Blue Coat® Systems

# User Management

*Identify and Control the State of Users Logged In to the Network*

Blue Coat®

BLUE COAT SYSTEMS, INC. AND BLUE COAT SYSTEMS INTERNATIONAL SARL (COLLECTIVELY "BLUE COAT") DISCLAIM ALL WARRANTIES, CONDITIONS OR OTHER TERMS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, ON SOFTWARE AND DOCUMENTATION FURNISHED HEREUNDER INCLUDING WITHOUT LIMITATION THE WARRANTIES OF DESIGN, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL BLUE COAT, ITS SUPPLIERS OR ITS LICENSORS BE LIABLE FOR ANY DAMAGES, WHETHER ARISING IN TORT, CONTRACT OR ANY OTHER LEGAL THEORY EVEN IF BLUE COAT SYSTEMS, INC. HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Americas:

**Blue Coat Systems, Inc.**
420 N. Mary Ave.
Sunnyvale, CA 94085

Rest of the World:

**Blue Coat Systems International SARL**
3a Route des Arsenaux
1700 Fribourg, Switzerland

## Document History

| Date | Version | Note |
|---|---|---|
| January 15, 2013 | v1.0 | Initial release |

# Contents

# List of Figures

# Introduction

## 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 in to the network. This includes, but is not limited to, the ability to query and filter users who are currently logged in to 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 control the frequency of user authentication with more granularity. Administrators can configure the ProxySG appliance to ignore cached browser credentials and force the user to re-enter credentials, or 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, he or she 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 logout 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 with more granularity that control the timeout values associated with configured realms, such as the surrogate refresh, credential refresh, and authorization refresh Administrators can also perform specific actions on users, such as logging them out based on predefined criteria. For extreme cases in which more immediate action is necessary, such as disconnecting a user that is being terminated, User Management functions, such as logging off a user, can be performed using the CLI or the Management Console.

## Scenario 1: Single User - Multiple Workstations

An administrator, who is 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 in to more than one workstation at a time.

With form or cookie-based authentication implemented, when any user who is already logged in to one workstation attempts to obtain authentication and authorization on another workstation, he/she is automatically logged off the original workstation. (For other authentication modes, the user would be denied login to a new workstation until he/she is manually logged off the original workstation.)

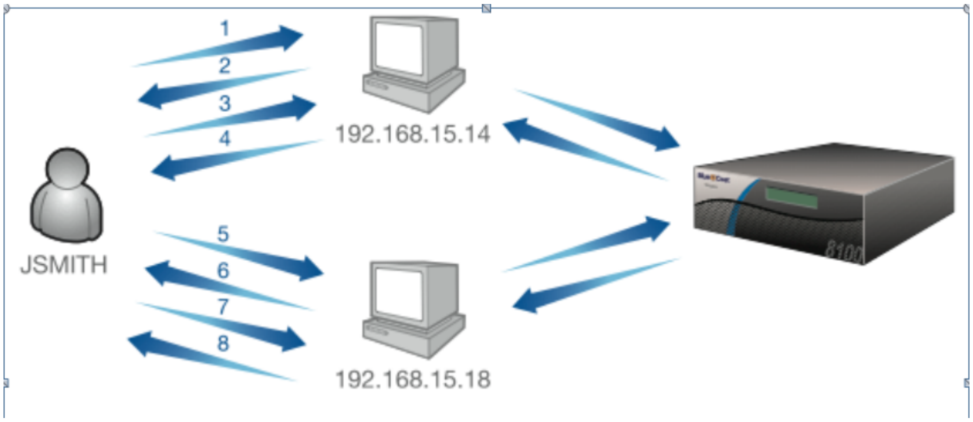


Figure 1–1 Single user accessing a network resource from multiple workstations

In the scenario shown in Figure 1–1:

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.

   The ProxySG appliance associates 192.168.15.14 with JSMITH.

4. JSMITH is provided with requested content.
5. JSMITH opens a browser on Workstation B and requests a network resource.
6. JSMITH provides authentication credentials.
    a. The ProxySG appliance automatically logs off JSMITH at 192.168.15.14.
    b. The ProxySG appliance associates 192.168.15.18 with JSMITH.
7. JSMITH is provided with requested content.

## Requirements

SGOS 4.1.x or later.

No other requirements are needed.

## Configuration Steps

This use case limits the number of active logins per user to only one. A common scenario that would use this configuration would be to limit a particular user from logging in to multiple workstations. Successfully logging in to one workstation when an active login for that user already exists on another workstation results in the older login on the previous workstation being logged out.

The high-level configuration steps are as follows.

1. Create an authentication realm that challenges for credentials (Local, RADIUS, LDAP, etc).
2. Authenticate users.
3. Create policy to log out any existing login sessions associated with the user when a new login is successful.

    To configure this policy with more granularity, complete the following procedure.

**Procedure:**

1. From the ProxySG Management Console, select **Configuration > Policy > Visual Policy Manager** to launch VPM. (See Figure 1–2.)
2. From the **Policy** menu, select **Policy > Add Web Authentication Layer**.
3. Name the **Web Authentication Layer** (optional), then click **OK**.
4. In the **Action** column, right-click and select **Set**.

    The **Set Action Object** dialog displays.
5. Click **New**, then select **Authenticate**.

    The **Add Authenticate Object** dialog displays.
6. Name the new action (optional).
7. Select the realm used to authenticate users from the list provided.

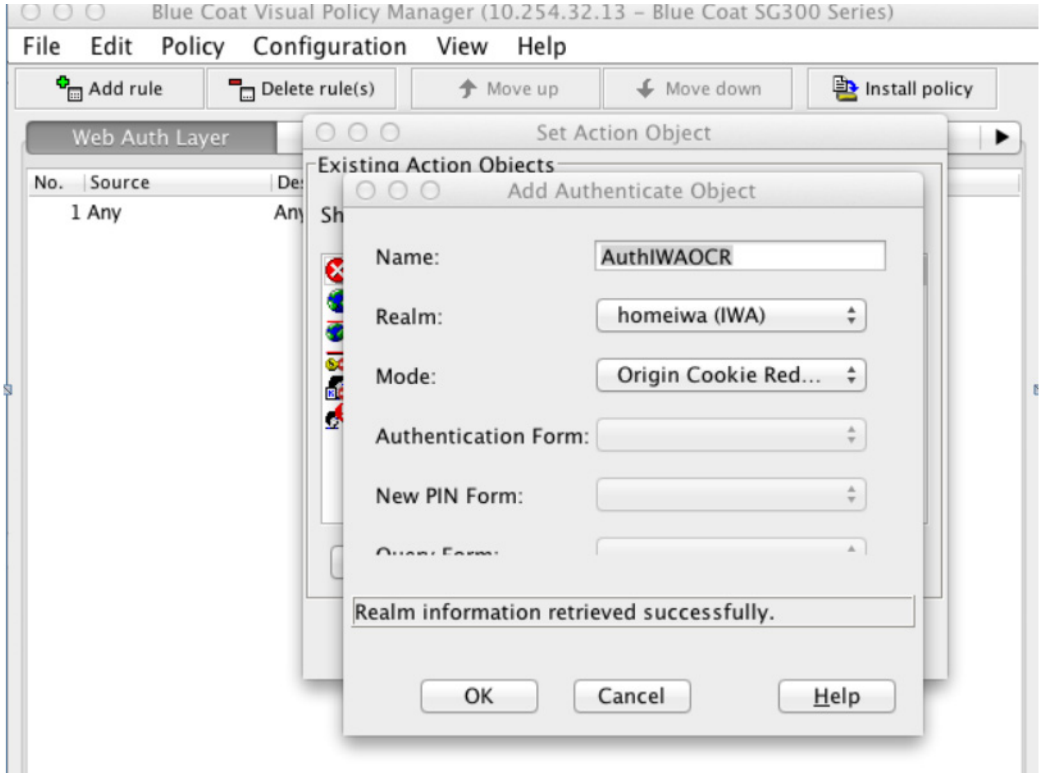
8. Choose either **Form Cookie Redirect** or **Origin Cookie Redirect** mode, depending on how you would like to challenge the user. A cookie-based surrogate is required for this use case to provide the ProxySG appliance with a mechanism for tracking the login session.

9. Click **OK**.

   The dialog closes and you return to the **Set Action Object** dialog.

10. Click **OK**.

    The dialog closes and you return to the **Web Authentication Layer** table. The new rule is listed in the table.



Name: AuthIWAOCR

Realm: homeiwa (IWA)

Mode: Origin Cookie Red...

Authentication Form:

New PIN Form:

Query Form:

Realm information retrieved successfully.

Figure 1–2 VPM - Web authentication

11. From the **Policy** menu, select **Policy > Add Web Access Layer.** (See Figure 1–3.)

12. Name the **Web Access Layer** (optional), then click **OK**.

13. In the **Source** column, right-click and select **Set**.

    The **Set Source Object** dialog displays.

14. Click **New**, then select **User Login Count**.

    The **Add User Login Count Object** dialog displays.

15. Name the new source object (optional), then enter a user login count of **2.** (This will match 2 or more logins.)

16. Click **OK**.

    The dialog closes and you return to the **Set Source Object** dialog.

17. Click **OK**.

    The dialog closes and you return to the **Web Access Layer** table.

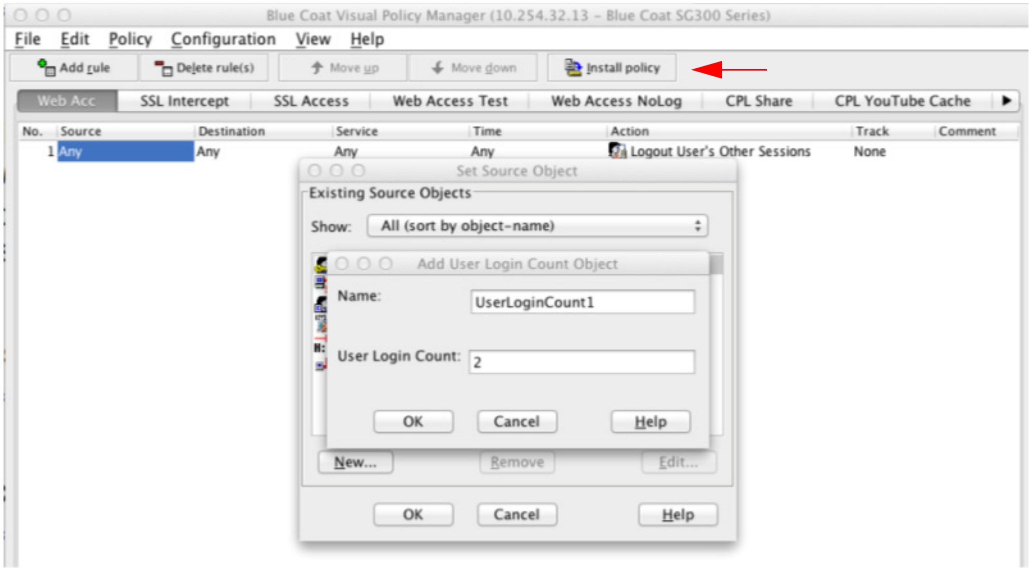
18. In the **Action** column, right-click and select **Set**.

    The **Set Action Object** dialog displays.

19. Select **Logout User's Other Sessions**, then click **OK**.

    The dialog closes and you return to the **Web Access Layer** table. The new rule is listed in the table.

20. Select **Install Policy** in the upper right corner of the VPM.



| No. | Source | Destination | Service | Time | Action | Track | Comment |
|---|---|---|---|---|---|---|---|
| 1 | Any | Any | Any | Any | Logout User's Other Sessions | None | |

Name: UserLoginCount1

User Login Count: 2

Figure 1–3 VPM - Web access

## Scenario 2: Multiple Users - Single Workstation

A network administrator, who is concerned about shared workstations that are located in various network labs, would like to implement a solution that will 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. (See Figure 1–4.)

- 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 only one login per IP address. This prompts any user opening 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 to which the users belong. 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.

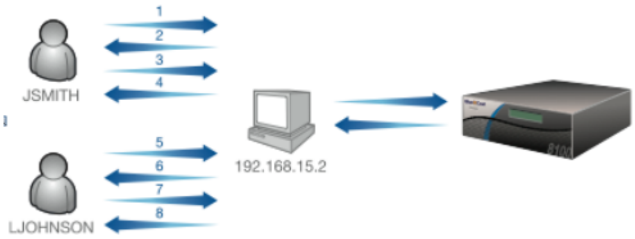


Figure 1–4 Multiple users accessing network resource from the same workstation

1. JSMITH opens a browser and requests a network resource.
2. JSMITH is challenged for authentication credentials.
3. JSMITH provides authentication credentials.
4. The ProxySG appliance associates 192.168.15.2 with JSMITH.
5. JSMITH is provided with requested content.
6. Ten minutes elapse.
7. The ProxySG appliance logs off JSMITH.
8. LJOHNSON accesses the open browser window on the workstation and requests a network resource.
9. LJOHNSON is challenged for authentication credentials.
10. LJOHNSON provides authentication credentials.
11. The ProxySG appliance associates 192.168.15.2 with LJOHNSON.
12. LJOHNSON is provided with requested content.

## Requirements

SGOS 4.1.x or later.

No other requirements are needed.

## Configuration Steps

This use case sets the inactivity timer to 10 minutes and limits the number of active logins per IP address to only one. A common scenario that would use this configuration would be to prevent multiple users from simultaneously logging in to the same workstation. A successful login on a workstation when an active login already exists on that same workstation results in the previous user being automatically logged out.

The high-level configuration steps are as follows.

1. Create an authentication realm that challenges for credentials (Local, RADIUS, LDAP, etc).
2. Authenticate users.
3. Create policy to prevent multiple users from simultaneously logging in to the same workstation.

   To configure this policy with more granularity, complete the following procedure.

**Procedure:**

1. Create an authentication realm that challenges for credentials (for example, Local, RADIUS, LDAP, etc).
2. Set the inactivity timer to 10 minutes.
   a. From the ProxySG Management Console, select **Configuration > Authentication > <*realm type*> > General**. For example, **Configuration > Authentication > IWA > General**.
   b. Change the inactivity timer to **600** seconds (10 minutes).
   c. Click **Apply**.
3. Authenticate users.
   a. From the ProxySG Management Console, select **Configuration > Policy > Visual Policy Manager** to launch VPM. (See Figure 1–5.)
   b. From the **Policy** menu, select **Policy > Add Web Authentication Layer**.
   c. Name the **Web Authentication Layer** (optional), then click **OK**.
   d. In the **Action** column, right-click and select **Set**.

      The **Set Action Object dialog box** displays.
   e. Click **New**, then select **Authenticate**.

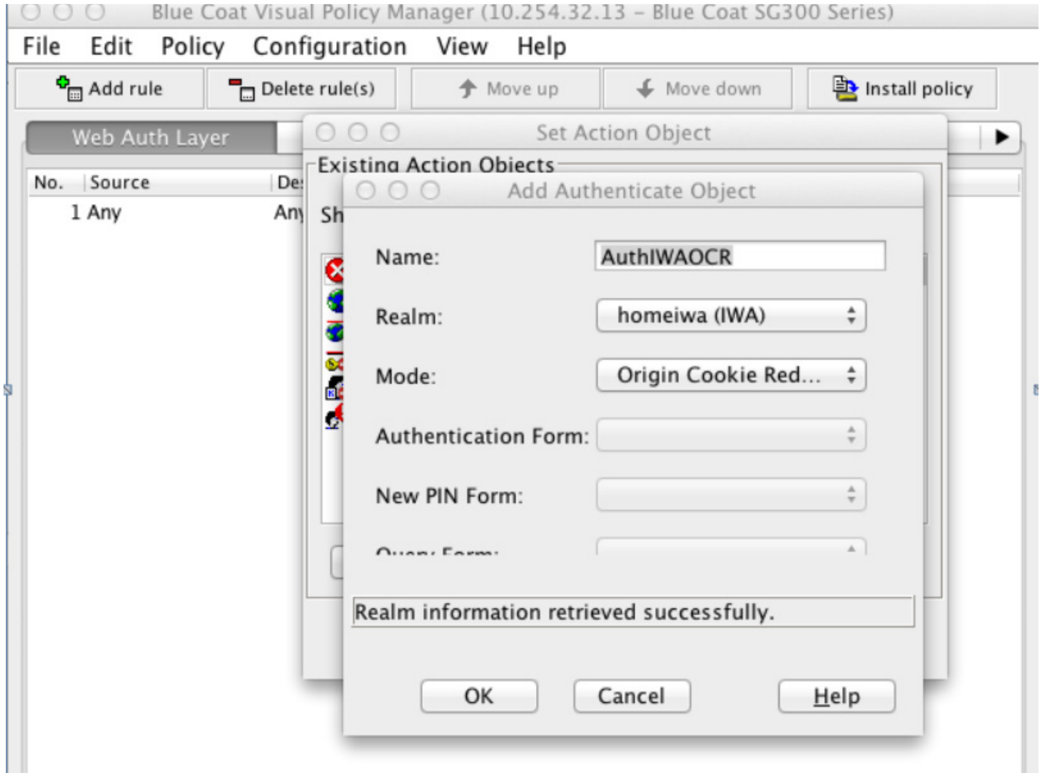
      The **Add Authenticate Object** dialog box displays.
   f. Name the action created (optional).
   g. Choose the realm used to authenticate users from the list provided.
   h. Choose either **Form Cookie Redirect** or **Origin Cookie Redirect** mode, depending on how you would like to challenge the user. A cookie-based surrogate is required for this use case to provide the ProxySG appliance with a mechanism for tracking the login session.

i. Click **OK**.

The dialog closes and you return to the **Set Action Object** dialog.

j. Click **OK**.

The dialog closes and you return to the **Web Access Layer** table.



Name: AuthIWAOCR

Realm: homeiwa (IWA)

Mode: Origin Cookie Red...

Authentication Form:

New PIN Form:

Query Form:

Realm information retrieved successfully.

Figure 1–5 VPM - Web authentication

4. Create policy to log out any existing login sessions associated with the IP address when a new login is successful. (See Figure 1–6.)

   a. From the VPM **Policy** menu, select **Policy > Add Web Access Layer**.

   b. Name the **Web Access Layer** (optional), then click **OK**.

   c. In the **Source** column, right-click and select **Set**.

   The **Set Source Object** dialog displays.

   d. Click **New**, then select **Client Address Login Count**.

   The **Add User Login Count Object** dialog displays.

   e. Name the source object you created (optional) and enter a client address count of **2**. (This will match 2 or more logins.)

   f. Click **OK**.

   The dialog closes and you return to the **Set Source Object** dialog.

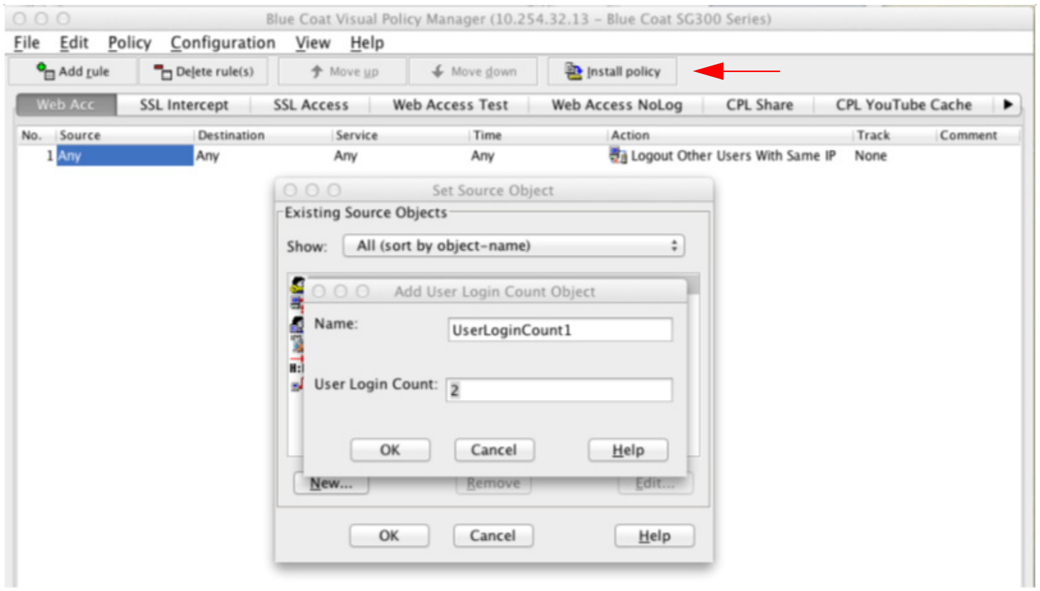
g. Click **OK**.

The dialog closes and you return to the **Web Access Layer** table.

h. In the **Action** column, right-click and select **Set**.

i. Select **Logout Other Users With Same IP**, then click **OK**.

j. Click **Install Policy** in the upper right corner of the VPM.



| No. | Source | Destination | Service | Time | Action | Track | Comment |
|---|---|---|---|---|---|---|---|
| 1 | Any | Any | Any | Any | Logout Other Users With Same IP | None | |

Show: All (sort by object-name)

Name: UserLoginCount1

User Login Count: 2

Figure 1–6 VPM - Web access

# Conclusion

## *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 in ensuring that network activities continue providing “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 using 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.

## About Technical Briefs

Technical briefs are designed to illustrate the features and capabilities of Blue Coat products. By describing generic solutions, technical briefs provide a foundation that Blue Coat customers can use to understand how Blue Coat products can be used to solve specific problems.

These technical briefs are not intended to solve customer-specific requests; if you need a customized solution to address a specific concern, contact Blue Coat Professional Services at professional-services@bluecoat.com.