Module 4: Manage Security Reports and AI

Section: Implement M365 Security and Threat Management

Module 4: Manage Security Reports and AI

Manage Service Assurance Dashboard

Protection.office.com: security and compliance

Service assurance

Region and industry settings

View service and compliance reports

View Trust documents provided by Microsoft

Manage Service Assurance Dashboard

SKYLINES ACADEMY

No added licenses	Easy to access	Easy to secure access	Accessibility to various resources
Included with Enterprise (E3 & E5) plans	Must be member of Service Assurance User Role	RBAC based controls allow limiting access to specific personnel	Download compliance reports, trust documents, and access audited control information

Microsoft 365

Check out the new homes for Microsoft 365 security and compliance

Check out the new homes for Microsoft 365 security and compliance. Designed with accessibility and usability in mind, Microsoft 365 security center and Microsoft 365 compliance center offer specialized workspaces for managing security and compliance across Microsoft 365 services. Learn more

Office 365

Customize

- Home
- Alerts
- Permissions
- Classification
- Data loss prevention
- Records management
- Information governance
- Supervision
- Threat management
- Mail flow
- Data privacy
- Search
- eDiscovery
- Reports

Welcome to the Security & Compliance Center

We're busy building a one-stop shop for security and compliance across Office 365. Keep an eye out for new features coming your way. As always, your feedback is a critical part of our blueprint, so take a look around and let us know what you think.

Take a tour

We're committed to helping on your GDPR journey

GDPR is all about protecting and enabling individuals' privacy rights inside the European Union (EU). Our tools can help you detect, classify, and secure this sensitive info across locations (like Exchange, OneDrive, and more) and can also help you quickly find and export content in response to data subject requests.

Go to the GDPR dashboard

Information governance

The tools on the information governance dashboard can help you manage the full content lifecycle from importing, storing, and classifying data at the

Search for users

Search for users

Microsoft Secure Score

Total score: 32/343

This score reflects the collective security state of your identities, data, devices, apps, and infrastructure.

Updated 03/09/2020

32

Recommended for you

Further protect shared content

Classify and govern user privacy data

General Data Protection Regulation (GDPR) requires organization like yours to properly govern EU personal sensitive information. See how you can classify and govern these data properly to minimize compliance risks.

View recommendation

Search for activity

Want to know what your users and admins are doing? Start recording activities in Office 365.

Start recording now

Records management
Information governance
Supervision
Threat management
Mail flow
Data privacy
Search
eDiscovery
Reports
Service assurance
Dashboard
Audit Reports
Compliance Manager

Service Assurance

Service Assurance provides transparency of operations and information on how Microsoft maintains the security, privacy and compliance of customer data in its cloud services. Customers can use the third-party reports on advanced security and compliance standards, along with a library of white papers, FAQs, and other materials on a variety of data protection topics to perform their own regulatory risk assessments. Service Assurance is powered by Microsoft's service trust platform, which is also available through the Service Trust Portal.

The Compliance Reports and Trust Documents are made available to you to help you perform your own risk assessment of Microsoft's cloud services to ensure that they meet your organization's security and regulatory requirements. Be sure to let information security, compliance, audit, and risk management teams from your organization know these resources are available, as they are designed to save your organization time and money.

What's new

Compliance Manager and Compliance Score
Compliance Manager is a workflow-based risk assessment tool that enables you to track, assign, and verify your organization's regulatory compliance activities related to Microsoft cloud services. Each Office 365 assessment in Compliance Manager includes a risk-based Compliance Score to help you assess the level of risk (due to non-compliance or control failure) associated with each control (including both Microsoft managed and customer managed controls).

Compliance Manager replaces Audited Controls, and like Audited Controls, Compliance Manager provides you with details about the controls Microsoft implements to protect its cloud services and customer data, and how and when third-party independent auditors tested and verified these controls. The customer-managed controls section of Compliance Manager also helps you manage the actions that you need to take to protect your data and manage your organization's regulatory compliance.

For more information about Compliance Manager, see Use Compliance Manager to help meet data protection and regulatory requirements when using Microsoft cloud services.

Service Trust Portal Search functionality
Search has been added for STP documents and resources, enabling you to search for regulatory compliance information by keywords and phrases.

Add users

Users from your organization will not have access to Service Assurance features until they are granted the **Service Assurance User** role.

Go to Permissions to assign this role to users.

Onboarding guide

Do non-admin users in your organization need Service Assurance resources? See the Onboarding Guide for details on how to grant access.

Region and industry settings

The Microsoft Cloud Service Assurance Portal contains Microsoft's confidential information. By accessing or using this web site, you agree not to disclose such information without Microsoft's prior written consent.

Select one or more regions and industries that are applicable to your organization, and we'll make sure to provide you with the service assurance resources that matter most to you.

Default Tenant Document Filters

These filters apply to all tenant users who have not chosen custom document filters

Region: North America **Industry:** Education

Your Custom Document Filters

These filters override the default tenant document filters

Region: North America **Industry:** Education

Save Undo Changes

Your region and industry settings have been saved. You can now access Compliance Reports, Trust Documents, and Audited Controls.

Data loss prevention
Records management
Information governance
Supervision
Threat management
Mail flow
Data privacy
Search
eDiscovery
Reports
Service assurance
Dashboard
Audit Reports
Compliance Manager
Settings

The tools on the information governance dashboard can help you manage the full content lifecycle from importing, storing, and classifying data at the beginning to retaining, monitoring, and then deleting it at the end.

Go to the information governance dashboard

Threat management

Cyberattacks are constantly evolving. Our threat management features help safeguard your organization against these attacks by providing insights and tools to help detect and respond to threats like phishing, malware, malicious links, and more.

linkText

- New ATP anti-phishing policy
- New spam policy
- View quarantine

Your score

Identity	12 / 203
Data	0 / 55
Device	No data to show
Apps	20 / 85
Infrastructure	No data to show

Microsoft Secure Score

- Create an import job
- More

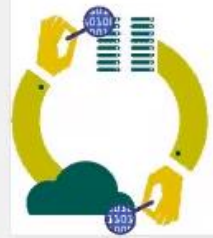
Information governance

It's your data. You own it. So we've developed features that let you take charge of how and when it is stored, used, and retained or removed.

Learn more about data management

- Enable extra storage
- Import data into Office 365

Search & investigation



You have a lot of data swarming around in the cloud. Luckily, the features in the Search & Investigation section can help you navigate through the swarm.

Learn more about search & investigation

- Search for content
- Search for admin and user activity

Service assurance

Does your organization need to comply with regulatory standards like HIPAA, SOC, and ISO? You're in luck. Our Service assurance page is the place to go.

Learn more about service assurance

- Update industry and geography settings
- View trust documents provided by Microsoft
- View service compliance reports

Home > Trust documents

Trust documents provided by Microsoft

Understand how Microsoft cloud services protect your data and how you can manage data security and compliance for your cloud services.

ISO Reports

ISO 27001, ISO 27017, ISO 27018 Standard audit assessment reports for Microsoft cloud services.

8993142 Report ISMS CAV MS Data Grid.pdf
9640167,9640303 Report ISMS and PII CAV MS NGP
Microsoft AME ISO 27001 and 27018 Certification Audit Report - 7.15.2019.pdf
Microsoft Azure and Dynamics - ISO 22301 Certificate - 7.22.2019.pdf

Assessment Reports

FAQ and White Papers

Pen Test and Security Assessments

Compliance Guides

Manage Tracing and Reporting on Azure AD Identity Protection

- Azure AD Identity Protection

Manage Tracing and Reporting on Azure AD Identity Protection

SKYLINE
ACADEMY

Azure AD Identity Protection

- Automate the detection and remediation of identity-based risks.
- Investigate risks using data in the portal.
- Export data to third-party utilities for further analysis.

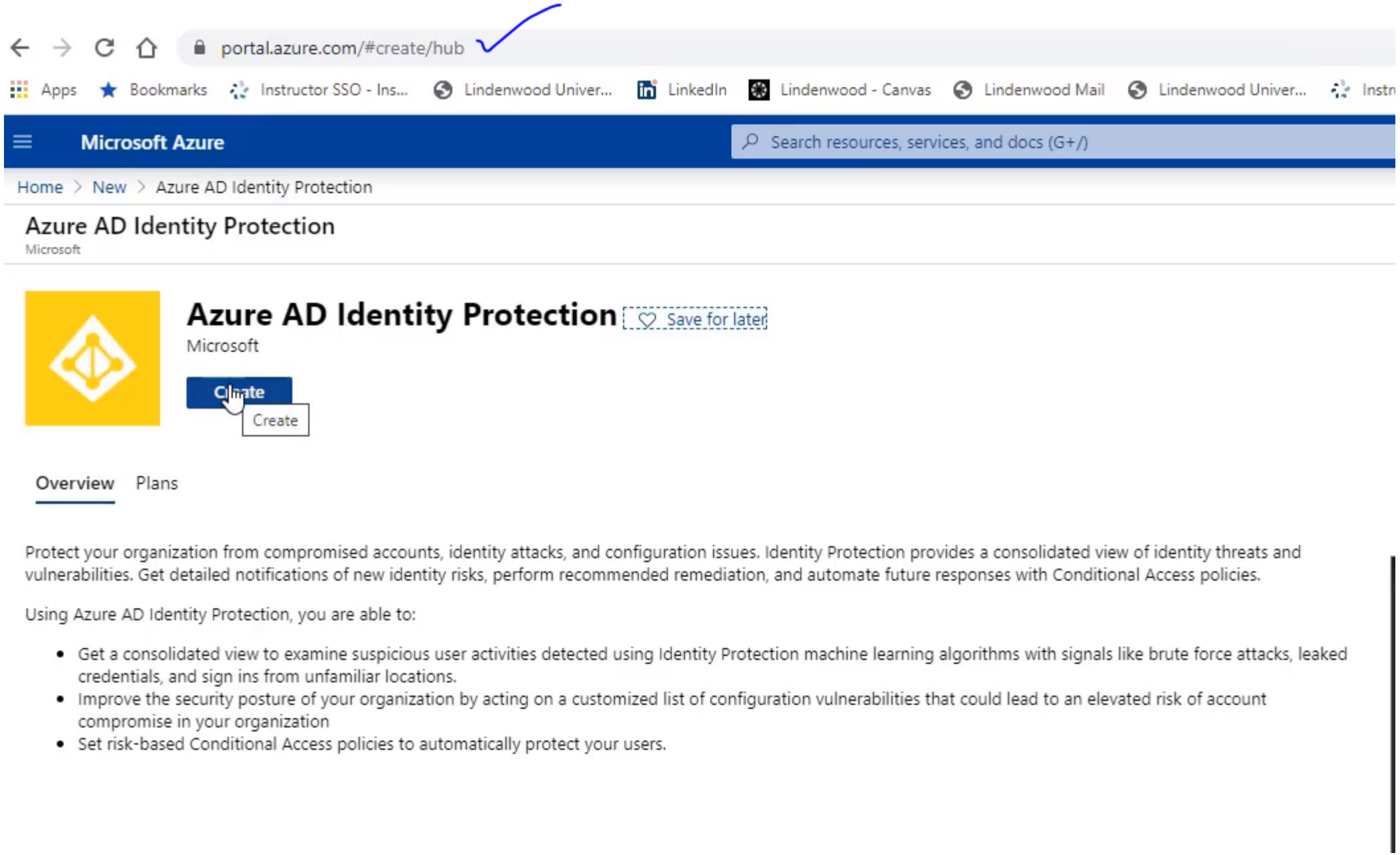
Licensing AAD Identity Protection

- Need Azure AD Premium P2 licensing
- Included with Enterprise Mobility + Security E5 or A5

Permissions

Requires users be one the following:

- Security Reader, Operator, or Administrator
- Global Reader or Administrator


portal.azure.com/#create/hub
Apps
Bookmarks
Instructor SSO - Ins...
Lindenwood Univer...
LinkedIn
Lindenwood - Canvas
Lindenwood Mail
Lindenwood Univer...
Microsoft Azure
Search resources, services, and docs (G+/)
Home > New > Azure AD Identity Protection
Azure AD Identity Protection
Microsoft
Azure AD Identity Protection
Save for later
Microsoft
Create
Create
Overview
Plans
Protect your organization from compromised accounts, identity attacks, and configuration issues. Identity Protection provides a consolidated view of identity threats and vulnerabilities. Get detailed notifications of new identity risks, perform recommended remediation, and automate future responses with Conditional Access policies.
Using Azure AD Identity Protection, you are able to:
Get a consolidated view to examine suspicious user activities detected using Identity Protection machine learning algorithms with signals like brute force attacks, leaked credentials, and sign ins from unfamiliar locations.
Improve the security posture of your organization by acting on a customized list of configuration vulnerabilities that could lead to an elevated risk of account compromise in your organization
Set risk-based Conditional Access policies to automatically protect your users.

Identity Protection | Overview

Search (Ctrl+/)

Learn more | Refresh | Got feedback?

- Overview

Protect

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

Report

- Risky users
- Risky sign-ins
- Risk detections

Notify

- Users at risk detected alerts
- Weekly digest

Troubleshooting + Support

- Troubleshoot
- New support request

Date range = **30 days**

New risky users detected

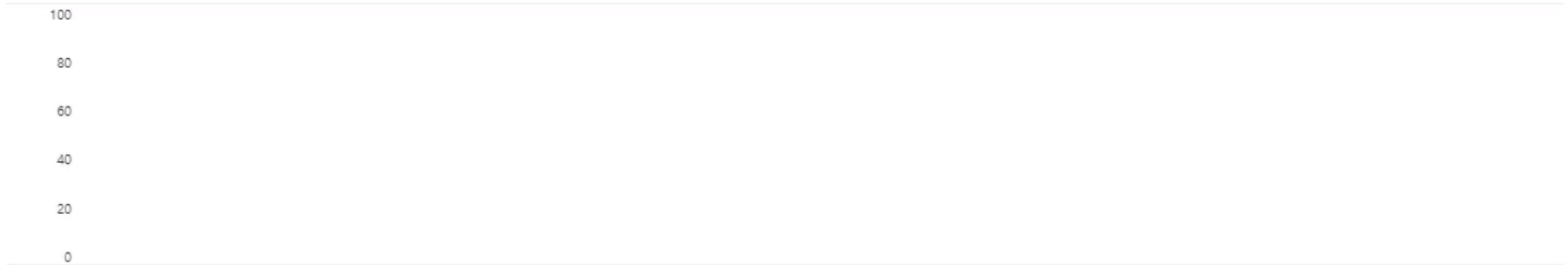
User risk level = **All**

Configure user risk policy >

New risky sign-ins detected

Sign-in risk type = **Real-time**

Sign-in risk level = **All**

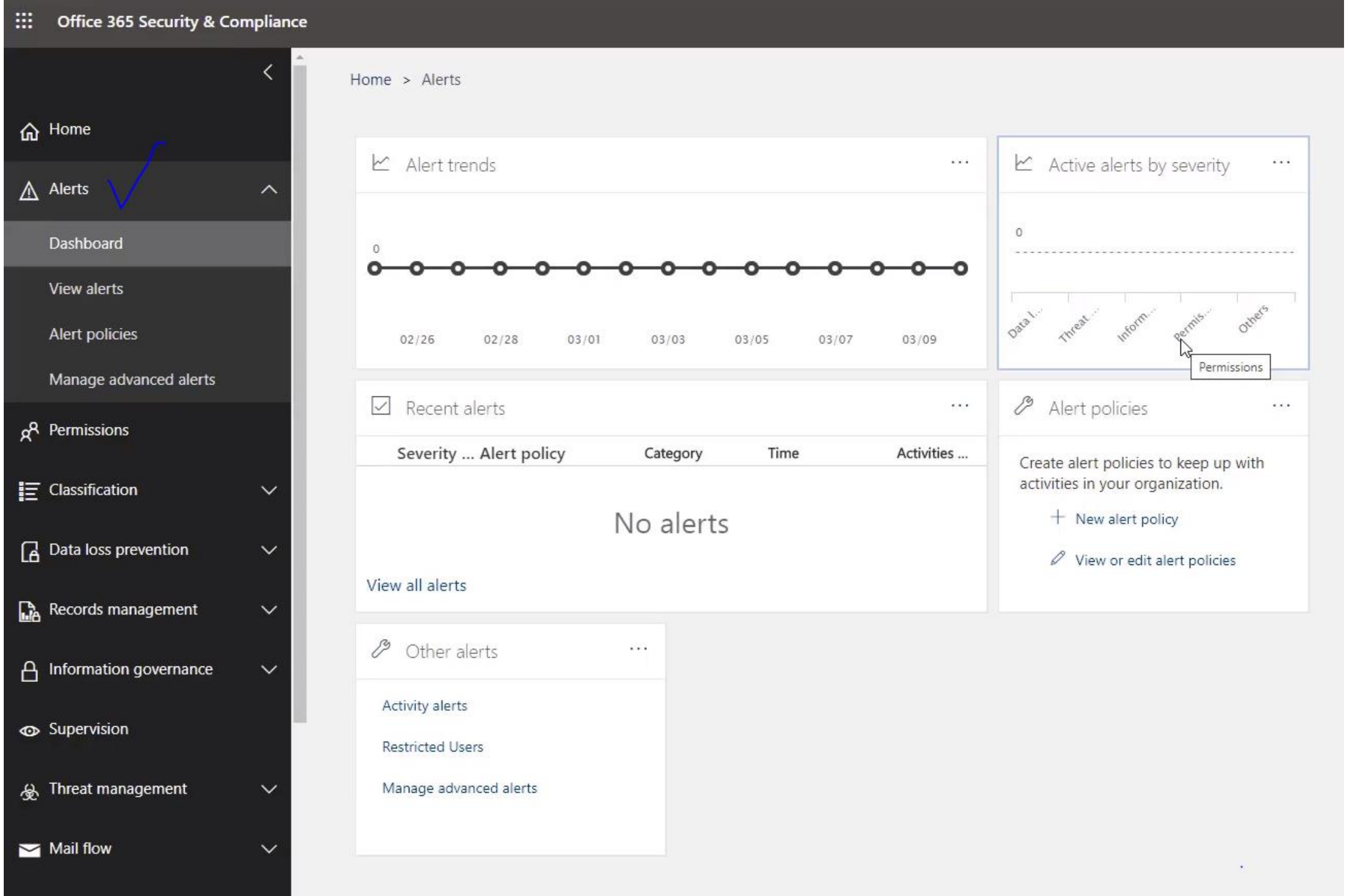


Identity Secure Score

12 / 203

Monitor and improve your identity security posture.

Configure and Manage M365 Security Alerts


Office 365 Security & Compliance
Home
Alerts
Dashboard
View alerts
Alert policies
Manage advanced alerts
Permissions
Classification
Data loss prevention
Records management
Information governance
Supervision
Threat management
Mail flow
Home > Alerts
Alert trends
0
02/26
02/28
03/01
03/03
03/05
03/07
03/09
Active alerts by severity
0
Data l...
Threat ...
Inform...
Permis...
Others
Permissions
Recent alerts
Severity ... Alert policy
Category
Time
Activities ...
No alerts
View all alerts
Alert policies
Create alert policies to keep up with activities in your organization.
New alert policy
View or edit alert policies
Other alerts
Activity alerts
Restricted Users
Manage advanced alerts

Alert policies

Use alert policies to track user and admin activities, malware threats, or data loss incidents in your organization. After choosing the activity you want to be alerted on, refine the policy by adding conditions, d
should receive notifications. Learn more about alert policies

+ New alert policy | Search

- Home
- Alerts
  - Dashboard
  - View alerts
  - Alert policies
  - Manage advanced alerts
- Permissions
- Classification
- Data loss prevention
- Records management
- Information governance
- Supervision
- Threat management
- Mail flow
- Data privacy

Name	Severity	Type	Category	Date
Suspicious email sending patterns detected	Medium	System	Threat management	-
Elevation of Exchange admin privilege	Low	System	Permissions	-
Email messages containing malware removed after delivery	Informational	System	Threat management	-
Malware campaign detected and blocked	Low	System	Threat management	-
Email reported by user as malware or phish	Informational	System	Threat management	-
Unusual volume of file deletion	Medium	System	Information governa...	-
Unusual external user file activity	High	System	Information governa...	-
eDiscovery search started or exported	Medium	System	Threat management	-
Malware campaign detected in SharePoint and OneDrive	High	System	Threat management	-
Admin Submission Result Completed	Low	System	Threat management	-
Email sending limit exceeded	Medium	System	Threat management	-

New alert policy

- Name your alert
- Create alert settings
- Set your recipients
- Review your settings

Name your alert, categorize it, and choose a severity.

Assign a category and severity level to help you manage the policy and any alerts it triggers. You'll be able to filter on these settings from both the 'Alert policies' and 'View alerts' pages.

Name *

User Permission Changes

Description

Enter a friendly description for your policy

Severity *

Medium

Category *

Select a category

- Data loss prevention
- Threat management
- Information governance
- Permissions
- Mail flow
- Others

ncel

New alert policy

- Name your alert
- Create alert settings
- Set your recipients
- Review your settings

Choose an activity, conditions and when to trigger the alert

You can only choose one activity but you can add conditions to refine what we'll detect.

What do you want to alert on?

* Activity is

Allowed user to create groups

Site administrator or owner adds a permission level to a site that allows a user assigned that permission to create a group for that site.

+ Add a condition

How do you want the alert to be triggered?

- (●) Every time an activity matches the rule
- ( ) When the volume of matched activities reaches a threshold
  - More than or equal to 15 activities
  - During the last 60 minutes
  - On All users
- ( ) When the volume of matched activities becomes unusual
  - On All users

Back | Next | Cancel

New alert policy

- Name your alert
- Create alert settings
- Set your recipients
- Review your settings

Review your settings

Name	User Permission Changes	
Description	Add a description	Edit
Severity	Medium	
Category	Permissions	
Filter	Activity is Allowed user to create groups	
Aggregation	Trigger an alert when any activity matches your conditions.	Edit
Scope	All users	
Recipients	dhood@skylinesacademydemo.onmicrosoft.com	
Daily notification limit	No limit	Edit

Do you want to turn the policy on right away?

- (●) Yes, turn it on right away.
- ( ) No, keep it off. I will turn it on later.

Back | Finish | Cancel

Home > Alert policies

Alert policies

Use alert policies to track user and admin activities, malware threats, or data loss incidents in your organization. After choosing the activity you want to be alerted on, refine the policy by adding conditions, deciding when to trigger the alert, and
should receive notifications. Learn more about alert policies

+ New alert policy | Search | Filt

Name	Severity	Type	Category	Date modified	Status
User Permission Changes	Medium	Custom	Permissions	3/11/20 2:22 AM	
Suspicious email sending patterns detected	Medium	System	Threat management	-	
Elevation of Exchange admin privilege	Low	System	Permissions	-	
Email messages containing malware removed after delivery	Informational	System	Threat management	-	
Malware campaign detected and blocked	Low	System	Threat management	-	
Email reported by user as malware or phish	Informational	System	Threat management	-	
Unusual volume of file deletion	Medium	System	Information governa...	-	
Unusual external user file activity	High	System	Information governa...	-	
eDiscovery search started or exported	Medium	System	Threat management	-	

Configure and Manage Azure Identity Protection Dashboard and Alerts

Identity Protection | Overview

Search (Ctrl+/)

- Overview

Protect

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

Report

- Risky users
- Risky sign-ins
- Risk detections

Notify

- Users at risk detected alerts
- Weekly digest

Troubleshooting + Support

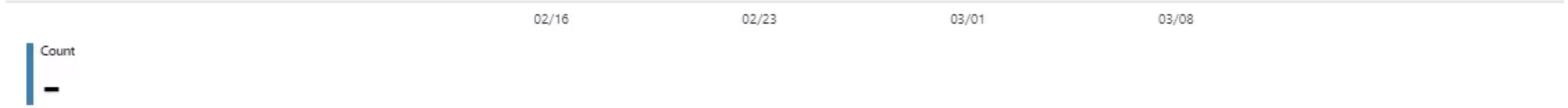
- Troubleshoot
- New support request

Learn more | Refresh | Got feedback?

Date range = **30 days**

New risky users detected

User risk level = **All**



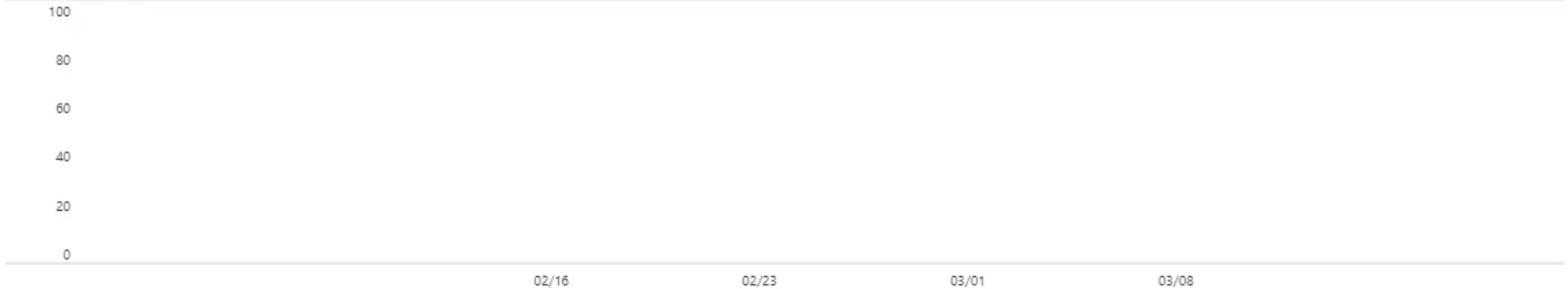
Count
-

Configure user risk policy >

New risky sign-ins detected

Sign-in risk type = **Real-time**

Sign-in risk level = **All**



Count
0

Unprotected
-

Protected
0

Identity Protection | User risk policy

Search (Ctrl+/)

- Overview

Protect

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

Report

- Risky users
- Risky sign-ins
- Risk detections

Notify

- Users at risk detected alerts
- Weekly digest

Troubleshooting + Support

- Troubleshoot
- New support request

Policy name

User risk remediation policy

Assignments

Users

All users

Conditions

Select conditions

Controls

Access

Select a control

Review

Estimated impact

Number of users impacted

Enforce Policy

On | Off