Using Azure AD Privileged Identity Management for elevated access

Throughout Microsoft, there are employees who require elevated access to Microsoft Online Services, Microsoft Azure, and on-premises services that they own, manage, or support. At Core Services Engineering and Operations (CSEO, formerly Microsoft IT), we knew that we needed to manage any potential risks that elevated access can introduce, such as “pass the hash” or credential theft. We wanted to better manage privileged identities and monitor elevated access for cloud resources.

Microsoft doesn’t allow persistent elevated access, so we use the Azure Active Directory (Azure AD) Privileged Identity Management (PIM) feature of just-in-time role activation (JIT) to temporarily elevate the role-based access as needed for a defined time. Before the release of Azure AD PIM, our Azure Active Directory administrative roles had persistent elevated access, monitoring was limited, and we didn’t have a fully managed lifecycle.

Azure Active Directory uses administrative roles to control access to various features within the tenant. Recent changes introduced in Azure AD PIM have enabled a cloud-based, JIT tool for Azure Active Directory administrative roles as well as Azure administrative roles. Both Azure Active Directory administrative roles as well as Azure administrative roles can be assigned and remain inactive until needed. We configured Azure AD PIM, available with the Premium P2 edition of Azure AD, to help us manage and monitor our Azure AD administrative roles through the Azure portal.

Identity management at Microsoft

Identity management at Microsoft encompasses all process and tools used to manage the lifecycle of all identities for all our corporate employees. Of the roughly 285,000 identities that we currently manage at Microsoft, there are approximately 10,000 on-premises accounts and 400 Azure AD accounts of users who require elevated access to data and services. When we started using PIM, we did an attestation to reduce the number of individual users who might need individual assignments. Since then, we have reduced the number of users who are candidates for global administrator by 83 percent, and removed all persistent users (except for a break-glass account) from the global-administrator role. We regularly add more roles that require elevated access, so we’ve seen the number of managed users grow slowly but consistently.

Privileged Identity Management focuses on the tools and processes we use for a subset of users that have administrative—or elevated—access to on-premises and cloud-hosted data and services at Microsoft.

Reducing the attack surface

There are a couple of obvious ways we can look at reducing the risks, or attack surface, of elevated access—by reducing the number of accounts or the duration that an account has elevated access. We rationalize incoming requests for elevated access, but we can’t necessarily reduce the number of people that require it to do their jobs. We’ve adopted the strategy of reducing risks by giving employees just enough access to the resources that they need, for only as long as they need it. At Microsoft, the only people who are authorized to assign others to roles are Privileged Role Administrators. We monitor unauthorized assignment of roles, and the addition of users who are not authorized to be assigned to roles. If anyone else tries to assign a role, it is automatically flagged as a violation of role-assignment policy.

Typically, the more elevated access a privileged role has, the more rigorously we protect it. At the front end of the process, the review board spends more time evaluating requests for more privileged roles. The employee request process requires multiple levels of approvals. After the request is approved, we can require tighter controls, including multifactor authentication or physical credential, like smart cards. We also set shorter access durations through JIT access.
Azure AD PIM

By configuring Azure AD PIM to manage our elevated access roles in Azure AD, we now have JIT access for more than 28 configurable privileged roles. We can also monitor access, audit account elevations, and receive additional alerts through a management dashboard in the Azure portal.

Elevated access workflow

Elevated access includes job roles that need greater access, including support, resource administrators, resource owners, service administrators, and global administrators. We manage role-based access at the resource level. Because elevated access accounts could be misused if they’re compromised, we rationalize new requests for elevated access and perform regular re-attestation for elevated roles.

At Microsoft, when an individual joins a team or changes teams, they might need administrative rights for their new business role. For example, someone might join a team in which their user account will require Exchange Online Administrator privileged access rights in the future. That user makes a request, then their manager validates that user’s request, as does a service owner. With those approvals, CSEO administrators in the Privileged Role Administrator role are notified. A CSEO administrator uses Azure AD PIM via the Azure Portal to make that user eligible for that role. The user can then use Azure AD PIM to activate that role.

Figure 1 shows a diagram of the elevated access workflow.

![Figure 1. Azure AD PIM elevated access workflow](image)

The following table describes the processes we use for granting elevated access for both on-premises and cloud-hosted resources. We’re currently building a solution that will combine the on-premises and Azure AD elevated access workflows into a single workflow with a centralized management point. For more information, see the “Looking
ahead: Expanding use of Azure AD PIM” section later in this article. CSEO and the product group are working together to automate the request-access process.

Table 1. Elevated access processes

<table>
<thead>
<tr>
<th>Process</th>
<th>On-premises</th>
<th>Azure</th>
</tr>
</thead>
<tbody>
<tr>
<td>User request</td>
<td>Employee submits access request through online form.</td>
<td>Employee submits access request through online form.</td>
</tr>
<tr>
<td>Request review</td>
<td>Management reviews request and approves or denies it. Online training and multiple levels of approval might be required, based on the type of request.</td>
<td>Management reviews request and approves or denies it. Online training and multiple levels of approval might be required based on the type of request.</td>
</tr>
<tr>
<td>Approval</td>
<td>User is added to the approved elevated access silo for the requested resource in the web portal that manages on-premises privileged access.</td>
<td>User is added to the approved elevated access role for the requested Azure or Microsoft Online Services resource in Azure’AD PIM.</td>
</tr>
<tr>
<td>Notification</td>
<td>Sent via email to employee.</td>
<td>Sent via email to employee.</td>
</tr>
<tr>
<td>Employee performs elevated action</td>
<td>Employee signs in using multifactor authentication and the on-premises JIT tool elevates their privileges for a specific time-bound duration.</td>
<td>Employee signs in to the Azure portal to manage their resource using multifactor authentication, and Azure AD PIM elevates their privileges for a specific time-bound duration.</td>
</tr>
</tbody>
</table>

**JIT administrator access**

Historically, we could assign an employee to an administrative role through the Azure portal or through Windows PowerShell and that employee would be a permanent administrator; their elevated access would remain active in the assigned role.

Azure AD PIM introduced the concept of permanent and eligible administrators in Azure AD and Azure. Permanent administrators have persistent elevated role connections; whereas, eligible administrators have privileged access only when they need it. The eligible administrator role is inactive until the employee needs access, then they complete an activation process and become an active administrator for a set amount of time. We’ve stopped using permanent administrators for named individual accounts, although we do have some automated service accounts that still use the role.

**Role activation in Azure Active Directory**

Azure AD PIM uses administrative roles, such as tenant admin and global admin, to manage temporary access to various roles. With Azure AD PIM, you can manage the administrators by adding or removing permanent or eligible administrators to each role. Azure AD PIM includes a number of built-in Azure AD roles as well as Azure that we manage.
To activate a role, an eligible admin will initialize Azure AD PIM in the Azure portal and request a time-limited role activation. The activation is requested using the Activate my role option in Azure AD PIM. Users requesting activation must satisfy conditional access policies to ensure that they are coming from authorized devices and locations, and their identities must be verified through multi-factor authentication.

To help secure transactions while enabling mobility, we use Azure AD PIM to customize role activation variables in Azure, including the number of sign-in attempts, the length of time the role is activated after sign-in, and the type of credentials required (such as single sign-in or multifactor authentication).

**Tracking the use of privileged roles using the dashboard**

A dashboard through the Azure portal gives a centralized view of:

- Alerts that point out opportunities to improve security.
- The number of users who are assigned to each privileged role.
- The number of eligible and permanent admins.
- Ongoing access reviews.

We can track how employees and admins are using their privileged roles by viewing the audit history or by setting up a regular access review. Both options are available through the PIM dashboard in the Azure portal.

The PIM audit log tracks changes in privileged role assignments and role activation history. We use the audit log to view all user assignments and activations within a specified period. The audit history helps us determine, in real time, which accounts haven’t signed in recently, or if employees have changed roles.

Access reviews can be performed by an assigned reviewer, or employees can review themselves. This is an effective way to monitor who still needs access, and who can be removed.

We’re looking at the data that’s collected, and the monitoring team is assessing the best way to configure monitoring alerts to notify us about out-of-band changes—for example, if too many administrator roles are being created for an Azure resource. The information also helps us determine whether our current elevation time settings are appropriate for the various privileged admin roles.

**Looking ahead: Expanding use of Azure AD PIM**

**Unified management point and automated end-to-end workflows**

We’re currently using similar processes but different methods and tools to manage privileged identities for Azure-based and on-premises assets or tenants.

We’re streamlining and operationalizing our process by customizing and deploying an application that will automate and provide a single management point for the entire workflow for both Azure AD and on-premises identity management. The application will integrate both the on-premises privileged identity management tools and Azure AD PIM through its APIs.

The application will provide a unified view for both cloud and on-premises elevated accounts, along with a single portal for our security administrators to monitor elevated access activity. The application will help operationalize our processes by automating:

- Access request process, including the workflow that secures all the required approvals.
- Multifactor authentication enforcement for access requests.
- Lifecycle management, through JIT access enablement and removal when action is complete.

To provide more security, we’ve integrated secure admin workstations for employees who have elevated administrator access to on-premises, tenant, and Azure subscription resources. The secure admin workstations include
enhanced hardware and configuration-based security features that help protect elevated credentials from being compromised. We’re considering required secure admin workstations for Azure AD global administrators.

**Using Azure AD PIM for managing your Tenant and Azure subscriptions**

With Azure Active Directory PIM, we manage, control, and monitor access within our organization. This includes access to Azure AD and other Azure resources, and Microsoft Online Services like Office 365 and Microsoft Intune. For more information on Azure AD PIM, [click here](https://microsoft.com/itsshowcase).

Like all organizations, we want to minimize the number of people who have access to our secure information or resources, because that reduces the chance of a malicious user getting access or an authorized user inadvertently impacting a sensitive resource. However, our people still need to carry out privileged operations in Azure AD, Azure, Office 365, and SaaS apps. We can give users privileged access to Azure resources like Subscriptions, and Azure AD. Oversight is needed for what our users are doing with their admin privileges. We use Azure AD PIM to mitigate the risk of excessive, unnecessary, and misused access rights.

We use Azure AD PIM in the following ways:

- See which users are assigned privileged roles to manage Azure resources, as well as which users are assigned administrative roles in Azure AD.
- Enable on-demand, “just in time” administrative access to Microsoft Online Services like Office 365 and Intune, and to Azure resources of subscriptions, resource groups, and individual resources such as Virtual Machines.
- See a history of administrator activation, including what changes administrators made to Azure resources.
- Get alerts about changes in administrator assignments.
- Require approval to activate Azure AD privileged admin roles.
- Review membership of administrative roles and require users to provide a justification for continued membership.

In Azure AD, we use Azure AD PIM to manage the users we assign to built-in Azure AD organizational roles, such as Global Administrator. In Azure, we use Azure AD PIM to manage our users and groups that we assign via Azure RBAC roles, including Owner and Contributor.

**For more information**

**Microsoft IT Showcase**

[microsoft.com/itsshowcase](https://microsoft.com/itsshowcase)

**Azure AD Privileged Identity Management**

© 2018 Microsoft Corporation. All rights reserved. Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners. This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY.