



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. As part of this solution, flexible access control through authentication and authorization is a requirement. Blue Coat's Permit Authentication Error feature provides a key component to this flexibility, providing administrators with the ability to allow users access to network resources who have failed the authentication and authorization process.

What is the Permit Authentication Error feature?

Permit Authentication Error is an authentication feature that enables administrators to permit users to access network resources who have not successfully authenticated or authorized. With the Permit Authentication Error feature, users who would have been considered unauthenticated and denied can be allowed to successfully make requests for network resources.

Why should I implement the Permit Authentication Error feature?

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 network access to resources, and user activity can be monitored through various logging mechanisms. There are, however, some enterprises that find authentication and authorization desirable, but not necessarily required for users to access resources. Some administrators would like authentication and authorization to be attempted, but for user requests to be allowed if an authentication or authorization failure occurs. Without implementing the Permit Authentication Error feature, user requests that fail authentication or authorization are terminated. The Permit Authentication Error feature provides a mechanism for selectively allowing certain types of failures to be tolerated. There are numerous reasons why authentication and authorization could fail including invalid credentials and failure to connect to the external authentication server. Some administrators would like the flexibility to allow user transactions to continue in the event of an external auth server failure, but terminate user transactions that explicitly offer invalid credentials. With the Permit Authentication Error feature, implementing this type of flexible authentication policy is possible.

How does the Permit Authentication Error feature work?

The Permit Authentication Error feature works by allowing user requests that have failed authentication or authorization depending on the type of failure that occurred. Normally when a user is authenticated and authorized, only successful authentication and authorization enables the user to access network resources. With the Permit Authentication Error feature, administrators configure the specific authentication or authorization failure(s) that they would like to permit. When the user is authenticated and authorized, if any of the specified failures occur, the user is still granted network access.



The Permit Authentication Error feature is configured in policy using either the Visual Policy Manager (VPM) or Content Policy Language (CPL). To provide the level of flexibility required by today's enterprises, multiple failure types are available such as those associated with authentication errors, authorization errors, timeout errors, and licensing errors to name a few.

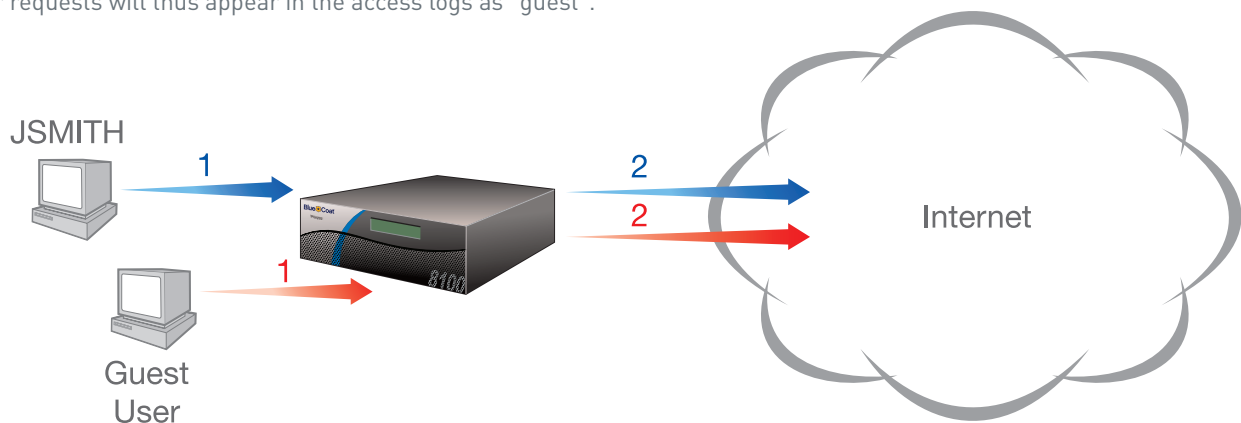
Since unauthenticated access is a security concern for most administrators, unauthenticated access can be controlled and monitored using various policy conditions available. For example, administrators can create specific policy for users who are not authenticated, perhaps only allowing them access to certain network resources instead of global access. Administrators also have the option in policy to designate users who have failed authentication as guest users, assigning them specific user attributes such as username, group, and realm.

Typical Use Cases

- > Allow users who are not logged into the single sign-on domain.
- > Allow users if an authentication server failure occurs.
- > Redirect a user to a password change page after password expiration.
- > Assign users to a default group if their authorization data cannot be obtained.

Example 1

A network administrator has successfully implemented Windows Single Sign-On (SSO) authentication (configured with client querying) on the local ProxySG appliance. The administrator would like authentication and authorization to be attempted for all users, but for those users not logged into the domain the administrator would like to go ahead and grant them access. The administrator would however like to categorize unauthenticated users as guest users for logging purposes. Unauthenticated user requests will thus appear in the access logs as "guest".



User logged into domain requesting Internet content

- 1 User **JSMITH** requests Internet content (with network credentials).
- 2 User request for Internet content is granted.

Access Log entry: 2007-08-14 19:21:45 26 10.167.45.15 **JSMITH** - - PROXIED "Search Engines/Portals" - 200 TCP_NC_MISS GET text/html;%20charset=UTF-8 http www.google.ca 80 / - - "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.0.11) Gecko/20070312 Firefox/1.5.0.11" 10.167.50.15 1787 494 -

User not logged into domain requesting Internet content

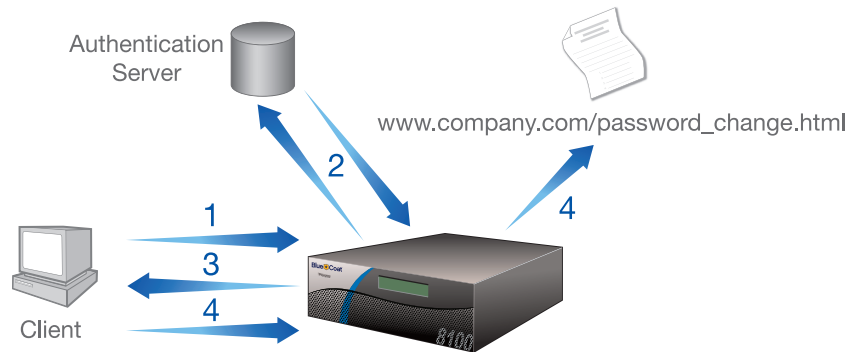
- 1 User requests network resource or Internet content (not logged into domain).
 - 1a ProxySG identifies user as a **guest user** due to lack of credentials.
- 2 User request for Internet content is granted.

Access Log Entry: 2007-08-14 19:24:01 26 10.167.45.15 **guest** - - PROXIED "Search Engines/Portals" - 200 TCP_NC_MISS GET text/html;%20charset=UTF-8 http www.google.ca 80 / - - "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.0.11) Gecko/20070312 Firefox/1.5.0.11" 10.167.50.15 1808 593 -



Example 2

A network administrator would like to use the Permit Authentication Error feature to allow authentication failures that occur due to password expiration. Instead of denying the user's request when an expired password is entered, the user will instead be redirected to the company's password change page.



Network user making a request with an expired password

- 1 User requests network resource or Internet content (with network credentials).
- 2 User is determined to have an expired password per the authentication server.
- 3 ProxySG responds with a redirect to the company password change page.
- 4 User is automatically redirected to the company password change page by the browser.

Blue Coat Difference

Flexible User Authentication and Authorization

For many security-conscious enterprises, authentication and authorization is an all-or-nothing transaction, with any error resulting in denied network access for the user. While halting productivity in the event of an authentication or authorization error may be an acceptable solution for some, waiting for an IT administrator to take action and restore service to a user may not be a realistic solution for others. With Blue Coat's Permit Authentication Error feature, administrators have the flexibility to grant users network access when encountering specific authentication and authorization errors. This allows users to remain productive while still ensuring a level of security that is consistent with corporate policies.

Visibility

When used in conjunction with Guest Authentication, the Permit Authentication Error feature allows administrators to have both flexibility and visibility. By assigning guest usernames and/or groups in policy, ProxySG access logs provide insight into user activity even if the users were unable to successfully authenticate or authorize.