Better Control & Visibility of All Your IoT Touchpoints

From nice-to-have technology, like smart home gadgets, to critical security devices, like safety alert beacons, the scope of the Internet of Things (IoT) is spreading rapidly into homes and businesses alike. Network security is crucial to maintaining IoT efficiency, health, and integrity. Eleven's *Enterprise Device Manager* simplifies complex network access control via a cloud-based dashboard.

Cloud IoT Device Management in ElevenOS

Enhanced Security

Security starts with knowing what's happening on your network. Unlike preshared keys (PSKs), 802.1x authentication keys are individual and unshared. Role assignment makes it possible to audit user behavior and remove any threats.

Simplified Management

Add IoT and BYOD devices in bulk, make changes, and easily remove them–all from a single pane of glass. Features also include network segmentation and device VLAN assignment. Deploy the service to multiple properties with confidence that it works reliably.

Scalable Framework

Ensure all devices, especially critical ones, are always online with a cloud-native architecture that leverages a suite of Amazon Web Services (AWS) to provide a reduntant and fault-tolerant infrastructure with 99.95% uptime.

Rapid Deployment With Your Existing Infrastructure

Eleven has pre-built integrations with best-in-breed network hardware and partnerships with leading network integrators, so you can leverage existing infrastructure and minimize cost. Skip the on-premise RADIUS server; Enterprise Device Manager can be used as a standalone service or as part of the ElevenOS platform.

ANTlabs · aruba a Hewlett Packard Enterprise company · CISCO · CISCO Meraki · MikroTik · NOMADIX · NETS · RUCKUS WIRELESS

Simplify Network Access Control via 802.1x Authentication

Easy Device Onboarding

Authenticating a new device is quick and straightforward for non-technical users, saving time for IT teams and service providers.

Streamlined Integrations

Integrating with external third-party identity systems (i.e. AD, SAML) enables both application access control and device credentials.

Reliable Brand Support

Pre-configured and tested to support brand-preferred devices and pre-connected to the identify platforms of major brands.

What is 802.1x?

Authentication means making sure that something is what it claims to be, or proof of identity. The IEEE 802.1X security standard is a framework that defines how to provide authentication and encryption for devices trying to connect with other devices on a network.

How does it work?

With 802.1x, the physical hardware does not need to know how to authenticate the client. All they do is pass the authentication information between the client and the authentication server (ElevenOS), which verifies the credentials. Ultimately, the authentication server decides if clients can access the network or not.
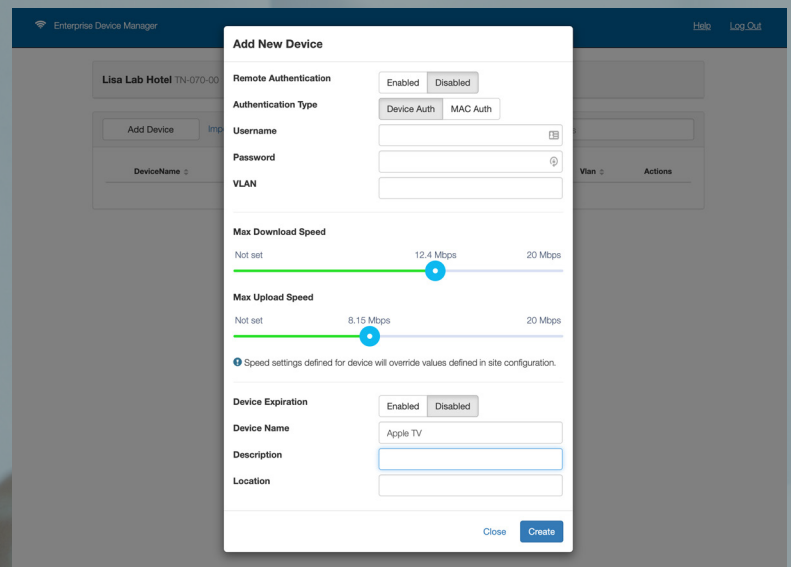
Strategic & Trusted Wi-Fi Expertise

3B+ Annual Authentications

With over 9 million authentications per day, ElevenOS is a proven platform powering connectivity.

6,000+ Global Customers

ElevenOS is trusted at thousands of locations across 50 countries in multifamily, hospitality, and beyond.

17+ Years of Innovation

Founded in 2002, Eleven truly understands the history of Wi-Fi and where its headed.