

Manage Failed Authentication

This page contains instructions on how to manage the failed authentication history of an account.

- [Clear logs](#)
- [View failed authentication attempts](#)
- [Search for failed authentication attempts](#)
- [Remove a session](#)

Clear logs

To manage the overall authentication history of all the accounts logged in the system:

1. Go to **Unified Communications Monitoring Web Interface Sessions** and click on the [Authentication History](#) icon.
2. The **Clear Logs** control allows you to remove the authentication logs from the database using one of the two criteria:
 - **Clear logs starting from <date> To <date>**: Clear the logs recorded in a certain period of time. Use the available text boxes or the calendar buttons to specify the interval's starting and end date. The accepted date format is yyyy-mm-dd.
 - **Clear logs older than <number> <period>**: Clear the logs older than the specified <number> of days/weeks/months/years. Use the drop-down list to select the <period>

View failed authentication attempts


All accounts that failed to authenticate in the system are listed in the **Failed Authentication Attempts** table, which you will find in **Unified Communications Monitoring Web Interface Sessions Failed Authentication**.

The **Resource** column refers to the authentication resource, for example Interface/Auth/Login or Interface/Auth/Logout, SystemAPI/Auth/Login, HG/Auth/Login, etc. While "Interface" refers to user authentication via VoipNow interface, "HG" refers to user authentication from Hubgets.

The **IP Address** column refers to the IP address the user tried to log in from.

Search for failed authentication attempts

You can filter the list of failed authentication attempts using the IP of the user and/or the User Login and/or the APIs (i.e. SystemAPI, UnifiedAPI, HubgetsAPI) used by applications to send authentication requests on behalf of the user:

1. Enter the IP of the session in the text box on top of the table and select User Login or one of the APIs from the drop-down list above the **Failed Authentication Attempts** table.
2. Click the  **Search** button. The system remembers the search criteria when a new search is performed and even after the user logs out.

Remove a session

You cannot delete your own sessions, but only those of the other users connected to the server.

The logs are added to the login history list based on the settings you have made in the **Log Messages on Level** drop-down list from the **Unified Communications Monitoring System Authentication User Login Preferences** page.

For more information, please read the [System Login Preferences](#) section.

Related topics

[Manage Authentication History](#)

[Manage System Authentication](#)