Identity and Access Management
advanced specialization

Program Overview and Requirements
Program Overview

Partners who demonstrate deep knowledge, extensive experience, and proven experience deploying Microsoft Identity workloads with Azure Active Directory (Azure AD) may seek the Identity and Access Management advanced specialization.

“Identity and threat protection are high on customers’ minds. Getting identity right is a critical part of a Microsoft 365 engagement and is the first place we start.”

-forrester 2020 Microsoft 365 Enterprise Total Economic Impact Study
(A commissioned study conducted by Forrester ConsultingTM on behalf of Microsoft, June 2020)

As our world undergoes rapid digital transformation, we are seeing both increasingly sophisticated security threats and protection measures. That new security paradigm is addressed by a Zero Trust framework, which puts identity at the forefront of verifying every access, and connects security solutions across the entire digital estate. From identity to data, apps, infrastructure, network, and endpoints, Microsoft 365 is built on the principles of Zero Trust, with a strong cloud identity at its core.

Customers today are facing many challenges related to identity and access management—like numerous apps, devices, and users across and outside of the corporate network. As the organizational barriers blur between who is in and out of your network, organizations struggle to manage identities for not only their employees, but also external partners, suppliers and distributors, and even end consumers and customers or citizens. In addition to this, COVID-19 accelerated this trend as organizations had to rapidly transition their employees to work remotely and identify secure and cost-effective solutions for business continuity.

There was a 300% increase in identity-related attacks last year, and customers are looking for reliable partners and new ways to proactively protect and monitor the security of IP and customer data to safeguard businesses. The Identity and Access Management advanced specialization is designed to help customers identify which partners have the technical capabilities and proven experience in deploying Microsoft Identity workloads with Azure AD.

Partners who earn this advanced specialization will have a customer-facing label displayed on their business profile in the Microsoft partner directory and be prioritized in customer searches to increase visibility to new business. For those reasons, this opportunity is available only to partners who meet these additional requirements.

Learn more about advanced specializations
What are the requirements?
Eligible partners must meet the highest standards for service delivery and support. All requirements will be verified by Microsoft and/or a third-party vendor, either automatically or by manual review, and are subject to change.

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Related competency</td>
<td>Maintain an active Gold Security competency.</td>
</tr>
<tr>
<td>Performance</td>
<td>Achieve a minimum of 2,000 Monthly Active Usage (MAU) growth of Azure Active Directory Premium (Azure AD Premium) in a trailing 12-month period (CPOR data).</td>
</tr>
<tr>
<td>Knowledge</td>
<td>Your organization must have at least six individuals who have passed MS-500: Microsoft 365 Security Administrator.</td>
</tr>
<tr>
<td>Customer references</td>
<td>Provide three customer references that demonstrate your organization's ability to deploy Microsoft Identity workloads with Azure AD. Review our guidelines for customer references before submitting.</td>
</tr>
<tr>
<td>Annual renewal</td>
<td>Your advanced specialization and associated benefits will remain in place for one year but require that you keep your Gold competency status in place. If you do not maintain your Gold cloud competency, you will lose your advanced specialization status. On your renewal date, you will need to meet the current requirements which may evolve over time.</td>
</tr>
</tbody>
</table>

How do I apply?
Only administrators of an organization's Microsoft partner account can submit an application for the Identity and Access Management advanced specialization on behalf of the organization. If you have the appropriate role and access, you can apply by signing in to Partner Center and navigating to your Partner Center dashboard > Competencies > Advanced Specialization. If you are still in PMC, review our help page and transition guide to learn more about how to move your membership to Partner Center. Once you have moved, you can apply through your Partner Center dashboard.