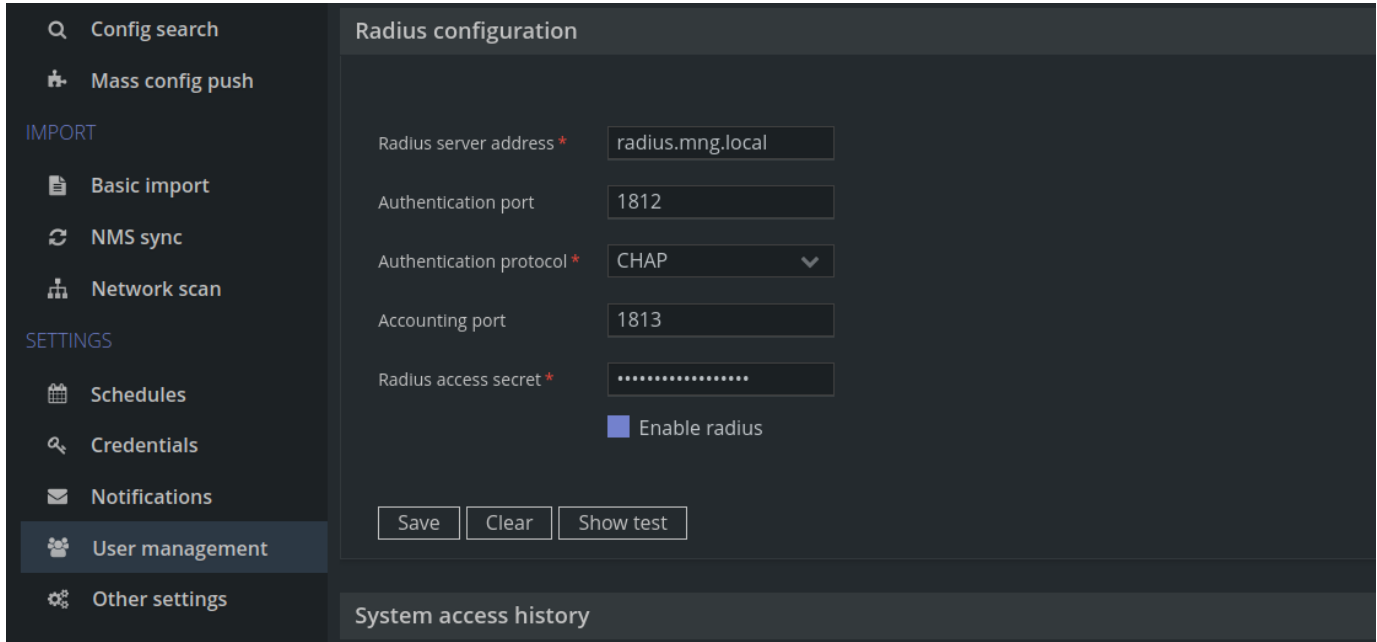


# Radius AAA

Unimus contains a Radius client, so it can AAA user logins against a central Radius server. You will need to configure a Radius server address (IP or FQDN) and a Radius shared secret. The "Enable Radius" check-box controls if Radius is used to AAA user logins or not. The "Show test" function uses currently configured Radius settings, even if they are not saved. This allows you to test your Radius configuration before saving it to the system.

Here is an example of a fully configured Radius client:



The screenshot shows a web application interface for configuring a Radius client. On the left is a sidebar with navigation options: 'Config search', 'Mass config push', 'IMPORT' (with sub-options 'Basic import', 'NMS sync', 'Network scan'), 'SETTINGS' (with sub-options 'Schedules', 'Credentials', 'Notifications', 'User management', 'Other settings'), and 'System access history'. The main panel is titled 'Radius configuration' and contains the following fields and controls:

- 'Radius server address \*': text input with value 'radius.mng.local'
- 'Authentication port': text input with value '1812'
- 'Authentication protocol \*': dropdown menu with 'CHAP' selected
- 'Accounting port': text input with value '1813'
- 'Radius access secret \*': text input with masked characters '.....'
- 'Enable radius': a checked checkbox
- Buttons at the bottom: 'Save', 'Clear', and 'Show test'

For more details of how Radius is used when a user attempts to log in, please see [System login](#).

## Default timeouts and configurable options

```
# NAS ID used in Radius requests
unimus.server.aaa.radius-nas-id=Unimus

# Radius request timeout, ms
unimus.server.aaa.radius-timeout=5000

# retry count for Radius requests
unimus.server.aaa.radius-retry-count=1
```