

An Introduction to the Access Manager for Apache

A tool of the NuSphere Security Console

By Paul DuBois, NuSphere Corporation

TABLE OF CONTENTS

How Does the Access
Manager Work

Features and
Functionality

How to Get Started

NuSphere Security
Console

NuSphere Security Scan

About NuSphere

NuSphere's Access Manager for Apache is an easy to use tool designed to help web site administrators implement access control policies for sensitive information with a minimum of effort. It is included with every NuSphere Advantage product and a tool of the NuSphere Security Console.

As you create content for your web site, some parts of the site may be completely public. But other parts may contain private, proprietary, or confidential information that needs to be restricted, with varying levels of control. For example, a business organization's web site may require access control at the following levels:

- Public information available for anyone who visits the site to view and use. A business might make product catalog information available on an unrestricted basis, as well as other general-purpose resources such as public contact information, or feedback and customer help desk applications.
- Information available to any staff member within the organization. This could include the calendar of upcoming company events, or an internal staff directory or newsletter—items that are not intended for public dissemination, but that any employee should be able to access.

- Information available only to specific groups, such as employees in particular departments. Staff in the shipping and warehouse departments may need access only to inventory applications, sales staff need access to sales recording and reporting applications, and the tech support group must be able to use the product support knowledge base. Other users might need to be members of several groups (for example, it's likely that business office staff would need to use both the inventory and sales applications).
- Information that is restricted to particular users. The CEO's appointment calendar may be private, with access allowed only to the CEO and to the secretary who updates the calendar.

Access Manager for Apache makes it easy to institute these kinds of access policies by allowing you to establish password-protected access to the restricted areas of your web site. You can define users and groups, and then associate them with specific directories, files, or applications within your web tree.

How the Access Manager for Apache Works

Access Manager uses a MySQL database named `ns_auth` and the primary Apache configuration file, `httpd.conf`. As you interact with Access Manager to define users and groups, it stores information about them in the `ns_auth` database. As you define which areas of your site are restricted and who may access them, Access Manager edits Apache's `httpd.conf` file on your behalf to add the appropriate configuration directives.

Access Manager sets up authentication information but does not monitor web requests. Monitoring is handled by an Apache module that takes over once you set up access controls. Requests for pages in protected areas of your site pass through this module, which authenticates users to prevent unauthorized access. The module is preconfigured into the version of Apache that ships with NuSphere Advantage products.

Apache supports a variety of authentication methods. These methods take the form of modules that are loaded into Apache and are used to control access to your site by monitoring requests for protected pages. However, many of these methods suffer the drawback that they are set up through hand editing of configuration files. The Access Manager for Apache solves this problem. It is a straightforward web-based application that provides a simple interface for authentication information management. Access Manager can be used easily from any browser by filling in forms to define web site users and groups, and to specify which areas of your site they can access.

Some Apache authentication methods store user information in plain text files, but this is extremely inefficient for lookups for all but a small number of users. Other methods improve on this by using indexed storage such as DBM files, which is more efficient but still limited to use with a single web server. A more flexible alternative is to store authentication information in a relational database such as MySQL. This is the approach used by NuSphere's Access Manager for Apache because it provides good performance and can be used with multiple web servers. Web site user credentials are stored in a MySQL database for quick access to information for an essentially unlimited number of users. And because MySQL is network-based, you can deploy many web servers throughout your enterprise, yet manage and control access to them through a single centralized database. With an easy-to-use interface, Access Manager combines ease of use for setting up your access policies with a high performance engine that enforces those policies.

Access Manager for Apache makes it convenient to establish access control throughout designated areas of your web site but it does not secure the connection between client users and the web server. The password protection method is based on HTTP Basic Authentication, which sends passwords in the clear. Should you need to secure the connection between client users and the web server (for example, if you allow access to protected areas to clients located outside the perimeter of your corporate Intranet), you may wish to consider further controlling access to your site. One way to do this is by establishing a secure connection for use during the authentication dialog and subsequent requests for protected pages.

Features and Functionality

Access Manager for Apache is easy to use, but its simplicity may be deceptive. As you get started with Access Manager, you'll begin to appreciate what it can do for you. Some things to consider:

- Access Manager is installed in your web tree, so it can be used to control access to itself. You do not need to set up a secondary mechanism to prevent unauthorized use of the Access Manager for Apache tool.
- Access Manager users and groups have names of your own choosing. They do not correspond to names for computer login accounts or to MySQL database account names, and thus cannot be used to mount attacks for gaining direct login access to your machines or a connection to your database server.
- The user information table in the `ns_auth` database allows you to define user names, and assign standard types of information such as name and phone number. It also provides several other general-purpose fields and gives you control over both the names and content of these fields. If you like, you can store additional information in them that may help you manage each user or group. For example, you may want to assign a *user ID* or an account expiration date to each user.
- Because user authentication information is stored in a MySQL database, you can write other utilities that work with the same information that the Access Manager for Apache uses. The `ns_auth` database is not special so you can query it from other applications, just like any database. This means you can write applications that use it for purposes other than access control. You could, for example, write a script that deletes users whose expiration date has passed.
- One of the problems with manually configuring access control directives in `httpd.conf` is that even if you're comfortable editing the file, it becomes more difficult to make sense of what you've done as the number of protected areas on your site increases. Access

Manager avoids this problem by presenting information in tabular format that is easy to read and understand.

- Access Manager for Apache can administer systems remotely. Because Access Manager is web-based, you are not required to use it from the machine where Apache is running. You can manage access control for multiple web servers right from where you are, simply by using just your browser. (Note: You do need access to the server host to restart Apache so that your changes will take effect.)
- It is not necessary to run the back end MySQL database on the web server machine. By default, Access Manager uses the `ns_auth` database on the web server host, but you can tell it to use a database located elsewhere. This benefits organizations that run multiple web servers but want to control access to all of them through a shared, centralized source of information. So, you can designate one machine as the `ns_auth` database host, then tell each of the web servers you wish to protect to use that host to check requests for protected pages. This allows you to implement and enforce a consistent access policy across an entire organization.
- You can tailor the error messages that are displayed when authentication failure occurs on a per-area basis. For example, a company news site area intended for use by staff of many different levels of sophistication, the message could be informative in nature, indicating the area's purpose, explaining why access was denied, and providing information about who to contact for assistance. For a more tightly controlled area that people are expected to know how to access prior to visiting, the message might be more concise—designed, in fact, to provide as little information as possible.
- Access Manager writes an audit trail of its activities to the `ns_auth` database to help you track who has done what. This can be helpful especially in an environment where there are multiple administrative Access Manager users.
- It is possible to write applications that allow users to move freely between protected areas that they have access and unprotected areas, without having to re-authenticate on

each entry to a protected area. The Access Manager for Apache documentation provides examples that show how to do this.

How to Get Started

Access Manager for Apache is included with all NuSphere Advantage products, and is a tool of the NuSphere Security Console. It comes preconfigured with an `ns_auth` database set up and is ready to use. After you install your NuSphere product, make sure your web and database servers are running, then point your browser to the following URL:

```
http://localhost:9000/
```

This URL takes you to the home page of the NuSphere Administrative web site that is accessible through port 9000 of your web server. Select the **Administration** button along the left edge of the page, and then select **Access Manager for Apache** from the list of tools in the next page. You can also access it through the NuSphere Security Console by selecting **Security Console** from your applications list.

When you use Access Manager for the first time, you should do three things:

1. Set up the initial Access Manager configuration controlling the administrative user name and password and other related parameters. These can be entered into the startup page that Access Manager presents when you invoke it initially.
2. The `ns_auth` database is initialized with an administrative user and a regular user. These initially have passwords that are documented in the User's Guide, so they are public and you should change them immediately.
3. Protect Access Manager itself. You can do this either by restricting access to the application, or by setting up protection over the entire NuSphere Administration site.

The preceding information is just an overview. Complete instructions can be found in the *NuSphere Advantage User's Guide* that is also included with the NuSphere Advantage distribu-

tion. From the NuSphere Administrative site, select the **Documentation** button and scroll or click to, "Using Access Manager for Apache."

NuSphere Security Console

The NuSphere Security Console focuses on securing your internal Internet environment through intrusion prevention. Several new security tools join the Access Manager for Apache to help you manage all of your security activities from one spot. They include:

Vulnerability Scan: This tool looks at the file system level of the Apache and MySQL database servers, and NuSphere applications, to determine where there are vulnerable spots. For instance, MySQL's default state for administrator access is "no password." The scan will surface that as a security risk and provide a "fix" to resolve the problem. This application has a plug-in architecture to enable you to write additional tests of your own.

Port Scan: When you install an operating system, many services are established which may not be necessary for your particular environment. For instance, you may have no need for FTP, yet it will be automatically assigned to a port. Every assigned port is a vulnerable spot within your Internet environment. This utility lets you see at a glance which ports are active so you can decide which can (or should) be shut down. While the Port Scan does not currently run on Windows, it can be run "against" a Windows server.

Weak Password Check: This utility identifies passwords that are deemed "weak," such as those that match a username, are a username with a number appended, or use any word found in the dictionary. All of these (and more) are considered easily hacked and need to be changed. You run the utility against the password file and it returns a list of usernames whose passwords may pose a security threat to your operating environment.

Since NuSphere Advantage components are inside your firewall, the NuSphere Security Console is designed to focus on internal intrusion prevention. But there are clearly more threats to your Internet environment that come from outside your firewall. For this, NuSphere offers the NuSphere Security Scan.

NuSphere Security Scan

Combined with the NuSphere Security Console, NuSphere has got your security needs covered *inside and out!* NuSphere Security Scan is an online vulnerability assessment service that evaluates the security of networks remotely. The service provides comprehensive, on-demand security audits that identify, analyze, and report on network security threats. By focusing on networks from a *hacker's* perspective, NuSphere is able to identify real-world weaknesses that elude traditional security solutions.

The NuSphere Security Scan (offered through a partnership with Qualys) sniffs all the external ports on a single IP address. It looks at what ports are open for what services. It checks vulnerabilities on routers, switchers, hubs, firewalls, web servers, mail exchangers, and more. It then provides its findings, and potential corrective actions, as a browser-based report at a secure site. The NuSphere Security Scan is only available to NuSphere Advantage customers. Learn more about the NuSphere Security Scan by visiting:

www.nusphere.com/products/ns_security_scan.htm. *Note: Qualys Map is not included with the NuSphere Security Scan.*

About NuSphere Corporation

NuSphere delivers the first Internet Application Platform (IAP) based on open source components, providing an integrated foundation that allows companies to deploy reliable, cost-effective, enterprise-class applications across Windows, UNIX and Linux environments. NuSphere® Advantage is an integrated software suite that pairs the reliability and cost-effectiveness of PHP, Apache, Perl and open source databases with new technology for building business-critical web applications and web services. Based in Bedford, Mass., the company's commercial software services include technical support, consulting and training. For more information, visit www.nusphere.com or call +1-781-280-4600.

NuSphere is a registered trademark in Australia, Norway, Hong Kong, Switzerland, and the European Community; NuSphere and PHPEd are trademarks of NuSphere Corporation in the U.S. and other countries. Any other trademarks or service marks contained herein are the property of their respective owners.

MySQL AB distributes the MySQL database pursuant to the applicable GNU General Public License that is available as of the date of this publication at <http://www.fsf.org/licenses/gpl.txt> and all of the terms and disclaimers contained therein. NuSphere Corporation is not affiliated with MySQL AB. The products and services of NuSphere Corporation are not sponsored or endorsed by MySQL AB.