

Identity and Access Control

(Formerly Network Access Control) End-to-end security and superior user experience.

HIGHLIGHTS

BUSINESS ALIGNMENT

- Protect corporate data by proactively preventing unauthorized users, compromised endpoints, and other vulnerable systems from network access
- Effectively balance security and availability for users, contractors and guests
- Proactively control the security posture of all devices, including employee owned (BYOD), on the network
- Efficiently address regulatory compliance requirements
- Cost-efficient protection for enterprise remote offices

OPERATIONAL EFFICIENCY

- Leverage existing assessment servers, authentication servers, software agents and identity sources avoiding forklift upgrades
- Enable business staff to easily sponsor guests and validate guest registration
- Protect physical and virtualized environments with flexible deployment -physical and virtual appliances

SECURITY

- Enable the strongest security with fine grained access control based on user, device, time, location and authentication type
- Assess end systems of any type for vulnerabilities or threats with agent-based or agent-less assessment
- Automate endpoint isolation, quarantine, and remediation, plus ongoing threat analysis, prevention, and containment

SERVICE AND SUPPORT

- Industry-leading first call resolution rates and customer satisfaction rates
- Personalized services, including site surveys, network design, installation and training



- Complete solution featuring both physical and virtual appliances
- Range of policy configuration options enables a uniquely fine-grained network control and flexibility
- Comprehensive dashboard reporting and advanced notification engine
- Managed guest access control with sponsorship

Product Overview

Extreme Identity and Access Control is a complete standards-based, multi-vendor interoperable pre-connect and post-connect solution for wired and wireless LAN and VPN users. Using Extreme Networks **Identity and Access** appliances and/or **Identity and Access Virtual Appliance** with **Extreme Control** management configuration and reporting software, IT administrators can deploy a leading-edge solution to ensure only the right users have access to the right information from the right place at the right time. Identity and Access Control is tightly integrated with the Extreme Networks Intrusion Prevention System (IPS) and Extreme Networks Security Information and Event Manager (SIEM) to deliver best-in-class post-connect access control.

The Identity and Access Control advantage is business-oriented visibility and control over individual users and applications in multi-vendor infrastructures, and protects existing infrastructure investments since it does not require the deployment of new switching hardware or that agents be installed on all end systems. Identity and Access Control performs multi-user, multi-method authentication, vulnerability assessment and assisted remediation. It offers the flexibility to choose whether or not to re-strict access for guests/contractors to public Internet services only—and how to handle authenticated internal users/devices that do not pass the security posture assessment. Businesses have the flexibility to balance user productivity and security. The assessment warning capability alerts users that they need to upgrade their system but can allow a grace period before they are quarantined.

Identity and Access Control policies permit, deny, prioritize, rate-limit, tag, redirect, and audit network traffic based on user identity, time and location, device type, and other environmental variables. Identity and Access Control supports RFC 3580 port and VLAN-based quarantine for Extreme Networks and third-party switches, plus more powerful isolation policies (which prevent compromised endpoints from launching attacks while in the quarantine state) on Extreme Networks switches. Identity and Access Control is adapt-able to any device using RADIUS for authorization with configurable RADIUS attributes such as Login-LAT or Filter ID. Enterprises can apply different policies depending on the RADIUS reject attribute. For example a different policy may be applied to user with an expired password than to a user who did not have an account. The solution offers unmatched interoperability, provides the widest number of authentication options, and supports Layer 2, Layer 3 and VPN access technologies.

Identity and Access Control enables the homogeneous configuration of policies across multiple switch and wireless access point vendors. This capability significantly reduces the burden of policy lifecycle management and eases deployment in wired and wireless heterogeneous infrastructures

With Extreme Identity and Access Control's flexibility, organizations have phased deployment options enabling immediate network protection and business value.

For example, an organization can start with simple endpoint detection and location directory information, then add authentication/authorization and/ or assessment, and then automate remediation.

Fine-Grained Configuration Options

Identity and Access Control configuration options provide an unparalleled range of choices for fine grained network control. These configuration options include time, location, authentication types, device and OS type, and end system and user groups. For example, enterprises can write and enforce policies that grant a precise level of network access based on the type of system connecting, an employee's role in the organization, the location of a user at the time the user is connecting, or the time of day. Device and OS type rules are particularly important in environments where users bring their own devices (BYOD). The enterprise can give these devices network access that is different than the access permitted corporate devices.

An enterprise's network is more secure with tighter control over who gains access, when and from what location. The granularity of these configuration options also provides flexibility for efficient deployment in large heterogeneous infrastructures.

Guest Account Services Included

Identity and Access Control includes automated guest registration access control features to assure secure guest

networking without burdening IT staff. Features such as expiration and account validity time control the guest account without any IT involvement. Identity and Access Control provides a self-registration portal for users to register multiple devices themselves offers advanced sponsorship capabilities such as email sponsorship and a simple portal for sponsors to use to validate guest registration. Registration capabilities are also available for automatic contact verification through SMS or email, secure wireless guest access providing access to the secured wireless network without an 802.1X certificate or involving any IT intervention. LDAP integration allows dynamic role assignment for authenticated registration. Authenticated registration allows enterprise network users to register devices and receive the proper role for non-802.1X capable devices. Multiple registration groups allow administrators to give different levels of access to different types of guests. Location based registration allows guest access to be limited to specific connection points (SSID, port, switch) or group of connection points.

Identity-Aware Networking

In an identity-aware network a user's capabilities are controlled based on the user's identity and the access policies attributed to the user. Identity and Access Control provides user identity functionality including discovery, authentication and role based access controls. Identity and Access Control integrates with identity sources such as Siemens Enterprise Communications HiPath DirX Identity and Microsoft Active Directory leveraging and extending the organization's existing directory investments. Users are managed centrally in the identity system for the network and all connected applications. The process of managing the user's lifecycle (e.g. enrollment, role changes, termination) can be automated and linked to other business processes with LDAP and RADIUS integration. Users can be automatically added or deleted when they join or leave the organization. Extreme Networks identity-aware networking capabilities provide stronger network security and lower operational cost.

Endpoint Baseline and Monitoring

All end systems in the network infrastructure should be incorporated in the network access control system for control to be most effective. Identity and Access Control provides agent-based or agent-less endpoint assessment capabilities to determine the security posture of connecting devices. Aligned with industry standards, the system works with multiple assessment servers, authentication servers and security software agents to match the needs of organizations who may have existing assessment technology. The agentless capability does not require the installation of a software security agent on the end system and is typically used for end systems such as guest PCs, IP phones, IP cameras or printers. The agent-less assessment scans for operating system and application vulnerabilities. The agent-based capability requires the

installation of a software agent on the end system. The endpoint agent scans for anti-virus status, firewall status, operating system patches and peer-to-peer file sharing applications. The agent can look for any process or registry entry and automatically remediate.

Notifications and Reporting

The advanced notification engine provides comprehensive functionality and integrates with the workflows of other alerting tools already in place. Enterprises can leverage and extend their existing automated processes to further reduce operational costs. Notifications occur for end-system additions or state changes, guest registration, any custom field change, and end-system health results. Notification is delivered through traps, syslog, email or web service. The notification engine has the ability to run a program triggered by a notification event. For example, integrated with the help desk application, notifications can be used to automatically map changes in the infrastructure to actions.

End-system reporting is simple with Identity and Access Control web-based end-system data views. The system provides easy-to-use dashboards and detailed views of the health of the end systems attached or trying to attach to the network. Analysts responsible for monitoring endsystem compliance can easily tailor the views to present the information in their preferred format. The reports can be generated as PDF files.

In addition, the end-system monitoring and management plays a key role in understanding the network. It allows administrators to understand the “who, what, when, where, and how” for the end-systems on the network providing better visibility, troubleshooting, and security. Now, tracking end-systems to find all information about them, including the NetFlow data is found by simply searching for a username, hostname, or address.

Integrations

The Extreme Connect API provides a simple, open, programmable and centrally managed way to implement Software Defined Networking (SDN) for any network. With Extreme Connect, business applications can be directly controlled from Extreme Control Center. The result is a complete SDN solution including integrations with the solution such as MDM integrations with vendors such as Airwatch, Mobile Iron, JAMF Software, and more, as well as datacenter management, integrations with iBoss web filters and many other products.

Extreme Control Management

Extreme Control software provides secure, policy-based management. From one centralized location, IT staff can configure and control the solution, simplifying deployment and ongoing administration. Identity and Access Control management also aggregates network connectivity and vulnerability statistics, audits network access activities, and provides detailed reports on vulnerabilities in the network.

Management is simplified with a hierarchical structure that places end systems into administrative zones.

ExtremeControl provides additional value through its integration with other Extreme Networks NetSight capabilities and Extreme Networks security products. For example, NAC management seamlessly integrates with NetSight policy management to enable “one click” enforcement of role-based access controls. The IP-to-ID Mapping feature binds together the User, Hostname, IP address, MAC and location (switch and port or wireless AP and SSID) along with timestamps for each endpoint—a key requirement for auditing and forensics. IP-to-ID Mapping is also used by NetSight Automated Security Manager to implement location-independent distributed intrusion prevention and by Extreme Networks Security Information and Event Manager (SIEM) or other third party SIEM/IPS solutions to pinpoint the source of a threat. NAC management in NetSight provides centralized visibility and highly efficient anytime, anywhere control of enterprise wired and wireless network resources. OneView, the unified control interface, enables simplified troubleshooting, help desk support tasks, problem solving and reporting. Users of any of the popular mobile devices can use their smart phone or tablet to access NAC end-system view, system location and tracking information and much more, anytime anywhere.

Extreme Networks Identity and Access Appliance

The Identity and Access appliance controls endpoint authentication, security posture assessment and network authorization. For authentication services, the Identity and Access appliance acts as a RADIUS proxy, or RADIUS server for MAC Authentication, which communicates with the organization’s RADIUS authentication services (e.g. interfaces with Microsoft Active Directory or another LDAP-based directory service). The Identity and Access appliance supports 802.1X (Extensible Authentication Protocol), MAC, Web-based and Kerberos Snooping (with certain restrictions) authentication. For endpoint assessment, the Identity and Access appliance connects to multiple security assessment servers.

For authorization services, the Identity and Access appliance communicates RADIUS attributes to the authenticating switch. This allows the switch to dynamically authorize and allocate network resources to the connecting endpoint based on authentication and assessment results.

The Identity and Access appliance also stores configuration information and the physical location of each endpoint. It easily scales to support redundancy and large deployments. Identity and Access appliance models are available to meet the needs of different-sized implementations.

Assessment is separately licensed and includes both agent-based and agent-less assessment.

Extreme Networks Identity and Access Virtual Appliance

The Identity and Access Virtual Appliance provides all the powerful endpoint authentication, security posture assessment and network authorization capabilities built on VMware®. Deploying Identity and Access Virtual Appliance, enterprises gain all the benefits of network access control with the advantages of a virtual environment — cost savings from using existing hardware and reduced time to value. Available with different sizing options for central locations as well as remote sites.

Additional Features

- “Bring your own device” (BYOD) control features including mobile device registration and session-based user login.
- IPv6 support for implementation in networks with IPv6 end systems.
- Proven interoperability with Microsoft NAP and Trusted Computing Group TNC.
- Automatic endpoint discovery and location tracking by identifying new MAC addresses, new IP addresses, new 802.1X / Web-based authentication sessions, or Kerberos or RADIUS request from access switches.
- Support for Layer 2 deployment modes and support for all five deployment models: intelligent wired edge, intelligent wireless edge, non-intelligent wired edge, non-intelligent wire-less edge, and VPN.
- Identity and Access Control provides VPN support and, with an Extreme Networks SSA switch in distribution, provides more flexibility through policy.
- Support for external RADIUS Load Balancers allows the external load balancer to evenly distribute the load for servicing authentication requests and configuring switches across a group of Access Control Appliances.
- Management options can be tailored to existing network management schemes and security requirements.
- Support for multiple RADIUS and LDAP server groups allows administrators to identify the server to which a request is directed.
- Macintosh agent support for agent-based assessment.
- Open XML API's support integration with IT workflows for automated streamlined operations
- Web-service based API simplifies integration with third party applications.
- 1 + 1 Redundancy for Layer 2 deployment modes: provides high-availability and eliminates the Identity and Access appliance as a single point of failure

- Risk level configuration allows flexibility in determining threat presented by the end system. Fine grained control allows NAC administrator to define High Risk, Medium Risk, and Low Risk thresholds based on local security policies and concerns.

System Requirements and Specifications

EXTREME NETWORKS IDENTITY AND ACCESS APPLIANCES

Physical Specifications

Height: 1.75" (4.45 cm) - 1U

Length: 27.95" (70.9 cm)

Width 16.93" (43 cm)

Weight 31.8 lbs (14.4 kg)

Power

Wattage: 750 Watt (max), each power supply

Voltage: 110/240 VAC;

Frequency 47- 63Hz

Environmental Specifications

Operating Temperature: 10° to 35°C (50° to 95°F)

Storage Temperature: -40° to 70°C (-40° to 158°F)

Operating Humidity: 5% to 90% (noncondensing)

Standards Compliance

Regulatory/Safety:

UL60950 - CSA 60950 (USA/Canada)

EN60950 (Europe)

IEC60950 (International)

CB Certificate and Report, IEC60950

GS Certification (Germany)

GOST R 50377-92 - Certification (Russia)

Ukraine Certification (Ukraine)

CE - Low Voltage Directive

2006/95/EC (Europe)

IRAM Certification (Argentina)

Emissions/Immunity:

FCC/ICES-003 - Emissions (USA/Canada)

CISPR 22 - Emissions (International)

EN55022 - Emissions (Europe)

EN55024 - Immunity (Europe)

EN61000-3-2 - Harmonics (Europe)

EN61000-3-3 - Voltage Flicker (Europe)

CE - EMC Directive 2004/108 EC (Europe)

VCCI Emissions (Japan)

AS/NZS 3548 Emissions (Australia/New Zealand)

BSMI CNS13438 Emissions (Taiwan)

GOST R 29216-91 Emissions (Russia)

GOST R 50628-95 Immunity (Russia)

Ukraine Certification (Ukraine)

KC Certification (Korea)

Extreme Networks Identity and Access Virtual Appliance

A virtual appliance is a software image that runs on a virtual machine. The Identity and Access Virtual Appliance is packaged in the .OVA file format defined by VMware and must be deployed on a VMware ESXTM 4.0, 4.1, 5.0, or 5.1 server or ESXiTM 4.0, 4.1, 5.0, or 5.1 server with a vSphere(TM) 4.0, 4.1, 5.0, or 5.1 client.

Virtual appliance requires 12 GB of memory, four CPUs, two network adapters, and 40 GB of thick-provisioned hard drive space.

Assessment Agent OS Requirements

Supported operating systems for end systems connecting to the network through an Extreme Networks Identity and Access Control deployment that is implementing Extreme Networks agent-based assessment.

- Windows 2000
- Windows 2003
- Windows 2008
- Windows XP
- Windows Vista
- Windows 7
- Windows 8
- Windows 8.1
- Mac OS X – Tiger, Leopard, Snow Leopard, Lion, Mountain Lion, and Mavericks

Certain assessment tests require the Windows Action Center (previously known as Windows Security Center) which is supported on Windows XP SP2+, Windows Vista, Windows 7, 8, and 8.1 operating systems.

ExtremeControl Management

Control Center provides the management capabilities for NAC. A single server will support: 100,000 end-systems; 50,000 end-system registrations; 12,000 end-systems with agent-based assessment; 35 appliances.

NETSIGHT SERVER AND CLIENT OS REQUIREMENTS

These are the operating system requirements for both the NetSight Server and remote NetSight client machines.

Windows (qualified on the English version of the operating systems)

Windows Server® 2003 w/ Service Pack 2 (64-bit and 32-bit)

Windows XP® w/ Service Pack 3 (32-bit only)

Windows Server® 2008 Enterprise and R2 (64-bit and 32-bit)

Windows Server 2012 Enterprise (64-bit only)

Windows® 7 (64-bit and 32-bit)

Windows® 8 and 8.1 (64-bit and 32-bit)

Linux

Red Hat Enterprise Linux WS and ES v5 and v6 (64-bit and 32-bit)

SuSE Linux versions 10, 11, and 12.3 (64-bit and 32-bit)

Ubuntu 11.10 Desktop version (32-bit , remote NetSight client only)

Ubuntu 11.10, 12.04, and 13.04 (64-bit)

Mac OS X® 64-bit (remote client only) Leopard®, Snow Leopard®, Lion®, Mountain Lion®, or Mavericks®

VMware® (64-bit Virtual Appliance) VMware ESXi™ 4.0, 4.1, 5.0, 5.1, or 5.5 server

Server and Client Hardware Requirements

These are the hardware requirements for the Server and client machines:

ExtremeControl Server

Minimum - 32-bit Windows 7; Dual-Core 2.4 GHz Processor, 2 GB RAM, 10 GB Free Disk Space

Medium - 64-bit Desktop, Windows 2008 R2 or Linux; Quad-Core 2.66 GHz Processor, 8 GB RAM, 40 GB Free Disk Space

Large - 64-bit Server Linux; Dual Quad-Core Intel® Xeon CPU E5530 2.4 GHz Processors, 12 GB RAM, 100 GB Free Disk Space

ExtremeControl Client

Recommended-Dual-Core 2.4 GHz Processor, 2 GB RAM Free Disk Space-100MB (User's home directory requires 50MB for file storage)

Java Runtime Environment (JRE) 6 or 7 (also referred to as 1.6 or 1.7)

Supported Web Browsers

- Internet Explorer version 8, 9, and 10
- Mozilla Firefox 23 and 24
- Google Chrome 29.x

Ordering Information

IDENTITY AND ACCESS APPLIANCES

PART NUMBER	DESCRIPTION
IA-A-20	Identity and Access appliance supports 3,000 to 6,000 end-systems based on options. HW-only appliance (IA-ES license required)
IA-A-300	Identity and Access appliance supports 6,000 to 12,000 end-systems based on options. HW-only appliance (IA-ES license required)
Virtual Appliances	Virtual appliances are included in NetSight Advanced (IA-ES license required)

POWER CORDS

In support of its expanding Green initiatives as of July 1st 2014, Extreme Networks will no longer ship power cords with products. Power cords can be ordered separately but need to be specified at the time order. Please refer to www.extremenetworks.com/product/powercords/ for details on power cord availability for this product.

EXTREME CONTROL MANAGEMENT

Models range from a cost-efficient entry solution to full functionality for device intensive enterprises. Flexible upgrade options support deployment growth.

The Three Models Are:

NMS-BASE-XX which includes basic wired/wireless management features as well as inventory management, policy management and OneView™ Basic (device management, alarm management and administration). 3 remote clients are included.

NMS-XX which includes basic wired/wireless management features as well as inventory management, policy management, NAC management, automated security management, mobile management, and the full OneView™ interface. 25 remote clients are included.

NMS-ADV-XX which includes basic wired/wireless management features as well as inventory management, policy management, Identity and Access Control management, automated security management, mobile management, and the full OneView™ interface. In addition, NetSight Advanced includes advanced wireless management, the OneFabric Connect API, ability to install on a primary server, redundant server and lab server, a 500 end-system license, and virtual NAC appliances for full NAC deployment flexibility (require end-system licenses if needed in addition to the 500 included). 25 remote clients are included.

LICENSES

PART NO.	DESCRIPTION
IA-ES-1K	Identity and Access 1,000 end-system license for use with Identity and Access appliances
IA-ES-3K	Identity and Access 3,000 end-system license for use with Identity and Access appliances
IA-ES-12K	Identity and Access 12,000 end-system license for use with Identity and Access appliances
IA-PA-3K	Identity and Access Posture Assessment license for 3,000 end-systems (includes both agent-based and agent-less assessment)
IA-PA-12K	Identity and Access Posture Assessment license for 12,000 end-systems (includes both agent-based and agent-less assessment)

SIZING CHART

# MANAGED DEVICES	# APS	MODEL NUMBERS		
5	50	NMS-ADV-5	NMS-5	
10	100	NMS-ADV-10	NMS-10	NMS-BASE-10
25	250	NMS-ADV-25	NMS-25	NMS-BASE-25
50	500	NMS-ADV-50	NMS-50	NMS-BASE-50
100	1,000	NMS-ADV-100	NMS-100	NMS-BASE-100
250	2,500	NMS-ADV-250	NMS-250	NMS-BASE-250
500	5,000	NMS-ADV-500	NMS-500	NMS-BASE-500
Unrestricted	Unrestricted	NMS-ADV-U	NMS-U	NMS-BASE-U

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.

The appliance 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: <http://learn.extremenetworks.com/rs/641-VMV-602/images/Extreme-Networks-Product-Warranty.pdf>

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, please go to: <http://www.extremenetworks.com/product/network-access-control>



<http://www.extremenetworks.com/contact> / Phone +1-408-579-2800

©2016 Extreme Networks, Inc. All rights reserved. Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries. All other names are the property of their respective owners. For additional information on Extreme Networks Trademarks please see <http://www.extremenetworks.com/company/legal/trademarks>. Specifications and product availability are subject to change without notice. 4334-0116-25