แบบรายงานการประชุม/ฝึกอบรม/สัมมนา/ศึกษาดูงาน

หน่วยงาน ศูนย์วิทยบริการ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏสวนสุนันทา

๑. ข้อมูลส่วนบุคคล

ชื่อ-สกุล นายนิคม อรุณฉาย **ตำแหน่ง** นักวิชาการคอมพิวเตอร์

กลุ่มบุคลากร ☐ สายวิชาการ ☑ สายสนับสนุนวิชาการ

๒. หลักสูตรหรือเรื่องที่เข้าร่วมประชุม/ฝึกอบรม/สัมมนา/ศึกษาดูงาน

โครงการอบรมสัมมนาออนไลน์ในหัวข้อ "เรียนรู้ระบบพิสูจน์ตัวตนโดยใช้ Microsoft Entra ID และฟีเจอร์ใหม่ในปี 2025"

๓. วิทยากรในการสัมมนา

อาจารย์วิสิทธิ์ ทองภู่ Microsoft MVP

๔. สถาบันหรือหน่วยงานที่จัดสัมมนา

บริษัทเทรโนเคท(ประเทศไทย) ร่วมกับ Microsoft ประเทศไทย

๕. ระยะเวลาที่เข้ารับการสัมมนา

วันจันทร์ที่ ๑๗ กุมภาพันธ์ ๒๕๖๘ เวลา ๐๙.๐๐ - ๑๒.๐๐ น. โดยออนไลน์สดผ่าน Microsoft teams

๖. งบประมาณที่ใช้ในการสัมมนา

ไม่มีค่าใช้จ่าย

๗. วัตถุประสงค์ของการสัมมนา

๑. เพื่อให้ผู้เรียนได้เรียนรู้โซลูชันการจัดการตัวตน การเข้าถึงทรัพยากรจาก Microsoft ที่ช่วยให้องค์กรสามารถจัดการ และปกป้องข้อมูลประจำตัวของพนักงานได้อย่างมีประสิทธิภาพ

๒. เพื่อให้ผู้เรียนได้เรียนรู้ถึงฟีเจอร์ใหม่ ๆ อัพเดตล่าสุดในปี 2025

๘. สรุปเนื้อหาสาระของการสัมมนา

Agenda

1. Identity Fundamental Concept
2. Introduction to Identity and Access Management (IAM)
3. Microsoft Entra & Microsoft Entra ID?
4. Microsoft Entra ID Use Cases

1. Identity Fundamental Concept

ตัวตนคืออะไร

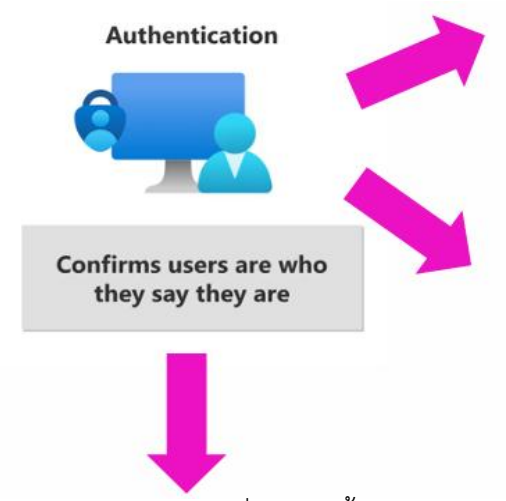
เป็นชุดของตัวระบุหรือคุณลักษณะเฉพาะที่แสดงถึงมนุษย์ ส่วนประกอบของซอฟต์แวร์ เครื่องจักร ทรัพย์สิน หรือทรัพยากรในระบบคอมพิวเตอร์ ตัวระบุอาจสามารถเป็นได้ดังนี้

- ที่อยู่อีเมลล์
- ชื่อผู้ใช้ และรหัสผ่าน
- การใช้งาน
- ฯลฯ

แบ่งเป็น 3 ประเภท

1. Human Identities คือ ตัวแทนของบุคคล เช่น พนักงาน (พนักงานภายในและบุคลากรหน้างาน คนงาน) และผู้ใช้ภายนอก (ลูกค้า ที่ปรึกษา ผู้ขาย และหุ้นส่วน)
2. Workload Identities คือ ปริมาณงานซอฟต์แวร์ เช่น แอปพลิเคชัน บริการ สคริปต์ หรือภาชนะ
3. Device Identities คือ อุปกรณ์ต่างๆ เช่น คอมพิวเตอร์ตั้งโต๊ะ โทรศัพท์มือถือ IoT เซ็นเซอร์ และอุปกรณ์ที่ได้รับการจัดการ IoT ข้อมูลระบุตัวตนของอุปกรณ์แตกต่างจากตัวตนของมนุษย์

การรับรองความถูกต้อง



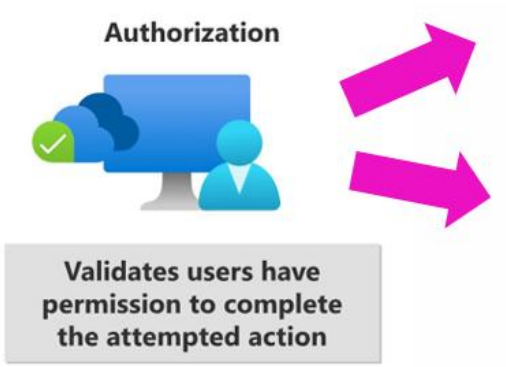
การรับรองความถูกต้อง เป็นกระบวนการท้าทายบุคคล ซอฟต์แวร์ หรืออุปกรณ์ฮาร์ดแวร์สำหรับข้อมูลรับรองเพื่อยืนยันตัวตน หรือพิสูจน์ว่าพวกเขาเป็นใครหรือสิ่งที่พวกเขาอ้างว่าเป็น การรับรองความถูกต้อง โดยทั่วไปต้องใช้ข้อมูลรับรอง (เช่น ชื่อผู้ใช้ และรหัสผ่าน ลายนิ้วมือ ใบรับรอง หรือ P. แบบครั้งเดียว บางครั้งการรับรองความถูกต้องจะสั้นลง

การรับรองความถูกต้องหลายปัจจัย (MFA)
เป็นมาตรการรักษาความปลอดภัยที่ กำหนดให้ผู้ใช้จัดเตรียมหลักฐานมากกว่า 1 ชิ้นเพื่อตรวจสอบ ตัวตนของพวกเขา เช่น

- สิ่งที่พวกเขารู้ เช่น รหัสผ่าน
- สิ่งที่พวกเขามี เช่น เหรียญตราหรือโทเค็นความปลอดภัย
- บางสิ่งบางอย่าง เช่น ไบโอเมตริกซ์ (ลายนิ้วมือหรือใบหน้า)

อนุญาตให้ใช้การลงชื่อเพียงครั้งเดียว (SSO) ผู้ใช้เพื่อตรวจสอบสิทธิ์ของตน ตัวตนครั้งแล้วครั้งเล่า ตรวจสอบสิทธิ์อย่างเงียบๆ เมื่อใด การเข้าถึงทรัพยากรต่างๆ ที่ต้องอาศัยอัตลักษณ์เดียวกัน

การอนุญาต



การอนุญาต ตรวจสอบว่าผู้ใช้ เครื่องจักร หรือซอฟต์แวร์ ได้รับสิทธิ์ในการเข้าถึงทรัพยากรบางอย่าง การอนุญาต บางครั้งก็สั้นลง

ในข้อกำหนดด้านความปลอดภัยทางไซเบอร์ การอนุญาตจะกำหนดระดับ ของการเข้าถึงหรือการอนุญาตที่บุคคลที่ได้รับการตรวจสอบสิทธิ์ต้องมี ข้อมูลและทรัพยากรขององค์กร

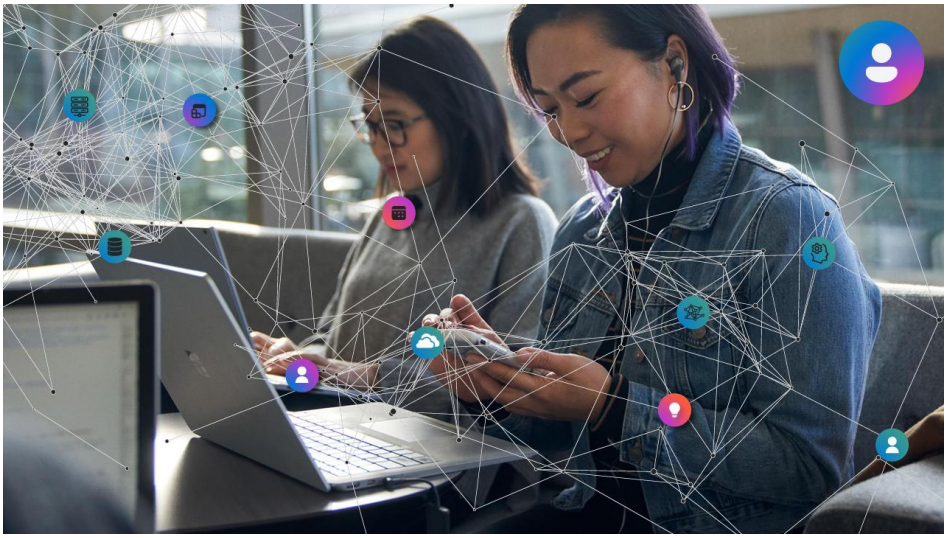
Identity Fundamental Concept | Identity Provider

การรับรองความถูกต้องสมัยใหม่เป็นคำศัพท์ทั่วไปสำหรับการรับรองความถูกต้องและการอนุญาตระหว่างไคลเอนต์ เช่น แล็ปท็อปหรือโทรศัพท์ และเซิร์ฟเวอร์ เช่น เว็บไซต์ หรือ แอปพลิเคชัน. ที่ศูนย์กลางของการรับรองความถูกต้องสมัยใหม่ คือบทบาทของ “ผู้ให้บริการข้อมูลประจำตัว”

ผู้ให้บริการข้อมูลประจำตัวจะสร้าง ดูแลรักษา และจัดการข้อมูลประจำตัวในขณะที่นำเสนอ บริการรับรองความถูกต้อง การอนุญาต และการตรวจสอบ

ด้วย Modern Authentication จะมีการจัดเตรียมบริการทั้งหมด รวมถึงบริการ Authentication ทั้งหมดด้วย โดยผู้ให้บริการข้อมูลประจำตัวกลาง ข้อมูลที่ใช้ในการตรวจสอบผู้ใช้กับเซิร์ฟเวอร์ ถูกจัดเก็บและจัดการจากส่วนกลางโดยผู้ให้บริการข้อมูลประจำตัว

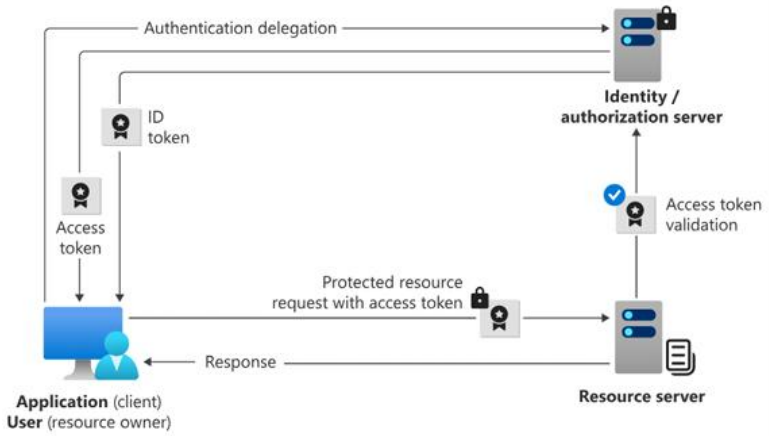
ด้วยผู้ให้บริการข้อมูลประจำตัวส่วนกลาง องค์กรต่างๆ สามารถสร้างการรับรองความถูกต้องและการอนุญาต นโยบาย ติดตามพฤติกรรมผู้ใช้ ระบุกิจกรรมที่น่าสงสัย และลดการโจมตีที่เป็นอันตราย

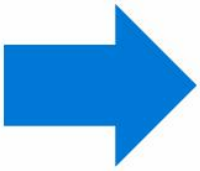


2. Identity and Access Management (IAM)

การจัดการข้อมูลประจำตัวและการเข้าถึงช่วยให้แน่ใจว่าบุคลากร เครื่องจักร และส่วนประกอบซอฟต์แวร์ที่เหมาะสมจะสามารถเข้าถึงสิทธิ์ได้ ทรัพยากรในเวลาที่เหมาะสม

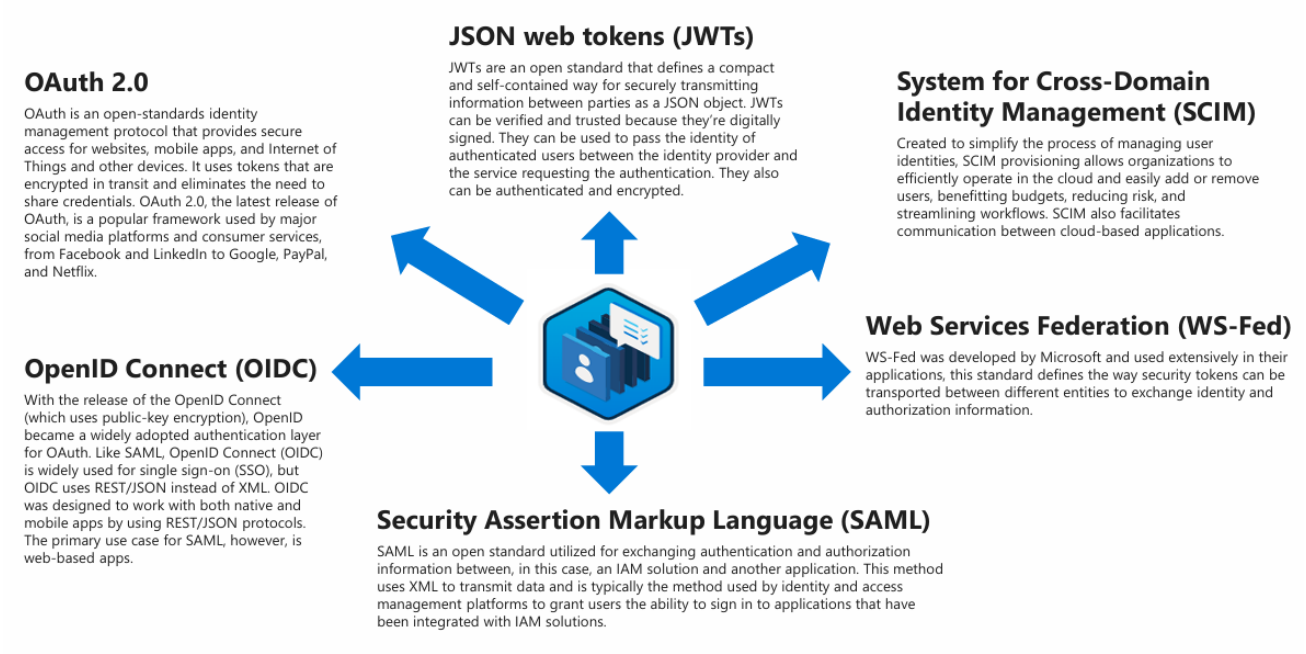
ขั้นแรก บุคคล เครื่องจักร หรือส่วนประกอบซอฟต์แวร์พิสูจน์ว่าพวกเขาเป็นใครหรือสิ่งที่พวกเขาอ้างสิทธิ์เป็นเจ้าของ จากนั้น บุคคล เครื่องจักร หรือส่วนประกอบซอฟต์แวร์จะได้รับอนุญาตหรือปฏิเสธการเข้าถึงหรือใช้งาน ของทรัพยากรบางอย่าง



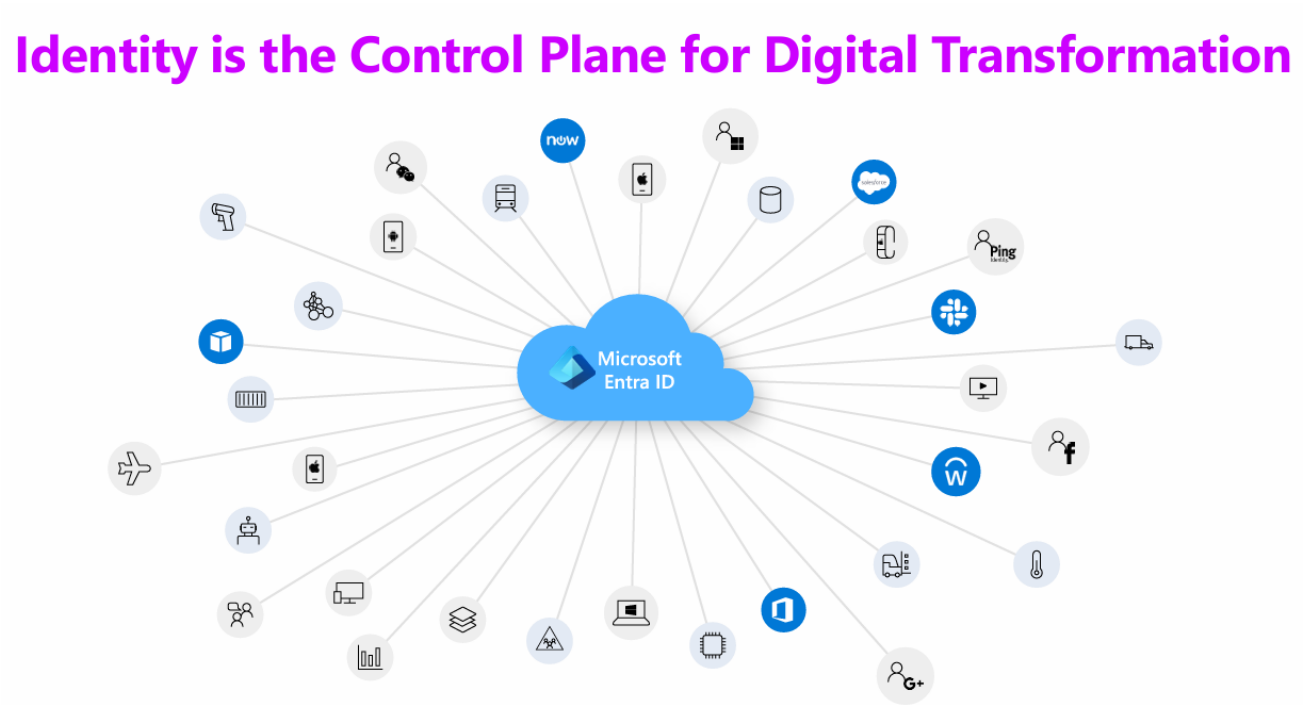


- **Identity management** - The process of creating, storing, and managing identity information. Identity providers (IdP) are software solutions that are used to track and manage user identities, as well as the permissions and access levels associated with those identities.
- **Identity federation** - You can allow users who already have passwords elsewhere (for example, in your enterprise network or with an internet or social identity provider) to get access to your system.
- **Provisioning and deprovisioning of users** - The process of creating and managing user accounts, which includes specifying which users have access to which resources, and assigning permissions and access levels.
- **Authentication of users** - Authenticate a user, machine, or software component by confirming that they're who or what they say they are. You can add multifactor authentication (MFA) for individual users for extra security or single sign-on (SSO) to allow users to authenticate their identity with one portal instead of many different resources.
- **Authorization of users** - Authorization ensures a user is granted the exact level and type of access to a tool that they're entitled to. Users can also be portioned into groups or roles so large cohorts of users can be granted the same privileges.
- **Access control** - The process of determining who or what has access to which resources. This includes defining user roles and permissions, as well as setting up authentication and authorization mechanisms. Access controls regulate access to systems and data.
- **Reports and monitoring** - Generate reports after actions taken on the platform (like sign-in time, systems accessed, and type of authentication) to ensure compliance and assess security risks. Gain insights into the security and usage patterns of your environment.

IAM | Authentication & Authorization Protocols

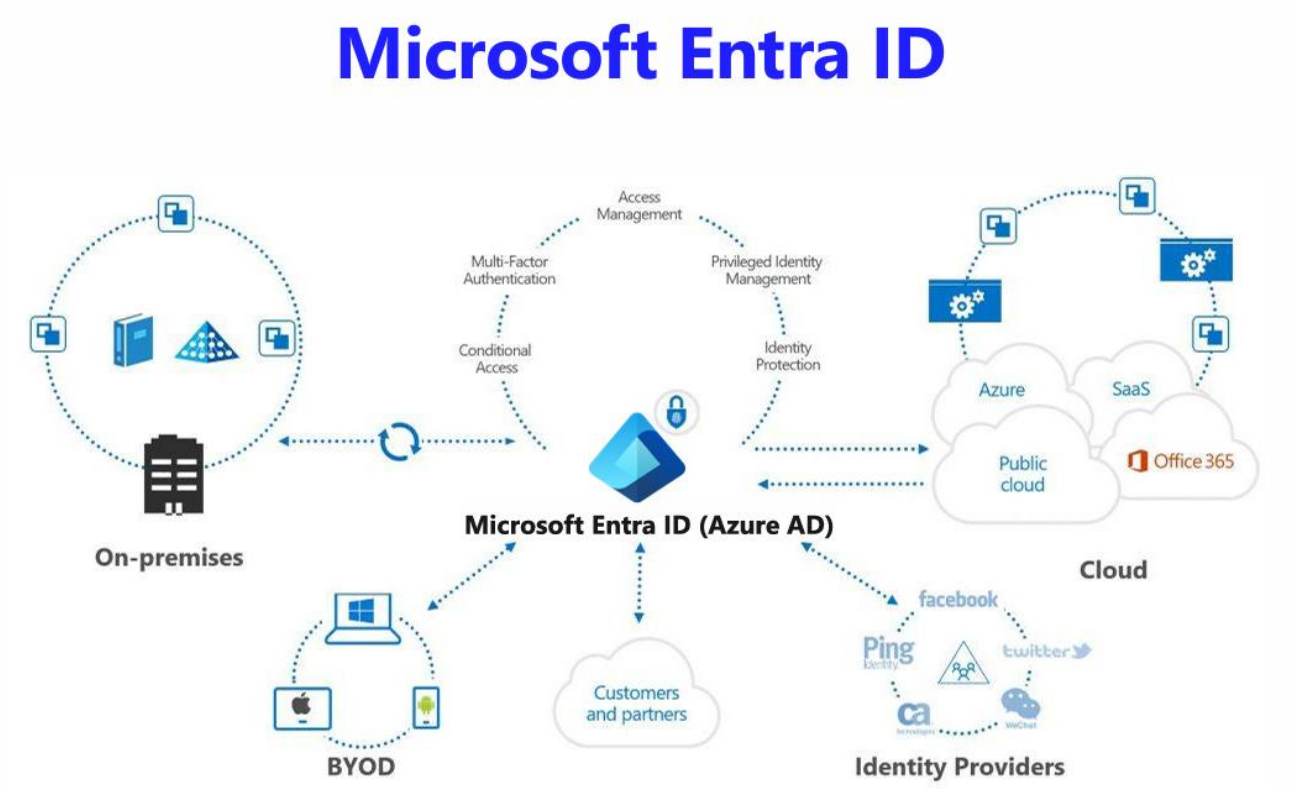


3. Microsoft Entra & Microsoft Entra ID



Microsoft Entra ID

หรือชื่อเดิมคือ Azure Active Directory (Azure AD) เป็น Service ที่ให้บริการเกี่ยวกับ Identity and Access Management (IAM) โดยตัวของ Microsoft Entra ID นั้นจะมาพร้อมกับ Cloud Services ของ Microsoft เช่น Microsoft Azure, Microsoft 365, เป็นต้น ถ้ามองในเรื่องของโครงสร้างของ Microsoft Entra ID จะมีโครงสร้างในลักษณะที่เป็น Flat Structure โดยเริ่มจาก Microsoft Entra Tenant (หรือเรียกสั้นๆ ว่า Tenant), และ Accounts ซึ่งใน Microsoft Entra ID supported Accounts อยู่ 2 ชนิด คือ User และ Group Accounts หรือจะเรียกว่า Identity ก็ได้ครับ ในส่วนของ Protocols ที่เกี่ยวข้องกับ Microsoft Entra ID มีหลาย Protocols ครับ เช่น OAuth, OpenID, SAML, และอื่นๆ นอกจากนี้แล้วตัวของ Microsoft Entra ID มีความสามารถในการไป Integrate ทำงานร่วมกับ Cloud/SaaS Apps, ,การบริหารจัดการ Devices, สามารถ Integrate กับ Active Directory Domain Service (AD DS) เพื่อทำ Hybrid Identity Scenario, และอื่นๆ

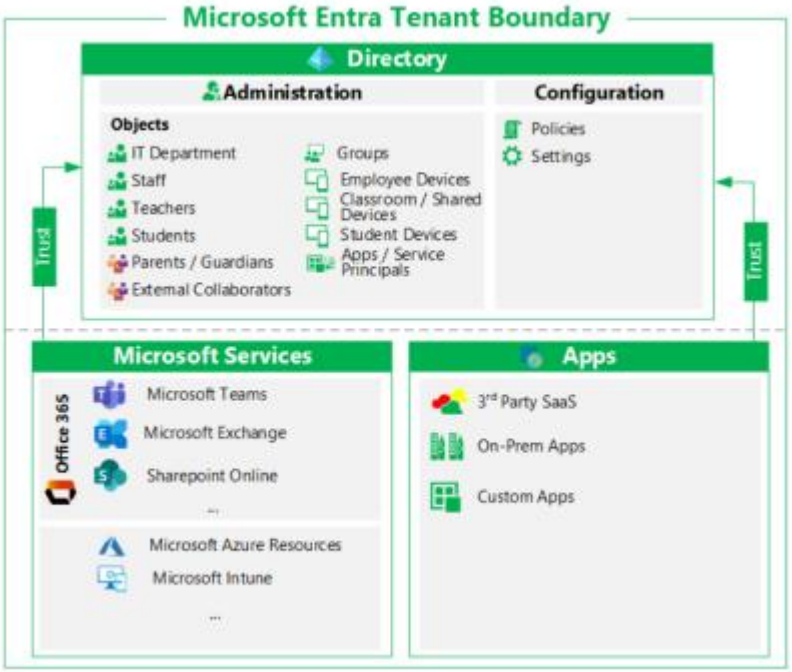


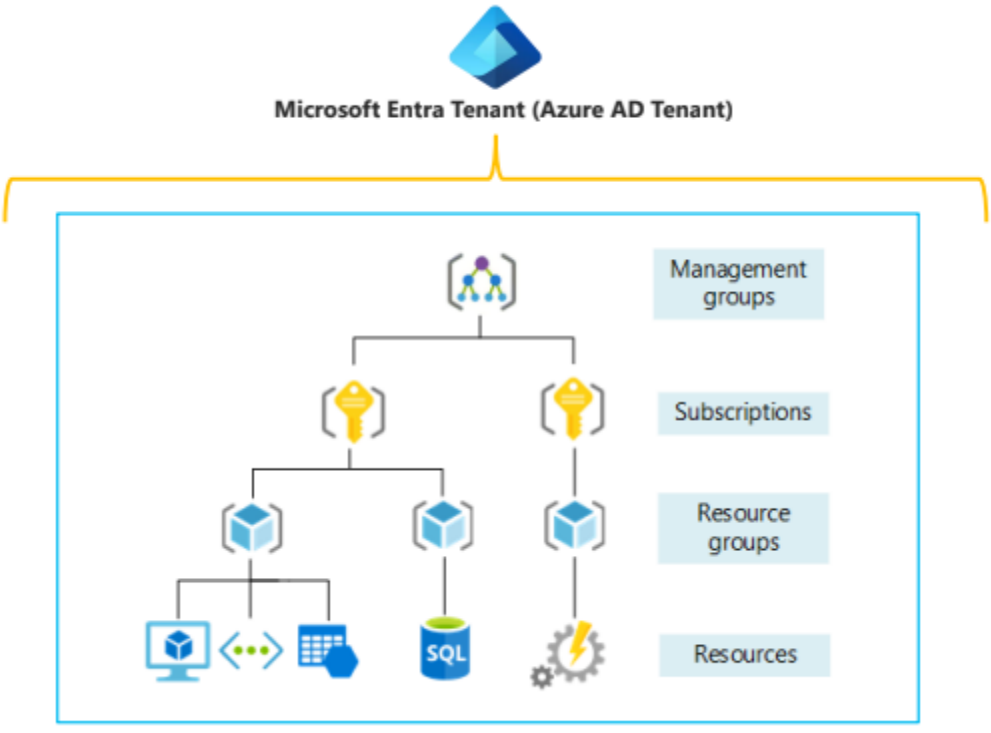
Microsoft Entra Terminology | Tenant

Microsoft Entra Tenant มอบข้อมูลประจำตัวและการเข้าถึง การบริหารจัดการ (IAM) แอปพลิเคชันและทรัพยากรที่องค์กรใช้

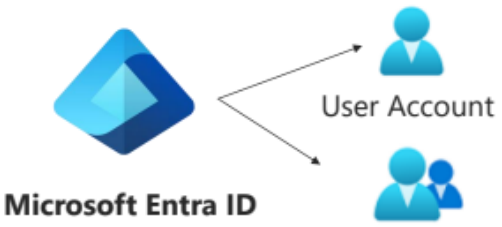
ข้อมูลประจำตัวสามารถรับรองความถูกต้องและได้รับอนุญาตสำหรับการเข้าถึงทรัพยากร มีตัวตนอยู่สำหรับอัตลักษณ์ของมนุษย์และอัตลักษณ์ที่ไม่ใช่มนุษย์

Microsoft Entra Tenant คือขอบเขตการรักษาความปลอดภัยของข้อมูลประจำตัวที่อยู่ภายใต้การควบคุมของแผนกไอทีขององค์กร ภายในขอบเขตความปลอดภัยนี้ การบริหารวัตถุ (เช่น ในฐานะผู้ใช้) และการกำหนดค่าการตั้งค่าทั่วทั้งผู้เช่าจะถูกควบคุมโดยผู้ดูแลระบบไอทีของคุณ





Microsoft Entra ID | Accounts



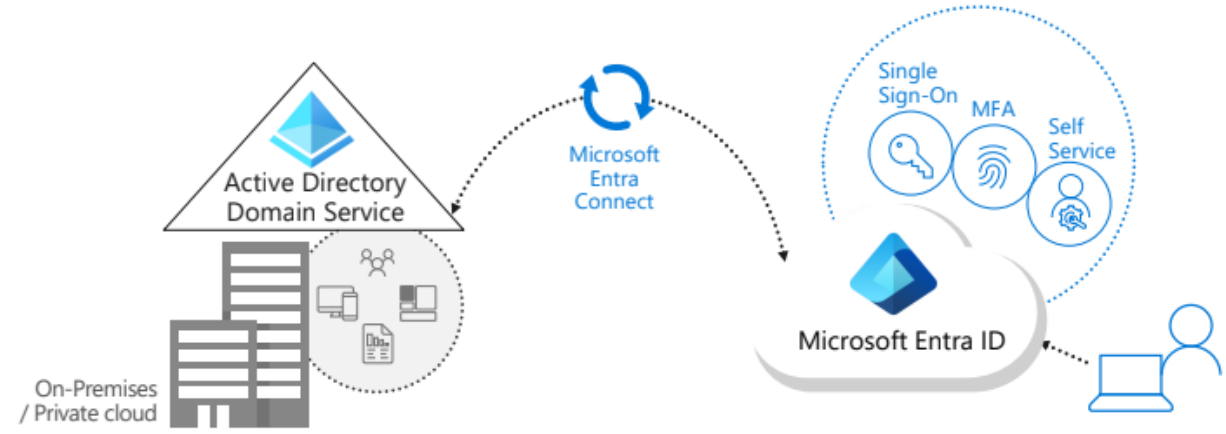
1. **Cloud User Account (Microsoft Entra Account)**
2. **Hybrid User Account**
3. **External User Account (Guest User Account)**

- **Security groups**. Security groups are used to manage member and computer access to shared resources for a group of users. For example, you can create a security group for a specific security policy. By doing it this way, you can give a set of permissions to all the members at once, instead of having to add permissions to each member individually. This option requires an Azure AD administrator.
- **Microsoft 365 groups**. Microsoft 365 groups provide collaboration opportunities by giving members access to a shared mailbox, calendar, files, SharePoint site, and more. You can give people outside of your organization access to the group. Both users and admins can use Microsoft 365 groups.

4. Microsoft Entra ID Use Cases

Active Directory-Based Identity Solutions

Microsoft Entra Domain Services	Microsoft Entra ID	Active Directory Domain Services
Provides managed domain services with a subset of fully compatible traditional AD DS features such as domain join, group policy, LDAP, and Kerberos / NTLM authentication.	Cloud-based identity and mobile device management that provides user account and authentication services for resources such as Microsoft 365, the Azure portal, or SaaS applications.	Enterprise-ready lightweight directory access protocol (LDAP) server that provides key features such as identity and authentication, computer object management, group policy, and trusts.



๙. ปัญหาอุปสรรคในการสัมมนา

-

๑๐. ประโยชน์ที่ได้รับจากการสัมมนา

: - ต่อตนเอง

๑. ทำให้ได้เรียนรู้โซลูชันการจัดการตัวตน การเข้าถึงทรัพยากรจาก Microsoft ทำให้สามารถจัดการ และปกป้องข้อมูลประจำตัวได้อย่างมีประสิทธิภาพ

๒. ทำให้ได้เรียนรู้ถึงฟีเจอร์ใหม่ ๆ ของ Microsoft ที่อัพเดตล่าสุดในปี 2025

: - ต่อหน่วยงาน/มหาวิทยาลัย

๑. ได้เรียนรู้โซลูชันการจัดการตัวตน การเข้าถึงทรัพยากรจาก Microsoft ที่ช่วยให้องค์กรสามารถจัดการ และปกป้องข้อมูลประจำตัวของพนักงานได้อย่างมีประสิทธิภาพมากยิ่งขึ้น

๒. ฟีเจอร์ใหม่ ๆ ของ Microsoft ที่อัพเดตล่าสุดในปี 2025 ทำให้สามารถช่วยเพิ่มประสิทธิภาพการทำงานขององค์กรได้

๑๑. เอกสารหรืออื่น ๆ ที่เกี่ยวข้องที่ได้รับจากสัมมนา

-

๑๒. สำเนาประกาศนียบัตร/วุฒิบัตรฯ ที่ได้รับจากการประชุม/ฝึกอบรม/สัมมนา/ศึกษาดูงาน

-

๑๓. ความคิดเห็นและข้อเสนอแนะ อื่น ๆ

-

(ผู้รายงาน) .....

(นายนิคม อรุณฉาย)

วันที่ ๒๗ กุมภาพันธ์ ๒๕๖๘

ความคิดเห็นของผู้บังคับบัญชาชั้นต้น

.....

.....

.....

.....

.....

(ลงชื่อ) .....

(อาจารย์เบญญา หวังมหาพร)

วันที่.....