Microsoft Security

Advanced Interactive Security Workshop

Benjamin Kovacevic
Microsoft 365 Technical Specialist
EMEA Advanced Cloud Expert – Security
Version: December, 2020

Table of Contents

Rules and what's covered

Advanced Interactive Security Workshop (AISW) is set of instructions that can be used for hands-on learning of Microsoft 365 Security and Compliance stack. For AISW it is recommended to open M365 E5 trial subscription (contact your Microsoft representative if help needed), add 20 test users, and preconfigure tenant with configuration below. For each feature in this document, I have had provided step-by-step instructions how the feature is enabled, as well as description how to test the feature and how to tune it more for your needs.

All headings are linked to Microsoft docs - if you want to learn more about specific feature or to find How-to guide or Tutorial on Microsoft docs.

Since I'm maintaining this document alone, errors and inaccuracies can happen. If you detect inaccuracy or you would like see specific feature in AISW or you have any other feedback, please submit your response on this form:
https://forms.office.com/Pages/ResponsePage.aspx?id=DQSIkWdsW0yxEjajBLZtrQAAAAAAAAAAAAN__rvUg1ZURE5ZOEVIQjkxVFc2RzY4S0RGRU9SSURGOC4u

or by scanning QR code:

I will be publishing new version every 3 months which will include fixes of the inaccuracies, new features, and/or extended configuration/testing for already included feature. I'll give my best to document all changes between the versions.

Advanced Interactive Security Workshop includes following pillars:

1. Identity protection
2. Device and app management
3. Information Protection
4. Threat Protection
5. Compliance

IDENTITY PROTECTION

1. Enable basic Identity protection like Conditional Access, Passwordless log-in, Self-Service Password Reset, Custom banned password list, Azure AD B2B for secure guest access
2. Enable advanced Identity Protection & Governance like Identity Protection with Sign-in risks and User risk, Privileged Identity Manager, Identity Governance

DEVICE & APP MANAGEMENT

1. Configure basic device and app management policy – Windows, Android, iOS
2. Push Microsoft 365 Apps (Office 365 ProPlus) to all Win devices

3. Add custom .msi application – ex. AIP UL client

INFORMATION PROTECTION

1. Configure DLP and Endpoint DLP, Retention policy, Unified Labeling
2. Enable Unified Labeling (including support for Teams, OneDrive and SharePoint Online)

THREAT PROTECTION

1. Configure Microsoft Defender for Office 365 (Safe Links, Safe Attachments) for EXO, SPO, and Teams – execute Attack Simulator; fine tune policies using Configuration Analyzer
2. Configure MD for Endpoint (enable all integrations and advance features, web content filtering, MCAS integration) plus do Evaluation labs and testing scenarios
3. Configure MCAS (make demo report, integration with AIP, MD for Endpoint, enable policies, admin quarantine, Configure Conditional Access App Control with AAD CA)
4. What is Microsoft 365 Defender and how it can help
5. How to use Secure Score
   Note: Microsoft Defender for Identity is not included in this workshop – but there is Security lab for Microsoft Defender for Identity available on Microsoft docs. Instructions for the same you can find in the MD for Identity segment of the document.

COMPLIANCE IN MICROSOFT 365

1. Compliance Manager and Compliance Score
2. Information Barriers, Insider Risk Management, and Communication Compliance
3. eDiscovery and GDPR Data Subject Requests

IMPORTANT NOTE

1. **Purpose of this document is to provide learning material about Microsoft Security solutions from Microsoft 365**
2. **It is recommended to use Trial tenant and that all devices and documents aren't connected to production environment in any way. If you are using your production tenant and environment, you are doing it on your own risk! Some of configuration CAN and WILL impact live environment!**
3. **This document doesn't state official Microsoft recommended configuration steps! This document cannot be used as set of instructions how to configure production tenant; it's made for testing purposes only. Because Microsoft must respond to changing market conditions, this should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this document.**
4. **Microsoft recommended configuration/best practices can be found only on official Microsoft Docs**
5. **Microsoft and/or Microsoft employees cannot be held responsible for any issues on customer environment/s while preforming Advanced Interactive Security Workshop.**

DATA TO BE USED

Custom banned password list

balkan
adriaticsea
sarajevo
zagreb
belgrade
ljubljana
miricina

Dummy Credit card number to test:

Number: 5137442089715279
CVV: 759
Expiry: 10/2022
Name: Emmye Kavanagh

Number: 4002628901732634
CVV: 598
Expiry: 03/2022
Name: Ligia Tickle

Number: 5314508210411593
CVV: 565
Expiry: 04/2022
Name: Kerri Ovellette

Dummy SSN numbers

111-22-3333
111-11-1111
111-11-1112
111-11-1113
111-11-1114

Groups and admins sample (if you change names of groups, be sure to use those names later in configuration)

All Employees – Office 365 – AIP, WIP, app protection – pre-created when creating tenant

sg-AutoPilot – Security – for AutoPilot devices

sg-M365D – Security – Onboarding MDE devices with Intune

Finance – Office 365 – For testing

HR – Office 365 – For testing

R&D – Office 365 – For testing

Management – Office 365 – For testing

IT – Office 365 – For testing

Purchasing – Office 365 – For testing

Sales – Office 365 – For testing

Please add few of each demo users to groups. It would be the best that Office 365 groups have different users because of testing!

Administrators

Global administrator
admin@xyz.OnMicrosoft.com

IDENTITY PROTECTION

Microsoft Azure Active Directory is a comprehensive identity and access management cloud solution that combines core directory services, application access management, and advanced identity protection. Let's try it!

Self-Service Password Reset

Self-service password reset (SSPR) gives users the ability to change or reset their password, with no administrator or help desk involvement. If a user's account is locked or they forget their password, they can follow prompts to unblock themselves and get back to work.

First, we enable one registration for Self-service Password Reset and MFA

1. https://aad.portal.azure.com/ > **Azure AD > User settings > Manage user feature preview settings**
2. **Users can use the combined security information registration experience > All users**

Now we configure SSPR

1. https://aad.portal.azure.com/ > **Users > Password Reset**
2. **Properties > Self-service password reset enabled > All**
3. **Authentication methods > Number of methods required to reset > 2**
    a. **Mobile app notification**
    b. **Mobile app code**
    c. **Email**
    d. **Mobile phone**
4. **Registration > Require users to register when signing in? > Yes; Number of days > 180**

Test

Go to portal.office.com in incognito tab, type user email and password, you should be asked to register details for MFA and SSPR. Once you register log-out and close browser. Re-open it and go again to portal.office.com from incognito tab. Enter email address and click on Next. Instead of entering Password, click on Forgotten my password. Go through process of SSPR.

Conditional access (with Azure AD Identity Protection)

Conditional Access is the tool used by Azure Active Directory to bring signals together, to make decisions, and enforce organizational policies. Conditional Access is at the heart of the new identity driven control plane.

First, we need to disable Security Defaults

1. https://aad.portal.azure.com/ > Azure AD > Properties
2. Click on **Managed Security defaults** on bottom of page
3. In **Enable Security defaults** click **No**, and check **My organization is using Conditional Access** and click on **Save**

Now, we can enable Conditional Access

1. https://aad.portal.azure.com/ > **Azure AD > Security > Conditional Access**
2. **Name – Conditional Access All Apps**
3. **Users and groups > All users**
4. **Cloud apps or actions > All cloud apps**
5. **Conditions**
    a. **Sign-in risk > All**
    b. **Device platforms > Any device**

6. **Grant > Grant access**
    a. **Require multi-factor authentication**
    b. **Require device to be marked as compliant** (if Intune is part of Advanced Interactive Security Workshop – jump to enrollment of devices to Intune and configure device management before testing)

    For multiple controls > Require one of the selected controls
7. **Enable policy > On**

Test
Log-in from incognito tab from managed device – you'll be asked for MFA
Log-in from standard tab from managed device – you'll not be asked for MFA
Log-in from incognito tab from any device – you'll be asked for MFA

Try creating more granular security policies, play with Locations, devices, Apps in Conditions, and see how they are affecting user access.

We can configure Identity Protection separately, and not as part of Conditional access
Identity Protection uses the learnings Microsoft has acquired from their position in organizations with Azure AD, the consumer space with Microsoft Accounts, and in gaming with Xbox to protect your users. Microsoft analyses 6.5 trillion signals per day to identify and protect customers from threats.

Create this on your own
1. https://aad.portal.azure.com/ **> Azure AD > Security > Identity Protection**
2. **User risk policy**
    a. Users > All users
    b. Conditions > User risk > High
    c. Access > Block access
    d. Enforce Policy > On
3. **Sign-in risk policy**
    a. Users > All users
    b. Conditions > Sign-in risk > Low and above
    c. Access > Allow access > Require multi-factor authentication
    d. Enforce Policy > On

Test
On **demo windows device** install Tor browser. Go to portal.office.com and log-in with one of the users. You'll get notification that there is sign-in risk and that you need to pass MFA.

It is possible to configure that SSPR registration can be done only from trusted location – like from inside your corporate network using Conditional access. Try it!
First we need to register trusted location. Go to https://aad.portal.azure.com/ > Azure AD > Security > Named locations. Click on **New location**, enter **HQ** as name and enter IP address and click on **Create**.
Now we need to make conditional access policy. Go to https://aad.portal.azure.com/ > Azure AD > Security > Conditional access and click to create new policy and enter name.
In **Cloud apps or actions** choose **User actions** and mark **Register security information.**
Choose **Conditions > Locations > Yes > Selected locations > Any location**. Now click on **Exclude** > **Selected locations > HQ**
Under **Access Control > Grant** choose **Block access**. Click on **Select** and turn on and save policy.

Test it!

Try more conditional access policies from this list:
Conditional Access - Block legacy authentication - Azure Active Directory | Microsoft Docs
Conditional Access - Require MFA for administrators - Azure Active Directory | Microsoft Docs
User risk-based Conditional Access - Azure Active Directory | Microsoft Docs
Conditional Access - Require compliant devices - Azure Active Directory | Microsoft Docs
Conditional Access - Block access - Azure Active Directory | Microsoft Docs

Passwordless sign-in (Preview)

Multi-factor authentication (MFA) is a great way to secure your organization, but users often get frustrated with the additional security layer on top of having to remember their passwords. Passwordless authentication methods are more convenient because the password is removed and replaced with something you have; plus, something you are or something you know.

1. https://aad.portal.azure.com/ **> Azure AD > Security > Authentication methods**
2. **Authentication method policy**
    a. **Enable FIDO2 Security Key** (if you have FIDO2 Key to test)
    b. **Enable Microsoft Authenticator passwordless sign-in**
3. From incognito browser go to https://myprofile.microsoft.com/ and log-in as user you want to enable passwordless sign in. Under **Security** info go to **Update info**. **Add method > Security Key** and follow instructions.
   For Microsoft authenticator, go to user and click on ^, click on Enable phone sign-in.

Test
Security Key
Go to portal.office.com from incognito tab, instead of typing email choose Sign-in options, choose Security key,

Microsoft Authenticator
Go to portal.office.com from incognito tab, type email and click Next. Instead of password, you'll get number, and on Microsoft Authenticator you need to choose that number from 3 options.

Custom banned password list

We can configure custom list for our environment so that we can block common words associated to location, organization, famous people, etc.

1. **https://aad.portal.azure.com/ > Azure AD > Security > Authentication methods > Password protection**
2. **Enforced custom list > Yes**
3. **Custom banned password list** (copy from page 6 or enter your own)
4. **Mode -> Enforced**

Test
Go to portal.office.com in incognito tab, type user email and click on Next. In next windows don't type password but click on Forgotten my password. In process of changing try any of passwords above and try changing O with 0 (zero), 1 with I or !, S with $. Even though you changed a bit, password will not be acceptable.

Try to add more password examples and test it.

Azure AD B2B for secure guest access

Azure Active Directory (Azure AD) business-to-business (B2B) collaboration lets you securely share your company's applications and services with guest users from any other organization, while maintaining control over your own corporate data. Work safely and securely with external partners, large or small, even if they don't have Azure AD or an IT department.

1. https://aad.portal.azure.com/ > **Azure AD > Security > Conditional Access -> New Policy**
2. **Name -> Guest MFA**
3. **Users and groups > Select users and groups > All guest and external users**
4. **Cloud apps or actions > Select Apps >** search for **Office 365 SharePoint Online** and Select it
5. **Grant > Grant access**
    a. **Require multi-factor authentication**

    For multiple controls > Require all the selected controls
6. **Enable policy > On**
7. **Create**

Test

Create demo user account on Gmail or Outlook, ad that user as guest in Teams group. When user try to log-in, he will need to register and pass MFA to have access to our internal documents. Same is with SharePoint Online. To test it, share file from SharePoint Online with the same external user. To access it, user will have to pass MFA.

Single Sign-On

Single sign-on (SSO) adds security and convenience when users sign-on to applications in Azure Active Directory (Azure AD). With single sign-on, users sign in once with one account to access domain-joined devices, company resources, software as a service (SaaS) application, and web applications.

First, we need to create free Salesforce Developer account

1. Go to https://developer.salesforce.com/signup and sign up for Developer edition of Salesforce. You'll receive email to verify email and enter password.
2. In Salesforce go to **Settings > Company Settings > My Domain >** enter your unique Salesforce Developer domain and click on **Register Domain**
3. Once your domain is registered, you'll get notification
4. Refresh your page in few minutes and your environment should be ready. Copy your domain (xyz-dev-ed.my.salesforce.com) and sign in using that domain. You'll need to register mobile phone for verification.
5. Don't close environment, you'll need it

Now go to Azure AD to register app and start SSO configuration

1. Go to https://aad.portal.azure.com/ > **Azure AD > Enterprise applications > New Application >** search for **Salesforce Sandbox** and click **Add**
2. Return to **Enterprise applications** and you'll see Salesforce Sandbox. Click on it. Then go to **Single sign-on**
3. Choose **SAML**
4. Download **Federation Metadata XML** from Step 3
5. Go back to your Salesforce environment, then **Settings > Identity > Single Sign-On Settings**
6. Click on **Edit** and check **SAML Enabled** (Federated Single Sign-On Using SAML part), click **Save**
7. In **SAML Single Sign-On Settings** click **New from Metadata File**

8. **Choose File** (file that we download from SAML Signing Certificate from Azure AD) and click **Create**
9. Change **Name** to **Azure AD SSO** and **API Name** to **AzureADSSO** and click **Save**
10. Click **Download metadata**
11. Now return to https://aad.portal.azure.com/ **> Azure AD > Enterprise applications > Salesforce Sandbox > Single sign-on > SAML**
12. Click on **Upload metadata file** (top bar) and upload metadata file we downloaded from Salesforce
13. Make sure that in **Identifier (Entity ID), Reply URL (Assertion Consumer Service URL),** and **Sign on URL** contains your Salesforce domain (like https:// xyz-dev-ed.my.salesforce.com) and click **Save**
14. Go to **Users and groups** and click **Add user.** Choose one of your users and assign him a Salesforce role. Click **Assign**
15. In Salesforce admin portal go **to Settings > Company settings > My Domain >** and click on **Deploy to users**
16. Go to **Authentication Configuration**, click **Edit** and add SSO profile that you created (Azure AD SSO) and click **Save**
17. Now go to **Administrator > Users > Users > New user** and create with same **Email**. For **User License** choose **Salesforce** and for **Profile** choose the same role as in Azure AD in step 14

Now we need to test it as user – add users as described in steps 14 and 17

1. In InPrivate Browsing go to https://myapplications.microsoft.com/ and log-in as user to whom you assigned Salesforce in step 14 above (admin@xyz.onmicrosoft.com)
2. In list of apps find Salesforce Sandbox and click on it
3. You'll go to Salesforce login page. Click on Azure AD SSO

Enable automatic provisioning – please not that if you don't have additional license, this step will not work

First get token from Salesforce

1. Go to your Salesforce domain, click on avatar in top right corner and choose **Settings**
2. From the list choose **Reset My Security Token** > **Rest Security Token**
3. You'll get you token in email

Now configure in Azure AD

1. Now return to https://aad.portal.azure.com/ **> Azure AD > Enterprise applications > Salesforce Sandbox > Provisioning > Get started**
2. Change **Provisioning Mode** to **Automatic**
3. Enter **Admin Username and Admin Password** for Salesforce admin and in **Secret Token** copy token from email from previous steps. Also copy yours Salesforce tenant in **Tenant URL**. Click on **Test Connection** to see is configuration completed
4. You can also add notification email by need
5. Click **Save**
6. Go back and click **Start provisioning**

Try adding new users and test SSO. Try applying conditional access to Salesforce and test connection to it.

Privileged Identity Manager

Azure Active Directory (Azure AD) Privileged Identity Management (PIM) is a service that enables you to manage, control, and monitor access to important resources in your organization. These

resources include resources in Azure AD, Azure, and other Microsoft Online Services like Office 365 or Microsoft Intune.

1. Open https://aad.portal.azure.com/ > **All services -> Azure AD Privileged Identity Management**
2. Click on **Azure AD roles** and then on **Assign Eligibility -> Add assignment**
3. In **Select role** choose **Exchange Administrator**
4. In **Select Member(s)** choose **Bianca Pisani,** click on **Next** and then **Assign**
5. In search type Exchange Administrator and select it. You will see Bianca in Eligible roles. Click on **Role settings**
6. Check eligibility and you can edit it later on to test it. You can assign approver who will need to approve access before Bianca can become Exchange Administrator
7. Go back to https://aad.portal.azure.com/ > **All services -> Azure AD Privileged Identity Management**, and click on **Discover**
8. You can see who is Eligible for which admin role, who has active role etc.
9. Login as user added and go to **Azure AD - PIM**
10. Open EXO admin page before user Activate PIM access. You do not have access
11. Go back to Azure AD PIM, go to **My roles** and activate roles. Choose how long you want to be admin and reason why you need access and click on **Activate**
12. Access EXO admin page in few minutes to see how it works now

Try adding some other user as SharePoint Online admin and test it! Go over My audit history, add approver and go through Approve request…

Identity Governance in Azure AD

Azure Active Directory (Azure AD) Identity Governance allows you to balance your organization's need for security and employee productivity with the right processes and visibility. It provides you with capabilities to ensure that the right people have the right access to the right resources.

Entitlement management with Access Packages

Azure Active Directory (Azure AD) entitlement management is an identity governance feature that enables organizations to manage identity and access lifecycle at scale, by automating access request workflows, access assignments, reviews, and expiration.

1. Go to https://aad.portal.azure.com/ > **All Services > Identity Governance**
2. Click on **Access Packages** > **New access package**
3. Enter **Name** and **Description** and click on **Next: Resource roles**
4. In **Groups and Teams** choose Sales and click **Select**. In **Role** segment choose **Member**
5. In **Applications** choose Salesforce Sandbox and click **Select**. In **Role** segment choose **Standard User**
6. In **SharePoint sites** choose **Sales and Marketing** and click **Select**. In **Role** segment choose **Sales and Marketing Member**
7. Click on **Next: Requests**
8. In **Users who can request access** choose **For users in your directory**. Choose **All members (excluding guests)**
9. In **Require approval** toggle to **Yes**
    a. **Require requestor justification > Yes**
    b. **How many stages > 1**
    c. **First approval > Choose Specific approvers > Add approvers and** select **Admin**
    d. **Decision must be made in how many days? > 14**
    e. **Require approver justification > Yes**

f. Click on **Show advanced request settings**
    i. **If no action taken, forward to alternate approvers? > Yes**
    ii. **Click on Add alternate approvers** and choose **Adele Vance**
    iii. **Forward to alternate approver(s) after how many days? > 8**
10. In **Enable new requests and assignments** toggle to **Yes** an click on **Next: Lifecycle**
11. In **Expiration** for Access package assignments expire leave Number of days, and in Assignments expire after leave 365
12. Click on **Show advanced expiration settings** and toggle to **Yes** for **Allow users to extend access** and **Require approval to grant extension**
13. In **Require access reviews** toggle to **Yes**
    a. **Starting on** > leave todays date
    b. **Review frequency** > **Monthly**
    c. **Duration (in days)** > **14**
    d. **Reviewers > Specific reviewers**. Click on **Add reviewers** and chose **Admin**
14. Click on **Next: Review + Create**. Check your settings and click **Create**

To test, go to http://myaccess.microsoft.com/ as regular user. Click on Access package you created and click Request access. Write justification and click Submit. Go back to Admin user profile and open Outlook. You'll get notification that user wants to join. Click on approve or deny request and approve access. Check Salesforce app in Azure AD and see is user added. Check also SharePoint site and Microsoft 365 group.

Go back to access policies and to Assignments. Remove user. Check again SharePoint site and Salesforce. User is removed.

Go back to Access package and make similar package but just for guest users.

Access reviews

Azure Active Directory (Azure AD) access reviews enable organizations to efficiently manage group memberships, access to enterprise applications, and role assignments. User's access can be reviewed on a regular basis to make sure only the right people have continued access.

1. Go to https://aad.portal.azure.com/ > **All Services > Identity Governance**
2. Click on **Access reviews** > **New access review**
3. Enter **Review name** and **Description**. For **Start date** leave todays date and **Frequency** as **One-time**. **End date** put 14 days from today
4. **Users to review** eave **Members of a group** and for **Scope** choose **Everyone**
5. Next step is to choose group to review and this time it will be **Management**
6. For **Reviewers** choose **Selected users** and from **Select reviewers** choose **Admin**
7. In **Upon completion settings** configure
    a. **Auto apply results to resource > Enable**
    b. **If reviewers don't respond > Take recommendations**
8. In **Advanced settings** configure following
    a. **Require reason on approval > Enabled**
    b. **Mail notifications > Enabled**
    c. **Reminders > Enabled**
9. Click on **Start**

You as Admin will receive mail to Start review so that you can approve or deny continued access. Log in and see data. Log in as user from Management group, but leave one user not to log-in with him. Check recommendations after 14 days.

We also made review in our Access package. After first review is done (14 days) go back to access package and to Access reviews. Explore results.

Now you try making access review for a guests in some of the groups. Leave Auto apply results field on Disabled and check how you can do it manually.

Azure AD Identity Secure Score

Go to https://aad.portal.azure.com/, go to **All Services** and choose **Azure AD Identity Secure Score**. Here you'll see your Azure AD identity secure score and how you can Improve it. Go through few recommendations and configure them. You'll notice that you security score is raising.

On this link, you can find useful Azure AD Adoption Kit material that can help your organization adopting Identity security and governance.
Download Azure AD Adoption Kits from Official Microsoft Download Center

DEVICE AND APP MANAGEMENT

Microsoft Intune is a cloud-based service that focuses on mobile device management (MDM) and mobile application management (MAM). Intune enables users to be productive while keeping your organization data protected. It integrates with other services, including Microsoft 365 and Azure Active Directory (Azure AD) to control who has access, and what they have access to, and Azure Information Protection for data protection. When you use it with Microsoft 365, you can enable your workforce to be productive on all their devices, while keeping your organization's information protected. Let's try it!

Windows

Here is how we can configure enrollment for Windows devices, as well as compliance policies and configuration profiles.

1. Go to http://endpoint.microsoft.com > **Devices** > **Windows -> Windows enrollment**
2. Under **Automatic Enrolment** make sure that **MDM** and **MAM user scope** are under **All**
3. Go to **Compliance policies > Create policy** > as **Platform** choose **Windows 10 and later** and click **Create**
4. Enter **Name** and **Description (Windows compliance policy)** and click **Next.** For **Compliance settings** and **Actions for noncompliance** no changes are made, just click **Next**.
5. For **Assignments** choose **All users** and click **Next**. Click **Create**

Now we will make Configuration profile

1. Go to http://endpoint.microsoft.com > **Devices** > **Windows**
2. Go to **Configuration profiles** > click on **Create profile >** as **Platform** choose **Windows 10 and later**. Under **Profile** choose **Device restrictions** and click **Create**
3. Enter **Name** and **Description (Windows configuration profile)** and click **Next.**
4. Under **Configuration settings** configure
    a. **Control Panel and settings**
        i. **Time and Language > Block**
    b. **Start**
        i. **Unpin apps from task bar > Block**
        ii. **Most used apps > Block**
        iii. **Sleep > Block**
5. Click on **Next**. For **Assignments** choose **All users** and click Next. Again, click **Next**. Click on **Create**

Now we will make Update ring

1. Go to http://endpoint.microsoft.com > **Devices** > **Windows**
2. Go to **Windows 10 update rings** > **Create profile**
3. Enter **Name** and **Description (General update ring)** and click **Next**
4. Under **Update ring settings** change
    a. **Quality update deferral period (days) > 2**
    b. **Feature update deferral period (days) > 2**
    c. **Use deadline settings > Allow**
        i. **Deadline for quality updates > 3**
5. Click on **Next**. Assign it for **All Users**, and **Create** update ring

Now we will assign Microsoft 365 Apps to be automatically installed on device

1. Go to **Intune -> Apps -> Windows**
2. Click on **+Add**, in **App type** choose **Microsoft 365 Apps -> Windows 10**
3. **App Suite information** leave unchanged and click on **Next**

0. In **Configure App Suite** change **Update channel** to **Current Channel** and click **Next**
0. **Assignments** -> **Required**, choose **Add all users**
1. Click **Next** and then **Create**

Test
Recommended to use the device that is not connected to your production environment!
Using test device sign in via Azure AD when starting Windows or connect device to Azure AD (Start > Settings > Accounts > Access work or school > Connect > Join this device to Azure Active Directory and enter credentials. Restart device and sign in with Azure AD credentials). Microsoft 365 Apps should start installing in background. Check do you have access to block functionalities from Configuration profile. Go to Configuration profile and make changes to see how it'll affect device.

Change Compliance profiles to see how to make device noncompliant.

Try adding Microsoft Edge or any MSI application trough Intune and Apps like it's done for Microsoft 365 Apps. Apps should be installed to device in background.

Windows Autopilot

Windows Autopilot is a collection of technologies used to set up and pre-configure new devices, getting them ready for productive use. You can also use Windows Autopilot to reset, repurpose and recover devices.

First create VM and get Serial Number and Hardware Hash needed for AutoPilot

1. Enable Hyper-V on one of demo devices (instruction to enable). Create and update Windows 10 VM
2. When created, open PowerShell and run commands
   Set-ExecutionPolicy Unrestricted
   md c:\\HWID
   Set-Location c:\\HWID
   Set-ExecutionPolicy -Scope Process -ExecutionPolicy Unrestricted
   Install-Script -Name Get-WindowsAutoPilotInfo
   Get-WindowsAutoPilotInfo.ps1 -OutputFile AutoPilotHWID.csv
3. Copy CSV file to your computer (saved under c:\\HWID
4. Reset the VM back to Out-Of-Box-Experience (OOBE) - Settings > Update & Security > Recovery and click on Get started under Reset this PC. Select Remove everything and Just remove my files. Finally, click on Reset

Now we go to Intune portal and Azure AD portal to configure AutoPilot

1. In Azure AD (http://aad.portal.azure.com) and create security group, Assigned devices, named **sg-Autopilot**, which we need to add devices to which we will later assign deployment profile
2. Go to Intune (http://endpoint.microsoft.com) -> **Devices -> Windows-> Windows enrolment -> Devices**
3. Click **on Import->Select file** and upload CSV that you download from VM (it can take up to 15 min to add device) you can see that this device is Not assigned in Profile status
4. Next step is to create deployment profile; I**ntune-> Devices -> Windows-> Windows enrolment -> Deployment profiles**
5. Click on **Create Profile**. In **Basic** put name and description (AutoPilot general policy) and put Yes to convert targeted devices (next time when they go OOBE)
6. In next step (OOBE) configure
   a. **Deployment mode -> User-driven**
   b. **Join to Azure AD as -> Azure AD joined**

    c. **Apply device name template -> Yes**
        i. **Enter a name -> AISW-%SERIAL%**
7. In Next step you need to assign users - in my case sg-Autopilot
8. Review and click **Create**
9. Go back to **Azure AD-> Groups -> sg-AutoPilot -> Members** and add device you added in Intune
10. If you want that device is for specific user, go to **Intune -> Devices -> Windows-> Windows enrolment -> Devices**, mark device and click on **Assign user->** choose user and click select, click on **Save**

Test

Recommended to use the device that is not connected to your production environment!
From test device/VM grab Serial number and Hardware hash using PowerShell above. Then do steps 1-3, and then 9-10.
When VM restarts, follow instructions (Choose keyboard, language, and you can skip adding of additional keyboard). When it goes through Network, it will check that it is connected to AutoPilot and you'll get option to sign-in with your Azure AD. Choose one user and sign in. Your OS version will be updated to Enterprise, and Microsoft 365 Apps will be installed. Play with configuration profile.

Note: Endpoint Security will be covered in Microsoft Defender for Endpoint segment!

Android

As we can configure enrolment for Windows, we can do it for Android. Here is example how to enable enrolment, as well as configure basic compliance policies and configuration profiles.

Connect to Managed Google Play Store

1. Go to http://endpoint.microsoft.com > **Devices > Android > Android Enrolment > Managed Google Play**
2. Mark, **I agree** checkbox and click on **Launch Google to connect now**. Sign in or create new Google account which will be connected to organization and where you'll publish managed apps

Now make Compliance policy for Personal device with Work Profile

1. Go to http://endpoint.microsoft.com > **Devices > Android > Compliance Policies**
2. Click on **Create Policy >** as **Platform** choose **Android Enterprise** > as **Policy** type choose **Work profile**. Click **Create**
3. Enter **Name** and **Description (Android comp policy - Work profile)** and click **Next**.
4. For **System Security** configure
    a. **Require a password to unlock mobile devices > Require**
    b. **Require password type > At least numeric**
    c. **Minimum password length > 4**
    d. **Block apps from unknown sources > Block**
5. Click **Next**. We will leave actions for noncompliance unchanged and click **Next**
6. For assignments choose group **All users** and click **Next**
7. Click **Create**

Compliance Policy for Fully managed corporate device

1. Go to http://endpoint.microsoft.com **> Devices > Android > Compliance Policies**
2. Click on **Create Policy** > as **Platform** choose **Android Enterprise** > as **Policy** type choose **Device Owner**. Click **Create**
3. Enter **Name** and **Description (Android comp policy - Device owner)** and click **Next**.

4. For **System Security** configure
    a. **Require a password to unlock mobile devices > Require**
    b. **Require password type > Numeric**
    c. **Minimum password length > 4**
5. Click **Next**. We will leave actions for noncompliance unchanged and click **Next**
6. For assignments choose group **All users** and click **Next**
7. Click **Create**

Next, we need to make Configuration Profiles for Work

1. Go to http://endpoint.microsoft.com > **Devices > Android > Configuration profiles**
2. Click on **Create profile** > as **Platform** choose **Android Enterprise** > as **Profile** choose **Work Profile – Device restrictions**
3. Enter **Name** and **Description (Android Conf Profile - Work Profile)** and click **Next**.
4. Under **Work profile settings** choose:
    a. **Copy and paste between work and personal profiles > Block**
    b. **Work profile notifications while device locked > Block**
    c. **Screen capture > Block**
8. Click **Next**. For assignments choose group **All users** and click **Next**
9. Click **Create**

Next, we need to make Configuration Profiles for Device owner

1. Go to http://endpoint.microsoft.com **> Devices > Android > Configuration profiles**
2. Click on **Create profile** > as **Platform** choose **Android Enterprise** > as **Profile** choose **Device owner – Device restrictions**
3. Enter **Name** and **Description (Android Conf Profile - Device owner)** and click **Next**.
4. Under **General** choose:
    a. **Screen capture > Block**
    b. **Camera > Block**
    c. **Status bar > Block**
    d. **USB file transfer > Block**
5. Click **Next**. For assignments choose group **All users** and click **Next**
6. Click **Create**

Now we will assign few apps for devices

1. Go to http://endpoint.microsoft.com **> Apps > Android**
2. Click **on Add > Managed Google Play app** and click on **Select**
3. Search for **Word** and select it. Click on **Approve** > check permissions that app will have and click on **Approve**. Choose what will happen if permissions are changed and click **Done**. Choose **Select** and then on **Sync** (which is on top left side)
4. You'll see Word as application. Click on it
5. Choose then **Properties** > **Assignments** > **Edit**
6. For required choose **Add all users**. Choose **Review+Save** and then **Save**.

Test

Recommended to use the device that is not connected to your production environment!
Enroll your device as Fully managed following these instructions - https://docs.microsoft.com/en-us/mem/intune/user-help/enroll-device-android-company-portal. Check how it looks. Make some changes into Device owner configuration profile and see how it affects device. Try adding more apps. Try to delete apps. When assigning apps make them Available for enrolled devices and see changes.

Enroll your device with Work profile following these instructions - https://docs.microsoft.com/en-us/mem/intune/user-help/enroll-device-android-work-profile. Check how it looks. Make some changes into Work profile configuration profile and see how it affects device. Try adding more apps. Try to delete apps from Work Profile. When assigning apps make them Available for enrolled devices and see changes.

Make changes in Compliance policies and make your devices noncompliance. See what will happen on Device. Make conditional policy and ask that device must be marked as compliant. Try to access corporate data when device is noncompliance.

Try adding more applications, adding as available for download etc.

App protection policies

App protection policies (APP) are rules that ensure an organization's data remains safe or contained in a managed app. A policy can be a rule that is enforced when the user attempts to access or move "corporate" data, or a set of actions that are prohibited or monitored when the user is inside the app.

First, we will configure Windows Information Protection

1. Go to http://endpoint.microsoft.com > **Apps > App protection policies**
2. Click on **Create policy > Windows 10**
3. Enter **Name** and **Description (Windows Information Protection)**, for **Enrollment state** choose **With enrollment**
4. In **Targeted apps** click on **+Add** and choose **Office-365-ProPlus, Microsoft OneDrive** and **Microsoft Team.** Click **OK** then **Next**
5. For **Windows Information Protection mode** Choose **Block** and then click on **Next**
6. **Advanced settings** leave unchanged and click **Next**.
7. Select **All Employees** group and click **Next** and then **Create**

We can create the same policy and just changed enrollment type to make it also for devices without enrollment

Now we will create it for Android devices

1. Go to http://endpoint.microsoft.com > **Apps > App protection policies**
2. Click on **Create policy > Android**
3. Enter **Name** and **Description (Android App protection policy)**
4. Leave **Target to apps on all devices types** (you can change it only for unmanaged devices or device under Android Enterprise)
5. Click on **+Select public apps** and add Word, Excel, Outlook, OneDrive, and Teams. Click on **Select** and on **Next**
6. In **Data protection** change following
    a. **Backup org data to Android backup services > Block**
    b. **Send org data to other apps > Policy managed apps**
    c. **Save copies of org data > Block**
        i. **Allow users to save copies to select services > OneDrive for Business**
    d. **Restrict cut, copy, and paste between other apps > Policy managed apps with paste in**
7. Click on **Next**. In **Access requirements** and **Conditional launch** make no changes and click on **Next**
8. Select **All Employees** group and click **Next** and then **Create**

Test

Recommended to use the device that is not connected to your production environment!
On test devices test above policies. Try to copy data from policy unmanaged app to managed app and vice versa. Try to save attachment to storage of Android devices or any other cloud provider. Change above policies and see how it will affect access.

MICROSOFT INFORMATION PROTECTION

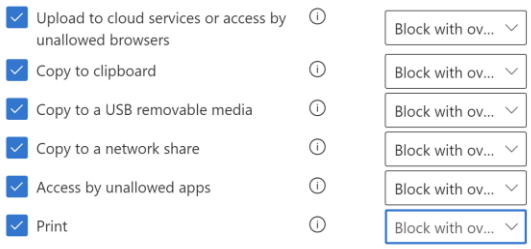
Microsoft Information Protection helps you to discover, classify, and protect sensitive information wherever it lives or travels. MIP services are:

1. Data Loss Prevention
2. Sensitivity labels (Azure Information Protection)
3. Microsoft Cloud App Security – covered in Microsoft 365 Defender segment
4. App Protection Policies – covered in Device & App Management segment

DLP (with Endpoint DLP)

To comply with business standards and industry regulations, organizations must protect sensitive information and prevent its inadvertent disclosure. Sensitive information can include financial data or personally identifiable information (PII) such as credit card numbers, social security numbers, or health records. With a data loss prevention (DLP) policy in the Office 365 Security & Compliance Center, you can identify, monitor, and automatically protect sensitive information across Office 365. Endpoint data loss prevention (Endpoint DLP) extends the activity monitoring and protection capabilities of DLP to sensitive items that are on Windows 10 devices. Let's try it!

1. Go to https://compliance.microsoft.com/, on left menu click on **Show all** and choose **Data loss prevention**, then click on **Create Policy.**
2. In Choose the information to protect, select **Financial**, search for **PCI Data Security Standard (PCI DSS)**, click on **Next**
3. For **Name your policy** leave pre-populated and click on **Next**
4. For **Choose locations** leave selected. You can click on **Let me choose specific location** and configure more granular DLP for specific email accounts, SharePoint sites etc.
5. In **Define policy settings** leave unchanged and click **Next**. Additionally you can choose **Create or customize advanced DLP rules** where you can choose what will happen when there is Low quantity detected (like 2 credit card numbers) and what when more detections are seen.
6. **Policy settings** change **Detect when this content is shared:** to **only with people inside my organization**. Click **Next**
7. In next step, for **Detect when content that's being shared contains:** change to 1, and click **Next**
8. In **Customize access and override settings** check **Restrict access or encrypt the content in Microsoft 365 locations**. Choose **Everyone. Only the content owner, the last modifier and the site admin will continue to have access**. Leave option to override checked.
9. In same window check **Audit or restrict activities on Windows devices** and put them all in **Block with override** mode and click on **Next**



10. Choose **Yes, turn it on right away** and click **Next**
11. Review policy and click **Submit**

When you are back to Data loss prevention site, choose **Endpoint DLP settings**

1. In **Unallowed apps** choose Notepad++ (notepad++.exe)

2. Check **Unallowed browsers** for the list of blocked browsers to share sensitive info, where you can add additional browsers if needed
3. You can also add service domains to block or allow (block – it'll block only those domains for upload; allow – it'll only allow upload to these domains – all other domains are blocked)

We also need to turn on onboard of devices:

1. Go to https://compliance.microsoft.com/ and click on Settings
2. Choose **Device onboarding (preview)** and click on **Turn on device onboarding**

You can Onboard by using script or Intune policy under **Onboarding** or by onboarding machine to Microsoft Defender for Endpoint (instructions in MD for Endpoint segment)

Test

Go to teams.microsoft.com, and share Credit Card info via chat with anybody from this tenant – it'll be blocked. Try the same via email. Dummy credit card numbers can be found on page 6.

Try testing the same with email and SharePoint Online.

Now try to upload document with these domain to Chrome or Notepad++ - it should be blocked. Try to Edge Chromium – it should work.

Now go and change some of the settings – see how it will affect your policy.

Retention policies

For most organizations, the volume and complexity of their data is increasing daily—email, documents, instant messages, and more. Effectively managing or governing this information is important because you need to:

- Comply proactively with industry regulations and internal policies that require you to retain content for a minimum period of time—for example, the Sarbanes-Oxley Act might require you to retain certain types of content for seven years.
- Reduce your risk in the event of litigation or a security breach by permanently deleting old content that you're no longer required to keep.
- Help your organization to share knowledge effectively and be more agile by ensuring that your users work only with content that's current and relevant to them.

A retention policy can help you achieve all off these goals. Let's try it!

1. Go to https://compliance.microsoft.com/, on left menu click on **Show all** and choose **Information governance > Retention**, then click on **New retention policy.**
2. As **Name** enter **7-year retention**
3. For **Locations** turn on **Exchange emails, SharePoint sites, OneDrive accounts, Microsoft 365 Groups** and click on **Next** (as a test later we will make retention for Teams chat and channel messages)
4. In **Retention settings** leave to **Retain items for a specific period -> 7 years -> When items were last modified** and for **at the end of the retention period -> Do nothing**
5. Click on **Next** and then on **Submit**

Test

Go to SharePoint Online site. Try deleting files from it. Go to recycle bin in SharePoint online and delete it from there. See what's happening. Do the same with emails – delete email, delete from deleted, and you'll have all emails in Recovery for 7 years. After testing, Disable policy so that we can test manual ones.

We can apply retention policies on emails, sites, or create multiple for specific sites etc., but we can also create retention labels and policies that you can publish to users so that they can use it, and with advance compliance license, you can even turn on automatic labeling per keywords/sensitive info types. Let's see how this can be done!

1. Go to https://compliance.microsoft.com/, on left menu click on **Show all** and choose **Information governance**
2. Under **Labels** click on **+ Create a label**
3. Enter **Name** and **Description** for users and admins and click on **Next**
4. In **Retention settings** leave to **Retain items for a specific period -> 7 years -> When items were last modified** and for **at the end of the retention period -> Do nothing**
5. Click on **Next** and then on **Create label**

Now we need to publish the label.

1. Click on **Label policies** and then on **Publish labels**
2. Click on **Choose labels to publish** and choose label we created above and click on **Next**
3. Leave **All locations** and click on **Next**
4. Enter the **Name** and **Description** of the policy and click on **Next**
5. Review your settings and click on **Submit**

Now go to SharePoint Online or OneDrive for Business and create document. Apply retention on it and try to delete it – see the message. Here is instruction how to manually apply retention label - Create retention labels and apply them in apps to retain or delete content - Microsoft 365 Compliance | Microsoft Docs

Once when you have created retention label that users can manually apply, and you have advance compliance licensing, you can configure auto-labeling.

1. Go to https://compliance.microsoft.com/, on left menu click on **Show all** and choose **Information governance**
2. Under **Labels** click on label you created above
3. Now in the menu above, choose **Auto-apply a label**
4. Enter **Name** and **Description** and click on **Next**
5. Leave selection on **Apply label to content that contains sensitive info** and click on **Next**
6. In Categories select **Financial**, search for **PCI Data Security Standard (PCI DSS)**, click on **Next**
7. Now we can do fine tuning of a policy and add some other Sensitive info that can be detected. In this case we will only change **Instance count** from **1 to** 9 to **1 to** Any and click on **Next**
8. For **Choose Locations** leave unchanged, and click on **Next**
9. Now you can replace a label if you want or just click on **Next** if it's OK
10. Review your configuration and click on **Submit**

Use same Credit Card numbers to test policy. Any document/email containing PCI DSS will get retention policy of 7 years. Test it with SharePoint document that contains Credit Card number – after saving it, try to delete it!

Please not that it can take 24-48 hours till policies starts applying once created!

Sensitivity labels

Sensitivity labels are a cloud-based solution that helps an organization to classify and optionally, protect its documents and emails by applying labels. Labels can be applied automatically by administrators who define rules and conditions, manually by users, or a combination where users are given recommendations. Let's try it!

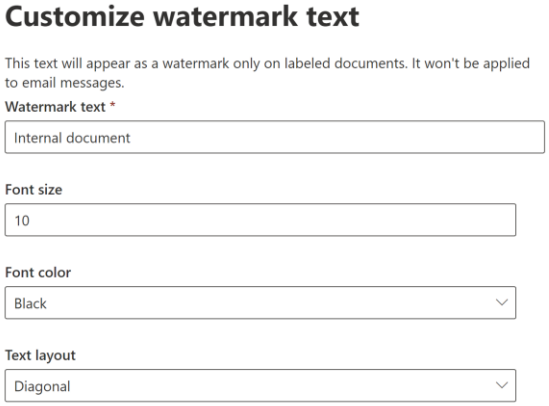
First, we need to enable Sensitivity labels for SharePoint Online and Teams
For Office files in SharePoint Online

1. Open PowerShell and run following commands
   Set-ExecutionPolicy Unrestricted
   Import-Module ExchangeOnlineManagement
   Connect-IPPSSession -UserPrincipalName admin@xyz.com
   Execute-AzureAdLabelSync

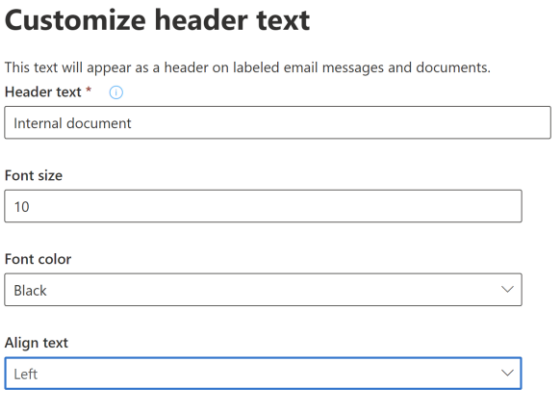
Sensitivity labels are enabled for SharePoint Online sites and Microsoft Teams.

Now we will configure Sensitivity labels:

1. Go to https://compliance.microsoft.com/, click on **Show all > Information Protection**. You can notice that all labels created in Azure Information Protection are synced. Click on **Create a label**
2. Enter a name (**Internal**) and Description (**Document for internal purposes**) and click on **Next**
3. In **Define the scope for this label** mark **Files & emails** and **Groups & sites** and click on **Next**
4. In **Choose protection settings for files and emails** mark **Encrypt files and emails** and **Mark the content of files** and click on **Next**
5.
6. In **Encryption** choose **Configure encryption settings**:
   a. **Assign permissions now or let users decide? -> Assign permissions now**
   b. **User access to content expires -> Never**
   c. **Allow offline access -> Never**
   d. Click on **Assign Permissions** and choose **+Add all users and groups in your organization**
   e. Click on **Next**
7. Enable **Content marking**, and check **Add a watermark** and click on **Customize text**



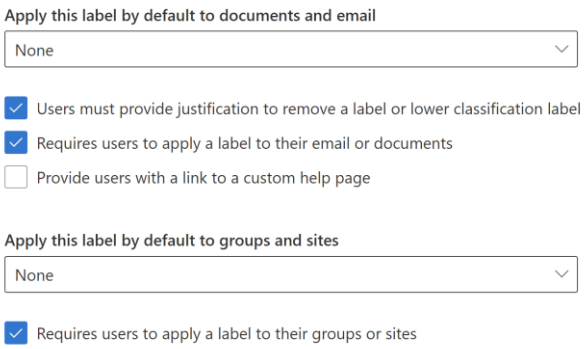
8. Click **Save,** check **Add a header** and click on **Customize text**



9. Click **Save**. You can do the same for footer and then click **Next**
10. Turn on **Auto-labeling for files and emails**. Under **Detect content that matches these conditions** click on **+Add condition** and choose **Content contains**. Click on **Add** and choose **Sensitive info types**. Find **Credit Card Number**, mark it and choose **Add**
11. Under **When content matches these conditions?** Make sure that it's **Automatically apply the label**, and under **Display this message to users when the label is applied** put "**Automatically labelled document – Credit Card info found"** and click on **Next**
12. In **Define protection settings for groups and sites** check **Privacy and external user access settings** and **Device access and external sharing settings** and click on **Next**
13. In **Define privacy and external user access settings** choose **Private** and don't mark **External user access** and click on **Next**
14. In **Define external sharing and device access settings** choose **Block access** and click on **Next**
15. Review your settings and click on **Create label**

After creating labels, it's time to create a policy

1. Go to https://compliance.microsoft.com/, click on **Show all > Information Protection**. Click on **Label policies > Publish labels**
2. Choose sensitivity labels and click on **Next**.
3. Leave all users or choose specific groups or users to apply this label to. Click on **Next**
4. Policy settings should look like this



5. Enter a name (**General**) and Description
6. Review policy and click on **Submit**

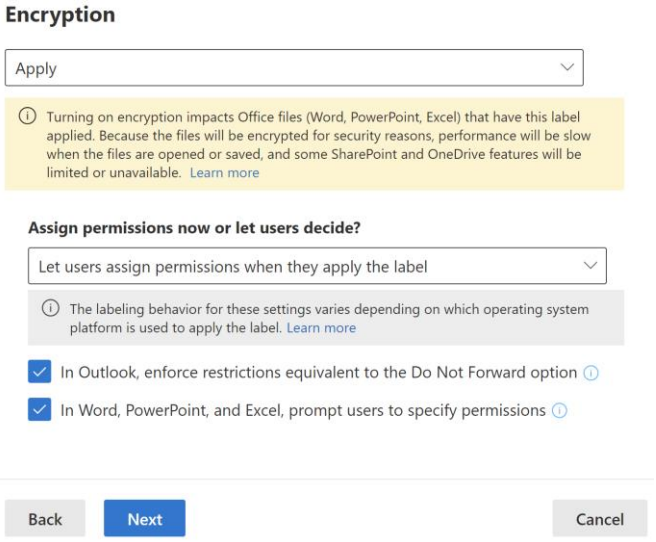
Test

On a device that is not connected to any production environment (test device) install Microsoft 365 Apps (Office 365 ProPlus). Sensitivity labels comes integrated into product itself- we only do not have Information bar for choosing sensitivity. Option to choose is on left side of home called Sensitivity. For Office 2016 Professional or so you need to install Azure Information Protection Unified Labeling client or for Microsoft 365 Apps so that we have Information bar.

Use dummy Credit Card numbers from page 6 and copy to word or excel. When trying to save document, it'll automatically be marked as Confidential.

Try sending protected and unprotected email and document inside of tenant. Together we will test with another trial tenant to see how it behaves outside of your organization.

Additionally, test Custom permissions, add a sub-label
Custom permission can be configured the same as standard label, but in Encryption part choose following:



To create sub label, go to https://compliance.microsoft.com/, click on **Show all > Information Protection** and next to the label you want to create sub label click on 3 dots and choose +Add sub label

Go to portal.office.com and open Word. Test sensitivity labels. Got to one SharePoint site and test labels. Upload one document protected with Azure Information Protection. You can notice that document protected with AIP you must open locally with desktop app, while those with Sensitivity labels you can open directly in SharePoint Online.

Go to teams.microsoft.com. Start creating new team. You'll have option to choose label for team and if you choose Internal, you'll be able to create only Private team, and you'll not be able to add any guests, even if they are part of your Azure AD as Guests.

Here is the link for end user training for Sensitivity Labels in Microsoft 365

End User Training for Sensitivity Labels in M365 – How to Accelerate Your Adoption - Microsoft Tech Community

Data Classification reporting

As a Microsoft 365 administrator or compliance administrator, you can evaluate and then tag content in your organization in order to control where it goes, protect it no matter where it is and to ensure that it is preserved and deleted according to your organization's needs. You do this through the application of sensitivity labels, retention labels, and sensitive information type classification. There are various ways to do the discovery, evaluation and tagging, but the end result is that you may have very large number of documents and emails that are tagged and classified with one or both of these labels. After you apply your retention labels and sensitivity labels, you'll want to see how the labels are being used across your tenant and what is being done with those items. The data classification page provides visibility into that body of content,

1. Go to https://compliance.microsoft.com **-> Data classification -> Overview**
   Here we ca get snapshots of how sensitive info and labels are being used across your organization's locations (top sensitive info types, top sensitivity labels, top activities detected, locations where labels are applied, etc.)

2. Click on **Sensitive info types** in the tab
3. Here we can see all different sensitive info types that you can use when creating label policies and policies in MCAS which we can use to detect specific data as ID number, credit card number, etc. If we have specific need for detection, we can create our own Sensitive info type by clicking on **Create info type**
   a. We will enter the name of sensitive type and click on **Next**
   b. In **Patterns** and click on **Create pattern**
      i. For **Confidence level** choose **Medium confidence**
      ii. In **Primary element** click on **Add primary element** and choose **Keyword list**
      iii. In **ID** put **Confidential** and in **Case insensitive** put **confidential**
      iv. Click on **Done** and on **Create**
   c. Click on Next and for confidence level choose **Medium confidence level** and click on **Next** and then on **Submit**
4. Now we can use this Sensitive type for auto labeling, retention, etc.

5. Go back to https://compliance.microsoft.com **-> Data classification** and choose **Content explorer**. Here we can explore emails and docs that have sensitive information or have labels applied. Currently it shows data only from Exchange Online, SharePoint Online, and OneDrive for Business.

6. In **Activity explorer** tab we can see information like what labels are applied, changed, files modified, etc. You can get exact location where file is located, if label is downgraded, etc. Go through data. DO some label changes and see how data is changed in Activity Explorer.

MICROSOFT 365 DEFENDER

Microsoft 365 Defender is a unified pre- and post-breach enterprise defense suite that natively coordinates detection, prevention, investigation, and response across endpoints, identities, email, and applications to provide integrated protection against sophisticated attacks. Microsoft 365 Defender services are:

1. Microsoft Defender for Office 365
2. Microsoft Defender for Endpoint
3. Microsoft Cloud App Security
4. Microsoft Defender for Identity – because for Microsoft Defender for Identity is recommended to be installed on production DC to analyze user behavior and detect anomalies, it's not included in Advanced Interactive Security Workshop. But I included MD for Identity security lab instructions if you want to deploy it in your test environment
5. Azure AD Identity Protection (we covered already in Identity part of document)

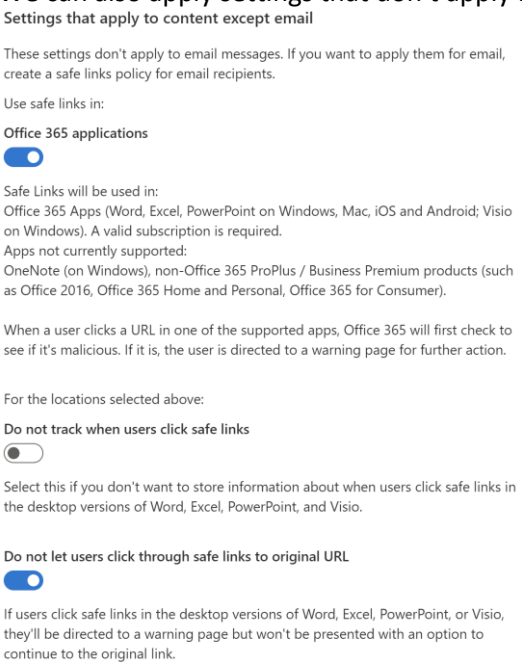
MICROSOFT DEFENDER FOR OFFICE 365

Microsoft Defender for Office 365 safeguards your organization against malicious threats posed by email messages, links (URLs) and collaboration tools. Let's try it!

Safe Links

Microsoft Defender for Office 365 Safe Links help protect your organization by providing time-of-click verification of web addresses (URLs) in email messages and Office documents.

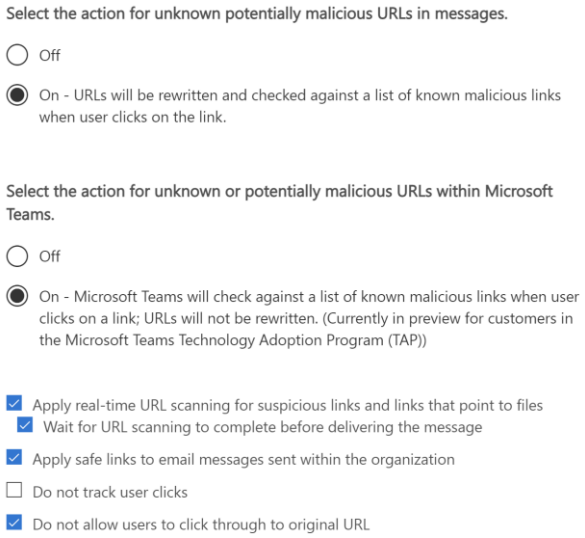
1. Open https://protection.office.com and click on **Threat Management-> Policy -> ATP Safe Links**
2. Click on **Global settings** (gear icon)
3. To block specific web pages on our email messages and in Office 365 Apps and Office for iOS and Android files, we can fill **Block the following URLs**. Note – it's one URL per line, you can use asterisks(*) as wildcard
4. We can also apply settings that don't apply for emails:



5. Click on **Save**

Now we will create new Safe Links policy

1. Click on **Create (+)**
2. Enter **Name** and **Description** (General)
3. Apply following settings and click on **Next**



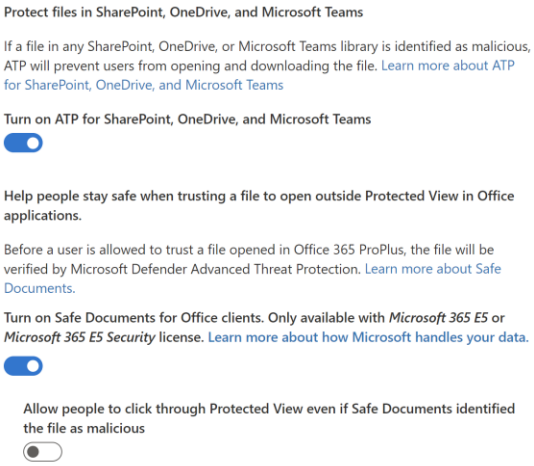
(Note: if you have some site from which you don't want to re-write URLs, enter those sites in the **Do not rewrite the following URLs**)

4. In **Applied to** click on **Add conditions** and choose **Applied if… The recipient is a member of** and search and choose group **Finance** and click on **Next**
5. Review your settings and click on **Finish**

Safe Attachments

The ATP Safe Attachments feature checks to see if email attachments are malicious, and then takes action to protect your organization.

1. Open http://protection.office.com and click on **Threat Management-> Policy -> ATP Safe Attachments**
2. Click on **Global settings** (gear icon)
3. Here we can configure protection for your organization from malicious content in email attachments and files in SharePoint, OneDrive, and Microsoft Teams. Configure as below and click on **Save**



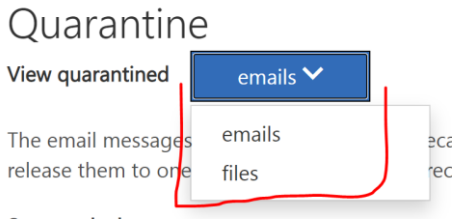
Now we will configure policy for emails:

1. Click on **Create(+)**

2. Enter **Name** and **Description** (General)
3. For **Safe attachments unknown malware response** choose **Replace**
4. In **Redirect attachment on detection**, mark **Enable redirect** and put admin email address
5. Mark **Apply the above selection if malware scanning for attachments times out or error occurs.** And click on **Next**
6. In **Applied to** click on **Add conditions** and choose **Applied if… The recipient is a member of** and search and choose group **Finance** and click on **Next**
7. Review your settings and click on **Finish**

To test Safe Links and Safe Attachments we would need some malicious content that I cannot share. Try testing using EICAR data. There are also free tools to send "simulated malicious email" if you are willing to test it in that way on your own risk – especially if you are using production environment in any way! It is recommended to use partners to do pen testing in safe manner!
If you have enabled protection for Teams, SharePoint Online, and OneDrive for Business, you can test by uploading EICAR test file to one of these systems.

Please note that for files and emails that are quarantined, you can access by going to http://protection.office.com and click on **Threat Management-> Review -> Quarantine**. You can change between emails (Exchange Online) and files (Teams, SharePoint Online and OneDrive for Business).



Configuration Analyzer

Configuration analyzer in the Security & Compliance center provides a central location to find and fix security policies where the settings are below the Standard protection and Strict protection profile settings.

1. Open http://protection.office.com and click on **Threat Management-> Policy -> Configuration analyzer**
2. You will be able to see standard recommendation changes. Since we didn't configure any rules for anti-spam, anti-phishing, and anti-malware – we can now easily click on each recommendation and click on **Adopt** which will automatically change our configuration in regards to Standard protection profile
3. By click on **View strict recommendations** our recommendation will refresh and we will be able to see all recommendations but not compared to Strict protection profile. Change of configuration is still the same, just click on **Adopt** and it will automatically be changed
4. In **Configuration drift analysis and history** we can see changes that happened in some time period. By click on the **Filter** you can change time span as well as are changes made in Standard or Strict profile.

Test

Go over config and try to balance between Recommended settings for EOP and Microsoft Defender for Office 365 - https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/recommended-settings-for-eop-and-office365-atp?view=o365-worldwide
Test your new settings. Go through anti-spam, anti-phishing, and anti-malware and change settings based on recommended configuration.

Preset security policy

A preset security policy is a compilation of settings for these security policies: anti-spam, anti-malware, anti-phishing, Safe Links, and Safe Attachments. When multiple security policies are applied a user, the Strict policy overrides the Standard policy and any custom policies. The Standard policy overrides custom policies.

1. Open http://protection.office.com and click on **Threat Management-> Policy -> Preset security policies**
2. Under **Standard protection** click on **Edit**
3. Click on **Next**
4. Under **EOP protections apply to** click on **Add condition,** choose **The recipients are members of** and then choose group **HR**
5. Under **Defender for Office 365 protections apply to choose** click on **Add condition,** choose **The recipients are members of** and then choose group **HR**
6. Click on **Next** and then on **Confirm**

Do the same for Strict protection and choose group **Purchasing**.
Now test sending same phishing emails to your custom user, user with Standard and user with Strict protection policy enabled. Note differences.

Attack simulator (public preview)

Attack simulator training through Microsoft Defender for Office 365 lets you run benign cyber-attack simulations on your organization to test your security policies and practices, as well as train the employees of your organization to increase their awareness and decrease their susceptibility to attacks. The following walks you through simulating a phishing attack using attack simulator training.

1. Go to https://security.microsoft.com and click on **Attack simulation training**
2. Click on **Simulations** -> **Launch a simulation**
3. In **Select Technique** choose **Credential Harvesting** and click on **Next**
4. Enter Simulation Name and Description (Credential Harvesting testing) and click on **Next**
5. In **Select Payload** choose **COVID 19 payroll adjustment** and click on **Next**
6. Choose few users from the list on page 7 and click on **Next**
7. In **Assign Training** under **Preferences** leave unchanged, but under **Due Date** change to **7 days after Simulation ends** and click on **Next**
8. In **Training landing page** leave unchanged. Click on **Preview** to see how user will see the page after the Simulation is successful. Click on **Next**
9. Leave lunch details unchanged (if you want, you can specify particular time when to do Simulation) click on **Next** and then on **Submit**

With this we will start simulation. Log-in as few users and with some of them go through process and provide credentials – check landing page and training instructions (with 2 users don't open email yet). Check phishing learning material that is assigned.

Go back to https://security.microsoft.com and click on **Attack simulation training**. Check statistics under **Overview**.

User tags (public preview)

User tags are identifiers for specific groups of users in Microsoft Defender for Office 365. There are two types of user tags:

- System tags: Currently, Priority accounts is the only type of system tag.

- Custom tags: You create these user tags yourself.

1. Open http://protection.office.com and click on **Threat Management-> User tags**
2. Choose **Priority accounts** and click on **Edit tag**
3. Click on **Add users** and add **Finance** group
4. Click on **Next** and then on **Submit**

Create custom tag (IT) and add group HR in it. When we go through Explorer we will be able to see Tags.

User Submissions

In Microsoft 365 organizations with Exchange Online mailboxes, you can specify a mailbox to receive messages that users report as malicious or not malicious. When users submit messages using the various reporting options, you can use this mailbox to intercept messages (send to the custom mailbox only) or receive copies of messages (send to the custom mailbox and Microsoft).

First we need to enable users to have possibilities to submit suspicions emails.

1. Open http://protection.office.com and click on **Threat Management-> Policy -> User submissions**
2. Mark **Enable the Report Message feature for Outlook** -> **Microsoft** and click on **Confirm**

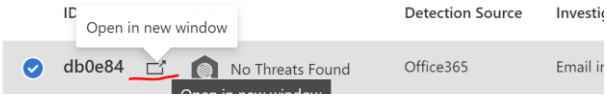
You can also configure end-user confirmation message when submitting email. It's important to have this option for users because they are our last line of defense, and you can configure Automated Investigations to automatically check message after submission.

Log in as those users that you didn't went through in Attack Simulator and report those emails as junk. You'll be able to see those emails in the Explorer and in the same time there will be Automated Investigation in behind.

Investigations

Microsoft Defender for Office 365 includes powerful automated investigation and response (AIR) capabilities that can save your security operations team time and effort. As alerts are triggered, it's up to your security operations team to review, prioritize, and respond to those alerts. AIR enables your security operations team to operate more efficiently and effectively. AIR capabilities include automated investigation processes in response to well-known threats that exist today.

After we have done user submission, we have Automated Investigation in the background. Go to http://protection.office.com and click on **Threat Management-> Investigations** where we will see all ongoing automated investigations in last 24 hours. When our automated investigation is over, click on investigation and click on **Open new Windows**



We will see all info in regards to investigation including graph, alerts, emails, users, machines, entities, logs, and actions. Once when investigation is done in **Actions** part we will be able to see what is recommended action and we will have option to **Approve** it or **Reject**. Investigate all tabs to see info you are receiving.

You can start automated investigation from Explorer as it is described below.

Explorer

With Explorer (or Real-time detections), you have a powerful report that enables your Security Operations team to investigate and respond to threats effectively and efficiently.

1. Open http://protection.office.com and click on **Threat Management-> Explorer**
2. In **View** choose arrow down (next to **Malware**) and choose **All emails**
3. You'll be able to see data for last 7 days with Trial and 30 days with Paid license
4. Now we can do filtering in search for more important data
5. Click on **Advanced filter** then on **Add a condition** and choose **Tags**. Enter **Priority accounts** and click on **Query** and now we will see all emails with users that have Priority account
6. Click on **Add a condition** again and choose **Delivery action** and mark **Delivered to junk** and click on **Query**

Go through results, now we can see all emails that are delivered to junk for Priority accounts so that we can check is there any false positives, especially for Priority accounts.

We will send few different emails to accounts and we will go and check additional filtering capabilities.

1. When you had done query above, you should have some result. When we scroll to results, we can see emails, URLs, top targeted users, email origin, etc.
2. Mark one email, click on **Action** and now we can move email to different folder or to delete email from users email account. We can also start automated investigation about sender, email, etc, as well as mark email as clean, phishing, malware, etc.
3. If we want see more details about email, check headers, email timelines, similar events,… we can do that by click on subject of the email
4. We can also investigate user by clicking on user in that email, and we can see related alerts from the user and decide is this something that we need to pay more attention to.

If there are no emails, we can generate some together.

MICROSOFT DEFENDER FOR ENDPOINT

Microsoft Defender for Endpoint is an enterprise endpoint security platform designed to help enterprise networks prevent, detect, investigate, and respond to advanced threats. Let's try it!

First, we will enable MD for Endpoint

1. Go to https://securitycenter.windows.com/, and follow few steps to enable Microsoft Defender for Endpoint (where data will be stored, what is retention period,..). Note: once you choose location where data is stored for MD for Endpoint it cannot be changed!

Enable Advance features and basic configuration

To have all integrations (MCAS, Microsoft Defender for Office 365, Intune, AIP…) we need to enable advance features. We also need to configure Device groups and remediation level, as well as web content filtering

1. Go to https://securitycenter.windows.com/, **Settings > Advance features** – make sure that all of them are turned on

2. Under **Settings > Device groups** make device group called **Pilot devices**, **Automation level > Full – remediate threats automatically**, **Members > Tag – Equals – Pilot**, click on **Done**
3. Click on **Apply Changes**
   (Please note that when you add devices, you need to go to device (Device inventory and click on device), then click on **Manage tags** and enter **Pilot**)

Onboarding using Intune (only if customer has dedicated testing device)

We need to enable connection of Windows devices with Microsoft Defender for Endpoint

1. Go to https://endpoint.microsoft.com
2. Select **Endpoint security > Microsoft Defender ATP,**
3. Under **MDM Compliance Policy Settings**, depending on your organization's needs:
   a. Set **Connect Windows devices version 10.0.15063 and above to Microsoft Defender ATP** to **On** and/or
   b. Set **Connect Android devices of version 6.0.0 and above to Microsoft Defender ATP** to **On**.
4. Select **Save.**

Now we need to create configuration profile for devices

1. Go to https://endpoint.microsoft.com
2. Select **Devices > Configuration profiles > Create profile**.
3. Enter a **Name** and **Description**.
4. For **Platform**, select **Windows 10 and later**
5. For **Profile type**, select **Microsoft Defender ATP (Windows 10 Desktop)**
6. As name put **Microsoft Defender ATP (Windows 10 Desktop)**
7. Configure the settings:
   a. **Sample sharing for all files: Enable**
   b. **Expedite telemetry reporting frequency: Enable**
8. Select **Next**, choose group **sg-M365D**(if want org level choose All Users)
9. Select **Next -> Next -> Create**

To test use test device and login to device using Azure AD (first add as Work or School account – join to Azure AD) account from sg-M365Dgroup. Device will be automatically joined to MD for Endpoint and you'll see device in few minutes under Device inventory.

MD for Endpoint and Intune Endpoint security

You can use Endpoint security in Intune to configure device security without the overhead of navigating the larger body and range of settings found in device configuration profiles and security baselines.

Antivirus

The Intune Endpoint security Antivirus policies can help security admins focus on managing the discrete group of antivirus settings for managed devices. To use Antivirus policy, integrate Intune with Microsoft Defender for Endpoint as a Mobile Threat Defense solution.

1. Go to https://endpoint.microsoft.com/ > **Endpoint security** > **Antivirus > Create Policy**
2. Choose **Windows 10 and later** in **Platform**, and choose **Microsoft Defender Antivirus** as **Profile.** Click on **Create**
3. Enter **Name(Win AV policy)** and **Description(Windows Antivirus policy)** and click on **Next**
4. In **Configuration settings** configure following
   a. In **Real-time protection** turn all to **Yes**
   b. In **User experience** change to **Yes** for **Allow user access to Microsoft Defender app**

5. Click on **Next** and again on **Next**
6. In **Assignment** assign to **sg-M365D** group and click on **Next**
7. On **Review + create** review config and click on **Create**

Do similar for MacOS. Change settings in Configuration settings – see what options you have with Remediation, Scan, Updates, Cloud protection...

Firewall

Use the endpoint security Firewall policy in Intune to configure a devices built-in firewall for devices that run macOS and Windows 10.

1. Go to https://endpoint.microsoft.com/ > **Endpoint security** > **Firewall > Create Policy**
2. Choose **Windows 10 and later** in **Platform**, and choose **Microsoft Defender Firewall** as **Profile.** Click on **Create**
3. Enter **Name(Win FW policy)** and **Description(Windows Firewall policy)** and click on **Next**
4. In **Configuration settings** configure following
    a. **Disable stateful File Transfer Protocol (FTP) > Yes**
    b. **Turn on Microsoft Defender Firewall for domain networks > Yes**
    c. **Turn on Microsoft Defender Firewall for private networks > Yes**
    d. **Turn on Microsoft Defender Firewall for public networks > Yes**
5. Click on **Next** and again on **Next**
6. In **Assignment** assign to **sg-M365D**group and click on **Next**
7. On **Review + create** review config and click on **Create**

Do similar for MacOS. Change settings in Configuration settings – see what more options you have with firewalls.

Create rules for Microsoft Defender Firewall rules which allows us to define more granular Firewall rules (rules with specific ports, protocols, applications and networks, to allow or block network traffic).

Endpoint detection and response

When you integrate Microsoft Defender for Endpoint with Intune, you can use endpoint security policies for endpoint detection and response (EDR) to manage the EDR settings and onboard devices to Microsoft Defender for Endpoint.

1. Go to https://endpoint.microsoft.com/ > **Endpoint security** > **Endpoint Detection and response > Create Policy**
2. Choose **Windows 10 and later** in **Platform**, and choose **Endpoint detection and response (MDM)** as **Profile.** Click on **Create**
3. Enter **Name(Win EDR policy)** and **Description(Windows Endpoint detection and response policy)** and click on **Next**
4. In **Configuration settings** turn on **Endpoint Detection and Response** to **Yes**
5. Click on **Next** and again on **Next**
6. In **Assignment** assign to **sg-M365D**group and click on **Next**
7. On **Review + create** review config and click on **Create**

Attack surface reduction

Attack surface reduction policies help reduce your attack surfaces, by minimizing the places where your organization is vulnerable to cyberthreats and attacks.

1. Go to https://endpoint.microsoft.com/ > **Endpoint security** > **Attack surface reduction > Create Policy**
2. Choose **Windows 10 and later** in **Platform**, and choose **Attack surface reduction rules** as **Profile.** Click on **Create**
3. Enter **Name(Win ASR rules policy)** and **Description(Windows Attack surface reduction rules policy)** and click on **Next**
4. In **Configuration settings** configure turn all settings to **Audit mode**
5. Click on **Next** and again on **Next**
6. In **Assignment** assign to **sg-M365D**group and click on **Next**
7. On **Review + create** review config and click on **Create**

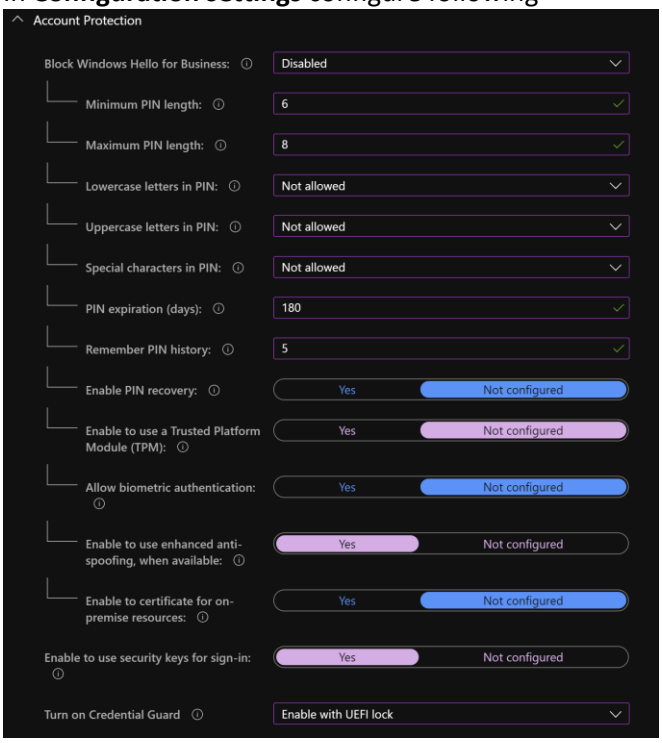
Change settings and change some from Audit mode to Enable and see how machines are behaving during Evaluation lab.

Let's try with other Attack surface reduction policies like Web protection, Device control, App and browser isolation, and check how these additional rules are helping you to reduce attack surface.

Account protection

Use Intune endpoint security policies for account protection to protect the identity and accounts of your users. The account protection policy is focused on settings for Windows Hello and Credential Guard, which is part of Windows identity and access management.

1. Go to https://endpoint.microsoft.com/ > **Endpoint security** > **Account protection > Create Policy**
2. Choose **Windows 10 and later** in **Platform**, and choose **Account protection (preview)** as **Profile.** Click on **Create**
3. Enter **Name(Win AP policy)** and **Description(Windows Account protection policy)** and click on **Next**
4. In **Configuration settings** configure following



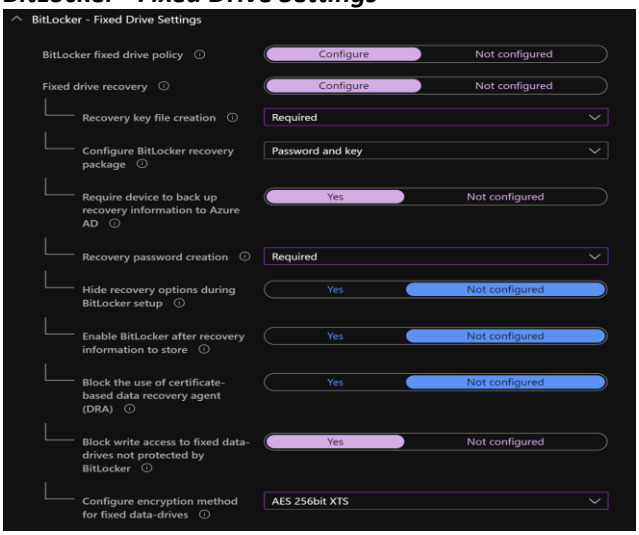
5. Click on **Next** and again on **Next**
6. In **Assignment** assign to **sg-M365D**group and click on **Next**

7. On **Review + create** review config and click on **Create**

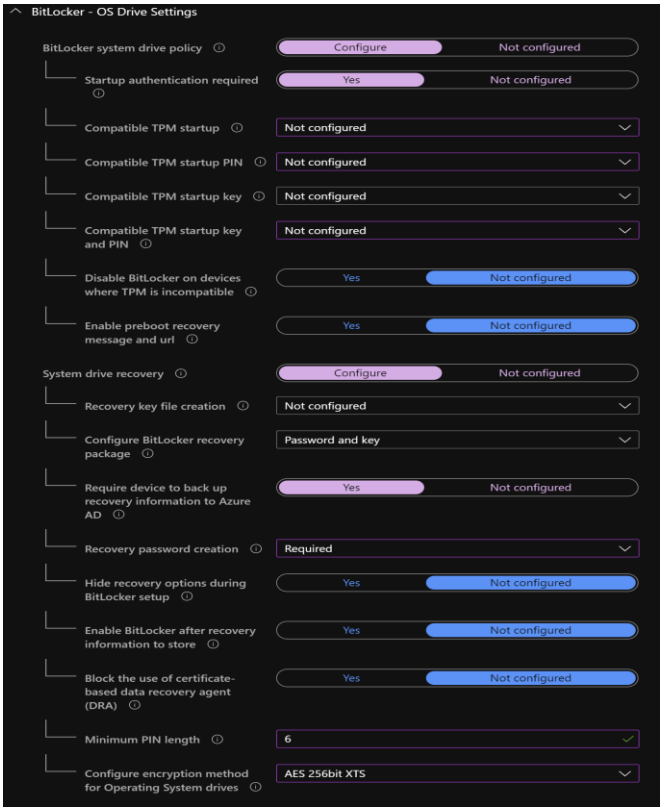
Disk encryption

Endpoint security Disk encryption profiles focus on only the settings that are relevant for a devices built-in encryption method, like FileVault or BitLocker. This focus makes it easy for security admins to manage disk encryption settings without having to navigate a host of unrelated settings.

1. Go to https://endpoint.microsoft.com/ > **Endpoint security** > **Disk encryption > Create Policy**
2. Choose **Windows 10 and later** in **Platform**, and choose **BitLocker** as **Profile.** Click on **Create**
3. Enter **Name(Win DE policy)** and **Description(Windows Disk encryption policy)** and click on **Next**
4. In **Configuration settings** configure following
    a. ***BitLocker - Base Settings***
        i. **Enable full disk encryption for OS and fixed data drives** > **Yes**
        ii. **Hide prompt about third-party encryption** > **Yes**
        iii. **Allow standard users to enable encryption during Autopilot** > **Yes**
        iv. **Configure client-driven recovery password rotation** > **Enable rotation on Azure AD-joined device**
    b. ***BitLocker - Fixed Drive Settings***



    c. ***BitLocker - OS Drive Settings***



d. BitLocker - Removable Drive Settings

i. **BitLocker removable drive policy** > **Yes**
ii. **Configure encryption method for removable data-drives** > **AES 256bit XTS**
iii. **Block write access to removable data-drives not protected by BitLocker** > **Yes**
iv. **Block write access to devices configured in another organization** > **Yes**

5. Click on **Next** and again on **Next**
6. In **Assignment** assign to **sg-M365D**group and click on **Next**
7. On **Review + create** review config and click on **Create**

Go to settings and change disc encryption. Test disk encryption with removable disk. Create policy for MacOS.

Security baselines

Use Intune's security baselines to help you secure and protect your users and devices. Security baselines are pre-configured groups of Windows settings that help you apply a known group of settings and default values that are recommended by the relevant security teams.

1. Go to https://endpoint.microsoft.com, **Endpoint security > Security baselines > Microsoft Defender ATP baseline**
2. Click on **Create Profile**, enter **Name** and **Description (MD ATP Security Baseline)**, and click on **Next**
3. In **Configuration settings** check configuration and click on **Next**
4. Click **Next** in **Scope tags**
5. In **Assignments** choose group **one test user who is not part of sg-M365D**and click **Next**
6. Click **Create**

Please note that with this config we put MD for Endpoint security baselines where we enabled some ASR rules, Smart Screen, Firewall, etc. It can impact RDP if using VMs. Configure based on needs.

It's best that you apply Security baselines on one device for testing, and on second device to use separate Security policies which are easier to change later on (AV, firewall, EDR,…)

Test
We will do it through Evaluation lab!

Live response

Live response is a capability that gives your security operations team instantaneous access to a device (also referred to as a machine) using a remote shell connection.

1. Go to https://securitycenter.windows.com/ **> Devices list** and choose device
2. In top right corner click on 3 dots and choose **Initiate Live Response Session**

Test
Go to https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/live-response-command-examples to find examples of Live response commands. Save .txt file in device and search for it and try getfile command.

You can also go to https://securitycenter.windows.com/ **> Evaluation and tutorials > Simulation and tutorials**. Under **Tutorials** choose **Scenario 5 – Live Response tutorial**.

Isolate device

Depending on the severity of the attack and the sensitivity of the device, you might want to isolate the device from the network. This action can help prevent the attacker from controlling the compromised device and performing further activities such as data exfiltration and lateral movement.

1. Go to https://securitycenter.windows.com/ **> Devices list** and choose device
2. In top right corner click on **Isolate device** (please note that if you are connected via RDP, you'll lose RDP connection). Enter comment for Isolation and click **Confirm**
3. Check what happened on device. After you remediate device, go back to device in **Device list** and click on **Release from isolation**

While you are on device please investigate all options like Timeline (to see events date back on devices, you can even Flag some events for later investigation), software inventory, discovered vulnerabilities, missing KBs, and you can also run AV scan, Collect investigation package

Device value

Defining a device's value to the organization as high, normal, or low helps you differentiate between asset priorities. A high value device will have a greater impact on your organization exposure score.

1. Go to https://securitycenter.windows.com/ **> Devices list** and choose device
2. In top right corner click on 3 dots and choose **Device value**
3. From **Device value** choose **High** and click on **Submit**
4. Return on device and note that device have **Tag** stating **Device value: High**

Evaluation 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. Here, we can test our configuration using known tools like SafeBreach and AttackIQ to test using simulations like Known Ransomware Infection, Code Execution, Defense evasion, Persistence Methods, as well as Microsoft prepared simulations like Automated Investigation, PowerShell script, Document drops backdoor, etc.

1. Go to https://securitycenter.windows.com/ **> Evaluation Lab**
2. Create Evaluation Lab per number of machines
3. Go to **Simulations and tutorials** where you can find some of the simulations to test MD for Endpoint response
4. Go to https://demo.wd.microsoft.com/, where you can find more demos available for MD for Endpoint like Potentially Unwanted Application, Controlled Folder Access, etc.
5. Go to http://demo.smartscreen.msft.net/ to test SmartScreen and link blocking
6. Check now **Incidents** and **Alerts queue** to see alerts happened during Evaluation
7. Go to **Reports** to see what was detected in reports
8. Go to **Automated investigations** to see are there any automated investigation and status of the same
9. Go to **Threat & Vulnerability Management** and check exposure score and configuration score

Threat and Vulnerability Management

Effectively identifying, assessing, and remediating endpoint weaknesses is pivotal in running a healthy security program and reducing organizational risk. Threat and vulnerability management serves as an infrastructure for reducing organizational exposure, hardening endpoint surface area, and increasing organizational resilience.
Discover vulnerabilities and misconfigurations in real time with sensors, and without the need of agents or periodic scans. It prioritizes vulnerabilities based on the threat landscape, detections in your organization, sensitive information on vulnerable devices, and business context. To get list of supported system for TVM please visit - Supported operating systems and platforms for threat and vulnerability management - Windows security | Microsoft Docs

1. Go to https://securitycenter.windows.com/ **> Threat & Vulnerability Management > Dashboard**

In **Dashboard** you will be able to see **Exposure score** (current exposure associated with devices in your organization), **Microsoft Secure Score for Devices** (collective security configuration posture of your devices across OS, Application, Network, Accounts and Security Controls), **Exposure distribution** (Low, Medium, and High), as well as **Top events, Top vulnerable software, Top remediation activities, Top exposed devices,** and **Top security recommendations**.
Go through data and check data shown. Install more software on test devices and check how it will affect your environment. Note: Be careful with installing unknown software or software that have any vulnerability/breach associated with it.

2. Go to https://securitycenter.windows.com/ **> Threat & Vulnerability Management > Security recommendations**

In **Security recommendations** you will be able to see list of all security recommendations associated with your environment. For each recommendation you will have weakness associated with it, how many devices are associated with it, is there any known public exploit/vulnerability/breach associated with each recommendation. We can also see what kind of remediation it's connected with, what impact on exposure score it will have, as well as tags (like EOS software). When we click on particular security recommendation, we will get more details about it like description, details, as well as on how many devices this software is installed and how many of those devices are exposed.

You can also see CVEs connected to it, and you can open Remediation options, Report inaccuracy, as well to open Software page. In lower steps, we will go over opening remediation for Security recommendation as well as **Remediation** page in MD for Endpoint.

3. Go to https://securitycenter.windows.com/ **> Threat & Vulnerability Management > Software inventory**

In this page we will see applications installed on your devices, as well as Weaknesses associated with each software, Threats detected, Exposed devices, as well as impact on score when we apply security recommendations detected with software.
Click on one of the software detected and click on **Software page.** Here we will see more details about software, including security recommendations associated with software, discovered vulnerabilities, what devices are exposed, version distribution detected, and event timeline.

4. Go to https://securitycenter.windows.com/ **> Threat & Vulnerability Management > Weaknesses**

Here we can see all CVEs detected in our environment, Severity of Each CVE as well as how old it is, when it is published, if updated – when it is updated, threats associated (exploit/breach), and how many exposed devices we have with each CVE. When we click on one of the CVEs, we will get Description of CVE as well as details about it

5. Go to https://securitycenter.windows.com/ **> Threat & Vulnerability Management > Event timeline**

Event timeline is a risk news feed that helps you interpret how risk is introduced into the organization through new vulnerabilities or exploits. You can view events that may impact your organization's risk. For example, you can find new vulnerabilities that were introduced, vulnerabilities that became exploitable, exploit that was added to an exploit kit, and more.

Open ticket from Threat and Vulnerability Management to Intune

There is integration between MD for Endpoint and Intune or ServiceNow for ticketing. We will show how to do it with Intune integration. You'll have to install few programs on machine to get data. Install programs like Office, Edge Chrome, Chrome, Adobe Reader,…

1. Go to https://securitycenter.windows.com/ **> Threat & Vulnerability Management > Security recommendations**
2. Click on one of recommendations related to software (like Update Windows or Update Office), and then click on **Remediation options**, check next to **Open a ticket in Intune**, select **Priority** and **Due date**, and you ca **Add notes** if needed
3. Now go to https://endpoint.microsoft.com/ > **Endpoint security > Security tasks**
4. Click on your task. You'll get **Details**, **Status**, **Impacted Devices**, as well as **Remediation** option
5. Click on **Accept** to accept a ticket. After finishing click on **Complete**. Note that statuses are changing in Intune
6. Go back to to https://securitycenter.windows.com/ **> Threat & Vulnerability Management > Remediation.** Note that remediation ticket is marked as completed in MD for Endpoint. Now you can check is it remediated in MD for Endpoint or person that needed to do remediation didn't do it. If it is done, you can click on remediation and click on **Mark as completed**

Advanced hunting

Advanced hunting is a query-based threat-hunting tool that lets you explore raw data for the last 30 days. You can proactively inspect events in your network to locate interesting indicators and entities. The flexible access to data facilitates unconstrained hunting for both known and potential threats.

1. Go to https://securitycenter.windows.com/ **> Advance hunting**
2. Inspect queries under **Shared queries** to see what you can do with advance hunting

We will have separate session to go over Advance hunting in Microsoft 365 Defender.

Web content filtering

Web content filtering is part of Web protection capabilities in Microsoft Defender for Endpoint. It enables your organization to track and regulate access to websites based on their content categories. Many of these websites, while not malicious, might be problematic because of compliance regulations, bandwidth usage, or other concerns. Let's configure it!

1. Go to https://securitycenter.windows.com/, **Settings > Web content filtering**, click on **+Add item**
2. Enter following details
    a. Policy – General
    b. In **Blocked categories** choose **Adult content** and **Leisure**
    c. Scope – All devices in my scope
    d. Save

Power Automate and MD for Endpoint integration

We will cover this later in document as part of Power Automate SOAR functionalities.

MICROSOFT CLOUD APP SECURITY

Microsoft Cloud App Security is a Cloud Access Security Broker that supports various deployment modes including log collection, API connectors, and reverse proxy. It provides rich visibility, control over data travel, and sophisticated analytics to identify and combat cyberthreats across all your Microsoft and third-party cloud services. Let's try it!

Enabling advance features

We need to make sure that MCAS and MD for Endpoint integration is on

1. Go to https://portal.cloudappsecurity.com, click on **Settings** (top right corner), and go to **Microsoft Defender for Endpoint**, make sure that **Block unsanctioned apps** is marked
2. Go to https://securitycenter.windows.com/ **> Settings > Advanced features >** make sure that **Microsoft Cloud App Security** is turned **On**
3. On devices where testing blocking of unsanctioned apps, we must enable Network Protection (via Intune policy, SCCM, GPO, or enabling with PowerShell - Set-MpPreference -EnableNetworkProtection Enabled)

After opening few applications on machines, go to https://portal.cloudappsecurity.com, **Discover > Cloud Discovery dashboard**. Make sure that for report in top right corner is chosen Win10 Endpoint Users. Go through menus and see what apps are discovered, what Risk Scores are for those apps, and block some of the apps. When you block some apps, it'll automatically create Indicators in MD for Endpoint to ban access to those sites. Go to https://securitycenter.windows.com/ choose Settings > Indicators > URLs/Domain, where you'll be able to see URLs that are blocked for those sites and in Created by you'll see Microsoft Cloud App Security. On one of the machines enrolled to MD for Endpoint try to open one of these sites, it should be blocked. Go back to https://securitycenter.windows.com/, click on Alerts – there should be Alert for this blocked site. (It can take couple of minutes all to sync)

To connect with Office 365 we need to enable File monitoring

1. Go to https://portal.cloudappsecurity.com, click on **Settings** (top right corner), click on **Files,** check **Enable file monitoring** and click on **Save**

Enable integration with Azure Information Protection

1. Go to https://portal.cloudappsecurity.com, click on **Settings** (top right corner), click on **Azure Information Protection** and check **Automatically scan new files** Click on **Save**
2. Click on **Grant permission** for inspection of protected files

Creating demo app discovery

It's important to upload a log manually and let Microsoft Cloud App Security parse it before trying to use the automatic log collector. If you don't have a log yet and you want to see an example of what your log should look like, download a sample log file. Follow the procedure below to see what your log should look like.

1. Go to https://portal.cloudappsecurity.com, click on **Discover** and then on **Create snapshot report**
2. Enter name and description (Test report). In **Data source** choose **Squid (Common)**, select **Anonymize private information**, and then click on **View and verify…** and then **Download sample log**. In **Choose traffic logs** click on **Browse** and upload sample log that you previously downloaded.
3. Click on **Create**

When report is ready make sure that that report is chosen in top right corner. Open it and click trough Dashboard, Discovered Apps, IP Addresses, and Users. Filter through Apps based on Risk Score. Choose Risk Score between 1 and 3 and mark few apps as unsanctioned. In top right corner click on 3 dots, and click on Generate block script…, choose one of the firewalls and download to see sample block policies.

Connecting Office 365 and 3rd party apps to MCAS

Organizations can integrate some 3rd party apps into MCAS like Salesforce, Box, Dropbox…, as well as Azure, AWS, and Google Cloud. This enables you greater control and visibility over other cloud apps that your organization uses. Let's see how it looks with Box.

First, we need to connect Office 365

1. Open https://portal.cloudappsecurity.com go to **Gear icon** in top right corner and choose **App connectors**
2. Click on the **+** button and choose **Office 365** Follow steps to connect

Now, we need to open Box developer account

1. Go to https://account.box.com/signup/n/developer and fill details
2. Open https://outlook.office365.com and verify email
3. Open https://portal.cloudappsecurity.com go to **Gear icon** in top right corner and choose **App connectors**
4. Click on the **+** button and choose **Box**
5. In the Instance name box, type **Box API**, and click **Connect Box**
6. In the Connect Box dialog, click **follow this link**
7. Use Box username and password
8. Click on **Grant access to Box**
9. Close the Connect Box dialog and click on **Box API** to expand and click on **Test**

Now go to Box developer account and upload some Word and PDF documents. Go to MCAS portal and click on Investigate > Files and for App choose Box. You'll be able to see all files. You can also apply Azure Information Protection label on them, make different policies, put files into Quarantine etc. Example of policies we will show below.

Add some documents to Box environment. Now you can test few of options mentioned above.

Block unsanctioned app on MD for Endpoint devices

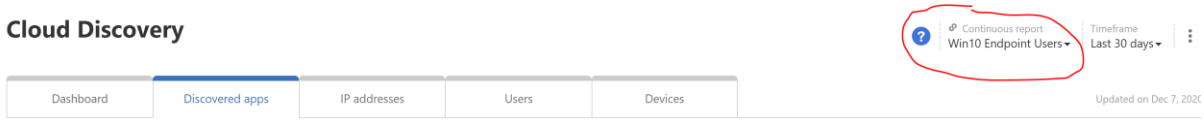
If we connect MCAS with MD for Endpoint, we can block access to unsanctioned apps of devices that are running MD for Endpoint.

First we need to make sure that connection between MCAS and MD for Endpoint on:

1. Go to https://portal.cloudappsecurity.com/ -> click on **gear icon** (**Settings**) and under **System** click on **Settings**
2. Under **Cloud Discovery** choose **Microsoft Defender for Endpoint** make sure that **Block unsanctioned apps** is marked, if not – check it and click **Save**
3. Go to https://securitycenter.windows.com/ -> click on **gear icon (Settings)** -> **Advanced features** and make sure that **Custom network indicators** and **Microsoft Cloud App Security** is turned on

Test

With of the Windows 10 machines that are connected to MD for Endpoint visit few web apps. After some time go to https://portal.cloudappsecurity.com/ -> **Discover -> Discovered apps**. Make sure that report you see is as below



You'll be able to see visited web apps. For some of them, in the **Actions** mark them as unsanctioned by clicking on **Tag as Unsanctioned**. After few moments, try visit those apps from connected machine, and try different browsers. On Edge Chromium you'll get info that web site is blocked (message by SmartScreen) but on other browser's you'll just not be able to visit a site since they don't have SmartScreen.

Go to https://securitycenter.windows.com/ -> click on **gear icon (Settings)** -> **Indicators -> URLs/Domains**. Here you'll be able to see all web apps that you blocked using MCAS Unsanctioned tag. If you want to add any URL manually, you can do it by clicking on **Add item.**

Session control via Conditional Access App Control

Conditional Access App Control uses a reverse proxy architecture and integrates with your IdP. When integrating with Azure AD Conditional Access, you can configure apps to work with Conditional Access App Control with just a few clicks, allowing you to easily and selectively enforce access and session controls on your organization's apps based on any condition in Conditional Access.

1. Go to https://aad.portal.azure.com/ **> Azure AD Security > Conditional Access > New policy**
2. Enter following:
    a. **Name > CA Access Control**
    b. **Users and groups > All users**
    c. **Cloud apps or actions > Selected apps** > search for **SharePoint Online** and **Exchange Online**

    d. **Session** > mark **Use Conditional Access App Control** and choose **Use custom policy**…
3. Enable policy and click **Save**
4. Open Exchange Online, SharePoint Online, and Box, sign out of them, and sign in again to start App Control
5. Go to https://portal.cloudappsecurity.com, click on **Settings > Conditional Access App Control**. You should be able to see SharePoint online and Exchange Online here now.

Block upload/download of sensitive info with CAAS, label when downloading

Let's see how we can block upload/download of sensitive information using CAAS, as well as labeling them using AIP or Sensitivity labels.

1. Go to https://portal.cloudappsecurity.com
2. On the left-hand side click on **Control** and then **Policies**.
3. Click on **Create Policy** and click on **Session policy**.
4. Name: **Proxy - Block sensitive files download**
5. Under **Session Control Type** choose **Control file download (with inspection)**
6. App equals **Microsoft Exchange Online**
7. Under **Inspection Method** click on **Data Classification Service** and choose **inspection type sensitive information type** and search for **SSN**. Click **U.S. Social Security Number** and Click **Done**.
8. Under **Actions**: go to **Block**
9. Click: **Customize block message**: This file contains SSN information and cannot be downloaded.
10. Verify that **Create an alert for each matching event with the policy's severity** is checked.
11. Check the **Send alerts to Power Automate** checkbox, select the Power Automate you created
12. Click: **Create**

Create doc containing demo SSNs from page 6!

Send this document to another user via Exchange Online. Log in to Exchange Online as other user and see file online – you can do it. Then try to download it – you'll get Block message. You can try to do the same with including SharePoint Online as an App in the session policy. Try also with Box.

Go to Teams group that you integrated MCAS and Power Automate for sending alerts. There should be notification that there is new Alert in MCAS.

Information protection with MCAS

We can integrate AIP and Sensitivity labels with MCAS so that we can make policies for automatic classification of data stored on cloud apps, as well to discover apps and label them manually.

1. Under **Settings > Admin quarantine** choose place where you want to put admin quarantine and make user notification like:
   Your file was put in quarantine in accordance with your organization's security policy. For more information, contact your network administrator.
2. Return to https://portal.cloudappsecurity.com, and go to **Investigate > Files** where you'll see all files from connected apps (in this case Office 365)
3. Click on file and investigate data. On right side click on **3 dots (Actions) > Apply classification label**. You'll get option to select classification label for that file. After choosing and clicking on **Apply**, file will be refreshed ad label will be applied. Download file and inspect new label.

Test more apps.

Policy for stale documents

Let's see how we can discover stale externally shared files that nobody had changed for some period. Using this we can see if documents are accessible externally using email sharing or link, as well as remove all or particular collaborators.

1. Go to https://portal.cloudappsecurity.com **> Control > Policies > Create policy > File policy**
2. In **Policy template** choose **Stale externally shared files** and click on **Apply template**
3. In Create a filter for the files this policy will act on check **Access level** and **Last modified**. In **Last modified** change from **180 days** to **5 days**
4. Click on **Create**

Share some files via OneDrive for Business or SharePoint Online. After 6 days go to **Investigate > Files** and under **MATCHED POLICY** choose **Stale externally shared files**. You'll be able to find files you shared previously. You can inspect them and manually remove collaborators, put label on it, or put it into quarantine. Go back to **Control > Policies** and find **Stale externally shared files** policy. Open it and change configuration. You can put that for OneDrive for Business automatically external collaborators are removed and for SharePoint Online that it will be marked as Private document, change configuration and see what will happen.

Policy for finding sensitive info

As we can find any stale document, we can also find any sensitive information that is available in files stored on connected apps. In this example we will search for any document that has US Social Security Number (SSN).

1. Go to https://portal.cloudappsecurity.com **> Control > Policies > Create policy > File policy**
2. In **Policy template** choose **File containing PII detected in the cloud (built-in DLP engine)** and click on **Apply template**
3. Click on **Create**

Go back to file used in policy blocking upload/download of sensitive info since it has SSN numbers in it. Make sure it's not deleted or changed. Go to **Investigate > Files** and under **MATCHED POLICY** choose **File containing PII detected in the cloud (built-in DLP engine)**, you'll be able to find particular document. Go back policy and change configuration. See differences on file.

Protect files in 3rd party apps (Box)

We can protect files in 3rd party apps as well. For example, Box also supports AIP integration se we can label files in Box using AIP and MCAS.

1. Go to https://portal.cloudappsecurity.com **> Control > Policies > Create policy > File policy**
2. In **Policy name** enter **Protect SSN files in Box**, and on **Description** we put **Protecting SSN files in Box**
3. In **Create a filter for the files this policy will act on** delete them and put this:
    a. App > equals > Box
4. In **Inspection method** choose **Data Classification Services** and search and choose **U.S. Social Security Number (SSN)**
5. In **Governance actions** under **Box** choose **Apply classification label** and choose one of the labels you created in Azure Information Protection and Unified Labeling sections (Confidential)
6. Click on **Create**

Create DOCX file containing SSN numbers and upload it to Box environment we connected above. After few hours go to **Investigate > Files** and under **MATCHED POLICY** choose **Protect SSN files in Box**. You should be able to find that particular document. Examine and see is label applied. Go back to policy and make some configuration changes. See what will happen.

Microsoft Defender for Identity

Microsoft Defender for Identity (formerly Azure Advanced Threat Protection, also known as Azure ATP) is a cloud-based security solution that leverages your on-premises Active Directory signals to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization.

As I mentioned, we are not covering Microsoft Defender for Identity in AISW, but you can follow this instruction to create your own lab (with step by step instructions) and test how MD for Identity works.
Microsoft Defender for Identity Security Alert lab tutorial overview | Microsoft Docs

Here is explanation how to install MD for Identity sensor on your domain controller.
Install Microsoft Defender for Identity sensor quickstart | Microsoft Docs

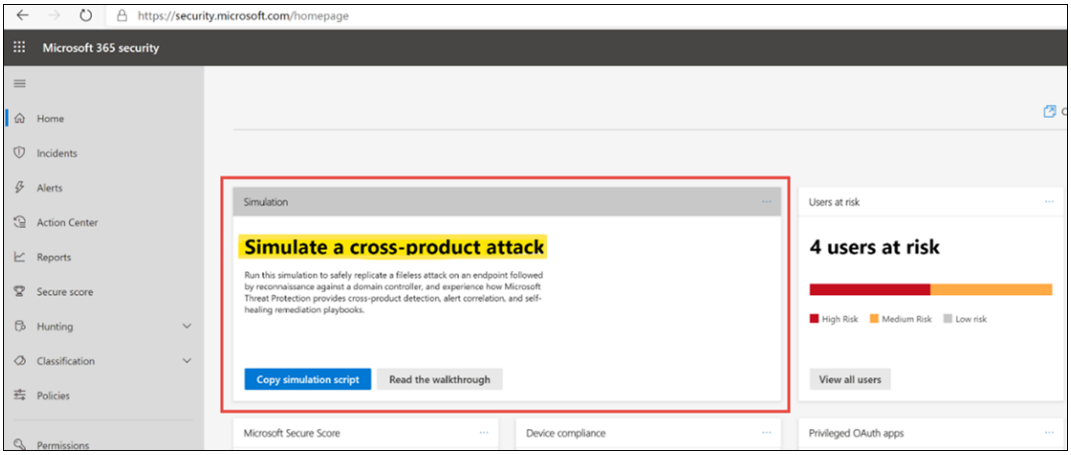
MICROSOFT 365 DEFENDER

As we mentioned above, Microsoft 365 Defender is a unified pre- and post-breach enterprise defense suite that natively coordinates detection, prevention, investigation, and response across endpoints, identities, email, and applications to provide integrated protection against sophisticated attacks. Let's take look!

1. Go to https://security.microsoft.com/, and click on **Incidents**. Check **Turn on Microsoft 365 Defender** and then **Accept**
2. After enabling it'll take few minutes to activate it. Refresh the page. You'll see all incidents from Microsoft Cloud App Security, Microsoft Defender for Endpoint, Microsoft Defender for Office 365, and Microsoft Defender for Identity. If you have any alerts trough solutions that part of same incident, they will be under same incident page
3. Go to **Hunting > Advance hunting**. Inspect possible queries. We will have separate session to go over Advance hunting in Microsoft 365 Defender and Microsoft Defender for Endpoint.

There is step-by-step instructions how to create simulation attack on Microsoft 365 Defender

1. Log on to https://security.microsoft.com
2. On the Home page, look for a tile titled Simulation. Review the walkthrough guide for steps to create a test incident in Microsoft 365 Defender.
   Image of simulation card in the Microsoft 365 Security dashboard



Please note that for this simulation you'll need 2 device – a test device and a domain controller. This is what you'll need:

1. Verify that your tenant has enabled Microsoft 365 Defender
2. Configure a test domain controller
    a. Setup a device with Windows Server 2008 R2 or above
    b. Onboard a test domain controller to Microsoft Defender for Identity and enable remote management
    c. Enable Microsoft Defender for Identity and Microsoft Cloud App Security integration
    d. Create a test user on your domain – no admin permissions needed
3. Configure a test device
    a. Requires Windows 10 1903 or above
    b. Join the test device to the test domain
    c. Turn on Windows Defender Antivirus
    d. Onboard to Microsoft Defender for Endpoint

After these steps follow walkthrough guide (see above picture where to find it) or access it from my GitHub – [AISW/MTP_PowerShellFilelessInjectionSMBRecon.pdf at main · BenjiSec/AISW (github.com)]

Advanced Hunting

Advanced hunting is a query-based threat-hunting tool that lets you explore up to 30 days of raw data. You can proactively inspect events in your network to locate threat indicators and entities. The flexible access to data enables unconstrained hunting for both known and potential threats.

1. Go to https://security.microsoft.com/ **-> Hunting -> Advanced Hunting**
   Let's do couple of queries. We will use emails since there are probably some email flow in your test tenant.
   In the query window enter

```
EmailEvents
```

   And run the query. You'll get all email events from your company. If you want to take only 10 email events (any 10) we can use command "take":

```
EmailEvents
| take 10
```

   Note that every time we can get 10 different results.
   To take only top 10 results, we will use command "top":

```
EmailEvents
| top 10 by Timestamp
```

We can use any column instead of “Timestamp”

In real life we will have tables that will have tens of thousands of lines and we will want to limit the results to specific number. For it we can use “limit” command

```
EmailEvents
| limit 10
```

If we want to search by specific information like sender, we will use command “where”

```
EmailEvents
| where SenderFromAddress contains "microsoft.com" //we can use any other info
that we found in column SenderFromAddress
```

Here it will list all email events where sender is Microsoft. Something that you maybe have noticed is that email events aren’t sorted by Timestamp and if we want to do that we can use command “sort”

```
EmailEvents
| where SenderFromAddress contains "microsoft.com"
| sort by Timestamp desc
```

To sort it ascending change from “desc” to “asc”

To get number of events we can use “count”

```
EmailEvents
| where SenderFromAddress contains "microsoft.com"
| count
```

, or if you want to get info how many emails events are connected to each sender with “microsoft.com” we can use “summarize”

```
EmailEvents
| where SenderFromAddress contains "microsoft.com"
| summarize count() by SenderFromAddress
```

Something that you have probably noticed is that we are getting many different columns. If we want to limit it only to specific number of columns, we can use command “project”

```
EmailEvents
| where SenderFromAddress contains "microsoft.com"
| project Timestamp, SenderMailFromAddress, RecipientEmailAddress,
Subject, EmailDirection, DeliveryAction, PhishFilterVerdict,
MalwareFilterVerdict
```

Now we got only column that are of interest to us. We can also change the names of the columns

```
EmailEvents
| where SenderFromAddress contains "microsoft.com"
| project Timestamp, Sender=SenderMailFromAddress,
Recipient=RecipientEmailAddress,
Subject, EmailDirection, DeliveryAction, Phish=PhishFilterVerdict,
Malware=MalwareFilterVerdict
```

And final command for this short tutorial is “extend”. We can use it to make new column, for example when we want to join 2 different columns into one. And we can use project to project that column as standard one:

```
EmailEvents
| where SenderFromAddress contains "microsoft.com"
| extend MalwareOrPhish = strcat(PhishFilterVerdict, "\\",
MalwareFilterVerdict)
| project Timestamp, Sender=SenderMailFromAddress,
Recipient=RecipientEmailAddress,
Subject, MalwareOrPhish
```

Once we create query that we want to use later as well, we can save it by clicking on Save and choose **Save as**, enter name and save to your queries.
Scroll down and locate **My queries**. Locate query you just saved and double click on it. It will automatically be shown in query window and you can run it. If you do any xhanges to it you can click on Save and choose **Save** to save the changes.

You’ll also see **Shared queries** and those are queries made by Microsoft experts that you can use for your day to day operations. Go to **Suggested** and click on **Microsoft 365 Defender**. Choose query called **PowerShell downloads**. This query finds PowerShell execution events that could involve a download.

We can also create **Custom detection** from Advanced Hunting. Let’s use this query:

```
EmailEvents
| where Subject contains "Custom detection rule test"
| project Timestamp, Sender=SenderMailFromAddress, RecipientEmailAddress,
Subject, EmailDirection, DeliveryAction, Phish=PhishFilterVerdict,
Malware=MalwareFilterVerdict, ReportId
```

First send sample email and wait until you can see it using query above. Please make sure that subject of email is “Custom detection rule test”. Sometimes it can take 10-20 minutes before we see result.

But what if we want to get alert once it gets detected in our environment? That’s where custom detection rule is helping. (Note: To create custom detection rule we must have at least these 2 columns in the query - Timestamp and ReportId. Also a column with impacted users, devices, or mailboxes cannot be renamed – in above example RecipientEmailAddress wasn’t be renamed, if we rename it – custom detection will not be able to create a rule. We can choose also SenderMailFromAddress as well.)

Now click on **Create detection rule** on the right side of window

1. For the **Detection name** enter **Custom detection example**
2. For **Frequency** choose **Every hour**
3. **Alert title** enter **Custom detection example**
4. For **Severity** choose **Low** and for **Category** choose **Suspicious activity**
5. In **Description** enter **Custom detection example** and click on **Next**
6. In **Impacted entities** choose **Mailbox** and **RecipientEmailAddress** and click on **Next** (if we leave SenderMailFromAddress not changed in above query, we would be able to choose between those 2 columns)

7. Check summary and create the rule

Now on the left menu under **Hunting** click on **Custom detection rules** and we will see rule we just created. Click on the rule and check info. See that we can run, edit, modify query, turn off, or delte the rule. So if we need to fine tune rule, we can do it at any point in time.

Now go to email and send again email with subject "Custom detection rule test". Wait for 10 minutes and go back to our **Custom detection rule** under **Hunting** in Security portal. We can wait for next schedule run (you can see when it will be under **Next run)** or to click on **Run** to run the detection rule immediately.

Go to **Incidents** in the Security portal(security.microsoft.com). You will see new Incident called **Custom detection example**. Open it and examine. You can see that alert that detected it is our custom detection rule, impacted user one to whom we had sent email.

If you want to learn more about KQL, please use these resources:

- Go through quick intro about KQL as language used for hunting - Learn the advanced hunting query language in Microsoft 365 Defender - Microsoft 365 security | Microsoft Docs
- If you are interested into deep dive learning, go through this training - Get expert training on advanced hunting - Microsoft 365 security | Microsoft Docs
- PluralSight KQL training - The Basics of Kusto Query Language | Pluralsight
- Visit GitHub site for many samples of the queries - GitHub - microsoft/Microsoft-365-Defender-Hunting-Queries: Sample queries for Advanced hunting in Microsoft 365 Defender

- **Webinars from Microsoft Security Community (highly recommended!)**

Episode1: KQL fundamentals	MP4	YouTube
Episode 2: Joins	MP4	YouTube
Episode 3: Summarizing, pivoting, and visualizing data	MP4	YouTube
Episode 4: Let's hunt! Applying KQL to incident tracking	MP4	YouTube

Sample files used in webinars can be found on GitHub - Microsoft-365-Defender-Hunting-Queries/Webcasts/TrackingTheAdversary at master · microsoft/Microsoft-365-Defender-Hunting-Queries (github.com)

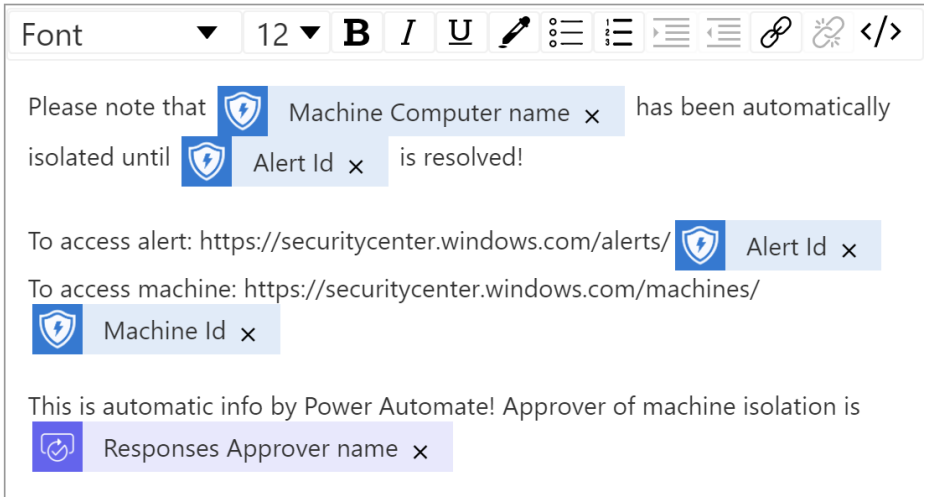
Power Automate as simple SOAR

Power Automate (previously known as Flow) can be used in many instances to automatize processes. In this part I'll make few Power Automate flows that will automize respond on particular alerts.

Isolate device when high alert detected on MD for Endpoint

In this example we will isolate device when there is High alert detected in MD for Endpoint, but we will also add step with approval for the isolation.

1. Go to https://flow.microsoft.com **->** and click on **Create**
2. Choose **Automated cloud flow** and as a name enter **Isolate device with High alert on MDE**
3. In **Choose your flow's trigger** search for **WDATP** and choose **Triggers - Trigger when new WDATP alert occurs** and click on **Create**
4. Click on **New step** search for **Microsoft Defender ATP** and choose **Alerts - Get single alert**
5. In **ID of the alert** choose **Alert ID**
6. Click on **New step** search for **Microsoft Defender ATP** and choose **Machines - Get single machine**
7. In **ID of the machine** choose **Alert Machine ID** that is under **Alerts – Get single alert**
8. Click on **New step** search for **Control** and choose **Condition**
9. In **Choose a value** search for **Alert Alert Severity** that is under **Alerts – Get single alert,** then **is equal to** and in **Choose a value** enter **High**
10. In **If yes** click on **Add an action** search for **Approvals** and choose **Start and wait for an approval**
11. In **Approval type** choose **Approve/Reject - First to respond**
12. In **Title** first enter **MDE - Approve Machine Isolation –** and then from Dynamic content choose **Machine Computer name**
13. In **Assign to** enter credentials of user who will be approving from demo tenant
14. In **Details** enter first **Please approve isolation of machine:** and from Dynamic content add **Machine Computer name**. After it enter **Here is link to alert https://securitycenter.windows.com/alerts/** and from Dynamic content add **Alert Alert ID**
15. In **Item link** add **Machine ID** from Dynamic content under **Triggers - Trigger when new WDATP alert occurs**
16. Click on **Add an action** search for **Control** and choose **Condition**
17. In **Choose a value** search for **Responses Approver response** that is under **Start and wait for an approval,** then **is equal to** and in **Choose a value** enter **Approve**
18. In **If yes** click on **Add an action** search for **Microsoft defender ATP** and choose **Actions – Isolate machine**
19. In **Machine ID** choose **Machine Id** that is under **Triggers - Trigger when new WDATP alert occurs**
20. In **Comment** enter **This machine is automatically isolated by approval of** and from Dynamic content add **Responses Approver name** then again add text **on** and from Dynamic content choose **Responses Response date**
21. Now as last step we will add email notification. Click on **Add an action** search for **Outlook** and choose **Send an email (V2)**
22. In **To** add email where this notification should be sent
23. In **Subject** add text **Notification:** then from Dynamic content choose **Machine Computer name** and then add this text after it **has been isolated**
24. For **Body** you can compose message with info that is useful to person to know why machine is isolated and who is approver – something like this:



Now you need to create High alert on your demo device to see how it works. Easiest way is to go to MD for Endpoint admin portal (https://securitycenter.windows.com/) go under **Settings** and choose **Indicators** and then choose **URLs/Domains**. Click on **Add item** and in URL paste web site link (like yahoo.com) and then click on **Next**. Choose **Alert and block**, for **Alert title** choose Yahoo.com access and for **Alert Severity** choose **High**. For **Description** add Block of Yahoo.com and click on **Next.** Choose **All devices in my scope** and click on **Next** and then on **Save.** After few moments go to a machine that is onboarded to MD for Endpoint and open site you added as indicator. It should be blocked and new alert will be available in MD for Endpoint portal. Now go to email you added for Approval and check email you got. Click on approve and go to machine and check can you open any site – all should be blocked. Go to Devices in MD for Endpoint and check device status. You should see that it is isolated and that you can release it from isolation. Click on it and try visiting few different sites on machine – now again it should be possible.

Try also to change flow and to send notification to your SOC Teams group. First create Team group named SOC, and then in this flow, after Outlook step, add new action with teams and posting a message to Teams group!

Microsoft Cloud App Security and Power Automate integration

Here is one basic that we can use to post message in Teams when policy is detected
We can integrate MCAS policies with Power Automate so that when we have policy match that we get automatic notification on email or Teams channel.

First, we need to generate token in MCAS

1. On the **Settings** menu (Gear in top right corner), select **Security extensions** and then **API tokens**.
2. Click the **plus icon**, **Generate new token** and provide a name (PowerAutomate integration) to identify the token in the future, and click **Generate**.
3. Copy the token value and save it somewhere for recovery - if you lose it you need to regenerate the token. The token has the privileges of the user who issued it. For example, a security reader can't issue a token that can alter data.
4. You can filter the tokens by status: Active, Inactive, or Generated.
5. Generated are tokens that have never been used.
    a. Active are tokens that were generated and were used within the past seven days.
    b. Inactive were used but there was no activity in the last seven days.
6. After you generate a new token, you'll be provided with a new URL to use to access the Cloud App Security portal. The generic portal URL continues to work but is considerably slower than

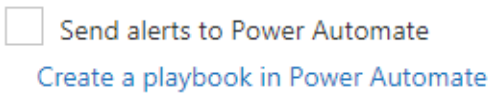
the custom URL provided with your token. If you forget the URL at any time, you can view it by going to the **?** icon in the menu and selecting About.

Go now to Flow/Power Automate

1. Navigate to the Microsoft Flow (go to portal.office.com and search for Power Automate) portal and choose **Create -> Automated flow**
2. In **Name** enter **MCAS integration**
3. In search connectors and triggers, type **Cloud App Security** and select **When an alert is generated**. Click on **Create**
4. Enter **Connection Name (PowerAutomate integration)** and API Key you generated before and click on **Create** and then on **New step**
5. Search for Teams and choose Post a message action. Then choose Team that you want and a channel, and configure post like - New alert: "**Description**" from "**IP Addresses**" Type: "**AlertType**". If you do not have Teams, create one.
6. **Save**

Configure a policy to use Flow

1. Go back to Cloud App Security https://portal.cloudappsecurity.com
2. Go to the **Policy section**.
3. Open Policy where you want to add Power Automate playbook
4. Go to the bottom of the page, check the **Send alerts to Power Automate** checkbox, select the Power Automate you created and click **Update**.



To test this one, just do the action to activate selected policy (like share of sensitive data – credit card). Pay attention to Teams group you choose, very soon you will get notification in it!

When it comes to automated actions like isolate device, block user, etc, we have group of 4 flows that are created by our team and which you can import to your tenant from our GitHub site - Microsoft-Cloud-App-Security/Playbooks at master · microsoft/Microsoft-Cloud-App-Security (github.com). Together with import package, there is blogpost with detailed instructions how to enable these flows.

Test them out and see how they work! To get unusual location (medium sign-in risk) easiest is to use Tor browser on your test machine. Open Tor browser and sign in to portal.office.com with one of enabled users.

SECURE SCORE

Microsoft Secure Score is a measurement of an organization's security posture, with a higher number indicating more improvement actions taken. From a centralized dashboard in the Microsoft 365 security center, organizations can monitor and work on the security of their Microsoft 365 identities, data, apps, devices, and infrastructure.

1. Go to https://security.microsoft.com/securescore. Analyze your Secure Score and Comparison.
2. Click on **Improvement actions** to see what you need to do to make your organization more secure. Click trough few suggestions. Notice that for each suggestion we also have **Implementation** steps.
3. Return to https://security.microsoft.com/securescore and click on **History**. You'll be able to see all changes that were made on tenant.
4. Now click on **Metrics & Trends** to see how your Secure Score was changing trough period of time

Try implementing few of suggestions and see change in Secure Score. Secure Score can be guidance how to make your environment more secure.

Disclaimer: Recommendations from Secure Score should not be interpreted as a guarantee of security! They are only suggestions what you can do to improve your organization's secure posture!

Compliance in Microsoft 365

Microsoft Compliance Manager and Compliance Score

Microsoft Compliance Score is a preview feature in the Microsoft 365 compliance center to help you understand your organization's compliance posture. It calculates a risk-based score measuring your progress in completing actions that help reduce risks around data protection and regulatory standards.

Think of Compliance Score as a simplified experience of Compliance Manager. While the two exist as distinct yet integrated tools, Compliance Score makes it easier to monitor your overall compliance posture and take steps to improve it.

Compliance Score shares the same backend with Compliance Manager. Anything that you do in one tool will surface in the other tool.

1. Log in to https://compliance.microsoft.com/ and click on **Compliance Manager**
2. Go through Overview, Improvement actions, Solutions, and Assessments to see what you can do in compliance manager

In **Overview** you can see your Compliance Score - it calculates a risk-based score measuring your progress in completing actions that help reduce risks around data protection and regulatory standards. It calculates how much points you can achieve vs how much you already achieved.

In **Improvement actions** you can find actions that you can take to improve your compliance score. Please note that points may take up to 24 hours to update. If you click on Filter on the right side, you can filter recommendations based on assessment or based by solution that has some improvement action.
Click on any improvement action. You will get new view with details about that specific action as well as instructions how to implement it. You can also add implementation notes so that you can have information later what you changed in that specific improvement action, as well as upload document related to that improvement action.

In **Solutions** you can see how solutions are contributing to your score (Azure AD, Audit, Cloud App Security, Exchange, Data Loss Prevention,…) and how many points they can bring in regards to Compliance Score as well what improvement actions are connected to those solutions.

Assessments help you implement data protection controls specified by compliance, security, privacy, and data protection standards, regulations, and laws. **Data Protection Baseline** is standard assessment that comes with Office 365. When you click and open it, you can check details like assessment progress, controls, improvement actions, as well as actions already completed by Microsoft. Open each one and examine content.

You can also add new assessment from **Assessment**

1. Go to https://compliance.microsoft.com/, click on **Compliance Manager -> Assessments -> Add assessment**
2. Select **Template** (**EU GDPR**) and click **Next**
3. Enter name (**GDPR)** and choose assessment group (Default one) and click **Next**
4. Click on **Create assessment**

5. When created, go over assessment details and see what steps you need to do to make organization more compliant. Try closing few actions and see how it affects your compliance score.

In **Assessment templates** you can examine each assessment for details before turning it on for you organization, as well as create your own assessment template based on your organizational needs.

On the right side of Compliance Manager you can click on **Compliance Manager settings**. In it, you can set up automated testing for your Compliance Manager improvement actions that are also monitored by Secure Score. Choose to turn on automated testing for all such actions, turn off for all actions, or turn on for individual actions. You can also use these settings to manage the data of users who work with improvement actions. You can export a report of user data, delete user data, and reasign improvement actions to different users.

Try implementing few improvement actions and see how it affects your Compliance Score.

Disclaimer: Recommendations from Compliance Manager should not be interpreted as a guarantee of compliance. It is up to you to evaluate and validate the effectiveness of customer controls per your regulatory environment. These services are subject to the terms and conditions in the Online Services Terms. See also Microsoft 365 licensing guidance

Microsoft Compliance Configuration Analyzer for Compliance Manager (preview)

The Microsoft Compliance Configuration Analyzer (MCCA) is a tool that can help you get started with Microsoft Compliance Manager. MCCA is a PowerShell-based utility that will fetch your organization's current configurations and validate them against Microsoft 365 recommended best practices. These best practices are based on a set of controls that include key regulations and standards for data protection and data governance.

1. Open PowerShell with admin privileges
2. Run command
   Install-Module -Name MCCAPreview
3. Run command
   Get-MCCAReport
   You'll need to sign in to get access to report
4. Once the report is made, you can open it and examine. Location of report is
   C:\Users<username>\AppData\Local\Microsoft\MCCA

The Solutions Summary section of the report gives an overview of improvement actions that your organization can take in Compliance Manager to help improve your compliance posture. MCCA evaluates your current configurations against the recommended improvement actions in Compliance Manager. Any improvement action identified by the MCCA tool as needing attention will be listed in this section.

Analyze report and it's data. Try to follow few instructions. You can also print report (top right corner) if needed.

Please note that this is a preview version of MCCA! Preview versions may contain errors which could result in an incorrect report. Verify the results and any configuration before deploying changes.

GDPR Data Subject Request tool

The EU General Data Protection Regulation (GDPR) is about protecting and enabling individuals' privacy rights inside the European Union (EU). The GDPR gives individuals in the European Union (known as data subjects) the right to access, retrieve, correct, erase, and restrict processing of their personal data.

1. Go to https://compliance.office.com/, **Show all > Data subject requests**, and then click **New DSR case**
2. Enter **Name** and **Description**
3. Find person for whom you want to find data and click **Next**
4. Click **Save** and then click on **Show me search results**
5. It will take some time to find all data about the user, but once it finds, you can export results by clicking on **More** and click on **Export report**. Choose the options and click on **Generate report**
6. If you want, before generating report you can revise the built-in search queries (where it's searched and what is searched) – follow this document for more data - https://docs.microsoft.com/en-us/microsoft-365/compliance/manage-gdpr-data-subject-requests-with-the-dsr-case-tool?view=o365-worldwide

Information Barriers

Microsoft cloud services include powerful communication and collaboration capabilities. But suppose that you want to restrict communications between two groups to avoid a conflict of interest from occurring in your organization. Or, perhaps you want to restrict communications between certain people inside your organization in order to safeguard internal information. Microsoft 365 enables communication and collaboration across groups and organizations, so is there a way to restrict communications among specific groups of users when necessary? With information barriers, you can!

1. Run PowerShell command below, sign in with admin credentials, and in the **Permissions requested** dialog box, review the information, and then choose **Accept**
   ```
   Connect-AzureAD
   $appId="bcf62038-e005-436d-b970-2a472f8c1982"
   $sp=Get-AzADServicePrincipal -ServicePrincipalName $appId
   if ($sp -eq $null) { New-AzADServicePrincipal -ApplicationId $appId }
   Start-Process
   "https://login.microsoftonline.com/common/adminconsent?client_id=$appId"
   ```
2. Now we need to make segments
   a. Segment Management
      ```
      New-OrganizationSegment -Name "Management" -UserGroupFilter "MemberOf -eq
      'management@xyz.OnMicrosoft.com'"
      ```
   b. Segment Purchasing
      ```
      New-OrganizationSegment -Name "Purchasing" -UserGroupFilter "MemberOf -eq
      'purchasing@xyz.OnMicrosoft.com'"
      ```
3. Now we will define information barrier policy so that Purchasing cannot speak with Management and vice versa
   ```
   New-InformationBarrierPolicy -Name "Purchasing-Management" -AssignedSegment
   "Purchasing" -SegmentsBlocked "Management" -State Inactive

   New-InformationBarrierPolicy -Name "Management- Purchasing" -AssignedSegment
   "Management" -SegmentsBlocked "Purchasing" -State Inactive
   ```

4. Now we need set policy to active
    a. First we need to get GUID
       Get-InformationBarrierPolicy
    b. We copy GUID and run following PoerShell
       Set-InformationBarrierPolicy -Identity GUID -State Active
    c. Now we need to start policy
       Start-InformationBarrierPoliciesApplication

Allow at least 30 minutes after applying to make them active in tenant. Try using users from groups above to speak with each other in Teams.

Now make your own policy following instructions above but making that HR can only speak to Management. You need to change steps 2 and 3 in above steps. For step 2 you need to create new segment HR. For step 3 please follow this instruction
https://docs.microsoft.com/en-us/microsoft-365/compliance/information-barriers-policies?view=o365-worldwide#scenario-2-allow-a-segment-to-communicate-only-with-one-other-segment
New-InformationBarrierPolicy -Name "HR-Management" -AssignedSegment "HR" -SegmentsAllowed "Management","HR" -State Inactive

Insider Risk Management

Insider risk management is a solution in Microsoft 365 that helps minimize internal risks by enabling you to detect, investigate, and take action on risky activities in your organization. Custom policies allow you to detect and take action on malicious and inadvertent risk activities in your organization, including escalating cases to Microsoft Advanced eDiscovery if needed.

1. First go to https://protection.office.com/permissions, and give to the admin user one of the following permissions: Insider Risk Management, Insider Risk Management Admin, Insider Risk Management Analysts, or Insider Risk Management Investigators (click for admin permissions description)
2. Now go to https://compliance.microsoft.com/, click on Show more and choose **Insider risk management**
3. Click **on Insider risk settings** (gear icon) and under **Policy indicators** select all and click **Save**
4. Go back to https://compliance.microsoft.com/ > **Policies** > **Create policy**
5. Enter **Name** and **Description**
6. In **Data leaks** choose **General data leaks** and click **Next**
7. Check next to **All users and mail-enabled groups** and click **Next**
8. Click on **Choose sensitivity labels** and choose created label **Internal**
9. Choose **DLP policy** we created (**PCI DSS)**, for indicators choose all and click on **Next**
10. In **Policy timeframes** don't change anything and click **Next**
11. Review and click on **Submit**

To test save some of files containing PCI DSS data on SharePoint online. Try sharing with test account outside organization. Try to send those documents via email to people outside tenant. Use Edge Chromium to copy files to personal cloud storage. Print documents. Copy files to USB.
Go to Alerts and check what's happening. Go on Cases tab and explorer cases created.

Create priority group in Insider Risk management portal (in Insider Risk settings pane) and when creating policy choose Data leaks by priority users. You can choose one of Sensitive info types available and test policy on them. After making changes, make alerts and inspect them.

eDiscovery in Microsoft 365

Electronic discovery, or eDiscovery, is the process of identifying and delivering electronic information that can be used as evidence in legal cases. You can use eDiscovery tools in Microsoft 365 to search for content in Exchange Online mailboxes, Microsoft 365 Groups, Microsoft Teams, SharePoint Online and OneDrive for Business sites, and Skype for Business conversations, and Yammer teams. You can search mailboxes and sites in the same eDiscovery search by using the Content Search tool. And you can use Core eDiscovery cases to identify, hold, and export content found in mailboxes and sites.

Core eDiscovery

You can use a Core eDiscovery case to create holds to preserve content that might be relevant to the case. You can place a hold on the Exchange mailboxes and OneDrive for Business accounts of people you're investigating in the case. You can also place a hold on the mailboxes and sites that are associated with Microsoft Teams, Office 365 Groups, and Yammer Groups. When you place content locations on hold, content is preserved until you remove the hold from the content location or until you delete the hold.

1. Go to https://compliance.microsoft.com/ **-> eDiscovery -> Core -> +Create a case**
2. Enter case name (eDiscovery example) and click **Save**
3. Choose **eDiscovery example** case and click on **Open case**
4. Choose **Holds** and click on **+Create**
5. As name enter **Example1 and click Next**
6. In **Choose users, groups, or teams** choose for a user or group
7. In **Choose sites** and add one site (you'll have to copy site URL)
8. Click on **Next**
9. Enter **Keyword** that you want search for or **Condition** like data, sender/author, received, to, compliance label,…
10. Click on **Next** and then on **Create this hold**

Test this on your own, adding keywords and sending emails by specific user, creating documents with keyword in it. Try deleting those document. See what's happening.

After a Core eDiscovery case is created and people of interest in the case are placed on hold, you can create and run one or more searches for content relevant to the case. Searches associated with a Core eDiscovery case aren't listed on the Content search page in the Microsoft 365 compliance center. These searches are listed on the Searches page of the Core eDiscover case the searches are associated with. This also means that searches associated with a case can only be accessed by case members.

1. Go to https://compliance.microsoft.com/ **-> eDiscovery example -> Open case**
2. Choose **Search -> New Search**
3. Enter **Keyword** or add **Conditions**, choose **Location/s** and click on **Save & run**

You'll see all data from your hold created above from users and/or groups.

After a search is successfully run, you can export the search results. When you export search results, mailbox items are downloaded in PST files or as individual messages. When you export content from SharePoint and OneDrive for Business sites, copies of native Office documents and other documents are exported. A Results.csv file that contains information about every item that's exported and a manifest file (in XML format) that contains information about every search result is also exported.

1. Go to https://compliance.microsoft.com/ **-> eDiscovery example -> Open case**

2. Choose **Exports** and Export Search that was run above. Explore your data!

Communication Compliance

Communication compliance is a insider risk solution in Microsoft 365 that helps minimize communication risks by helping you detect, capture, and act on inappropriate messages in your organization. Pre-defined and custom policies allow you to scan internal and external communications for policy matches so they can be examined by designated reviewers. Reviewers can investigate scanned email, Microsoft Teams, Yammer, or third-party communications in your organization and take appropriate actions to make sure they're compliant with your organization's message standards.

1. First go to https://protection.office.com/permissions, and give to the admin user one of the following permissions: Communication Compliance Admin, Communication Compliance Analysis, Communication Compliance Investigation, Communication Compliance Viewer, or Communication Compliance Case Management (click for admin permissions description)
2. Now go to https://compliance.microsoft.com/, click on **Show all** and choose **Communication compliance**
3. Click on **Policies > Create policy > Monitor for sensitive info**
4. In **Users or groups to supervise** choose Sales group, and for **Reviewers** leave Admin
5. In **Keyword dictionary** choose **Credit Card Number** and click on **Create policy**

Test

It can take up to 24 hours to start detecting communication, so after 24 hours share credit card numbers internally via Teams and emails. Return to https://compliance.microsoft.com/ and go to Communication compliance and choose Alerts – find one of the alerts and analyze it.

Go to Notice templates and create one template.

Now go back to Alerts and check policy violations. Choose one alert and send notification to that user. Log-in as that user and check notification you received.

Create your own compliance policy for Offensive language and use English offensive language. Check Alerts and do the same as above. You can use your own keyword dictionary or to use trainable classifiers.