Executive Summary

As the leader in Wide Area Application Delivery, Blue Coat products accelerate and secure applications within your WAN and across the Internet. Blue Coat provides a robust and flexible solution that controls users and network resources, protects against Web-based threats, and accelerates the broadest range of WAN-based applications. Whether deployed on either end of a WAN, at Internet access points, or in front of business-critical services, Blue Coat ProxySG appliances provide control points that stop the bad and accelerate the good. Playing an important role in Blue Coat authentication and authorization is the ability to implement User Management, providing administrators with the ability to effectively manage users on the network.

What is User Management?

User Management is an authentication feature that provides administrators with the ability to identify and control the state of users logged into the network. This includes, but is not limited to, the ability to query and filter users that are currently logged into the network, manually log out users, and control user login counts and login times.

Why should I implement User Management?

Most security-conscious enterprises today implement some form of authentication and authorization for accessing network resources. The benefits to this approach are clear – user permissions can be verified before granting access to resources, and user activity can be monitored through various logging mechanisms. This solution is not without its limitations however. In typical authentication and authorization deployments, administrators have various options available with regard to how users are authenticated, but have little control over how often users are authenticated. User Management enables administrators to more granularly control the frequency of user authentication, allowing them to configure the ProxySG to ignore cached browser credentials and force the user to re-enter credentials, or to require more frequent authentication only if the user is accessing critical resources. This kind of flexibility allows administrators to implement authentication-based policies that more closely match their network security policies.

The User Management logout capability also provides more secure control over the state of users. For example, when using IP authentication mode users are identified by the specified IP address until the IP surrogate time expires. If another person were to use that computer before the IP surrogate time expired, they would be treated as the original user. The common solution for preventing this scenario is to decrease the IP surrogate expiry time, causing the user to be challenged more often. User Management allows administrators to instead configure user log out based on inactivity timeouts, user access to a specific “logout” URL, or by manually logging out the user. For ease of use, logout capability is available though policy, the CLI, or the Management Console.

Another key benefit of User Management is visibility into active user sessions. Using the Management Console and CLI, administrators can view all active users and filter display data by user, IP address, or realm for easier viewing. This can be useful for identifying the general login status of users or for making real-time decisions such as immediately logging off a user.

How does User Management work?

User Management is based on the concept of users logging in and logging out of the ProxySG appliance. A login is the combination of a unique IP address with a unique username in a unique realm. A user is considered logged in when first authenticated to the ProxySG appliance. Identifying users as logged in, or active, allows administrators to create flexible User Management policies to fine tune user access and control.
The majority of User Management is done in policy using either the Visual Policy Manager (VPM) or Content Policy Language (CPL). Using policy, administrators can create rules that more granularly control the timeout values associated with configured realms, such as the surrogate refresh, credential refresh, and authorization refresh, and they can perform specific actions on users such as logging them out based on predefined criteria. For extreme cases where more immediate action is necessary, such as disconnecting a user being terminated, User Management functions such as logging off a user can be performed via the CLI or the Management Console.

### Typical Use Cases

- Log out users after a period of inactivity.
- Provide a logout URL for users to manually log out.
- Limit the number of IP addresses associated with a single username.
- Limit the number of logins associated with a single IP address.
- Force a re-authentication to gain access to a particular network resource.
- Limit the login session time allowed in a particular timeframe.

### Example 1

An administrator concerned about users who access several workstations throughout the day would like to implement a solution that provides better user management of the user’s network activity. To accomplish this, the administrator implements policy that prevents any user from logging into more than one workstation at a time. With form or cookie-based authentication implemented, the behavior that results is that when any user already logged into one workstation attempts to obtain authentication and authorization on another workstation, they are automatically logged off of the original workstation. (For other authentication modes the user would be denied logging on to a new workstation until manually logging off of the original workstation)

---

**One user accessing network resource from multiple workstations**

1. JSMITH opens a browser on Workstation A and requests a network resource.
2. JSMITH is challenged for authentication credentials.
3. JSMITH provides authentication credentials.
4. The ProxySG associates 192.168.15.14 with JSMITH.
5. JSMITH opens a browser on Workstation B and requests a network resource.
6. JSMITH is challenged for authentication credentials.
7. JSMITH provides authentication credentials.
9. The ProxySG associates 192.168.15.18 with JSMITH.
10. JSMITH is provided with requested content.
Example 2
A network administrator concerned about shared workstations located in various network labs would like to implement a solution that will help address the growing problem of users not logging off before leaving workstations. To address this problem the administrator decides to implement two User Management features – restricting the number of logins associated with a particular IP address and imposing an inactivity timeout. To restrict the number of logins associated with a particular IP address to only one, the administrator creates policy that implements a cookie-based authentication mode and allows one login per IP address at most. This prompts any user opening up a browser on the workstation for credentials and logs off any users previously logged on to that same workstation. To impose an inactivity timeout, the administrator sets a 10-minute inactivity timeout for the authentication and authorization realm that the users belong to. Using the inactivity timeout, even if a user leaves a browser window open but is inactive for a set period of time, the next user to perform a request using that browser will be prompted for credentials. The previous user will have already been logged out automatically after the inactivity timeout.

Multiple users accessing network resource from the same workstation
1. JSMITH opens a browser and requests a network resource.
2. JSMITH is challenged for authentication credentials.
3. JSMITH provides authentication credentials.
4. JSMITH is provided with requested content.
<10 minutes elapse>
3a. The ProxySG associates 192.168.15.2 with JSMITH.
4a. The ProxySG logs off JSMITH.
5. LJOHNSON walks up to the open browser window on the workstation and requests a network resource.
6. LJOHNSON is challenged for authentication credentials.
7. LJOHNSON provides authentication credentials.
7a. The ProxySG associates 192.168.15.2 with LJOHNSON.
8. LJOHNSON is provided with requested content.

Blue Coat Difference

Flexible User Authentication
Used in conjunction with the Guest Authentication and Permit Authentication Error features, the User Management feature provides a flexible way for administrators to not only track and control users, but also handle user scenarios that may require a unique solution. As any administrator knows, network access is not always black and white. The ability to handle the shades of grey with which administrators are sometimes presented can therefore be critical to ensuring that network activities continue “business as usual” and are consistent with corporate policy.

Visibility
User Management ensures that a major requirement for network administrators — visibility — is met. Administrators can easily determine who is logged in at any time via the Active Users Console and also view other pertinent information such as the associations between users and IP addresses.

User-Based Policy
The ability to identify users on the network not only provides visibility into user behavior, but also enables administrators to control users with user-based policies. By creating user-based policies, administrators can not only dictate how, when, and where users make requests, but also apply other policy features to users such as imposing bandwidth management restrictions.