Overview

The EZproxy/Blackboard Building Block allows users of EZproxy and enterprise versions of Blackboard 8.0 through 9.1 to perform seamless user authentication and authorization. Through this integration, EZproxy starting point URLs can be located inside or outside of Blackboard. When located inside of Blackboard, users are not required to re-authenticate to access resources. When located outside of Blackboard, users are required to authenticate once using the normal Blackboard login page. Existing sites that migrate to the Building Block are able to use all of their existing URLs without changing anything. In shared installations, the Building Block allows one Blackboard server to be linked to several EZproxy servers, with the ability to apply different authorization rules to each EZproxy server.

The EZproxy/Blackboard Building Block is available for no charge to licensed users of EZproxy. The link to download the Building Block is located in the installation instructions. Use the installation instructions whether you are installing the Building Block for the first time or if you are installing an updated version of the Building Block. During an update, all EZproxy server configuration information is retained automatically.

The EZproxy/Blackboard Building Block supports a flexible set of authorization mapping rules to indicate which users should have access to EZproxy resources. Review the authorization mapping rules for more information on the directives available and how to apply them.

V. 1.5 Install/Update

Required versions of Blackboard

The enterprise version of Blackboard 8.0 or later is required.

Change history

This is version 1.5 of the EZproxy/Blackboard Building block. See EZproxy/Blackboard Building Block Changes for information about changes that have appeared in different versions of this building block.

Install/update

The following instructions describe how to install or update to the current version of the EZproxy/Blackboard Building Block. The instructions for installing and updating are the same except where noted.

1. Download ezproxybbb.1.5.80.zip and save it to your computer.
2. Log in to Blackboard as a system administrator.
3. Go into the Blackboard System Admin area.
4. In Blackboard Building Blocks Management, click Manage Building Blocks.
5. If a version of the EZproxy/Blackboard Building Block is already installed and has a version number starting 2006, you have the original beta version installed. You will need to remove this version before you can install the production release. When you remove the building block, your settings will be retained and will reappear when you install the current version.
6. In Manage Building Blocks, click Install Building Block.
7. Browse to the zip file downloaded in the first step, highlight it, click OK, click Submit. Blackboard should confirm installation of the Building Block, click OK. If you are updating and Blackboard complains about a newer version being installed, you may need to remove the existing version then reinstall.
8. Now back at the Manage Building Blocks, change the status of the EZproxy Building Block to Available. Review the permissions page, click OK. Blackboard confirms the Building Block is available, click OK.
9. This building block does not have any visible presence within courses or organizations, so whether the Course/Org Default option is left in the default Unavailable or changed to Available there is no effect on this building block.
10. Next to the EZproxy Building Block, click Properties.
11. If you are installing for the first time, you will need to create an EZproxy server configuration:
   1. In Add/Modify EZproxy Server Configurations, click Add EZproxy server configuration.
   2. Fill in the fields in Add EZproxy Server Configuration as follows:
      - Auth: pick an arbitrary text string to identify the EZproxy server.
      - EZproxy server URL: enter the URL to your EZproxy server, including the port number if your server requires a port (e.g. http://ezproxy.yourlib.org:2048).
      - SHA1 shared secret: this is an arbitrary string used to digitally sign the information sent to the EZproxy server. The SHA1 secret should be kept secure. If compromised, you can change it on this page and in the user.txt configuration file to a new value.
      - Authorization Mapping: leave this blank for now, which authorizes all users who can log into Blackboard to also access EZproxy. See Authorization Mapping for information on how to build an authorization mapping
      - Click Submit. If necessary, correct errors, then submit again until the configuration is accepted. Click OK.
   12. Click Suggested user.txt configuration.
      If you are installing for the first time, review the information provided for the entries needed in user.txt to complete integration. Copy and paste the appropriate configuration information into user.txt.
      If you are updating, cross-check the suggested information with the settings on your existing EZproxy server as the settings may have changed.
      If Blackboard is set to require SSL on the log in page, you will need to change the URL in the suggested configuration that appears after CGI= from http:// to https://.
13. If your config.txt file has an AutoLoginIP entry for your current workstation, the following changes will not have any effect and you will need to test from a machine that is not within an AutoLoginIP range. With the changes complete, try accessing the login URL of your EZproxy server (e.g. http://ezproxy.yourlib.org:2048/login). If you chose full integration, you should move right through to the menu. If you chose mixed integration, you should have
the option to log in to Blackboard.

14. If necessary, return to the EZproxy Building Block properties and use Modify to change any of the settings.

15. To link Blackboard with another EZproxy server, return to the EZproxy Building Block properties and use either Add EZproxy server configuration or Copy for one of the existing configurations.

Changes

Version 1.4

Version 1.4 corrected a problem that was preventing authorization mapping group assignments from being accepted by EZproxy.

Version 1.3

Version 1.3 introduced support for Blackboard 7.2.

Version 1.2

The following changes appeared in version 1.2:

1. The suggestion configuration is now compatible with sites that use the Gateway Option Direct Entry.
2. Messages that appear on the suggested user.txt configuration page are now customized based on the version of Blackboard installed.

Version 1.1

Version 1.1 was the original production release of the EZproxy/Blackboard building block.

Versions starting with 2006

The version number for beta releases of this building block started with 2006. If you are updating from a beta version, you must first remove the beta version and then install the production version. When you remove the old version, your settings will still be retained and will reappear when you install the new version.

Authorization mapping

Lookup user

In the EZproxy/Blackboard Building Block properties, you can use "Lookup user" to verify the names and roles associated with particular users, which will help you build the authorization rules to allow and disallow access. In addition, "Lookup user" will verify whether or not the current rules allow specific users to gain access, and if you use group mappings, will allow you to test into which groups specific users will be mapped.
Working with a copy of your configuration

When you are developing a new authorization mapping, to minimize user disruption, you should use the Building Block copy feature to copy the existing EZproxy configuration to an alternate name, work on the alternative version to develop the mapping, use Lookup user on the alternative version to verify access, and then copy and paste the authorization mapping from the alternate version into the active version.

Contents of an authorization mapping

An authorization mapping is composed of a series of conditions that the Build Block should evaluate and a series of actions that the Building Block should take based on those conditions. In the absence of an authorization mapping, any user who can log into Blackboard is given access to EZproxy. Through an authorization mapping, you can fine-tune which users are able to access EZproxy, and you can also map users into groups to determine which users have access to which EZproxy resources.

Conditions

Course [-Literal] [-Role= SomeRole[,SomeRole]] CourseName

Tests to see if the user is a member of CourseName. Unless you include the optional -Literal qualifier, CourseName may include the wildcard * to match 0 or more characters and ? to match one or more characters. You can also use -Role to further specify that the user must have one or more specific roles in the course. Standard course roles include Student, Instructor, Grader, Teaching_Assistant, and Course_Builder.

If the user is in the Student role, then the Course must be available to the user for this test to be true.

DataSource [-Literal] DataSourceName

Tests to see if the user was loaded from the specified DataSourceName. Unless you include the optional -Literal qualifier, DataSourceName may include the wildcard * to match 0 or more characters and ? to match one or more characters.

NoGroups

NoGroups is true if the user has not been assigned to any groups.

Not

Not may appear in front of any condition to reverse the condition tested. For example, "Not User jdoe" would be true if the user did not have the username jdoe.

Portal -Role= SomeRole[,SomeRole]]

Tests to see if the user's is assigned one of the portal roles specified. Standard portal roles include Student, Faculty, Staff, and Alumni, along with a series of site-specific portal roles that can be found with the "Lookup user" feature.

User [-Literal] [-Role= SomeRole[,SomeRole]] UserName

Tests to see if the user's username matches Username. Unless you include the optional -Literal qualifier, UserName
may include the wildcard * to match 0 or more characters and ? to match one or more characters. You can also use -Role to further specify that the user must have one or more specific system roles. Use the "Lookup user" feature to verify the system roles available on your system.

Actions

Deny denial message

Deny the user access and send the denial message to provide feedback on why access was denied. The denial message may not contain any semi-colons. This form is best for very short messages or testing. For longer messages, see Deny -Inline.

Deny -Inline

One or more lines of
denial text; may contain semi-colons.

/Deny

Deny the user access and send the message that appears after Deny -Inline up until the line that starts /Deny to provide feedback on why access was denied.

Deny -URL= http://www.yourlib.org/denied.html

Deny the user access and redirect the user to the specified URL to provide feedback on why access was denied.

Group [+|-]GroupName[+|-]GroupName

Add or remove the user from groups. Individual groups are separated by + and -. If the first group name does not start with + or -, all existing groups are removed from the user and the first specified group is added to the user. When a group name is preceded by +, the group is added to the user's authorized groups. When a group name is preceded by -, the group name is removed from the user's authorized groups. You can specify the special GroupName NULL to remove the user from all groups.

Stop

Stop indicates that authorization mapping should stop without consideration for anything else that follows.

Examples

In this example, any username that starts with abc is allowed to EZproxy, but all others are denied access.

User abc*; Stop
Deny -Inline
Only users whose usernames start with abc are allowed to access EZproxy.
/Deny

In this example, all users are granted access to the EZproxy Default group. Users who are are enrolled in courses...
starting with Law. are included in the EZproxy Law group. Users who are enrolled in courses starting with Medical.* are included in the EZproxy Medical group. Users who are enrolled both a course that starts Law. and a course that starts with Medical. are included in the EZproxy MedicalLaw group. who are faculty in any course at all are included in the Faculty group.

<table>
<thead>
<tr>
<th>Group Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Course Law.*; Group +Law</td>
</tr>
<tr>
<td>Course Medical.*; Group +Medical</td>
</tr>
<tr>
<td>Course Law.<em>; Course Medical.</em>; Group +MedicalLaw</td>
</tr>
<tr>
<td>Course -Role=Faculty *; Group +Faculty</td>
</tr>
</tbody>
</table>

Creating/updating an authorization mapping

In older releases of Blackboard, the term System Extension appeared in places where Building Block now appears. If you are installing on an older release of Blackboard, the option to use at a given step may be named slightly differently from what is shown (e.g. for Manage Building Blocks, you might have Manage System Extensions instead).

1. Log in to Blackboard as a system administrator.
2. Go into the Blackboard System Admin area.
3. In Blackboard Building Blocks Management, click Manage Building Blocks.
4. Next to the EZproxy Building Block, click Properties.
5. If you need to create a new EZproxy Server Configuration, Add EZproxy server configuration and fill in the fields in Add EZproxy Server Configuration as follows:
   - Auth: pick an arbitrary text string to identify the EZproxy server.
   - EZproxy server URL: enter the URL to your EZproxy server, including the port number if your server requires a port (e.g. http://ezproxy.yourlib.org:2048).
   - SHA1 shared secret: this is an arbitrary string used to digitally sign the information sent to the EZproxy server. The SHA1 secret should be kept secure. If compromised, you can change it on this page and in the user.txt configuration file to a new value.
   - Authorization Mapping: leave this blank or enter the initial authorization mapping.
   - Click Submit. If necessary, correct errors, then submit again until the configuration is accepted. Click OK.
6. For an existing EZproxy configuration, click Modify to access and update the authorization mapping.
7. If you change group assignments, make certain to click the Suggested user.txt configuration to check if the AcceptGroup directive changes.
8. As you make changes to the authorization mapping, use the Lookup user feature to enter various usernames and receive feedback regarding the type of access that will be granted to the user.