ALFA Connections WiFi Authentication with Microsoft Entra Domain Services

What is Microsoft Entra Domain Services

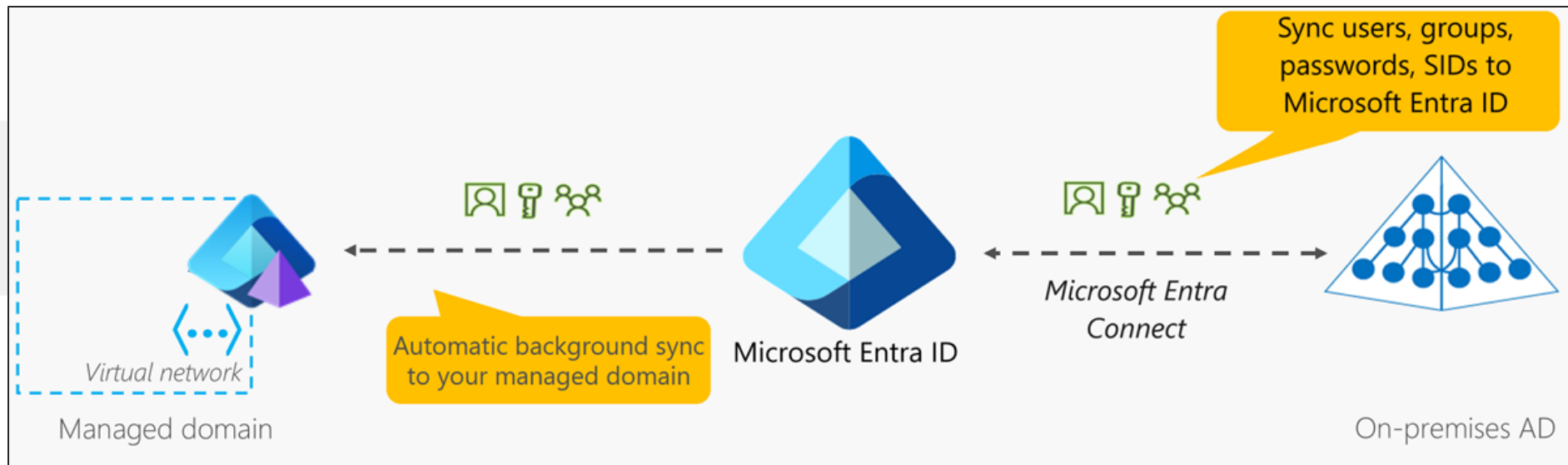**Microsoft Entra Domain Services** provides **managed domain services** such as:
- **Lightweight LDAP, Kerberos/NTLM authentication**
- **Domain join, Group Policy**, and more

✔️ No need to deploy Domain Controllers
✔️ Seamless for **legacy apps** and **lift-and-shift** scenarios
✔️ Works with **Azure Virtual Network**
✔️ Integrated with **Entra ID (Azure AD)**

🔐 Ideal for hybrid cloud setups needing traditional domain features without the overhead.

🧠 **Key Considerations**

- Best for **"lift-and-shift"** apps needing domain join
- Not a full replacement for **on-prem AD** in complex setups
- Use with **Azure IaaS**, **legacy apps**, and **hybrid scenarios**
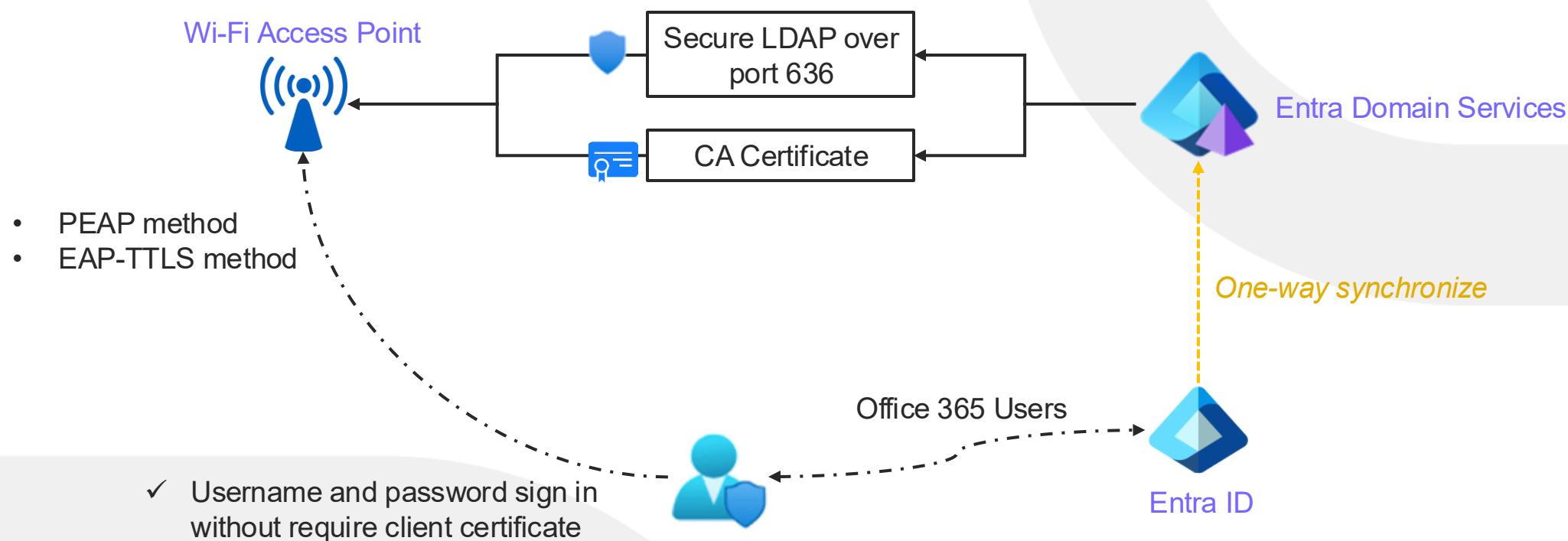
Microsoft Entra Domain Services – How It Works

- **Unique Namespace**: e.g., aaddsdomain.com
- **Replica Set**: Two managed domain controllers in your chosen Azure region
- **One-way Sync**: From Entra ID to Domain Services (not bidirectional)
- **Identity Sources**: Cloud-only users (or) synced from on-prem AD via Entra Connect
- **Supports**: Domain join, Group Policy, LDAP, Kerberos, NTLM
- **Managed & Secure**: Azure fully manages DCs, handling all patching, backups, encryption, and updates automatically.
- **Scalable**: Deploy across multiple Azure regions to ensure disaster recovery and high availability.

Differences of how devices are represented and can authenticate themselves against the directory

Aspect	Microsoft Entra joined	Domain Services-joined
Device controlled by	Microsoft Entra ID	Domain Services managed domain
Representation in the directory	Device objects in the Microsoft Entra directory	Computer objects in the Domain Services managed domain
Authentication	OAuth / OpenID Connect based protocols	Kerberos and NTLM protocols
Management	Mobile Device Management (MDM) software like Intune	Group Policy
Networking	Works over the internet	Must be connected to, or peered with, the virtual network where the managed domain is deployed
Great for...	End-user mobile or desktop devices	Server VMs deployed in Azure

Microsoft Entra Domain Services - LDAP Integration with Access Points

Wi-Fi Access Point

Secure LDAP over port 636

CA Certificate

Entra Domain Services

One-way synchronize

Office 365 Users

Entra ID

- PEAP method
- EAP-TTLS method

✓ Username and password sign in without require client certificate

Microsoft Entra Domain Services can act as standalone authentication source for Wi-Fi access points that support LDAP or LDAPS authentication – without requiring additional components like

- A Radius/NPS server
- An on-premises Active Directory
- Client certificates

Entra Domain Services – Implementation Phases

Phase 1   Project kick-off

Phase 2   Tenant Assessment & Prerequisites

Phase 3   Art of the possible workshops

Phase 4   Microsoft Entra Domain Services Implementation & Support

Phase 5   User Acceptance Test (UAT)

Phase 6   Documentation

Phase 7   Knowledge Transfer

Phase 8   Project sign-off

Phase 9   Service Warranty (1 consecutive calendar month)

Total 10 man-days

Thank You