

Appendix F: Controlling Everweb Access

This appendix discusses how to further control access to the Everweb (GUI) functionality for Everserve. It describes how to setup and maintain additional control over user's ability to access the Everweb interface beyond the OS-level access control mechanism.

This functionality is intended for use by systems administrators who wish to restrict access to Everweb and is useful when multiple user accounts exist on the system where Everserve is installed or in Active Directory or Windows 2000 Domain environments.

Overview	2
Description of the Everweb Access Control File – ao.properties	2
<i>Basic Authorization Rules:</i>	2
<i>Values in "ao.properties"</i>	3
<i>Default Domain</i>	4
<i>Notes and special rules</i>	4
Example: Sample ao.properties file	5

Overview

Controlling access to Everweb functionality is highly desirable since unrestricted community management and publisher activities may be performed via this interface. Normally, access to Everweb is gated by OS level controls. Users with valid login credentials and permissions on the system where Everweb is installed can access Everweb and can control Everserve -- as determined by community role and/or role capabilities chosen at installation time.

Everserve offers additional functionality that allows a system administrator to further control access to Everserve community management and publisher capabilities via Everweb. Access to Everweb is restricted by using an access control list file called `ao.properties`. This functionality is beneficial where multiple user accounts exist on the system where Everserve is installed and in networking environments using Active Directory or Windows 2000 Domains where other users can access the system running Everweb.

The default installation of Everweb does not include the `ao.properties` file. If the `ao.properties` file does not exist in the correct location, then the access control functionality is not enforced. If the file `ao.properties` does exist, you must explicitly grant permission to the users you want to access Everweb.

Description of the Everweb Access Control File – `ao.properties`

The Everweb access control list `ao.properties` is a Java properties file created and maintained by systems administrators. The format for entries in the file is of the form `"name=value"`, and comments within the file are preceded with the `#` character.

This file is a simple text file that can be created in any editor. It is strongly recommended that permissions to access and read/write this file be closely controlled.

The file is not created at installation time and must be created by the administrator. This file must be placed in the Everserve "server" directory, which is typically

```
\program files\Synchron Networks\Everserver\Server
```

Basic Authorization Rules:

- The `ao.properties` file only restricts access to Everweb, the web-based administration tool in Everserve. The `ao.properties` file does not restrict access to the Everserve CLI because the CLI must be run on the server where Everserve is installed.
- If the file `ao.properties` is not found or if it contains no entries, then all login attempts using valid system accounts will be *allowed*.
- User names in `ao.properties` are case-sensitive and must match the case of the user name specified in the Local Users list or in the Active Directory Domain.
- If a user name is found in `ao.properties`, and the value is "permit", that user will be allowed to log in to Everweb.

- If a user name is found in `ao.properties`, and the value is "deny", that user will not be allowed to log in to Everweb.
- If a user name is not found in `ao.properties`, that user will not be allowed to login in to Everweb. This means that new users are automatically "denied" access until the administrator explicitly grants a "permit".
- If a user name is found, but the value is neither "permit" nor "deny", that user *will not* be allowed to log in to Everweb.
- If a user is not allowed to login, either because they are denied permission in `ao.properties` or if their username is missing from the `ao.properties` file, they will receive the same basic login error as when a login is rejected due to invalid credentials.
- The `ao.properties` is re-read each time a login occurs (the file is not cached). Consequently, the administrator can edit the `ao.properties` file at any time without having to restart Everserve.
- The `ao.properties` file acts as a pre-filter. It does not negate the need for users to have valid login permissions on the system where Everweb is running.

Values in "ao.properties"

There are five main types of entries in the `ao.properties` file:

<code>Everserve.defaultDomain = domain</code>	Attempt to authorize users by prepending <code>\\domain</code> to their username listed in the <code>ao.properties</code> file. See the next section for more information.
<code>username = permit</code>	Allow the user named <code>username</code> to access Everweb if they are permitted to by the operating system.
<code>DOMAIN\\username = permit</code>	Allow the user named <code>username</code> in the domain <code>DOMAIN</code> to access Everweb if they are permitted to by the operating system. Note that double backslashes "\\ " are used to separate the name of the domain from the username. The domain specified here overrides the default domain specified in the <code>Everserve.defaultDomain</code> entry.
<code>username = deny</code>	Deny the user named <code>username</code> from accessing Everweb. Do not query the operating system for authorization.
<code>DOMAIN\\username = deny</code>	Deny the user named <code>username</code> in the domain <code>DOMAIN</code> from accessing Everweb even if they are permitted to by the operating system. Note that double backslashes "\\ " are used to separate the name of the domain from the username. The domain specified here overrides the default domain specified in the <code>Everserve.defaultDomain</code> entry.

Default Domain

If there is an entry in the `ao.properties` file in the form:

```
Everserve.defaultDomain = domain
```

then the domain "*domain*" will be prepended to the user names in the list before checking for permissions.

For example, if the `ao.properties` file includes the lines:

```
Everserve.defaultDomain = WIDGETCORP
```

```
Fred = permit
```

then the user [\\WIDGETCORP\Fred](#) will be allowed to use the Everweb interface. This feature may be used to simplify the `ao.properties` file.

Notes and special rules

- Do not include the same login name more than once in the `ao.properties` file. The behavior of multiple entries is undefined.
- Because `ao.properties` is a Java properties file, the single backslash is an escape character. Therefore, the correct syntax for a domain name plus user name inside `ao.properties` requires a double backslash, such as "DOMAIN\\user".

Example: Sample ao.properties file

Sample Properties File

Here is a sample of what might be in a typical ao.properties file:

```
# Files was created and maintained by Mark S. Hill
# Last updated on 10/09/2002

# Declare the Everserve default domain.
Everserve.defaultDomain= WIDGETCORP

# Grant permission for user Ralph Sync in the domain WIDGETCORP
# The ActiveDirectory username is \\WIDGETCORP\rsync
# but don't specify the domain because it is the same as the default domain
rsync=permit

# Grant permission for user David in the domain WIDGETCORP
david=permit

# Deny permission for user Michael in the domain WIDGETCORP
michael=deny

# Grant permission for user Alice in a different domain WIDGETACCT
# Note the use of two backslashes separating the domain from the username
WIDGETACCT\\alice=permit

# end of file
```