Wireless Network Manager

Cloud-Based Unified Dashboard for Management of Access Points (APs) and Switches

Scalable for any size organization, SonicWall Wireless Network Manager (WNM) is an intuitive, centralized wireless and switching network management system. It delivers rich analytics, powerful features and easy onboarding from a single pane of glass.

Its cloud-based infrastructure simplifies access, control and troubleshooting by unifying multiple tenants, locations and zones. WNM supports thousands of SonicWave APs and SonicWall Switches, without the cost of complex overlay management systems.

HIGHLIGHTS

Business

- Reliable operation, cloud stability, and security
- Reduced security management overhead
- Achieve IT organization efficiency while reducing admin burnout
- Lower TCO

Operational

- Zero-Touch Deployment for rapid onboarding and provisioning
- Onboard and manage SonicWall Switches and Access Points with ease
- Integrated advanced site survey tool
- Powerful network topology mapping
- Unified visibility and control via cloud-based single-pane-of-glass dashboard
- Seamless integration with Capture Security Center
- Detailed reporting, logs, and alerts
- Real-time, rich data analytics

Security

- Supports private pre-shared keys (PPSK), SAML authentication, and DHCP fingerprinting
- Audit, commit, and enforce consistent security policies across all wired and wireless networks
- Monitor and track results of policy actions with greater clarity
- Prevent unauthorized user authentication

Move to a secure, integrated wired-and-wireless network management solution:

sonicwall.com/wnm

Create a unified policy and manage anywhere from a few APs and switches to thousands, all via a single cloud-based dashboard.

Single-Pane-of-Glass Management

WNM lets you easily manage global networks from a single pane of glass. An integrated part of the SonicWall Capture Security Center ecosystem, its intuitive dashboard offers unified visibility and control. Network hierarchy allows you to view single policies created at the tenant level that are pushed down to various locations and zones. Drill down on managed devices for granular data. WNM is highly scalable, from a single site to global enterprise networks with tens of thousands of managed devices supporting multiple tenants.

Onboarding and deployment is automatic. Your network is up in minutes.

Pre-Shared Key

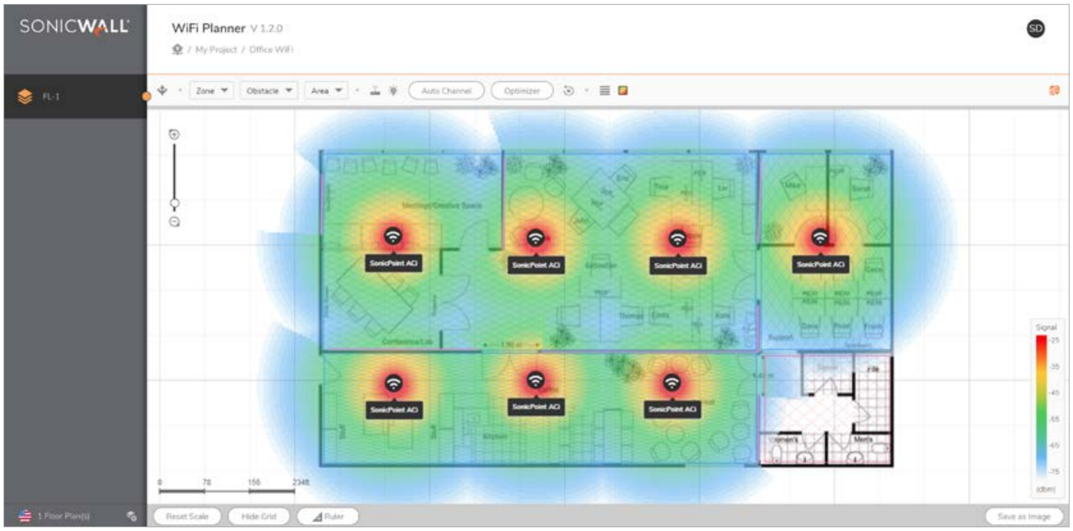
Private pre-shared keys (PPSK) are an important tool for protecting networks. Each one consists of a long, random series of combined numbers and letters that is generated when a device joins a network. Because each client device has its own unique pre-shared key, PPSK is an effective way to secure a guest network or to deactivate an individual's access to the network when the individual leaves an organization. PPSK allows for easier use and management of the network, compatibility for legacy clients, and support for different VLANs.

SAML Authentication Support

Security Assertion Markup Language (SAML) is a way to authenticate data between parties, particularly between an identity provider and a service provider. It allows a user to access multiple web applications using a single set of login credentials. In short, SAML is a way to tell external applications that a user is who they say they are. This single sign-on results in a better user experience and can also result in improved security, because the identity provider – not the service provider – is responsible for storing user credentials.

DHCP Fingerprinting

With the proliferation of BYOD (Bring Your Own Device) in today's workplace, network administrators are challenged with dynamically detecting and identifying these devices to ensure they're compliant. DHCP fingerprinting is a technique for identity verification that allows devices to be tracked and, most importantly, blocks those that are not allowed.



Advanced Security Options

Keeping your network protected from malware, viruses and infections is critically important. Content Filtering Service (CFS) does just that by inspecting web page access and taking action when a threat is detected. CFS provides administrators with the tools to create and apply policies that allow or deny access to sites based on individual or group identity, or by time of day, for over 56 predefined categories. As part of the advanced capabilities package, WNM includes the ability to add Content Filtering Service, Capture ATP, and GAV directly to the access point.

Reliable Operation

WNM delivers the stability and reliability of the cloud. In case an internet outage, access points and switches can continue to work without WNM, ensuring business continuity. Two-factor authentication and packet encryption heighten security, while automatic firmware and security updates keep managed devices up to date. WNM allows admins to selectively apply production, beta or patch firmware on each managed device as needed, and enables automatic sending of reports to multiple recipients simultaneously.

Zero-Touch Deployment

With Zero-Touch Deployment, your SonicWall APs and switches are up and running in minutes. And you can register and onboard them from anywhere with the SonicExpress app.

Advanced Analysis Tools

Conducting a wireless site survey before deploying access points can help ensure performance and productivity. WNM's WiFi Planner tool helps you strategically deploy access points to optimize Wi-Fi user experience and avoid costly mistakes. WiFi Planner analyzes placement, building materials, power, signal strength, channel width and radio bands. This lets you optimize coverage in new or existing networks using the fewest number of APs. Auto-channel assignment prevents interference. WNM's Topology tool provides network topology maps and managed device statistics.

Lower TCO

Cloud-based WNM drives down total cost of ownership (TCO) by shifting capital expenditures (CAPEX) to operating expense (OPEX). WNM cuts out the cost and maintenance of redundant hardware-based controllers and optimizes data center rack space. Its intuitive interface reduces training and administrative overhead costs.

Feature Summary

Management

- Centralized Dashboard
- SonicWall Access Point Management
- SonicWall Switch Management
- Zero-Touch Onboarding
- Device Zone level management
- Multi-device firmware upgrade
- Role-based administration
- Customizable Wi-Fi Guest Portal & certificate management
- Network Hierarchy View
- Topology View
- Policy Hierarchy, Centralized Policies, and Objects
- Device health and status
- License and support status
- Network/Threat summary
- Audit logs
- Topology view
- Air Marshal
- QoS Policy

Analytics

- RF Survey and Spectrum Analysis
- Wi-Fi Planner
- Logs, Alerts, and Notifications

Reporting

- On-demand and Scheduled PDF reports - Tenant
- Customizable reports

Security

- Account lockout
- Account access control
- 2FA support
- Authenticator App support
- 365 days of Audit Log storage

To learn more about the ultimate scalability and reliability of this cloud-based management platform, visit:

SonicWall Wireless Network Manager

About SonicWall

SonicWall is a cybersecurity forerunner with more than 30 years of expertise and a relentless focus on its partners. With the ability to build, scale and manage security across the cloud, hybrid and traditional environments in real time, SonicWall can quickly and economically provide purpose-built security solutions to any organization around the world. Based on data from its own threat research center, SonicWall delivers seamless protection against the most evasive cyberattacks and supplies actionable threat intelligence to partners, customers and the cybersecurity community.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Refer to our website for additional information.
www.sonicwall.com