



SECURE GUEST ACCESS

Simplifies administration of guest access while ensuring network security by enforcing appropriate access policies for guests, partners, contractors, and other authorized external users.



Guests, business partners, and contractors need flexible network access in order to interact with various groups within an organization. Access privileges must be aligned with each user's role in supporting the business, and must follow the user regardless of location or access method, including wired and wireless LAN connections.

Bradford Secure Guest Access, a solution set built on Bradford's Network Sentry™ platform, lets organizations extend appropriate access privileges to authorized visiting users, while enforcing strict policy controls to maintain security. Enterprises can empower non-technical staff as authorized sponsors to set up network access for non-employee users.

Secure Guest Access automates the provisioning of guest access accounts, which frees IT staff from daily administrative burdens. IT retains control and gains network-wide visibility with logging and reporting to satisfy regulatory compliance requirements.

Role-based Access

Automates user authentication, device registration, and assessment for guest users on wired and wireless networks, and enforces role-based access policies.

Sponsorship

Allows authorized internal sponsors, including non-technical staff outside of IT, to set up user accounts without the need to engage IT staff.

Self-Service

Easy-to-use web portal allows visiting users to self-register for guest access, while capturing all necessary user data specified by IT.

Standalone Authentication Option

Authentication for guest accounts can be performed locally on the Bradford platform or via integration with existing directory services such as Active Directory or LDAP.

E-mail and SMS Integration

Login credentials such as username and password for guest users can be printed or sent via e-mail or SMS text messages.

Conference Setup

Groups of guest access accounts with unique usernames and passwords can be created dynamically for meetings and conferences, saving time and resources.

Endpoint Compliance Validation

Security posture of endpoint devices can be assessed via persistent or dissolvable software agents.

Device Tracking and "Rogue" Detection

All known devices authorized to be on the network can be registered and tracked, allowing any "rogue" (unknown) devices to be easily detected.

Detailed Historical Reporting

Guest access data is continuously logged and available for building reports to satisfy internal and external regulations.

CHALLENGE

Network access for external users (non-employees) with unmanaged endpoint devices.

Guests

Suppliers, customers, and others need basic Internet access while on-site for meetings.

Conference Attendees

Attendees of meetings and conferences require Internet access during specific hours.

Partners

Business partners need greater access to network resources on a recurring basis.

Contractors

Contractors are often an extension of regular staff and require access to internal systems for extended periods of time.

SOLUTION

Dynamic identification of authorized external users and unmanaged devices, with the ability to validate device security posture and enable role-based network access.

BENEFITS

Greater productivity for visiting users, internal sponsors, the IT department, and the organization as a whole.

Visiting Users

- Quick network access
- Simple interface for logging in

Internal Sponsors

- Quick and easy user account setup
- No need to engage IT

IT Department

- Security and control
- Visibility and tracking
- Automation of routine tasks

The Organization

- Increased user satisfaction
- Enhanced security



HOW IT WORKS

When visiting users require access to the network, designated internal sponsors (e.g., receptionists, event coordinators, or department managers) can quickly create temporary network access accounts via an easy-to-use web interface. Sponsors select account types for visiting users based on profiles that are pre-defined by the IT group.

Each account profile is associated with a different type of user (e.g., Guest, Contractor, or Conference Attendee) and defines appropriate network access rights. When a sponsor creates a new account for a visitor, Bradford's Network Sentry platform generates a unique username and password that can be emailed to the user in advance of their visit, or printed when they arrive.

When a guest user attempts to connect to the network, the edge switch or wireless access point alerts Network Sentry which then presents the user with a captive portal web page for logging in. After the user enters a valid username and password, a quick scan of their device is performed to check for up-to-date operating system patches, anti-virus and anti-spyware software, or other system checks defined by IT.

If the scan is successful, Network Sentry instructs the switch or wireless access point to allow network access—typically by assigning the user to an appropriate VLAN, such as a Guest VLAN. If a problem is found when scanning the device—such as anti-virus software that is out-of-date or not turned on—a Remediation VLAN is used to limit or prevent network access. Network Sentry can also provide users with easy instructions for updating their systems so they can get normal network access.

If a rogue user attempts to log in without a valid username and password, Network Sentry prevents network access by telling the switch or wireless access point to assign a Quarantine VLAN or to disable the user's physical connection. An alert can also be sent to let IT know that an unauthorized user has attempted to access the network.



INTEGRATES EASILY WITH EXISTING NETWORKS

Secure Guest Access utilizes Network Sentry's unique out-of-band architecture that leverages the network infrastructure—including switches, wireless access points and controllers—to enforce security policies at the network edge. Network Sentry integrates with network equipment from all major manufacturers, with no network upgrades or major configuration changes required.

A NETWORK SENTRY™ FAMILY SOLUTION SET

Secure Guest Access is built upon the Bradford Network Sentry family, an Adaptive Network Security platform that greatly enhances security and automates IT operations. The Network Sentry family consists of the Foundation, an intelligent base platform, along with software-based Solutions and Extensions which can be deployed in combination to meet the needs of any environment. The Secure Guest Access solution set consists of the following combination of hardware and software components from the Network Sentry family:

Foundation	Intelligent base platform, deployed either on hardware appliances or as a virtual server application
Guest Manager	Software solution for securing network access for guests and simplifying administration
Device Tracker	Software solution providing management and monitoring of all known endpoint devices
Endpoint Compliance	Software extension enabling validation of security posture of endpoint devices



Address 162 Pembroke Road, Concord, New Hampshire 03301, USA
 Toll Free +1 866.990.3799
 Phone +1 603.228.5300
 Fax +1 603.228.6420
 Email info@bradfordnetworks.com

Bradford Networks offers the best network security solutions for evolving IT environments. The company's flexible Network Sentry platform is the first network security offering that can automatically identify and profile all devices and all users on a network, providing complete visibility and control. Unlike vendor-specific network security products, Network Sentry provides a view across all brands of equipment and devices so nothing falls through the cracks. Hundreds of customers and millions of users worldwide rely on Bradford to secure their IP networks. Visit www.bradfordnetworks.com

Copyright © 2009 Bradford Networks. All rights reserved. Printed in USA. Bradford Networks and the logo are registered trademarks of Bradford Networks in the United States and/or other countries. Adaptive Network Security, Network Sentry, Campus Manager and NAC Director are either trademarks or registered trademarks of Bradford Networks or one of its affiliated companies in the United States and/or other countries. All other trademarks or registered trademarks are the property of their respective owners. Bradford Networks reserves the right to change, without notice.