AutoLoginIP

Last updated: Tue, 12 Mar 2019 19:56:25 GMT

Learn how to use the AutoLoginIP config.txt directive to identify computers that should be automatically logged into EZproxy.

AutoLoginIP (also written as A) is a position-dependent config.txt directive that interacts with ExcludeIP, IncludeIP and Group directives, database definitions, and other AutoLoginIP directives. AutoLoginIP is used to identify computers that should be automatically logged into EZproxy. It accepts a single parameter that is either an IP address or an IP address range.

AutoLoginIP and ExcludeIP are normally used to modify EZproxy's behavior for computers you manage, with ExcludeIP as the recommended and more commonly used option. AutoLoginIP is used in instances where a computer or group of computers must be proxied to be able to access a database, but where you do not need to challenge the user to authenticate first. ExcludeIP is used in instances where a computer or group of computers do not need to be proxied and the user should be redirected to the real URL, without a challenge for user authentication and without the user being proxied.

Unlike ExcludeIP and IncludeIP, AutoLoginIP is affected by Group statements. In most instances, if an AutoLoginIP statement appears multiple times in config.txt with the same IP address or IP address range, you will want to have the same Group statement appear before the AutoLoginIP statement.

CIDR Notation

Starting with EZproxy V6.3, AutoLoginIP accepts IP address ranges in CIDR notation. For example:

| AutoLoginIP 192.168.0.0/16 |

Examples

Example: transparently proxy on-site users for select databases

In this example, there is a main branch IP address range of 192.168.0.0-192.168.255.255 .

Some Database only recognizes the IP address of the EZproxy server.

In this configuration, when people access from a main branch IP address, if they access Some Database, EZproxy performs an automatic login and proxies their access, whereas if they access Other Database, EZproxy redirects them to the real URL. The redirection for Other Database occurs even if they had been automatically logged in earlier to Some Database.

When people access from a remote location, they are required to login first, and then their access is proxied.

Here is the example configuration:

| # This AutoLoginIP only affects Some Database as it is reversed |
Example: transparently proxy VPN users

In this example, there is a main branch IP address range of 192.168.0.0-192.168.255.255 which includes a series of addresses 192.168.90.0-192.168.90.255 that are assigned for VPN users. This example assumes that the VPN users only come through the VPN link to reach the local network, but do not go through the VPN for accessing other resources, such as remote library databases.

In a configuration such as this, if you are using only ExcludeIP for your local addresses, including the VPN address, then remote users who access through the VPN will be redirected to the real database URL. When their browsers access the real URL, they will be connecting directly, not through the VPN, so their access is not allowed.

In this configuration, when people access from a main branch IP address, they are not proxied but rather redirected to the real URL.

When people access through a VPN IP address, EZproxy performs an automatic login and proxies their access.

When people access from a remote location without going through the VPN, they are required to login first, and then their access is proxied.

Here is the example configuration.

# This ExcludeIP specifies that all local addresses should be excluded.
# The AutoLoginIP that follows it reverses this for the VPN users.
# This sequence of broad range exclusion first, followed by narrow range
# automatic login is crucial for this to work correctly.
ExcludeIP 192.168.0.0-192.168.255.255
AutoLoginIP 192.168.90.0-192.168.90.255

Title Some Database
URL http://www.somedb.com/
Domain somedb.com

Title Other Database
URL http://www.othertdb.com/
Domain othertdb.com
Example: transparently proxy users at a remote location for select databases

In this example, there is a main branch IP address range of 192.168.0.0-192.168.255.255 and a remote branch IP address range of 176.16.1.0-176.16.1.255.

Some Database only recognizes the main branch IP address range whereas Other Database recognizes both IP address ranges.

In this configuration, when people access from a main branch IP address, they are not proxied but rather redirected to the real URL.

When people access from the branch location, if they access Some Database, EZproxy performs an automatic login and proxies their access, whereas if they access Other Database, EZproxy redirects them to the real URL. The redirection for Other Database occurs even if they had been automatically logged in earlier to Some Database.

When people access from a remote location, they are required to login first, and then their access is proxied.

Here is the example configuration.

```plaintext
# This ExcludeIP will affect both databases since there is no other
# AutoLoginIP, ExcludeIP, or IncludeIP that reverses it.
ExcludeIP 192.168.0.0-192.168.255.255
# This AutoLoginIP only affects Some Database as it is reversed
# later by ExcludeIP.
AutoLoginIP 176.16.1.0-176.16.1.255

Title Some Database
URL http://www.somedb.com/
Domain somedb.com

# This ExcludeIP reverses the earlier AutoLoginIP so that people accessing
# Other Database from a branch location will not be proxied
ExcludeIP 176.16.1.0-176.16.1.255

Title Other Database
URL http://www.otherdb.com/
Domain otherdb.com
```

Advanced example

For an advanced example that demonstrates automatic login for all users to access one resource but restricted access for all other resources, see OPAC proxying.

For an advanced example that demonstrates automatic login for select IP address to select resources while requiring users of those machines to authenticate for other resources, see Selective AutoLoginIP.

Related directives

AutoLoginIPBanner, ExcludeIP, Group, IncludeIP, RejectIP