

User Profile Validators

Theresa Henze - 2025-12-16 - [Miscellaneous](#)

When creating or editing attributes in the user profile (profile fields), validators can be added. These check user input for a specific format.

Different validators are available depending on the attribute type.

Available Validators for “Input Field” Type Attributes

Length

The “Length” validator checks whether the input has a specific minimum and/or maximum length.

Length 

ensures a minimum and optional maximum length

| | |
|----------------------|----------------------|
| Minimum | Maximum |
| <input type="text"/> | <input type="text"/> |

Trim
Trim input before applying min and max checks

- “Minimum”: Defines the minimum number of characters the input must have.
- “Maximum”: Defines the maximum number of characters the input can have.
- “Trim”: Removes leading and trailing whitespace from the input before checking the length.

Email

The “Email” validator checks whether the input is a valid email address.

Email 

Validates the input to be a valid email address

Maximum length for the local part

- “Maximum length for the local part”: Defines the maximum length of the local part of the email address (before the @ symbol). A value of 64 characters is recommended.

Email MX Record

The “Email MX Record” validator checks whether the domain of the entered email address has an MX record.

Email MX Record

Validates the email domain to check if an actual MX record is available



An MX (Mail Exchange) record is a DNS record that specifies which mail servers are responsible for receiving emails for a specific domain. For email address validation, a DNS query is performed to check whether an MX record exists for the domain.

Block Emails by Domain

The “Block Emails by Domain” validator checks whether the domain of the entered email address is on a defined blocklist.

Block Emails by Domain

Validates the email domain to check, if it's blocked



Use Default List

Block emails with domains from default list

+ Add Domain

- “Use Default List”: If this option is enabled, a [predefined list of domains](#) that are often used for spam or fraudulent activities is used. If the entry is not enabled, only the user-defined domains are considered.
- “Add Domain”: Here you can specify additional domains that should be blocked.

Username Prohibited Characters

The “Username Prohibited Characters” validator checks whether the input of a username contains special characters that typically do not belong in usernames.

Username Prohibited Characters

Blocks usually invalid values from being used as username characters



Prohibited characters include special characters such as <, >, &, ", ', \$, %, !, #, ?, @, ,, ;, :, *, ~, /, |, ^, =, [,], {, }, (,), control characters, and whitespace.

Note: This validator is ignored if “Email address as username” is enabled in the [User Profile Settings](#). Therefore, this validator should really only be used for the “username” field.

Username Not IDN Homograph

The “Username Not IDN Homograph” validator checks whether the input of a username contains potential IDN homograph attacks.

Username Not IDN Homograph

Prevents usage of IDN homographs for usernames



IDN homograph attacks use visually similar characters from different scripts (e.g., Latin and Cyrillic letters) to create deceptive copies of usernames. This validator helps prevent such attacks by ensuring that the username does not contain such character combinations.

Person Name Prohibited Characters

The “Person Name Prohibited Characters” validator checks whether the input of a person’s name contains characters that typically do not belong in personal names (first, middle, and last names).

Person Name Prohibited Characters
Blocks non-name related characters 

Prohibited characters include special characters such as <, >, &, ", \$, %, !, #, ?, \$, ;, *, ~, /, |, ^, =, [,], {, }, (,) and control characters.

Double

The “Double” validator checks whether the input is a valid number.

Double
Validates the input to be any kind of number 

Minimum **Maximum**

- “Minimum”: Defines the minimum value the input must have.
- “Maximum”: Defines the maximum value the input can have.

Integer

The “Integer” validator checks whether the input is a valid integer.

Integer
Validates input to be an integer or long 

Minimum **Maximum**

- “Minimum”: Defines the minimum value the input must have.
- “Maximum”: Defines the maximum value the input can have.

ISO Date

The “ISO Date” validator checks whether the input is a valid date in the [ISO 8601 format](#).

ISO Date
Validates a date in ISO format 

Local Date

The “Local Date” validator checks whether the input is a valid local date according to the user’s language settings.

Locale Date

Validates a date and takes format of current locale into account



Local date formats can vary depending on language and region. For example, the format MM/DD/YYYY is commonly used in the United States, while the format DD.MM.YYYY is common in Germany.

Multiple Values

The “Multiple Values” validator checks whether the number of entered values is within a defined range (only for input fields with allowed multiple values).

Multiple Values

Validates number of entries in a multivalued attribute



Minimum

Maximum

- “Minimum”: Defines the minimum number of values that must be entered.
- “Maximum”: Defines the maximum number of values that can be entered.

Pattern

The “Pattern” validator checks whether the input matches a defined regular expression (regex).

Pattern

Validates against a regular expression



Pattern

- “Pattern”: Defines the regular expression that the input must match. See also: [MDN Web Docs: Regular Expressions](#)

URI

The “URI” validator checks whether the input is a valid URI.

URI

Block malformed or non-URI inputs



+ Add Scheme

Allow Fragment

Require valid URL

- “Add Scheme”: Here you can specify certain URI schemes (e.g., http, https, ftp) that are allowed. If no schemes are defined, all valid URI schemes are allowed.
- “Allow Fragment”: If this option is enabled, URI fragments (the part after the # character) are allowed in the input.

- “Require valid URL”: If this option is enabled, the input must be a valid URL (i.e., it must contain a scheme and a host).

CEL Program

The “CEL Program” validator checks whether the input can be validated using the defined CEL program.

CEL Program 

Validates the input using a CEL program

CEL Program

 Ignore empty values

- “CEL Program”: Defines the CEL program used to validate the input. See also: [CEL Functions](#)
- “Ignore empty values”: If this option is enabled, validation is skipped when the input is empty.

Available Validators for “Checkbox” Type Attributes

Multiple Values

The “Multiple Values” validator checks whether the number of entered values is within a defined range.

Multiple Values 

Validates number of entries in a multivalued attribute

Minimum **Maximum**

- “Minimum”: Defines the minimum number of values that must be entered.
- “Maximum”: Defines the maximum number of values that can be entered.

Available Validators for “Date” Type Attributes

Age

The “Age” validator checks whether the entered date of birth results in an age within a defined range.

Age 

Validates if the input is in a valid age range

Minimum age

- “Minimum age”: Defines the minimum age that the input must have.