Secure Wi-Fi

**THE STANDARD UNSECURE WAY**

Multiple SSIDs per Customer One password per customer for VLAN Access

Manually provisioned Shared passwords pose security threats 3% performance degradation per SSID added Password reset affects all users

User access limited across the site Ex-users retain access to corporate Wi-Fi

**THE [YOUR COMPANY] WAY**

Single SSID for all Customers One password per user for VLAN access

Users provisioned automatically via secure platform Vastly reduced performance degradation

VLAN accessible across the site Seamless guest access globally

User-specific password

Device-limited to prevent password sharing

User tracking enabled to prevent security breaches

Contact your center manager for more information

Powered by

Insert logo

# always-on, always secure

In today's increasingly digital and connected world, at [YOUR COMPANY] we know you need to be online at all times and that security is a top priority. We've invested in advanced technology with the necessary security measures in place to prevent vulnerabilities to our network and its users.

# how it works

The username-based Wi-Fi solution uses a single SSID across our location. Each user is created securely within our IT management software, Connect, and is sent a unique username and password. With those login credentials, the user connects to the single SSID and is put into a dedicated and secure company VLAN with the correct bandwidth profile.

# the [YOUR COMPANY] difference

the benefits of Wi-Fi authentication

As a basic standard of security, our Wi-Fi network is set up with WPA-enterprise protocols that use an 802.1X authentication mechanism. The 802.1X authentication operates in conjunction with two secure networking protocols: Extensible Authentication Protocol Over Lans (EAPoL) and Remote Authentication Dial-In User Service (RADIUS) server. These make 802.1x inherently more secure than your standard WPA-PSK or WPA2-PSK which require a shared password for all users to access the network.