FORCAM FORCE IIOT User Administration

Version 5.11

Manual

Document: Manual - FORCAM FORCE IIOT User Administration.docx

Release date: 27.09.22

Document version: 1

Author: Ali Egilmez

FB_8-41 CREATED: 30.05.22 CHANGED: 27.09.22 VERSION: V1
APPROVED BY: HEAD OF TTE AUTHOR: TECHNICAL WRITER CLASSIFICATION: PUBLIC

Contents

1 Concept[*]

The Workbench is a multilingual, web-based application for configuring master data and other terminal-specific settings. The Workbench is used to configure FORCAM FORCE IIOT.

This manual provides an overview and guidance for the following basic Workbench configuration options:

- Creating a user
- Assigning rights and roles
- Defining password policies

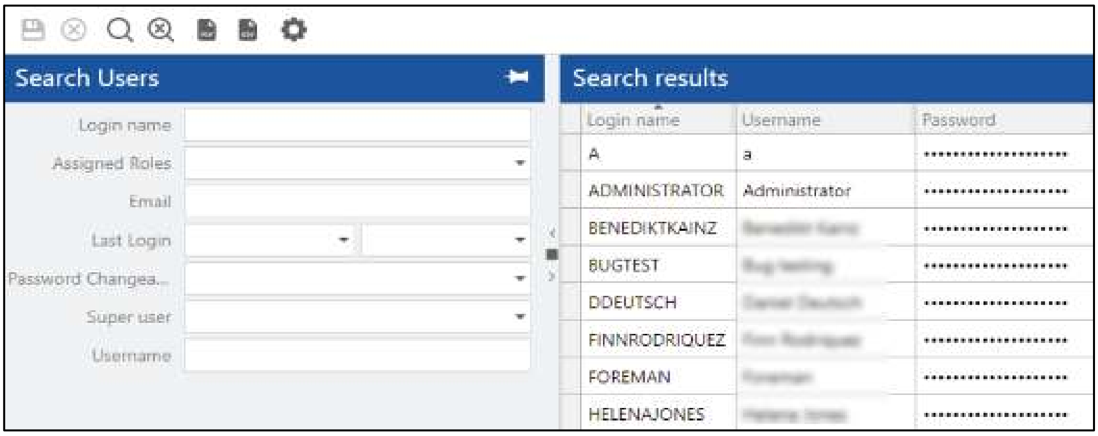
Other functions are covered in separate manuals also provided by FORCAM.

[*] For better readability, we generally use the generic masculine in the text. These formulations, however, are equally inclusive of all genders and address all equally.

2 User Editor

Path: User Administration > User Editor

Each user of the Workbench can have their own dedicated user account. One or more roles can be assigned to a user account. The assignment of a role is not mandatory.



Search Users

Login name

Assigned Roles

Email

Last Login

Password Changea...

Super user

Username

Search results

Login name	Username	Password
A	a	••••••••••••••••••••
ADMINISTRATOR	Administrator	••••••••••••••••••••
BENEDIKTKAINZ	[redacted]	••••••••••••••••••••
BUGTEST	[redacted]	••••••••••••••••••••
DDEUTSCH	[redacted]	••••••••••••••••••••
FINNRODRIQUEZ	[redacted]	••••••••••••••••••••
FOREMAN	[redacted]	••••••••••••••••••••
HELENAJONES	[redacted]	••••••••••••••••••••

Fig. 1: User Editor

To create a new user account:

1. Right-click at the search results table at the right and click **Create New User** in the context menu.
2. Enter the desired data (see below).
   The fields marked with a blue dot are mandatory fields.
3. Save.

ⓘ A Super User has access to all functions of the system.

ⓣ You can make changes to the user account directly in the search results table.

The following fields or settings are possible:

Table 1: Parameters for configuring a user account in FORCAM FORCE IIOT

Field	Description
Login Name	Mandatory field. Name with which the user logs in to the Workbench. Appears in the upper right corner of the screen after login. The following characters are allowed for the name: Capital letters, digits and underscore (_).
Username	Mandatory field. Name stored as additional information about the account. Can consist of any characters.
Password	Mandatory field. Password which is to be entered next to the login name when logging in to the Workbench. Can consist of any characters and be of any length as long as no password rule is applied (see below).
Email	Email address to be assigned to the account. Used, for example, to send a notification to the user in case of limit violations.

Field	Description
User Locked	Indicates whether the account is locked. An account will be locked if the password is entered incorrectly too often. The number of failed attempts is configured in the password rules. A super user can unlock an account by right-clicking the locked account and clicking **Unlock user** in the context menu.
Use Password Rules	If a check mark is set, all configured password rules apply to this account.
Password Changeable	If a check mark is set, the password may be changed by the respective users themselves. A super user may change any password.
Super User	If a check mark is set, the account becomes a super user. A super user has extensive rights and can enter all areas of the Workbench and perform all options.
Assigned Roles	Roles assigned to the account (see below). Rights and roles are configured in the Rights- & Roles Editor (see chapter 3).
Time Zone	Time zone of the account
Last Login	Date at which the user last logged in
Localization	Localization for the account (see section 2.1). Localization of the account is mandatory if it has been defined.

To assign a role to a user account:

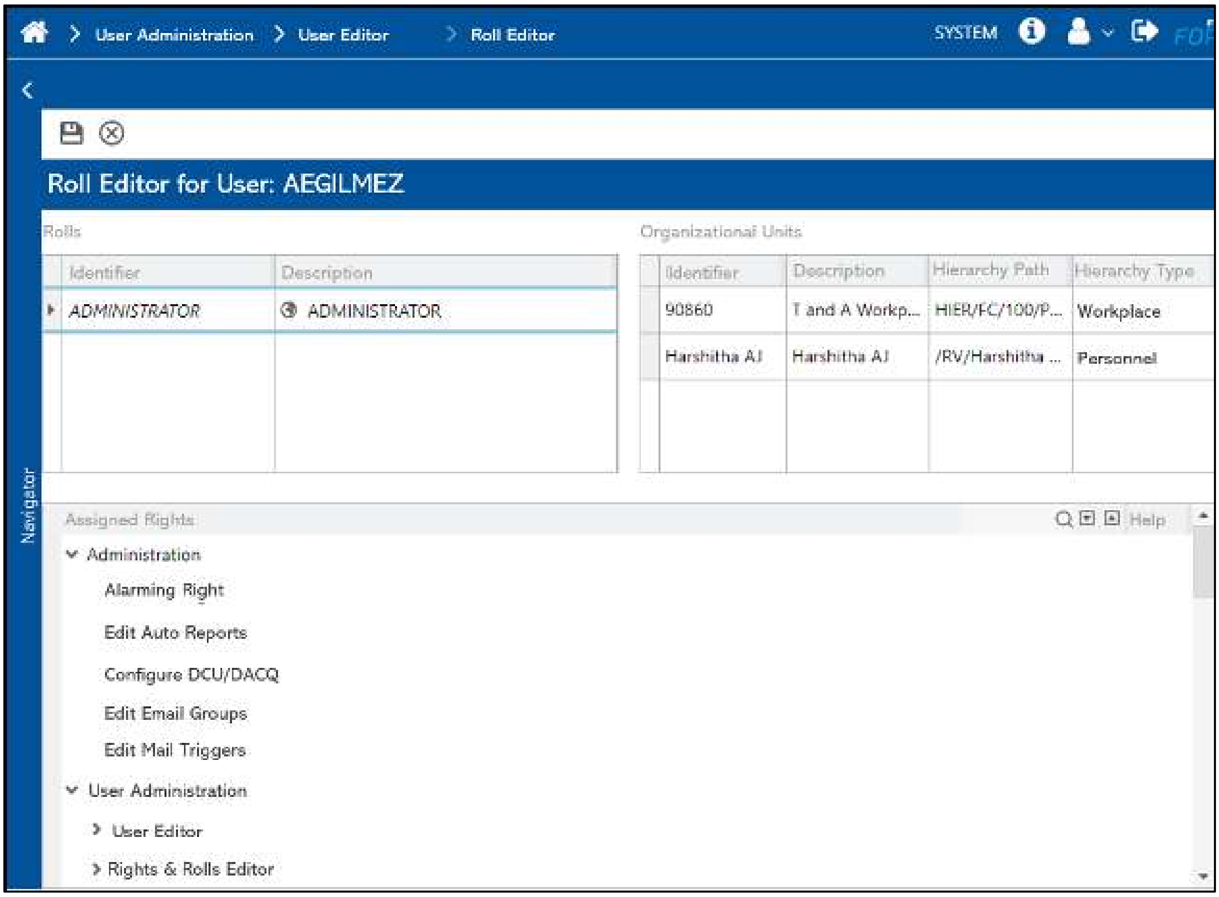
✓ A user account is already created and saved.

1. Right-click on the desired user account and click **Edit Role Assignments** in the context menu.

→ The view changes to the role editor.

2. In the upper left-hand area, right-click on **Roles** and click **Assign Role** in the context menu.
3. Select and confirm the desired roles in the next dialog.
   You can also assign multiple roles to a user account.
4. In the upper right area, right-click on **Organizational Units** and click on **Add** in the context menu.
5. Select and confirm the desired workplace hierarchy in the next dialog.
6. Right-click in the **Organizational Units** area and click on **Add Personnel Organizational Unit** in the context menu.
7. Select and confirm the desired person or cost center in the next dialog.
8. Save.

ⓘ The **Assigned Rights** area below indicates all rights for the selected role in a detailed tree structure.



Roll Editor for User: AEGILMEZ

Rolls

Identifier	Description
ADMINISTRATOR	ADMINISTRATOR

Organizational Units

Identifier	Description	Hierarchy Path	Hierarchy Type
90860	T and A Workp...	HIER/FC/100/P...	Workplace
Harshitha AJ	Harshitha AJ	/RV/Harshitha ...	Personnel

Assigned Rights

- Administration
  - Alarming Right
  - Edit Auto Reports
  - Configure DCU/DACQ
  - Edit Email Groups
  - Edit Mail Triggers
- User Administration
  - User Editor
  - Rights & Rolls Editor

Fig. 2: Role Editor

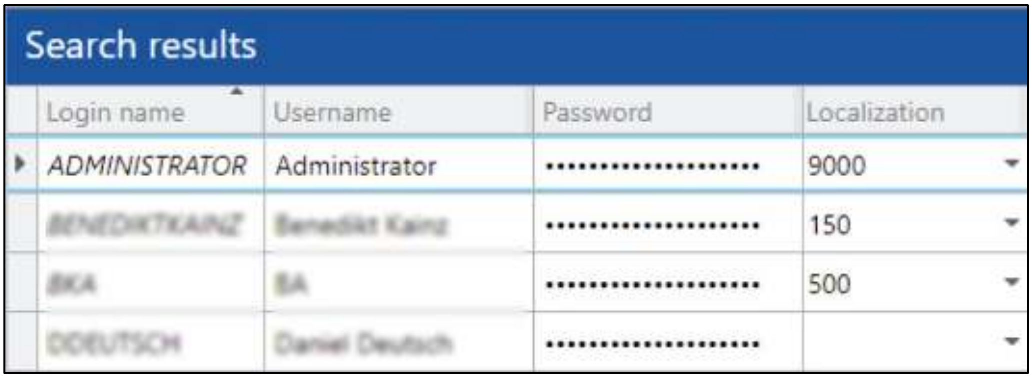
2.1 Localization

If Multi-Site Administration is actively used, all users must generally be localized. Only localized users and super users can exist.

ⓘ For detailed information on Multi-Site, see the Multi-Site Administration manual.

A user is assigned instances of the defined localization level for multi-site during localization. The localization level instances from the ORG hierarchy have assigned configured attributes.
A super user can create local administrators by localizing users. A super user has no restrictions on viewing data and has access to all localizations.
A localized user can only see his own assigned localizations. In general, the user gets viewing, editing and creation rights based on the existing rights & roles management.
Example:
In an ORG hierarchy there is the localization **GER** (Germany). The workplaces **760-1** and **760-2** were assigned to the sub node **MUC** (Munich). In the user administration the localization **GER** was assigned to the users. These two users can only view and edit data localized to the Munich location.

ⓘ A local administrator must have at least one localization, but can have multiple localizations.



Search results

	Login name	Username	Password	Localization
▸	ADMINISTRATOR	Administrator	••••••••••••••••••••	9000 ▾
	[redacted]	[redacted]	••••••••••••••••••••	150 ▾
	[redacted]	[redacted]	••••••••••••••••••••	500 ▾
	[redacted]	[redacted]	••••••••••••••••••••	▾

Fig. 3: User Localization

A local administrator can localize other users with appropriate rights, as long as they are a part of the administrator's own localization. A user can also carry a foreign localization (foreign key).
When editing localizations of other users, a local administrator can only share or remove his own localization. If he creates other users himself, they also automatically share his localizations.
Example:
A super user localizes user X to plant A. X is local administrator for plant A.
X localizes user Y. Y is thus also local administrator for plant A.
Y creates user Z. Z is not an administrator, but automatically belongs to plant A.

ⓘ A user may only manage the master data of their own localization.

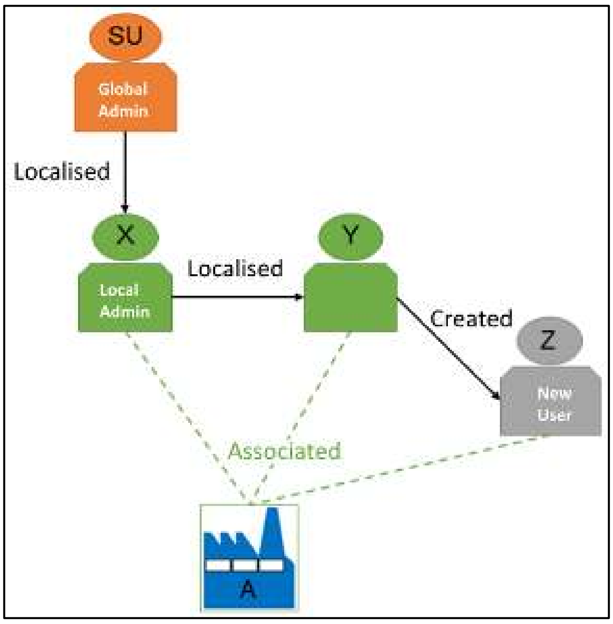
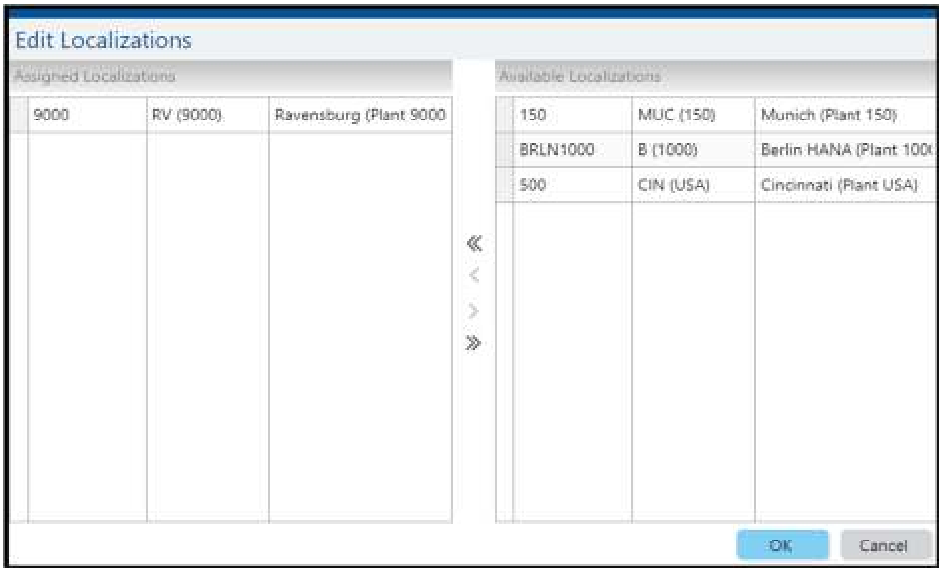


Fig. 4: User localization (example)

To localize a user:

- ✓ The ORG hierarchy is configured.
- ✓ A hierarchy tree is created.

1. Open the drop-down menu for the desired user in the **Localization** column.
2. Select and confirm the desired localizations in the next dialog.
3. Save.



Edit Localizations

Assigned Localizations

9000	RV (9000)	Ravensburg (Plant 9000

Available Localizations

150	MUC (150)	Munich (Plant 150)
BRLN1000	B (1000)	Berlin HANA (Plant 100(
500	CIN (USA)	Cincinnati (Plant USA)

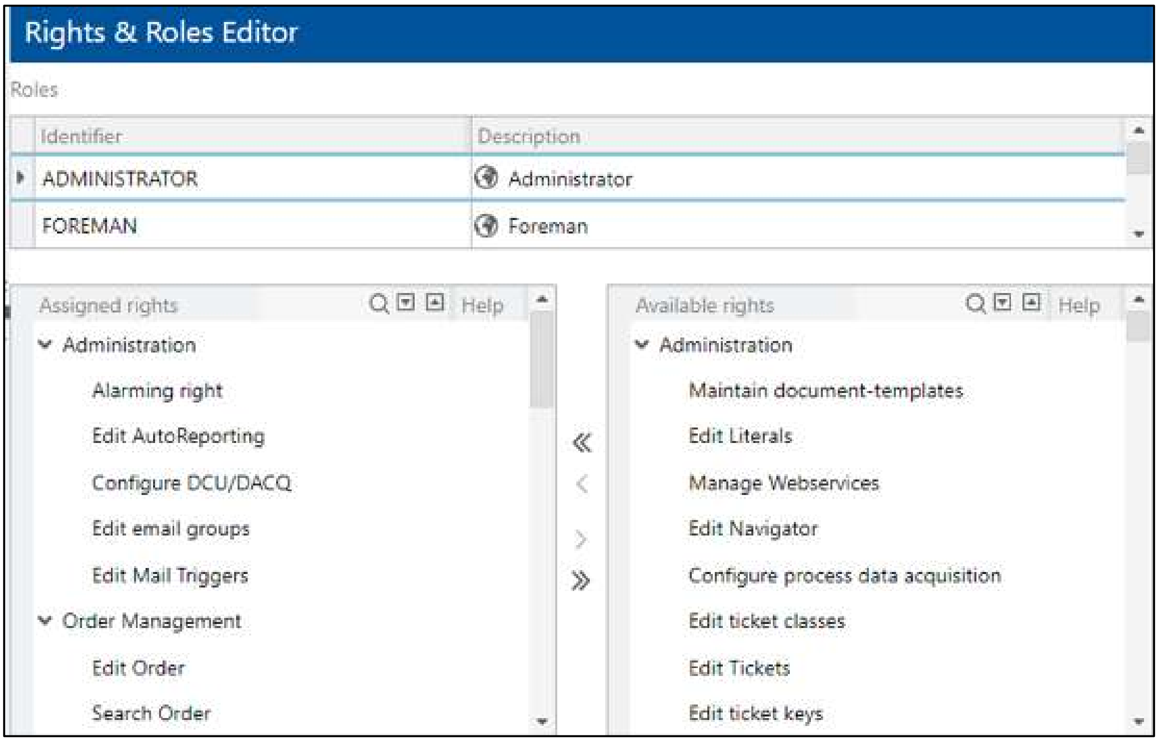
Fig. 5: Adding a user localization

ⓘ A super user has no localization. This means that the super user is a global administrator and is not restricted in rights.

3 Rights & Roles Editor

Path: User Administration > Rights & Roles Editor

Users of FORCAM FORCE IIOT can be divided into different groups with different rights. These groups are referred to as roles (e.g. manager, foreman, maintenance, etc.). Rights or functions that are required for the respective task can be assigned to each role. Accordingly, rights that are not assigned cannot be exercised by the respective role.



Rights & Roles Editor

Roles

Identifier	Description
ADMINISTRATOR	Administrator
FOREMAN	Foreman

Assigned rights

- Administration
  - Alarming right
  - Edit AutoReporting
  - Configure DCU/DACQ
  - Edit email groups
  - Edit Mail Triggers
- Order Management
  - Edit Order
  - Search Order

Available rights

- Administration
  - Maintain document-templates
  - Edit Literals
  - Manage Webservices
  - Edit Navigator
  - Configure process data acquisition
  - Edit ticket classes
  - Edit Tickets
  - Edit ticket keys

Fig. 6: Rights & Roles Editor

The use of rights and role management is necessary to handle the visibility and maintenance of data and user interfaces within FORCAM FORCE IIOT.

It is mandatory for a local administrator to have the assignment of the organizational unit to which he is localized (required branches of the ORG hierarchy of localization). The assignment essentially defines which hierarchy and branches of a hierarchy the user is allowed to see and assign to other users in roles.

ⓘ For detailed information on Multi-Site, see the Multi-Site Administration manual.

To create a new role:

1. Right-click in the upper area under **Roles** and click **Create new role** in the context menu.
2. Optional: Enter description.
3. Save.

To assign rights to a role:

✓ A role is defined.

1. Select the desired role in the upper area under **Roles**.
2. In the lower right area **Available Rights** select one or more rights and move them to the left using the move icon.
3. Save.

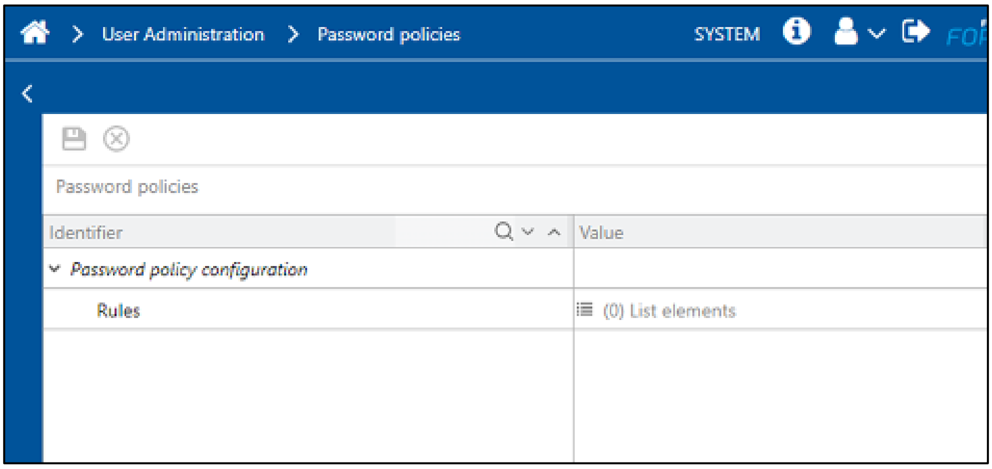
→ The role has all the rights listed under **Assigned Rights**.

4 Password Policies

Path: User Administration > Password Policies

Password policies provide the option to set individual or custom policies for user passwords. For example, it can be defined that passwords may or may not contain specific characters or must correspond to a specific length.

⚠ The password policies affect the Workbench and Office services. The Shopfloor Terminal is excluded from this. Passwords for the Shopfloor Terminal are defined in the profile configuration.



Password policies

Identifier	Value
Password policy configuration	
Rules	(0) List elements

Fig. 7: Configured password rules

There are a total of eleven different rules available. The rules can be combined in any way, but they do not have an AND connection. For example, if four rules are configured and the first rule is violated, the password is already invalid even if the other three rules are not violated.
Applying the password policy for a user account (see chapter 2) also applies to all configured rules of a line.

To add a password rule:

1. Right-click in the right area under **List Elements** and click on **Add New List Element** in the context menu.

➔ A new list element is added, but initially it is collapsed.

2. Open the new rule row via the drop-down icon at the left.
3. In the **Rule Configuration** row, select the desired password rule from the drop-down menu.

➔ Other additional parameters appear depending on the selection.

4. Define the selected rule as desired using the parameters.
5. Save.

The following rules are supported by FORCAM FORCE IIOT:

Table 2: Possible password policies in FORCAM FORCE IIOT

Rule	Parameter	Description
Username		The username must not be included in the password. Here, the case-sensitivity is irrelevant.
Permitted Characters		Characters that the password must consist of or begin/end with
	Characters	Definition of characters for match behavior
	Match behavior	The rule changes depending on the selected match behavior: – Contains: The password must consist of the characters defined here and may not contain any other characters. – Starts with: The password must start with one of the characters defined here. – Ends with: The password must end with one of the characters defined here.
Failed Logins		Determines the amount of failed login attempts before the user account is locked
	Number of failed logins	Specifies the exact number of possible misses. For example, if 3 is entered, the account will be locked after the third failed attempt.
Minimum and Maximum Length		Determines the password character length
	Minimum length	Minimum number of password characters
	Maximum length	Maximum number of password characters
Expiration Rule		Defines the expiration time for passwords (e.g. 14 days)
	Unit	Unit for the expiration time
	Unit count	Number of units for the expiration time
Password History		The password may not have been used before.

Rule	Parameter	Description
	Number of password history entries	Defines how many of the last passwords may not be used (e.g. the last three passwords)
Regular Expression: Accepts Password		The password must match this regular expression to be accepted.
	Regular expression	Regular expression to which the password must correspond
Regular Expression: Rejects Password		The password must not match this regular expression to be accepted.
	Regular expression	Regular expression to be excluded from the password
Forbidden Characters		Characters that the password may not contain or begin/end with
	Characters	Definition of characters for match behavior
	Match behavior	The rule changes depending on the selected match behavior: – Contains: The password may not contain any of the characters defined here, but must contain other characters. – Starts with: The password may not start with any of the characters defined here. – Ends with: The password may not end with any of the characters defined here.
Number Range		Range of numbers that may not appear in the password. Example: If the range is set between 22 and 33, no number sequences may be used that are in between those numbers (e.g. 23, 32). ⚠ If the range is set between 0 and 9, no numbers may be used at all, since every sequence of numbers falls in between these.
	Start number range	Start of the number range
	End number range	End of the number range
	Match behavior	Determines at which specific place of the count is to be considered

Rule	Parameter	Description
Character groups to be used		Characters from a group of characters that the password must contain. Example: For the password to contain an uppercase letter, **uppercase letters A-Z** with the minimum number 1 must be selected. Only one character group can be configured per rule. If the password should additionally contain a number, another rule must be added to which **numbers 0-9** must be selected.
	Character group	Character group, from which the password should contain at least n characters
	Minimum count	Minimum number of characters of the selected group that the password must contain
	Definition of special characters	Determines which characters are considered special characters. Only relevant if **special characters** have been selected as the character group.

5 Annex

5.1 Document Conventions

Table 3: Fonts, formatting and characters used

Conventions	Description
Bold Type	Buttons and options names are written in bold type.
Italics	Highlighted words are in italics.
Icons	For a function that is represented by an icon, the icon is referenced as the object.
Action Result	Action results are indicated by →.
Prerequisites	Prerequisites are indicated by ✓.
Warnings	Warnings are indicated by ⚠.
Notes	Notes are indicated by ⓘ .
Tips	Tips are indicated by ⓣ.

5.2 Table of Figures