

EWS1000

WIRELESS LAN CONTROLLER

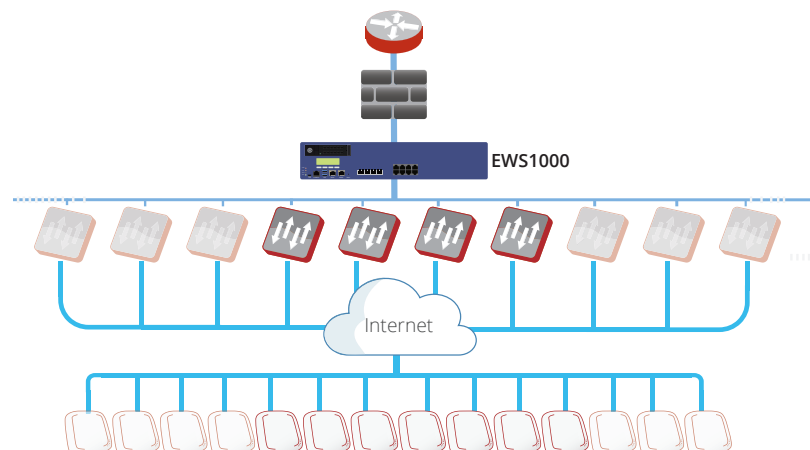


INTRODUCTION

The EWS1000 is an enterprise-grade wireless LAN controller that provides establishments such as hotels, universities, or even complete municipalities with a comprehensive set of managed Wi-Fi features at a competitive license-free price point. With AP management, user authentication, policy assignment, traffic shaping, firewall features, and much more all packaged into a single box, the EWS1000 provides network administrators with a reliable, easy-to-use, and centralized management console for an entire organization's wireless network infrastructure.

The EWS1000 is capable of managing up to 10,000 ECW-series wireless access points and can be directly integrated with Edgecore unified access switches, all of which can be deployed and configured easily by anyone, including non-wireless savvy users. For example, automated AP discovery prevents network administrators from having to go through the hassle of individually adding and configuring each access point. Access points as well as connected Wi-Fi devices can then be monitored and managed from a centralized point, with extensive logging and reporting features to assist in troubleshooting and maintenance.

For user management, the EWS1000 allows up to 100,000 connected clients. Moreover, as Wi-Fi-enabled handheld devices, such as smartphones and tablets, become ever so prevalent in our daily lives, businesses and network operators alike are faced with a mind-boggling dilemma - how to simultaneously address the needs of BYOD (Bring Your Own Device), manage Wi-Fi users, and maintain network service quality for mission-critical applications. The EWS1000 is designed exactly with these requirements in mind, and with a total cost of ownership that satisfies even the most price conscious, organizations are guaranteed to receive an unmatched ROI on their wireless LAN infrastructure.



FEATURES

SECURITY

Security is often one of the most important concerns when it comes to enterprise wireless networks. From the most basic need of preventing network access by unauthorized users to performing rogue AP detection and enforcing network isolation, the Edgecore Controllers provide a complex set of features that prevent malicious activities in an organization's network.

For deployment flexibility, the Edgecore Controllers support user authentication via both the industry standard 802.1X as well as web-based captive portals. The highly customizable captive portals with integrated walled garden capability can be adapted to suit the needs of hotels, schools, and other public venues. For unregistered users without an account, guest access can be provided by simply entering an e-mail address, logging in with social media accounts, or purchasing a data plan through PayPal.

With various account generation methods, the Edgecore Controllers are able to identify users and track user activities, ensuring network security in public Wi-Fi.

The Edgecore Controllers also support remote access via VPN, which is crucial for travelling businessmen. At the same time, site-to-site VPN establishes secure connections between corporate headquarters and branch offices.

| USER SECURITY | |
|--------------------------------------|---|
| Authentication Types | <ul style="list-style-type: none"> 802.1X UAM (browser-based) IP or MAC-based |
| Authentication Servers | <ul style="list-style-type: none"> Local On-Demand Guest RADIUS LDAP NT Domain SIP POP3 |
| Customizable Captive Portal | <ul style="list-style-type: none"> Yes |
| Customizable Wild Card Walled Garden | <ul style="list-style-type: none"> Yes |
| User Blacklisting | <ul style="list-style-type: none"> Yes |
| ACCOUNT GENERATION | |
| On-demand Account | <ul style="list-style-type: none"> SMS registration Purchase via PayPal Hotel PMS integration Selectable Billing Plans Keypad-based Account Ticket Printer |

| Guest Wi-Fi Account | <ul style="list-style-type: none"> Limitation by duration Configurable reactivation time E-mail registration and activation |
|---------------------|--|
| Social Media Login | <ul style="list-style-type: none"> Yes |
| NETWORK SECURITY | |
| VPN | <ul style="list-style-type: none"> Remote Site-to-Site |
| Tunneling Protocols | <ul style="list-style-type: none"> IPSec PPTP |
| Network Isolation | <ul style="list-style-type: none"> Intra-VLAN or Port Inter-VLAN or Port |
| Rogue AP Detection | <ul style="list-style-type: none"> Yes |
| Certificates | <ul style="list-style-type: none"> Built-in Root CA |

MOBILITY

The advent of the era of smartphones and tablets has opened a chasm between how the Internet is used and how organizations provide Internet connectivity. Wireless networks have transformed from a luxury to a necessity, in order to support devices that don't have legacy wired capability. Furthermore, additional features need to be provided in order to address the rapidly changing usage behavior.

The Edgecore Controllers support a variety of mobility features that aim to make enterprise Wi-Fi both easier to use and simpler to manage. For example, by supporting fast roaming, users on mobile devices can be on-the-go without worrying about interrupted connections. It is also not uncommon to see a single user with multiple handheld devices - with the Edgecore Controller all of the devices can login to Wi-Fi using the same username and password. Finally, mobile-optimized captive portals and ticket-printed QR code automatic login are both easy methods for a user to get online from their mobile device.

| DEVICE MOBILITY | |
|--|---|
| Fast Roaming Between Access Points | <ul style="list-style-type: none"> Yes |
| Cross Gateway Roaming | <ul style="list-style-type: none"> Yes |
| WISPr Smart Client | <ul style="list-style-type: none"> Yes |
| Mobile Device Recognition for Optimized Captive Portal | <ul style="list-style-type: none"> Yes |
| Multiple Device Logins Per Account | <ul style="list-style-type: none"> Yes |
| QR Code Automatic Login | <ul style="list-style-type: none"> Yes |
| Device Plug-and-Play | <ul style="list-style-type: none"> Yes |

MANAGEMENT

In a wireless LAN, the Edgecore Controller is the central point of management for network administrators, whether it is monitoring current online users or troubleshooting network connectivity issues. The management console of the Edgecore Controller is a browser-based GUI that is simple and intuitive to operate. From this interface, network administrators can configure traffic shaping profiles, track previous network usage, perform system backup and restore, and much more.

From the user management perspective, one of the core benefits of the Edgecore Controller is its ability to enforce different traffic profiles based on both the location (Service Zone) of the user and the time of access. For example, the profiles applied during work hours can be different from that of during after-work hours. From bandwidth limitations to specific routing rules, network administrators gain fine-grained control over Wi-Fi users.

For access points, Edgecore Controllers support automatic discovery and provisioning, eliminating many repetitive and cumbersome tasks often faced during initial network deployment. Centralized AP configuration and monitoring also greatly reduces maintenance overhead for IT staff.

SYSTEM MANAGEMENT

| | |
|-----------------------------|---|
| Browser-Based Configuration | <ul style="list-style-type: none"> Yes |
| Administrator Accounts | <ul style="list-style-type: none"> Multiple tiered access privileges Monitor each admin's current accessed page Local database and RADIUS authentication |
| System Time | <ul style="list-style-type: none"> NTP synchronization Manually configured |
| System Backup & Restore | <ul style="list-style-type: none"> Yes |
| SNMP | <ul style="list-style-type: none"> Yes; v2c |
| Network Utilities | <ul style="list-style-type: none"> Yes; built-in packet capture |

AP MANAGEMENT

| | |
|-----------------------------------|---|
| Automatic AP Discovery | <ul style="list-style-type: none"> Yes |
| Automatic AP Provisioning | <ul style="list-style-type: none"> Yes; template-based |
| Automatic AP Firmware Upgrade | <ul style="list-style-type: none"> Yes |
| AP Configuration Backup & Restore | <ul style="list-style-type: none"> Yes |
| AP Firmware Batch Upgrade | <ul style="list-style-type: none"> Yes |
| Tunneled AP Management | <ul style="list-style-type: none"> Yes; both L2 & L3 APs |
| AP Load Balancing | <ul style="list-style-type: none"> Yes |

| | |
|---------------------------|---|
| Individual AP Information | <ul style="list-style-type: none"> Associated Clients Power & Channel SNR report |
|---------------------------|---|

INVENTORY MANAGEMENT

| | |
|------------------|--|
| AP Planning Type | <ul style="list-style-type: none"> New Stock Pre-configured Configured-in-use Not-to-use |
|------------------|--|

| | |
|----------------------|---|
| AP Entry Preparation | <ul style="list-style-type: none"> CSV file uploadable Manual added |
|----------------------|---|

SWITCH MANAGEMENT

| | |
|---------------------------------------|---|
| Automatic Switch Discovery | <ul style="list-style-type: none"> Yes |
| Automatic Switch Provisioning | <ul style="list-style-type: none"> Yes; template-based |
| Switch Configuration Backup & Restore | <ul style="list-style-type: none"> Yes |
| Switch Power Scheduling | <ul style="list-style-type: none"> Yes |

USER MANAGEMENT

| | |
|------------------------------------|---|
| User Policy Assignment | <ul style="list-style-type: none"> Role-based Time & location dependent |
| Bandwidth Limitation | <ul style="list-style-type: none"> Yes |
| Traffic Classification / Remarking | <ul style="list-style-type: none"> Yes; 802.1p / DSCP |
| Stateful Firewall | <ul style="list-style-type: none"> Yes; each rule with individual enforcement schedules |
| Static Route Assignment | <ul style="list-style-type: none"> Yes |
| Concurrent Session Limit | <ul style="list-style-type: none"> Yes |
| IP Address Reassignment | <ul style="list-style-type: none"> Allow clients to obtain different IP addresses after authentication |

SERVICES

As wireless networks increasingly become the primary network used by organizations, it is crucial to take into consideration fundamental network services, such as DHCP, NAT, and routing. In addition to providing these functions, the Edgecore Controller also implements the concept of a "Service Zone", which essentially segments the controller into multiple virtual controllers, each with its own associated network services, user policies, authentication settings, etc.

On the reliability end, the Edgecore Controller supports WAN port failover, which helps businesses reduce the chance of network downtime and prevents lost productivity and revenue. Furthermore, load balancing between the WAN ports increases overall performance by alleviating congestion and distributing traffic between the two outgoing links.

Finally, the Edgecore Controller provides unique value-added capabilities, such as a direct integration with Micros Opera PMS that greatly simplifies the overhead of providing managed Wi-Fi in hotels.

NETWORK SERVICES

| | |
|--------------------------------|--|
| Redundancy (High Availability) | <ul style="list-style-type: none"> N+1 with automatic synchronization |
| Internet Protocols Supported | <ul style="list-style-type: none"> IPv4 IPv6 |
| DHCP Server / DHCP Relay | <ul style="list-style-type: none"> Yes |
| Network Address Translation | <ul style="list-style-type: none"> Yes |
| Built-in HTTP Proxy Server | <ul style="list-style-type: none"> Yes |

| | |
|--|--|
| WAN Port Load Balancing | ✦ Yes |
| Dynamic Routing | ✦ Yes |
| Local DNS Records | ✦ Yes |
| Hotel PMS Integration | ✦ Direct interface with Micros Opera PMS |
| Integrated Billing & Accounting System | ✦ Yes |
| Billing Quota Types | ✦ By duration ✦ By traffic volume |

REPORTING

Whether it is real-time monitoring of network activity or tracking the usage of previous Wi-Fi users, network administrators need the appropriate tools at their disposal to increase efficiency and reduce workload. The Edgecore Controllers have an extensive set of logging and reporting features that allow network administrators to easily find any information related to the wireless network.

The built-in system dashboard provides a quick overview of the current system status, along with graphical reports of network traffic and system performance. In addition, there is a simple interface for viewing online devices and their associated detailed statistics, including but not limited to the roles they belong to, enforced network policies, and packets transferred.

Alongside network monitoring, the Edgecore Controller also performs detailed logging of all network activity. For example, the User HTTP Web Log allows network administrators to track users who visited malicious websites, while the DHCP Lease Log can assist in troubleshooting clients who cannot receive an IP address. Lastly, the Configuration Change Log shows administrators which settings have been modified in the past, in case there are configuration errors that need to be reverted.

SYSTEM & NETWORK STATUS

| | |
|---|-------|
| System Dashboard | ✦ Yes |
| Dashboard Customization | ✦ Yes |
| Graphical System Performance Reports | ✦ Yes |
| Report Customization | ✦ Yes |
| Traffic Volume Reports | ✦ Yes |
| System Process Monitor | ✦ Yes |
| Online Device Monitoring | ✦ Yes |
| Active Sessions List | ✦ Yes |
| Configurable SYSLOG Severity | ✦ Yes |
| SMTP (E-mail) Notifications | ✦ Yes |
| Multiple Concurrent E-mail Notification Receivers | ✦ Yes |

NETWORK ACTIVITY LOGS

| | |
|---------------------|-------|
| System Log (SYSLOG) | ✦ Yes |
| CAPWAP Log | ✦ Yes |

| | |
|---|---------------------|
| Configuration Change Log | ✦ Yes; History View |
| RADIUS Server Log | ✦ Yes |
| User Events Log | ✦ Yes |
| User HTTP Web Log | ✦ Yes |
| Firewall Log | ✦ Yes |
| DHCP Server/Lease Log | ✦ Yes |
| PMS Interface Log | ✦ Yes |
| On-Demand Billing Report | ✦ Yes |
| AP Status E-mail Notification | ✦ Yes |
| Logging to External FTP | ✦ Yes |
| Configurable Logs & Reporting Intervals | ✦ Yes |

SPECIFICATIONS

SYSTEM CAPACITY*1

| | |
|--------------------|--|
| Managed APs | ✦ Up to 10,000 AP managed by split tunnels; or up to 1500 AP managed by full tunnels |
| Local Accounts | ✦ Up to 120,000 |
| On-Demand Accounts | ✦ Up to 120,000 |

HARDWARE SPECIFICATIONS

| | |
|--------------------------|---|
| Form Factor | ✦ 19" (2U) Rack Mount (Mounting bracket included) |
| Dimensions (W x D x H) | ✦ 43.8 cm x 57.0 cm x 8.8 cm |
| Weight | ✦ 19.00 kg (41.90 lbs) |
| Power | ✦ Input: 100-240 VAC, 50/60 Hz (Power cord included) ✦ Power Redundancy ✦ Hot-swappable |
| Interfaces | ✦ WAN: 2 x 10/100/1000Base-T Ethernet, Auto-MDIX, RJ-45 ✦ WAN: 2 x 10G SFP+ ✦ LAN: 2 x 10/100/1000Base-T Ethernet, Auto-MDIX, RJ-45 ✦ LAN: 2 x 10G SFP+ ✦ Console: 1 x RJ-45 ✦ USB ports: 2 x USB 3.0 ✦ Management: 2 x RJ-45 |
| LED Indicators | ✦ Power ✦ HDD ✦ Status ✦ System Fail |
| LCD Display | ✦ Yes |
| Hot-Swappable Fan | ✦ Yes (3 x Fans) |
| Environmental Conditions | ✦ Operating Temperature: 0°C (32°F) to 40°C (104°F) ✦ Operating Humidity: 10% to 90% non-condensing |

*1: Capacity limits may vary depending on configuration parameters

FEATURES HIGHLIGHTS

System Management Features

- Allow the management and configuration via console, SSHv2 and HTTPs with access control through user and password with multiple tiered access privilege
- Web administration interface is compatible with the browser Firefox and Internet Explorer
- Multiple simultaneous connections (at least 2) through SSHv2 (Secure Shell) and HTTPs
- System configuration is stored in SSD (256G)
- Network Timing Protocol (NTP - RFC 1305) is supported for clock synchronization with other devices;
- Must have installed at least 256 (two hundred and fifty-six) licenses for APs

System Network Features

- Supports Multiple VLANs (least 256) and IEEE 802.1Q standard with VLAN ID between 1 (one) and 4000 (four thousand)
- Supports WI-FI multimedia QOS (WMM) IEEE802.11e standard for traffic prioritization

Wi-Fi Management / AP Configuration Features

- Simultaneous 2.4GHz and 5GHz Wi-Fi radio operation according to IEEE802.11a/b/g/n/ac
- AP's radio frequency scanning function in the IEEE802.11a/b/g/n/ac bands for the identification of rogue APs and interferences
- Automatic or manual tuning of AP channels RF power for the optimization of wireless coverage
- Automatic load balancing between APs within the same group; Administration can define groups by selecting nearby APs
- Assign SSIDs jointly or independently in the APs
- IEEE802.1Q in the WLAN network and allows the association of at least 01 (one) VLAN for each SSID
- Each SSID can associate with a security protocol (IEEE802.11i, WPA2, WPA and AES), allowing a combination of encryption and compatible authentication specified by the IEEE802.11i protocol
- Equipment visualization by device type
- Report of access point failures
- Current associated customers' reports and SSID statistics

Web Authentication Features

- Captive Portal function, Portal Authentication or similar functionality as Web redirection for authentication, integrated in the controller or through external application
- Captive Portal function, Portal Authentication or similar, authenticate the internal user database to the controller or to an external user database server
- The Captive Portal function should allow the following types of authentication/access:
 1. Authentication with auto-register: The user accesses a captive portal and informs its data as name, email, ID and telephone and then obtains access to network
 2. Social authentication: The user accesses a captive portal and has the option to register using the Facebook or Gmail user and then logs in to the captive portal
 3. Voucher Authentication: The user receives a voucher with a registered user and password and then logs in to the captive portal
- Supports a Local database for the storage of registered users of the captive portal; for large population, the system supports external RADIUS/LDAP system as external user database. It is recommended to use external user database for a large population deployment. The external database can be a virtualized application the virtualization software must be compatible with the VMware VSPHERE 6.0 operating system
- All forms of authentication allow at least the total number of clients (100,000 connected clients) requested in the solution
- System events can be recorded and redirected remotely using a SYSLOG