Highlights

Device Profiling and Onboarding

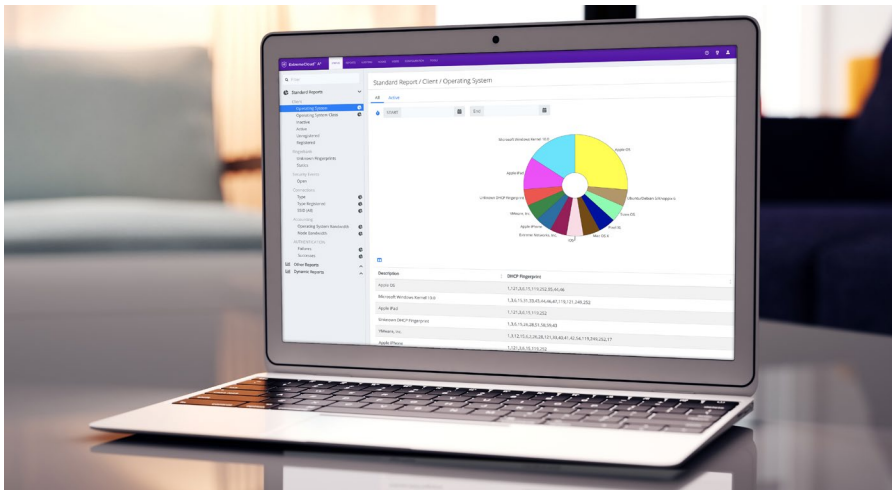
- Device fingerprinting and profiling by type, model, OS version, etc.
- Certificate management and AD integration
- IoT network access management

Authentication and Registration

- Intuitive UI for ease of corporate, guest, BYOD, and IoT policy configuration and management
- Streamlined workflows for bulk registration of users and devices
- Guest access: extensive Captive Web Portal customization, sponsor-based approvals, and Hotspot 2.0 support

Network Compliance

- Network Access Control (NAC) for multi-vendor wireless, wired and VPN networks
- Comprehensive NAC for mobile devices, with MDM integration
- Comprehensive Reporting: advanced reporting and granular alerts



ExtremeCloud™ A3

Security and Control for All Devices on the Access Network

ExtremeCloud A3 is an innovative Cloud-Managed Network Access Control (NAC) solution. It secures, manages, and controls all devices on your Access Network – from standard wireless and wired clients to IoT and BYOD.

ExtremeCloud A3 provides complete functionality for device onboarding, guest management, automated device provisioning, device profiling and access control. The industry-first cloud management option significantly streamlines the deployment and management of ExtremeCloud A3.

ExtremeCloud A3 is vendor-agnostic and runs on access networks from all major vendors.

Key Features and Benefits

Supports All Devices and Users on the Access Network

ExtremeCloud A3 secures standard wireless and wired corporate clients, BYOD, IoT and guest devices alike. It also supports the creation and administration of granular network access policies (e.g., by access to applications, time of day, location on the network) depending on the user's role.

Complete Onboarding for Guest and Corporate Devices

ExtremeCloud A3 includes a highly customizable captive web portal that supports self-service onboarding for visitor devices, while a comprehensive management interface and automated device provisioning of 802.1X certificates enables onboarding of corporate devices.

Comprehensive Authentication Toolset

For authentication of corporate devices, ExtremeCloud A3 supports 802.1X certificates with its built-in RADIUS server. Where certificates are not practical, ExtremeCloud A3 provides alternative authentication methods like Pre-Shared Keys (PSK) or Social Login (e.g., for Guest authentication).

Compliance and Remediation

ExtremeCloud A3 provides complete functionality for security posture enforcement that ensures authorized devices stay secure over time. Features include device scanning for security compliance, quarantining of non-compliant devices to prevent network access, and guided self-remediation to reduce IT helpdesk calls.

Security for the Internet of Things (IoT)

Connected user-less "things" like thermostats and lighting systems present a unique set of challenges for IT security. ExtremeCloud A3 is equipped to onboard, secure and control "Things", with the ability to automatically identify IOT, and then onboard them with appropriately restricted network access rights.

Seamless Integration With Existing IT Security Infrastructure

ExtremeCloud A3 can directly integrate with the market leading firewalls, MDM and endpoint security systems, Intrusion Detection Systems (IDS) and Posture Assessment solutions they already have installed. These integrations boost overall network security and allows customers to continue to leverage their existing security investments.

Cloud or On-premises Management

ExtremeCloud A3's industry first cloud-management option enables centralized deployment and ongoing management of local A3 instances, which greatly streamlines setup and maintenance of the solution and ensures consistent policy application and enforcement. On-premises management of ExtremeCloud A3 instances is also supported.

Device Fingerprinting and Profiling

ExtremeCloud A3 includes the world's largest continuously updated device fingerprint database. Device fingerprinting is the most comprehensive method for identifying a device type (e.g. laptop vs. smartphone vs. HVAC sensor) automatically when a device requests network access. ExtremeCloud A3 can then leverage this information to grant appropriate network access rights to each device based on its type.

Supports Access Networks From All Leading Vendors

Access networks typically include wired and wireless infrastructure components from multiple vendors. ExtremeCloud A3 supports WLAN equipment and switches from Extreme Networks and other leading vendors, which provides customers added deployment flexibility.

Usability

One of the design tenets of ExtremeCloud A3 is streamlining workflows to help simplify complex tasks. For example, the setup of new Virtual Appliances and clusters can be performed directly from the UI, and can be completed in as little as 30 minutes. A comprehensive set of troubleshooting tools is also available through the UI. These powerful tools remove the need for tedious, error-prone CLI configuration and allow administrators to be more efficient.

Product Specifications

Management Features

- Role-based Access Control *(RBAC)*
  - Per User
  - Per Switch
  - Per VLAN
  - Per Client
  - Per Client Category
  - Per Device Type
  - Per Time
  - Per Location
- Object based configuration management
  - Define roles, domains, authentication sources, switches and WLANs,and connection profiles easily
- Automated checkup and fix permissions tasks
- Accounting based on several criteria
- Node, switch groups, user, role, OS, source, realm, SSID, profile, and domain
- Violations, failures, successes, registration type, and state

Guest, BYOD and IoT Management

- Customizable Captive Web Portal
- Wireless ISP Roaming (WISPR), Eduroam, and Hotspot 2.0
- Supports billable hotspots
  - Billing and service tiers
  - Payment processing through Paypal, Mirapay, Authorize.net, Stripe
- Guest Access Self Registration
  - With or without credentials
  - Self-registration with Social login
- User device registration
- Employee sponsorship
- Email Validation
- SMS Validation
- Password-of-the-day
- "Device profile" or "device fingerprint" based onboarding

Authentication

- EAP Protocols
  - EAP-FAST, EAP-PEAP, EAP-TTLS, EAP-TLS, PAP, CHAP, MSCHAPv1 and 2, EAP-MD5
- 802.1X Support
  - RADIUS to AD/LDAP server support for 802.1X authentication
  - 802.1X (PEAP) or Certificate (TLS) BYOD automated onboarding
  - User Authentication Portal (AD/LDAP)
  - PKI with EAP EAP-TLS, EAP-TTLS, EAP-LEAP, EAP-PEAPv0,EAP-PEAPv1, EAP-MSCHAPv2
- Authentication Types
  - LDAP
    - *Microsoft Active Directory*
    - *Novell eDirectory*
    - *OpenLDAP*
    - *Any LDAP-compliant services*

Authentication (cont.)

- Authentication Types (cont.)
  - RADIUS
    - Cisco ACS
    - RADIUS *(FreeRADIUS, Radiator, etc.)*
    - Microsoft NPS
    - *Any RADIUS-compliant services*
- Local user file (Apache httpasswd format)
- OAuth2
  - Facebook
  - Google
  - GitHub
  - LinkedIn
  - Microsoft Live
  - Twitter
- SAML
- Additional built-in SQL DB for User store for deployments without LDAP

Secure Provisioning

- Android
- Windows
- APIs for all Apple devices

Network Access Control

- Realtime security policy assessment (posture assessment) and notification for multiple OS
- Gradual Deployment
  - Pre-registration
  - Per location/switch/port deployments
- Automated Device Registration
  - By network device
  - By device fingerprinting
  - By MAC address vendor
  - Integrates with third party solutions to extend device registration capabilities
  - Snort, Nessus, OpenVAS, Browser User-Agent and more
  - VLAN isolation and quarantining (See supported switches below)
- Netflow / IPFIX
- Bandwidth accounting
- Floating device support
  - Switches and APs

Profiling

- Functionality
  - Profiling of devices / IoT device recognition
  - Group based policies for network devices
  - Device visibility and identification
- Device Fingerprinting
  - World's largest device fingerprinting database
  - DHCP v4 & v6
  - User Agent
  - MAC address Patterns
  - OUI
  - TCP fingerprints
  - Behavioral analysis

Integration Capability with Complementary Security Infrastructure

ExtremeCloud A3 optionally integrates with these 3rd party IT security solutions:

- Intrusion Detection (IDS):
- OPSWAT Meta defender
- Snort
- Suricata
- Fortigate
- TrendMicro
- Vulnerability / Posture Assessment
  - Nessus
  - OpenVAS
  - Windows Management Interface
  - TNC Statement of Health protocol
- Endpoint Security
  - OPSWAT Meta defender Agent
  - Symantec SEPM
  - Sentinel One
- Mobile Device Management (MDM)
  - Mobile Iron
  - JAMF
  - AirWatch
  - Microsoft Intune
  - IBM
- Firewalls
  - Barracuda
  - Checkpoint
  - Cisco ISE-PIC
  - Fortinet
  - Fortigate
  - iBoss
  - JuniperSRX
  - PaloAlto Networks
  - Watchguard
  - JSONRPC
  - LightSpeedRocket
  - SmoothWall
- Microsoft PKI
  - Simple Certificate Exchange Protocol (SCEP)
  - Network Device Enrollment Service (NDES)

Deployment Flexibility

- Simplified Deployment
  - Out of band deployment
  - Hybrid out of band
- High Availability
  - Active/Active Clustering
  - Supports deployments of millions of devices
- Supported deployment models:
  - VMWare Virtual Appliance
  - Hyper-V Virtual Appliance

Deployment Flexibility (cont.)

- Supports WLAN Infrastructure from the following vendors:
  - Aerohive, Aruba Networks, AnyFi, Avaya, BelAir, Brocade, Cisco, D-Link, Dell, Extreme Networks, Enterasys, Extracom, Hewlett-Packard, Huawei, Juniper, Meraki, Meru Networks, MicroTik, Mojo Networks, Motorola/Zebra, Ruckus Wireless, and Xirrus Networks
- Supports network switches from all leading vendors:
  - Aerohive, Alcatel-Lucent, Avaya, Brocade, Cisco, Dell, D-Link, Enterasys, Hewlett-Packard, Huawei, Juniper, Linksys, Ubiquiti,
  - Support for Fabric Attach with EXOS switches
  - Extreme VOSS, Extreme Universal hardware and more
  - VoIP support, also in heterogenous environments, for multiple switch vendors
  - Extreme Networks, Avaya, Cisco, Hewlett-Packard and more

Hardware Requirements

- Virtual Appliance Support
  - Deployed as VA
  - VMWare ESXi 4.0 and above
  - Hyper-V Server 2021
- Minimum System requirements
  - Intel or AMD CPU 3 GHz
  - 16 GB of RAM
  - 250 GB of disk space (RAID-1 recommended)
  - 1 network card (2 recommended)
- High Performance Active Clustering
  - Minimum recommended cluster is 3 hosts for high availability, load balancing and failover
  - Significantly increases capacity and throughput
  - Enables sharing of device licenses across different customer sites.
  - SSO from XIQ
  - Improved Layer 3 Replication
  - VOSS
    - MAC Authentication 802.1X NSI assignment to Fabric Connect Reauthentication (CoA) Location based rules
  - ExtremeCloud Compliance (XCC)
    - MAC Authentication 802.1X Mac Authentication + Captive Portal Redirection 802.1X + Captive Portal Redirection,Location based rules (based on SSID)
  - EXOS MAC Authentication
    - 802.1X Mac Authentication + Captive Portal Redirection, 802.1X + Captive Portal Redirection, Vlan Assignment, Policy Assignment, NSI assignment through Fabric Attach, Re-authentication (CoA), Location based rules

Contact your ExtremeCloud A3 partner or representative for configuration assistance.

Warranty

As a customer-centric company, Extreme Networks is committed to providing quality products and solutions. In the event that one of our products fails due to a defect, we have developed a comprehensive warranty that protects you and provides a simple way to get your product repaired or media replaced as soon as possible.

ExtremeCloud A3 comes with a one year warranty against manufacturing defects. Software warranties are ninety (90) days and cover defects in media only.

For full warranty terms and conditions please go to extremenetworks.com/support/policies.

Service and Support

Extreme Networks provides comprehensive service offerings that range from Professional Services to design, deploy and optimize customer networks, customized technical training, to service and support tailored to individual customer needs. Please contact your Extreme Networks account executive for more information about Extreme Networks Service and Support.

Additional Information

For additional technical information on ExtremeCloud A3, please go to extremenetworks.com/product/A3/.

Extreme networks

http://www.extremenetworks.com/contact