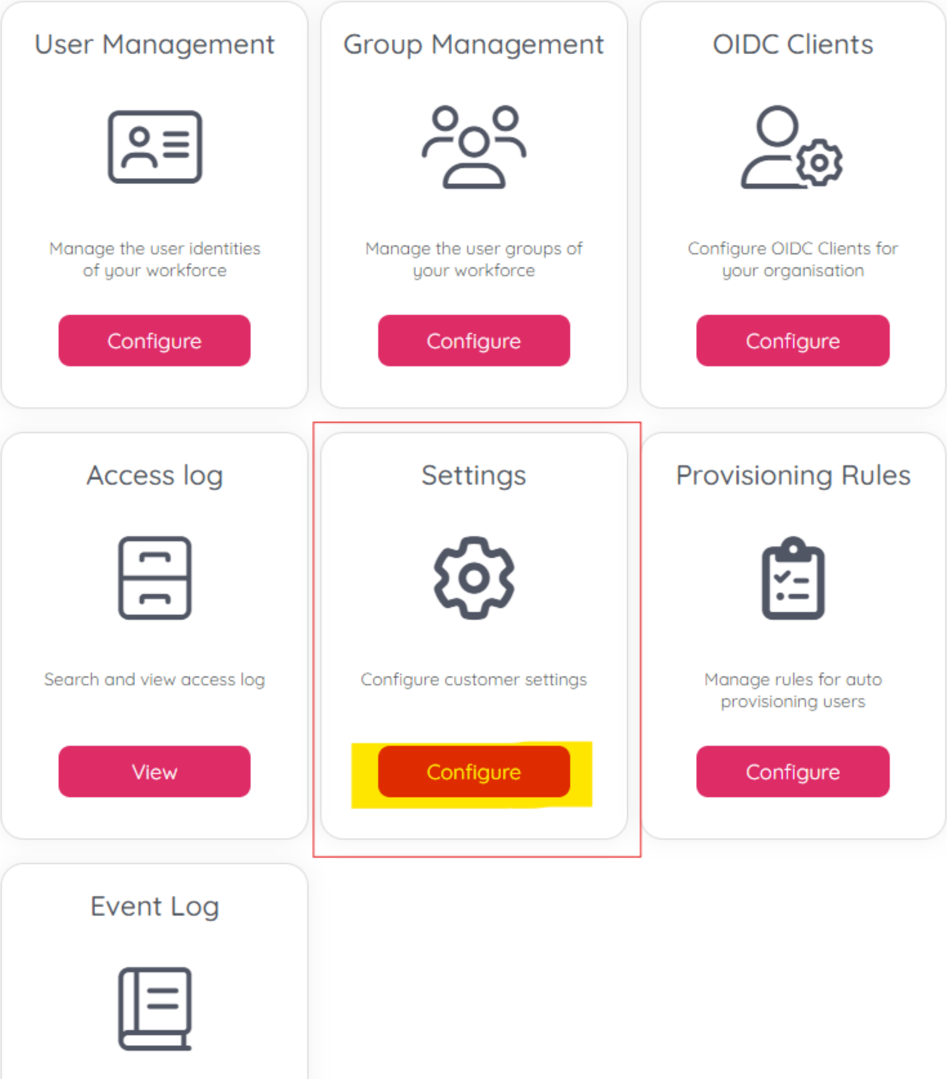
Settings configurations for your organisation

As an administrator you can configure settings applying to the whole organisation (i.e. all the users in the solution) via the Organisation Settings' submenu called “Settings”.

To access it, you will need to:

1. Access the Puzzel application
2. Click on the profile icon to the right side of the top bar
3. Select Organisation Settings from the drop down menu
4. You will then see the Organisation Settings home screen below, where you can click "Configure" under "Settings".

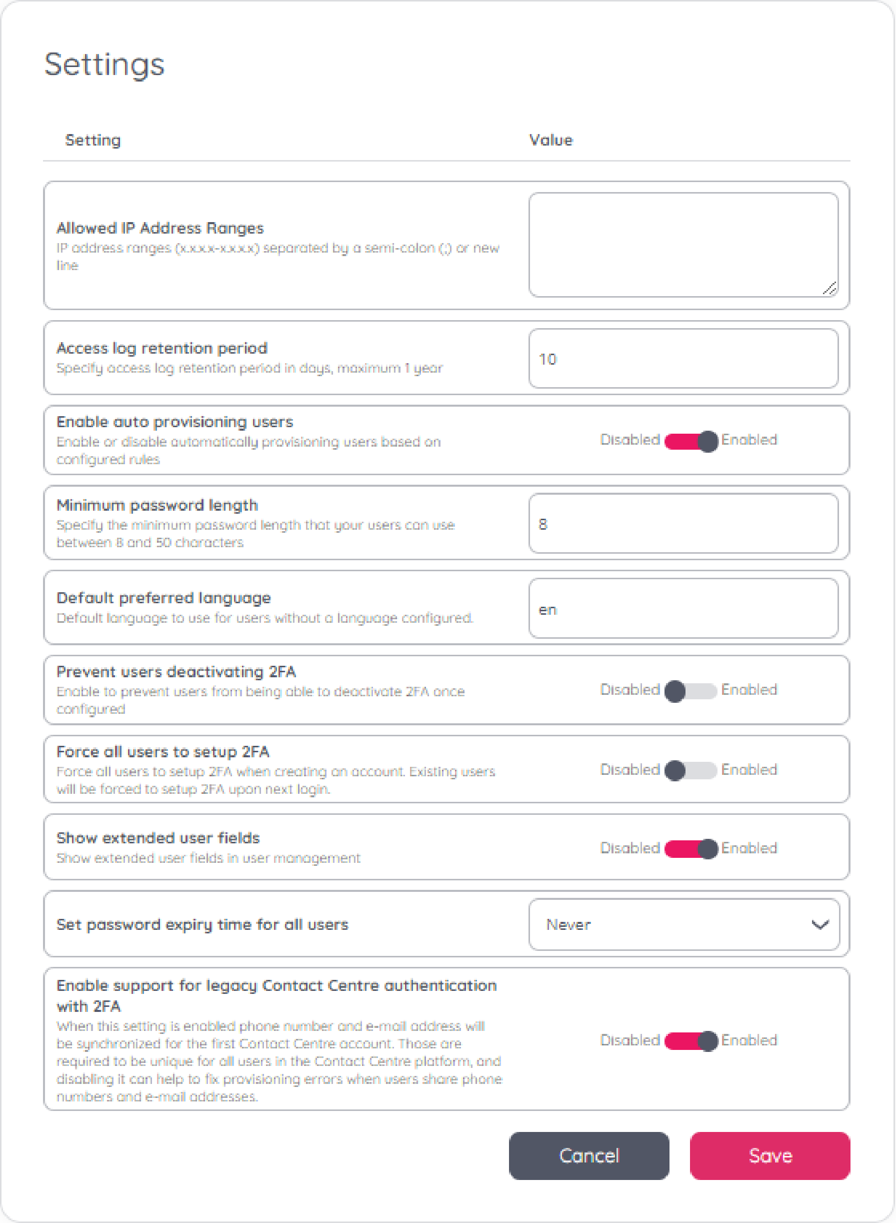

User Management
Manage the user identities of your workforce
Configure
Group Management
Manage the user groups of your workforce
Configure
OIDC Clients
Configure OIDC Clients for your organisation
Configure
Access log
Search and view access log
View
Settings
Configure customer settings
Configure
Provisioning Rules
Manage rules for auto provisioning users
Configure
Event Log

The Settings page will offer you several input boxes and toggles:

- **Allowed IP Address Ranges** - Allowed IPs can be entered, separated by IPs with a semicolon or new line
- **Access log retention period** can be configured in days up to a maximum of 1 year
- **Enable auto provisioning users** - that’s for enabling, but just as much for disabling respectively the users auto

provisioning based on configured rules. So even if there are rules set already, new users won’t be provisioned if this option here is disabled

- **Minimum password length** can be entered as number of characters. It can be between 8 and 50 characters.
- **Default preferred language** would apply to those users who have no preferred language defined for them individually
- **Prevent users deactivating 2FA** - Generally the 2-Factor Authentication can be configured, thus activated or deactivated, by every user when they navigate to the “User Profile” menu on the top right of the Puzzel app. But if the administrator selects this one, users with active 2FA won’t be able to disable it.
- **Force all users to setup 2FA** - Coming naturally from the above one, if the administrator wants everyone to use 2FA, the above option will ensure the ones who already do, won’t go back to not using it. This option here would ensure the ones who don’t use 2FA yet, will be forced to set it up.
- **Show extended user fields** - This toggle would enable or disable the extended user fields in “User Management”. That includes details like employee number, cost center, organisaton, division, department and manager.
- **Set password expiry time for all users** - By default this dropdown would be set to “Never”, but the administrator can specify an expiry time at their discretion, choosing between 2, 4, 6 weeks, 3 or 6 months, or 1 year.
- **Enable support for legacy Contact Centre authentication with 2FA** - When this setting is enabled phone number and e-mail address will be synchronized for the first Contact Centre account. Those are required to be unique for all users in the Contact Centre platform, and disabling it can help to fix provisioning errors when users share phone numbers and e-mail addresses



Settings

Setting	Value
Allowed IP Address Ranges IP address ranges (x.x.x.x-x.x.x.x) separated by a semi-colon (;) or new line	
Access log retention period Specify access log retention period in days, maximum 1 year	10
Enable auto provisioning users Enable or disable automatically provisioning users based on configured rules	Disabled [✓ Enabled]
Minimum password length Specify the minimum password length that your users can use between 8 and 50 characters	8
Default preferred language Default language to use for users without a language configured.	en
Prevent users deactivating 2FA Enable to prevent users from being able to deactivate 2FA once configured	[✓ Disabled] Enabled
Force all users to setup 2FA Force all users to setup 2FA when creating an account. Existing users will be forced to setup 2FA upon next login.	[✓ Disabled] Enabled
Show extended user fields Show extended user fields in user management	Disabled [✓ Enabled]
Set password expiry time for all users	Never
Enable support for legacy Contact Centre authentication with 2FA When this setting is enabled phone number and e-mail address will be synchronized for the first Contact Centre account. Those are required to be unique for all users in the Contact Centre platform, and disabling it can help to fix provisioning errors when users share phone numbers and e-mail addresses.	Disabled [✓ Enabled]

Once the configurations have been inserted or edited accordingly, select “Save” for them to be set.