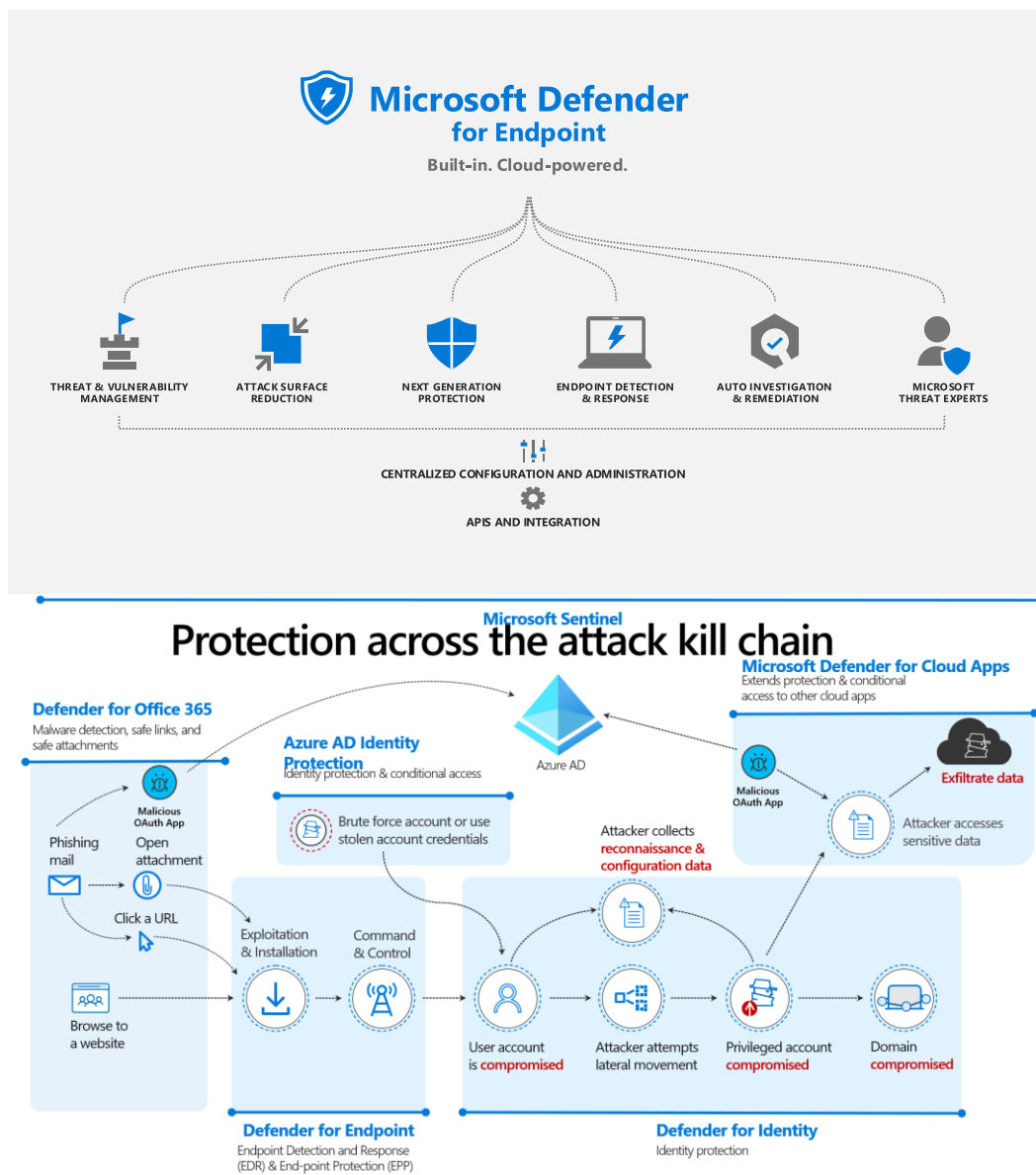


Attendees will get an opportunity to try their hands at configuration, detection and security analysis using MS tools such as the Defender XDR products and Azure Sentinel.

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

First - M365 Defender XDR.....	1
PRE workshop - Preparations.....	4
Data storage location	6
Settings And Preview features	7
Security Console Welcome wizard	7
Turn on Preview features and other features:.....	7
Enroll Evaluation LAB	9
Turn on auditing.....	11
Test users and groups	12
Turn off “Security Defaults”	12
Enable basic conditional access policies	12
Azure Active Directory identity Protection	13
Setup and configuration.....	13
Risk Based Conditional Access	18
Test scenario – Identity Protection	18
Defender for Endpoint	20
Setup and configuration.....	20
Disable Network Level Autentication (NLA) – NOT recommended in Production.....	20
Run a evaluation lab test scenario	20
Intune integration and configuration policies.....	21
Security Baselines.....	21
Security Policies.....	21
Endpoint Detection and Response.....	23
Attack Surface Reduction	25
Enroll your testmachine to intune	26
Test scenario	29
Defender for Office 365	30
What is Defender for Office 365 security.....	30
Setup and configuration.....	31
Anti-phishing	31
Test scenario	33
Safe Attachments	34
Global Settings – Safe ATTACHMENTS	34
POLICY SETTINGS - Safe ATTACHMENTS	34

TEST SCENARIO	35
SAFE LINKS	37
Global Settings – Safe Links	37
POLICY SETTINGS – SAFE LINKS	38
TEST SCENARIO	39
Microsoft Cloud App Security	40
Setup and configuration	40
Connect apps to MCAS	40
Initial configuration of MCAS	41
Create a Policy from existing template	42
UnSanction and block access to Facebook	43
Test scenario	44
1. Mass download of files from Office 365	44
2. Blocked access to Facebook from Device	44
Extra: Azure Sentinel	45
Special Requirements	45
Setup of Microsoft Sentinel	47
Configuration of Microsoft Sentinel	49
Test Scenario	49
Lab Simulation question	50
AttackIQ - Persistence methods	50
SafeBrach and Known Ransomwre Infection:	50

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

You've selected Microsoft 365 E5 Trial

1 Let's get you started

Enter your work or school email address, we'll check if you need to create a new account for Microsoft 365 E5 Trial.

Email

Next

2 Tell us about yourself

3 How you'll sign in

4 Confirmation details

You've selected Microsoft 365 E5 Trial

1 Let's get you started

2 Tell us about yourself

First name Middle name (Optional) Last name

Business phone number

Company name Company size

Country or Region

Next

3 How you'll sign in

4 Confirmation details

You've selected Microsoft 365 E5 Tria

1 Let's get you started

2 Tell us about yourself

A text or phone call helps us make sure this is you.
Enter a number that isn't VoIP or toll free.

☒ Text me
☐ Call me

Country code Phone number

We don't save this phone number or use it for any other purpose.

Send verification code Back

3 How you'll sign in

4 Confirmation details

You've selected Microsoft 365 E5 Trial

- 1 Let's get you started
- 2 Tell us about yourself
- 3 How you'll sign in



To set up your account, you'll need a domain name. [What is a domain?](#)

You'll probably want a custom domain name for your business at some point. For now, choose a name for your domain using **onmicrosoft.com**.

firsttest2 .onmicrosoft.com

firsttest2.onmicrosoft.com is available.

Check availability

Next

- 4 Confirmation details

You've selected Microsoft 365 E5 Trial

- 1 Let's get you started
- 2 Tell us about yourself
- 3 How you'll sign in



Now create your username and password to sign in to your account.

Username

admin @firsttest2.onmicrosoft.com

Password

.....

Confirm password

.....

By selecting **Sign up**, you agree to our [trial agreement](#).

I understand that Microsoft may contact me about my trial.

☐ I would like information, tips, and offers about Solutions for Businesses and Organizations, and other Microsoft products and services. [Privacy Statement](#)

☐ I would like Microsoft to share my information with select partners so I can receive relevant information about their products and services. [Privacy Statement](#)

Sign up

Back

You've selected Microsoft 365 E5 Trial

- 1 Let's get you started
- 2 Tell us about yourself
- 3 How you'll sign in
- 4 Confirmation details



Thanks for signing up for Microsoft 365 E5 Trial

Your username is **admin@firsttest2.onmicrosoft.com**


We've sent a confirmation email to **fristtest1@outlook.com**

Get Started

Manage your subscription

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.



Step 1

Set up permissions

Step 2


Get started

Step 3

Set up preferences

Step 4

Onboard a device



Microsoft Defender for Endpoint is almost ready

To start experiencing Microsoft Defender for Endpoint, you need to onboard at least one device and run a detection test on that device. Ensure you:

- Onboard a device

First device onboarded: Incomplete

Onboard devices to Microsoft Defender for Endpoint using the onboarding configuration package that matches your preferred deployment method. For other device preparation instructions, read [Onboard and set up](#).

Deployment method

Local Script (for up to 10 devices)

You can configure a single device by running a script locally.

Note: This script has been optimized for usage with a limited number of devices (1-10). To deploy at scale, please see other deployment options above.

For more information on how to configure and monitor Microsoft Defender for Endpoint devices, see [Configure devices using a local script](#) section in the [Microsoft Defender for Endpoint guide](#).

Download onboarding package

- Run a detection test

First device detection test: Incomplete

To verify that the device is properly onboarded and reporting to the service, run the detection script on the newly onboarded device:

- Open a Command Prompt window
- At the prompt, copy and run the command below. The Command Prompt window will close automatically.

```
powershell.exe -NoExit -ExecutionPolicy Bypass -WindowStyle Hidden $ErrorActionPreference= 'silentlycontinue'; (New-Object System.Net.WebClient).DownloadFile('http://127.0.0.1/1.exe', 'C:\test-MDATP-test\invoice.exe'); Start-Process 'C:\test-MDATP-test\invoice.exe'
```

Copy

If successful, the detection test will be marked as completed and a new alert will appear in few minutes.

[Start using Microsoft Defender for Endpoint](#)

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](https://security.microsoft.com) and complete the wizard.



[Minimum requirements for Microsoft Defender for Endpoint | Microsoft Docs](#)

Browser requirements

Access to Defender for Endpoint is done through a browser, supporting the following browsers:

- Microsoft Edge
- Google Chrome

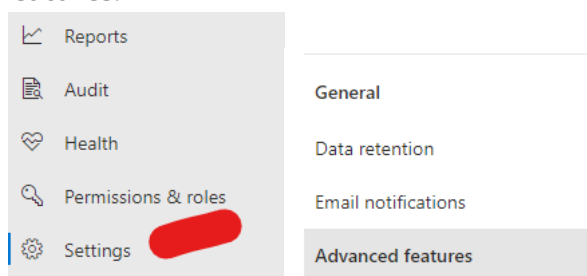
Note

While other browsers might work, the mentioned browsers are the ones supported.

























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"

	Automated Investigation Enables the automation capabilities for investigation and response.
	Live Response Allows users with appropriate RBAC permissions to investigate devices that they are authorized to access, using a remote shell connection.
	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.
	Live Response unsigned script execution Enables using unsigned PowerShell scripts in Live Response.
	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.
	Automatically resolve alerts Resolves an alert if Automated investigation finds no threats or has successfully remediated all malicious artifacts.
	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.
	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.
	Tamper protection Keep tamper protection turned on to prevent unwanted changes to your security solution and its essential features. <div>  MAPS (Cloud-delivered Protection) is required. Learn more. </div>
	Show user details Enables displaying user details: picture, name, title, department, stored in Azure Active Directory.
	Skype for business integration Enables 1-click communication with users.
	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. <div>  Feature has not been fully enabled. Enable integration on the Advanced Threat Analytics portal. </div>
	Office 365 Threat Intelligence connection  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 .
	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.
	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.
	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 .
	Download quarantined files Backup quarantined files in a secure and compliant location so they can be downloaded directly from quarantine.
	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.
	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.
	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.
	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.

[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.

Lab configuration

- Select your lab configuration
- Install simulators agent
- Summary

Select your lab configuration

ⓘ Please note, first set up can not be edited. [Learn more](#)

The following lab configuration options allows you to choose to run fewer devices for a longer period or more devices for a shorter period. When the allotted time is met, devices are automatically deleted.

- ☐ 3 devices For 72 hours each
- ☐ 4 devices For 48 hours each
- ☐ 8 devices For 24 hours each
- ☒ 16 devices For 12 hours each

When you've used up these devices and need more, you can submit a request for more devices. Once you've selected the configuration for the added devices, it cannot be modified. A deleted device can't be restored in any way and does not refresh the available test device count.

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

Lab configuration

Select your lab configuration

Install simulators agent

Summary

Install simulators agent

Threat simulator details

Install threat simulation agents to safely run breach and attack scenarios on the evaluation lab devices. See the power of Microsoft Defender for action as simulated threats unfold. Explore simulation gallery.

Microsoft privacy statement

Accept and provide consent to the statements

☐ Microsoft information sharing statement

Provide consent by accepting the Microsoft terms

☐ Microsoft information sharing statement

Provide consent by accepting the information sharing statement

Select vendors

☐ Note: You must first provide consent to the statements above to enable any of the simulators.

☐ AttackIQ

Note you must first provide consent to the EULA before enabling AttackIQ. View EULA

AttackIQ Platform packages adversarial behavior including MITRE ATT&CK tactics, techniques, and procedures into a fully automated platform to continuously test and measure the efficacy of your security controls.

☐ SafeBreach

SafeBreach safely and continuously simulates real attack scenarios in production to enable security teams to discover, investigate and remediate misconfigurations.

Microsoft terms

Please read and accept

By clicking you accept, you agree to the following terms. Microsoft is making available the above third party solutions to you for testing purposes only. Microsoft is not responsible for, and disclaims all liability related to any errors, output, or actions taken in response to use of such third party solutions. Except as set forth below, Microsoft will process your data from such testing according to the Microsoft Privacy Statement, Online Services Terms, and other terms you've agreed to as part of using Microsoft 365 Defender solutions.

Back **Next** **Accept**

Choose both "AttackIQ" and "SafeBreach" and fill in your trial email and name

- Click on the Setup lab

Back **Setup lab**

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

Your evaluation lab

Manage your test devices, attack simulations and reports. Learn and experience the Microsoft Defender for Endpoint capabilities through a guided walkthrough in the trial environment. See it in action as it prevents, detects, and remediate sophisticated attacks.

Overview **Devices** **User Actions** **Simulations** **Report**

Device allocation

No provisioned devices

Provisioned devices are limited to 16 devices.

Add device

Simulations overview

Add simulations

Create simulation

Go to simulations gallery

Report overview

Provision some devices.

You'll never know until you try. Provision a few devices to start your evaluation.

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

Add device

The lab only provides 16 test devices. Each device is only available for 12 hours. When these resources are deleted, no new devices are provided.

You have used up 1 of 16 devices.

Device type

Windows 10

Device connection details

The password is only displayed once. Save the device connection details in a safe place.

Device name: testmachine1

User name: Administrator1

Password: Hcxdq_%0Yrbc

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

Your evaluation lab

Manage your test devices, attack simulations and reports. Learn and experience the Microsoft Defender for Endpoint capabilities through a guided walkthrough in the trial environment. See it in action as it prevents, detects, and remediates the most sophisticated attacks.

Overview

Devices

User Actions

Simulations

Report

1 item

+ Add device

Device name	OS Platform	Status	Simulator status	Time left	Risk level	Exposure level	Alerts number	Network	IP address
testmachine1	Windows 10	<div>Setting up</div>	<div>Multiple</div>	<div>00:00:00</div>	<div>Low</div>	<div>Low</div>			

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.

Audit

[Search](#) [Audit retention policies](#)

Need to find out if a user deleted a document or if an admin reset someone's password? Search the Office 365 audit log to find out what they have been doing. You'll be able to find activities related to email, groups, documents, permissions, directory services, and much more. [Learn](#)

Start recording user and admin activity

Search

Activities

Show results for all activities

View all activities

Users

Search

File, folder, or site ¹

Add all or part of a file name, folder name ...

Start date

Tue May 18 2021

Start time

00:00

End date

Tue May 25 2021

End time

00:00

Search

Clear all

- 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:

The screenshot shows the 'MFA registration policy' configuration page in the Azure Portal. The left sidebar contains navigation links: Overview, Diagnose and solve problems, Protect (User risk policy, Sign-in risk policy, MFA registration policy), Report (Risky users, Risky sign-ins, Risk detections), and Notify (Users at risk detected alerts, Weekly digest). The main content area is titled 'Identity Protection | MFA registration policy'. It includes a search bar, a 'Policy Name' field with the value 'Multi-factor authentication registration policy', and an 'Assignments' section with a dropdown menu showing 'All users'. The 'Controls' section has a checkbox for 'Require Azure AD MFA registration' which is checked. The 'Include' tab is selected, showing options for 'All users' (selected) and 'Select individuals and groups'. A message states: 'MFA registration policy only affects cloud-based Azure MFA. If you have MFA Server it will not be affected.' The 'Enforce policy' section has a toggle switch set to 'On'. A 'Save' button is at the bottom.

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:

Microsoft Azure Search resources, services, and docs (G+/)

Home > Northgrove > Security > Identity Protection

Identity Protection | User risk policy

Search (Ctrl+ /)

- Overview
- Diagnose and solve problems
- Protect**
 - User risk policy**
 - Sign-in risk policy
 - MFA registration policy
- Report**
 - Risky users
 - Risky sign-ins
 - Risk detections
- Notify**
 - Users at risk detected alerts
 - Weekly digest

Policy Name
User risk remediation policy

Assignments

- Users
1 user included
- User risk ⓘ
Low and above

Controls

- Access ⓘ
Require password change

Enforce policy
☒ On ☐ Off

Save

Include Exclude

Select the users and groups to include in this policy

☐ All users

☒ Select individuals and groups

Selected users and groups

1 user

Allan Deyoung
AllanD@demogrove.OnMicro...

Assignments: Assign this policy only to “testUser1”

Home > Northgrove > Security > Identity Protection

Identity Protection | User risk policy

Search (Ctrl+ /)

- Overview
- Diagnose and solve problems
- Protect**
 - User risk policy**
 - Sign-in risk policy
 - MFA registration policy
- Report**
 - Risky users
 - Risky sign-ins
 - Risk detections
- Notify**
 - Users at risk detected alerts
 - Weekly digest

Policy Name
User risk remediation policy

Assignments

- Users
1 user included
- User risk ⓘ
Low and above

Controls

- Access ⓘ
Require password change

Enforce policy
☒ On ☐ Off

Save

User risk

User risk remediation policy

Configure user risk levels needed for policy to be enforced

Select the controls to be enforced.

☐ High

☐ Medium and above

☒ Low and above

Done

User risk: choose “Low and above”

Home > Northgrove > Security > Identity Protection

Identity Protection | User risk policy

Search (Ctrl+J)

- Overview
- Diagnose and solve problems

Protect

- User risk policy**
- Sign-in risk policy
- MFA registration policy

Report

- Risky users
- Risky sign-ins
- Risk detections

Notify

- Users at risk detected alerts
- Weekly digest

Policy Name
User risk remediation policy

Assignments

- Users
1 user included
- User risk ⓘ
Low and above

Controls

- Access ⓘ
Require password change

Enforce policy

On Off

Save

Access

User risk remediation policy

Control access enforcement to block or grant access.

Select the controls to be enforced.

☐ Block access

☒ Allow access

☒ Require password change

Done

Controls: Allow access + require password change

Create a risky sing-in policy

Microsoft Azure

Search resources, services, and docs (G+ /)

Home > Northgrove > Security > Identity Protection

Identity Protection | Sign-in risk policy

Search (Ctrl+ /)

- Overview
- Diagnose and solve problems
- Protect**
 - User risk policy
 - Sign-in risk policy**
 - MFA registration policy
- Report**
 - Risky users
 - Risky sign-ins
 - Risk detections
- Notify**
 - Users at risk detected alerts
 - Weekly digest

Policy **Users**

Include Exclude


Select the users and groups to include in this policy

☐ All users

☒ Select individuals and groups

Selected users and groups

1 user

 Benny Fransen
benny@northgrove.no

Enforce policy

☒ On ☐ Off

Save

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

Home > Northgrove > Security > Identity Protection

Identity Protection | Sign-in risk policy

Search (Ctrl+/)

- Overview
- Diagnose and solve problems
- Protect**
 - User risk policy
 - Sign-in risk policy**
 - MFA registration policy
- Report**
 - Risky users
 - Risky sign-ins
 - Risk detections
- Notify**
 - Users at risk detected alerts
 - Weekly digest

Policy Name
Sign-in risk remediation policy

Assignments

- Users
 - 1 user included
- Sign-in risk ⓘ
 - Low and above

Controls

- Access ⓘ
 - Require multi-factor authentication

Enforce policy
☒ On ☐ Off

Save

Sign-in risk

Sign-in risk remediation policy

Configure user risk levels needed for policy to be enforced

Select the controls to be enforced.

☐ High

☐ Medium and above

☒ Low and above

Done

Sign-in risk: choose “Low and above”

Home > Northgrove > Security > Identity Protection

Identity Protection | Sign-in risk policy

Search (Ctrl+/)

- Overview
- Diagnose and solve problems
- Protect**
 - User risk policy
 - Sign-in risk policy**
 - MFA registration policy
- Report**
 - Risky users
 - Risky sign-ins
 - Risk detections
- Notify**
 - Users at risk detected alerts
 - Weekly digest

Policy Name
Sign-in risk remediation policy

Assignments

- Users
 - 1 user included
- Sign-in risk ⓘ
 - Low and above

Controls

- Access ⓘ
 - Require multi-factor authentication

Enforce policy
☒ On ☐ Off

Save

Access

Sign-in risk remediation policy

Control access enforcement to block or grant access.

Select the controls to be enforced.

☐ Block access

☒ Allow access

☒ Require multi-factor authentication

Done

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
 - o (if no Suspicious 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.azure.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
 - o (if no Suspicious 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.**

Your evaluation lab

Manage your test devices, attack simulations and reports. Learn and experience the Microsoft Defender for Endpoint capabilities through a guided walkthrough in the trial environment. See it in action as it prevents, detects, and remediates the most sophisticated attacks.

Overview **Devices** User Actions Simulations Report

1 element + Add device Tilpass kolonner

Device name	OS Platform	Status	Simulator status	Time left	Risk level ⓘ	Exposure level ⓘ	Alerts number	Network	IP address	Actions
testmachine1	Windows 10	Active	Multiple ⓘ	11h	■ ■ ■ Ingen	▲ Lav		LabVnet	20.93.157.156	<div><div>⋮</div><div>Connect</div><div>Reset password</div></div>

DISABLE NETWORK LEVEL AUTHENTICATION (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”

1 element Create simulation

End time	Executed by
14. nov. 2021 kl. 18:37	KjetilNordlund@N...

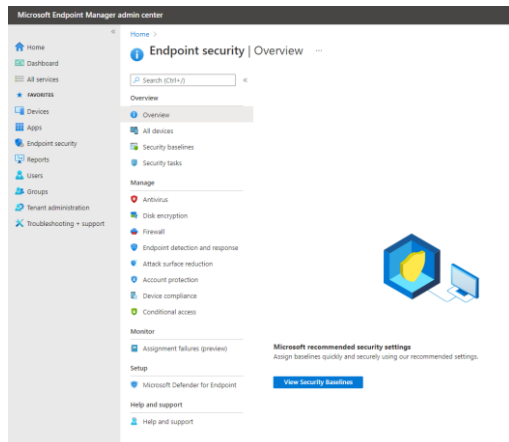
Choose:

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

Security Baseline for Windows 10 and later

Home > Endpoint security > Endpoint security > MDM Security Baseline > Create profile

Basics Configuration settings Scope tags Assignments Review + create

Name *

Description

Platform

Baseline version

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)

Windows Security

Enable tamper protection to prevent Microsoft Defender being disabled ⓘ	Enable
Hide the Virus and threat protection area in the Windows Security app ⓘ	Not configured
Hide the Account protection area in the Windows Security app ⓘ	Not configured
Hide the Firewall and network protection area in the Windows Security app ⓘ	Not configured
Hide the App and browser control area in the Windows Security app ⓘ	Not configured
Hide the Device security area in the Windows Security app ⓘ	Not configured
Hide the Device performance and health area in the Windows Security app ⓘ	Not configured
Hide the Family options area in the Windows Security app ⓘ	Yes
Windows Security app notifications ⓘ	Not configured
Hide the Windows Security icon from the notification area ⓘ	Not configured
Disable the Clear TPM option in the Windows Security app ⓘ	Not configured
Prompt users to update TPM firmware if vulnerability is discovered ⓘ	Not configured
Organization's support contact information ⓘ	Not configured

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.

✓ Basics 2 Configuration settings 3 Scope tags 4 Assignments 5 Review + create

Settings

Search for a setting

Cloud protection

Turn on cloud-delivered protection ⓘ	Yes
Cloud-delivered protection level ⓘ	Zero tolerance
Defender Cloud Extended Timeout In Seconds ⓘ	50

Microsoft Defender Antivirus Exclusions

Real-time protection

Turn on real-time protection ⓘ	Yes
Enable on access protection ⓘ	Yes
Monitoring for incoming and outgoing files ⓘ	Monitor all files
Turn on behavior monitoring ⓘ	Yes
Turn on intrusion prevention ⓘ	Yes
Enable network protection ⓘ	Enable
Scan all downloaded files and attachments ⓘ	Yes
Scan scripts that are used in Microsoft browsers ⓘ	Not configured
Scan network files ⓘ	Not configured
Scan emails ⓘ	Not configured

Remediation

Number of days (0-90) to keep quarantined malware 30 ✓

Submit samples consent Send all samples automatically ✓

Action to take on potentially unwanted apps Enable ✓

Actions for detected threats Configure Not configured

Low threat Quarantine ✓

Moderate threat Quarantine ✓

High threat Quarantine ✓

Severe threat Quarantine ✓

Scan

Scan archive files Not configured ✓

Use low CPU priority for scheduled scans Not configured ✓

Disable catch-up full scan Not configured ✓

Disable catch-up quick Scan Not configured ✓

CPU usage limit per scan ✓

Scan mapped network drives during full scan Not configured ✓

Run daily quick scan at Not configured ✓

Scan type Quick scan ✓

Day of week to run a scheduled scan Everyday ✓

Time of day to run a scheduled scan Not configured ✓

Check for signature updates before running scan Not configured ✓

Updates

Enter how often (0-24 hours) to check for security intelligence updates 4 ✓

Define file shares for downloading definition updates 0 items ✓

Define the order of sources for downloading definition updates 0 items ✓

User experience

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.

Select operating system to start onboarding process:

Windows 10 and 11

1. Onboard a device

First device onboarded: Completed ✓

Onboard devices to Microsoft Defender for Endpoint using the onboarding configuration package that matches your [preferred deployment method](#). For other device preparation instructions, read [Onboard and set up](#).

Deployment method

Mobile Device Management / Microsoft ...

You can use Mobile Device Management solutions, such as Microsoft Intune to configure and monitor your devices.

For more information on how to configure and monitor Microsoft Defender for Endpoint devices, see [Configure devices using Mobile Device Management tools](#) section in the [Microsoft Defender for Endpoint guide](#).

↓ Download onboarding package

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

Create profile ...

Endpoint detection and response

✓ Basics ② Configuration settings ③ Scope tags ④ Assignments ⑤ Review + create

Settings

Search for a setting

Endpoint Detection and Response

Sample sharing for all files ⓘ

Yes

Not configured

Expedite telemetry reporting frequency ⓘ

Yes

Not configured

- 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

^ Attack Surface Reduction Rules

Block persistence through WMI event subscription	Block
Block credential stealing from the Windows local security authority subsystem (lsass.exe)	Enable
Block Adobe Reader from creating child processes	Enable
Block Office applications from injecting code into other processes	Block
Block Office applications from creating executable content	Block
Block all Office applications from creating child processes	Block
Block Win32 API calls from Office macro	Block
Block Office communication apps from creating child processes	Enable
Block execution of potentially obfuscated scripts (js/vbs/ps)	Block
Block JavaScript or VBScript from launching downloaded executable content	Block
Block process creations originating from PSExec and WMI commands	Block
Block untrusted and unsigned processes that run from USB	Block
Block executable files from running unless they meet a prevalence, age, or trusted list criteria	Block
Block executable content download from email and webmail clients	Block
Use advanced protection against ransomware	Enable
Enable folder protection	Audit mode
List of additional folders that need to be monitored	0 items

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

The screenshot shows the Microsoft Intune configuration page. At the top, there's a blue header with the Microsoft Azure logo, an 'Upgrade' button, and a search bar. Below the header, the breadcrumb trail is 'Home > Northgrove > Configure'. The main heading is 'Configure' with a subheading 'Microsoft Intune'. There are three action buttons: 'Save', 'Discard', and 'Delete'. The page is divided into two sections: MDM (Mobile Device Management) and MAM (Mobile Application Management). The MDM section has a 'MDM user scope' dropdown set to 'All', and three URL fields: 'MDM terms of use URL' (https://portal.manage.microsoft.com/TermsOfUse.aspx), 'MDM discovery URL' (https://enrollment.manage.microsoft.com/enrollmentserver/discovery.svc), and 'MDM compliance URL' (https://portal.manage.microsoft.com/?portalAction=Compliance). There is a link 'Restore default MDM URLs'. The MAM section has a 'MAM user scope' dropdown set to 'None', and three URL fields: 'MAM terms of use URL' (empty), 'MAM discovery URL' (https://wip.mam.manage.microsoft.com/Enroll), and 'MAM compliance URL' (empty). There is a link 'Restore default MAM URLs'.

Set "MDM user scope" to all. Click Save

Login to your testmachine with "Administrator1" and the provided password.

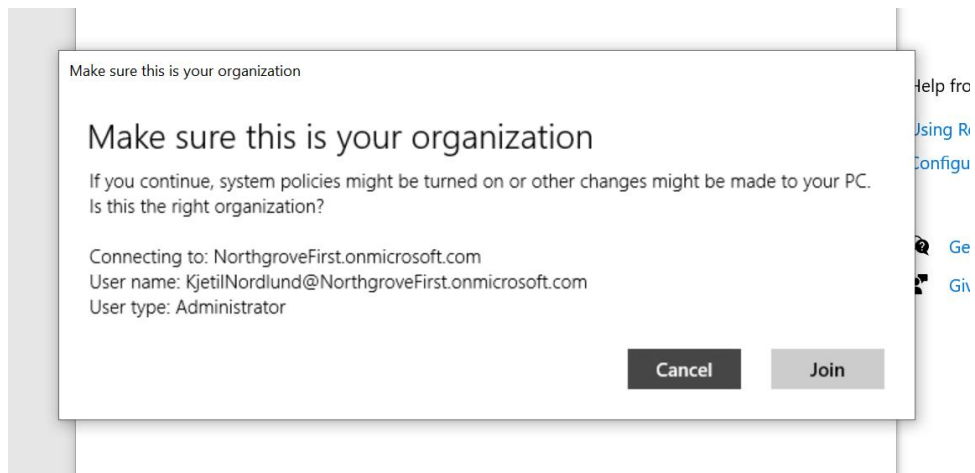
Go to: Start -> Settings -> Accounts -> Access Work or School

Click "Connect"

The screenshot shows a dialog box titled 'Set up a work or school account'. It has a close button (X) in the top right corner. The text inside says: 'You'll get access to resources like email, apps, and the network. Connecting means your work or school might control some things on this device, such as which settings you can change. For specific info about this, ask them.' Below this is an input field labeled 'Email address'. At the bottom, there are two links: 'Join this device to Azure Active Directory' and 'Join this device to a local Active Directory domain'. A 'Next' button is at the bottom right.

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

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

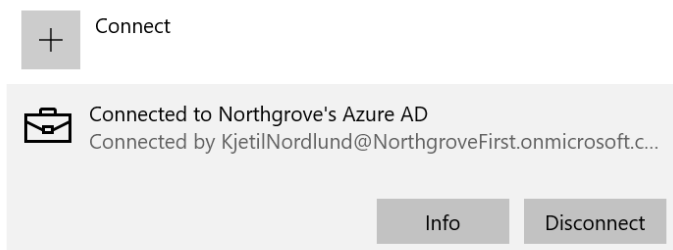


Click join

Click done

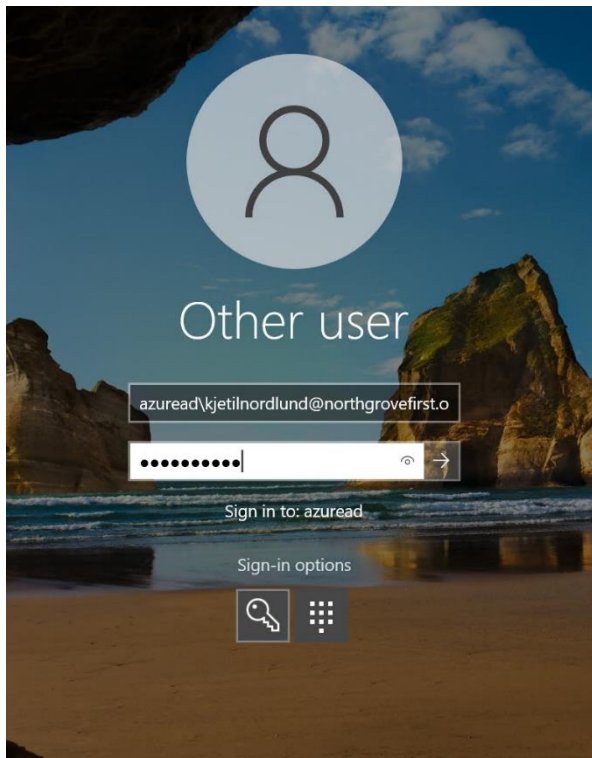
Access work or school

Get access to resources like email, apps, and the network. Connecting means your work or school might control some things on this device, such as which settings you can change. For specific info about this, ask them.



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](#)

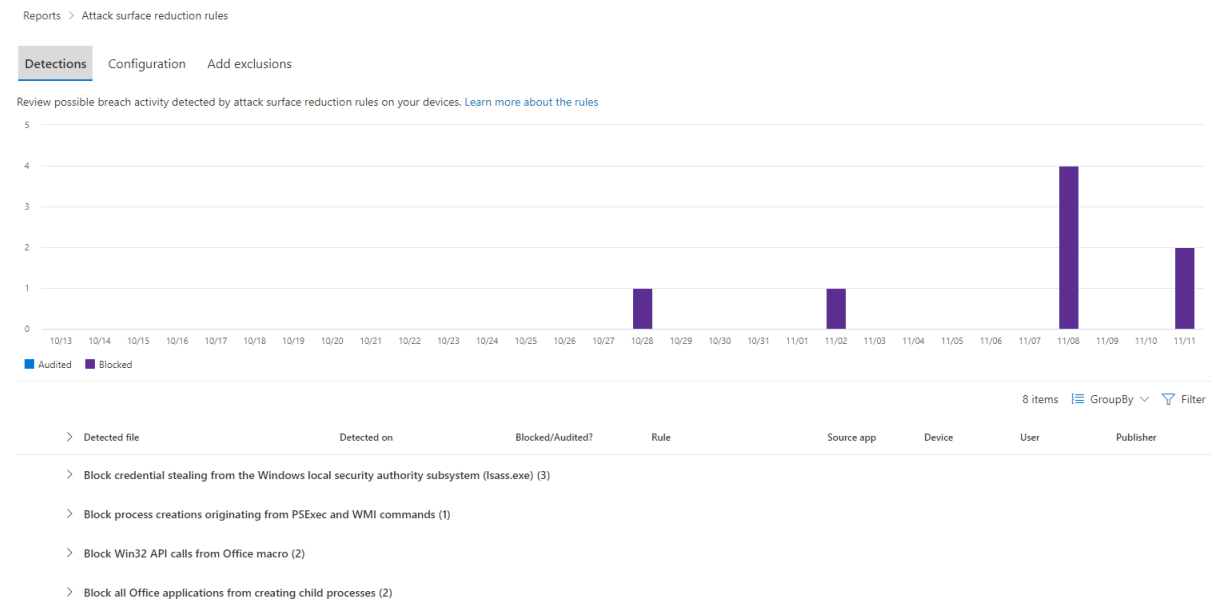
<https://demo.wd.microsoft.com/> - contains several test scenarios for Defender and ASR

<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.



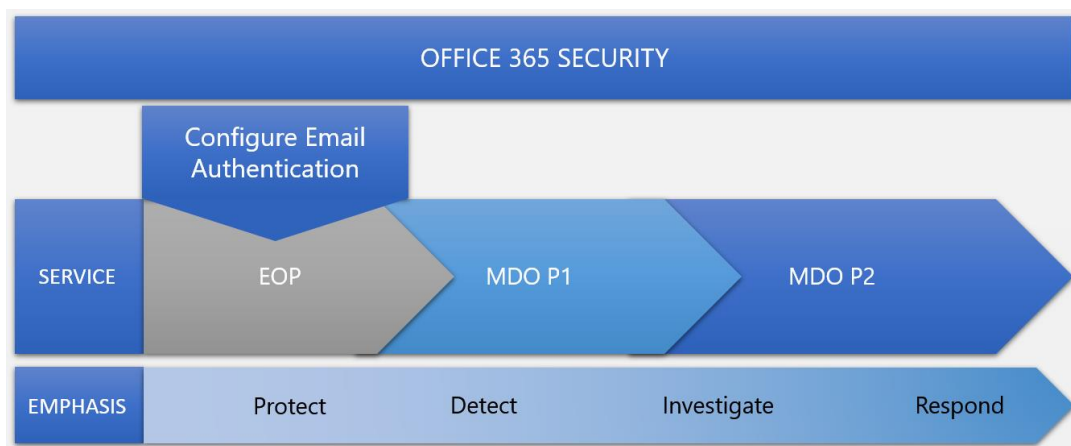
DEFENDER FOR OFFICE 365

WHAT IS DEFENDER FOR OFFICE 365 SECURITY

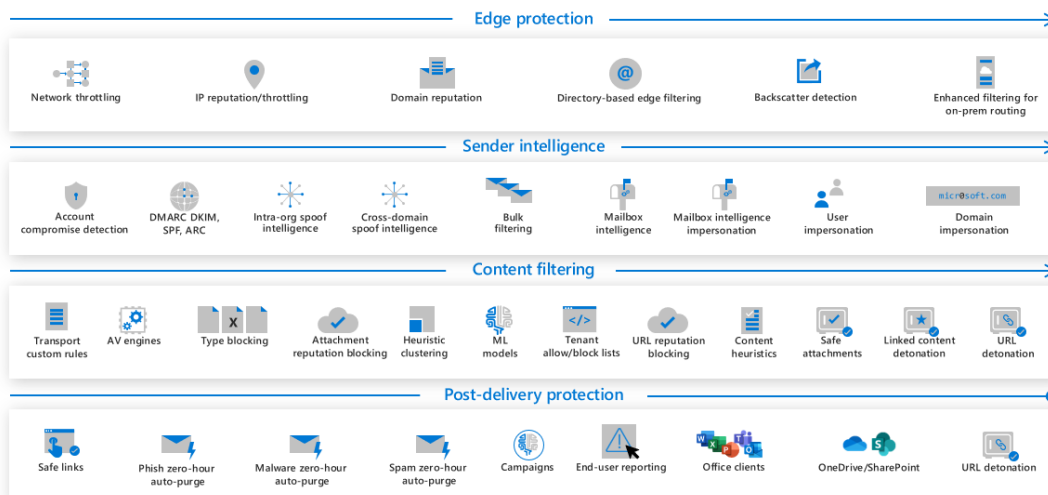
Every Office 365 subscription comes with security capabilities. The goals and actions that you can take depend on the focus of these different subscriptions. In Office 365 security, there are three main security services (or products) tied to your subscription type:

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](#)



Microsoft Defender for Office 365 protection stack



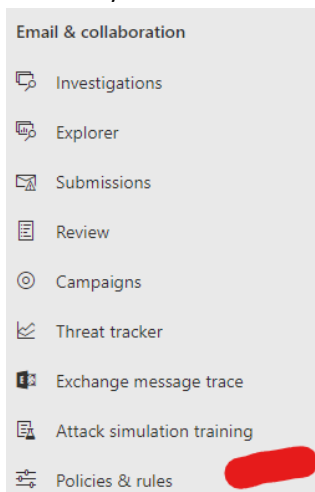
SETUP AND CONFIGURATION

[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**.


Policies

	Anti-phishing	Protect users from phishing attacks, and configure safety tips on suspicious messages.
	Anti-spam	Protect your organization's email from spam, including what actions to take if spam is detected
	Anti-malware	Protect your organization's email from malware, including what actions to take and who to notify if malware is detected
	Safe Attachments	Protect your organization from malicious content in email attachments and files in SharePoint, OneDrive, and Teams
	Safe Links	Protect your users from opening and sharing malicious links in email messages and Office apps

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

Policy name

Add a name and description for your custom anti-phishing policy.

Name * ⓘ

Anti Phish

Description

3. Add your tenant domain(s)

Users, groups, and domains

Add users, groups and domains to include or exclude in this policy.

Include these users, groups and domains

Users

Groups

Domains

firsttest2.onmicrosoft.com X

☐ Exclude these users, groups and domains

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

Phishing threshold & protection

Set your phishing thresholds and desired impersonation and spoof protections for this policy. [Learn more](#)

Phishing email threshold ⓘ

2 - Aggressive

Messages that are identified as phishing with a high degree of confidence are treated as if they were identified with a very high degree of confidence.

Impersonation

☒ **Enable users to protect (0/350)** ⓘ

Enable impersonation protection for up to 350 internal and external users.
[Learn more about adding users to impersonation protection](#)

Manage 0 sender(s)

☒ **Enable domains to protect (1)**

Enable impersonation protection for these internal and external sender domains.

☒ Include domains I own ⓘ

View my domains

☐ Include custom domains ⓘ

Add trusted senders and domains (0)

Add trusted senders and domains so they are not flagged as an impersonation-based attack

Manage 0 trusted sender(s) and domain(s)

☒ **Enable mailbox intelligence (Recommended)**

Enables artificial intelligence (AI) that determines user email patterns with their frequent contacts to identify potential impersonation attempts [Learn more](#)

☒ **Enable Intelligence for impersonation protection (Recommended)**

Enables enhanced impersonation results based on each user's individual sender map and allows you to define specific actions on impersonated messages

Spoof

☒ **Enable spoof intelligence (Recommended)**

Choose how you want to filter email from senders who are spoofing domains. To control which senders are allowed to spoof your domains or external domains, use the [Tenant Allow/Block List Spoofing page](#).
[Learn more about Spoof Intelligence](#)

5.

6. Click on manage 0 sende(s)

Manage senders for impersonation protection

Add up to 350 internal and external senders to protect from being impersonated by attackers. We recommend adding people in key roles.
[Learn more about adding senders to protect](#)

2 items

Display name	Sender email address
First Woman	FirstWoman@firsttest2.onmi...
First Man	admin@firsttest2.onmicrosof...

7.

Actions

Set what actions you'd like this policy to take on messages. You may need to turn on certain protections to access all available policy action

Message actions

If message is detected as an impersonated user

Move message to the recipients' Junk Email folders

Move message to the recipients' Junk Email folders

If message is detected as an impersonated domain

Move message to the recipients' Junk Email folders

Move message to the recipients' Junk Email folders

If Mailbox Intelligence detects an impersonated user

Move message to the recipients' Junk Email folders

Move message to the recipients' Junk Email folders

If message is detected as spoof

Move message to the recipients' Junk Email folders

Move message to the recipients' Junk Email folders

Safety tips & indicators ⓘ

- ☒ Show first contact safety tip (Recommended) ⓘ
- ☒ Show user impersonation safety tip ⓘ
- ☒ Show domain impersonation safety tip ⓘ
- ☒ Show user impersonation unusual characters safety tip ⓘ
- ☒ Show (?) for unauthenticated senders for spoof ⓘ
- ☒ Show "via" tag ⓘ

8.

TEST SCENARIO

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

Email address needs to 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)

Policies & rules > Threat policies > Safe attachments

Set up an safe attachments policy for specific users or groups to help prevent people from opening or sharing email attachments that contain malicious content. [Learn more about safe attachments for email](#)

+ Create ↓ Export ↻ Refresh 📄 Reports ⚙️ Global settings

Name	Status	Priority
------	--------	----------

Activate Global Settings for:

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

Global settings ×

Use this page to protect your organization from malicious content in email attachments and files in SharePoint, OneDrive, and Microsoft Teams.

Protect files in SharePoint, OneDrive, and Microsoft Teams

If a file in any SharePoint, OneDrive, or Microsoft Teams library is identified as malicious, Safe Attachments will prevent users from opening and downloading the file. [Learn more](#)

Turn on Defender for Office 365 for SharePoint, OneDrive, and Microsoft Teams

☒

Help people stay safe when trusting a file to open outside Protected View in Office applications.

Before a user is allowed to trust a file opened in a supported version of Office, the file will be verified by Microsoft Defender for Endpoint. [Learn more about Safe Documents.](#)

Turn on Safe Documents for Office clients. Only available with *Microsoft 365 E5* or *Microsoft 365 E5 Security* license. [Learn more about how Microsoft handles your data.](#)

☒

Allow people to click through Protected View even if Safe Documents identified the file as malicious

☐

Save Cancel

POLICY SETTINGS - SAFE ATTACHMENTS

1. Create a new Policy

Policies & rules > Threat policies > Safe attachments

Set up an safe attachments policy for specific users or groups to help prevent people from opening or sharing email attachments that contain malicious content. [Learn more about safe attachments for email](#)

+ Create ↓ Export ↻ Refresh 📄 Reports ⚙️ Global settings

Name	Status	Priority
------	--------	----------

2. Give the Policy a Name and a Description

Name your policy

Name *

Description

3. Add your domain(s) to the policy

Users and domains

Include these users, groups and domains

Users

Groups

Domains

firsttest2.onmicrosoft.com first.kents-events.com

☐ Exclude these users, groups and domains

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

4. Configure the behavior of the Sandbox.

Settings

Safe Attachments unknown malware response

Select the action for unknown malware in attachments. [Learn more](#)

Warning

- **Monitor, Replace and Block** actions might cause a significant delay in message delivery. [Learn more](#)
- **Dynamic Delivery** is only available for recipients with hosted mailboxes. [Learn more](#)
- For **Block, Replace, or Dynamic Delivery**, messages with detected attachments are quarantined and can only be released by an admin.

- ☐ Off - Attachments will not be scanned by Safe Attachments.
- ☐ Monitor - Deliver the message if malware is detected and track scanning results.
- ☒ Block - Block current and future messages and attachments with detected malware.
- ☐ Replace - Block attachments with detected malware, but deliver the message.
- ☐ Dynamic Delivery (Preview feature) - Immediately deliver the message without attachments. Reattach files after scanning is complete.

Redirect messages with detected attachments

☐ Enable redirect ⓘ

Send messages that contain blocked, monitored, or replaced attachments to the specified email address.

☒ Apply the Safe Attachments detection response if scanning can't complete (timeout or errors).

If you turn on this setting, you should also turn on and configure redirection. Otherwise, messages might be lost.

Security feature name	Default	Standard	Strict
Safe Attachments unknown malware response	Off	Block	Block
	<input type="checkbox"/> Enable \$false and <input type="checkbox"/> Action Block	<input type="checkbox"/> Enable \$true and <input type="checkbox"/> Action Block	<input type="checkbox"/> Enable \$true and <input type="checkbox"/> Action Block
Enable and Action			

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.

test

 Copy report text below  Prepare and email extended report

Sender

AzKehusvik@outlook.com

Recipient

admin@first.kents-events.com

Received

Processed

Not yet delivered

Status

Office 365 received the message that you specified, but delivery to the recipient (admin@first.kents-events.com) has been delayed. We're working on delivering it.

This is the last record we have for the message: In process

More Information

Check the Message Events table below for any additional information about why message delivery might be delayed. For example, it might be due to a temporary issue trying to connect to the recipient's email server outside of Office 365. Many such delays clear up on their own, and the message gets delivered. If Office 365 isn't able to send or deliver the message within 48 hours, the sender will receive a non-delivery report (NDR) message with more information about how to fix the issue.

If you don't want to wait for the message to finish being processed, consider asking the sender to send the message again using a different email address.

Message events

▼	Date (UTC+01:00)	Event	Detail
▼	10/26/2021, 11:16 AM	Receive	Message received by...
			Message received by: OLAP279MB0088.NORP279.PROD.OUTLOOK.COM using TLS1.2 with AES256
▼	10/26/2021, 11:17 AM	Defer	Reason: 400 4.7.721 ...
			Reason: 400 4.7.721 Advanced Threat Protection scanning in progress.
▼	10/26/2021, 11:17 AM	Spam	No detail informatio...
			No detail information available.

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 Word, Excel, Power Point etc..

Policies & rules > Threat policies > Safe links

Safe Links helps prevent your users from following links in email and document

+ Create ↓ Export ↻ Refresh 📄 Reports ⚙ Global settings

Name

Safe Links settings for your organization

Global settings for users included in active Safe Links policies

When users click a blocked URL, they're redirected to a web page that explains why the URL is blocked.

These URLs will be blocked in email messages and in Office 365 Apps and Office for iOS and Android files.

You can use three wildcard asterisks (*) per URL entered.

[Get help with this](#)

Block the following URLs:

Settings that apply to content in supported Office 365 apps

These settings don't apply to email messages. If you want to apply them for email, create a Safe Links policy for email recipients.

Use Safe Links in Office 365 apps:

☒

Use Safe Links protection in:

Supported Office 365 desktop, mobile, and web apps. [Learn more](#).

When a user clicks a URL in a supported Office 365 app, Safe Links will check the link. If the link is found to be malicious, the user is redirected to a warning page for further action.

In supported Office 365 apps:

Do not track when users click protected links in Office 365 apps

☐

Turn on this setting if you don't want to store information about user clicks in supported Office 365 apps.

Do not let users click through to the original URL in Office 365 apps

☐

When this setting is turned on, users can't click through to the original URL on the warning page that's displayed.






Save

Cancel

POLICY SETTINGS – SAFE LINKS

Policies & rules > Threat policies > Safe links

Safe Links helps prevent your users from following links in email and documents.

 Create  Export  Refresh  Reports  Global settings

Name

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

Name your policy

Add a name and description for your safe links policy.

Name *

Safe Links

Description

3. Add your domain(s) to the policy

Users and domains

Add users, groups and domains to include or exclude in this policy.

Include these users, groups and domains

Users

Groups

Domains

 first.kents-events.com   firsttest2.onmicrosoft.com 

☐ Exclude these users, groups and domains

4. Activate following settings

Protection settings

Select the action for unknown potentially malicious URLs in messages.

- ☐ Off
- ☒ On - URLs will be rewritten and checked against a list of known malicious links when user clicks on the link.

Select the action for unknown or potentially malicious URLs within Microsoft Teams.

- ☐ Off
- ☒ On - Microsoft Teams will check against a list of known malicious links when user clicks on a link; URLs will not be rewritten.

- ☒ Apply real-time URL scanning for suspicious links and links that point to files
- ☒ Wait for URL scanning to complete before delivering the message
- ☒ Apply Safe Links to email messages sent within the organization
- ☐ Do not track user clicks
- ☒ Do not let users click through to the original URL
- ☒ Display the organization branding on notification and warning pages
- ☐ Do not rewrite URLs, do checks via Safe Links API only. [View supported clients.](#)

Do not rewrite the following URLs

http(s)://www.example.com

Add

5. Use the default notification and Submit the policy.

Notification

How would you like to notify your users?

- ☒ Use the default notification text
- ☐ Use custom notification text

TEST SCENARIO

Send an Email with the following link included [https://smartscreentestratings2\(.\)net/](https://smartscreentestratings2(.)net/) - Remove the (.) from the URL.

You can also test with a link to a

 <https://eur04.safelinks.protection.outlook.com/?url=https%3A%2F%2F01support-dhl.com%2F&data=04%7C01%7Ckehusvik%40kents-events.com%7Cced4d2bfd4eb43ce18ab08d9a2b5b032%7C5ebe5a510b5c4841977dffcea8c10c70%7C19>



This website has been
classified as malicious.

Opening this website might not be safe.

<https://01support-dhl.com/>

We recommend that you don't open this website, as opening it might not be safe and could harm your computer or result in malicious use of your personal data.

[Continue anyway \(not recommended\)](#)

For Feedback on [Microsoft Defender for Office 365](#)

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>



Cloud App Security

Connected apps

App connectors provide you with greater visibility and control over your cloud apps.

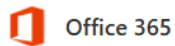
Filters:

App: Select apps... App category: Select category... Connected by: Select users...

+ Connect an app

App	Status
Office 365 Collaboration	Connected
Microsoft Azure Cloud computing platform	Connected

Click "Connect an app" and Choose "Office 365"



Connect Office 365

Before you connect Office 365, we highly recommend reviewing the [Office 365 connection guide](#). Follow these steps in order to connect Office 365.

1 Select Office 365 components

- ☒ Azure AD Users and groups ⓘ
- ☒ Azure AD Management events ⓘ
- ☒ Azure AD Sign-in events ⓘ
- ☒ Azure AD Apps ⓘ
- ☒ Office 365 activities ⓘ
- ☒ Office 365 files ⓘ

2 Connect app

Connect

Close

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”

Edit anomaly detection policy

[View open alerts \(27\)](#) [?](#)

[?](#) This is a built-in anomaly detection policy.
[Learn more about it](#) | [Send us feedback](#)

Policy name *

Risky sign-in

Category *

Threat detection

Description

Azure Active Directory (Azure AD) detects suspicious actions that are related to your user accounts. For each detected action, a record called a risk event is created. For more details, see Azure AD risk events.

Alerts suppression

Trigger alerts with a minimum severity of:

Low

This policy was modified 10 months ago

We secure your data as described in our [privacy statement](#) and [online service terms](#).

[Update](#)

[Cancel](#)

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”

?

☐ Advanced filters

Type: **Select type...** Severity: Name: Category: **Select risk category...**

1 - 20 of 42 Templates  Hide filters  Table settings 

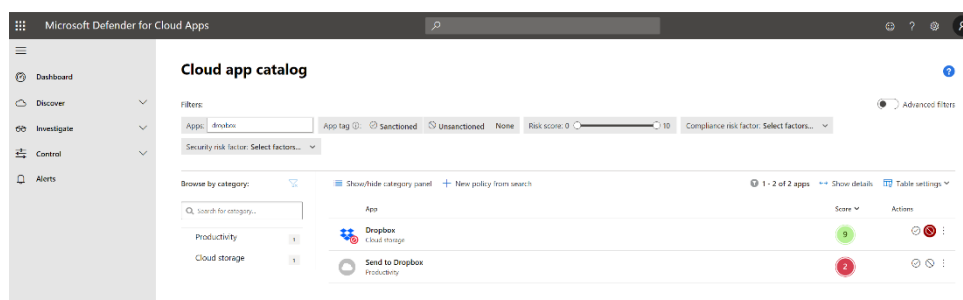
Configure the policy to reflect sensible settings. In this scenario we do set a configuration that's makes it easy to trigger an alert:


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

Search for Facebook in the Cloud app catalog

Deep link:

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

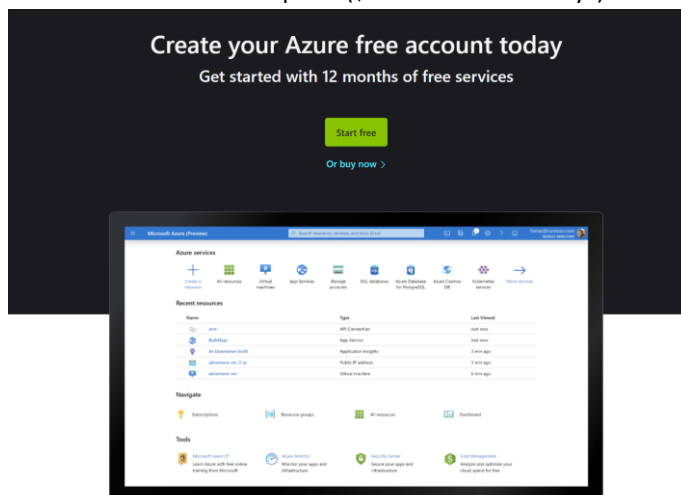
EXTRA: AZURE SENTINEL

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 self

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



What do I get?

With your Azure free account, you get all of this—and you won't be charged until you choose to upgrade.

12 months of popular free services	+	\$200 credit to explore Azure for 30 days	+	Always free 25+ services
--	---	---	---	------------------------------------

<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

The screenshot shows the Azure sign-up page for Norway. The form includes fields for First name (Kjetil), Middle name (Optional), Last name (Nordlund), Email address (kjetil-first@outlook.com), and Phone (474 81 19715). There are checkboxes for using a different phone number, being an authorized purchaser, and agreeing to terms. A 'Next' button is at the bottom of the form. To the right, a sidebar lists 'Popular services free for 12 months', '25+ services always free', and 'USD200 credit to use in your first 30 days'. A 'No automatic charges' section explains the credit. A 'Sign up' button is at the bottom right.

Norway

Choose the location that matches your billing address. **You cannot change this selection later.** If your country is not listed, the offer is not available in your region. [Learn More](#)

First name
Kjetil

Middle name (Optional)

Last name
Nordlund

Email address [i](#)
kjetil-first@outlook.com

Phone [i](#)
474 81 19715

☐ Use a different phone number to verify your identity.
[Text me](#) [Call me](#)

☐ Select here if you are an authorized purchaser for a VAT registered company [i](#)

By proceeding you acknowledge that if you use your organization's email, your organization may have rights to access and manage your data and account. [Learn More](#)

☐ I agree to the [customer agreement](#) and [privacy agreement](#)

☐ I would like to receive information, tips, and offers from Microsoft about Azure and other Microsoft products and services, and for Microsoft to share my information with select Partners so I can receive relevant information about their products and services.

[Next](#)

Identity verification by card [v](#)

[Sign up](#)

Popular services free for 12 months

25+ services always free

USD200 credit to use in your first 30 days

No automatic charges
After your credit is over, we'll ask you if you want to continue with pay-as-you-go. If you do, you'll only pay if you use more than the free amounts of services.

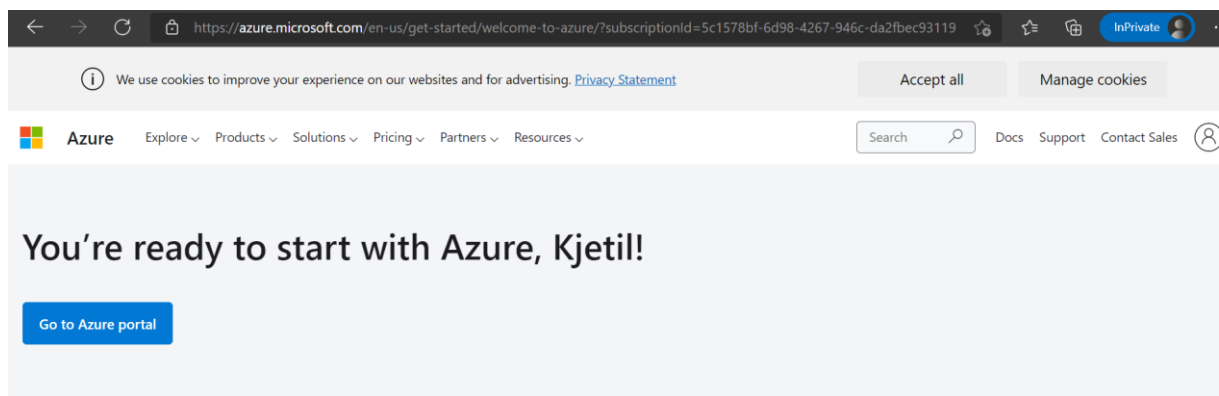
[Chat with Sales](#)

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 see a Azure Subscription:

Home >

Subscriptions

Northgrove (NorthgroveFirst.onmicrosoft.com)

+ Add Manage Policies View Requests

View list of subscriptions for which you have role-based access control (RBAC) permissions to manage Azure resources. To view subscriptions for which you have billing access, [click here](#)

Showing subscriptions in Northgrove directory. Don't see a subscription? [Switch directories](#)

My role 8 selected Status 3 selected

Apply

Showing 1 of 1 subscriptions ☒ Show only subscriptions selected in the [global subscriptions filter](#)

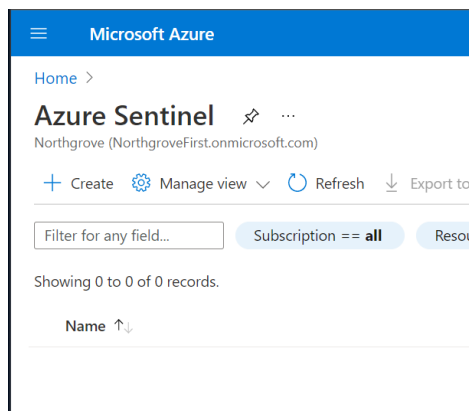
Search

Subscription name ↑↓	Subscription ID ↑↓	My role ↑↓	Current cost	Status ↑↓
Azure subscription 1	5c1578bf-6d98-4267-946c-da2fbec93119	Owner		Active

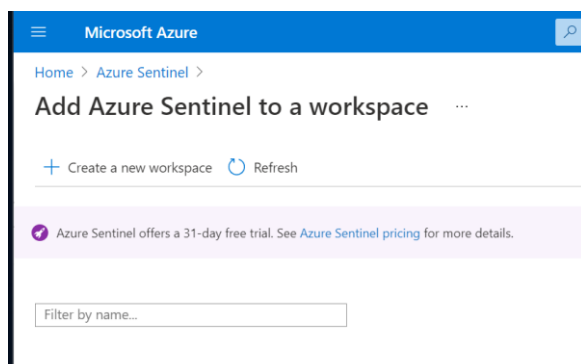
SETUP OF MICROSOFT SENTINEL

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 Log Analytics workspace

Basics Tags Review + Create

A Log Analytics workspace is the basic management unit of Azure Monitor Logs. There are specific considerations you should take when creating a new Log Analytics workspace. [Learn more](#)

With Azure Monitor Logs you can easily store, retain, and query data collected from your monitored resources in Azure and other environments for valuable insights. A Log Analytics workspace is the logical storage unit where your log data is collected and stored.

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *

Azure subscription 1

▼

Resource group *

(New) rgSentinel

▼

[Create new](#)

Instance details

Name *

AzureSentinelWorkspace

✓

Region *

North Europe

▼

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

Click Create

Submitting deployment...

Running

Submitting the deployment template for resource group 'rgSentinel'.

a few seconds ago

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

Add Azure Sentinel to a workspace

+ Create a new workspace Refresh

Azure Sentinel offers a 31-day free trial. See [Azure Sentinel pricing](#) for more details.

Filter by name...		
Workspace ↑↓	Location ↑↓	ResourceGroup ↑↓
AzureSentinelWorkspace	northeurope	rgsentinel

Choose the workspace and click “add”

Adding Azure Sentinel

Adding Azure Sentinel to workspace 'AzureSentinelWorkspace'

Wait for Microsoft Sentinel to be provisioned

Microsoft Azure

Search resources, services, and docs (G+)

Kjetil NORTH

Home > Azure Sentinel > Add Azure Sentinel to a workspace > Azure Sentinel

Azure Sentinel | News & guides

Selected workspace: 'azuresentinelworkspace'

Search (Ctrl+J)

Documentation

General

Overview

Logs

News & guides

Threat management

Incidents

Workbooks

Hunting

Notebooks

Entity behavior

Threat intelligence

Content management

Content hub (Preview)

Repositories (Preview)

Community

Configuration

Data connectors

Analytics

Watchlist

Automation

Settings

Azure Sentinel free trial activated

The free trial is active on this workspace from 14.11.2021 to 15.12.2021 at 23:59:59 UTC. During the trial, up to 10 GB/day are free for **both Azure Sentinel and Log Analytics**. Data beyond the 10 GB/day included quantity will be billed. [Learn more.](#)

OK

Azure Sentinel

A cloud-native SIEM to help you focus on what matters most

Collect and analyze data from any source, cloud or on-premises, in any format, at cloud scale. With AI on your side, find, investigate, and respond to real threats in minutes, with built-in knowledge and intelligence from decades of Microsoft security experience.

1. Collect data

Collect data at cloud scale across the enterprise, both on-premises and in multiple clouds

Connect

2. Create security alerts

Focus on what's important using analytics to create alerts

Create

3. Automate & orchestrate

Use or customize built-in playbooks to automate common tasks

Create

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 type 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 python.exe establishes an outbound connection to?

SAFEBRACH AND KNOWN RANSOMWARE 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?

