Recast

Authenticators

Last Modified on 04.16.26

Authenticators are used to provide multi-factor authentication in the Application Workspace. Currently, only RADIUS is supported.

Authenticators list

This list displays all authenticators currently available in the Application Workspace System.

Selecting multiple rows from the table

- To select multiple adjacent rows, click on the first row, then hold down the Shift key and click on the last row in the range; all rows between will be selected.
- To select multiple non-adjacent rows, hold down the Ctrl key (or "Command" on Mac) and click on each row you want to select individually.
- To select multiple adjacent rows using the mouse only, click and hold the left mouse button on the first row, then drag the cursor up or down across the rows to highlight the desired ones.
- Selecting rows using only the keyboard is not possible.

Table toolbar

To create a new authenticator, click on the **Create** button; to view the details of an authenticator or edit it, double-click its entry or select the authenticator and click the **Edit** button.

Views gives you control on how the table is displayed.
The default view contains all your authenticators in alphabetic ascending order, and only a few columns: **Name**, **Type**, **Identifier** and **Enabled**.
You can create your own personalized view of the table, by filtering the authenticators or adding/deleting columns and clicking **Save as** in the drop-down menu of **Views**.

Detailed view of an authenticator

See below the description of each screen in the detailed view of an authenticator, and what actions you can perform in each of them.

Overview screen

This screen provides a few basic options to configure the authenticator.

Identifier – This is what will be presented to the user when the authenticator response is requested. You could for example write "Enter SMS code" for an SMS authenticator, prompting the user to enter the code sent to their mobile.
Authentication type – Select here if the RADIUS server requires a challenge or OTP authentication.

- The challenge type will start the authentication with the username and password and expects a challenge back from the RADIUS server for a token code.
- OTP will directly provide the username and token code and expects an authentication result.

Servers screen

This screen lets you add the servers that provide the multi-factor authentication.

General tab

Address – The host name or the IP address of the RADIUS server.
Port – The port number on which the RADIUS server can be accessed.
Encryption – The encryption type the server uses. Currently only 'PAP' is supported.
Shared secret – The character string configured on the client hardware and on the RADIUS server.

Advanced tab

Priority – The priority of the server; the lower the number the higher the priority.
Timeout – The number of seconds a server will wait for a response from the RADIUS server.
Retry – The number of attempts to connect the RADIUS server after a timeout occurs.

Identity sources screen

You can add one or more existing identity sources that will be used by this authenticator. Refer to theIdentity Source documentation for more information.

Identity source – The identity source for which the authenticator will provide multi-factor authentication
Prefix – If the authenticator has a realm prefix string specified, it is appended to the beginning of the username when it is submitted to the RADIUS server.
Suffix – If the authenticator has a realm suffix string specified, it is appended to the end of the username when it is submitted to the RADIUS server.