

# Fresh Tenant Setup

These are the steps I typically take to set up a fresh M365 E5 tenant.

## Work in Progress

This is very much a continuous work in progress. I publish changes as I go. Screenshots might be out of date.

## Use at your own risk

These are my personal steps. This should not be construed as official guidance. Always refer to the official Microsoft documentation available at [learn.microsoft.com](https://learn.microsoft.com)

## Entra

### Entra Cloud Sync

 [Portal](#)  [Docs](#)

Cloud Sync is the lightweight replacement for AAD Connect. Follow the instructions in the Docs link for a step-by-step example for a single forest install.

For conditional access, be sure to exclude the Directory Synchronization Accounts role from any MFA policies.

### Hybrid Cloud Trust

 [Docs](#)

#### Create EntraID Kerberos Server

```
# Install the AzureADHybridAuthenticationManagement module
Install-Module -Name AzureADHybridAuthenticationManagement -AllowClobber

# Specify the on-premises Active Directory domain. A new Azure AD
# Kerberos Server object will be created in this Active Directory domain.
$domain = "contoso.com"
```

```

# Enter a UPN of an Azure Active Directory global administrator
$UserPrincipalName = "admin@contoso.com"

# Enter a domain administrator username and password.
$DomainCred = Get-Credential

# Create the new Azure AD Kerberos Server object in Active Directory
# and then publish it to Azure Active Directory.
# Open an interactive sign-in prompt with given username to access the Azure
AD.
Set-AzureADKerberosServer -Domain $domain -UserPrincipalName
$UserPrincipalName -DomainCredential $DomainCred

# Verify server
Get-AzureADKerberosServer -Domain $domain -DomainCredential $DomainCred -
UserPrincipalName $UserPrincipalName

Id : 17530
UserAccount : CN=krbtgt_AzureAD,CN=Users,DC=contoso,DC=com
ComputerAccount : CN=AzureADKerberos,OU=Domain
Controllers,DC=contoso,DC=com
DisplayName : krbtgt_17530
DomainDnsName : contoso.com
KeyVersion : 27591
KeyUpdatedOn : 10/13/2022 9:23:43 PM
KeyUpdatedFrom : CONTOSO-DC-01.contoso.com
CloudDisplayName : krbtgt_17530
CloudDomainDnsName : contoso.com
CloudId : 17530
CloudKeyVersion : 27591
CloudKeyUpdatedOn : 10/13/2022 9:23:43 PM
CloudTrustDisplay :

```

## Device Settings

 [Portal](#)

- Disable adding GA to local admin.

## Microsoft Entra join and registration settings

Users may join devices to Microsoft Entra ⓘ

☒ All ☐ Selected ☐ None

Selected

No member selected


Users may register their devices with Microsoft Entra ⓘ

☐ All ☐ None

[Learn more on how this setting works](#)

Require Multifactor Authentication to register or join devices with Microsoft Entra ⓘ

☐ Yes ☒ No

 We recommend that you require Multifactor Authentication to register or join devices with Microsoft Entra using [Conditional Access](#). Set this device setting to No if you require Multifactor Authentication using Conditional Access.

Maximum number of devices per user ⓘ

50 

## Local administrator settings

Global administrator role is added as local administrator on the device during Microsoft Entra join (Preview) ⓘ

☐ Yes ☒ No

Registering user is added as local administrator on the device during Microsoft Entra join (Preview) ⓘ

☒ All ☐ Selected ☐ None

Selected

No member selected

[Manage Additional local administrators on all Microsoft Entra joined devices](#)

Enable Microsoft Entra Local Administrator Password Solution (LAPS) ⓘ

☒ Yes ☐ No

## Other settings

Restrict users from recovering the BitLocker key(s) for their owned devices ⓘ

☐ Yes ☒ No

## App Registrations

### MS Graph PowerShell SDK

To enable use of the [MS Graph PowerShell SDK](#), create an app registration for app-only for use with the SDK.

 [Portal](#)

1. Create the app registration.

#### Register an application ...

##### \* Name

The user-facing display name for this application (this can be changed later).

MS Graph PowerShell SDK



##### Supported account types

Who can use this application or access this API?

- ☒ Accounts in this organizational directory only (chrisbues.ms only - Single tenant)
- ☐ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)
- ☐ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- ☐ Personal Microsoft accounts only

[Help me choose...](#)

##### Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web



http://localhost



2. Grant application permissions for Microsoft Graph that are necessary for your use cases.
3. I prefer to do app consent cert-based authentication. Here's a couple of links explaining the process:


- a. [How to use Connect-MgGraph - All Options – LazyAdmin](#)
- b. [Use app-only authentication with the Microsoft Graph PowerShell SDK | Microsoft Learn](#)

## Identity Protection

### Self Service Password Reset


 [Portal](#)  [Docs](#)

- Enable Self service password reset
- Target a group that excludes service accounts. Easiest way to do this is with a dynamic group. Example rule: `(user.displayName -ne "On-Premises Directory Synchronization Service Account") and (user.userPrincipalName -notStartsWith "svc")`
- Enable Password writeback in On-premises integration

 **Password reset** | On-premises integration ...








chrisbues.ms

« ✔ We detected an agent has been configured. Password writeback can now be enabled

 Diagnose and solve problems



---

**Manage**

-  Properties
-  Authentication methods
-  Registration
-  Notifications
-  Customization
-  On-premises integration
-  Administrator Policy


---

**Activity**

-  Audit logs
-  Usage & insights

---

**Troubleshooting + Support**

-  New support request

Microsoft Entra Connect Sync agent  
Status: ● Not detected

Microsoft Entra Connect provisioning agent (cloud sync)  
Status: ● Set up complete  
[View details](#)

**Manage settings**

- ☒ Enable password write back for synced users ⓘ
- ☒ Write back passwords with Microsoft Entra Connect cloud sync ⓘ
- ☒ Allow users to unlock accounts without resetting their password? ⓘ

## Authentication Methods

 [Portal](#)  [Docs](#)

### POLICIES

For methods, enable

- Passkeys

- Authenticator

Enable and Target Configure

Note: Users must be included as part of the Microsoft Authenticator targeted groups under the 'Enable and Target' tab.

GENERAL

Allow use of Microsoft Authenticator OTP ☐ Yes ☒ No

**Require number matching for push notifications**

Note: This feature has been enabled for all users of the Microsoft Authenticator. [Learn more](#)

Status

Target Include

- ☒ All users  
☐ Select group

**Show application name in push and passwordless notifications**

Note: If the feature status is set to Microsoft-managed, it will be enabled by Microsoft at an appropriate time after the preview. [Learn more](#)

Status

Target Include Exclude

- ☒ All users  
☐ Select group

**Show geographic location in push and passwordless notifications**

Note: If the feature status is set to Microsoft-managed, it will be enabled by Microsoft at an appropriate time after the preview. [Learn more](#)

Status

Target Include Exclude

- ☒ All users  
☐ Select group

**Microsoft Authenticator on companion applications**

Note: If the feature status is set to Microsoft-managed, it will be enabled by Microsoft at an appropriate time after the preview. [Learn more](#)

Status

Target Include Exclude

- ☒ All users  
☐ Select group

- Temporary Access Pass

AUTHENTICATION METHODS MIGRATION

Optional - may not be necessary in newer tenants. If you see Migration status: Complete, you can skip this.

Migration status

✔ Complete ([change](#))


- Disable verification options in the [legacy MFA settings portal](#)


Methods available to users:

- ☐ Call to phone
- ☐ Text message to phone
- ☐ Notification through mobile app
- ☐ Verification code from mobile app or hardware token

Disabling all authentication methods could lock out your users. Ensure that you have enough authentication methods enabled in the new authentication methods policy before saving. [Learn more](#)

- Disable Authentication methods in [SSPR Authentication Methods](#)

 Authentication Methods for SSPR and Signin can now be managed in one converged policy. [Learn more](#)

Number of methods required to reset 

☒ 1 ☐ 2

Before saving, confirm that your users have enough methods enabled across this policy and the new authentication methods policy to register for SSPR. [Learn more](#)

Methods available to users

- ☐ Mobile app notification
- ☐ Mobile app code
- ☐ Email
- ☐ Mobile phone
- ☐ Office phone
- ☐ Security questions

- Migrate to the [Converged Authentication Methods Policy](#)

## Manage migration



On September 30th, 2025, the legacy multifactor authentication and self-service password reset policies will be deprecated and you'll manage all authentication methods here in the authentication methods policy. Use this control to manage your migration from the legacy policies to the new unified policy.

[Learn more](#) 

☐ Pre-migration:

Use policy for authentication only, respect legacy policies.

☐ Migration In Progress:

Use policy for authentication and SSPR, respect legacy policies.

☒ Migration Complete:

Use policy for authentication and SSPR, ignore legacy policies.

## User Settings

### Portal


- Toggle Off
- Users can register Applications
- Show keep user signed in
- Toggle On
- Restrict non-admin users from creating tenants



- Restrict access to Entra ID administration portal


### Default user role permissions

[Learn more](#) 

Users can register applications 


☐

No

Restrict non-admin users from creating tenants 

☒


Yes


Users can create security groups 

☒

Yes

### Guest user access

[Learn more](#) 

Guest user access restrictions 


☐ Guest users have the same access as members (most inclusive)

☒ Guest users have limited access to properties and memberships of directory objects

☐ Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)

### Administration portal

[Learn more](#) 


Restrict access to Microsoft Entra ID administration portal 

☒

Yes

### LinkedIn account connections

[Learn more](#) 


Allow users to connect their work or school account with LinkedIn  \*

☒ Yes

☐ Selected group

☐ No

### Show keep user signed in

Show keep user signed in 

☐

No

## User Feature Settings

 [Portal](#)

- Select All for Users can use preview features for My Apps

## Device Settings

### Cloud LAPS

 [Portal](#)  [Docs](#)

- Enable LAPS

Enable Microsoft Entra Local Administrator Password Solution (LAPS) ⓘ

☒ Yes ☐ No

### Enterprise State Roaming

 [Portal](#)

- Enable Enterprise State Roaming



## Devices | Enterprise State Roaming ...

chrisbues.ms - Microsoft Entra ID



Save



Discard



Got feedback?



Overview



All devices

#### Manage



Device settings



Enterprise State Roaming



BitLocker keys (Preview)



Local administrator password  
recovery

Users may sync settings and app data across devices ⓘ

☒ All

☐ Selected

☐ None

#### Selected

No member selected

## Identity Protection

### Multifactor authentication registration policy


- Create a EntraID group called Service Accounts, add any service accounts that should be excluded from MFA registration

- Enable the policy, targeting all users and excluding the group you just created.

Policy Name

Multifactor authentication registration policy

Assignments

 Users

All users included and 1 group excluded

Controls

☒ Require Microsoft Entra ID multifactor authentication registration

Include

Exclude

Select the users and groups to exclude from this policy

Select excluded users and groups

1 group

SA

Service Accounts

...

 Multifactor authentication registration policy only affects cloud-based Azure multifactor authentication. If you have multifactor authentication server it will not be affected.

Policy enforcement

Enabled

Disabled

### Diagnostic Settings

 [Portal](#)  [Docs](#)

Prior to doing so, create a Log Analytics workspace and add Sentinel to it.

- Enable all diagnostic settings to log to your Sentinel's log analytics workspace

**Diagnostic setting** ...

Save

Discard

Delete

Feedback

A diagnostic setting specifies a list of categories of platform logs and/or metrics that you want to collect from a resource, and one or more destinations that you would stream them to. Normal usage charges for the destination will occur. [Learn more about the different log categories and contents of those logs](#)

Diagnostic setting name      AzureSentinel\_security

Logs

Categories

☒ SignInLogs

☒ AuditLogs

☒ NonInteractiveUserSignInLogs

☒ ServicePrincipalSignInLogs

☒ ManagedIdentitySignInLogs

☒ ProvisioningLogs

☒ ADFSSignInLogs

☒ UserRiskEvents

☒ RiskyUsers

☒ NetworkAccessTrafficLogs

☒ RiskyServicePrincipals

☒ ServicePrincipalRiskEvents

☒ EnrichedOffice365AuditLogs

☒ MicrosoftGraphActivityLogs

Destination details

☒ Send to Log Analytics workspace

Subscription

Log Analytics workspace

☐ Archive to a storage account

☐ Stream to an event hub

☐ Send to partner solution

Global Secure Access


Portal Docs

Enable GSA


# Click Activate to enable GSA in your tenant

[Home](#) > [Authentication methods | Policies](#) > [chrisbues.ms](#) >



## Welcome to Global Secure Access ...

 Global Secure Access is now generally available. Licensing requirements have been updated. [Learn more](#)


Activate the Global Secure Access, which includes Microsoft Entra Internet Access and Microsoft Entra Private Access. [Learn more](#)



### 1. Global Secure Access prerequisites

-  You have the required administrator role to activate the Global Secure Access.
-  You have the required license to start using Global Secure Access


A Global Secure Access Administrator, Security Administrator, or Global Administrator must be assigned to activate and manage Global Secure Access features [Learn more](#)



### 2. Activate Global Secure Access in your tenant

To activate Global Secure Access, click the activate button below. Note activation will not impact any workload in your tenant until preview features are enabled.

[Activate](#)



### 3. Get started with Global Secure Access

Learn about Global Secure Access and the next steps for getting started.


[Get Started](#)

## Internet Access

### 1. Enable the Microsoft Profile

[Home](#) > [Get started](#) > [chrisbues.ms](#) >

## Traffic forwarding ...

 Global Secure Access is now generally available. Licensing requirements have been updated. [Learn more](#)



















Enabling this profile directs Global Secure Access clients to acquire traffic for this profile.

Are you sure you want to proceed?

[OK](#)

[Cancel](#)

Traffic forwarding profiles enable admins to forward specific traffic to Global Secure Access. Assign traffic forwarding profiles to users running the Global Secure Access client. For clientless devices, use the Microsoft profile to assign to remote networks. [Learn more](#)

<div><div></div><div><div>Microsoft traffic profile</div><div>Disabled</div><div>Last modified on 08/15/2024, 11:42 PM</div></div></div> <div><div> Applies to</div><div>Internet traffic to Microsoft services</div></div> <div><div> Microsoft traffic policies</div><div>3 policies <a href="#">View</a></div></div> <div><div> Linked Conditional Access policies</div><div>None</div></div> <div><div> User and group assignments</div><div>0 users, 0 groups assigned <a href="#">View</a></div></div> <div><div> Remote network assignments</div><div>0 assigned remote networks <a href="#">View</a></div></div>	<div><div></div><div><div>Private access profile</div><div>Disabled</div><div>Last modified on 08/15/2024, 11:42 PM</div></div></div> <div><div> Applies to</div><div>Private resources</div></div> <div><div> Private access policies</div><div>Quick Access, 0 Applications</div></div> <div><div> Linked Conditional Access policies</div><div>None</div></div> <div><div> User and group assignments</div><div>0 users, 0 groups assigned <a href="#">View</a></div></div> <div><div> Remote network assignments</div><div>Not applicable</div></div>	<div><div></div><div><div>Internet access profile</div><div>Disabled</div><div>Last modified on not available</div></div></div> <div><div> Applies to</div><div>All internet traffic, except for the Microsoft traffic profile</div></div> <div><div> Internet access policies</div><div>3 policies <a href="#">View</a></div></div> <div><div> Linked Conditional Access policies</div><div>None</div></div> <div><div> User and group assignments</div><div>0 users, 0 groups assigned <a href="#">View</a></div></div> <div><div> Remote network assignments</div><div>Not applicable</div></div>
--	---	--

2. Download the [GSA Client](#) and deploy to Windows devices.

## Active Directory

Deploy 3 VMs

- 2 Domain Controllers running 2022
- 1 2022 Server for Entra Cloud Sync

## Intune

### Tenant Administration Settings

#### Windows Data Connector

[Portal](#)

##### Windows data

Some Intune features, including Windows update reports, require sharing Windows diagnostic data with Intune. [Learn more about features that require Windows diagnostic data](#)

Enable features that require Windows diagnostic data in processor configuration ⓘ




##### Windows license verification

Some Intune features require specific Windows licensing to use them. Features including the Windows 11 Upgrade Readiness report and Remediations require Windows license verification.

If you want to use these features, confirm your tenant has one of the following licenses:

- Windows 10 or later Enterprise E3 or E5; or Microsoft 365 F3, E3, or E5
- Windows 10 or later Education A3 or A5; or Microsoft 365 A3 or A5
- Windows Virtual Desktop Access E3 or E5

You must be a Global Administrator or Intune Service Administrator to confirm licenses. [Learn more about Roles in Endpoint Manager](#)

I confirm that my tenant owns one of these licenses.  On

#### Defender for Endpoint Connector

[Portal](#)

You need to enable the Defender side first.

## Endpoint Security Profile Settings

Allow Microsoft Defender for Endpoint to enforce Endpoint Security Configurations ⓘ

Off On

## Compliance policy evaluation

Connect Android devices version 6.0.0 and above to Microsoft Defender for Endpoint ⓘ

Off On

Connect iOS/iPadOS devices version 13.0 and above to Microsoft Defender for Endpoint ⓘ

Off On

Connect Windows devices version 10.0.15063 and above to Microsoft Defender for Endpoint ⓘ

Off On

Enable App Sync (sending application inventory) for iOS/iPadOS devices ⓘ

Off On

Send full application inventory data on personally owned iOS/iPadOS devices ⓘ

Off On

Block unsupported OS versions ⓘ

Off On

## App protection policy evaluation

Connect Android devices to Microsoft Defender for Endpoint ⓘ

Off On

Connect iOS/iPadOS devices to Microsoft Defender for Endpoint ⓘ

Off On

## Windows Autopatch

 Portal

 Docs

- Run the prereq check. You'll see an advisory for co-management, this can be safely disregarded.

[Home](#) > [Tenant admin](#) | [Tenant enrollment](#) >

### Management settings ...

[Export](#) [Run checks](#) ⓘ [Learn more about each check](#)

Last updated 9/11/2024, 3:51 PM

Readiness ↑↓	Setting ↑↓
⚠ Advisory	Co-Management
✅ Ready	Licenses
✅ Ready	Update rings for Windows 10 or later

### Co-Management ×

#### Readiness

⚠ Advisory

#### Reason

To successfully enroll in devices that are Co-Managed, it is necessary that the following Co-Managed workloads are switched to Intune.

1. Device Configuration
2. Windows Update policies
3. Office 365 Client Apps

#### How to remediate

Follow the steps described in [how to switch co-management workloads](#) for the above workloads.

Note: Should co-management not apply to your tenant this check can be safely disregarded and will not block deployment of devices.

- Grant admin access for Microsoft

## Allow administrator access for Microsoft

To get started, Microsoft needs your permission to take a few actions in your Microsoft Entra organization and on devices you want to enroll in Windows Autopatch. With your permission, Microsoft will do the following:

- Create a Microsoft application that we use to run the Windows Autopatch service. [Learn more about Windows Autopatch enterprise applications](#)
- Create the policies, groups and scripts necessary to run the service. This involves excluding Windows Autopatch device groups, where applicable, for any of your existing policies that may cause conflicts. Windows Autopatch update policies must take precedence to avoid any conflicts. [Learn more about Changes made at tenant enrollment](#)
- Manage devices using Intune.
- Collect and share info on usage, status, and compliance for devices and apps.
- Collect and share Windows Diagnostic data on usage, status, and compliance for devices and apps. [Learn more about the data we collect](#)
- Store Windows Autopatch data securely in Azure data centers based on your data residency. [Learn more about Windows Autopatch data storage](#)



I give Microsoft permission to manage my Microsoft Entra organization on my behalf.

Revoking this access at any point terminates the service.

Agree

- Provide Admin contact info.
- Add devices to the the default autopatch group **Windows Autopatch Device Registration**
- Wait a few minutes, then ensure the devices show in the Windows Autopatch devices [here](#)
- Put a couple of devices in the Test ring by clicking on the device name, then selecting Device Actions -> Assign Ring. In the flyout, choose the Test ring

The screenshot shows the Windows Autopatch management interface. On the left, a table lists registered devices. The first device, 'DESKTOP-KFH589M', is selected. A 'Device actions' menu is open, showing 'Assign ring' and 'Exclude device' options. On the right, the 'Assign ring' flyout is displayed, showing a dropdown menu with the selected ring: 'Windows Autopatch - Test: Modern Workplace Devices-Windows Autopatch-Test'. Below this, a table shows the details of the selected device.

Microsoft Entra device ID	Serial Number	Autopatch group	Deployment ring	Ring assigned by
8f42f67d-3977-4da2-88ea-5d0470cd1a98	PF30CCZG	Windows Autopatch	Test	Admin



## Applications

 [Portal](#)  [Docs](#)

## Windows

Add app -> Microsoft 365 Apps for Windows 10 and Later. Assign to all devices.

[Home](#) > [Apps | Windows](#) >

## Windows | Windows apps ...

[Add](#) [Refresh](#)

Filters applied: Platform, A

**Name** ↑↓

No applications found

## Select app type

Create app

App type

Windows 10 and later

Store app

Microsoft Store app (new)

Microsoft Store app (legacy)

Microsoft 365 Apps

Windows 10 and later

Microsoft Edge, version 77 and later

Windows 10 and later

## Add Microsoft 365 Apps ...

Microsoft 365 Apps (Windows 10 and later)

Select Office apps ⓘ 

8 selected

Select other Office apps (license required) ⓘ 

0 selected

### App suite information

These settings apply to all apps you have selected in the suite. [Learn more](#)

Architecture ⓘ 

32-bit 64-bit

Default file format \* 

Office Open Document Format

Update channel \* ⓘ 

Current Channel (Preview)

Remove other versions ⓘ 

Yes No

Version to install ⓘ 

Latest Specific

Specific version 

Latest version

### Properties

Use shared computer activation ⓘ 

Yes No

Accept the Microsoft Software License Terms on behalf of users 

Yes No

Install background service for Microsoft Search in Bing ⓘ 

Yes No

Languages ⓘ 

1 language(s) selected

## Devices




### Windows Automatic Enrollment

[Portal](#)

- Set MDM and MAM user scopes to all

## Configure ...

Microsoft Intune

 Save  Discard  Delete

---

MDM user scope ⓘ None Some **All**

MDM terms of use URL ⓘ  ✓

MDM discovery URL ⓘ  ✓

MDM compliance URL ⓘ  ✓

[Restore default MDM URLs](#)

MAM user scope ⓘ None Some **All**

MAM terms of use URL ⓘ  ✓

MAM discovery URL ⓘ  ✓

MAM compliance URL ⓘ  ✓

[Restore default MAM URLs](#)

## Windows Autopilot



Follow this guide: [Overview for Windows Autopilot device preparation user-driven Microsoft Entra join in Intune | Microsoft Learn](#)

Prereqs:

- Create Entra Groups
- Automatic Enrolment Set
- Enrolled devices. Windows Autopilot device preparation devices
  - Set App ID f1346770-5b25-470b-88bd-d5744ab7952c as the owner.
  - Targeted Users - Windows Autopilot device preparation users
- Create/update an Office deployment, target the device group created above.

Create a device prep policy

# Device Enrollment ...

Windows Autopilot device preparation policies

- ☒ Deployment settings
- ☐ Review + save

Deployment settings

^

Deployment mode ⓘ

User-driven

\*

Deployment type

Single user

\*

Join type ⓘ

Microsoft Entra joined

\*

User account type ⓘ

☒ Administrator

Out-of-box experience settings

^

Minutes allowed before showing installation error

30

Custom error message ⓘ

Contact your organization's support person for help.

\*

Allow users to skip setup after multiple attempts ⓘ

☒ Yes

Show link to diagnostics

☒ Yes

Apps

^

Select up to 10 managed apps you want to reference with this deployment. These apps should be assigned to the device security group you selected earlier. You can check the installation status for these apps in the device details for devices in this deployment.

+ Add — Remove

<input type="checkbox"/>	Allowed Applications ↑	Publisher	Version
<input type="checkbox"/>	Company Portal	Microsoft Corporation	
<input type="checkbox"/>	Microsoft 365 Apps for Windows 10 a...	Microsoft	

Scripts

^

Select up to 10 PowerShell scripts to install during this deployment. These scripts should be already assigned to the Device group selected earlier. You can check the installation status for these scripts in the device details for devices in this deployment.

[+ Add](#) [— Remove](#)

☐ **Allowed Scripts** ↑



### No values added

There are no values added. Click on the 'Add' command above to add a new value.

## iOS Enrollment

[Portal](#)

User-driven iOS enrollment is a two step process - the push certificate and the enrollment profile.

CONFIGURE APPLE MDM PUSH CERTIFICATE

[Docs](#)

# Configure MDM Push Certificate



Delete

## Essentials

Status	Days until expiration
Active	365
Last updated	Expiration
10/11/2023	10/10/2024
Apple ID	Subject ID
	com.apple.mgmt.External.
Serial number	

You need an Apple MDM push certificate to manage Apple devices with Intune.

### Steps:

- I grant Microsoft permission to send both user and device information to Apple. [More information on Microsoft permission.](#)  
☒ I agree.

- Download the Intune certificate signing request required to create an Apple MDM push certificate.  
[Download your CSR](#)

- Create an Apple MDM push certificate. [More information on Apple MDM push certificate.](#)  
[Create your MDM push Certificate](#)

- Enter the Apple ID used to create your Apple MDM push certificate.  
Apple ID \*

- Browse to your Apple MDM push certificate to upload  
Apple MDM push certificate \*

Upload

## ENROLLMENT PROFILE

Portal

### Native iOS enrollment

There's this nifty-keen **account driven user enrollment** available in iOS 15+, but you'll need a web server to serve up the json file Apple expects.

- Configure an enrollment profile
- Create a profile that allows user choice of type of device (corporate vs user), target all users.

[Home](#) > [Devices | Overview](#) > [iOS/iPadOS | iOS/iPadOS enrollment](#) > [Enrollment type profiles](#) >

## Create enrollment type profile ...

Apple enrollment

✓ Basics   ✓ **Settings**   ③ Assignments   ④ Review + create

If you require users to select their device type, personal devices will enroll with user enrollment, and corporate devices will enroll with device enrollment. If you don't require users to select their device type, devices will enroll with the selected default option.

[Learn more](#) about the differences between user enrollment and device enrollment.

Enrollment type \*

Determine based on user choice

### SUPERVISED IOS ENROLLMENT WITH APPLE CONFIGURATOR

[Portal](#) [Docs](#)

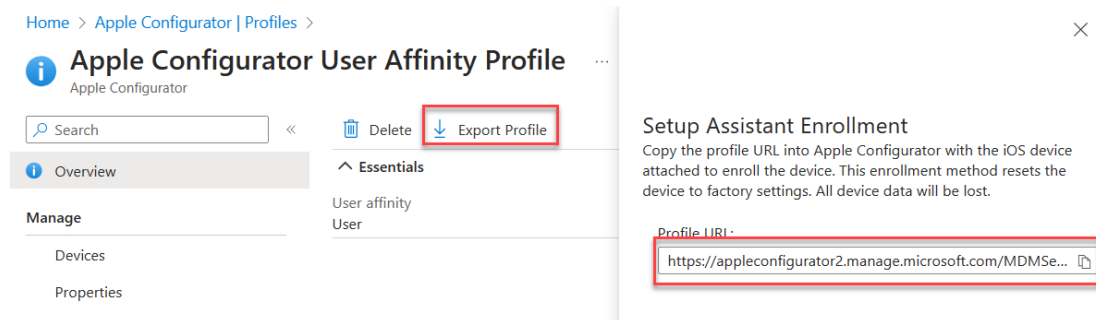
There are two options for Apple Config profile - with user affinity and without. For testing, enrollment with User Affinity with the Company Portal app mimics how devices might be distributed to end users.

1. Create a new Enrollment Profile. On the settings step, select:

User affinity: Enroll with User Affinity

Select where users must authenticate: Company Portal

2. Export the profile you just created. Copy the URL.



Home > Apple Configurator | Profiles >

### Apple Configurator User Affinity Profile

Apple Configurator

Search << Delete Export Profile

Overview

Manage

- Devices
- Properties

Essentials

User affinity

User

Setup Assistant Enrollment

Copy the profile URL into Apple Configurator with the iOS device attached to enroll the device. This enrollment method resets the device to factory settings. All device data will be lost.

Profile URL:

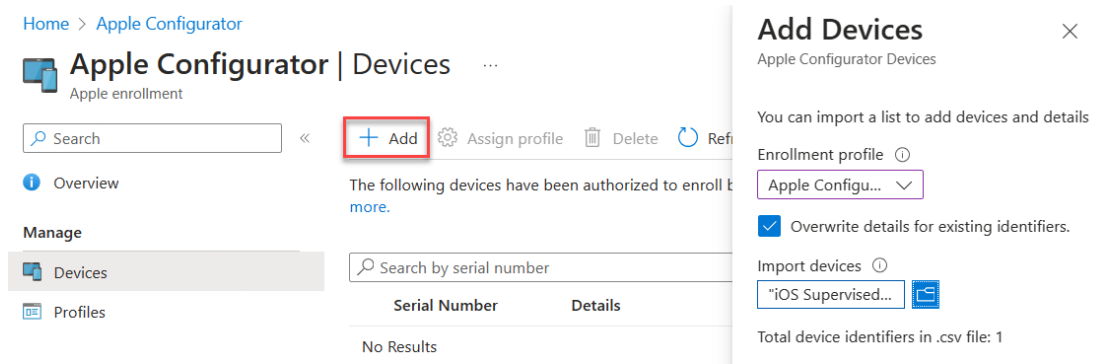
<https://appleconfigurator2.manage.microsoft.com/MDMSe...>

3. Create a csv file with the serial numbers of iPads you wish to enroll.

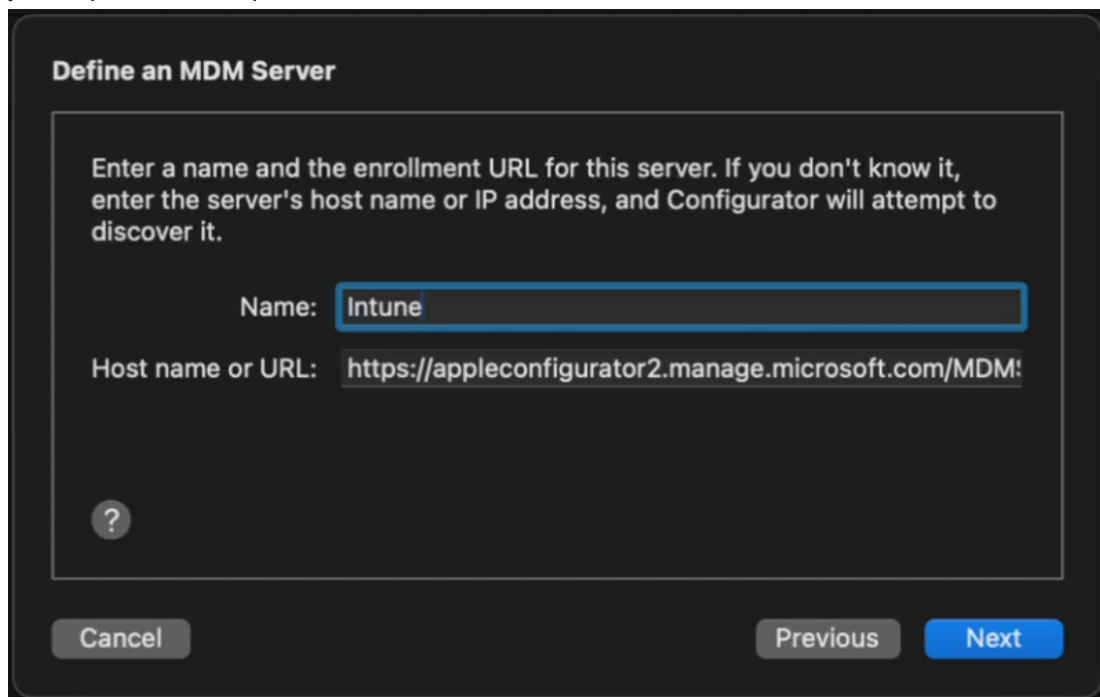
Serial number, device details



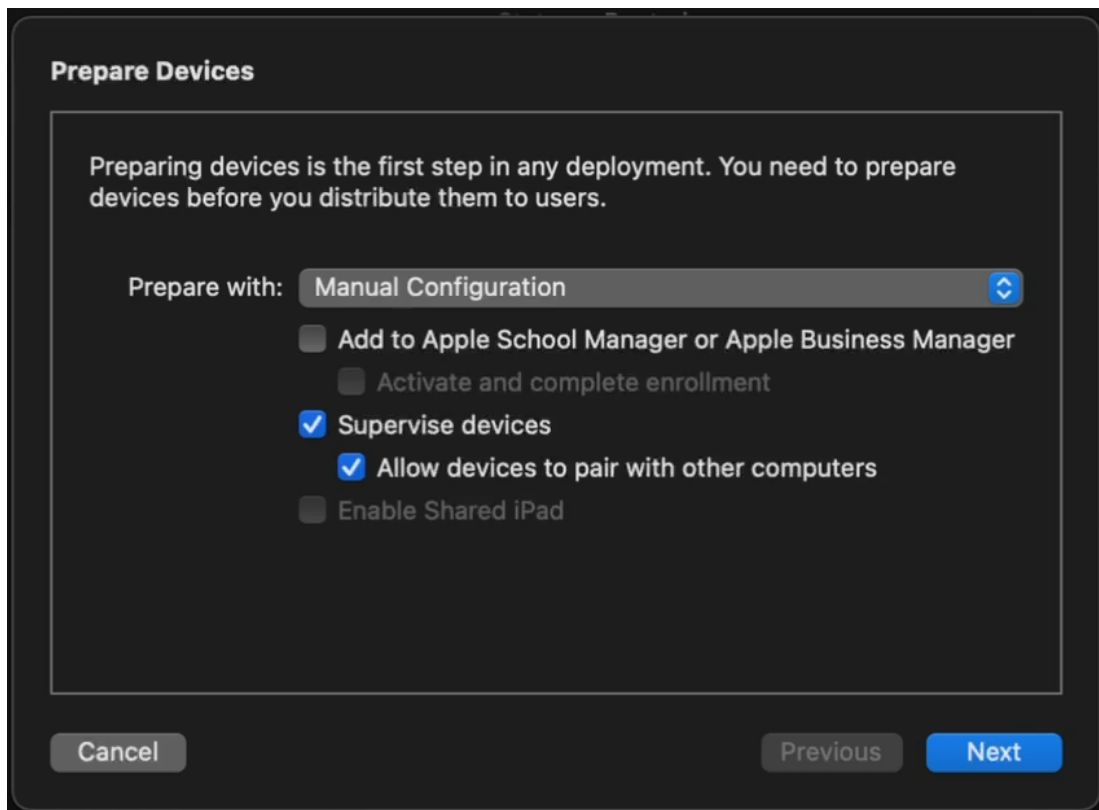
4. Upload the csv file in the portal under **Devices**. Assign the profile you just created.



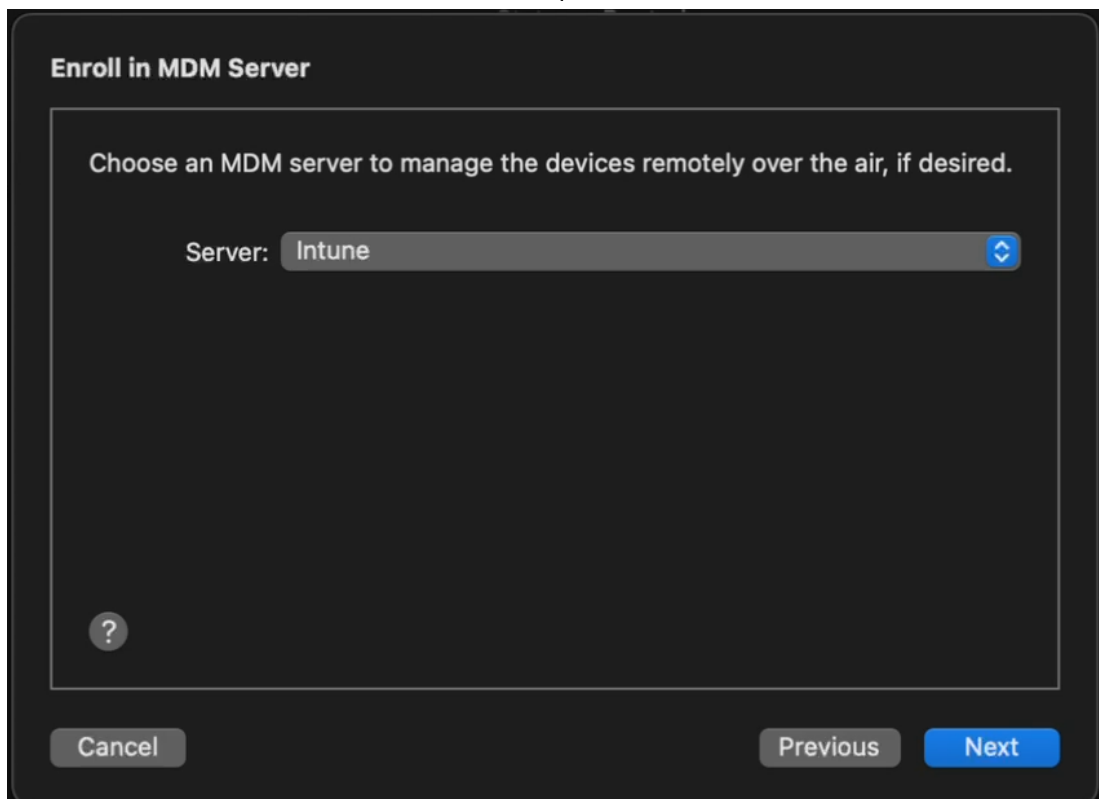
5. In Apple Configurator, choose Settings -> Servers. Click + to add a server. Add the URL you copied from step 2.



6. Connect a device, and at the main screen, click Prepare. Leave the default options unchanged.



7. Choose the Intune MDM server defined in Step 5.



8. Skip Apple Business Manager sign-in if prompted. At the Organization screen select a previous org or create a new one. This is shown in the settings app in iOS.

9. Choose to generate a new supervision Identity or reuse an existing one.

10. Choose which steps to display in the Setup Assistant. Click Prepare to start the process.

## Android Enrollment


 [Portal](#)  [Docs](#)

User-driven Android enrollment is a two step process - the managed Google Play account linking and the enrollment profile.

### MANAGED GOOGLE PLAY ACCOUNT LINKING




## Managed Google Play

Android enrollment

 Disconnect

---

^ Essentials

Status	Google account
 Setup	
Organization	Registration date
	10/11/2023, 11:54:46 AM

---

You must connect Intune to your company's managed Google Play account to manage Android enterprise devices. Follow the steps below to enable Android enterprise enrollment. [Learn more.](#)

1. I grant Microsoft permission to send both user and device information to Google. [Learn more.](#)

☒ I agree.

---

2. Connect your Intune tenant to an administrative Google account to enable Android enterprise enrollment.

Launch Google to connect now.

---

## MacOS Enrollment

 [Portal](#)  [Docs](#)

As with MDE for MacOS, this tends to change, so be sure to check the docs for the most recent steps.

:material-head-sync: tl;dr

- Create a MacOS enrollment profile [here](#) if you didn't for iOS yet - they're shared between iOS and MacOS.
- Download the Company Portal app for MacOS from [here](#) and deploy the company portal app as a MacOS LOB app

## App information [Edit](#)

Name	Company Portal
Description	CompanyPortal-Installer.pkg
Publisher	Microsoft
Category	No Category
Information URL	No Information URL
Privacy URL	No Privacy URL
Developer	No Developer
Owner	No Owner
Notes	No Notes
Logo	No logo

## Program [Edit](#)

Pre-install script	No Pre-install script
Post-install script	No Post-install script

## Requirements [Edit](#)

Minimum operating system	macOS Sonoma 14.0
--------------------------	-------------------

## Detection rules [Edit](#)

Ignore app version	Yes
Included apps	org.cocoapods.RxSwiftExt 6.2.1 org.cocoapods.AppleClientLogger 0.1.0 org.cocoapods.PowerLiftKit 5.2.0 org.cocoapods.Cache 5.2.0 com.microsoft.CPCore-PushNotifications-Mac 1.0 org.cocoapods.RxRelay 6.6.0 org.cocoapods.CocoaLumberjack 3.6.1 org.cocoapods.FluentIcons 1.1.136 org.cocoapods.FluentUI 0.2.10 org.cocoapods.Zip 2.1.1 org.cocoapods.MSAL 1.4.1 org.cocoapods.Alamofire 4.9.1 com.microsoft.AADNGCAuthenticationMacOS 1.0 com.microsoft.NGCKeyProviderMacOS 1.0 com.microsoft.MSAuthNetworkingMacOS 1.0.0 org.cocoapods.RxCocoa 6.6.0 com.microsoft.CommonFramework 1.0 org.cocoapods.RxSwift 6.6.0 com.microsoft.CompanyPortalMac 5.2409.1 com.microsoft.autoupdate2 4.74

## Assianments [Edit](#)

Group mode	Group
✓ Required	
⊕ Included	All devices
Available for enrolled devices	

## MacOS Platform SSO

Use the instructions [here](#) as a guide.

tl;dr

Use the settings below in a config profile to deploy platform sso with the following options:

- Password authentication which syncs the Entra password with the local account password
- Create new users as admins

## Extensible Single Sign On (SSO)

Remove subcategory

Configure an app extension that enables single sign-on (SSO) for devices.

32 of 47 settings in this subcategory are not configured

Authentication Method (Deprecated) Password

Extension Identifier com.microsoft.CompanyPortalMac.ssoextension

### Platform SSO

Authentication Method Password

Enable Create User At Login Enabled

New User Authorization Mode Admin

### Token To User Mapping

Account Name preferred\_username

Full Name name

Use Shared Device Keys Enabled

Registration Token {{DEVICEREGISTRATION}}

Screen Locked Behavior Do Not Handle

Team Identifier UBF8T346G9

Type Redirect

URLs

Delete Sort Import Export

- https://login.microsoftonline.com
- https://login.microsoft.com
- https://sts.windows.net

# Endpoint security

 Portal

## Windows

- Endpoint Detection and Response
- Create a new EDR policy targeting Windows. Target all devices.

Create a profile

×

Platform

Windows

▼

Profile

Endpoint detection and response

▼

### Endpoint detection and response

Microsoft Defender for Endpoint endpoint detection and response capabilities provide advanced attack detections that are near real-time and actionable. Security analysts can prioritize alerts effectively, gain visibility into the full scope of a breach, and take response actions to remediate threats

This policy applies to: Windows 10, Windows 11, and Windows Server

The settings in this policy can be targeted to: MDM, MicrosoftSense supported devices

## Create profile ...

Endpoint detection and response

- ✓ Basics

**2 Configuration settings**

③ Scope tags

④ Assignments

⑤ Review + create

^ Microsoft Defender for Endpoint

Microsoft Defender for Endpoint client configuration package type ⓘ

Auto from connector

▼

Sample Sharing ⓘ

All

▼

[Deprecated] Telemetry Reporting Frequency ⓘ

Not configured

▼

- Antivirus

- Create a new Microsoft Defender Antivirus profile

Create a profile

✕

Platform

Windows

Profile

Microsoft Defender Antivirus

Microsoft Defender Antivirus

Windows Defender Antivirus is the next-generation protection component of Microsoft Defender for Endpoint. Next-generation protection brings together machine learning, big-data analysis, in-depth threat resistance research, and cloud infrastructure to protect devices in your enterprise organization.

This policy applies to: Windows 10, Windows 11, and Windows Server

The settings in this policy can be targeted to: MDM, MicrosoftSense supported devices

- Enable Network Protection in Block mode. Target all devices.

- ✓ Basics

✓ Configuration settings

✓ Scope tags

✓ Assignments

● Review + create

Basics	^
Name	Windows Defender AV
Description	

Settings	^
Defender	
Enable Network Protection	Enabled (block mode)

Scope tags	^
Name	Description
Default	Default Role Scope Tag. This will exist by default on all Intune entities whenever a user ...

Assignments

Group

Target type

Filter

AD

All devices

Include



## MacOS

Deploying MDE on MacOS is a multi-step manual process, and changes occasionally. Refer to [Intune-based deployment for Microsoft Defender for Endpoint on Mac - Microsoft Defender for Endpoint | Microsoft Learn](#) for the most current steps.

🔗 tl;dr

If you want a sample combined deployment, I've combined mobileconfig files here to set the following settings

- AutoUpdate enabled, broad channel
- Network protection set to block
- All other required mobileconfig settings, such as full disk access, etc.
- Deploy the combined profile
- Create a device configuration profile for macOS devices using a custom template

### Create a profile



Platform

macOS

Profile type

Templates

Templates contain groups of settings, organized by functionality. Use a template when you don't want to build policies manually or want to configure devices to access corporate networks, such as configuring WiFi or VPN. [Learn more](#)

Search by profile name

Template name

Custom ⓘ

- For configuration settings, upload the mobileconfig from above. Target device channel.
- Target all MacOS devices
- Deploy MDE
- Deploy the [MDE packageMDE App in Intune](#)
- Deploy the Onboarding Package

- Download the MDM/Intune onboarding package from [Defender XDR](#)

Select operating system to start onboarding process:

macOS

Onboard macOS devices through Microsoft Defender

## 1. Install the agent and onboard a device

Connectivity type

Streamlined

This package allows devices to onboard using [streamlined connectivity method](#). Check devices you onboard meet specific prerequisites. Install the agent on the macOS device using the installation package, then onboard devices to Microsoft Defender using the configuration package that matches your [preferred deployment method](#). For other device preparation instructions, read [Onboard and set up](#).

**Note:** Streamlined connectivity is supported on MDE product version released in February 2024 and above.

Deployment method

Mobile Device Management / Microsoft ...

You can use Mobile Device Management solutions, such as Microsoft Intune to configure and monitor your devices. Before downloading the packages, review the [instructions](#).



Download installation package




Download onboarding package

- Deploy via Intune as a Custom Config template

✓ Basics
**2 Configuration settings**
③ Assignments
④ Review + create

Custom configuration profile name \* ①  ✓

Deployment channel \* ①  ▼

Configuration profile file \*  

```

1 <?xml version="1.0" encoding="utf-8"?>
2 <!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/Property
3 <plist version="1">
4   <dict>
5     <key>PayloadUUID</key>
6     <string>A27F524F-7A54-4E9A-B459-B50A321C4295</string>
7     <key>PayloadType</key>
8     <string>Configuration</string>
9     <key>PayloadOrganization</key>
10    <string>Microsoft</string>
11    <key>PayloadIdentifier</key>
12    <string>A27F524F-7A54-4E9A-B459-B50A321C4295</string>
13    <key>PayloadDisplayName</key>
14    <string>WDATP settings</string>
15    <key>PayloadDescription</key>
16    <string>WDATP configuration settings.</string>
17    <key>PayloadVersion</key>
18    <integer>1</integer>
19    <key>PayloadEnabled</key>
20    <true/>

```

## Security Baselines

- Create a new Microsoft Defender for Endpoint Baseline policy and target all devices.

Security baselines ...

Use security baselines to apply Microsoft-recommended security configuration settings to your enrolled devices. [Learn more.](#)

Security Baselines	↑↓ Last Published
 Security Baseline for Windows 10 and later	10/21/21, 12:00 AM
 Microsoft Defender for Endpoint Baseline	12/08/20, 12:00 AM
 Security Baseline for Microsoft Edge	05/24/23, 8:00 PM
 Windows 365 Security Baseline	10/20/21, 12:00 AM
 Microsoft 365 Apps for Enterprise Security Baseline	05/24/23, 8:00 PM

## Account Protection (LAPS)

 [Portal](#)

- Enable LAPS in the portal

- Create a Windows LAPS profile and apply to all devices.

Account protection

+ Create Policy

Refresh

Search by profile name

Policy name

↑↓

Policy type

No results

Create a profile

×

Platform

Windows 10 and later

Profile

Local admin password solution (Windows LAPS)

Local admin password solution (Windows LAPS)

Windows Local Administrator Password Solution(Windows LAPS) is a Windows feature that automatically manages and backs up the password of a local administrator account on your Azure Active Directory - joined or Windows Server Active Directory - joined devices.

[Home](#) > [Endpoint security](#) | [Account protection](#) >

## Create profile ...

Local admin password solution (Windows LAPS)

[✓ Basics](#) [2 Configuration settings](#) [3 Scope tags](#) [4 Assignments](#) [5 Review + create](#)

### ^ LAPS

Backup Directory ⓘ

Backup the password to Azure AD only

Password Age Days ⓘ

☒ Not configured

30

Administrator Account Name ⓘ

☒ Not configured

Password Complexity ⓘ

Not configured

Password Length ⓘ

☒ Not configured

Post Authentication Actions ⓘ

Not configured

Post Authentication Reset Delay ⓘ

☒ Not configured

## M365 Defender

[Portal](#)

XDR

- Enable unified SIEM and XDR.

## Get your SIEM and XDR in one place

Connect Microsoft Sentinel and Microsoft Defender XDR to unify your security operations in a single portal with more AI, automation, search, and threat intelligence.

Connect a workspace

## Email & collaboration

- Preset Security Configuration Policies
- Enable Standard Protection Preset Policies.

### Standard protection



A baseline protection profile that protects against spam, phishing, and malware threats.

- ✓ Balanced actions for malicious content
- ✓ Balanced handling of bulk content
- ✓ Attachment and link protection with Safe Links and Safe Attachments



Standard protection is off

### Manage protection settings

#### Apply Exchange Online Protection

Add the users, groups, and domains to protect using Exchange Online Protection capabilities, including inbound anti-spam, anti-malware, and anti-phishing. [Learn more about preset security policies](#)

Apply protection to:



All recipients



Specific recipients



None

## Apply Defender for Office 365 protection

Add the users, groups, and domains to protect using Defender for Office 365 capabilities, including Safe Attachments and Safe Links. [Learn more about preset security policies](#)

Apply protection to:

- ☐ Previously selected recipients
- ☒ All recipients
- ☐ Specific recipients
- ☐ None

## MDCA

- System
- IP Address Ranges
  - If you have IP Ranges as Trusted Named Locations in EID, add them as Custom IP Address Ranges in MDCA with the category of Corporate

### New IP address range

[Learn more](#)

Name \*

Type range name...

IP address ranges \*

For example: 192.168.1.1/32

Category \*

Corporate


Tags

Type to create a new tag...

Override automatic data enrichment ⓘ

☐ Override registered ISP

☐ Override location

 Only future events will be affected by the new or modified IP address range.

Create

Cancel

- Cloud Discovery
- Defender for Endpoint
  - Enforce App Access with Defender for Endpoint

#### Microsoft Defender for Endpoint Integration

☒ Enforce app access

Enabling this will Block access to apps that were marked as Unsanctioned and will deliver a Warning on access and allow bypass to apps marked as Monitored.

- User Enrichment

- Enable User Enrichment

#### User enrichment

User enrichment automatically matches, enriches and replaces discovered user identifiers with their Azure Active Directory username.

- ☒ Enrich discovered user identifiers with Azure Active Directory usernames.  
Enabling this after you uploaded data might result in user duplication.

- Information Protection

- Microsoft Information Protection

- Enable automatically scan new files
- Enable scanning protected files. You'll need to go through the OAUTH grant process.

#### Microsoft Information Protection settings

- ☒ Automatically scan new files for Microsoft Information Protection sensitivity labels and content inspection warnings  
When enabled, the App connector will scan new files, searching for sensitivity labels embedded by Microsoft Information Protection.
- ☐ Only scan files for Microsoft Information Protection sensitivity labels and content inspection warnings from this tenant  
When enabled, all Microsoft Information Protection sensitivity labels that were set by external tenants will be disregarded.

Get more info in the [Microsoft Information Protection integration guide](#).

Save

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

#### Inspect protected files

File policies can inspect content and/or read labels in Microsoft Information Protection protected files.  
To inspect protected files, read labels from protected files, grant Defender for Cloud Apps permission in Azure AD.

- ☒ **Active**  
Protected files can be inspected by file policies. [Learn more](#)

- Files

- Enable file monitoring

- ☒ **Enable file monitoring**  
This enables to see files in your SaaS apps.

- App governance

- Service Status

- Turn on app governance

Get comprehensive visibility and control over cloud apps that authenticate through Azure Active Directory, Google, and Salesforce. [Learn more about app governance](#)


☐ Use app governance

- Connected Apps


- App Connectors

- Click Connect an app, choose Microsoft 365 from the list. Select all options.


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

 To connect this app, provide your access credentials. We secure your data as described in the [privacy statement](#) | [Terms](#)


☒

Azure AD Users and groups 


☐

Azure AD Management events 


☐

Azure AD Sign-in events 


☐

Azure AD Apps 

☐

Azure AD activities 



☐


Azure AD files 

Enable file monitoring before enabling Office 365 files.


- SIEM Agents
- Add the Azure Sentinel integration

## SIEM agents

 Add SIEM agent 

 Generic SIEM 

Integrate with your SIEM server

 Azure Sentinel 

Integrate to Microsoft cloud-native SIEM



## Configure Azure Sentinel integration PREVIEW

[? Integration guide](#)



DATA TYPES

CONFIGURE

Select the data type you want to forward to Azure Sentinel



### Alerts

Alerts for suspicious activities, possible security violations, or other issues



Apply to:

All alerts



### Discovery logs

Analyzed traffic for your cloud applications



Apply to:

All data streams



Next >

Quit

## Endpoints

- Advanced Features

- Ensure your settings match those below:

This section provides a set of advanced features you can enable. These features require integration with other products. You need to verify that these settings are enabled to use the features.

☐ Off

#### Restrict correlation to within scoped device groups

When this setting is turned on, alerts are correlated into separate incidents based on their scoped device group. By default, incident correlation happens across the entire tenant scope.

① Changing this setting impacts future alert correlations only.

☐ Off

#### Enable EDR in block mode

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

☒ On

#### Automatically resolve alerts

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

☒ On

#### Allow or block file

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

☒ On

#### Hide potential duplicate device records

When turned on, this setting will hide duplications that might occur for the following reasons:

- Devices that were discovered more than once
- Discovery of onboarded devices
- Unintentionally discovered onboarded devices

These duplications will be hidden from multiple experiences in the portal to create a more accurate view of the device inventory. The affected areas in the portal include the Device Inventory, Microsoft Defender Vulnerability Management screens, and Public API for machines data. Notably, you will still be able to view these devices in global search, advanced hunting and alert and incidents pages.

① When activated, this heuristic might hide some discovered devices in certain cases. You can always come back here and choose to view all devices.

☒ On

#### Custom network indicators

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

☒ On

#### Tamper protection

Stop unwanted changes to your security solution and its essential functions. With tamper protection, malicious apps are prevented from turning off security features like virus & threat protection, behavior monitoring, cloud-delivered protection, and more. [Learn about tamper protection requirements](#)

☒ On

#### Show user details

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

☒ On

#### Skype for business integration

Enables 1-click communication with users.

☒ On

#### Microsoft Defender for Cloud Apps

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

 On

#### Web content filtering

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

 On

#### Unified audit log

When an audited activity is performed by a user or admin, an audit record is generated and stored in the Office 365 audit log for your organization. For more information, see the [Search the audit log in the Security & Compliance Center](#).

 On

#### Device discovery

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

 On


#### Download quarantined files

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

 On

#### Default to streamlined connectivity when onboarding devices in Defender portal


With streamlined connectivity, devices connect to fewer URLs and static IPs. You'll still be able to select standard connectivity. [Learn about streamlined connectivity](#).

 To avoid service connectivity issues, update devices and ensure they can connect to '\*.endpoint.security.microsoft.com' before onboarding. [View requirements](#)

 On

#### Apply streamlined connectivity settings to devices managed by Intune and Defender for Cloud

With streamlined connectivity, devices connect to fewer URLs and static IPs. [Learn about streamlined connectivity](#).

 These settings will apply with

- new EDR policies that select "Auto from connector" in Intune and
- new devices added to Defender for Cloud.

To avoid connectivity issues, update devices and ensure they can connect to "\*.endpoint.security.microsoft.com" before turning this feature on. [View requirements](#)

 On

#### Live Response

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

 On

#### Live Response for Servers

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

 Off

#### Live Response unsigned script execution

Enables using unsigned PowerShell scripts in Live Response.

 On

#### Deception

Manage and deploy lures and decoys to catch attackers in your environment. After you turn this on, go to Rules > Deception rules to run deception campaigns.

 On

#### Share endpoint alerts with Microsoft Compliance Center

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

 On

#### Microsoft Intune connection

Connects to [Microsoft Intune](#) to enable sharing of device information and enhanced policy enforcement.

Intune provides additional information about managed devices for secure score. It can use risk information to enforce [conditional access](#) and other security policies.

 On

#### Authenticated telemetry

Keep authenticated telemetry turned on to prevent spoofing telemetry into your dashboard

☒ On

**Preview features**  
 Allow access to preview features. Turn on to be among the first to try upcoming features.

See the [Microsoft Defender for Endpoint preview features](#) section in the [Microsoft Defender for Endpoint guide](#).

**Endpoint Attack Notifications**  
 Enables Microsoft to actively hunt for critical threats to be prioritized based on urgency and impact over your endpoint data. For proactive hunting across the full scope of Microsoft Defender XDR including threats that span email, collaboration, identity, cloud applications, as well as endpoints, [learn more](#) about Microsoft Defender Experts.

Apply

## Identities

- Sensors
- Click +Add Sensor, and download the installer and copy the Access key

The screenshot shows the 'Microsoft Defender for Identity' console. On the left, the 'Sensors' tab is selected. In the center, the 'Add sensor' button is highlighted with a red box. On the right, a modal window titled 'Add a new sensor' is open. It contains a 'Download installer' button (also highlighted with a red box) and an 'Access key' field with a copy icon. Below the key is a 'Regenerate key' button.

- Install the sensor on all DCs in AD. Use the access key when prompted by the installer.

The screenshot shows the 'Configure the Sensor' window. It has two main sections: 'Installation path' and 'Access key'. The 'Installation path' is set to 'C:\Program Files\Azure Advanced Threat Protection Sensor'. The 'Access key' field is filled with a long string of characters and has a question mark icon next to it. At the bottom right, there are 'Back' and 'Install' buttons.

- Active Directory
- **Configure Event Collection via GPO**
- Configure Group Managed Service Account account

- On the first DC
- Create root KDS key

```
Add-KdsRootKey -EffectiveTime ((get-date).addhours(-10))
```

- Purge kerberos tickets

```
klist purge -li 0x3e7
```

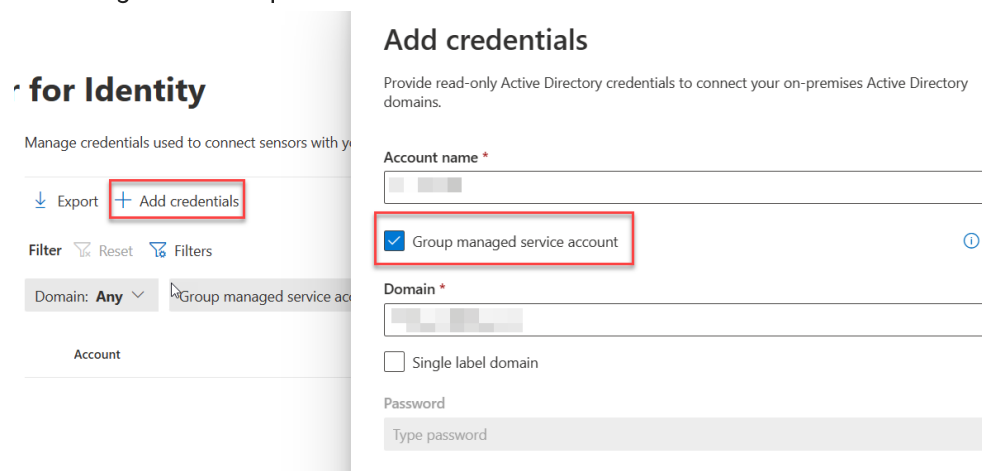
- Create the gMSA

```
New-ADServiceAccount accountname -  
PrincipalsAllowedToRetrieveManagedPassword "Domain Controllers" -  
DNSHostName accountname.domain.contoso.com
```

- Install the gMSA on the DC

```
Install-ADServiceAccount -Identity 'accountname'
```

- On the other DCs, purge kerberos tickets and install the service account
  - Add the gMSA in the portal



The screenshot shows the 'Add credentials' portal. On the left, a sidebar titled 'for Identity' has a button 'Add credentials' highlighted with a red box. The main area is titled 'Add credentials' and contains a form. In the 'Account name' field, there is a red box around the 'Group managed service account' checkbox, which is checked. Below this, the 'Domain' field is visible, followed by a 'Single label domain' checkbox and a 'Password' field with a 'Type password' label.

## Purview

### Advanced Audit

#### Portal

- Enable Auditing
- With the **ExchangeOnlineManagement** module in PS5/PS7+

```
Enable-OrganizationCustomization
Set-AdminAuditLogConfig -UnifiedAuditLogIngestionEnabled $true
```

## Device Onboarding

 [Portal](#)  [Windows](#)  [Mac](#)

- Enable Windows and Mac device onboarding. This requires MDE.

## Sensitivity Labels

### Enable labeling for Protected content & PDFs

 [Enable Sensitivity Labels for Protected Content](#)

 [Enable labeling support for PDFs](#)

- Enable labeling for Protected content & PDFs
- Using the [SharePoint Module](#) in PowerShell 5

```
connect-sposervice -url 'https://<tenant>-admin.sharepoint.com/'
Set-SPOTenant -EnableAPIIntegration $true
Set-SPOTenant -EnableSensitivityLabelforPDF $true
```

### Enable Labeling for Containers

In a fresh tenant, there will not be any EntraID group settings configured, so those [need to be created](#). Then [enable labeling](#) for containers. After that, you can [enable the label sync](#).

- With the Graph SDK in PS7+

```
Connect-MgGraph -Scopes "Directory.ReadWrite.All"
$TemplateId = (Get-MgBetaDirectorySettingTemplate | where { $_.DisplayName
-eq "Group.Unified" }).Id
$params = @{
    templateId = "$TemplateId"
    values = @(
        @{
            name = "EnableMIPLabels"
            value = "True"
        }
    )
}
New-MgBetaDirectorySetting -BodyParameter $params
```

- With the [ExchangeOnlineManagement module](#) in PS5/PS7+

```
Connect-IPPSSession
Execute-AzureAdLabelSync
```

## Enable co-authoring for Encrypted Files

This can be [done in the portal](#), or via PowerShell.

- With the [ExchangeOnlineManagement module](#) in PS5/PS7+

```
Connect-IPPSSession
Set-PolicyConfig -EnableLabelCoauth:$true
```

## Implement Secure by Default Labeling

Rationale and planning guidance are [here](#). I've changed some of the configurations to more closely match what I've seen done with customers.

### LABEL DEFINITIONS

#### Personal

Name & Display Name: `Personal`

Description for users: `Non-business data, for personal use only`

Scope: `Files & other data assets, Emails, Meetings`

Control access: `No` Content marking: `No` Auto-labeling: `Off`

#### Public

Name & Display Name: `Public`

Description for users: `Organization data that's specifically prepared and approved for public consumption.`

Scope: `Files & other data assets, Emails, Meetings`

Control access: `No`

Content marking: `No`

Auto-labeling: `Off`

Groups & Sites Protection Settings:

- Privacy and User Access: `Public or Private (depending on needs)`

- External user access: `Off`

#### General

Name & Display Name: `General`

Description for users: `Business data that isn't intended for public consumption.`

`However, this can be shared with external partners, as required.`

Scope: `Files & other data assets, Emails, Meetings`

Control access:

- Assign permissions: `Now`

- Access expiration: `Never`



- Offline access: Always
  - Permissions:
  - Users and Groups: All users and groups in your organization
  - Permissions: Editor (Co-Author)
- Content marking:
- Footer: Classified as Confidential
- Auto-labeling: Off
- Groups & Sites Protection Settings:
- Privacy and User Access: Public or Private
  - External user access: Off

### **Confidential\All Employees**

Name: Confidential - All Employees

Display Name: All Employees

Description for users: Sensitive business data that could cause damage to the business if shared with unauthorized people. Examples include contracts, security reports, forecast summaries, and sales account data.

Scope: Files & other data assets, Emails, Meetings, Groups & Sites

Control access:

- Assign permissions: Now
  - Access expiration: Never
  - Offline access: Always
  - Permissions:
  - Users and Groups: All users and groups in your organization
  - Permissions: Editor (Co-Author)
- Content marking:
- Footer: Classified as Confidential
- Auto-labeling: Off
- Groups & Sites Protection Settings:
- Privacy and User Access: Private
  - External user access: Off

### **Confidential\Specific People**

Name: Confidential - Specific People

Display Name: Specific People

Description for users: Confidential data that can be shared with trusted people inside and outside your organization. These people can also reshare the data as needed.

Scope: Files & other data assets, Emails, Meetings

Control access:

- Assign permissions: Let users decide
- Outlook: Encrypt Only
- Word, Excel, PowerPoint: Prompt

Content marking:

- Footer: Classified as Confidential

Auto-labeling: Off

### **Confidential\Internal exception**

Name: Confidential - Internal exception

Display Name: Internal exception

Description for users: Confidential data that doesn't need to (or cannot) be encrypted. Use this option with care and appropriate business justification.

Scope: Files & other data assets, Emails, Meetings

Content marking:

- Footer: Classified as Confidential

Auto-labeling: Off

### **Highly Confidential\All Employees**

Name: Highly Confidential - All Employees

Display Name: All Employees

Description for users: Sensitive business data that could cause damage to the business if shared with unauthorized people. Examples include contracts, security reports, forecast summaries, and sales account data.

Scope: Files & other data assets, Emails, Meetings, Groups & Sites

Control access:

- Assign permissions: Now

- Access expiration: Never

- Offline access: Always

- Permissions:

- Users and Groups: All users and groups in your organization

- Permissions: Editor (Co-Author)

Content marking:

- Footer: Classified as Highly Confidential

Auto-labeling:

- Content Contains: All Credential Types

- Instance Count: 1 to many

- Confidence: High

Groups & Sites Protection Settings:

- Privacy and User Access: Private

- External user access: Off

### **Highly Confidential\Specific People**

Name: Highly Confidential - Specific People

Display Name: Specific People

Description for users: Highly confidential data that requires protection and can be viewed only by people you specify and with the permission level you choose.

Scope: Files & other data assets, Emails, Meetings

Control access:

- Assign permissions: Let users decide
- Outlook: Encrypt Only
- Word, Excel, PowerPoint: Prompt

Content marking:

- Footer: Classified as Highly Confidential

Auto-labeling: Off

### Highly Confidential\Internal exception

Name: Highly Confidential - Internal exception

Display Name: Internal exception

Description for users: Highly Confidential data that doesn't need to (or cannot) be encrypted. Use this option with care and appropriate business justification.

Scope: Files & other data assets, Emails, Meetings

Content marking:

- Footer: Classified as Confidential

Auto-labeling: Off

There's a **nifty button** to do this for you (with some differences from the guide above) if you haven't set up any labels previously. It also implements publishing and client-side labeling policies so buyer beware.

## No sensitivity labels yet



Quickly set up and publish 12 recommended labels in one click.

[Learn about our recommended labels](#)

Get started

DLP

### Settings

 [Portal](#)

ENDPOINT DLP

 [Docs](#)

- Advanced classification scanning and protection: On
- Advanced label-based protection for all files on devices On
- Setup Evidence collection for file activities on devices: On
  - Storage type: Microsoft managed
- Browser and domain restrictions to sensitive data
  - Full URL for 'File copied to cloud: On

#### ANALYTICS

- Activate analytics: On

#### JUST IN TIME PROTECTION

##### Docs

- Locations to monitor: Devices
- Fallback action: Block

## MIP Scanner

##### Portal

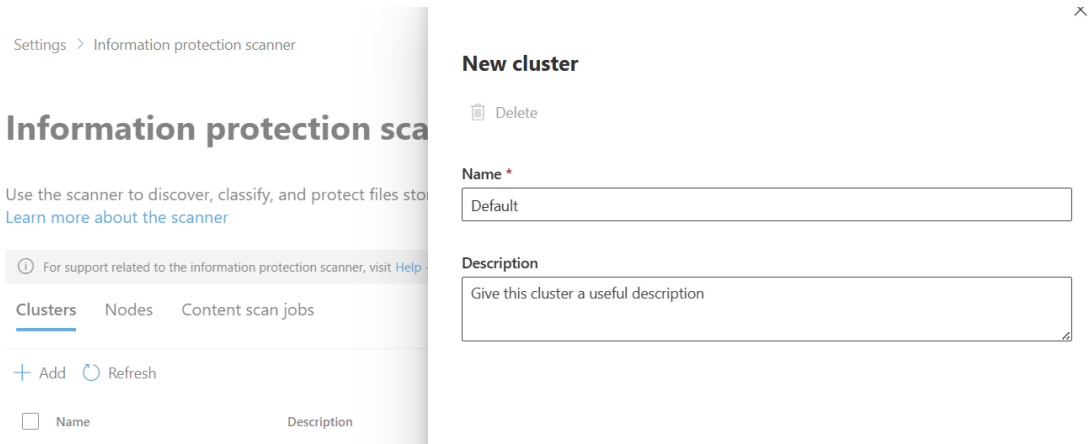
##### Docs

#### Prerequisite

- Service account in AD, exclude from MFA registration and CAs
- SQL server for the scanner, as well as a windows server.

#### Deployment

- Create a Scanner Cluster



The screenshot shows the 'Information protection scanner' settings page. The breadcrumb is 'Settings > Information protection scanner'. The title is 'Information protection scanner'. Below the title, it says 'Use the scanner to discover, classify, and protect files stored on your devices. [Learn more about the scanner](#)'. There is a help link: 'For support related to the information protection scanner, visit [Help](#)'. Below this are three tabs: 'Clusters' (selected), 'Nodes', and 'Content scan jobs'. Under the 'Clusters' tab, there are '+ Add' and 'Refresh' buttons. At the bottom, there is a table with columns 'Name' and 'Description'. To the right of the screenshot is a 'New cluster' form with a 'Delete' button, a 'Name' field (with a red asterisk) containing 'Default', and a 'Description' field with the placeholder text 'Give this cluster a useful description'.

- Create a Content Scan Job. Be sure to disable any of the auto options - this will just be for scanning.

# Edit content scan job

## General

Content scan jobs specify how the on-premise repositories should be scanned

Content scan job name \*

Default

Description

Cluster

Default

Schedule ⓘ

Manual

Info types to be discovered ⓘ

All

Treat recommended labeling as automatic ⓘ

☐ Off

Enable DLP policy rules ⓘ

☐ Off

Enforce sensitivity labeling policy ⓘ

☐ Off

Label files based on content ⓘ

☒ On

Default label ⓘ

None

Relabel files ⓘ

☐ Off

Preserve "Date modified", "Last modified", and "Modified by" ⓘ

☒ On

Include or exclude file type to scan ⓘ \*

☒ Exclude

☐ Include

#### Include or exclude file type to scan

.lnk,.exe,.com,.cmd,.bat,.dll,.ini,.pst,.sca,.drm,.sys,.cpl,.inf,.drv,.dat,.tmp,.msp,.msi,.pdb,.jar,.oc...

#### Default owner ⓘ

Scanner Account

#### Set repository owner ⓘ

☐ Off

### Exact Data Match

[Portal](#) [Docs](#)

#### EDM SIT

- Create a new EDM SIT. Since I work in healthcare, I typically use [Synthea](#) to generate patient records. We do have [sample industry files](#) you can use.
- Make note of the datastore name when you finish the EDM wizard. You'll need it for the EDM uploader.

#### EDM UPLOADER TOOL

1. Create a service account for the EDM upload agents to run as.
2. Create a EntraID security group named `EDM_DataUploaders` and add the service account to it.
3. Install the EDM upload tool to `c:\EDM`
4. Place sample data in `c:\EDM\Data`
5. Save the schema `.\EdmUploadAgent.exe /SaveSchema /DataStoreName your_data_store_name /OutputDir c:\edm\data`
6. Create `c:\EDM\hash`
7. Upload the data `.\EdmUploadAgent.exe /uploaddata /datastorename your_data_store_name /datafile C:\edm\data\your_data.csv /hashlocation c:\edm\hash /schema C:\edm\data\your_data_store_name.xml /allowedbadlinespercentage 5`

### Insider Risk Management

#### Work in Progress

This section is not complete.

### Roles



- Add your account to the `Insider Risk Management` role.
- Create a role group called `Data Connector Admins`, add the `Data Connector Admin` role to it and add your account to the role group.

## Browser Activity Plugins

- Deploy the Edge profile via Intune as described [here](#)
- Deploy the Chrome profile via Intune as described [here](#)

## Settings



- Analytics
- Insights at tenant & user level: `On`
- Data sharing
  - Share user risk details with other security solutions: `On`
- Policy indicators
- Select all indicators under the following categories
  - Office
  - Microsoft Defender for Cloud Apps
  - Cumulative exfiltration detection
  - Risk score boosters
  - Generative AI Apps
  - Microsoft Copilot Experiences
  - Microsoft Entra
  - Risk Detection indicators

### ANALYTICS

- Toggle analytics on

### POLICY INDICATORS

- Select all indicators under the following categories
- Office
- Device
- Microsoft Defender for Endpoint

- Risky Browsing
- Microsoft Defender for Cloud Apps

## Adaptive Protection

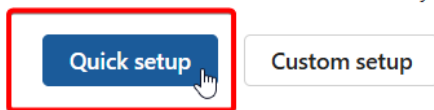


1. Turn on adaptive protection with the quick setup option

### Adaptive Protection

## Turn on Adaptive Protection to get started

Adaptive Protection integrates Insider Risk Management, Data Loss Prevention, and Conditional Access capabilities to help detect potentially risky activity and dynamically enforce protection actions based on users' insider risk levels. You can set everything up quickly in one-click or customize your configuration.



### Here's what we'll set up when you turn on Adaptive Protection

- Insider risk policy scoped to all users in your org
- Built-in insider risk levels to define how risky a user's activity might be
- Data Loss Prevention policy enabled in audit mode
- Conditional Access policy in report-only mode.

[Learn more about Adaptive Protection](#)

2. Wait for that to process. Once complete, go back and enable Adaptive Protection under Adaptive Protection settings

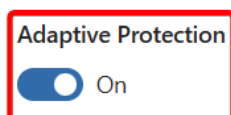
### Adaptive Protection settings

When turned on, Adaptive Protection detects users who match your defined insider risk levels. If those risk levels are included as a condition of a Data Loss Prevention policy or a Conditional Access policy, the Data Loss Prevention policy or the Conditional Access policy will apply the configured actions to that user's activity.

[Learn more about Adaptive Protection](#)

To maintain referential integrity, pseudonymization of usernames (if turned on) isn't preserved for users from Adaptive Protection who have alerts or activity appear outside Insider Risk Management. Actual usernames will appear in related Data Loss Prevention alerts and activity explorer.

If Adaptive Protection is turned off after having been on and active, insider risk levels will stop being assigned to users and shared with DLP and Conditional Access. After turning off, it might take up to 6 hours to stop assigning risk levels to user activity and reset them all.



## Polices



## 1. Create a Data Leaks policy from the template

### Choose a policy template

Policy templates specify the conditions and indicators that define the risk activities you want to be alerted to.

#### Data theft

Data theft by departing users

#### Data leaks

Data leaks

Data leaks by priority users

Data leaks by risky users

#### Security policy violations (preview)

Security policy violations (preview)

Security policy violations by departing users (preview)

Security policy violations by risky users (preview)

Security policy violations by priority users (preview)

#### Health record misuse (preview)

Health record misuse (preview)

#### Risky browser usage (preview)

Risky browser usage (preview)

#### Data leaks

Detects data leaks by any user included in this policy. Data leaks can range from accidental oversharing of information outside your organization to data theft with malicious intent.

##### Prerequisites

☒ DLP policy OPTIONAL

☒ Devices onboarded OPTIONAL

☐ Physical badging connector OPTIONAL

Physical badging connector configured to periodically import access events to priority physical locations. [Set up badging connector](#)

##### Triggering event ⓘ

- User performs selected exfiltration activities that exceed specific thresholds.
- User performs an activity matching specified DLP policy.

##### Activities detected include ⓘ

- Downloading files from SharePoint
- Printing files
- Copying data to personal cloud storage services

## 2. Target all users

## 3. Choose not to prioritize content.

### Decide whether to prioritize content

You can prioritize content based on factors like where it's stored and how it's classified. Risk scores are increased for any activity that contains priority content, which in turn increases the chance of generating a high severity alert. [Learn about the benefits of prioritizing content](#)

- ☐ I want to prioritize content  
Choose what to prioritize. You'll add the specific items in the next step.
- ☒ I don't want to prioritize content right now  
You can return to this step after the policy is created

## 4. For triggering events, choose User performs an exfiltration activity

## 5. For thresholds, choose Apply built-in thresholds.

## 6. For indicators, leave the default ones checked.

## Communication Compliance

- Grant Teams meeting recording access.