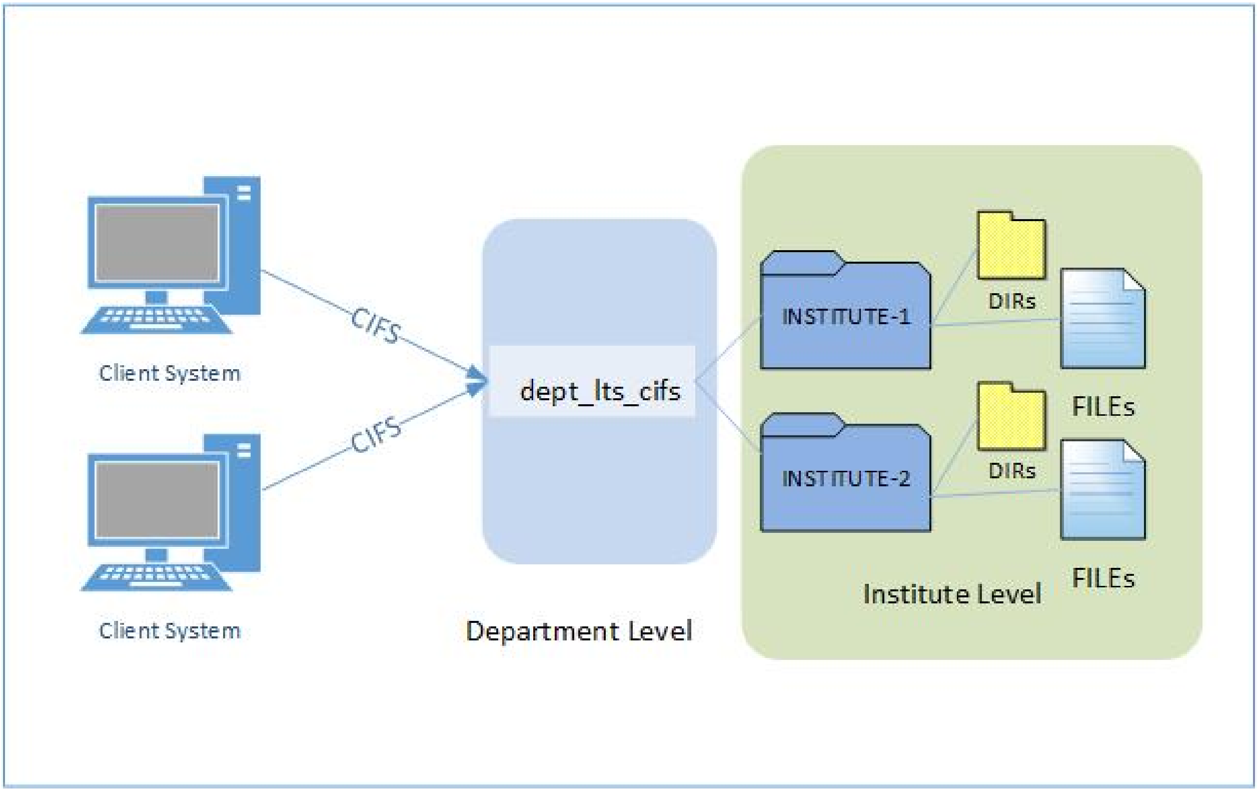
## CIFS Shares



*CIFS Access*

### Permissions on the department level

- AD group(s) authorized to mount the share
- The above is determined by the ISG
- They are configured on the LTS share by LTS admins.

### Permissions on the institute level

- Institute base directories are created by the ISG.
- At the same time, AD permissions must be set on the Directory.
- Permission can be given to separate AD groups for each institute Directory.

### Mounting shares

- Users that should see the contents of the entire department share (e.g. ISG) should mount on the department level.
- User that only need to see the contents of an single institue (e.g. working group) should mount on the institute level.

### Restrictions

### StrongBox: Modifying CIFS shares

After a client establishes a connection to a StrongBox CIFS share, changes to the share — including disabling or deleting the Active Directory user who established the connection, removing the Active Directory user or group used in the connection, changing read-write access of the share to read-only, and deleting the share — are not seen on the client until the connection is re-established.

The change will take effect on the client when the connection to the share is terminated and then, if possible, re-established.

**StrongBox: CIFS clients are unaffected by rights changes after connection**

Once a CIFS client has established a connection to a StrongBox share, the access rights in force at connection time remain in force for the life of the connection. Changes to a share's access permissions do not affect clients that are already connected. (AN-3319)

Examples of revoking access rights include:

- The Active Directory user specified at client connection time is disabled or deleted from its Windows domain.
- The lists of users or groups permitted access to a StrongBox CIFS share are changed.
- A StrongBox CIFS share configuration is changed from read-write access to read-only access.
- A StrongBox CIFS share configuration is deleted.

In all the above cases, CIFS clients that were connected to the share prior to the configuration changes are unaffected by revoked access rights.