

**DELIVER**  
High Availability & Secure Infrastructure

**REDUCE**  
Administrative Overhead and Costs

**EASY**  
Integration with Single User Interface



## Education Quotes

“The Infoblox solution met the University’s requirements of built-in reliability and features that allow delegated management with data-entry templates for the various departments. And, Infoblox made the process of implementing our student authentication portal seamless.”

Mike Levoir,  
University of Minnesota

“Our DNS and DHCP system has gone from academic probation to the Dean’s List in a matter of a semester. We have not experienced one outage. The updates and patching that used to take two days worth of man power can be done in minutes.”

Bradley Thomas,  
University of Wyoming

The blacklisting functionality in the Infoblox DNS solution is a powerful value-added tool that can help customers, such as educational institutions and libraries, achieve compliance requirements that mandate blocking access to specific sites and content. Blacklisting functionality exists within the Infoblox Network Infrastructure Automation and Control suite of products, and is one more tool that can be used to create customized solutions to individual customer problems.

At no added cost, blacklisting affords organizations one more way to protect their networks by not answering the DNS query from the client to sites that are on the prohibited or questionable list. In conjunction with Infoblox Grid™ technology, blacklisting can assign different prohibited domains to subgroups, such as varied access restrictions for high schools, middle schools, elementary schools, and administration, all within the same school district.

Because the blacklisting functionality allows Infoblox customers to deny access to all sites on any list of imported domains, blacklisting can also serve the enterprise that wants to control access internally, as well as monitor usage within the company or quarantine groups of users. Blacklisting can also serve to carve access niches for specific divisions within a corporation, at both headquarters and branch locations alike.

## Benefits of Blacklisting for Educational Institutions and Libraries:

- Enables CIPA Compliance for Users of the E-Rate Program
- Lets Users Manage, Monitor, and Update with a Single User Interface
- Decreases Reliance on In-line Filters and Can Reduce that Expense
- Is Provided at No Additional Cost
- Allows Customized Access for Different Subgroups of Users
- Includes Auditing Capability to Monitor Individual User Activity

## Blacklisting Enables CIPA Compliance for E-Rate Users

Those educational institutions and libraries that receive discounts for Internet access or internal connections through the E-rate program must comply with the Children's Internet Protection Act (CIPA) of 2001. CIPA is a federal law enacted by Congress and implemented by the FCC to address concerns about the availability of offensive materials on school and library computers. Compliance requires blocking sites or filtering pictures that are obscene, contain child pornography, or are harmful to minors. The Infoblox blacklisting functionality can help affected organizations achieve compliance.

The process is simple to effect with Infoblox assistance. The educational institution or library obtains the list of prohibited domains, and imports the list into Infoblox products. The list can be managed, monitored, and updated with a single user interface. The list can be augmented with additional domains as desired, and using Infoblox Grid technology, the blacklisting can be applied differently across various sets of users. For example, one set of prohibitions can be assigned to elementary school users, while a different prohibited list can be applied to middle school users, and still other lists to high schools in the district. Administrative offices can have yet another set of blacklisted sites, or none at all.

## Blacklisting Can Be a Cost-Saver and an Adjunct to School District Consolidation

Many security-oriented solutions to meeting CIPA compliance make use of in-line filtering, and these solutions usually charge by the seat. Infoblox blacklisting instead blocks the DNS request, and so the query never reaches the filter, thereby decreasing the impact on the URL filter and improving performance, and potentially eliminating the need and the cost of the in-line filter. The blacklisting functionality in Infoblox solutions is not an additional cost, but rather is included as part of NIOS, the embedded processor.

As school districts across the country pursue cost-cutting measures, including school district consolidation, the blacklisting functionality can serve as an extra tool in segregating the various members within the Grid. Besides providing differing access to different subgroups, blacklisting can also be used to segment the administrative entities within the various schools so that school records are secure and not available from one school to another without permission. All school traffic can be centrally located and funneled through that location to the service provider, thereby reducing connectivity costs.

## Blacklisting Gives Enterprises Customized Control over Access

Blacklisting can serve multiple purposes in the enterprise world, as well. Positioning the blacklisting functionality within the enterprise's recursive server, where the employees enter the network, allows a company to segregate groups in a variety of ways. From a central location, a company can monitor employee activity on the network, control employee usage by blocking access to various sites, and even quarantine groups of users as needed. Additionally, in an Infoblox solution all the information of blacklist activity is logged. This feature affords the enterprise the ability to perform forensics to determine who has accessed — or tried to access — any specific site.



+1.408.625.4200

1.866.463.6256 (toll-free, U.S. & Canada)

[info@infoblox.com](mailto:info@infoblox.com)

[www.infoblox.com](http://www.infoblox.com)

## Infoblox Product Warranty and Services

The standard hardware warranty is for a period of one year. The system software has a 90-day warranty that will meet published specifications. Optional service products are also available that extend the hardware and software warranty. These products are recommended to ensure the appliance is kept updated with the latest software enhancements and to ensure the security and availability of the system. Professional services and training courses are also available from Infoblox. Information in this document is subject to change without notice. Infoblox Inc. assumes no responsibility for errors that appear in this document