



# WILAS IAM FOR ENTERPRISE AND SMALL BUSINESSES

Enhancing Client Visibility and Wi-Fi Onboarding Efficiency

IAM (Intelligent Access Management) is a Wi-Fi onboarding captive portal and an independent module in the WILAS platform. It enables a smooth Wi-Fi onboarding journey for guests and employees, reducing the need for intervention from IT resources. The portal captures the user profiles connected to your Wi-Fi, enhancing the auditability of your network and protects your company from liability risks.



## 9 Authentications

Provide 9 authentication options for visitor access control



## CMS

User-friendly content management system for the non-technical



## Dynamic Contents

Display different contents to different target audience



## Profiling

Generate reports on visitor demographics, devices, and Wi-Fi usage



## SSM

Manage Wi-Fi access privilege and duration



## Languages

Multi-languages support





## AUDITABILITY & ACCOUNTABILITY

Capture user profiles, knowing who is connected to your Wi-Fi

With the visibility, IAM provides a better assistance in IT investigation or audit

Enforce clickwrap agreement upon signing up for your Wi-Fi service to protect company from liability risks



## ENGAGEMENT

Take advantage of the professionally designed Wi-Fi login page as an engagement channel to disseminate information to your guests or employees



## PRIVILEGED ACCESS MANAGEMENT

Add extra security layers by enabling authenticated Wi-Fi for staff members with credentials that are synchronized with corporate AD (active directory), encouraging better governance and compliance with regulations

Control access policies for different groups (e.g. VIP, Employees, Guests, e.t.c.)

## RESOURCES OPTIMIZATION

Promote self-service Wi-Fi onboarding, eliminating the need for intervention from IT resources and reducing guests' & staff's waiting time

Manage multiple locations in a single platform



# HOW WILAS WORKS WITH ZERO INTERVENTION?

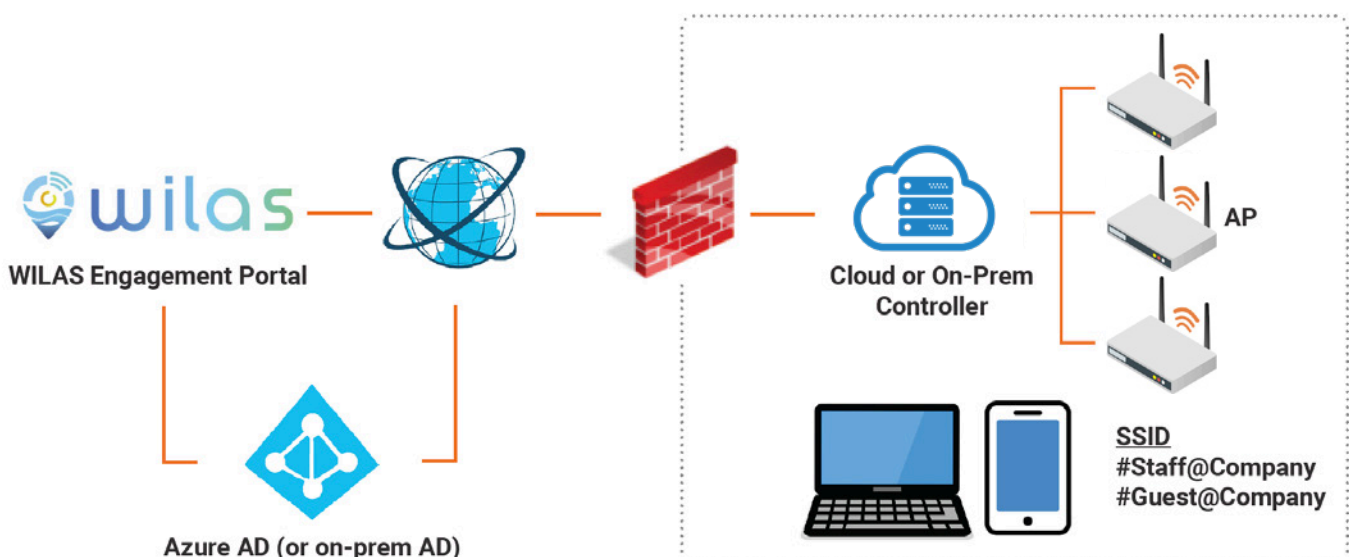


## VISITORS

- Visitors can simply connect to the guest Wi-Fi and perform the self-service onboarding.
- They will be required to accept the T&Cs and provide their basic information before connecting to the Wi-Fi. OTP can be adopted to validate their contact information.
- Upon completion, visitor will automatically be granted a restricted period of Wi-Fi access based on company policy.

## STAFF

- Once staff are onboarded to the company's AD, they will automatically be granted the staff Wi-Fi access using the same credential.
- When they connect to the Wi-Fi for the first time, Captive Portal will be presented to them to provide their company credential.
- Credential will be authenticated against the AD server. WILAS will then provision the device access to the controller with the defined policy if the authentication is successful.
- Staff will be able to connect to the Wi-Fi seamlessly until the next authentication is required based on the company policy.



### Integration of Enterprise Wi-Fi Network with WILAS

Zero-Appliance & Zero-Incoming Traffic to the enterprise network ensuring optimal security assurance