User management

System access handling

Unimus supports internal and external user authentication. Radius and LDAP are currently supported for external authentication (see below for more details).

For more information on how Unimus handles system access (logins), please see this article: System login.

Local user database management

Local system users can be managed in "User management > Local users". You can create and/or remove local user accounts here.

One local Administrator-level user account must always be present, so deleting the last user is not possible.

User access roles and access limitation

Unimus support RBAC (role-based access control) - you can limit certain user accounts to specific role-based operations.
For more information please see this article: Account security roles.

In addition to RBAC, Unimus also allows for limiting access of specific accounts to only selected devices in the system (for example, limit junior admins to only see specific switches in Unimus).
For more information please see this article: Device access restrictions

External Auth / AAA

Unimus supports full external AAA with Radius, and / or external auth with LDAP.

Please see the following articles for each respective auth scheme:

- Radius AAA
- LDAP Auth

System access history

The system access history table shows all accounting records written to the local database. It will tell you who, when and how logged in to Unimus. Session start and end timestamps are logged, as well as the final session duration. You can also configure notifications on failed (or even successful) login attempts into Unimus in the "Notifications" menu. All login attempts (successful and failed) are also logged into the log file.

Login notifications, as well as log file logging support standard proxy headers to properly report login attempt IP address when using a reverse proxy (Apache / NGINX). Supported proxy headers:

- X-Forwarded-For
- X-Originating-IP
- X-Real-IP