phishing policy

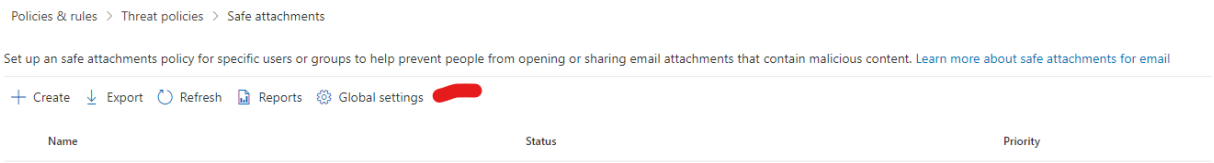
SAFE ATTACHMENTS

Safe attachments is extra layer of protection known as Sandbox detonation.
For reference to Default, Standard or strict setting open the Safe Attachments doc.

In Threat policies, click on Safe Attachments.

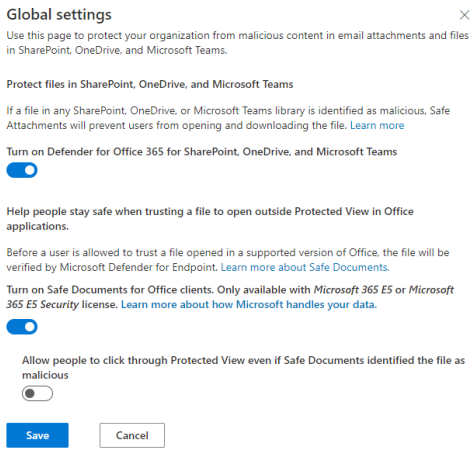
GLOBAL SETTINGS – SAFE ATTACHMENTS

Open Global Settings. (Global means tenant wide settings)



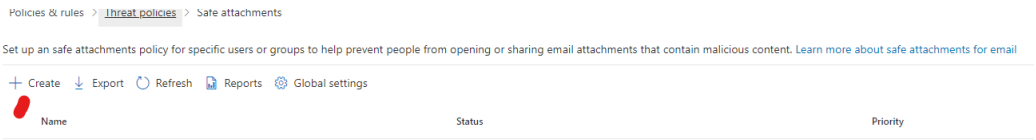
Activate Global Settings for:

- Defender for O365, SharePoint, OneDrive, and Microsoft Teams
- Safe Documents for Office Client.

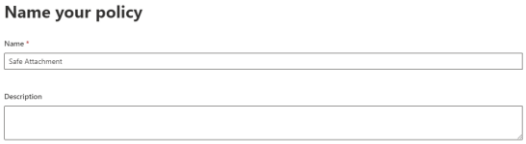


POLICY SETTINGS - SAFE ATTACHMENTS

1. Create a new Policy



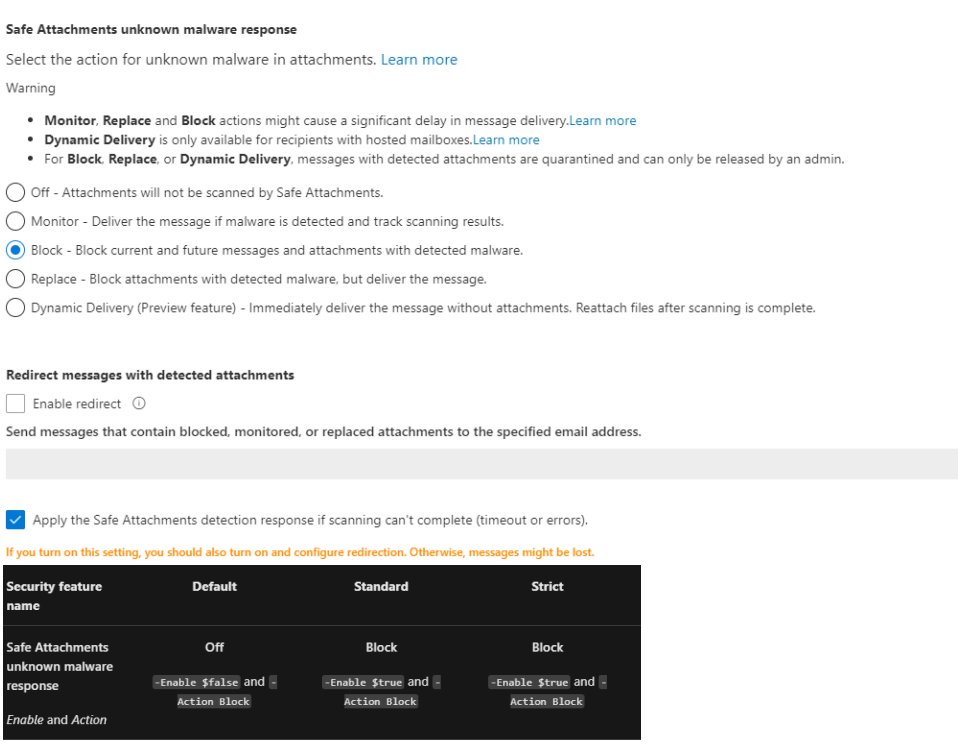
2. Give the Policy a Name and a Description



3. Add your domain(s) to the policy

Add exclusions if you need to Bypass the Sandbox for any reason.

4. Configure the behavior of the Sandbox.



Security feature name	Default	Standard	Strict
Safe Attachments unknown malware response *Enable* and *Action*	Off `-Enable $false` and `-Action Block`	Block `-Enable $true` and `-Action Block`	Block `-Enable $true` and `-Action Block`

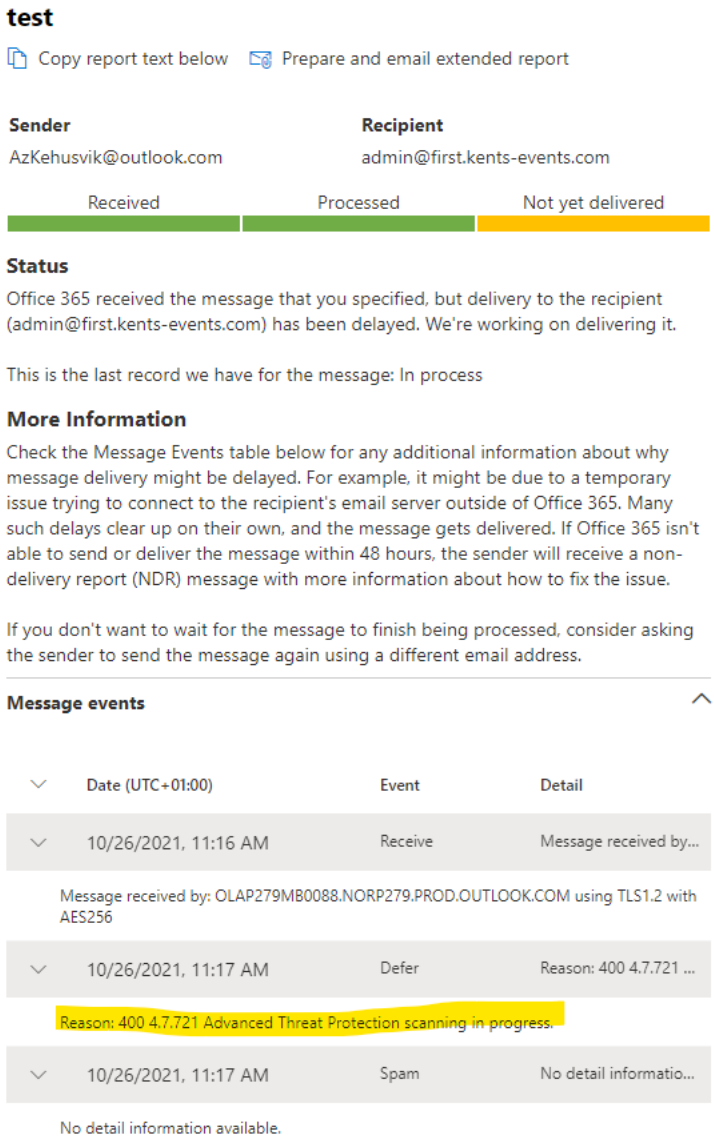
TEST SCENARIO

For Sandbox to be triggered we need to send an email to a protected user with an attachment that is not yet scanned by any Defender service.
From a Machine with a Excluded folder or a machine with EPP that is not Defender.

1. Download a test file with the number you are assigned from M365DefenderTraining/Sonar at Sonar · northgrove/M365DefenderTraining (github.com) (eks : first17.doc if you are assigned nr 17)

2. Send the testfile as Attachment to an email address on your tenant.

3. From Exchange Message Trace, search for the email and look for the following :
Reason: 400 4.7.721 Advanced Threat Protection scanning in progress.

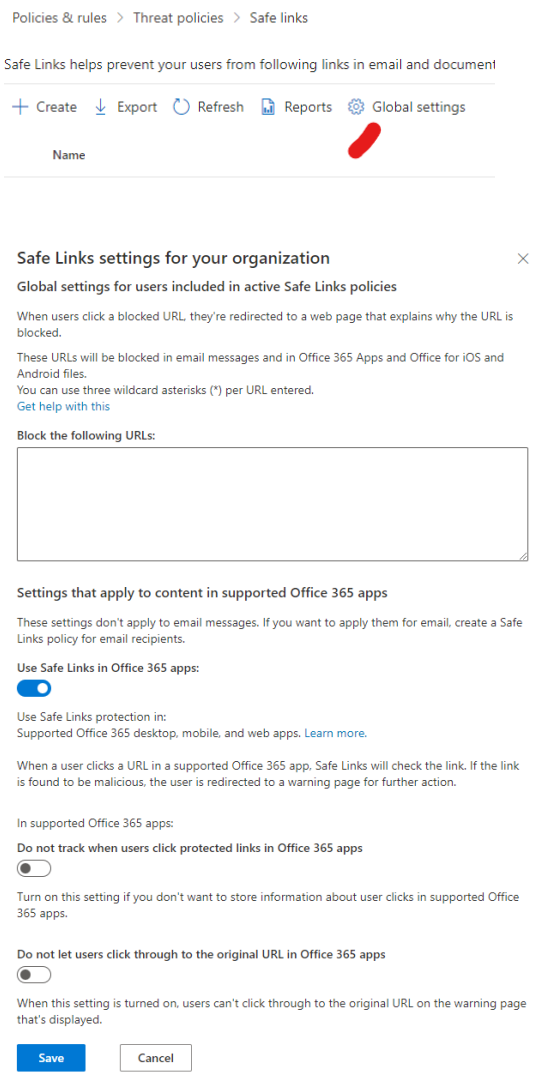


SAFE LINKS

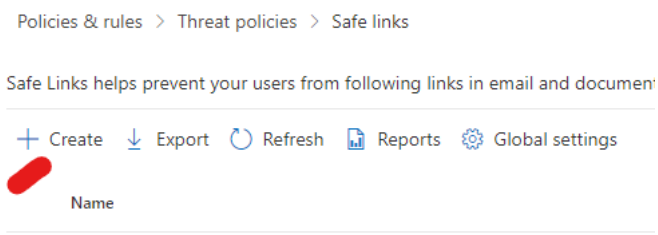
Safe Links helps prevent your users from following links in email and documents that go to web sites recognized as malicious.
Time of click Protections

GLOBAL SETTINGS – SAFE LINKS

Open Global Settings and Make Sure – Use Safe Links in Office 365 is Enabled. This will make Sure Safe Link work in Office Applications like Work, Excel, Power Point etc..

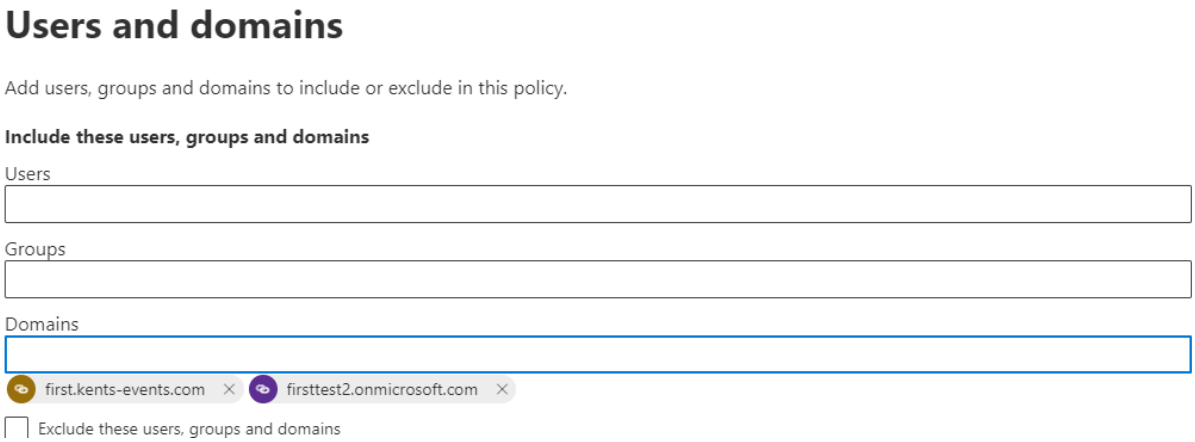


POLICY SETTINGS – SAFE LINKS

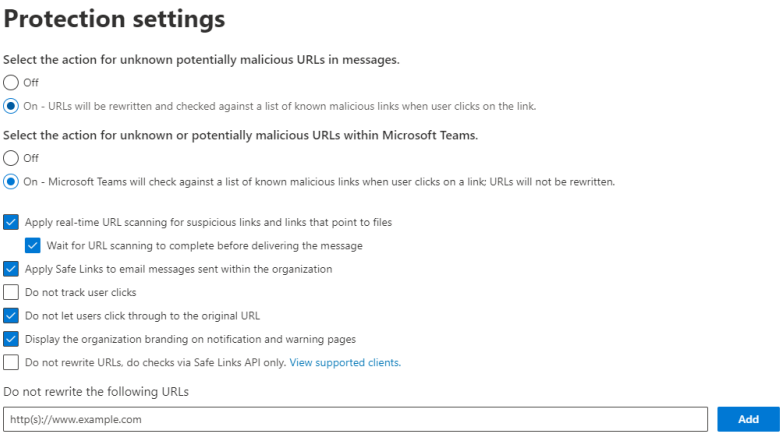


1. Create a new Safe Links Policy
2. Give the Policy a Name and a Description

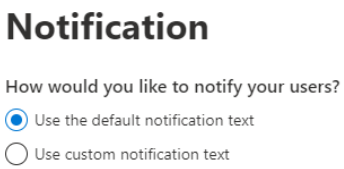
3. Add your domain(s) to the policy



4. Activate following settings

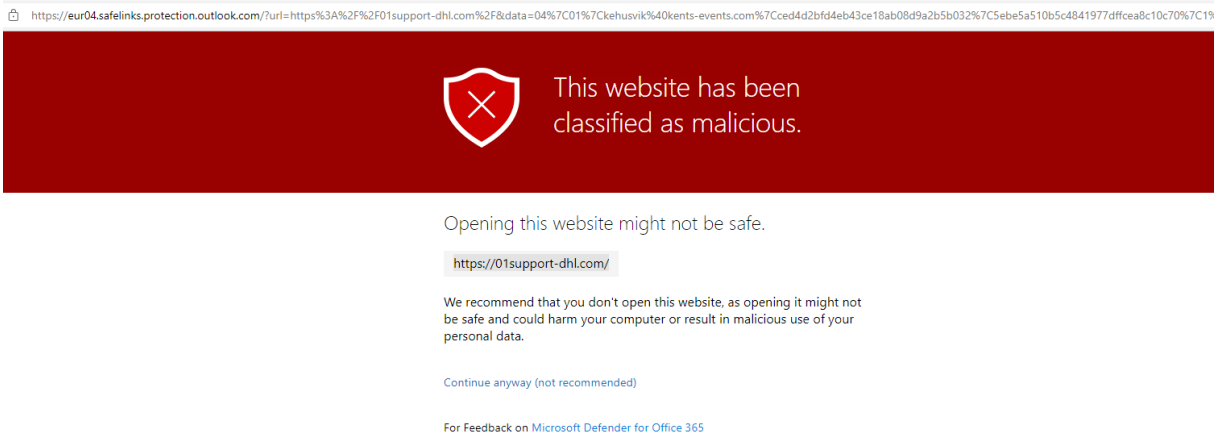


5. Use the default notification and Submit the policy.



TEST SCENARIO

Send an Email with the following link included https://smartscreentestratings2(.)net/ - Remove the () from the URL.
You can also test with a link to a



MICROSOFT CLOUD APP SECURITY

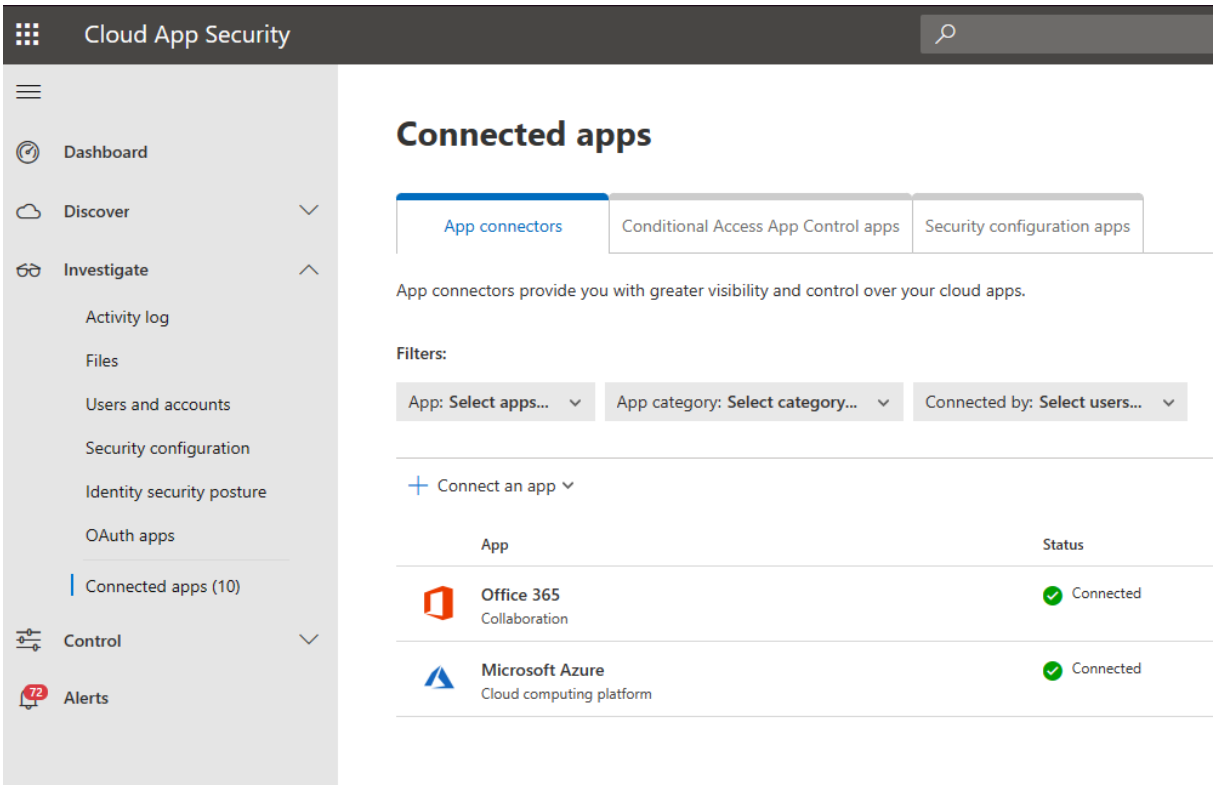
SETUP AND CONFIGURATION

CONNECT APPS TO MCAS

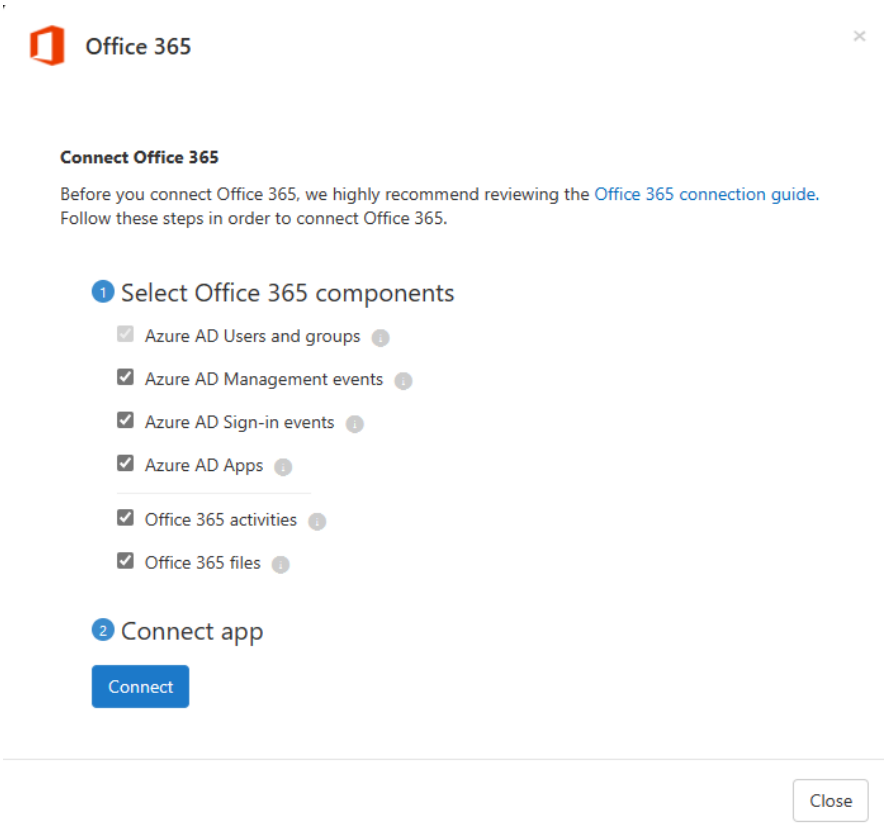
To get insight into Office 365 activities and files the app must be connected in MCAS.

Cloud App Security Portal -> Investigate -> Connected apps

Deep link: https://portal.cloudappsecurity.com/#/connected-apps



Click “Connect an app” and Choose “Office 365”



Choose all components and click connect. Authenticate with your admin user.

INITIAL CONFIGURATION OF MCAS

Initial configuration is done in the “settings” page of MCAS.

Click  in the top right corner -> choose “Settings”

Deep link: https://portal.cloudappsecurity.com/#/settings

Scroll down to “Microsoft Defender for Endpoint” in the Settings menu

- Enable “Enforce app access”
- Alerts: Informational

Scroll down to “User enrichment”

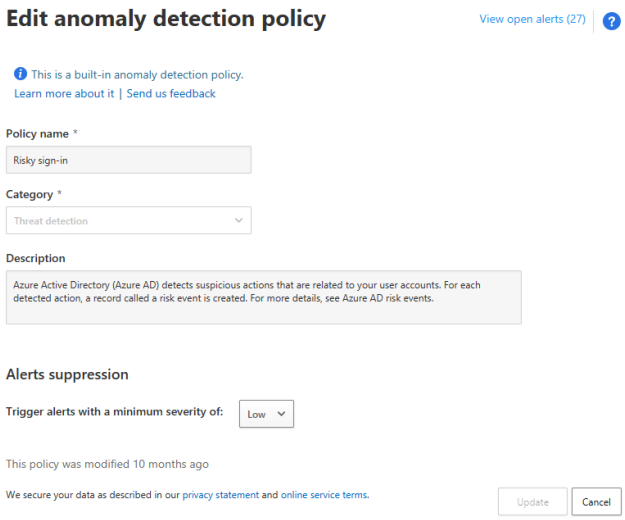
- Enable “enrich discovered user identifiers with Azure Active Directory usernames”

Scroll down to “Microsoft Defender for Identity”

- Normally “Microsoft defender for identity data integration” should be enabled, but this will require an on-premises Domain Controller with Defender for identity connector installed. This will therefore be skipped in this lab.

Scroll down to “Azure AD Identity Protection”

- Enable “Azure AD Identity protection alert integration”
- Click in “edit Policies” after “Only alerts with high severity are triggered by default. Change the severity level of all policies to “low”



Scroll down to “App Governance”

- Enable “App Governance integration”

Scroll down to “Microsoft information protection”

- Enable “automatically scan new files for Microsoft Information Protection sensitivity labels and content inspection warnings”
- **Don’t** enable “only scan files for Microsoft Information Protection sensitivity labels and content inspection from this tenant”
- Grant permission to inspect protected files

Scroll down to “Files”

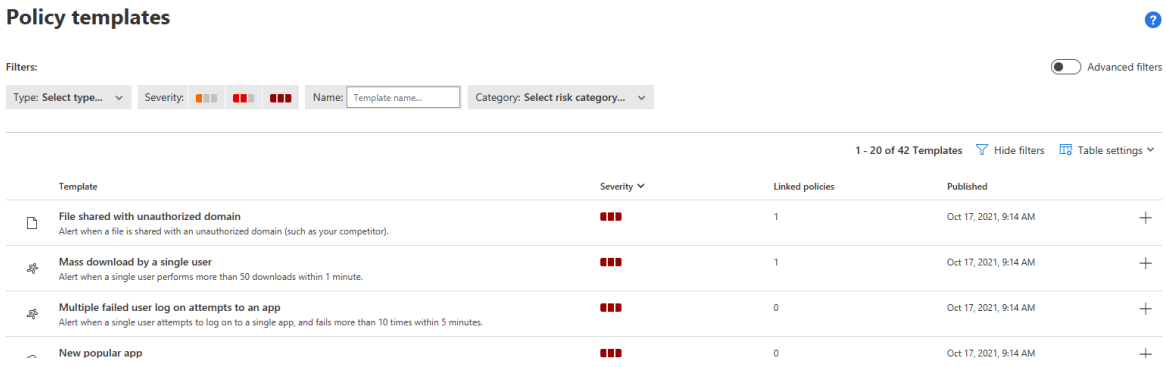
- Enable “File monitoring”
- Go to connected apps and update the Office 365 connector with Office 365 Files

CREATE A POLICY FROM EXISTING TEMPLATE

Cloud App Security Portal -> Control -> Templates

Deep link: https://portal.cloudappsecurity.com/#/policy/templates

Scroll down to or search for “mass download by a single user”



Click on the + sign in the colum to right for that policy template

Configure the policy to reflect sensible settings. In this scenario we do set a configuration that's makes it easy to trigger an alert:

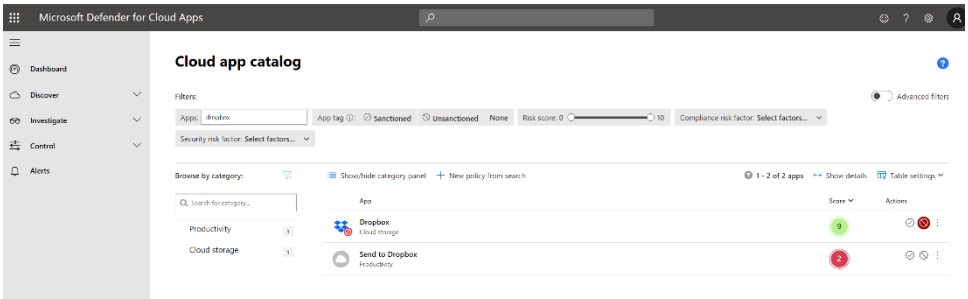
- Repeated activity:
  - Minimum repeated activities: 5
  - Whitin timeframe: 5 minutes
- Turn of the "count only unique target files or folders pr user"
- Create the Policy

UNSANCTION AND BLOCK ACCESS TO FACEBOOK

Search for Facebook in the Cloud app catalog

Cloud App Security Portal -> Discover -> Cloud App Catalog -> search for "dropbox"

Deep link:
https://portal.cloudappsecurity.com/#/catalog?text=contains(o:(searchType:i:1,adv:b:false),dropbox)



In the Actions column, click on the ⃠ icon for the Facebook app.

Confirm that you want to block the app.

With this MCAS will put the URL identifier for Facebook as a Custom Indicator in Defender for Endpoint. Defender for Endpoint with network protection will then block any access to that URL from the device.

TEST SCENARIO

1. MASS DOWNLOAD OF FILES FROM OFFICE 365

Log inn to https://portal.office.com with your testuser3

- Start Teams
- Create a new Team
- Access the files tab
- Create 6 new Office 365 files with random content (=rand())
- Download each of the 6 files to your computer, one by one, within 5minutes.

Expected result:

An alert about “Mass download by single user” are created in MCAS

2. BLOCKED ACCESS TO FACEBOOK FROM DEVICE

Log inn to your test computer, enabled with Microsoft Defender for Endpoint

- Try access www.facebook.com from a browser session

Expected result:

- Smart screen will block access to www.facebook.com showing a red alert page
- An alert is triggered in Defender for Endpoint

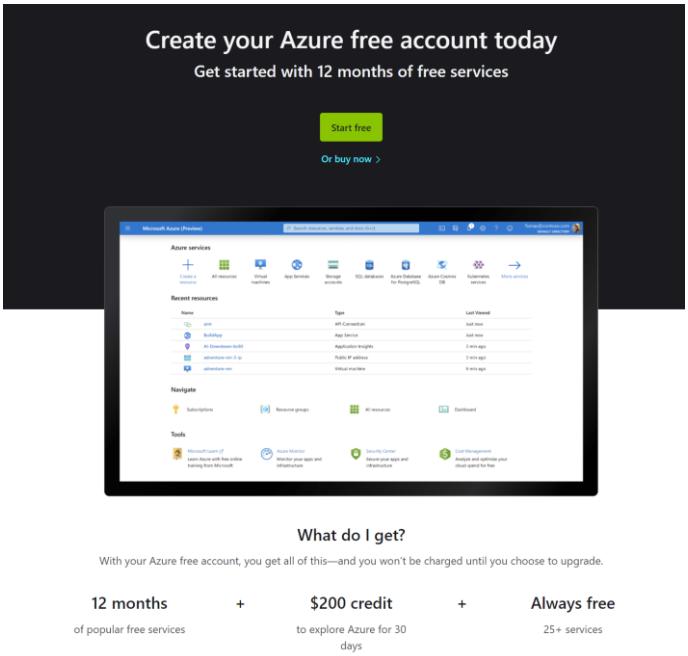
EXTRA: AZURE SENTINEL

SPECIAL REQUIREMENTS

For this extra task you will need an Azure Subscription – You will need a valid credit card to complete this sign-up.

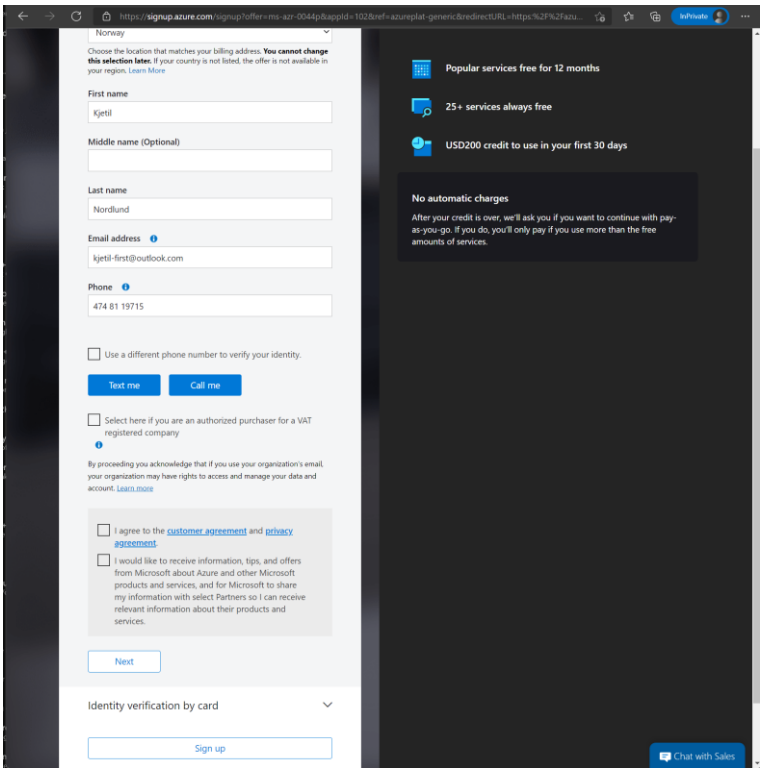
The credit card will not be used, unless you choose to purchase some Azure services your selv

Create free Azure Subscription ($200 credit for 30days):



https://signup.azure.com/signup?offer=ms-azr-0044p&appId=102&ref=azureplat-generic&redirectURL=https%3A%2F%2Fazure.microsoft.com%2Fen-us%2Fget-started%2Fwelcome-to-azure%2F&l=en-us&correlationId=4fb68cb5b20240c884a3e2ac0f885a90

Make sure you are logged in with the same account you created the Microsoft 365 E5 trial with

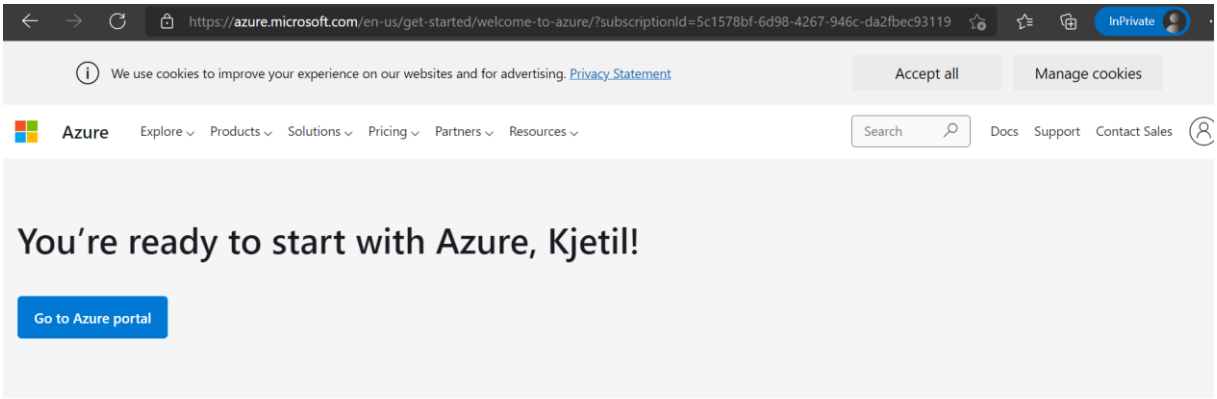


Verify your phone number by clicking “text me”

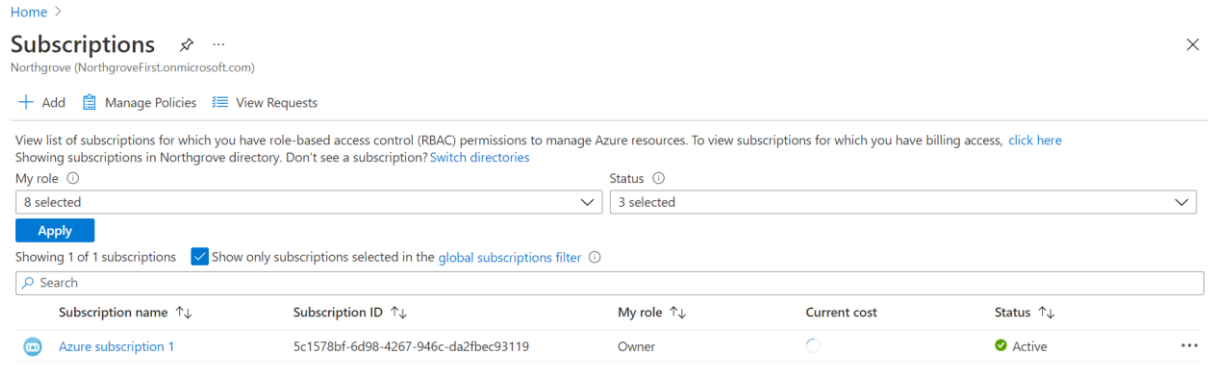
Agree to the licensing terms and click next

You will need to register a valid Credit Card.

Click “sign-up”



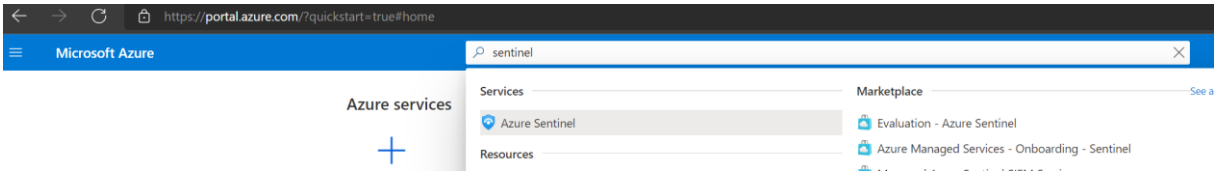
Under Subscriptions in the Azure portal you should now se a Azure Subscription:

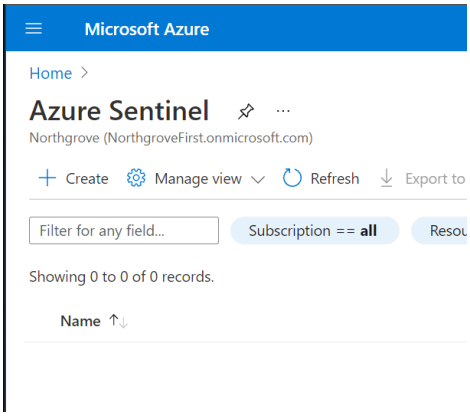


SETUP OF MICROSOFT SENTINEL

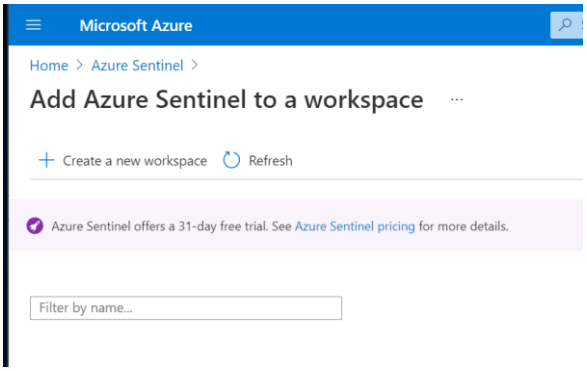
Create a Microsoft Sentinel workspace:

In the search bar in portal.azure.com, search for “Sentinel” and click “azure sentinel”:

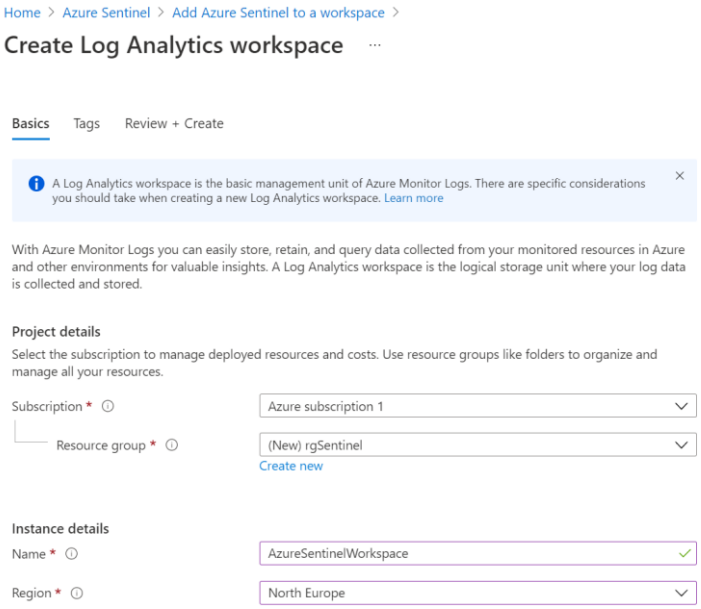




Click “create” or “create azure sentinel”

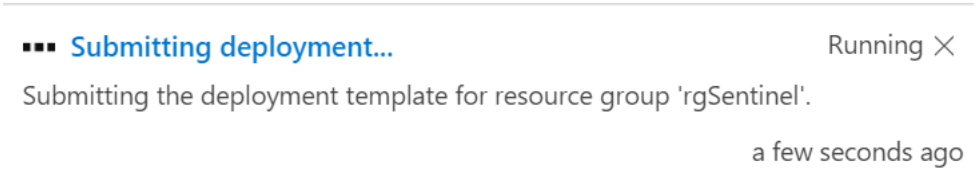


Create a new workspace

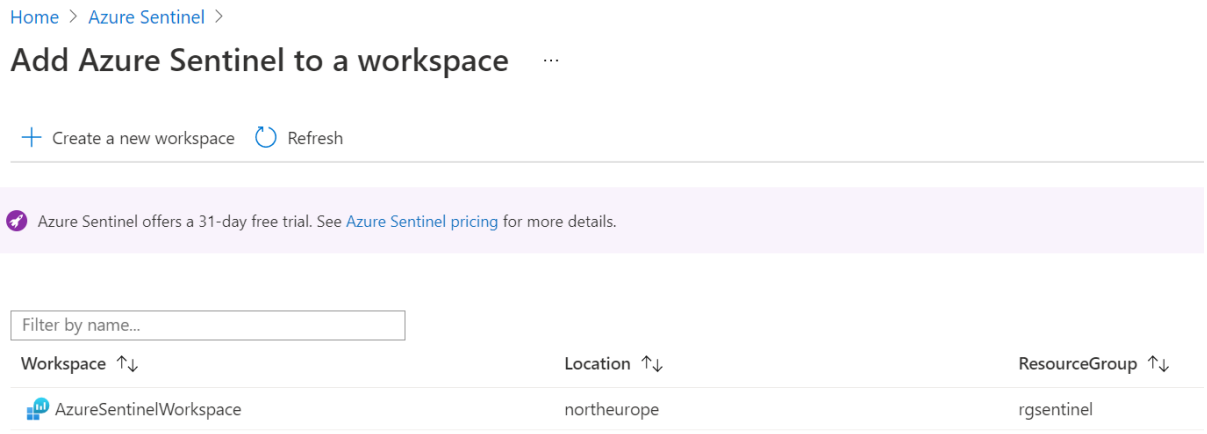


Create new resource group, choose a region and name your log analytics workspace

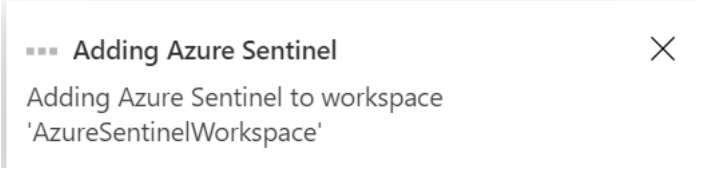
Click Create



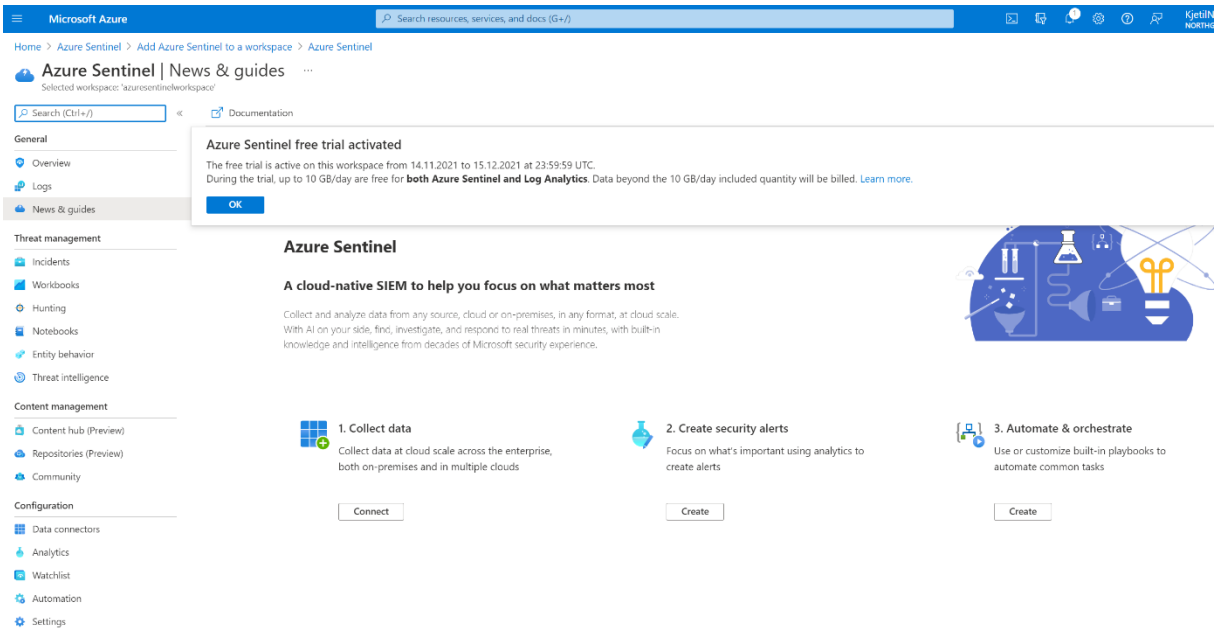
Wait for deployment to be ready – and your Log Analytics workspace will show up in the workspace list



Choose the workspace and click “add”



Wait for Microsoft Sentinel to be provisioned



Microsoft Sentinel is ready to use

CONFIGURATION OF MICROSOFT SENTINEL

TEST SCENARIO

LAB SIMULATION QUESTION

ATTACKIQ - PERSISTENCE METHODS

1. What is the IP from where the RDP brute-force happened?
2. Describe the changes made to file association on the computer?
3. What script language executable was used to run the commands?
    a. What was the name of the script file?
4. What is the Registry key, Value name, value data and value tape for the registry changed for logon script registration?
    a. What was the previous values?
5. Which URL does ai_exec_server.exe connect to?
6. What is the InitiatingProcessCommandLine for the process creating the attackiq_appcert_dll.dll file?
7. What is the remote IP and URL that pyhton.exe establishes an outbound connection to?

SAFEBRACH AND KNOWN RANSOMWRE INFECTION:

1. What is the original name of the initial file first run with malware to the computer?
    a. What kind of malware was detected?
2. What is the IP and TCP port to the host the SafeBreach simulator is connecting to?
3. What is the name of the activity group associated to this attack?
4. What is the filename for the WannaCrypt ransomware detected?
    a. What is the Virus Total ratio for this file?