Indio Networks

UniNAC

Network Access Controller for enterprises.

Introduction

Today, we live in a dynamic BYOD work culture, where workplaces encourage and allow their employees to bring in their own devices. People are constantly connected, with each person on average having 2 WiFi enabled devices with them at all times. Ethernet-based internet connectivity is going away at a fast rate in offices, more and more companies are adopting WiFi to secure their connectivity requirements. Enterprise level deployment of wireless technology holds many challenges. Security of the network is a primary concern of enterprise networks, many office devices store and retrieve sensitive data on a daily basis.

The biggest challenge of BYOD is ensuring security of the network, internally. Even if the network is externally secure, the BYOD paradigm opens several, potentially threatening, security gaps in corporate networks. Strengthening the security fabric of the network with robust responsiveness to threats and potential threat agents, with scalability for accommodating any kinds, and any number of devices is imperative.

High throughput is an important parameter to be considered while designing enterprise networks. Devices are constantly transmitting and receiving data through different channels. The amount of this data can be quite large in areas of the workplace where intensive processing takes place. Enterprises need hardware elements which can manage these requirements.

However, fulfilling all these requirements in itself is not enough. Enterprises should ensure that the entire network can be controlled and monitored from a single console which makes the work of the network operator much easier. The network administrators need tools to control the network access, provisioning endpoints, get deeper visibility into the network and enforce the organisation's policies while strengthening their network security. Network Access Controllers are responsible for hardening the security of the enterprise network by controlling access of endpoints to the network resources and by enforcing security policies on each device.

Our solution, for you.

UniNAC, is our network access controller that controls and manages all your core network elements while securing your network with the highest resilience possible. It implements Network Access Control, endpoint provisioning and validation, enterprise security with 802.1x, LDAP/AD integration, VPN termination, bandwidth throttling, firewall rules, user administration and network monitoring from a single appliance. Our solution creates a comprehensive security posture which delivers a highly secure, scalable enterprise network with a consistent security fabric. It allows administrators to enforce policies, keep security transparent, with high availability for voice, data and mobility.

Single Console Management & Unified Endpoint Management

UniNAC comes with an intuitive, all-inclusive smart management console which allows IT administrators to configure, monitor and get rich analysis from one single source. The Dashboard displays real-time information about network traffic, internet usage, health of Access Points connected to the network, and much more.

Enterprise Mobility Management (BYOD)

UniNAC can intelligently provision & authorise BYOD endpoints, monitor their activity and track them throughout the premises. Endpoint checks and audits make it easy for administrators to revisit points of failure and check if certain devices might have been responsible for them. Rogue devices or malicious endpoints are identified and quarantined with swift, proactive security mechanisms. IT admins can set up MAC filtering rules to prevent unauthorised devices from accessing the corporate network. With more than 12 authentication methods, including enterprise grade 802.1x Authentication, UniNAC secures all your enterprise requirements for a dynamic, inclusive BYOD culture.

Strong Security Posture

UniNAC comes with Dynamic VLAN assignment capabilities which allow configuration of multiple VLANs across different sections throughout the enterprise. VLAN segregation helps the administrators configure policies selectively, isolate certain policies to certain groups, or apply them as a whole to every endpoint connected to the network. Reliable device fingerprinting allows administrators to ensure that devices connected onto the network are using trusted firmware and hardware. With secure VPN tunnelling, UniNAC facilitates branch networking channels for enterprise.

Optimised networking, higher performance.

UniNAC's intelligent network monitoring capabilities makes your network work at its highest level of competency. UniNAC allows the administrator to set policies based on bandwidth, VLANs and more. UniNAC's dynamic bandwidth allocation feature sizes up a resource's requirement and allocates bandwidth efficiently. With support for multi-WAN and load balancing, UniNAC effectively aggregates bandwidth between all available connections which optimally utilises network resources while reducing performance losses. UniNAC's load balancing feature is a seamless failover mechanism which loads onto the secondary ISP in case the primary ISP fails, this ensures maximum uptime and no network failure. UniNAC can also handle multiple LAN subnets and VLANs with group based routing. UniNac seamlessly allocates dedicated Internet bandwidth to groups of users to provide QoS guarantee to endpoints.

Higher visibility, better monitoring.

With UniNAC's Network Monitoring System, you gain complete visibility of the network. From real-time AP health status, heat maps and concurrency status and more, the administrator gets a consistent, unified view of the network at all times. Admins can monitor event logs and setup alerts when malicious activity is detected. UniNac provides several troubleshooting tools for admins to gain in-depth visibility into the network.

Simplified policy enforcement.

Difficulties in policy enforcement often counteract with the steps we take to optimise our networks. UniNAC allows very easy and simplified configuration of policies to be applied to the network. UniNAC's access control policies allow the administrator to set up MAC blacklists that disallow a MAC ID from accessing the network. You can set bandwidth policies which are based on daily usage quotas, session quotas, concurrency limits and fair usage policies. UniNAC can enforce multiple compliance related functions with ease. UniNAC comes with compliance features which include Web Filtering, Web Logging, URL filtering and Call Detail Records (CDR) that ensure complete adherence to compliance related issues, at all times. UniNAC can also track real-time User Activity, adding on top of that, you can isolate users to check their website access logs.

Deeper Insights, Sharper Decisions.

UniNAC's rich dashboard enables real-time user-activity tracking with deeper insights into user behaviour. The dashboard gives you usage reports segregated by day, date and time in the form of a rich graphical chart which makes it easy for readers to comprehend information and take quicker decisions. Network diagnostics provides deep visibility into network issues, application usage and port traffic. Admins can analyse system logs and event logs to troubleshoot problems in network in real-time. UniNac also provides insights into type of devices being used, operating system information, user activities inside the network.

Leverage our solution for your enterprise requirements.

We provide a single vendor solution that enables you to get the most out of your network. UniNAC controller is deployed on premise with Falcon Series enterprise-grade UniMax Access Points. UniMax Access Points offer high concurrency, up to 128 concurrent users per Access Points, and data rates up to 1750 Mbps. All access points can be centrally managed, configured and monitored inside UniNac. UniNac comes with full featured AP controller to manage access points from single console. The entire solution takes less than *one hour* to be fully functional and deployment ready.

While it is best practice to deploy single vendor solutions for maximum performance, UniNAC can also work seamlessly with third party access points thus can be easily retrofitted into your existing networks.

Impactful solutions drive growth.

Our enterprise solutions have been deployed all over the world, we have worked with various enterprises and system integrators, all from diverse cultures. We have learned about cultural nuances, and how they impact people and stories. We understand what you need, and work with you. Here are a few ways in which our solutions helped people:

- Provides consistent performance
- Improves network security posture
- Single network dashboard
- Dashboard facilitated easy decision making
- Facilitate easy monitoring of network elements
- Layered security provided higher protection
- Ensured 100% coverage of WiFi on premise

Connect with our sales team.

sales@indionetworks.com