

Account security roles

Account role-based access privilege system is available since v. 1.4.0.

Each system user has a role (Administrator, Operator, Read-only, None). Access to various parts of the application is limited according to users access role.

This article describes the access that each role has.

Administrator

Accounts with the 'Administrator' access role have full access to Unimus and all features within.

In other words, 'Administrator' users are not limited in any way.

Operator

Accounts with the 'Operator' role have full read/write access to Unimus, except:

- Operators have no access to the 'User management' screen
- Access to 'License settings' is read-only (can see, but can't change license key)

We recommend that most users have 'Operator' set as their access role.

Users authenticated from Radius are assigned the 'Operator' role.

Access for operator accounts can be further restricted using 'Device access tags'.

Please see this wiki article for more information: [Device access tags](#).

Read-only

'Read-only' role accounts have read-only access to Unimus - they can not configure or change any settings.

Additionally, read-only accounts have these limitations:

- Read-only accounts have no access to the 'User management' screen
- Read-only accounts have no access to the 'License settings' menu

Access for read-only accounts can be further restricted using 'Device access tags'.

Please see this wiki article for more information: [Device access tags](#).

None

Accounts with the 'None' role have no access to the application - they can not even log in.

This role is meant to deny access to Unimus for a particular account, without the need to delete that account.

System access table

	Administrator	Operator	Read-only	None
Login				X
Access to all features			read-only access	X
Change any settings			X	X
License settings		read-only access	X	X
User management		X	X	X