Understanding Case Access Control

Access modes

Access to cases is by default `roleBased`, meaning that users with rolebased access to the customer and service of the case, has access to it. There are different roles for `read` and `write` access, and a separate role for "tech users", generally meaning users representing the service provider.

A case can be given `restricted` access mode, meaning that access to customer users are explicit, and not rolebased. Tech users will still have normal access to the case. This use case is for cases which are handled by the service provider as normal, but which are sensitive for the customer.

The explicit access mode means that only users/user groups which are on the explicit access list have access to the case. This also applies to tech users.
Note: System administrators may still access the case without explicit access.

The explicit access list may also extend normal role based access, by giving explicit users/user groups access to a case, which do not have role based access to the case at all.

Access levels

For each individual case, a user may be granted one of the following access levels, depending on role-based and/or explicit access settings:

- **Read** privileges
  - permits fetching all case details
- **Write** privileges
  - Read privileges
  - updating case priority, status, reference, category, assignedUser
  - adding comments
  - adding/removing tags, links and attachments.
- **Owner** privileges
  - Write privileges
  - changing access mode
  - granting/revoking access
  - changing the reporter of a case (implicit owner)
  - changing *subject* and *description* on the case
  - changing watcher settings for other users

This table maps out which users get these roles:

Access mode	Read access	Write access	Owner access
roleBased	Case reporter Users with service read role All ACL members	Case reporter Users with service write role ACL members with accesslevel `write`	Case reporter Administrators
writeRestricted	Case reporter Users with service read role All ACL members	Case reporter **Users with service tech role** ACL members with accesslevel `write`	Case reporter Administrators
readRestricted	Case reporter **Users with service tech role** All ACL members	Case reporter Users with service tech role ACL members with accesslevel `write`	Case reporter Administrators
explicit	Case reporter All ACL members	Case reporter All ACL members	Case reporter Administrators

Access roles

In addition to access levels, there are also a set of access roles: **user, tech** and **admin**.

User role

All users with read and/or write access to a case, assume the "user" role.

Tech role

Users with the role "tech" have additional privileges, which ordinary users do not:

- update *restricted fields*
- view or create *internal comments*
- update case workflows
- create an "unpublished" case, which are not visible to non-tech users
- publish an "unpublished" case
- change watcher settings for other users.
- delete comments and see deleted objects

Any change to the case also requires access level "write". A tech user with only "read" access level, can only view additional information.

Admin role

Users with the admin role have additional privileges, which users and techs do not

- assume "owner" role for the case, allowing override of case access settings and explicit access grants.
- users with "admin" role always have full write access level (implied by "owner"), as well as "tech" role.

Determining access level and role

To see which access level the current user has on a particular case, each case contains a field "currentUserAccess":

```
"currentUserAccess": {
  "level": "write",
  "role": "user"
}
```

- The field "level" may return "read", "write" or "owner". Write implies read. Owner implies both read and write.
    - If the user has no read access, the case will not be returned from the API
- The field "role" may return "user", "tech" or "admin". Tech implies user. Admin implies both tech and user.

Changing case access mode

> Changing the access mode requires access level **owner**

To change the access mode of a case, use the access PUT endpoint:

```
curl -X PUT -H "Argus-API-Key: my/api/key" -H "Content-Type: application/json"  https://api.mnemonic.no/cases/v2
/case/123456/access -d '{
  "accessMode": "readRestricted"
}'
```

Granting case access

> Granting case access requires access level **owner**

To grant access to a case for a user or user group, POST to the access endpoint with the subjectID of the user or group. The `level` parameter will determine the level of access granted to that user or group.

```
curl -X POST -H "Argus-API-Key: my/api/key" -H "Content-Type: application/json"  https://api.mnemonic.no/cases
/v2/case/123456/access -d '{
  "subjectID": <userID>,
  "level": "read"
}'
```

List case access

Depending on the case `accessMode`, different users have *role-based* access to the case, according to the table above. Use the Get case endpoint to see the `accessMode` of a case.

Explicit access granted to single users or user groups can be listed using the access endpoint:

```
curl -H "Argus-API-Key: my/api/key" https://api.mnemonic.no/cases/v2/case/123456/access
```

Revoking case access

> Revoking case access requires access level **owner**

To revoke access from a user on the case ACL, use the DELETE access endpoint with the ID of the ACL entry to delete:

```
curl -X DELETE -H "Argus-API-Key: my/api/key" https://api.mnemonic.no/cases/v2/case/123456/access/c2134bd3-9d88-4d6c-a395-d8d2241b4cbd
```


Please note, that users with role based access to a case cannot be explicitly revoked. To limit users with role based access from accessing a case, you need to change to a stricter `accessMode` on the case.