

NAC Director

Comprehensive NAC Solution

- Identity Management
- Endpoint Compliance
- Usage Policy Enforcement
- Historical Auditing and Reporting

Out-of-Band Architecture

- Leverages existing network and security infrastructure
- Non-intrusive deployment and flexible implementation options
- Highly scalable: one appliance manages policy across wired, wireless and VPN networks

Edge Enforcement

- Enforces access policies at the point of access to the network
- Distributes enforcement load across the network fabric
- Provides highest security, flexibility and scalability

High Performance and Availability

- High-performance architecture
- Fully redundant appliances
- High-availability configurations

Out-of-Band Network Access Control for Wired, Wireless and VPN Networks



NAC Director is a comprehensive Network Access Control (NAC) solution offering enterprises role-based identity management, endpoint compliance verification and usage policy enforcement capabilities across wired, wireless or VPN connections. Easily integrated into existing network environments, NAC Director's out-of-band architecture leverages the inherent security capabilities of existing network equipment along with standard or de facto standard authentication and authorization technologies such as 802.1X, RADIUS, and Active Directory to control network access down to the point of access. By leveraging existing technology investments, enterprises can quickly add advanced NAC capabilities to their current networks and avoid the need for expensive forklift upgrades or the scalability and management challenges of adding in-line equipment.

Through an easy-to-use web interface, NAC Director gives network and security administrators powerful tools to create 7-point identity profiles for users and devices on the network. Comprehensive access policies can be applied to users, including employees, contractors or guests, as well as devices including PCs, laptops, servers, printers, IP phones, and other network-attached devices. Utilizing either persistent or dissolvable agents, NAC Director enables thorough posture assessment of Windows, Linux, and Apple OS devices. NAC Director then uses this information to determine the appropriate level of network access for authorized users and devices, or the required remediation services for unauthorized users or non-compliant devices. By automating the process of authentication, assessment, authorization, and remediation, NAC Director offers enterprises a comprehensive user-focused, network-based access control solution.

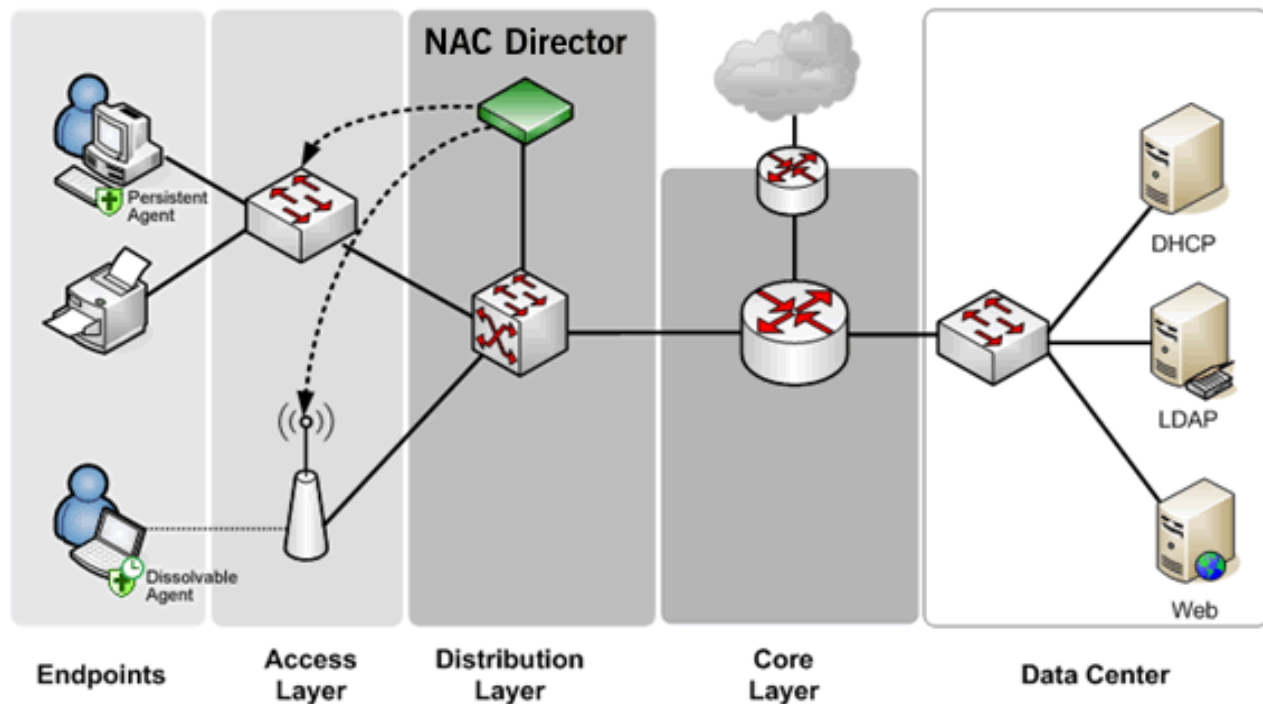
NAC Director's distributed, highly scalable, high availability architecture supports a broad range of wired, wireless, and VPN networks. Its inherent flexibility lets IT organizations gracefully evolve their NAC projects from initial trials to pilot roll-outs to full deployments to ensure effective security policy implementations with minimal impact on user experience.



NAC DIRECTOR SOLUTION COMPONENTS

Bradford's NAC Director solution consists of NAC Director appliances, an optional Network Security Manager (NSM) appliance, and agent software. These components are deployed in a variety of configurations based on the enterprise environment.

Component	Description
NAC Director Appliance	Out-of-band appliance that provides enterprise-wide policy management and enforcement. (Larger enterprises may deploy multiple appliances, depending on the size of the user environment)
Network Security Manager (NSM) Appliance	Centralized management appliance that provides management and control for multiple distributed NAC Director appliances via a common console. Used in larger enterprise environments where two or more appliances are deployed.
Persistent or Dissolvable Agent	Lightweight client software used in assessing endpoint device posture. The persistent agent is installed on the host for continuous monitoring, while the dissolvable agent is a run-once executable.



APPLIANCES

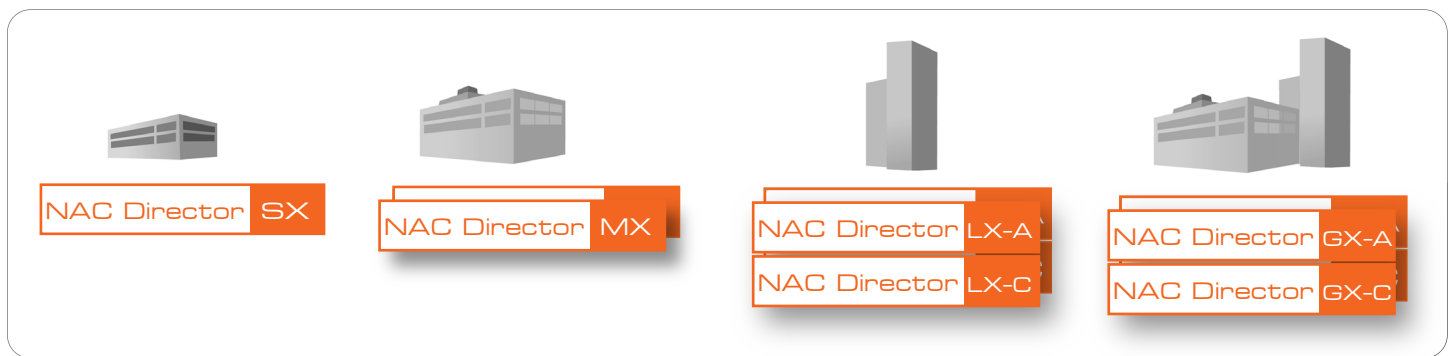
NAC Director offers comprehensive NAC services – identity management, endpoint compliance, and usage policy enforcement – across the entire product family. These services can be deployed in phases moving from passive monitoring to active enforcement in settings as small as a branch office or as large as a multi-national enterprise's global network. NAC Director's high performance architecture and enterprise-wide scalability deliver effective access control in any enterprise environment with complete implementation flexibility.

The NAC Director family includes the SX, MX, LX and GX platforms, allowing solutions to be tailored based on the number of concurrent users, the number of network devices, authentication methods used, and access policy complexity. NAC Director SX and MX are each a single stand-alone appliance. NAC Director LX and GX support higher capacities by splitting functionality between two paired appliances – an Application Server and a Control Server – allowing for increased performance and load sharing of NAC functions. NAC Director LX appliance pairs are available in both standard configurations and redundant configurations with RAID 10 and hot-swappable dual power supplies. NAC Director GX pairs include RAID 10 and hot-swappable dual power supplies as part of the standard offering for appliance-level redundancy. NAC Director MX, LX, and GX platforms also support optional high-availability, hot-failover configurations for environments requiring the highest levels of system uptime.

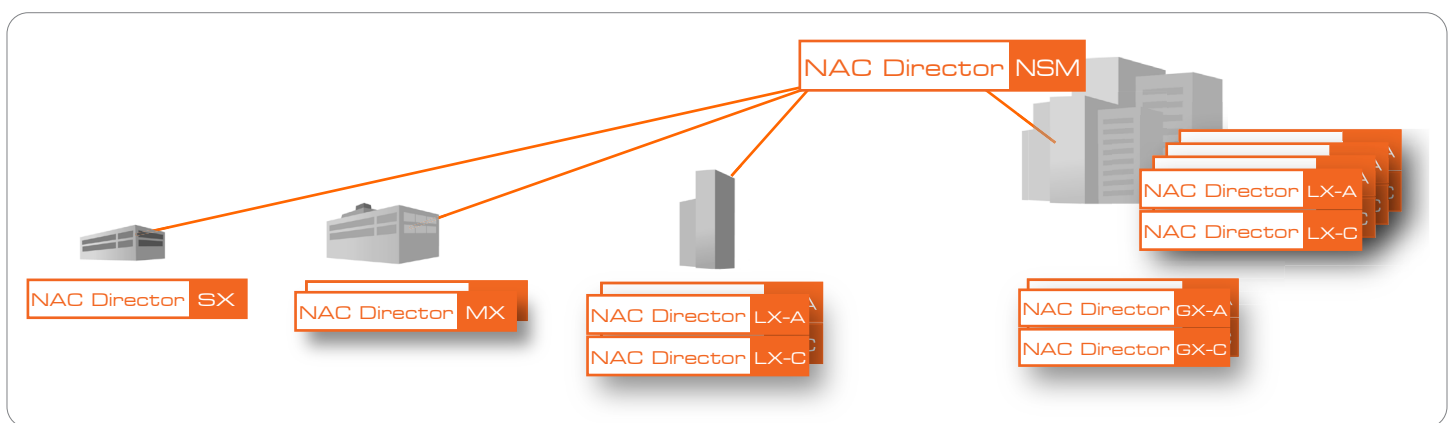
Platform	Type	Target Environment	Concurrent Users
NAC Director SX, SXR	Standalone Appliance	Small/Branch Office Environments	Up to 100
NAC Director MX, MXR	Standalone Appliance	Medium/Regional Office Environments	Up to 1,000
NAC Director LX: LX-A and LX-C, LX-AR and LX-CR	Standard Appliance Pair: Network Control Server / Network Application Server	Large/Headquarters Office Environments	Up to 6,000
NAC Director GX: GX-AR and GX-CR	High-Performance Appliance Pair: Network Control Server / Network Application Server	Large/Headquarters Office Environments	Up to 12,000
NAC Director NSM, NSMR	Management Appliance	Multi-site Environments with multiple Network Sentry clusters	Greater than 12,000

Note: Redundant versions are designated with "R" added to the platform name, and include RAID 10 and hot-swappable dual power supplies.

NAC Director's flexible hardware architecture allows enterprises to start with a single NAC Director SX appliance and then expand to higher capacities with the MX, LX, or GX as needed via incremental software upgrades, rather than wholesale hardware replacement. This cost-effective approach ensures that initial capital investments in NAC Director can easily scale to support larger environments.



Larger enterprises can deploy any combination of NAC Director appliances required to meet the needs of their particular environment, with centralized management and control provided by NAC Director Network Security Manager (NSM).



Host Vulnerability Assessment Using Nessus Engine

NAC Director appliances seamlessly integrate Nessus vulnerability scans of host devices to assist with endpoint assessments. With native support for a Nessus client, NAC Director enables Nessus scans for completely agent-less assessment of host vulnerabilities. NAC Director can also combine Nessus scans with Bradford's agent technology to enable both network-based and agent-based assessment for detailed vulnerability and compliance checking.

AGENT TECHNOLOGY

Bradford Networks' NAC Director solution offers both dissolvable and persistent agents for comprehensive host assessment.

Dissolvable Agent: Available for Windows, Mac OS X* and Linux operating systems, the dissolvable agent is a run-once executable that is integrated into the registration and authorization process. The dissolvable agent can be customized to run based on a user's role, the network access method (e.g. wired or wireless LAN, VPN, etc.), as well as on a regularly scheduled interval.

Persistent Agent: Available for Windows and Mac OS X operating systems, the persistent agent is installed on the host and provides additional functionality including non-intrusive user and device authentication and posture assessment.

Comprehensive assessment capabilities of dissolvable and persistent agents:

- | | |
|--|---|
| <ul style="list-style-type: none"> • Operating System Type, Patch Levels and Hotfixes
Identify OS type (Windows, Mac OS X, Linux), along with patch or service pack (e.g. SP2) and/or hotfixes • Anti-virus Applications, Engine and Definitions Version
Identify AV applications status and ensure current definitions • Anti-spyware Applications, Engine and Definitions Version
Identify AS application status and ensure current definitions • Required and Prohibited Applications
Identify all applications, whether required or prohibited | <ul style="list-style-type: none"> • Active Processes
Identify actively running processes • File Presence and Status
Identify specific filenames and present status • Wireless drivers*
Identify wireless driver being used (important as some drivers are known to have existing security vulnerabilities) • Patch Management Integration
Integrate with patch servers such as BigFix to verify endpoint posture and automatically remediate non-compliant devices |
|--|---|

Additional capabilities of the persistent agents include:

Continuous Windows Monitoring*

As a lightweight application installed on the host device, the Windows persistent agent can provide continuous monitoring of files, applications, and processes. Whereas pre-connect assessment provides a single "snapshot" view of host compliance, the ability for continuous post-connect monitoring enables greater control over host activity throughout the network session.

Messaging and Emergency Notification

The persistent agent can also be used as a means for communicating directly with users on the network, providing an effective method for quickly reaching the user community with important information or alerts. Messages configured and sent from a centralized management interface will instantaneously launch a customizable pop-up message box on the end user's computer screen.

* Available in next major release.

SYSTEM FEATURES AND BENEFITS

Feature	Description	Benefits	
IDENTITY MANAGEMENT	Device registration	Each device is forced to register prior to accessing the live network	Maintains a comprehensive view of devices connected to the network at all times
	Standards-based authentication	Support for standards such as 802.1X, LDAP, RADIUS based authentication	Leverages existing infrastructure and widely deployed authentication technologies
	7-point identity profile	Identity profile with user name; user role; device name; MAC address; IP address; network access point; time	Enables precise identity definitions for granular policy assignment
	"Get Out/Stay Out" control	Quickly locate and disable any user or device starting with a suspect IP address	Removes suspicious users immediately and prevents them from reconnecting until vetted
	Dynamic VLAN assignment	Assign appropriate VLAN based on user, device, location, time-of-day, etc.	Ensures users' access to appropriate resources based on pre-defined business rules
	Comprehensive role assignment	Assign all users to distinct groups with specific policies	Enforces policies by group, versus individual user, streamlining policy enforcement process
	Port-level role assignment	User roles can be mapped to individual network access ports	Provides high degree of granularity in assigning role-based policies
ENDPOINT COMPLIANCE	Persistent and dissolvable agents	Lightweight client software to assess endpoint device posture	Enables assessment of campus-owned endpoints and visitor/guest devices
	Continuous endpoint posture analysis	Pre- and post-admission endpoint analysis	Ensures endpoints remain compliant with policy throughout their network session
	Self-remediation	Guide users with non-compliant devices to download new software updates/patches	Empowers users to update their own systems, reducing the need for helpdesk intervention
	NESSUS scanning	Network-based device vulnerability scanner	Allows agent-less assessment of endpoints for known security vulnerabilities
	Windows agent monitoring*	Monitoring of file status, processes, registry keys	Provides enhanced assessment of Windows endpoints for additional policy controls
	Patch integration*	Integration with patch management systems such as BigFix	Drives operational efficiencies for staff and users through patch automation
	Wireless driver checks*	Checks Windows wireless drivers against known list of suspect drivers	Reduces wireless network vulnerabilities and potential performance problems
USAGE POLICY ENFORCEMENT	Broad range of acceptable use policies	Ability to define any number of acceptable use policies	Quickly implement company-specific security policies
	Four simultaneous user and device isolation methods	802.1X, MAC-based RADIUS authentication, DHCP and VLAN steering	Enables consistent user and device isolation capabilities for multi-vendor environments
	Alarm and trap triggers	Taking automatic policy-based action upon alarm receipt	Automates manual processes to stop unauthorized activity at network access point
	Integration with deep packet inspection solutions	Action mechanism for violations triggered by deep packet inspection solutions like IDS, IPS, etc.	Enforces policy at the edge to block unwanted activities at the point of access to the network
	Phased policy activation	Allows roll-out by port, device or location	Enables phased, logical deployment of the solution to minimize business disruptions
MANAGEMENT OPERATIONS	Intuitive management interface	Powerful web-based system management homepage	Drives operational efficiencies; enables quick troubleshooting capabilities
	Consistent user experience	Common registration, authentication, and remediation functions across wired, wireless and VPN connections	Increases user satisfaction; reduces support burden
	Remote registration	Allows users to register and verify endpoint devices before arriving on-site	Saves time for users and administrators; reduces load on network and IT staff during peak periods
	Standard reports	Set of standard, out-of-the-box report formats	Allows on-demand reporting for standard network performance metrics
	Customizable reports	Sort data by deleted parameters, including time-of-day, user, location, etc.	Allows administrators to generate custom reports on-demand
	Standard SQL logs	Standard database infrastructure for data import/export	Enables enhanced reporting for regulatory compliance, trend analysis, and other uses

* Available in next major release.

TECHNICAL SPECIFICATIONS

Standard Appliances

	ND-SX	ND-MX	ND-LX-A / ND-LX-C	ND-NSM
SYSTEM	CPU	CORE 2 DUO E8400 3.0 GHZ		
Memory	4 GB DDR II SDRAM (4 x 1 GB)		ND-LX-A 4 GB DDR II SDRAM (4 x 1 GB) ND-LX-C 4 GB DDR II SDRAM (4 x 1 GB)	8 GB DDR II SDRAM (4 x 2 GB)
Memory bus clock	1333-MHz FSB			
Hard disk	1x 160-GB Enterprise SATA drive			
Network Interface	3 x 10/100/1000 Ethernet, Auto-negotiation, RJ-45		3 x 10/100/1000 Ethernet, Auto-negotiation, RJ-45 2 x 10/100/1000 Ethernet, Auto-negotiation, RJ-45	2 x 10/100/1000 Ethernet, Auto-negotiation, RJ-45
Console Access	1x Fast UART 16550 serial port			
Form factor	Rack-mountable 1 RU			
Dimensions	16.8"Wx1.7"Hx22.6"D 426mmx43mmx574mm			
Weight	26.5lbs (12.0kg)			
Power supply	300 W AC Power Supply, auto switching 100-240VAC, 50-60Hz, 10A (115V) to 5 A (230V) maximum, 1120 BTUs/hr (for rated output power of 300W)			
Cooling	3 x 3-pin counter-rotating cooling fans, front/back airflow			
Panel Display	Power, Hard drive activity, 2x Network activity, System Overheat			
ENVIRONMENT	Temperature Operating	10 to 35°C (50° to 95° F)		
Temperature Non-Operating	-40 to 70°C (-40° to 158° F)			
Relative Humidity Operating	8-90% non-condensing			
Relative Humidity Non-Operating	5-95% non-condensing			
CERTIFICATION	Emissions	FCC Part 15, Subpart B, Class A, Canada ICES-003 (2004), Class A, Japan VCCI Class A, EN55022(1998)/CISPR 22(1997) Class A, EN55024 (1998), EN61000-3-2(2000) and EN61000-3-3(1995)+A1(2001)		
Safety	UL 60950-1 1st Edition, 2006-07-07, CSA 22.2 No. 60950-1-03 1st Edition, 2003-11, IEC 60950-1:2001 1st Edition, EN 60950-1:2001 1st Edition			

TECHNICAL SPECIFICATIONS

Redundant Appliances

	ND-SXR ND-MXR	ND-LX-AR	ND-LX-CR ND-NSMR
SYSTEM	CPU	Dual-Core Intel® Xeon 3000 2.66 GHz	
	Memory	4 GB DDR II SDRAM (4 x 1 GB)	8 GB DDR II SDRAM (4 x 2 GB)
	Memory bus clock	1066-MHz FSB	
	Hard disk	4 x 160-GB Enterprise SATA drives, RAID 10	
	Network Interface	3 x 10/100/1000 Ethernet, Auto-negotiation, RJ-45	2 x 10/100/1000 Ethernet, Auto-negotiation, RJ-45
	Media	CD/DVD-ROM	
	Console Access	1x Fast UART 16550 serial port	
	Form factor	Rack-mountable 1 RU	
	Dimensions	17.2"Wx1.7"Hx25.6"D 437mm x 43mm x 650mm	
	Weight	40 lbs (18.1 kg)	
	Power supply	Two (2) 450W redundant, hot swappable AC power supplies, 1+1 redundancy w/ PFC, 100-240VAC, 50-60Hz, 8A (115V) to 4A (230V) maximum, 2192 BTUs/hr (for rated output power of 450W)	
	Cooling	Three (3) 40mm heavy-duty counter-rotating fans, front/back airflow	
	Panel Display	Power, Hard drive activity, 2x Network activity, System Overheat	
ENVIRONMENT	Temperature Operating	10 to 35°C (50° to 95° F)	
	Temperature Non-Operating	-40 to 70°C (-40° to 158° F)	
	Relative Humidity Operating	8-90% non-condensing	
	Relative Humidity Non-Operating	5-95% non-condensing	
CERTIFICATION	Emissions	FCC Part 15, Subpart B, Class A, Canada ICES-003 (2004), Class A, Japan VCCI Class A, EN55022(1998)/CISPR 22(1997) Class A, EN55024 (1998), EN61000-3-2(2000) and EN61000-3-3(1995)+A1(2001)	
	Safety	UL 60950-1 1st Edition, 2006-07-07, CSA 22.2 No. 60950-1-03 1st Edition, 2003-11, IEC 60950-1:2001 1st Edition, EN 60950-1:2001 1st Edition	

Note: ND-SXR, ND-MXR, ND-LX-AR, ND-LX-CR and ND-NSMR appliances require software release 3.1.9 or higher

TECHNICAL SPECIFICATIONS

High-Performance Appliances

	ND-GX-AR	ND-GX-CR
SYSTEM	CPU	2 x Dual-Core Xeon 5150 2.66 GHz
	Memory	8 GB DDR II SDRAM (4 x 2 GB))
	Memory bus clock	1333-MHz FSB
		4 x 160-GB Enterprise SATA drives. RAID 10
	Hard disk	2 x 10/100/1000 Ethernet, Auto-negotiation, RJ-45
	Media	CD/DVD-ROM
	Console Access	1x Fast UART 16550 serial port
	Form factor	Rack-mountable 1 RU
	Dimensions	17.2"Wx1.7"Hx25.6"D 437mm x 43mm x 650mm
	Weight	41 lbs (18.6 kg)
	Power supply	Two (2) 650W redundant, hot swappable AC power supplies, 1+1 redundancy w/ PFC, 100-240VAC, 50-60Hz, 10A (115V) to 5 A (230V) maximum 3186 BTUs/hr (for rated output power of 650W)
	Cooling	Four (4) 40mm heavy-duty counter-rotating fans, front/back airflow
	Panel Display	Power, Hard drive activity, 2x Network activity, System Overheat
ENVIRONMENT	Temperature Operating	10 to 35°C (50° to 95° F)
	Temperature Non-Operating	-40 to 70°C (-40° to 158° F)
	Relative Humidity Operating	8-90% non-condensing
	Relative Humidity Non-Operating	5-95% non-condensing
CERTIFICATION	Emissions	FCC Part 15, Subpart B, Class A, Canada ICES-003 (2004), Class A, Japan VCCI Class A, EN55022(1998)/CISPR 22(1997) Class A, EN55024 (1998), EN61000-3-2(2000) and EN61000-3-3(1995)+A1(2001)
	Safety	UL 60950-1 1st Edition, 2006-07-07, CSA 22.2 No. 60950-1-03 1st Edition, 2003-11, IEC 60950-1:2001 1st Edition, EN 60950-1:2001 1st Edition

Note: ND-GX-AR and ND-GX-CR appliances require software release 3.1.9 or higher

ABOUT BRADFORD NETWORKS

Bradford Networks develops advanced network access control solutions for wireless, wired and VPN networks. Bradford's out-of-band appliances leverage existing network infrastructures and investments to deliver automated identity management, endpoint compliance and usage policy enforcement services. Bradford helps IT managers address the challenges of guest access, unmanaged devices and regulatory compliance.