Security

Security is increasingly important. As PMA.core has been deployed in increasingly complex scenarios over the years, its security features have evolved, too.

Security pertaining to root-directories is situated at two levels:

- Security features that enable root-directories to access content, such as:
  - Configure public/secret key combinations for S3 resources
  - Configure account credentials to be used when accessing a UNC network resource path
- Prevent users from access mounted content through root directories that they are or are not allowed to do
  - Define Access control lists

The following paragraphs elaborate on these respective subjects:

Accessing secured content

Public vs private

Public root directories can be accesses by anybody who is a registered user in the PMA.core user repository.

Private root directories are only accessible by those who have been explicitly given access to be allowed to access the folder through the directory's access control list.

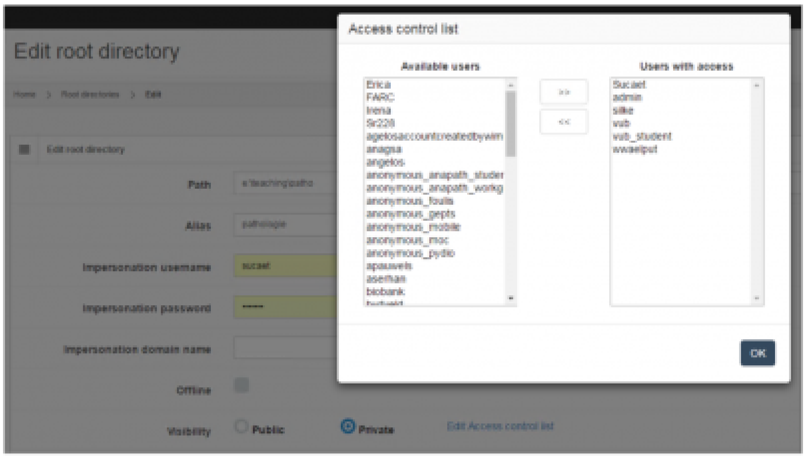
Access control lists

As you have more users and more root-directories, it becomes undesirable that everybody is allow to see everything.

Therefore, root-directories can be marked "public" or "private":

- Unordered List ItemWhen they are marked "public", it means every user has access to them.
- Unordered List ItemWhen they are marked "private", it means only select users can see the content

Once marked private, you can select what users are allowed to see the content of the root directory, and which ones aren't: Do this by pressing the "Edit access control list" link after you selected the "private" option:



From:
https://docs.pathomation.com/pma.core/2.0.1/ - **PMA.core 2.x**

Permanent link:
https://docs.pathomation.com/pma.core/2.0.1/doku.php?id=rootdir_security&rev=1644499945

Last update: **2022/02/10 16:32**