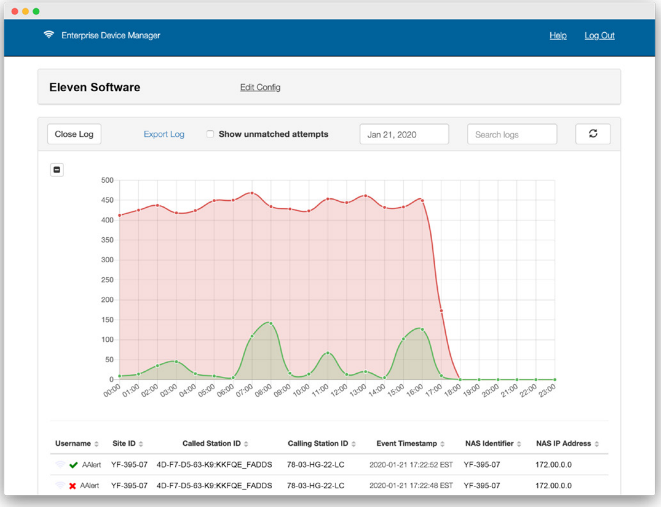
Enterprise Device Manager

A cloud-based network access control and 802.1x authentication service for IoT & BYOD management.

Product Overview

Eleven's ***Enterprise Device Manager*** is a highly available cloud-based 802.1x authentication service for IoT devices. Eliminating the onerous process of setting up a dedicated, on-premise RADIUS server, it is an easy-to-use, cloud-hosted 802.1x service that enables service providers to offer secure authentication to IoT devices, from nice-to-have technology, like smart home gadgets, to critical security devices, like safety alert beacons.



Eleven Software

□ Show unmatched attempts

Jan 21, 2020

Username	Site ID	Called Station ID	Calling Station ID	Event Timestamp	NAS Identifier	NAS IP Address
✓ AAlert	YF-395-07	4D-F7-D5-63-K9:KKFQE_FADDS	78-03-HG-22-LC	2020-01-21 17:22:52 EST	YF-395-07	172.00.0.0
✗ AAlert	YF-395-07	4D-F7-D5-63-K9:KKFQE_FADDS	78-03-HG-22-LC	2020-01-21 17:22:48 EST	YF-395-07	172.00.0.0

Key Features

Scalable Framework: Cloud-native architecture leverages Amazon Web Services (AWS) to provide a scalable and fault-tolerant infrastructure with better than 99.95% uptime.

Self-service Dashboard: An intuitive, web-based user interface enables non-technical staff to add, remove, and troubleshoot devices on the fly without IT intervention.

Easy Device Onboarding: Quickly add one device or bulk upload an entire list with defined attributes like authentication type, credentials, bandwidth speeds, and more.

Real-time Analytics: Troubleshoot IoT issues by searching for a specific device, easily exporting a list of devices, or analyzing the AAA and change logs.

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

Top 5 Benefits

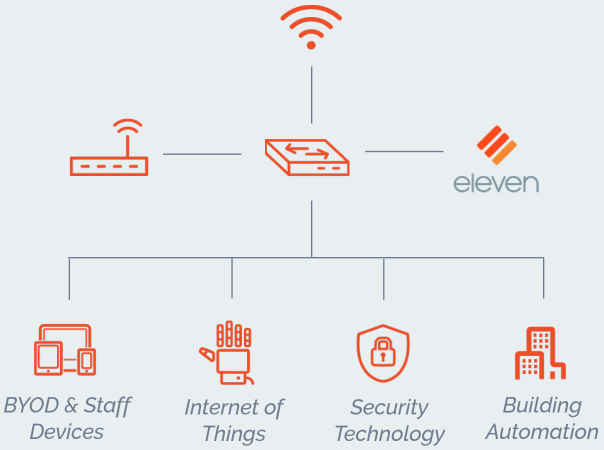
1. **Increased Stability**: Count on Eleven's redundant and robust infrastructure.
2. **Enhanced Scalability**: Ensure all devices are always online with a cloud-native architecture
3. **Better Visibility**: Access device troubleshooting information from a single pane of glass.
4. **Added Security**: Take control of your IoT and network security with 802.1x authentication.
5. **More Efficiency**: Reduce IT help desk calls with a user-friendly web-based dashboard.

How it Works

Enterprise Device Manager enables enhanced visibility and control of connected devices across the enterprise. As the authentication server, ElevenOS uses the 802.1x framework to securely allow (or reject) devices onto your network.

RADIUS traffic is balanced over multiple servers, which are evenly spread across at least three availability zones. If a server or zone goes down, it is automatically removed from the load balancer pool and the traffic is routed to the other servers.

Every cluster has redundant load balancers, deployed in a hot-failover configuration residing in separate availability zones. If the primary load balancer goes down, the backup takes over automatically.



ENTERPRISE DEVICE MANAGER

Flexible Device Options

- **Authentication Type**: Choose username/password, MAC address, or certificate-based authentication.
- **Wildcard Support**: Device usernames can be wildcarded using * or ^ characters.
- **MAC Address**: Define the credential used to authenticate users via a device's unique MAC address.
- **Remote Authentication**: Allow or dissalow devices to authenticate remotely.
- **VLAN Assignment**: Segment your network by assigning devices to specific VLANs.

Setup & Deployment

Free Up to 20 Devices: The free version included in ElevenOS provides basic network security that is best for non-critical devices, like staff laptops and digital signage.

Upgrade for High Capacity: For over 20 devices and mission-critical technology, opt for the more robust version, which can also be used as a standalone service, independent of ElevenOS.

Rapid Deployment: Set up 802.1x authentication at multiple properties with confidence that it works reliably and without having to access the physical network hardware.

No Licenses to Manage: Continue to add new devices as your IoT footprint grows without having to add licenses and incur additional cost.

Major Brand Support: Pre-configured and tested to support brand-preferred devices and pre-connected to the identity platforms of major brands (i.e. Marriott).

Common Use Cases

Hotel Staff Security Alerting

Recent events have given way to technology that equips housekeeping and other staff with safety alert pendants that, when activated, ping the nearest beacon to notify others of their location. It's of utmost importance that there is increased reliability and security for these devices.

Smart Apartment Devices

Today's residents expect more out of their rental experience, including high-tech features like smart thermostats and automated door locks. Forward-thinking property managers are using network access control systems to ensure they have visibility into all of these devices.

Connected Campus Technology

From printers to computer labs to staff laptops, there are myriad connected devices that a typical campus manages. Without a central hub to keep track of them, IT teams are burdened when it comes to troubleshooting and management.