

*Intelligent switching, with its ability to control users and applications, and IPAM, with its focus on controlling the IP address space, provide the perfect complement to each other for securing non-user devices.*

## APPLICATION SOLUTION BRIEF: **INFOBLOX INTEGRATION**

# How IPAM and ConSentry Intelligent Switching work together

*A perfect storm is brewing within enterprise networks, with IT organizations struggling to protect resources on the LAN, support a changing workforce, roll out new applications such as wireless and VoIP, troubleshoot issues quickly, and meet the demands of compliance and auditing. To get a handle on this broad range of demands, IT needs more intelligence in the LAN to identify and control users and applications.*

But addressing the user issues solves only half the problem – a host of non-user, non-PC devices populate LANs today, and they and their ports must also be identified and controlled. Network cameras, printers, environmental sensors, badge readers, robotic devices, medical equipment – the number and types continue to grow, and they operate across the spectrum of industries. Their operation is critical to the enterprise, but they present unique challenges. Unlike devices that authenticate, such as PCs, thereby announcing their presence and relaying their identity, these non-user devices are quiet and can remain undetected. And they themselves, as well as the network ports they're attached to, can create vulnerabilities within the enterprise.

To date, efforts to bring them under IT's control have relied on only manual processes, such as whitelisting their MAC addresses to give them "authenticated" access onto the LAN. In many organizations, though, a more automated option already exists. An IP Address

Management (IPAM) system likely holds the information needed to identify these devices automatically. Integrating that IPAM system with intelligent switching can provide IT with the means for securing and controlling both user and non-user devices across the entire network.

### **SHOULD I FEAR MY BADGE READER?**

An obvious first question is "Why should I fear my network-attached badge reader enough to need to control it?" The answer is, for three reasons:

1. To protect the device
2. To protect the network against someone who pretends to be the device
3. To prevent someone from co-opting the device and using it to launch an attack

A badge reader, though critical, is a very simple device from a networking perspective. It's not meant to withstand any amount of tampering, so simply being

<b>Authentication</b>	Allow only valid users onto the network
<b>Role Derivation</b>	Query identity store for group/role info
<b>Host Assessment</b>	Check endpoint posture
<b>User Behavior Analysis</b>	Decode every flow, tied to user and app
<b>Policy Enforcement</b>	Apply access policy to each flow
<b>Audit Trail</b>	Track each flow by username, app, file, server

**Functions of an Intelligent Switch**

in the flow of a virus outbreak could render the device inoperable – and leave a lot of people standing out in the parking lot.

Identifying the device as a badge reader, and ensuring that only the badge reader-server can talk to it using the badge-reader protocol, protects it from harm. The same goes for the robots on the manufacturing floor, the CT scan machines in the hospital, the voice over IP phones, the printers, and all the other non-user devices.

In addition, these static network devices can provide mischievous users with an easy entry point onto the network. They could “clone” the device, copying its MAC address and IP address in a bid to get network access. Or they could let the device retain its identity and load malware onto it in a bid to launch an attack, run an open-port scan, or attempt to retrieve data from other network devices.

In any of these cases, identifying these devices and applying role-based controls to limit the devices they could communicate with and the protocols involved provides a vital layer of security in today’s IP-based, interconnected systems.

**WHAT IS IPAM?**

IP Address Management (IPAM) provides the ability to effectively manage, control, monitor, and assign the IP address space within an enterprise. Effective IP address management requires two key services that provide the naming and delivery of IP addresses – DNS and DHCP. An IPAM system, then, combines DNS and DHCP services, along with a backend database that archives the description, location, and other parameters associated with a device. IPAM replaces the static spreadsheet that IT used to rely on for tracking IP addresses. Often outdated and error-ridden, these manual spreadsheets are ripe for quickly losing control of the IP space. To meet enterprises’ scalability and

high-availability requirements, IPAM is most effectively delivered in a purpose-built appliance.

**HOW DO IPAM AND INTELLIGENT SWITCHING WORK TOGETHER?**

Intelligent switching, with its ability to control users and applications, and IPAM, with its focus on controlling the IP address space, provide the perfect complement to each other for securing non-user devices. Since intelligent switches seek to control every device on the LAN, non-user devices typically force significant manual efforts to incorporate them into those LAN control processes. Under these manual systems, every printer, camera, badge-reader, VoIP phone, robot, or medical device needs to be identified and have its MAC and IP address entered into the policy and control systems of the intelligent switches.

When intelligent switching and IPAM systems are integrated, the switch, whenever it identifies a non-user device, can simply query the IPAM database to learn the device’s name. IT can create policies that rely on a portion of the device name to identify the device type and associate it with the appropriate role. Given that the role limits which systems the device can talk to and which protocols it can use, IT gains an automated way to protect these vital non-user devices from being the victim of or launch point for an attack.

**CONSENTRY NETWORKS AND INFOBLOX – WORKING TOGETHER**

The best-of-breed example of intelligent switching / IPAM integration is ConSentry Networks and Infoblox.

ConSentry Networks is the leader in intelligent switching, delivering user and application control in its LANShield family of controllers and access switches. The ConSentry devices sit in the data path, performing deep packet inspection on every flow and applying policy to enable role-based control. ConSentry enforces policy on a combination of user, device, destination, and Layer 7 application information. The ConSentry devices are self-contained, applying controls directly on each flow, so they have no dependencies on VLANs, ACLs, or other network segmentation constructs. This self-contained architecture enables the ConSentry devices to be deployed with no changes to existing infrastructure, clients, or identity stores.

Infoblox is an industry-recognized leader in IPAM, DNS, and DHCP servers. The company’s appliance, running a hardened operating system, allows these critical network functions to be scaled, distributed, and highly

available. The Infoblox NIOS software integrates DNS and DHCP with built-in IPAM, offering an integrated IP management console and a single database for serving and reporting on DNS and DHCP data. The system provides address history tracking, dynamic address control, device classification, and IP address status viewing and threshold alerting. It also offers DNS Hostname templates and reports, DHCP network templates, and global search capabilities. The appliance and hardened OS provides IT with the peace of mind of assured data integrity, with no data loss, corruption, or latency.

Together, the two companies combine the benefits of Infoblox's excellent accounting of non-user devices with ConSentry's ability to deliver role-based control. Leveraging the naming conventions already in the Infoblox systems, IT can create policies on the ConSentry solution that use those names and automatically place non-user devices into the appropriate roles. This integration automates a previously manual process, saving extensive staff time on the initial deployment and every time non-user devices are added to the network. With ConSentry and Infoblox, IT can much more easily extend the critical network and data protection that intelligent switching provides to every user and every device within the enterprise.

#### ABOUT CONSENTRY NETWORKS

The ConSentry Networks Intelligent Switching architecture delivers native user and application control at the LAN access edge. With this technology, ConSentry's award-winning LANShield product family enables IT managers to improve the visibility, control, and performance of users and applications and radically simplify LAN deployment and operations. ConSentry is backed by blue-chip venture capital firms Accel Partners, DAG Ventures, INVESCO Private Capital, and Sequoia Capital and is headquartered in Milpitas, California.

##### Corporate Headquarters

ConSentry Networks  
1690 McCandless Drive  
Milpitas CA 95035  
**Phone** 408.956.2100  
**Fax** 408.956.2199  
**Toll-Free** 866.841.9100  
Email [info@consentry.com](mailto:info@consentry.com)  
[www.consentry.com](http://www.consentry.com)

##### Worldwide Locations

London, United Kingdom  
**Phone** +44 (0) 00870 351 9494  
  
Frankfurt, Germany  
**Phone** +49 69677 33 4  
  
Tokyo, Japan  
**Phone** +813 5532 7630

For a complete listing of all our office locations go to:  
[www.consentry.com/company.html](http://www.consentry.com/company.html)