Azure Privileged Identity Management- Adoption Kit

Contents

Awareness

This section helps you to analyze the benefits of Azure Active Directory (Azure AD) Privileged Identity Management. 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

Organizations want to minimize the number of people who have access to secure information or resources to reduce the chance of unauthorized access, or an authorized user damaging critical organization information.

Azure AD Privileged Identity Management (PIM) helps you manage privileged administrative roles across Azure AD, Azure resources, and other Microsoft Online Services. PIM provides solutions like just-in-time access, request approval workflows, and fully integrated access reviews so you can identify, uncover, and prevent malicious activities of privileged roles in real time.

To learn more, refer to What is Azure AD Privileged Identity Management?

Pricing and Licensing Requirements

Azure PIM capability requires you to use Azure Active Directory Premium P1, Premium P2. Refer to License requirements to use PIM.

For more information about Azure AD licensing and pricing, refer to Azure AD pricing.

Key Benefits

The key benefits of using Azure PIM are:

Manage Risk
Secure your organization by enforcing the principle of Least Privilege Access and just-in-time access. By minimizing the number of permanent assignments of users to privileged roles and enforcing approvals and Multi-Factor Authentication (MFA) for elevation, you can greatly reduce security risks related to privileged access in your organization. It also allows you to view a history of access to privileged roles and track down security issues as they happen.

Address Compliance and Governance
Just-in-time elevation of privileged identities provides a way for PIM to keep track of privileged access activities in your organization. You are also able to view and receive notifications for all assignments of permanent and eligible roles inside your organization. Through access review, you can regularly audit and remove unnecessary privileged identities and make sure your organization is compliant with the most rigorous identity, access, and security standards.

Reduce Costs
Reduce costs by dropping inefficiencies, human error, and security issues by deploying PIM correctly. The net result is a reduction of cyber-crimes associated with privileged identities, which are costly and difficult to recover from. PIM also helps your organization reduce costs associated with auditing access information associated with regulations and standards compliance.

Customer stories/Case studies

Discover how most organizations mitigate risk of excessive, unnecessary, or misused access rights using Azure PIM. The following featured stories demonstrate these needs.

University of Southern Denmark – Research university reduces security workload by 60 percent with automated protection features. SDU team uses Azure AD to synchronize employee identities and help protect them from being compromised, manage their network authentication, and control access to valuable resources. They use Azure AD PIM for critical employee roles.

Mediterranean Shipping Company – Shipping company boosts protection with tighter integration between security layers. IT team manages user identities and access with Microsoft Azure Active Directory (Azure AD)—including its Privileged Identity Management and Identity Protection features.

ASICS EMEA hits the ground running with cloud-based mobility solutions. ASICS EMEA is planning on upgrading to the EMS E5, to take advantage of Microsoft Azure AD Premium P2 which helps to manage and protect privileged accounts using PIM so ASICS can discover, restrict, and monitor administrators and their access to resources and provide just-in-time access when needed.

To learn more about the customer and partner experiences on Azure PIM, 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:

- September 21 2018, Azure AD Privileged Identity Management approval workflows is now available
- June 13 2018, Delegate administration of applications in Azure Active Directory

Training/Learning Resources

The section provides concepts, role-based guidance, and lists the various training resources available on Azure PIM.

Level 100 Knowledge/Concepts

Azure PIM helps you manage the who, what, when, where, and why for resources that you care about. Here are the key features of PIM:

- Provide **just-in-time** privileged access to Azure AD and Azure resources
- Assign **time-bound** access to resources using start and end dates
- Require **approval** to activate privileged roles
- Enforce **multi-factor authentication** to activate any role
- Use **justification** to understand why users activate
- Get **notifications** when privileged roles are activated
- Conduct **access reviews** to ensure users still need roles
- Download **audit history** for internal or external audit

For more information about Azure PIM, refer to the links below:

- What is Azure AD Privileged Identity Management?
- Learn the license requirements to use PIM
- Know the roles you cannot manage in PIM
- Securing privileged access for hybrid and cloud deployments in Azure AD
- Understand Multi-factor authentication (MFA) and PIM
- Use a resource dashboard to perform an access review
- Learn email notifications in PIM
- Understand Microsoft Graph APIs for PIM (Preview)

Role-Based Guidance

IT Administrator Staff

Azure PIM enables you to manage the following roles:

Azure AD roles – These roles are all the directory roles inside Azure Active Directory (such as Global Administrator, Exchange Administrator, and Security Administrator).

Azure resource roles – These roles are linked to an Azure resource, resource group, subscription, or management group. PIM provides just-in-time access to both built-in roles like Owner, User Access Administrator, and Contributor, as well as custom roles. These roles also include the custom roles attached to your management groups, subscriptions, resource groups, and resources. However, there are few roles that you cannot manage. See Roles you cannot manage in PIM

Refer to the following links to learn more on Azure PIM support:

- What are the administrator role permissions in Azure Active Directory?

- What are the administrator roles by admin task in Azure Active Directory?
- What is role-based access control (RBAC) for Azure resources?
- What is Azure AD Privileged Identity Management?
- How do you deploy Azure AD Privileged Identity Management (PIM)?
- How can you start using PIM?
- Start monitoring Azure PIM

Help Desk Staff

- Search for PIM Terminology to better understand PIM and its documentation
- Search the Microsoft Support Knowledge Base for solutions to common technical issues.
- Search for and browse technical questions and answers from the community, or ask questions in the Azure Active Directory forums.

Training

On-Demand Webinars

Reserve here – Azure AD Identity Protection and Privileged Identity Management

Videos

- Azure videos - Lock down access to Azure using Identity
- YouTube - Protect the Keys to your Kingdom: Azure Privileged Identity Management
- Channel 9 - Azure AD Privileged Identity Management
- Channel 9 - Approval Workflows for Azure Active Directory Privileged Identity Management
- Channel 9 - Azure AD Privileged Identity Management: Security Wizard, Alerts, Reviews

Online Courses

- PluralSight.com- Implementing Microsoft Azure Privileged Identity Management
  "In this course, you'll learn how to use Microsoft PIM to manage, control, and monitor access within Azure AD, Azure resources, and Microsoft Online Services."

- SkillUp.Online- Securing Identities
  "This course focuses on three key areas for defending against attackers who target security vulnerabilities, focused on credential theft and compromised identities: Role-Based Access Control (RBAC), Multi-Factor Authentication (MFA), and Azure Active Directory Privileged Identity Management (PIM)."

Whitepaper

- Published August, 2018, Security best practices for Azure solutions
  This paper is a collection of security best practices to use when designing, deploying, and managing your cloud solutions using Azure.

- Published October 31, 2017, Azure security technical capabilities

This white paper focus on Microsoft Azure technical capabilities available to you as a customer to fulfill your role in protecting the security and privacy of your data.

End-user Readiness and Communication

This section provides customizable posters and email templates to roll out Azure PIM to your organization.

Depending on the number of impacted administrators, organizations often elect to create an internal document, a video, or an email about the change. Refer to Communicate PIM to affected stakeholders when you deploy Azure AD Privileged Identity Management (PIM).

Planning and Change Management

This section provides the resource links to Azure PIM deployment plan and topology to help you determine your PIM strategies, and document your decisions and configurations to prepare for implementation.

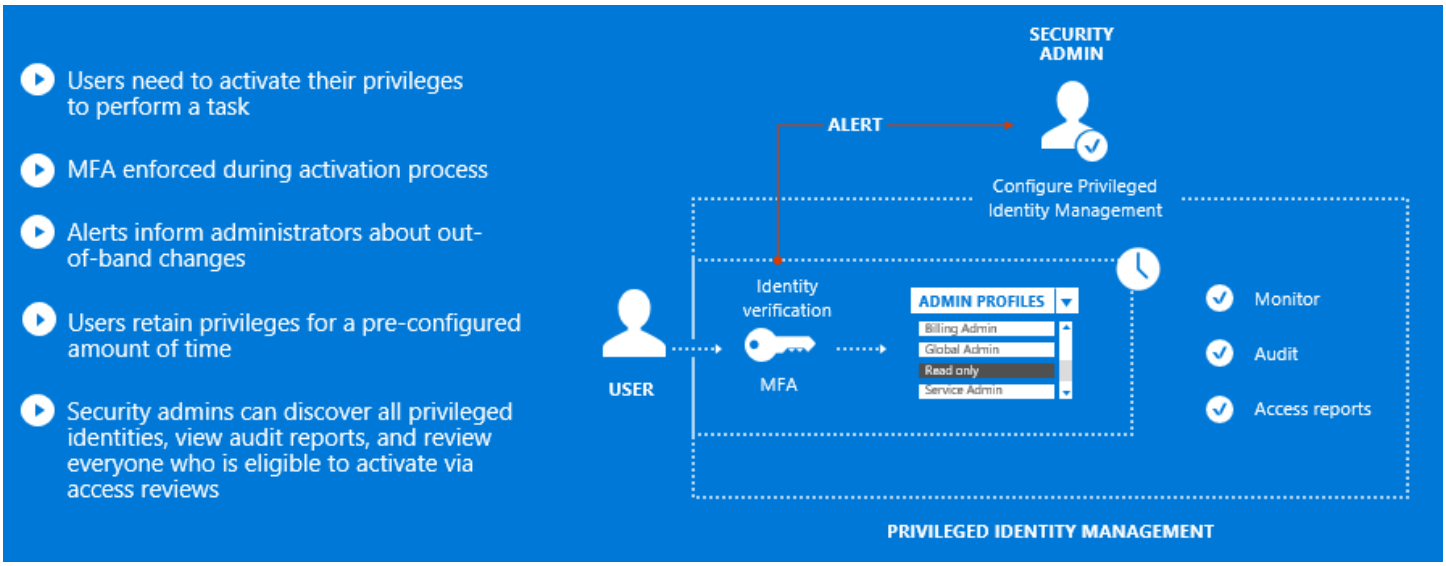
Deployment Plan

Refer to Deploy Azure AD Privileged Identity Management (PIM). Follow the steps below:

1. Learn about PIM
2. Plan your deployment

Architecture Plan/Topology

High-level overview of how PIM works



Testing

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

Refer to Implement your solution when you deploy Azure AD Privileged Identity Management (PIM). Follow the steps below:

1. Identify test users to validate the implementation.
2. Use test implementation to configure PIM for your test users.

Deployment

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

Deployment

Refer to Implement your solution when you deploy Azure AD Privileged Identity Management (PIM). Follow the steps below:

1. Once testing is complete and successful, move to production by repeating all the steps in the testing phases for all the users of each role defined in your PIM configuration.
2. Follow the rollback steps in the case a rollback is needed when PIM failed to work as desired in the production environment.

With the deployment of PIM comes added PIM features that you should use for security and compliance. See Next steps after deploying PIM.

Readiness Checklist

Refer to License requirements to use PIM.

Design Template

Refer to Deploy Azure AD Privileged Identity Management (PIM).

Operations

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

Operations

Refer to Start using PIM to enable and get started with PIM.

Monitoring

Administrators and Azure AD members can refer to the following links to monitor Azure PIM:

Activate My Roles

- Activate my Azure AD directory roles in PIM
- Activate my Azure resource roles in PIM

Configure PIM

- Azure AD roles security wizard in PIM
- Discover Azure resources to manage in PIM
- Grant access to other administrators to manage PIM
- Elevate access to manage all Azure subscriptions and management groups

Manage Directory Roles

- Assign Azure AD administrator roles in PIM
- Approve or deny requests for Azure AD directory roles in PIM
- Configure Azure AD directory role settings in PIM
- Configure security alerts for Azure AD directory roles in PIM
- View audit history for Azure AD directory roles in PIM

Manage Azure Resources Roles

- Assign Azure resource roles in PIM
- Invite guest users and assign Azure resource access in PIM
- Approve or deny requests for Azure resource roles in PIM
- Extend or renew Azure resource role assignments in PIM
- Configure Azure resource role settings in PIM
- Configure security alerts for Azure resource roles in PIM
- View activity and audit history for Azure resource roles in PIM
- Use custom roles for Azure resources in PIM

Review Access

Directory Roles

- Perform an access review of my Azure AD directory roles in PIM
- Start an access review for Azure AD directory roles in PIM
- Complete an access review for Azure AD directory roles in PIM

Azure Resources Roles

- Perform an access review of my Azure resource roles in PIM
- Start an access review for Azure resource roles in PIM
- Complete an access review for Azure resource roles in PIM

Troubleshooting

References

Refer to Privileged Identity Management: Terminology

Support and Feedback

How can we improve Azure AD PIM? 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.