Cnergee
Secure by design

Cnergee WiFiguard



Copyright © 2025 | Cnergee Technologies Private Limited

Overview

The Cnergee Wifiguard family is a portfolio of unified, secure, and scalable Managed Wi-Fi solutions, designed to deliver high-performance wireless connectivity from basic office needs to complex enterprise and smart campus environments. Unlike traditional siloed Wi-Fi systems, Wifiguard integrates Network Access Control (NAC) and Security Gateway features directly into a highly flexible, cloud-managed platform, ensuring a robust and future-proof network fabric.

Platform Feature	Cnergee Wifiguard Capability	Key Use Case / Industry Alignment
Centralized Management	Unified Cloud Controller for configuration, monitoring, and remote diagnostics.	Multi-site Retail, Distributed Branch Offices (SMB/Enterprise).
Wi-Fi Optimization	**Automatic Channel Selection (ACS), Dynamic Frequency Selection (DFS),** Smart Load Balancing.	High-Density Venues (Auditoriums, Public Spaces) ensuring optimal channel utilization and interference mitigation.
Zero-Cabling Deployment	Wireless Mesh Backhaul: Add-on APs connect wirelessly to the Master AP.	Heritage Buildings, Warehouses, or temporary deployments where running new Ethernet cable is not feasible.
Authentication/AAA	Full RADIUS/802.1X integration, Captive Portals, MAC binding, and Active Directory synchronization.	Educational Institutions (Campus Wi-Fi), Corporate Enterprises requiring secure, credential-based access.
Network Redundancy	Unique Feature: Direct WAN Link Termination with SIM Failover Backupintegrated into the Access Point/Gateway.	Critical Business Branches, ATMs, or remote monitoring stations demanding near 100% network uptime.
Integrated Security	Application Control, Domain Filtering, and Rogue AP Protection (Shield Variant).	Banking, Healthcare, or regulated sectors requiring strict compliance and advanced security at the edge.

Copyright © 2025 | Cnergee Technologies Private Limited

Product Variants

Wifiguard family is structured into three primary tiers: Core, Access, and Shield, each escalating in security, control, and complexity of customer feature requirement.

WIFIGUARD CORE

Small Offices (SOHO), Simple Enterprises requiring basic managed Wi-Fi.

WIFIGUARD ACCESS

SMB, Branch Offices needing secure guest access, traffic prioritization, and high availability.

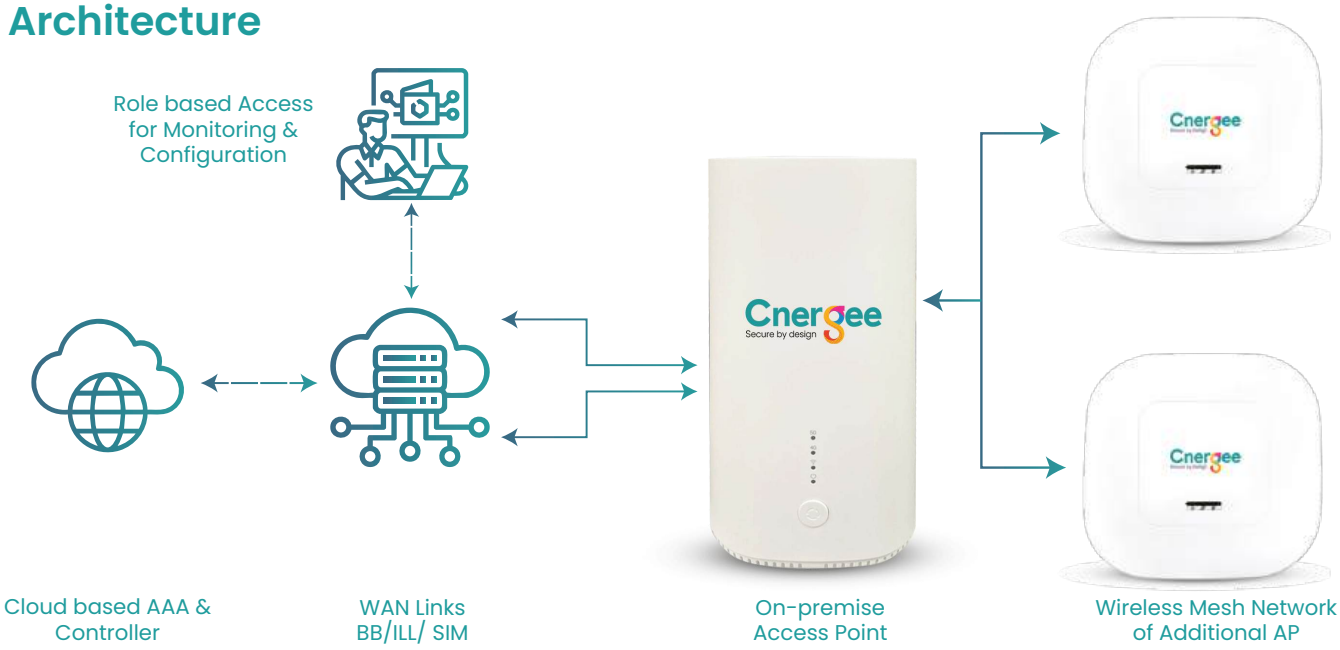
WIFIGUARD SHIELD

Large Enterprises, Campuses, Smart Cities needing maximum security and content policy enforcement.

WifiGuard Core

Core offers a managed Access points network either as standalone or in a mesh network. This is useful for small offices looking for basic WiFi connectivity for users with a centralized portal for configuration.

Architecture



Components

- Access Points (APs): Wireless devices (indoor/outdoor) that transmit the Wi-Fi signal with ability to create mesh
- Cloud based Controller : Access Reports and manage configuration for AP's

Copyright © 2025 | Cnergee Technologies Private Limited

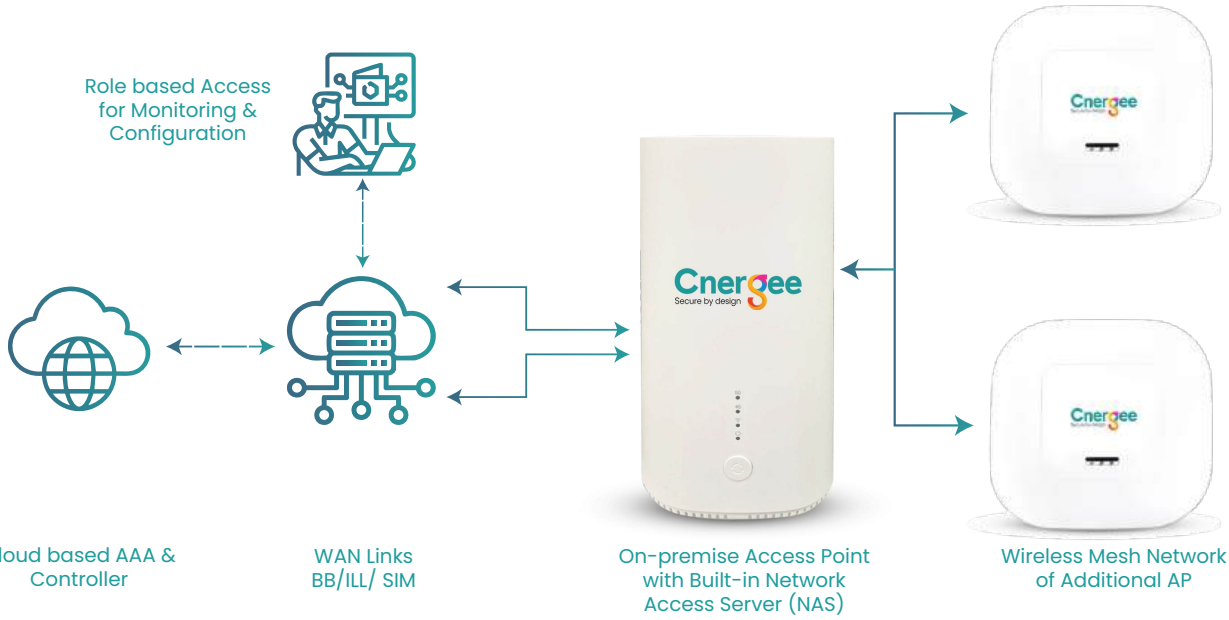
Supported Features

Feature	Functionality
Access Points	WiFi 6 Enabled Access Points
Authentication	Shared Pre-Shared Key (PSK)
AP Configuration	Zero-Touch Provisioning (ZTP): APs automatically fetch configuration upon connection. Bulk firmware upgrades and configuration pushes from a single dashboard.
Backhaul	Wired only (Ethernet required for all APs)
Monitoring	Real-time AP status (up/down), device health checks, channel utilization, and noise floor levels. Rogue AP Detection and containment capabilities.
RF Management	Auto-Channel/Power Adjustment: Automatically adjusts AP channel and transmit power to minimize interference and optimize coverage
WiFi Standards	Support for modern standards like Wi-Fi 6/6E (802.11ax/802.11ax-6GHz) and WPA3 encryption.

WifiGuard Access

Access expands on Core by introducing separate, secure access for guests via a Captive Portal. Access offers an all-in-one edge device for remote or branch offices, converging networking, Access policies, and backup connectivity into a single, compact appliance. The Access Point is a feature-rich device with built-in Network Access Server (NAS) functionality to handle policy enforcement (acting as the RADIUS client). This AP also has a built-in capability to terminate WAN links and includes a SIM backup for failover, essentially functioning as a converged Router/Gateway and NAS enforcement point.

Architecture



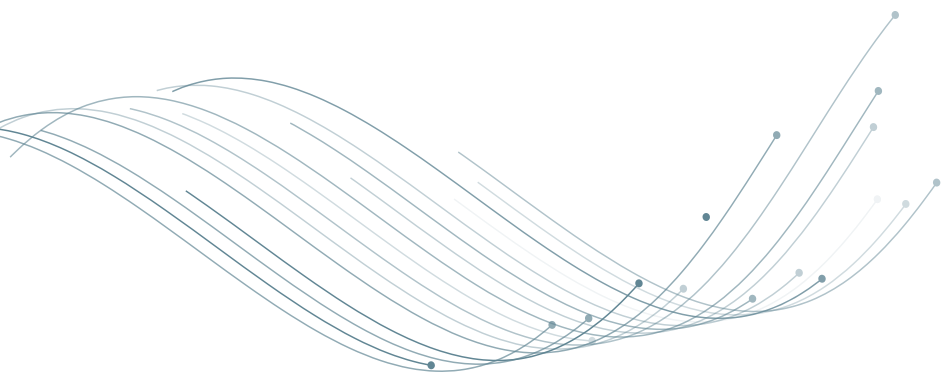
Copyright © 2025 | Cnergee Technologies Private Limited

Components

- Integrated AP/Router: A single hardware unit with built-in Wi-Fi functionality and a routing/gateway engine with NAS
- Multi-WAN aggregation module: Built-in ports/slots to accept multiple WAN connections with proprietary PMTA™.
- SIM Module: An integrated 4G/LTE/5G modem for cellular backup.
- Built in NAS : Enable policy enforcement based on type of device via speaking to external authentication mechanism and creating Guest WiFi through captve portal.
- Cloud based AAA & controller : Manage configuration and reporting, with ability to create Guest wi-fi via authentication via Captive Portal, Coupons,Mac id or RADIUS integration.

Supported Features

Feature	Functionality
Access Points	WiFi 6 Enabled Access Points
Authentication	802.1X (RADIUS) for Employees / Captive Portal for Guests
Security	Firewall Policy with Domain Filter and Simple Network Access Control (NAC) based on MAC/Device type.
AP Configuration	Zero-Touch Provisioning (ZTP): APs automatically fetch configuration upon connection. Bulk firmware upgrades and configuration pushes from a single dashboard.
Backhaul	Wired only (Ethernet required for all APs)
Monitoring	Real-time AP status (up/down), device health checks, channel utilization, and noise floor levels. Rogue AP Detection and containment capabilities.
Add on Features	Guest WiFi Bandwidth management via separate SSID with enforcement of browsing, bandwidth rate limit policies. VLan segmentation for guest traffic.

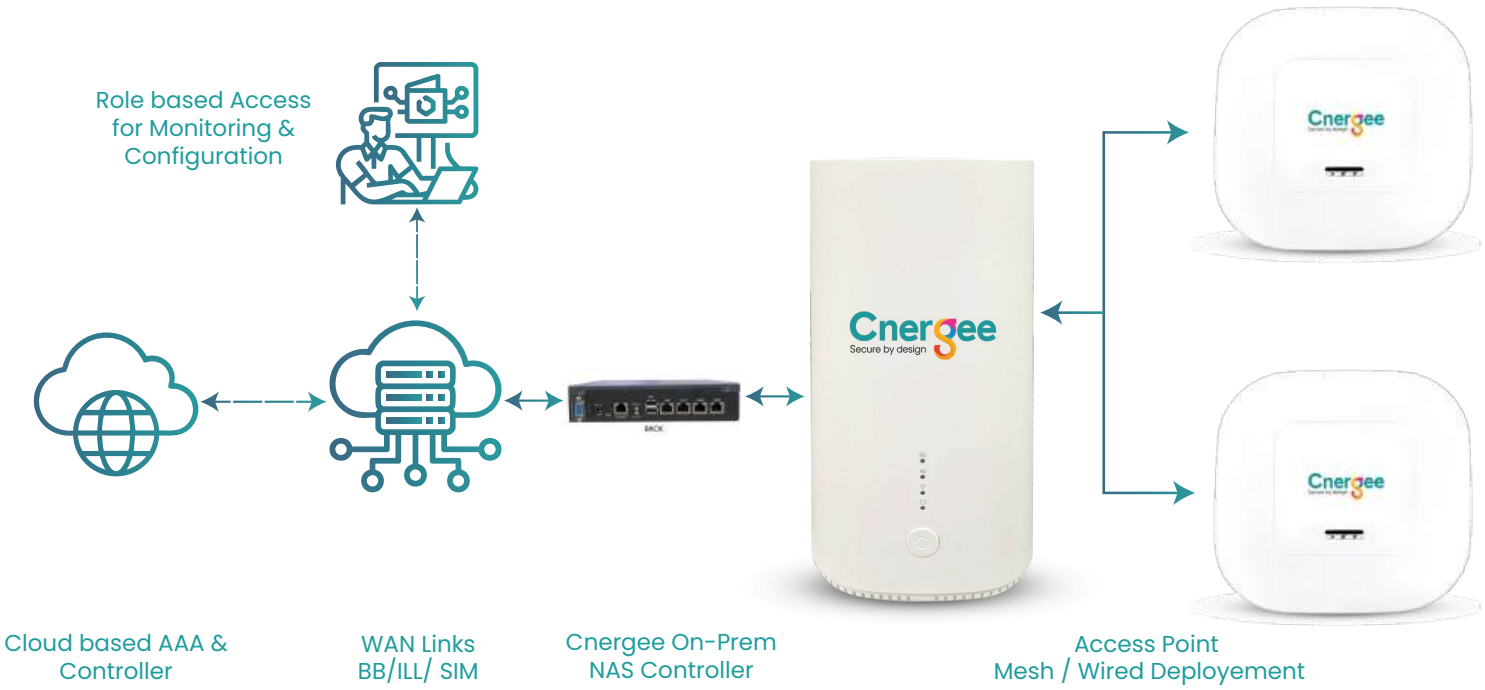


Copyright © 2025 | Cnergee Technologies Private Limited

WifiGuard Shield

The Wifiguard Shield is the top-tier, most secure solution in the Cnergee Managed Wi-Fi portfolio, designed for large enterprises, campuses, and environments with complex security demands. It utilizes a centralized cloud architecture for AAA and policy management but deploys a dedicated on-site Network Access Server (NAS) to enable advanced features like comprehensive content, application, and category filtering. Crucially, Shield includes Rogue AP Protection for continuous threat mitigation and supports flexible Wireless Mesh backhaul, providing uncompromising security and scalable deployment across wide areas. This variant represents a unified, full-stack security and access solution, ensuring maximum protection and simplified operations for high-density, critical networks.

Architecture



Copyright © 2025 | Cnergee Technologies Private Limited

Feature Category	Wifiguard Shield Capability	Cnergee Differentiator
I. Unified Access Control (NAC)		
Authentication & Authorization	Full 802.1X (EAP-TLS/PEAP) support, WPA3 Enterprise, and Role-Based Access Control (RBAC).	Integrates NAC policy enforcement into the localNAS server for lower latency decision-making.
Device Posture Assessment	Checks device health (Antivirus status, OS patch level) before granting network access.	Granular control facilitated by the dedicated On-Site NAS Server.
II. Advanced Security & Threat Mitigation		
Rogue AP Protection	Automatic Detection, Classification, and Containment of unauthorized and "Evil Twin" Access Points.	Unified management with application control and simplified remediation from a single dashboard.
Gateway Security Stack	Anti-Virus (AV), Intrusion Prevention System (IPS), and Stateful Firewall (Layer 3/4).	Delivered via the Shield NAS Server as a robust, dedicated on-site appliance.
Application Filtering	Layer 7 visibility and control for granular blocking or prioritization of specific applications (e.g., Netflix, P2P file sharing).	Dedicated On-Site NAS Server ensures low-latency enforcement of thousands of application signatures.
Content & Category Filtering	Blocks access to malicious, adult, or non-business-related website categories.	Real-time URL filtering powered by local processing capability of the NAS Server.
III. Network Resiliency		
Bandwidth Aggregation	Aggregation of multiple WAN links (BB, ILL, MPLS) into a single virtual pipe.	PMTA-Enabled Bandwidth Aggregation: Provides Packet- Based-Multi-Tunnel Aggregation across diverse links for maximum utilization and seamless redundancy
SIM Failover	Direct termination of BB/ILL links with integrated 4G/5G SIM as immediate backup.	High-resilience design ensures critical operations (POS, CCTV) maintain connectivity during primary link failures.
Wireless Mesh Backhaul	Add-on APs require no cabling for network connectivity (only power).	Simplifies installation in complex physical layouts (e.g., campuses, warehouses).
Backhaul	Wired and Wireless Mesh	Supports both wired backhaul and new wireless mesh backhaul for add-on APs, requiring no cabling for those units

Copyright © 2025 | Cnergee Technologies Private Limited

TECHNICAL SPECIFICATION

Standards	IEEE 802.11b/g/n/ax on 2.4GHz | IEEE802.11a/n/ac/ax on 5GHz
Processor	Qualcomm® 1Ghz Quad-Core CPU with dedicated NSS
Antenna	Inbuilt 5 dBi omnidirectional antennas
Physical Interfaceipset	2x 10/100/1000 BASE-T, RJ-45 Ethernet Port
LED Indicators	1 x Power| 2 x LAN | 1 x 2.4 GHz/ 5 GHz
Power Source	Power-over-Ethernet: 802.3af/at or Proprietary 48V |IEEE 802.11e Compliant Source| Active Ethernet (PoE)
Maximum Power Consumption	20W
Surge Protection	2KV

WIRELESS SPECIFICATIONS

Operating Frequency	Dual-Radio Concurrent 2.4GHz & 5 GHz
Operation Modes	AP, Mesh
Frequency Radio	2.4GHz: 2400 MHz ~ 2482 MHz 5GHz: 5150 MHz ~ 5250 MHz, 5250 MHz ~ 5350 MHz, 5470 MHz ~ 5725 MHz, 5725MHz ~ 5850MHz
Transmit Power	2.4 GHz: 26 dBm | 5 GHz: 26 dBm
Radio Chains/Spatial Stream	2x2:2
Supported Data Rates (Mbps):	2.4 GHz: Max 600 | 5 GHz: Max 2400
Supported Radio Technologies	802.11b: Direct-Sequence Spread Spectrum (DSSS) 802.11a/g/n/ac: Orthogonal Frequency-Division Multiplexing (OFDM) 802.11n/ac: 2x2 MIMO with 2 Streams
Channelization	802.11ac supports very high throughput (VHT)—VHT 20/40/80/160 MHz 802.11n supports high throughput (HT)—HT 20/40 MHz 802.11n supports very high throughput (VHT) under the 2.4 GHz radio—VHT (256-QAM) 802.11n/ac packet aggregation: AMPDU, ASPDU

MANAGEMENT

Multiple BSSID	8 SSIDs for both 2.4GHz and 5GHz radios
VLAN Tagging	Supports 802.1q SSID-to-VLAN Tagging| Cross-band VLAN Pass Through Management VLAN
Spanning Tree	Supports 802.1d Spanning Tree Protocol
QoS (Quality of Service)	Compliant with IEEE 802.11e Standard | WMM
SNMP	v1, v2c, v3 | MIBI/II, Private MIB
Wireless Security	WPA2 AES-PSK/WPA2 Enterprise Hide SSID in Beacons MAC Address Filtering, Up to 32 MACs per SSID Wireless STA (Client) Connected List Https SSH Client Isolation

Copyright © 2025 | Cnergee Technologies Private Limited

MECHANICAL SPECIFICATION

Temperature Range	Operating: -4°~140°F/-20°C~60°C | Storage: -40F°~176°F/-40°C~80°C
Humidity (non-condensing)	Operating: 90% or less | Storage: 90% or less
Waterproof & Dustproof	IP60-Rated Enclosure
Dimensions	Weight: 0.5Kg | Width: 7" (180 mm)| Length: 7" (180 mm)| Height" 2" (50 mm)





Proudly
MADE IN INDIA

Copyright © 2025 | Cnergee Technologies Private Limited

Cnergee

Secure by design

Contact Us:

info@cnergee.com

+91 22 613 77777

S-10, Arenja Towers, Sec-11,
CBD Belapur, Navi Mumbai, India - 400614

www.cnergee.com

For more Updates, Follow Us

Copyright © 2025 | Cnergee Technologies Private Limited