Enterasys PODNet

Registration, Tracking and Secure, Differentiated Access for Mobile Devices in Education

Complete BYOT or iDevice solution providing registration, sponsorship, tracking, security and appropriately provisioned access

Easy directory integration via LDAP

Automated access control and bandwidth management for any wired or wireless device

Manages access based on device type, OS type, user group, OUI, access method, location or time-of-day

Product Overview

The Enterasys PODNet solution is a standards-based, multi-vendor interoperable, pre-connect and post-connect Network Access Control solution for BYOT (bring your own technology), iDevice and or 1 to 1 programs in schools. It enables self-registration of personal or district devices, incorporates optional sponsored and guest access and works across both wired and wireless networks. With Enterasys' PODNet, network administrators can deploy a simple-to-use access control solution that registers and tracks every device and user on the network. With our LDAP integration, access for each device type, OS type or user group can be automatically provisioned with appropriate access to applications, bandwidth and Internet resources from an approved location and at an approved time. PODNet is tightly integrated with the Enterasys Wireless and Enterasys Network Management Suite (NMS) to deliver optimal pre and post-connect visibility and control.

The Enterasys PODNet advantage is education-oriented visibility and control over individual students, devices and applications in wired and wireless infrastructures. PODNet protects existing infrastructure investments since it does not require the deployment of new switching hardware or that agents be installed on end systems. The Authentication Gateway appliance performs registration, multi-user/multi-method authentication and policy enforcement. Optional features include vulnerability assessment and assisted remediation. The system offers the flexibility to choose whether or not to restrict access and bandwidth for personal devices/guests to public Internet services only—and allows differentiated access for authenticated internal users/devices. School districts now have the flexibility to easily support enhanced learning initiatives, through BYOT, iDevice or 1 to 1 programs, without the potential chaos that would ensue without proper management and security.

Enterasys PODNet policies permit, deny, prioritize, rate-limit, tag, re-direct, and audit network traffic based on user identity, time and location, device type, and other environmental variables. The authentication gateway supports RFC 3580 port and VLAN-based quarantine for Enterasys and third-party switches, plus more powerful isolation policies (which prevent compromised endpoints from

Benefits

Business Alignment

- Protects the school network while providing appropriate access to applications and the Internet
- Effectively balances security and availability for personal devices use
- Proactively controls access and bandwidth utilization for all devices on the network
- Simplifies the management of BYOT, iPad or 1 to 1 deployments
- Provides network-based support for success with Digital Driver's License programs

Operational Efficiency

- Leverages existing directory, RADIUS servers and network infrastructure
- Allows administrative staff to easily validate and sponsor device registration
- Automation allows technology staff to spend more time on technology integration in the classroom

Security

- Enables the strongest security with fine grained access control based on user, device, OS, time, location and authentication type
- Efficiently address CIPA and AUP compliance requirements
- 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

There is nothing more important than our customers.

launching attacks while in the quarantine state) on Enterasys switches. Enterasys PODNET is adaptable 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.

Enterasys PODNET 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 Enterasys PODNET's flexibility, organizations have phased deployment options enabling immediate network protection and educational value. For example, a school district can start with simple endpoint detection and location directory information, then add authentication/authorization, registration and/ or assessment, and then automate remediation.

Fine-Grained Configuration Options

Enterasys PODNET configuration options provide an unparalled range of choices for fine grained access control. These configuration options include time, location, authentication types and end system and user groups. For example, schools can write and enforce policies that grant a precise level of network access based on the type of system connecting, a user's role in the organization, the location of a user at the time the user is connecting, or the time of day. A school district'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

Enterasys PODNET includes automated guest registration access control features to assure secure guest networking without burdening IT staff. PODNET capabilities automate or delegate guest access management. Features such as expiration and account validity time control the guest account without any IT involvement. Enterasys PODNET provides a self-registration portal for users to register multiple devices themselves. PODNET offers advanced sponsorship capabilities such as email sponsorship and a simple portal for sponsors to use to validate guest registration. LDAP integration allows dynamic role assignment for authenticated registration. Authenticated registration allows students 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 devices/users.

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. Enterasys PODNET provides user identity functionality including discovery, authentication and role -based access controls. Enterasys PODNET 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, and termination) can be automated and linked to other processes with LDAP and RADIUS integration. Users can be automatically added or deleted when they join or leave the organization. Enterasys identity-aware networking capabilities provide stronger network security and lower operational cost.

Endpoint Base-lining and Monitoring

All end systems in the network infrastructure should be incorporated in the network access control system for control to be most effective. Enterasys PODNET provides agent-based or agent-less endpoint assessment capabilities to determine the security posture of connecting devices. Enterasys PODNET, aligned with industry standards, works with multiple assessment servers, authentication servers and security software agents to match the needs of organizations who may have existing assessment technology. The agent-less 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 Enterasys 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. This combination of agent and agent-less capabilities in the Enterasys PODNET solution enables more efficient management and reporting.

Notifications and Reporting

The advanced notification engine in Enterasys PODNET provides comprehensive functionality and integrates with the workflows of other alerting tools already in place. School districts can leverage and extend their existing automated processes to further reduce operational costs. Notifications occur for end-system state changes, device registration and end-system health results. Notification is delivered through traps, syslog, and 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, PODNET notification can be used to automatically map changes in the infrastructure to actions.

End-system reporting is simple with Enterasys PODNET web-based end-system data views. PODNET provides easy-to-use dashboards and detailed views of the health of the end systems attached or trying to attach to the network.

NMS NAC Manager

NMS NAC Manager Software provides secure, policy-based NAC management. From one centralized location, IT staff can configure and control the PODNET solution, simplifying deployment and on-going administration. NAC Manager also aggregates network connectivity and vulnerability statistics, audits network access activities, and provides detailed reports on vulnerabilities in the network.

NMS NAC Manager provides additional value through its integration with other Enterasys NMS applications and Enterasys security products. For example, Enterasys NMS NAC Manager seamlessly integrates with NMS Policy Manager to enable "one click" enforcement of role-based access controls. The NMS NAC Manager 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 NMS Automated Security Manager to implement location-independent distributed intrusion prevention and by Enterasys Security Information and Event Manager (SIEM) or other third party SIEM/IPS solutions to pinpoint the source of a threat.

Rogue DHCP and Downstream Loop Prevention

The Enterasys PODNet solution, when extended to wired networks, prevents rogue DHCP and downstream network loops by forcing authentication and dynamic application of access controls. Neither authorized users/devices or guests are allowed to source DHCP, only approved servers. If any non-approved hub, switch or access point is connected to any wired port, it will be denied access. This prevents unauthorized modification to the district network and eliminates the possibility of debilitating downstream loops which are commonly found in K-12 networks. This functionality, when combined with other Enterasys switch control features can completely prevent any and all loop conditions from impacting the network and creating a disruption in service.

Enterasys Authentication Gateway

The Enterasys Authentication Gateway controls endpoint authentication, security posture assessment and network authorization. For authentication services, the Enterasys Authentication Gateway 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 Enterasys Authentication Gateway supports 802.1X (Extensible Authentication Protocol), MAC, Web-based and Kerberos Snooping (with certain restrictions) authentication. For endpoint assessment, the Enterasys Authentication Gateway connects to multiple security assessment servers.

For authorization services, the Enterasys Authentication Gateway 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 Enterasys Authentication Gateway appliance also stores PODNET configuration information and the physical location of each endpoint. It easily scales to support redundancy and large PODNET deployments.

Enterasys Authentication Gateway models are available to meet the needs of different-sized implementations. It is also available as a security module for popular Enterasys switches.

Assessment for the Authentication Gateway is separately licensed and includes both agent-based and agent-less assessment.

Enterasys Authentication Gateway Virtual Appliance

Enterasys Authentication Gateway Virtual Appliance provides all the powerful endpoint authentication, security posture assessment and network authorization capabilities built on VMware®. Deploying Authentication Gateway 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.

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

Additional Features

- 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 and Layer 3 deployment modes and support for all five PODNET deployment models: intelligent wired edge, intelligent wireless edge, non-intelligent wired edge, non-intelligent wireless edge, and VPN.
- Management options (in-band or Authentication) 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 PODNET API simplifies integration with third party applications.
- 1 + 1 Redundancy for both Layer 2 and Layer 3 deployment modes: provides high-availability and eliminates the Inline or Authentication Gateway as a single point of failure
- Risk level configuration allows flexibility in determining threat presented by the end system. Fine grained control allows the PODNET administrator to define High Risk, Medium Risk, and Low Risk thresholds based on local security policies and concerns.
- The Enterasys Inline and Authentication Gateway are upgradable, allowing assessment to be integrated onto a single box with the other PODNET functions. The upgraded appliances are capable of supporting both network-based and/or agent-based assessment.

Specifications

NMS NAC Manager

NMS NAC Manager is a plug-in application for the Enterasys Network Management Suite (NMS). NMS is available for 32-bit operating systems:

Windows (qualified on the English version of the operating systems)
Windows Server® 2003 w/ Service Pack 2
Windows XP® w/ Service Pack 2 or 3
Windows Vista® (Service Pack 1 Optional)
Windows Server® 2008 Enterprise
Windows Server® 2008 Enterprise 64-bit (as 32-bit application)

Linux
Red Hat Enterprise Linux WS and ES v4 and v5
SuSE Linux versions 10 and 11

Hardware Requirements
Recommended P4-2.4 GHz, 2GB RAM
(User's home directory requires 50MB for file storage)
(Windows Vista requires 2GB RAM)
Free Disk Space - 1GB

Remote Client
Recommended P4-2.4 GHz, 1GB RAM
(Windows Vista requires 2GB RAM)
Free Disk Space - 100MB
(User's home directory requires 50MB for file storage)
Supported Web Browsers:
Internet Explorer version 7 and 8
Mozilla Firefox 2.0 and 3.0
Java Runtime Environment (JRE) 1.5 or higher
(Windows Vista requires JRE 1.6 or higher)

Enterasys Authentication Gateway

Physical Specifications
NAC-A-20
Height: 1.68" (4.26 cm); Width: 18.99" (includes rack latches) (48.24 cm); Depth: 30.39" (includes PSU handles and bezel) (77.2 cm); Weight: 39 lbs. (17.69 Kgs)

SNS-TAG-HPA
Form Factor: 19" rack mount; Height: 1.75" (44.4 mm); Width: 17.2" (437 mm); Depth: 17.8" (452.16 mm); Weight: 15.4 lbs. (7 kg)

Power
NAC-A-20
Wattage: 717 Watt (high output), 570 Watt (Energy Smart); Voltage: 90- 264 VAC, auto ranging, 47- 63Hz

SNS-TAG-HPA
Wattage: 400 watts maximum; Input Frequency 50 to 60 Hz; Input Voltage: Range 100 to 125 VAC; Input Current: 120 V 6 Amps; 240 V 3 Amps

Environmental Specifications
NAC-A-20
Operating Temperature: 10° to 35°C (50° to 95°F) with a maximum temperature gradation of 10°C per hour. Note: For altitudes above 2950 feet, the maximum operating temperature is de-rated 1°F/550 ft.; Storage Temperature: -40° to 65°C (-40° to 149°F) with a maximum temperature gradation of 20°C per hour; Operating Humidity: 20% to 80% (non-condensing) with a maximum humidity gradation of 10% per hour

SNS-TAG-HPA
Operating Temperature: 5° C to 40° C (41° F to 104° F); Storage Temperature: -30° C to 73° C (-22° F to 164° F); Operating Humidity: 5% to 90% RH, non-condensing

Agency and Regulatory Standard Specifications
Safety
NAC-A-20
UL 60950-1, CSA 22.1 60950, EN 60950-1, and IEC 60950-1, NOM

SNS-TAG-HPA
UL 60950, CSA C22.2 No. 60950, EN 60950, IEC 60950

Electromagnetic Compatibility
NAC-A-20
FCC Part 15 (Class A), ICES-003 (Class A), BSMI, KCC, VCCI V-3, AS/NZS CISPR 22 (Class A), EN 55022 (Class A), EN 55024, EN 61000-3-2, EN 61000-3-3

SNS-TAG-HPA
FCC: 47 CFR Parts 2 and 15, ICES-003, EN 55022, EN 61000-3-2, EN 61000-3-3, EN 55024, AS/NZS CISPR 22, VCCI V-3

Enterasys Authentication Gateway Virtual Appliance

Packaged in the .OVA file format defined by VMware and must be deployed on a VMware ESX(TM) 4.0 server or ESXi(TM) 4.0 server with a vSphere(TM) 4.0 client.

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

NAC Assessment Agent OS Requirements

Supported operating systems for end systems connecting to the network through an Enterasys PODNET deployment that is implementing Enterasys agent-based assessment.

- Windows 2000
- Windows 2003
- Windows 2008
- Windows XP
- Windows Vista
- Windows 7
- Mac OS X (Tiger, Leopard)

Certain assessment tests require the Windows Security Center which is only supported on Windows XP SP2+, Windows Vista, and Windows 7.

Ordering Information

PODNET Authentication Gateway

Part Number	Description
NAC-A-20	Enterasys Authentication Gateway 3,000 endpoints, optional on-board assessment
NAC-V-20	Enterasys Authentication Gateway Virtual Appliance 3,000 endpoints, optional on-board assessment
NAC-VB-20	Enterasys Virtual Gateway Bundle with 4 Authentication Gateway Virtual Appliances (500 endpoints each), optional on-board assessment
WS-VBYOD-NAM	Enterasys Virtual Gateway Bundle with V-NAC 500 endpoint license and V2110 Virtual Wireless Controller for 16 access points (expandable to 120 access points with optional license)

NAC Manager/NMS Bundles

Part Number	Description
NS-NAC	NMS NAC Manager. Requires existing Enterasys Network Management Suite NMS-BASE-X
NMS-5	NMS Suite Bundle (5 device license includes Console, Inventory, Policy, NAC, OneView and ASM. Appropriate for wireless only deployments)
NMS-10	NMS Suite Bundle (10 device license includes Console, Inventory, Policy, NAC, OneView and ASM. Appropriate for small wired and wireless deployments)
NMS-25	NMS Suite Bundle (25 device license includes Console, Inventory, Policy, NAC, OneView and ASM. Appropriate for small wired and wireless deployments)
NMS-50	NMS Suite Bundle (50 device license includes Console, Inventory, Policy, NAC, OneView and ASM. Appropriate for medium wired and wireless deployments)
NMS-100	NMS Suite Bundle (100 device license includes Console, Inventory, Policy, NAC, OneView and ASM. Appropriate for medium to large wired and wireless deployments)
NMS-250	NMS Suite Bundle (250 device license includes Console, Inventory, Policy, NAC, OneView and ASM. Appropriate for large wired and wireless deployments)

NAC Assessment

Part Number	Description
NAC-ASSESS-LIC	Enterasys NAC Assessment, includes both agent-based and agent-less assessment

Warranty

As a customer-centric company, Enterasys 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 products repaired or media replaced as soon as possible.

Enterasys Authentication Gateway 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://www.enterasys.com/support/warranty.aspx.

Service & Support

Enterasys 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 Enterasys account executive for more information about Enterasys Service and Support.

Additional Information

For additional technical information on Enterasys PODNET http://www.enterasys.com/products/advanced-security-apps/enterasys-network-access.aspx

Contact Us

For more information, call Enterasys Networks toll free at 1-877-801-7082, or +1-978-684-1000 and visit us on the Web at enterasys.com

enterasys® Secure Networks™

Delivering on our promises. On-time. On-budget.

10/11

Thought Leadership
Patented Innovation