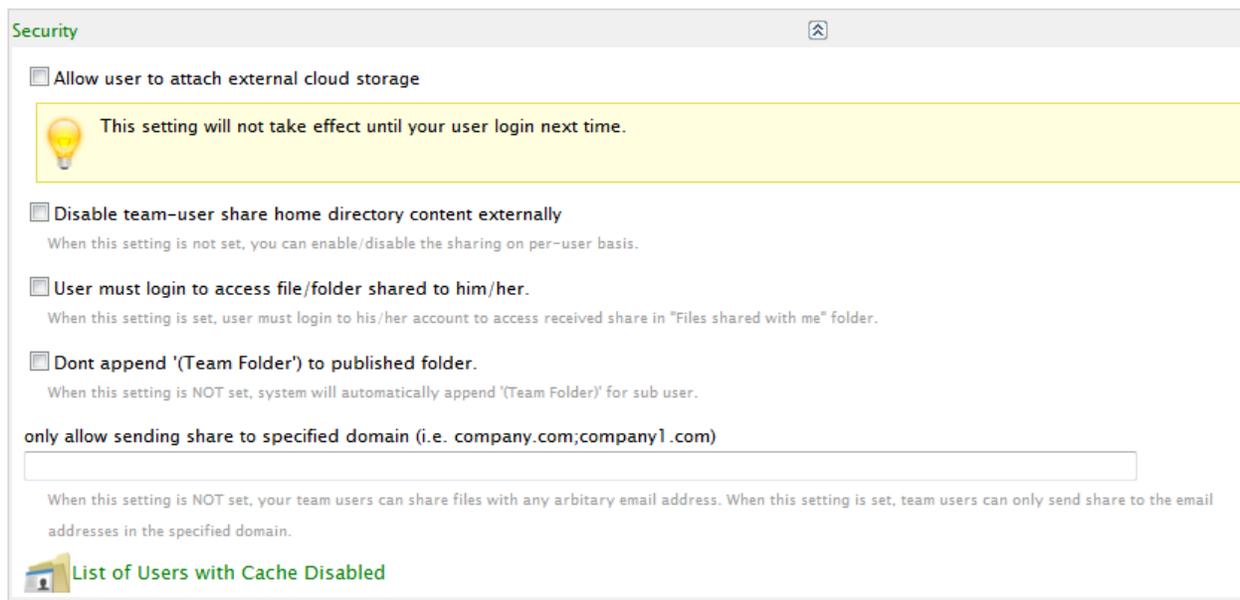Cloud Storage & Access Solutions

Group Policy in Gladinet Cloud

Group Policy is inside the Management Console on Gladinet Cloud web portal. Administrator can use group policy to define how the web portal, local client and server work in Gladinet. This article documents the group policies inside Gladinet Cloud.

Security

- o Allow user to attach external cloud storage
  When it is checked, sub users will see a link to 'Attach Cloud Storage' on web portal. They can attach their own cloud storage. Some examples are Amazon S3, OpenStack and HPCloud.

- o Disable team-user share home directory content externally
  When it is checked, sub users can not share their own private folders to others. The folders affected are those owned by the users, like Documents/Pictures. Or any folder they created themselves.

- o User must login to access file/folder shared to him/her
  When a file/folder is shared to someone, the person will get an email with the share URL. He can click the URL to access the shared file/folder immediately. When the setting is checked, click the URL will show the file/folder. However, to access it, he has to login to Gladinet Cloud. He needs to have an account in Gladinet Cloud, to access the share.

  o Don't append '(Team Folder)' to published folder
    When admin publish a team folder, on the user's portal, the folder shows as '<folder name>
    (Team Folder)', to distinguish it with other folders. When the setting is checked, Gladinet
    will not appended '(Team Folder)' to the team folder name any more.

  o Only allow sending share to specified domain
    By default, user can share file/folder to anyone with an email. When the setting is defined,
    user can only share to emails within the defined domains

  o List of Users with Cache disabled
    When users are added to the list, team client logged in with the user will not keep cached
    copy of the cloud files. For some operation, like edit files in Gladinet drive directly, cache is
    used. However, it will be deleted automatically, once the edit is done.

Desktop Client/File Server Client Settings

  o Enable distributed locking when accessing files in team folder
    When distributed locking is enabled and user 1 edits a file in team folder, a lock is applied on
    the file. When others open the same file, they'll get a warning that the file is editing by
    user1.

  o Disable backup/attach local folder from client device
    When it is checked, user cannot attach local folder in team client.
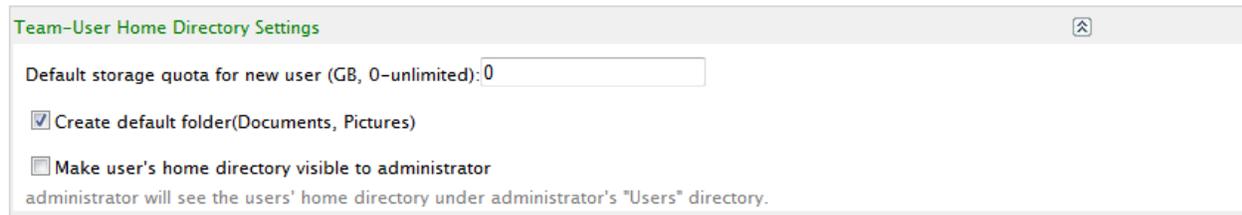
Retention Policy

It defines how many versions the versioned folder will keep. By default, the versioned folder keeps all the versions. When the number of versions to keep is defined, it will delete old versions. Please notice that the old versions are only deleted, when the file is accessed.

Team User Home Directory Settings

- o Default storage quota

  By default, each user created in Gladinet Cloud can use all the storage allocated to the admin account. Admin can define the default quota here. The quota can be changed during the user creation.

- o Create default folder (Documents, Pictures)

  When create user, Gladinet will automatically create two default folders, Documents and Pictures. When it is unchecked, Gladinet will not create the two folders for any new users created.

- o Make user's home directory visible to administrator

  By default, each user's private folder is only visible to the user. When the setting is checked, admin can view the user's private folders, under the folder 'Users' in admin root. The setting only affects users created after it is updated. It doesn't affect any existing users.