Azure Active Directory Identity Protection- Adoption Kit

Contents

Awareness

This section helps you to analyze the benefits of Azure Active Directory (Azure AD) Identity Protection. You will learn about the ease of use, pricing and licensing model, as well as customer stories about how it helped improve their business. You will also receive up-to-date announcements and access to blogs that discuss ongoing improvements.

Business Overview

Microsoft has secured cloud-based identities for more than a decade. With **Azure AD Identity Protection**, you can use the same protection systems Microsoft uses to secure identities, in your environment, to:

- Proactively prevent compromised identities from being abused
- Automatically mitigate risk when suspicious activity is detected
- Investigate risky users and sign-ins to address potential vulnerabilities
- Be alerted when a user's risk reaches a specified threshold

The Identity Protection experience has been improved over time to better protect your organization's identities. Refer to What is Azure Active Directory Identity Protection (refreshed)? to learn about the new capabilities.

Discovering compromised identities is no easy task. Azure Active Directory uses adaptive machine learning algorithms and heuristics to detect anomalies and suspicious incidents that indicate potentially compromised identities. Using this data, Azure AD Identity Protection generates reports and alerts that enable you to evaluate the detected issues and take appropriate mitigation or remediation actions.

Check out this video to learn more about this feature: Channel 9: Azure AD and Identity Show: Identity Protection Preview

Refer to Azure Active Directory Identity Protection FAQ for common questions.

Pricing and Licensing Requirements

Azure AD Identity Protection capability requires you to use Azure Active Directory Premium P1, Premium P2. During public preview of Azure AD Identity Protection (refreshed), only Azure AD Premium P2 customers will have access to the risky users report and risky sign-ins report. Refer to Licensing.

For more information on pricing, refer to Azure Active Directory pricing.

Key Benefits

Detection

- Vulnerabilities detected by Azure Active Directory Identity Protection
  Azure AD Identity Protection analyzes your configuration and detects vulnerabilities that can have an impact on your user's identities.

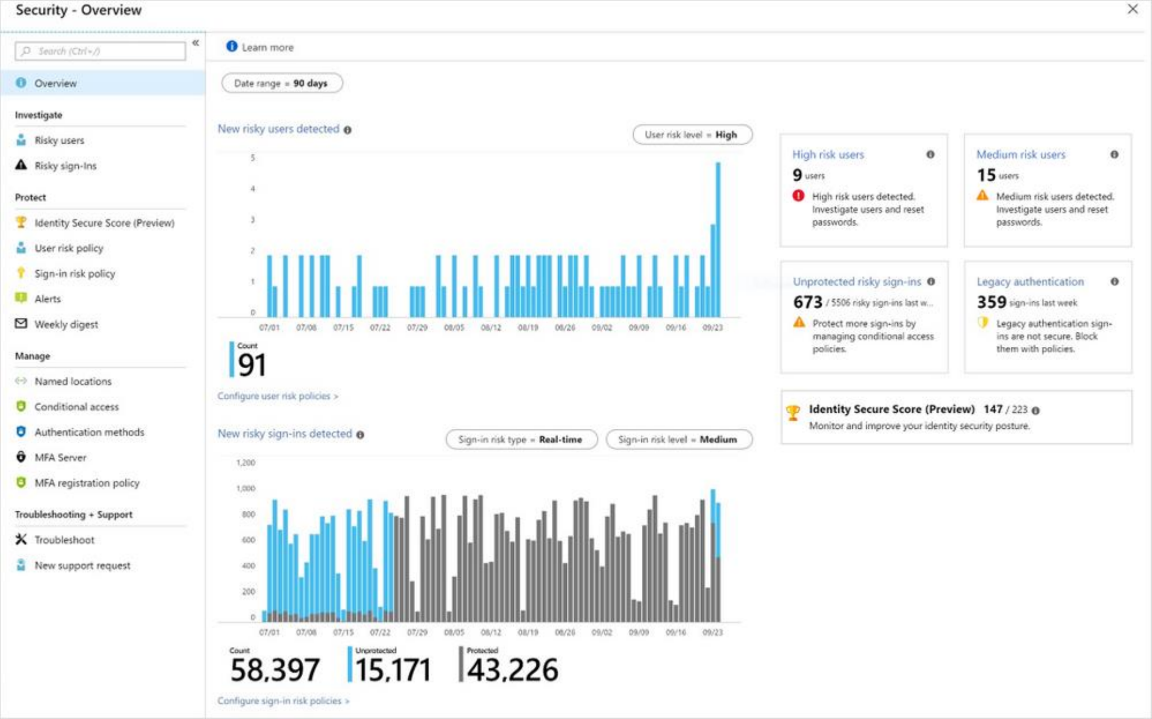
- Azure Active Directory risk events

Azure AD uses adaptive machine learning algorithms and heuristics to detect suspicious actions that are related to your user's identities. The system creates a record for each detected suspicious activity. These records are also known as risk events.

Investigation

Exploration of Identity Protection starts with the Identity Protection Dashboard. The dashboard gives you access to:

- Reports such as **Users flagged for risk, Risk events, and Vulnerabilities**
- Settings such as the configuration of your **Security Policies, Notifications, and Multi-Factor Authentication registration**



Date range = **90 days**

User risk level = **High**

Count 91

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

Sign-in risk level = **Medium**

Count 58,397 | Unprotected 15,171 | Protected 43,226

High risk users
9 users
High risk users detected. Investigate users and reset passwords.

Medium risk users
15 users
Medium risk users detected. Investigate users and reset passwords.

Unprotected risky sign-ins
673 / 5506 risky sign-ins last w...
Protect more sign-ins by managing conditional access policies.

Legacy authentication
359 sign-ins last week
Legacy authentication sign-ins are not secure. Block them with policies.

Identity Secure Score (Preview) **147** / 223
Monitor and improve your identity security posture.

Policies

To implement automated responses, Azure AD Identity Protection provides you with three policies:

- Multi-factor authentication registration policy
- User risk policy
- Sign-in risk policy

Customer Stories/Case Studies

Discover how most organizations use Azure AD Identity Protection to help detect potential vulnerabilities affecting their organization's identities. The following featured stories demonstrate these needs.

Hearst Corporation - Eight things this media giant likes about Microsoft Enterprise Mobility + Security and Azure Active Directory. With Azure AD Identity Protection, Hearst can monitor network vulnerabilities, secure compromised identities, and safeguard confidential information.

One Horizon Group – Optimized VoIP startup gains global markets with move to the Microsoft cloud. The entire solution is secured by Azure AD Identity Protection and Conditional Access, for its internal documentation repositories. This move immediately launched the company into the global, agile, scalable world of doing business in the cloud.

To learn more about customer and partner experiences with Azure AD Identity Protection, visit - See the amazing things people are doing with Azure.

Announcements/Blogs

Azure AD receives improvements on an ongoing basis. To stay up to date with the most recent developments, refer to What's new in Azure Active Directory?

Blogs by the Tech Community and Microsoft Identity Division:

- 29 January 2019, Four major Azure AD Identity Protection enhancements are now in public preview
- 06 September 2018, Azure AD Identity Protection is in public preview!
- 07 September 2018, Azure AD Identity Protection
- 26 September 2018, Secure your hybrid-cloud environments with Azure AD Identity Protection and Azure ATP
- 26 September 2018, Announcing password-less login, identity governance, and more for Azure Active Directory

Training/Learning Resources

The section provides concepts, role-based guidance, and lists the various training resources available for Azure AD Identity Protection.

Level 100 Knowledge/Concepts

Follow the links below to get an overview of how Azure AD Identity Protection functions.

- Watch “Channel 9: Azure AD and Identity Show: Identity Protection Preview”
- Watch “What is Identity Protection? | Azure Active Directory”
- Learn “What is Azure Active Directory Identity Protection?”
- Know “Vulnerabilities detected by Azure Active Directory Identity Protection”
- Find “Azure AD Identity Protection Notifications”
- Learn “Sign-in experiences with Azure AD Identity Protection”
- Follow the “Azure Active Directory Identity Protection FAQ” for common questions

- Learn "What is Azure Active Directory Identity Protection (refreshed)?"
- Know "Azure Active Directory Identity Protection - Security overview"
- Follow "FAQs and known issues with identity protection (refreshed) in Azure Active Directory"

Role-Based Guidance

IT Administrator Staff

To load balance the management activities around your Identity Protection implementation, you can assign several roles. Azure AD Identity Protection supports 3 directory roles - Global Administrator, Security Administrator, and Security Reader. See Identity Protection roles.

Here are some useful links to help you get started:

- What is Azure Active Directory Identity Protection?
- What is Azure Active Directory Identity Protection (refreshed)?
- Azure Active Directory Identity Protection - Security overview
- Channel 9: Azure AD and Identity Show: Identity Protection Preview
- Enabling Azure Active Directory Identity Protection
- FAQs and known issues with identity protection (refreshed) in Azure Active Directory
- Azure Active Directory Identity Protection Glossary

Help Desk Staff

- Typically, a blocked user contacts the help desk to be unblocked. See How To: Unblock users
- Refer to the FAQs and Known Issues with identity protection (refreshed) in Azure Active Directory for common questions.

Training

On-Demand Webinars

Register here – Azure AD Identity Protection and Privileged Identity Management

Videos

- YouTube - Azure Friday | Azure Active Directory Identity Protection
- Azure videos - Azure Active Directory: Overview
- Azure videos - Azure Active Directory Identity Protection
- YouTube - What is Identity Protection? | Azure Active Directory
- YouTube - How to deploy Identity Protection | Azure Active Directory
- YouTube - How to use Identity Protection | Azure Active Directory
- Channel 9- Azure AD and Identity Show: Identity Protection Preview
- Azure videos - Securing your hybrid cloud environments with Azure ATP and AAD Identity Protection

Online Courses

- SkillUp.Online- Managing Identities
  "In this course, you are introduced to Azure AD Identity Protection, and learn how you can use it to protect your organization from compromised accounts, identity attacks, and configuration issues."

- PluralSight.com- Microsoft Azure Active Directory Managing Identities
  "In this course, you will learn the basics of Azure AD environment, including users, groups, devices and applications. You will understand how you can detect risky behavior and vulnerabilities automatically." Azure AD Identity Protection is covered in "Managing Access in Azure AD module."

Books

Refer to Active Directory Identity Protection Playbook. This playbook helps you to:

- Populate data in the Identity Protection environment by simulating risk events and vulnerabilities
- Set up risk-based conditional access policies and test the impact of these policies

Tutorial

Quickstart: Block access when a session risk is detected with Azure Active Directory Identity Protection

This quickstart shows how to configure a sign-in risk conditional access policy that blocks a sign-in when a medium and above sign-in risk level has been detected.

Whitepaper

- Published November 2017, Introduction to Azure Security
  This whitepaper describes the collection of security controls implemented in Azure from both the customer's and Microsoft operations' perspectives.

- Published December 2018, Advanced threat detection
  This whitepaper guides you through the Azure approaches towards threat vulnerability assessments, diagnostics, and analysis. It explains how Microsoft uses advanced threat detection mechanisms to secure the platform. It also explains how Microsoft includes these mechanisms in public facing features and services.

FAQ

- Azure Active Directory Identity Protection FAQ
- FAQ's and known issues with identity protection (refreshed) in Azure Active Directory

End-user Readiness and Communication

This section provides customizable posters and email templates to roll out Azure AD Identity Protection to your organization.

One of the consequences of implementing Azure AD Identity Protection is the need to configure Azure AD Self-Service Password Reset (SSPR), and Azure Multi-Factor Authentication (MFA). Refer to the following adoption kits for end-user readiness material:

- Azure AD SSPR adoption kit
- Azure AD MFA adoption kit

Planning and Change Management

This section provides the resource links to Azure AD Identity Protection deployment plan and topology

Deployment Plan

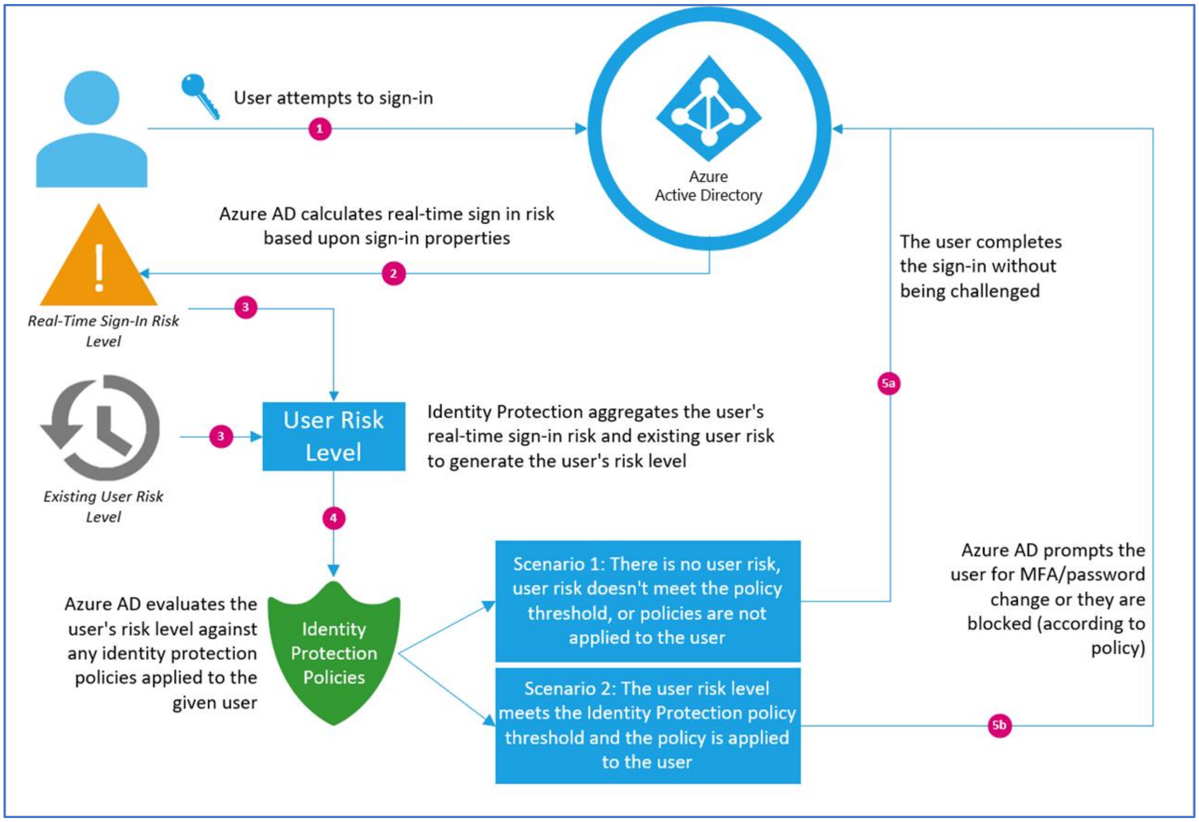
Refer to the following links:

- Deployment plan *coming soon!*
- Enabling Azure Active Directory Identity Protection

Architecture Plan/Topology

How Identity Protection detects risks

Azure AD uses machine learning to detect anomalies and suspicious activity, using both signals detected in real-time during sign-ins as well as non-real time signals related to users and their sign-in activities. Using this data, Identity Protection calculates a real-time sign-in risk each time a user authenticates, as well as determining an overall user risk level for reach user. Identity Protection allows you to automatically take action on these risk detections by configuring Identity Protection user risk and Sign-In Risk policies.


User attempts to sign-in
1
Azure Active Directory
Azure AD calculates real-time sign in risk based upon sign-in properties
2
Real-Time Sign-In Risk Level
3
Existing User Risk Level
3
User Risk Level
Identity Protection aggregates the user's real-time sign-in risk and existing user risk to generate the user's risk level
4
Azure AD evaluates the user's risk level against any identity protection policies applied to the given user
Identity Protection Policies
Scenario 1: There is no user risk, user risk doesn't meet the policy threshold, or policies are not applied to the user
Scenario 2: The user risk level meets the Identity Protection policy threshold and the policy is applied to the user
5a
The user completes the sign-in without being challenged
5b
Azure AD prompts the user for MFA/password change or they are blocked (according to policy)

Testing

This section provides the plan to test the functionality of Azure AD Identity Protection in a sandbox or test lab environment before the customer rolls it into production.

To keep your environment protected, you might want to block suspicious users from signing in. Azure AD Identity Protection analyzes each sign-in and calculates the likelihood that a sign-in attempt was not performed by the legitimate owner of a user account.

To test this functionality in a test lab environment, follow Quickstart: Block access when a session risk is detected with Azure Active Directory Identity Protection

Deployment

How can I get Azure AD Identity Protection deployed in my environment? This section provides resource links to help with implementation of your solution.

Deployment

In this video, learn how to deploy Azure AD Identity Protection by configuring risk-based policies (user risk and sign-in risk) in your organization. You'll also learn best practices on how to gradually roll-out these policies and MFA registration in your organization. Watch How to deploy Identity Protection | Azure Active Directory

Design Template

This will be available in the deployment plan *coming soon!*

Operations

How do I manage and maintain Azure AD Identity Protection? This section provides troubleshooting info, Azure AD Identity Protection operation and management details, and other important references.

Operations

Watch How to use Identity Protection | Azure Active Directory

Refer to the following links:

- How To: Configure the multi-factor authentication registration policy
- How To: Configure the sign-in risk policy
- How To: Configure the user risk policy
- How To: Configure risk policies in Azure Active Directory identity protection (refreshed)

Monitoring

Refer to the following links:

- How To: Close active risk events
- How To: Unblock users
- How To: Investigate risky users and sign-ins
- How To: Improve the detection accuracy

Troubleshooting

Refer to the following FAQs for common troubleshooting questions and known issues-

- Azure Active Directory Identity Protection FAQ
- FAQs and known issues with identity protection (refreshed) in Azure Active Directory

References

- Get started with Azure Active Directory Identity Protection and Microsoft Graph
  Microsoft Graph is the Microsoft unified API endpoint and the home of Azure Active Directory Identity Protection APIs.

- Azure Active Directory Identity Protection risk events reference
  Azure Active Directory uses adaptive machine learning algorithms and heuristics to detect suspicious actions that are related to your user accounts. Each detected suspicious action is stored in a record called risk event.

- Security reports
  Lists the Azure AD anomalous activity security reports, and corresponding risk event types in the Azure portal.

- Azure Active Directory Identity Protection Glossary

Support and Feedback

How can we improve Azure AD Identity Protection? This section provides links to discussion forums and technical community support email IDs.

We encourage you to join our Technical Community, a platform to Microsoft Azure Active Directory users and Microsoft to interact. It is a central destination for education and thought leadership on best practices, product news, live events, and roadmap.

If you have technical questions or need help with Azure, please try StackOverflow or visit the MSDN Azure AD forums.

Tell us what you think of Azure and what you want to see in the future. If you have suggestions, please submit an idea or vote up an idea at our User Voice Channel - feedback.azure.com.