



# Environment Management Gadget

Planon Software Suite

Version: L105

© 1997 - 2024 Planon. All rights reserved.

Planon and the Planon logo are registered trademarks of Planon Software Development B.V. or its affiliates. All other product and company names mentioned herein are trademarks or registered trademarks of their respective companies. Planon Software Development B.V., its affiliates and/or licensors own the copyright to all Planon software and its associated data files and user manuals.

Although every effort has been made to ensure this document and the Planon software are accurate, complete and up to date at the time of writing, Planon Software Development B.V. does not accept liability for the consequences of any misinterpretations, errors or omissions.

A customer is authorized to use the Planon software and its associated data files and user manuals within the terms and conditions of the license agreement between customer and the respective legal Planon entity as soon as the respective Planon entity has received due payment for the software license.

Planon Software Development B.V. strictly prohibits the copying of its software, data files, user manuals and training material. However, customers are authorized to make a back-up copy of the original CD-ROMs supplied, which can then be used in the event of data loss or corruption.

No part of this document may be reproduced in any form for any purpose (including photocopying, copying onto microfilm, or storing in any medium by electronic means) without the prior written permission of Planon Software Development B.V. No copies of this document may be published, distributed, or made available to third parties, whether by paper, electronic or other means without Planon Software Development B.V.'s prior written permission.

# About this Document

## Intended Audience

This document is intended for *Planon Software Suite* users.

## Contacting us

If you have any comments or questions regarding this document, please send them to: [support@planonsoftware.com](mailto:support@planonsoftware.com).

## Document Conventions

### **Bold**

Names of menus, options, tabs, fields and buttons are displayed in bold type.



### *Italic text*

Application names are displayed in italics.

### CAPITALS

Names of keys are displayed in upper case.

## Special symbols

	Text preceded by this symbol references additional information or a tip.
	Text preceded by this symbol is intended to alert users about consequences if they carry out a particular action in Planon.

# Table of Contents

About Environment Management gadget.....	5
Accessing the Environment Management gadget.....	6
Understanding the Environment Management gadget.....	7
Environment Management details.....	9
Disk.....	9
Customize.....	10
Backups.....	12
Restoring a backup.....	14
Cloning a Cloud environment.....	17
Importing a clone.....	18
Logs.....	19
Log file contents.....	20
Danger zone.....	22
Reset service passwords (WebDAV and Web service console).....	24
Improved features.....	25
Domain settings.....	26
Custom URLs and certificates.....	27
Enabling a portal integration in the Cloud.....	28
Mutual SSL settings.....	29
SSO.....	30
OpenID Connect.....	32
Privacy sandbox compatibility.....	35
IP Whitelisting.....	39
Alerts.....	40
Cloud e-learning.....	42
Index.....	43

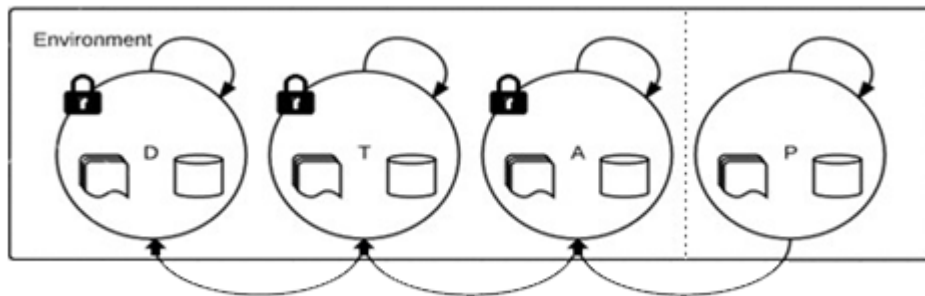
# About Environment Management gadget

Planon Cloud is a fully web-based infrastructure that safely runs in a secure data center. Planon's Environment Management gadget provides an overview of:

- Available environments,
- Environments that are up and running,
- Available disk space on each environment,
- Pending updates on the environments.

## Environment/Instances

A Cloud environment can contain multiple instances (such as Production and Acceptance).



The following Planon instances are available:

Instances	Description
Development	This environment is used for developing interfaces and/or Tailor Made Software (TMS).
Test	This environment is used for testing (parts of) the software, configuration, interfaces and/or TMS.
Acceptance	This environment is used for accepting changes to the software. The Acceptance environment is the first instance to be upgraded when a new version is installed.
Production	This is the main operational environment and actual work must be done in this environment.



Most customers only have Production and Acceptance environments. In such cases, testing can also be done in the Acceptance environment.

## Accessing the Environment Management gadget

The Environment Management gadget, amongst various other Planon gadgets, is available on the Planon application homepage.



During minor updates of the backend, the Environment management gadget will be temporarily unavailable. The gadget will then display the message 'The gadget is temporarily unavailable'. It is then not possible to use the gadget or its functionality. The Planon application, however, will remain operational and you can use the application as regular.


See also: [Cloud maintenance](#).

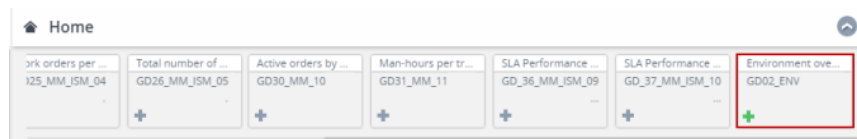
To access the Environment Management gadget, you must first log on to the Planon application .


### Procedure

1. To log in to the Planon application , click the URL provided.
2. On the Login screen, enter your user name and password.
3. Click OK. You are logged into the Planon application .

The homepage is displayed.

If the **Environment Management** gadget is not displayed on the homepage, click the **Edit**  button on the right. The gadget library appears and the existing gadgets on your homepage are unlocked.




4. Select the Environment overview gadget from the library by clicking the name or the  icon on the gadget. The gadget is added to the workspace.
5. To move the gadget around on the workspace, hold the gadget (with the four-arrowed cursor) and drag it to the required position.
6. Click the Edit button again. The library will be closed and the Environment Management gadget becomes available on the homepage.



This gadget is configured in Web Configuration. You may not see this gadget due to authorization.

# Understanding the Environment Management gadget

The Environment Management gadget has a Cloud  symbol on the top left to indicate that it is a Cloud gadget. The gadget provides a visual representation of the available Planon instances:

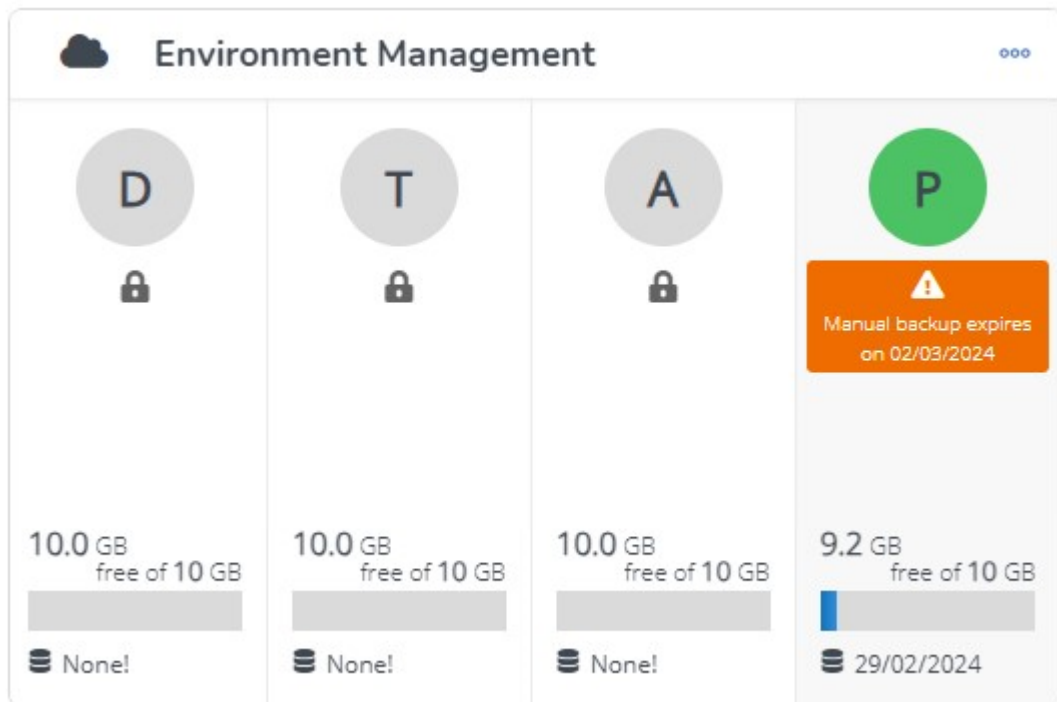
**D** - Development

**T** - Test



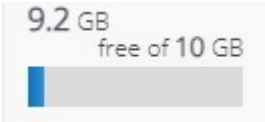

**A** - Acceptance

**P** - Production

If an environment is available in the Cloud, the relevant segment is highlighted in green. If a manual backup is going to expire, a notification will be shown in the Environment Management gadget:



The following conventions apply to the Environment Management gadget:

Convention	Description
Grey	Indicates that the environment is unavailable - either turned off or not running.
Green	Indicates that the environment is available and is running.
Yellow	Indicates that the environment is running but cannot be logged in as the machine may be restarting or upgrading.
Red	Indicates an error on the server. Please contact the Cloud support team.
Lock 	Indicates that the environment is currently not available (but the customer can purchase it).
Cloud arrow pointing up 	Indicates that an upgrade (a service pack) is available.  The cloud image is not seen, if the environment is running the latest service pack.
Free space indicator – progress bar 	The Blue color on the indicator denotes the currently used space.  Grey indicates the available space.
Date 	The date below the free space indicator denotes the last backup date.  If 'None' is displayed, it means no backup is performed.  A notification that indicates the name and the expiry date of the manual backup. There can be up to two notifications displayed at once.




Convention	Description
Cloud wrench 	Indicates that an hotfix is available on the current version of the Planon application.  The hotfix can be applied by restarting the instance (see danger zone).

## Environment Management details

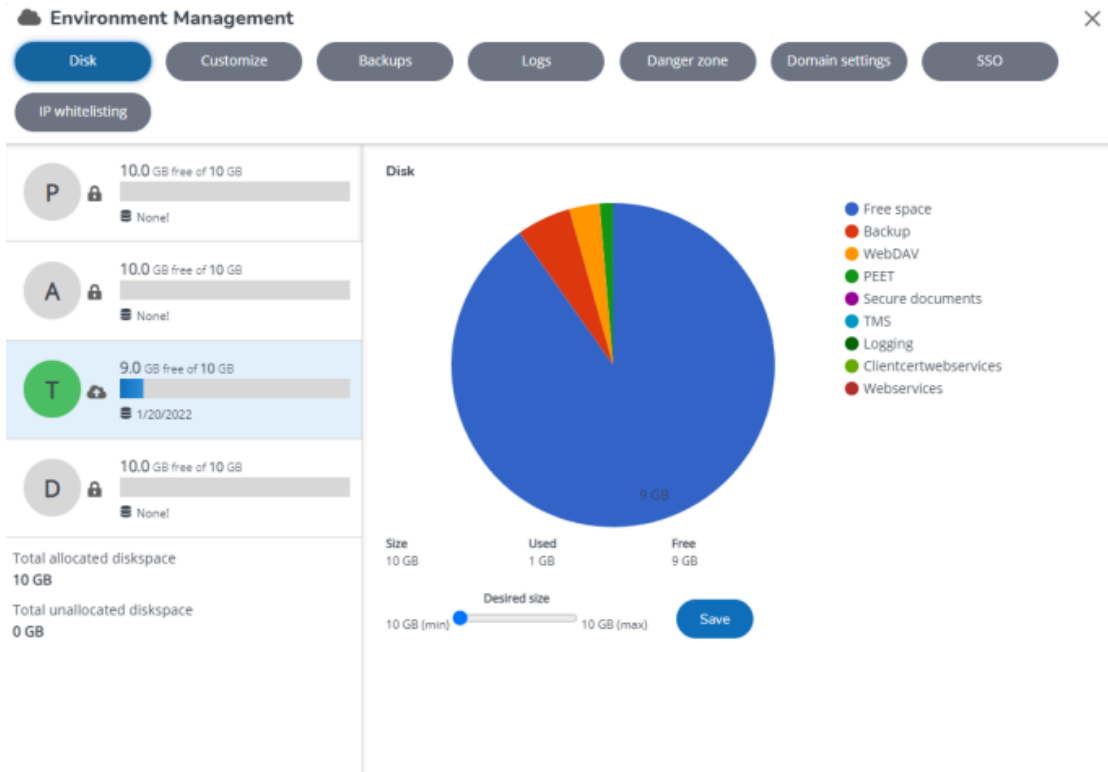
Clicking the Cloud gadget's details icon  opens the **Environment Management** details, listing the following tabs:

- [Disk\\*](#)
- [Customize](#)
- [Backups](#)
- [Logs](#)
- [Danger zone\\*](#)
- [Domain settings](#)
- [SSO](#)
- [IP whitelisting](#)
- [Alerts](#)

 \* The functionality on most tabs relates to your current environment. On the **Disk** and **Danger zone** tabs, however, if enabled, you can also make settings for DTAP environments other than your current environment. Here, simply click any of the other environments and perform the actions that are available.

### Disk

Displays the environment's disk space usage in the Cloud. The chart legend indicates the components of the disk space usage.



Use the slider to allocate additional disk space to an environment (if available). In a Production environment, you can also change the disk allocation for other environments (the other way around is not possible).

**i** You cannot allocate less than 10 GB or less than the current instance usage.

To allocate extra disk space

#### Procedure

1. Select the instance whose total disk space you want to change.
2. Use the **slider** to select the correct amount of disk space.

**i** If less than 5 GB is available, you can either add it or not (typically increments of 5 GB are used).

3. Click **Save**. The settings are saved.

## Customize

On this tab you can customize / configure:

- the **Welcome page image**, the background image that is displayed when starting up the application.
- the **Favicon image** of your Planon application, the icon that serves as a visual reminder of the website identity.

- the Planon **Login logo image**, this logo is displayed on top of the login screen.
- a **URL** to a redirect page that should be displayed if the Planon application is temporarily unavailable, for example due to technical issues, an upgrade or a restart.

The current welcome page image and the favicon image are displayed on the left.

## Customize

The screenshot displays the 'Environment Management' interface with a navigation bar containing 'Disk', 'Customise', 'Backups', 'Logs', 'Danger zone', 'Domain settings', and 'SSO'. The 'Customise' tab is active, showing settings for the welcome image, favicon, login page logo, and error page.

**Current welcome image:** A photograph of a hospital hallway with people in scrubs. To the right, there are options to 'Change the welcome image' (with a warning that it affects all users), 'Reset to factory settings', and a 'Restore original welcome image' button.

**Current favicon image:** A green circular icon. To the right, there are options to 'Change the favicon image' (with a warning that it affects all users), 'Reset to factory settings', and a 'Restore original favicon image' button.

**Current login page logo:** The Planon logo. To the right, there are options to 'Change the current login page logo' (with a warning that it affects all users), 'Reset to factory settings', and a 'Restore original login page logo' button.

**Error page:** A text area with the message: 'If the Planon application is unavailable (for example during an upgrade or restore process), please redirect to the following URL (starting with 'http://' or 'https://').' Below this is a text input field containing 'example: https://planonsoftware.com' and a 'Set URL' button.

## Procedure

1. To change the **Welcome page image**, drag & drop the file or click **Browse** and select an image file.  
The selected **Welcome page image** is displayed on the left.  
You can restore the original image by clicking **Restore original welcome image**.
2. To change the **Favicon image**, drag & drop the file or click **Browse** and select a new image file.  
The selected **Favicon image** is displayed on the left.  
You can restore the original image by clicking **Restore original favicon image**.
3. To change the **Login page logo**, drag & drop the file or click **Browse** and select a new image file.  
The selected **Login page logo** is displayed on the left.  
You can restore the original image by clicking **Restore original login page logo**.
4. To select the web page to which users must be redirected when their Planon environment is temporarily unavailable, enter the relevant URL in the **URL** field.  
If no redirection page is configured here, the default message *503 Service is temporarily unavailable* will be displayed.
5. Click **Apply** to save your changes.


## Backups

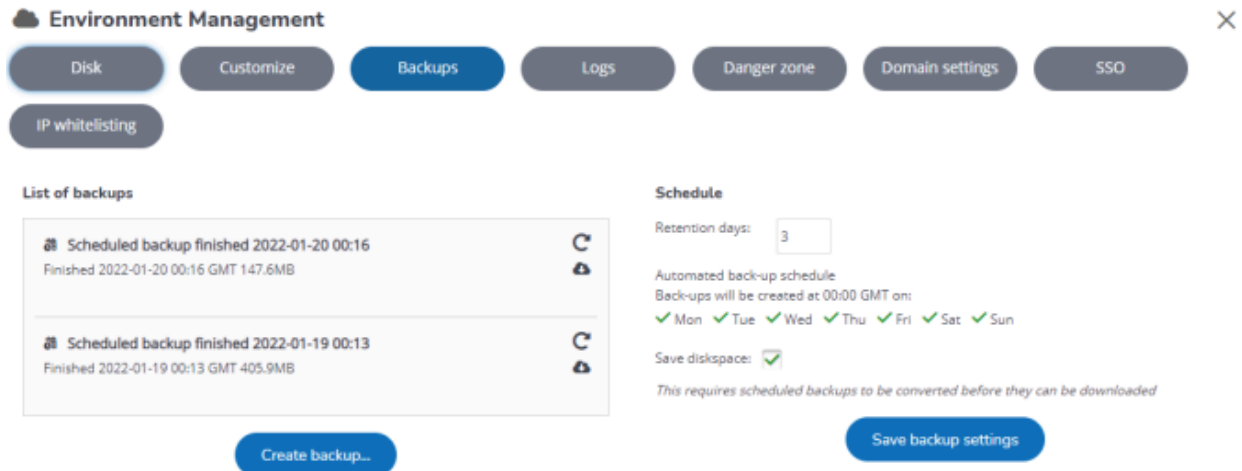
On this tab you can create backups that you can download to your computer at any time. You can download backups from a Cloud environment, but you cannot upload a backup to the Cloud again.

A Planon Cloud environment backup includes:

- Software version (release)
- Database
- File server (storing, for example, all WebDAV files)
- TMS
- Audit logs

Backups of the Production environment can be restored to any of the **Development**, **Test** and **Acceptance** (DTA) environments (the other way around is not possible). Only backups made on the **Production** environment can be restored to **Production**. Within the DTA environments, all backups are interchangeable.

 The encryption key to encrypt the passwords for access to external systems is unique for every environment, to prevent interference from DTA to Production. In general, this applies to the passwords in System Settings; for example, WebDAV, Connect for AutoCAD, Connect for Calendars (C4C) and default user passwords. This implies that if you restore Production to DTA, all these passwords have to be re entered before they will work again.




The screenshot shows the 'Environment Management' interface with a navigation bar containing buttons for 'Disk', 'Customize', 'Backups', 'Logs', 'Danger zone', 'Domain settings', and 'SSO'. Below the navigation bar, there is a 'List of backups' section with two entries: 'Scheduled backup finished 2022-01-20 00:16' (147.6MB) and 'Scheduled backup finished 2022-01-19 00:13' (405.9MB). To the right, the 'Schedule' section shows 'Retention days: 3', 'Automated back-up schedule' set to '00:00 GMT on: Mon, Tue, Wed, Thu, Fri, Sat, Sun', and 'Save disk space: checked'. A note states 'This requires scheduled backups to be converted before they can be downloaded'. At the bottom, there are 'Create backup...' and 'Save backup settings' buttons.

The database and the file server backups are automated to create the backups at scheduled times.

By default, an automated backup schedule is set up for a specific time on all the week days.

The automatic backup schedule is follows:

- A full backup is created each Saturday.

 The full backup that is created, is not necessarily always visible in the Cloud **Environment Management** gadget. The full backup will be used as the *master* for the incremental backups. Consequently, you may see this backup via WebDAV, but not in the gadget itself.

- If the **Save disk space** check box is selected, incremental backups of all files (the database backup always comprises the entire database) are created during the remaining days of the week. These incremental backups are created in small chunks that will have to be merged again when downloading an environment. (This does not affect exchanging backups).
- If the **Save disk space** check box is not selected, a full backup is created every day. This will consume disk space significantly.

## Manual backup

You can download a manual backup by clicking the **Download backup icon**.



- To improve efficiency and for reasons of performance, you can create a manual backup every two hours.
- While creating a backup, you cannot restore or edit it, until it is completed.
- To improve backup speed you can select to back up only the database. This backup can only be restored on Development, Test or Acceptance.

You can edit a manual backup and:

- Change the **Name** of the backup.
- Note down a relevant **Comment** about the backup.
- Select an **Expiry date**. By default, the expiry date is set to 3 months, which also is the maximum selectable expiry date.  
10 days prior to expiration, a notification will be shown on the Environment Management gadget. The manual backup that is going to expire will be highlighted. When this happens, you can:
  - Do nothing: the manual backup will be deleted after it is expired.
  - Extend the expiry date (up to 3 months).
  - Delete the manual backup (if it is obsolete).
  - Download the backup first to save it locally, then delete it from your environment.



The manual backup will be **permanently** deleted after the expiry date.

To edit manual backup details:

### Procedure

1. Choose the manual backup that you want to edit.
2. Click the **Edit** icon. A pop-up opens.
3. Modify the manual backup details.

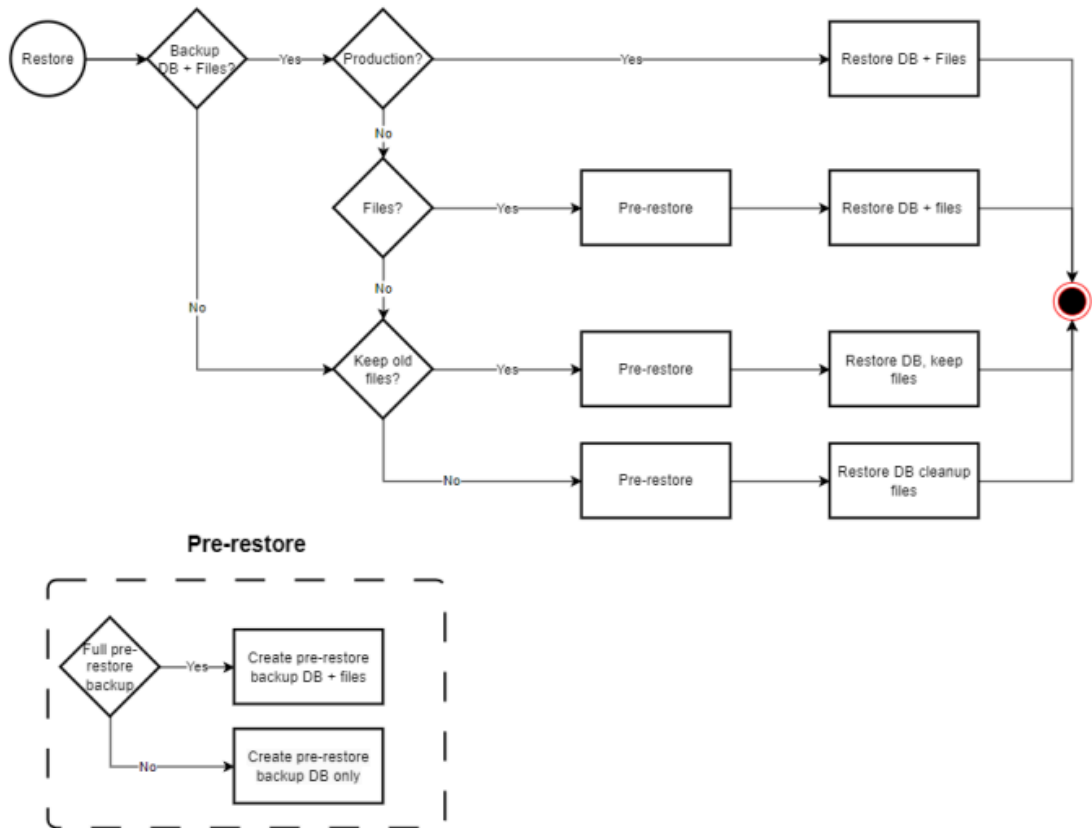


You cannot make a manual backup when the environment is out of disk space. In such a situation, please consider cleaning up older backups or allocating more disk space. After a manual/ automated deletion of a backup, it will take up to 24 hours to free up the disk space.

To improve efficiency and for reasons of performance, you can only make a manual backup every two hours.

## Restoring a backup

You can restore a backup from the list of backups available on the gadget.




## Procedure


1. Select a backup that you want to restore and click Restore .

**The Restore backup pop-up appears.**

2. Click Restore backup.
3. Select the instance (DTAP) the backup should be restored to.
4. If available for the selected instance, you can decide not to include Files in your restore.

 If you clear the **Files** check box, the restore will be much faster because only the database is restored. The files will be purged, when you clear the check box, a warning message will appear to notify you of the impending file purge.

5. In the Restore all user passwords to the initial password option, select Yes, if you want to reset all the user passwords to the default password. Users will then be prompted to change their password when logging on. If you select No, the user will retain their password.
6. Click Restore backup to complete the process.

 While the backup restore is in progress, access to the environment where the backup is restored to is disabled.

Please note: Restoring a backup to a *non-production environment* (Acceptance / Test / Development) will:



- disable all **scheduled tasks and restore the original license**.
- disable all User extensions
- deactivate all **active Platform Apps**, unless the app developer explicitly indicated in the app that the app can remain 'Active'. Apps with other statuses than 'Active', such as 'Failed', 'Install', and so on will retain their current status.
- The access key used to encrypt and decrypt passwords for connections to external systems, such as WebDAV, Connect for AutoCAD, Connect for Calendars (C4C), and default user passwords, is unique per installation. This prevents interference from DTA to Prod. Consequently, you need to re-enter passwords if you restore Prod to DTA.

If you restore a backup to a *production environment*, active apps will not be deactivated. They will retain their 'Active' status.

## Restoring files from a backup


You can restore a specific set of files, for example when a WebDAV file has been overwritten with a wrong version.

### Procedure


1. Select the backup that contains the working version of your file and click the  button. The **Download a backup** pop-up appears.
2. Click **Prepare: Download files**. The pop-up closes. The status will show **Conversion requested**.
3. After a few minutes refresh the page and wait until the status changes to **Finished**.
4. Click the  button and click **Download files** to download a zip archive containing your files.

### Other backup settings

---

Field	Description
Retention period (in days)	<div data-bbox="558 1556 1317 1648" style="border: 1px solid black; padding: 2px;"> Retention defines the period a backup is retained and can be restored. The maximum retention period is 365 days.</div> <p>For each environment there is an allowed minimum number of retention period:</p> <ul style="list-style-type: none"><li>• Development - 1 day</li><li>• Test - 1 day</li><li>• Acceptance - 1 day</li></ul>



Field	Description
Save disk space	<ul style="list-style-type: none"> <li>Production - 7 days</li> </ul> <p>Select the <b>Save disk space</b> check box to enable incremental backups. This splits backups into smaller chunks during the backup process to save lot disk space.</p> <div style="border: 1px solid #0070C0; padding: 5px;"> <p> This procedure, takes more time while downloading the backups, because merging chunks into a whole backup takes extra time.</p> </div>

**Always click Save backup settings to save your changes.**

### Frequently asked questions


The following list provides an overview of Frequently Asked Questions.

Question	Answer
File settings are copied over automatically, which is good to know. These need to be set back to the URL for the <b>Acceptance</b> environment. Is that a manual change that needs to be done afterwards?	<p>All file locations/configurations are set correctly for the specific environment. Cloud takes care of all the configuration.</p> <p>The Enterprise Talk locations will have the values as specified in the <a href="#">Environment delivery information</a> for that specific environment, the same for Web configuration.</p> <p>Regarding URLs, no manual action is required after restoring a backup.</p>
Will the 'Acceptance icon' at the top of the screen be replaced by a DB restore from <b>Production</b> , and be replaced by a different icon and name?	<p>The <b>Acceptance</b> environment will always have <b>Acceptance</b> icon at the top of the screen. <b>Test</b> and <b>Development</b> each have their own icons, no matter what backup you restore.</p> <p>Your <b>Production</b> environment will not display an icon.</p>

## Cloning a Cloud environment

By using the **Clone** feature, you can clone a Cloud environment to another Cloud environment.

This feature can, for example, be used for cloning a Cloud project street to a Cloud production street.

<p> This feature is not available by default. If you want to use the cloning feature, please contact <a href="#">Planon support</a>.</p>
---

### Creating a clone

1. In the Environment Management gadget > Backup tab, select a *manual* backup of the environment that you want to copy to another environment.


**If you do not have a manually created backup yet, create one first, as cloning is not possible for scheduled backups.**

2. Select this backup to be used as a *clone*.
3. Click Download... and click Generate clone voucher.

**Within a couple of seconds, a backup voucher is displayed. This unique voucher can be shared / stored and used to import it to another Cloud environment.**

 This backup voucher is valid for 1 week. After that, a new voucher needs to be generated.

## Importing a clone

 This feature is not available by default. If you want to use the cloning feature, please contact [Planon support](#).

This procedure can be performed on another Cloud environment

1. On the Backup tab, click Import Clone....
2. Enter the voucher and click Import Clone... again.


**The import process will now start. After a while, the clone will be visible in the List of backups.**

3. You can now restore the clone to the environment.

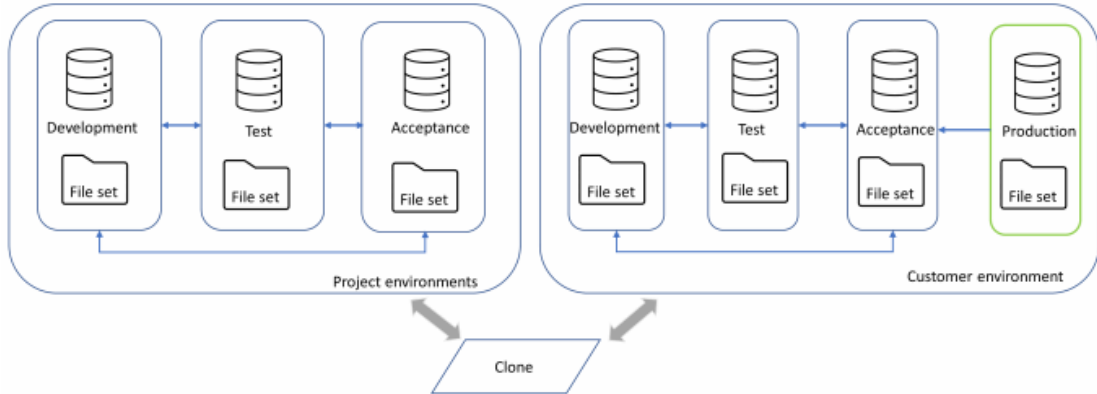
**This is the same procedure as for [Restoring a backup](#).**

### An example...

You are working in your Cloud project environment. In this environment, you can use the standard backup feature to create/restore, move files, data and configuration between other instances. When you are done configuring, you may want to copy your whole environment to another Cloud environment. If this is a different Cloud environment, you can only use the Clone feature.

 You cannot import a clone into a Production environment.

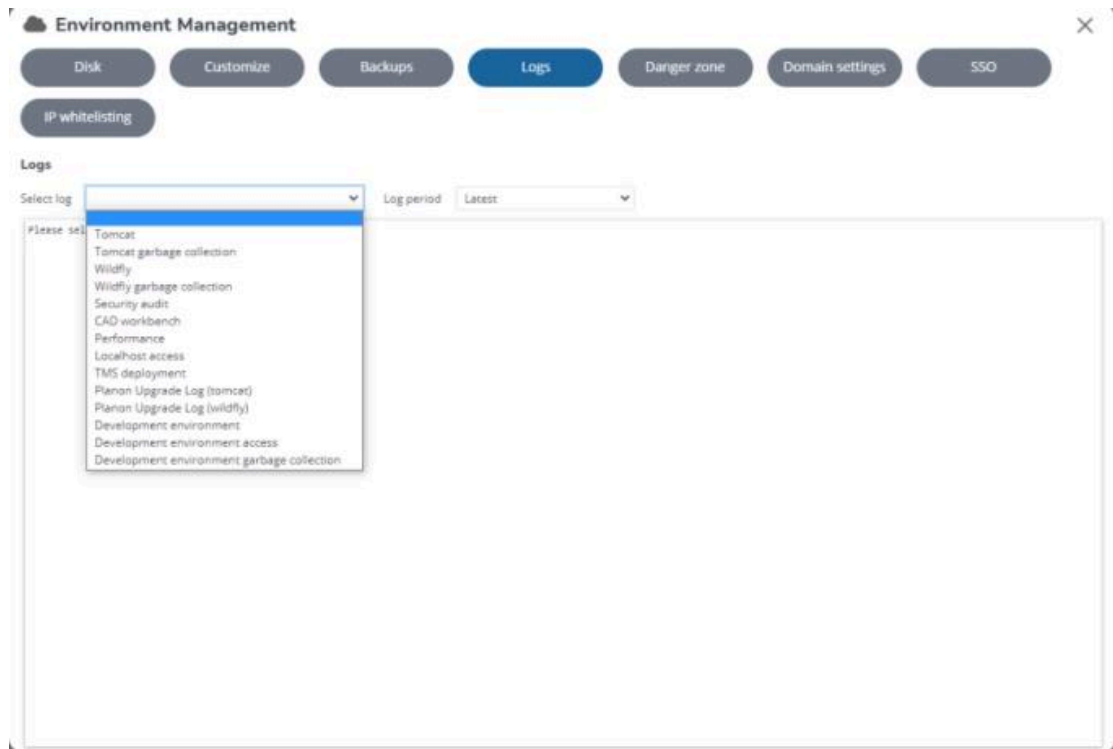
### Overview of backup and clone functionality



## Logs

On the **Logs** tab, you can view or download the required logging for your environment. This can be helpful for analysis, or in order to share logs with Planon Support.

## Logs



- Select the log file you want to view / download

- Select the log period



If you select **Latest**, the logging is shown real-time. When you scroll to the top, a new set of 5000 lines will be displayed. New log lines will be added at the bottom of the log viewer. When new lines are being added to the log file, the focus will remain on the data in selection.

- When selecting a log period other than **Latest**, the log is not displayed but you can download it.
- When you select a specific date, a full 24 hours of data is displayed (starting at 00:00 - 23:59).
- Logs will be available for
  - a day in the last week
  - two weeks
  - a month
- Select **All** to download all log files at once - you can then download a zip file containing all logs for the selected period.



For a description of the contents and the difference of the available log files, see [Log file contents](#).

## Log file contents


The following overview describes which content you can find in the various logs available in the **Environment Management** gadget.

Log file new	Log file old	Description
Tomcat	catalina.out tomcat_startup.log c4c.log c4o.log kiosk.log mobile.log pss2.log sdk.log	The web server main log file.
Wildfly	server.log wildfly_startup.log	The application server's main log file.
Security audit	securityaudit.log	If you want to log the login and logout timings of the users (in the selected user group), go to the <b>User groups TSI &gt;</b>

<b>Log file new</b>	<b>Log file old</b>	<b>Description</b>
		<b>User groups</b> and enable the <a href="#">Additional security logging</a> .
CAD workbench	(new)	CAD workbench log.
Performance	perfmonstandard.log	Irrespective of whether performance logging is enabled, the application will always log basic performance data in this log file.
Performance (Extended)	perfmon.log	When performance logging is enabled, next to the Performance data field in the application this log files also contains the results, which will also contain PSS2 - and runtime proxy view data - if enabled.
Localhost access	localhost_access_log.txt	Web server access log, information about the users entering the system.
Planon Upgrade Log (tomcat)	Clientupgrade.log	Client upgrade log.
Planon Upgrade Log (wildfly)	upgrade.log	Upgrade information
Development environment	(new)	Workspace logging for Planon as a Platform.
Development environment access	(new)	Workspace logging for Planon as a Platform.
Development environment garbage collection	(new)	Workspace logging for Planon as a Platform.
No longer available	TMS-deployed.out	List of all deployed TMS, also available

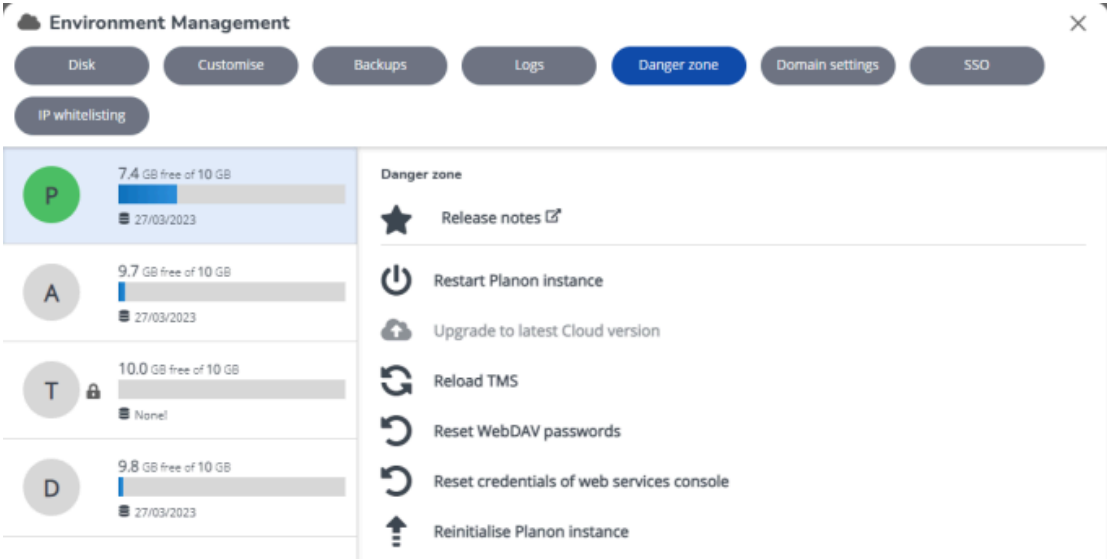
Log file new	Log file old	Description
No longer available	startup_script.log	in the User extension usage report.
No longer available	Clientcert_access_log.txt	OpenShift log, which is no longer available in the new setup.
No longer available	audit.log	Mutual SSL for Nyx, no longer supported.
No longer available	audit.log	Old audit log file, no longer supported, see <a href="#">security audit log file</a> for the information that was in this file.

## Danger zone

 This tab is called **Danger zone** because actions on this tab can affect all environment users, such as, **Restart Planon instance**.

This tab displays the Planon environments in the left panel and the actions you can perform on these environments in the right panel. These actions can be performed only when the environment is available and not locked.

The actions can only be performed for the environment to which the user is logged on, with the exception of Production. From the Production environment, it is possible to execute these actions for all other DTA environments.



**Environment Management**

Disk Customise Backups Logs **Danger zone** Domain settings SSO

IP whitelisting

Environment	Free Space	Last Update
P	7.4 GB free of 10 GB	27/03/2023
A	9.7 GB free of 10 GB	27/03/2023
T	10.0 GB free of 10 GB	None!
D	9.8 GB free of 10 GB	27/03/2023

**Danger zone**

- ★ Release notes [↗](#)
- ⏻ Restart Planon instance
- 📦 Upgrade to latest Cloud version
- 🔄 Reload TMS
- 🔄 Reset WebDAV passwords
- 🔄 Reset credentials of web services console
- ⬆️ Reinitialise Planon instance

## Environment credentials

As from Planon L96, a more modern method is introduced to deliver Planon Cloud environment credentials. All environment credentials, such as WebDAV and Web services, can subsequently be obtained and administered via the Environment Management gadget.

If you need to retrieve the credentials on first use or have lost your credentials, you can reset them on this page. In compliance with security standards, environment credentials will only be shown once - customers performing a reset will be guided through the process via the user interface.

Planon urges customers to safely and securely store credentials.


## Available actions

The following actions can be performed in the right panel.

- **Release notes:** A shortcut to the [Online Release Notes](#).
- **Restart Planon instance:** Perform this action, only if you are absolutely sure that you need to restart an environment.



All users of this Planon environment will be affected by this action.

- Scheduled tasks on Acceptance, Test and Development environments will be disabled.
- The  icon is displayed if there is a hotfix available on the current version of your Planon application. Restarting your Planon instance, automatically applies the available hotfix.
- Restarting a Planon instance, will **restore the original license** and in all non-production environments **disable all scheduled tasks**.
- You can restart **Now** or specify a **Schedule** in the date-time picker. When using a schedule, the restart will happen automatically at the specified date-time. (You can also cancel the schedule).

- **Upgrade to latest Cloud version:** Perform this action, only if you want to upgrade the environment to the latest version. Note that all users of this Planon environment will be affected. Also, during the upgrade, the environment will not be available for use. To help you schedule the upgrade effectively, the gadget will show the total time of the previous upgrade.



- This option is disabled if there is no latest version available.
- DTA environments can be independently upgraded to the latest release version.
- In order to be able to upgrade, all (available) DTA environments must have the same release version.

## Upgrade

Because a full upgrade (database and files) can take quite some time, you can choose to upgrade only the database. The upgrade will then be much faster.

- **Now**
- **Scheduled**

Click **Next** to proceed. In the following screen you can indicate whether to:

- **Back up database and files**
- **Back up database only, to speed up throughput time**

You can use the last available backup (scheduled or manual) to restore the environment, if required.

- **Reload TMS:** Perform this action to reload **TMS solutions**. All the available solutions will be enabled by this action.
- **Reset WebDAV passwords:** Use this feature to reset the passwords for various WebDAV accounts. The selected password(s) will be shown once after the reset.



The password that is generated, consists of 10 to 17 characters and can contain the following characters: 0-9 a-z A-Z !#\$%^\*(){}[]\_

- **Reset credentials of Web services console:** Use this feature to reset the password for the Web services console (NYX). The selected password(s) will be shown once after the reset.
- **Reinitialize Planon instance:** This action is intended for the initial deployment of a Planon Cloud environment. This feature is meant for Planon staff as it requires a best practice key which is only available within Planon internally.



*Planon-internal:* When using this action, the current environment will be overwritten with a best practice environment, a backup of the initial database will automatically be created.

### *Reset service passwords (WebDAV and Web service console)*

## Reset service passwords (WebDAV and Web service console)

For security reasons, it is possible to reset service passwords for WebDAV and Web service console (NYX).

- If used, the new password(s) are shown, one time only, in the Environment Management gadget after a reset. After closing the one-time window, the credentials can no longer be shown again for security reasons.
- These administrative interfaces should only be used by administrators or services.



- These administrative interfaces are not part of the regular end-user access to Planon Universe.
- Since these services are used by other services, Multi-Factor Authentication (MFA) is not possible.
- Access to these administrative interfaces requires authentication based on user name and password. Both user name and password are randomly generated and consists of 10 to 17 characters.
- For WebDAV, there is a lockout mechanism that locks the service account for a certain time if the correct user name is used in combination with several invalid password attempts.



If you reset the WebDAV password and you have a clustered (multiple application servers and/or web servers) you need to restart your environment, before the new password works.

### *Danger zone*

## Improved features

**Improved Features** displays a list of pending new features that the customer can either immediately start using or postpone using until a specified deadline. During this time frame, customers can take action required to prepare for the implementation of the new feature.

Whenever the implementation deadline of an improved feature has passed and the feature is not switched on, Cloud customers will now be notified before upgrading to a newer version.

1. When opening the Planon application, Cloud customers may notice in the Environment Management gadget that an upgrade is available. When proceeding to upgrade their environment (Environment Management gadget > Danger zone tab > Upgrade to latest Cloud version) and they still have improved feature(s) pending to be activated, they will now receive a notification pop-up.
2. The pop-up lists the improved feature(s) whose implementation deadline has/have passed. Customers can then decide to Cancel or Continue with the upgrade.
  - **Cancel**  
You can manually activate the improved feature before upgrading by going to **System Settings > Improved Features** and activating the required feature(s). Subsequently, you can then resume the upgrade.
  - **Continue**  
You are prompted to confirm starting the upgrade. After confirming, the upgrade will start and the pending improved feature(s) whose preparation deadline has/have passed will be activated.



For more information, see [Improved Features](#).

## Domain settings

On this tab you can configure your own domain aliasing for your individual Planon instances.



- Only one domain alias is allowed at a time. Adding another will delete the current one.
- When SSO is enabled in your environment, please make sure to first follow the instructions for enabling the [Privacy Sandbox compatibility](#) before enabling the Custom Domain.



When SSO is enabled in your environment, please modify the configuration in the Identity Broker Solution to allow the new to be configured Custom Domain URL as a valid redirect URL in the Planon Client. For more information, see [Custom domain allowance](#) (Cloud Configuration).

- In the **Domain name** field, enter the domain alias name that you want to configure.
- Choose files and upload SSL certificate, SSL chain and Private key.
- Finally save the domain settings.

A message is displayed when the domain alias is set successfully.

### Certificate requirements

- Certificate files must be Base64 PEM-encoded and typically have a .crt or .pem extension.
- Private key file must be a RSA or DSA private key file for the root certificate in PEM-encoded format.
- Other certificate and/or private key formats will not be loaded and will return an error message.

**Environment Management** X

[Disk](#)
[Customize](#)
[Backups](#)
[Logs](#)
[Danger zone](#)
[Domain settings](#)
[SSO](#)

[IP whitelisting](#)

**Domain alias**

A domain alias enables you to configure your own domain name for aaras78demo-test.plnd.cloud. Make sure the CNAME record is set up with your DNS provider. Next, configure Planon to use your alias.

Domain alias \*

Upload an SSL-certificate\* [Choose File...](#)

Upload an SSL-chain\* [Choose File...](#)

Upload a private key\* [Choose File...](#)

Private Key Pass Phrase

[Upload and save](#)


For more information on certificates, see [Custom URLs and certificates](#).

### DNS administration

Finally, the customer's DNS administrator needs to create a reference to the original Planon URL via a CNAME record (DNS alias). Also, the DNS administrator is responsible for maintaining this certificate.

## Custom URLs and certificates

The following steps are an example.

 If you require assistance with the configuration, please contact your account manager.

### Prerequisites

- Make sure you have installed openssl on your device.
  - Make sure you have the pfx password.
1. Open a command box and go to the openssl\bin installation folder.
  2. Execute the following commands:

**Change the location for the `-in` and `-out` parameters and make sure to use the pfx password for all passwords requested in these commands.**

a. Private key

```
openssl pkcs12 -in file.pfx -nocerts -out filekeyfileencrypted.key
```

```
openssl rsa -in filekeyfileencrypted.key -aes128 -outform PEM -out filekeyfileencryptedpem.key
```

b. Certificate

```
openssl pkcs12 -in file.pfx -clcerts -nokeys -out filecert.crt
```

c. Chain

```
openssl pkcs12 -in file.pfx -cacerts -nokeys -out filechain.crt
```


**Additional configuration**

If you are using SSO/KeyCloak, you must complete the following steps also:


1. Login on the KeyCloak admin page
2. Go to the clients
3. Click on Planon
4. Search for the field 'valid redirect URIs'
5. Add your custom URL (change the URL): <https://newcustomurl.com/>\*

## Enabling a portal integration in the Cloud

To enable clients to include Self-Service forms in a client portal.

 With the upcoming deprecation of third party cookie support by Google (see [Privacy Sandbox for the Web](#) for more information), the Planon Self-Service integration support will become deprecated per January 1<sup>st</sup> 2024. To maintain the same functionality, the link should be opened in a new browser tab instead of using an iframe.

Customers would like to embed Self-Service forms in their portal, which has now been made possible by specifying and enabling your portal URL.

-  • As a precondition, domain settings must be configured in order to use **Portal integration**. The domain alias is required for end user access.
- Contact Planon Support to enable Portal integration for your Cloud environment. The Cloud environment needs to be prepared to be able to switch it on.

After completing your domain settings and saving them, a number of new settings will be available after refreshing your page.

1. Enter your Portal URL.

**It is only possible to use one portal URL. When ready, set the Enabled field to Yes.**

 As long as this field is **No**, the portal will not be able to display the forms.

2. Click Save portal URL.

**Once the Enabled field is set to Yes, you can embed the Self-Service form URLs in your portal. The link between your portal and your Planon environment is established.**

3. If the customer has enabled SSO, the configuration in the Identity Broker must be updated. In Clients > Planon, add both the domain alias and the portal URL in the Valid redirect URIs field and in the Web Origins field.

### Example

Customer has a portal and wants to include Self-Service forms:

- Portal is running under domain: <https://portal.customer.com>
- Planon Cloud environment is running at: <https://customer-prod.planoncloud.com>
- Customer has set up a domain alias at: <https://facilities.customer.com>
- End user access is via: <https://facilities.customer.com>
- Gadget is configured to have portal integration as source: <https://portal.customer.com>
- Portal contains iframes with link to: [customer-prod.planoncloud.com/case/BP/..](https://customer-prod.planoncloud.com/case/BP/)

## Mutual SSL settings

It is possible to add trusted CAs via the Environment Management gadget into Planon. When saved, the keys will be stored.

**i** If you want to use this feature it must be enabled first. Submit a request at Planon Global Support to have this feature activated.

1. Put the public key of the CA in the **Mutual SSL** field. The field is only visible if Mutual SSL is enabled for your environment.

The screenshot shows the 'Environment Management' interface with several tabs: Disk, Customise, Backups, Logs, Danger zone, Domain settings, and SSO. The 'Domain settings' tab is active. Under 'Domain alias', there is a text input field and a 'Choose File...' button. Below that are three more 'Choose File...' buttons for 'Upload an SSL-certificate\*', 'Upload an SSL-chain\*', and 'Upload a private key\*'. A 'Private Key Pass Phrase' field with a toggle for visibility is also present. At the bottom, there is a 'Mutual SSL' section with a text area for entering public keys and a 'Save keys' button. The text area contains the placeholder text 'Please provide your CA keys here...'.

If you have multiple CAs, separate them with a new line as shown in the following example:

**Example**

```
-----BEGIN CERTIFICATE-----
MIIHcjCCBlqgAwIBAgIQBalcDTSoMfN/il9ynMI8dDANBgkqhkiG9w0BAQsFADBw
```

```

MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
8lmJTFTb3chy1pgBs1m+5HMIUsB/pHBXMNQy6vvlKX322p+n4SxbGawq6HUiriJn
JygAmoBouOPh1iLhmVbwb+8bJVHjQGT7NQQO/Ey5YCsEzRX5bOpKaMzLjuB7NKiM
boP5kFGg/O83SyabEtWcDjxDvndb44xCJXJbAjVdqM1OI7V0Mt0=
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----

MIIHcjCCBlqgAwIBAgIQBalcDTSoMfN/il9ynMI8dDANBgkqhkiG9w0BAQsFADBw
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
8lmJTFTb3chy1pgBs1m+5HMIUsB/pHBXMNQy6vvlKX322p+n4SxbGawq6HUiriJn
JygAmoBouOPh1iLhmVbwb+8bJVHjQGT7NQQO/Ey5YCsEzRX5bOpKaMzLjuB7NKiM
boP5kFGg/O83SyabEtWcDjxDvndb44xCJXJbAjVdqM1OI7V0Mt0=
-----END CERTIFICATE-----

```

2. Finally, save the keys.

**A message is displayed indicating that the CA is saved, but not yet effective until a restart of the environment. You can restart the environment later.**

3. Use the following URL to check if mutual SSL is working: <https://environmentname-dtaorp-tls.planoncloud.com/clientcertnyx>

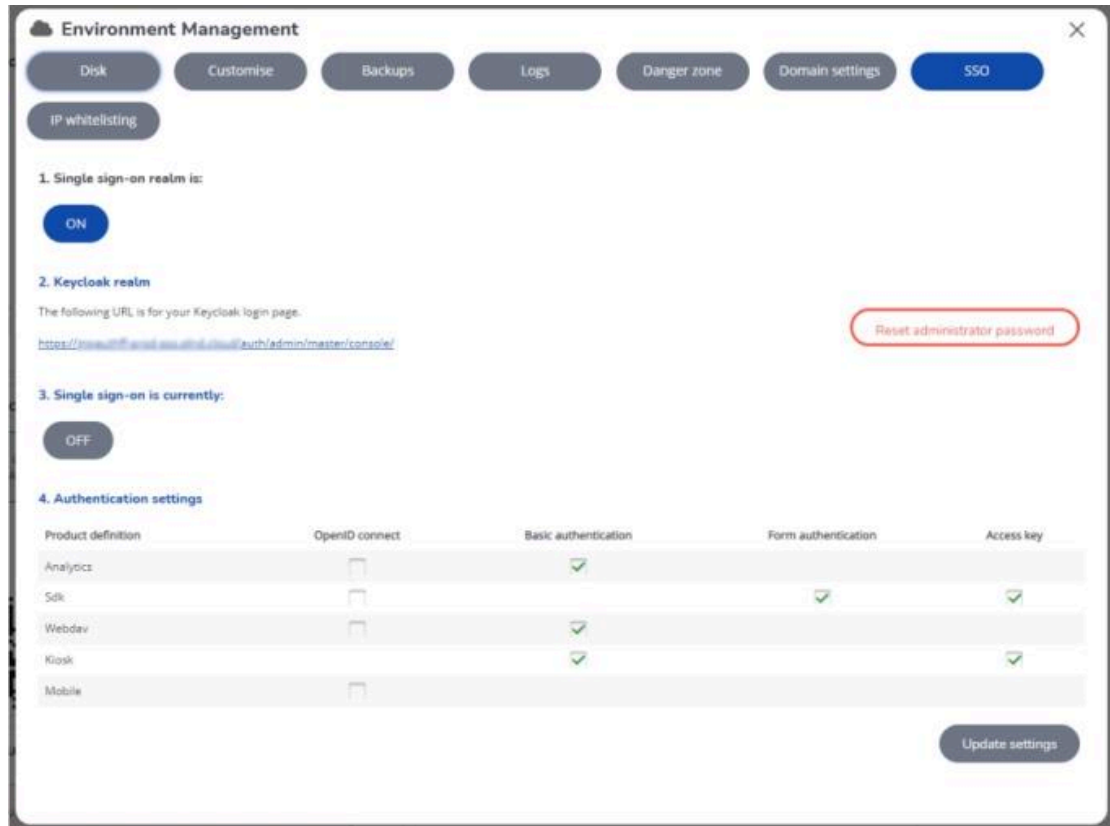
To use this URL, first replace the parameters **environment** and **dtaorp** with the corresponding names in your own specific set-up.

If everything is configured as expected, the browser will prompt you to select the certificate when you browse to this URL.

## SSO

When you are enabling SSO and click the tab for the first time, only a button is displayed indicating that the single-sign-on realm is **Off**.

## SSO



**i** A realm is used to manage a set of users, credentials, roles, and groups. A user belongs to and logs into a realm. Realms are isolated from one another and can only manage and authenticate the users that they control.

Consequently, you first need to create a realm.

1. Click the **Off** button.  
A warning message appears asking you to confirm enabling SSO.
2. Click **Enable SSO realm**.  
The log in credentials appear (user name & password).
3. Store these credentials safely for later use. When this is done, select the check box and click **Continue**.

**i** If you misplace the credentials, you can reset the admin password here.

Your Keycloak environment is created, the login URL is displayed. You have finished creating the realm. Now, you can enable SSO.

4. In **3. Single-sign on is currently**, click the **Off** button to enable SSO.

**!** A warning message appears. Read it carefully - restarting your environment may have some serious implications.

5. It is possible to switch the authentication method of the Connect for Analytics solution to OpenID Connect authentication.  
Additional configuration of your BI Tool is required, for more information please contact Planon Support.
6. It is possible to switch the SDK authentication method to OpenID Connect authentication.  
Additional configuration is required, for more information please see [OpenID Connect](#).
7. It is possible to switch the authentication method of WebDAV to OpenID connect authentication.  
Additional configuration is required, for more information see [OpenID Connect > WebDAV](#).
8. It is possible to switch the authentication method for Mobile to OpenID connect authentication.  
For more information see [OpenID Connect > Mobile](#).
9. Click **Save & rebuild**.  
You have enabled SSO.



If you later disable SSO, the configuration will remain, but will be hidden.

## OpenID Connect

It is possible to switch the Planon SDK to OpenID Connect (OIDC) authentication in the Environment management gadget.



This will currently break the Planon AutoCAD Plugin implementation, so if the Planon AutoCAD Plugin integration is used, do not switch your environment to OIDC authentication. This will be fixed in a newer version of Planon so that the Planon AutoCAD Plugin will support OpenID Connect in the near future.

The default behavior of the SDK is unchanged, this means if no additional configuration is done, form authentication and Planon access key is present.

Enabling OpenID connect disables form authentication. Planon Access key is optional supported in combination with OIDC, or Planon Access Key only. For more information, see the following table:

	<b>Form Authentication</b>	<b>Planon Access Key</b>	<b>OpenID Connect</b>
Option 1 (default)	Enabled	Enabled	Disabled
Option 2	Disabled	Enabled	Enabled
Option 3	Disabled	Disabled	Enabled



	Form Authentication	Planon Access Key	OpenID Connect
Option 4	Disabled	Enabled	Disabled

## Installation

### Planon Cloud configuration

1. Enable OpenID Connect authentication for SDK in the Environment Management gadget.

**i** In order to see this option, your environment must be running on the latest Cloud platform and SSO must be enabled.

2. In Keycloak, create a client with a self chosen client name (in the following image: *sdk-example1*). The root URL should be equal to the SDK interface URL.

The screenshot shows the 'Add Client' form in Keycloak. The 'Client ID' field contains 'sdk-example1', the 'Client Protocol' dropdown is set to 'openid-connect', and the 'Root URL' field contains 'https://customername-env.planoncloud.com/sdk'. There are 'Save' and 'Cancel' buttons at the bottom of the form.

3. In the next screen, configure the client to meet up to your security policies and save the changes.

**i** • Both **Client credentials** as well as **Authorization code flow** are supported.  
 • When using **Client credentials** flow make sure that **Service account** is enabled.

4. In Planon make sure a user is present that can be used by the configured client above. When **Client Credentials** flow is used, a service account user for the client must be present in Planon.

#### Example

If the client name is *sdk-example1*, then a user with the account name *service-account-sdk-example1* must be present and active in the Planon application.

## Usage

To get access to the SDK service via OpenID Connect, take the following steps:

1. Retrieve an access token at the keycloak service via the Client created in the installation step.
2. Send this token as Bearer token to the Planon SDK service.

## Troubleshooting

The following table lists a few common errors.

Error	Description
401 Unauthorized	Either no access token or an expired access token has been sent to the Planon application.
500 Internal error	The user account does not exist in the Planon application.

## WebDAV

When enabling OpenID connect for WebDAV, in addition to the configuration mentioned in this article, you must also assign product definitions to the proper user groups.

When using Basic authentication, you can log on to the various WebDAV locations by using your environment's credentials.

After enabling OpenID connect for WebDAV, these credentials will no longer work. Instead, please assign the various product definitions for WebDAV to the relevant user groups.

The following WebDAV product definitions will be available:

- WebDAV
- WebDAV\_Audit
- WebDAV\_Backup
- WebDAV\_PEET
- WebDAV\_TMS
- WebDAV\_Webservices

These product definitions will enable you to determine/authorize access to the various WebDAV locations.



Please note that assigning a WebDAV product definition to a user group is explicit. Without assigning WebDAV product definitions, no user can access WebDAV locations! See also: [Arranging access to Planon products](#) and subsequent articles.

## Mobile

The Planon Live app will use offline tokens when OIDC has been enabled. The advantage of using offline tokens is that users need to authenticate a lot less.

Default behavior is that after initial log in, a user can use the app without further authentication once per 30 days. If the user uses the app at least once per 29 days he/she can use the app without re-authentication for maximum 180 days (from the initial log in).

If an administrator wants to change the default timings, this is configured in the Identity Broker environment under Clients / PlanonMobile / Advanced Settings.

- Client Offline Session Idle = 30 days (default)
- Client Offline Session Max = 180 days (default)



Please make sure the Offline Session times are always longer than 1 hour!! If set to a shorter timing unexpected behavior will occur.

## Privacy sandbox compatibility

As of version L99, Planon provides the feature of Privacy sandbox compatibility. This feature ensures that your Planon cloud environment is compliant with upcoming deprecation of third party cookie support by Google (see [Privacy Sandbox for the Web](#) for more information).

- For environments enabling SSO the very first time, this feature is by default enabled.
- For existing customers already using SSO, additional configuration is required before this option can be enabled.

## Prerequisites

The configuration of the Identity Provider (IDP) needs to be modified before you can enable this setting. Kindly request your IT organization to expand the current SSO configuration (configuration of your external Identity Provider (IDP)) for your Planon environment.

Request to add two additional redirect URLs alongside the existing allowed redirect URL.

- The first URL should be identical to the existing URL, but without the "-sso" part in the hostname.
- The second URL should be customized to match your custom domain (if no custom domain is configured, only the first additional URL is needed).

## Example

Current redirect URL in the IDP configuration:

```
https://customerenvironment-prod-sso.planoncloud.com/auth/realms/planon/broker/saml/  
endpoint
```

First redirect URL to be added:

```
https://customerenvironment-prod.planoncloud.com/auth/realms/planon/broker/saml/endpoint
```

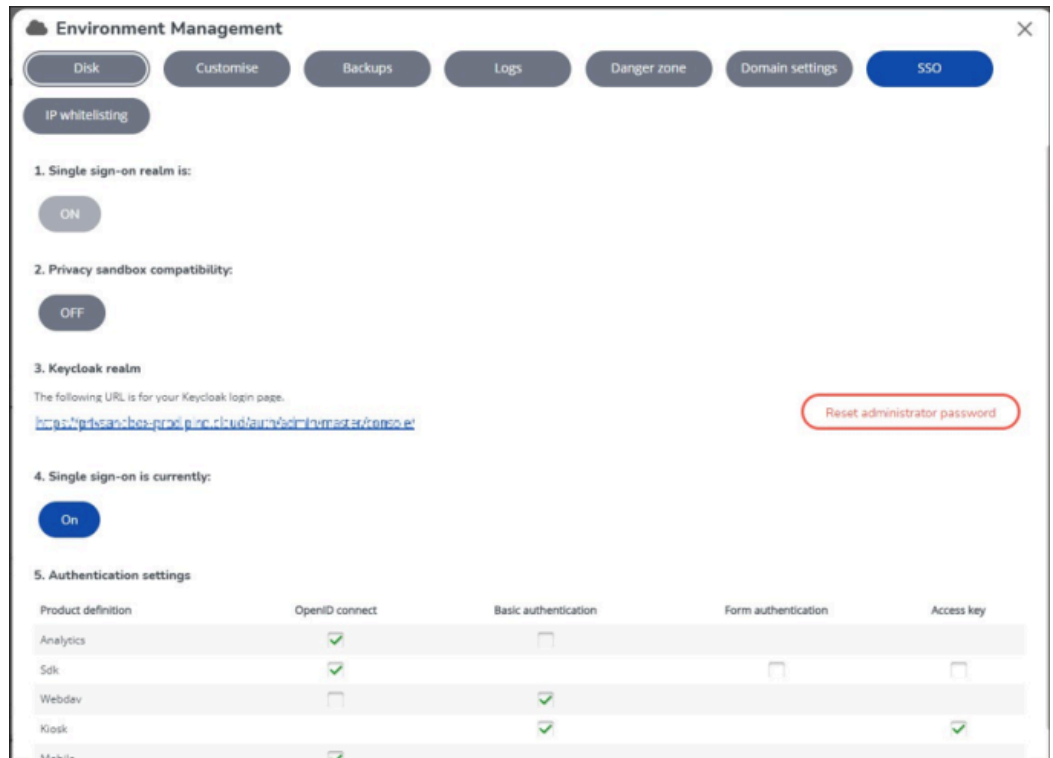
Optional, when a custom domain is configured (custom domain used in this example is `facilities.customer.com`):

```
https://facilities.customer.com/auth/realms/planon/broker/saml/endpoint
```

After the IT department confirmed the requested change, you can proceed.

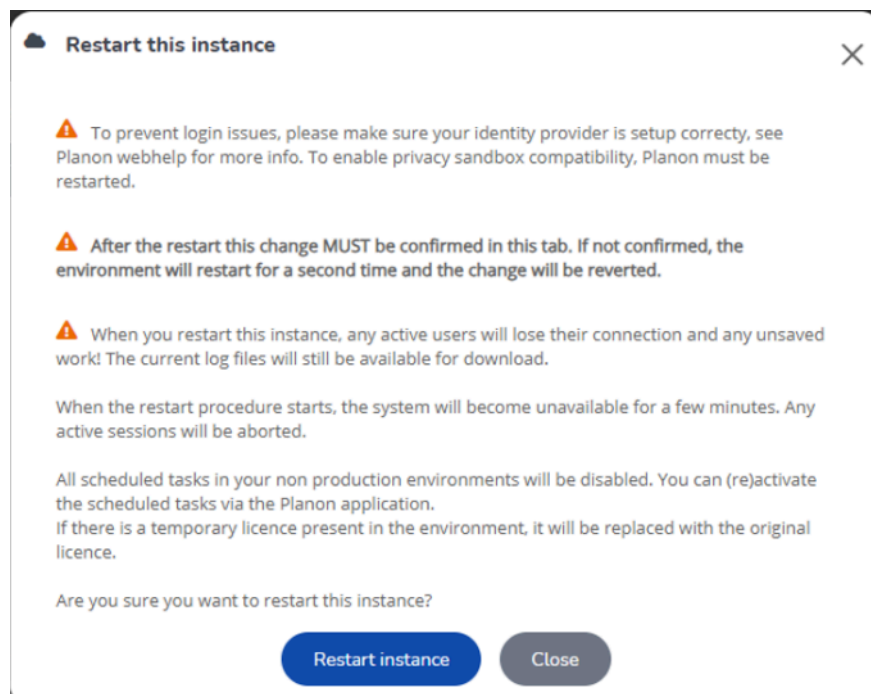
## Configuration

1. Enable the setting in the Environment Management gadget > **SSO** tab under the **Privacy sandbox compatibility** option by clicking the **OFF**



button.

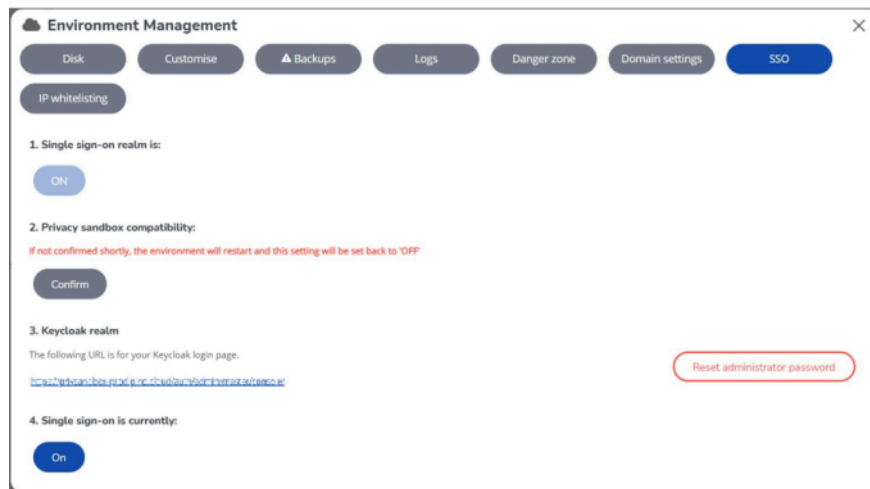
2. A pop-up will appear. Click **Restart Instance** to restart the environment.



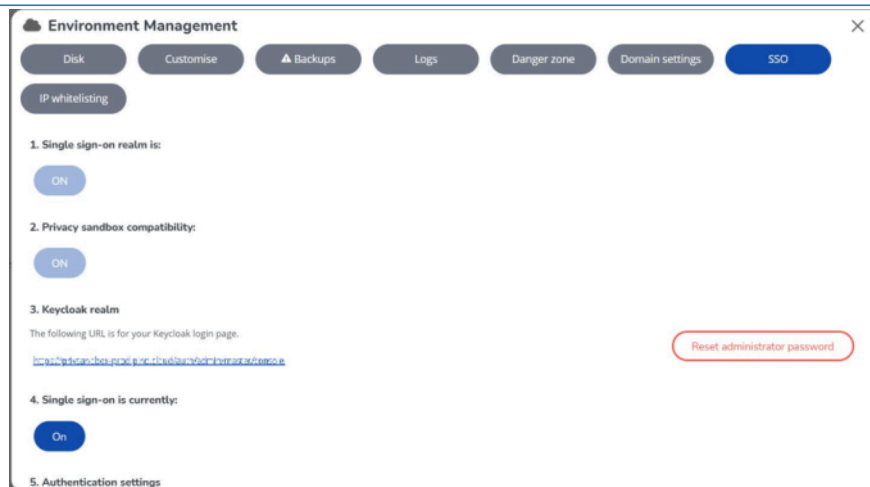


It is crucial that you log on to Planon and access the Planon Environment Management Gadget within 10 minutes after the environment restarts. **Always Log on to your environment via Single Sign On (not as supervisor).**

On the **SSO** tab, please verify that the change has been successfully implemented. If the confirmation is not confirmed within 10 minutes after the environment has restarted, the environment will restart for a second time and the change will be reverted. This step is essential to prevent any configuration errors resulting in making the Planon Cloud environment unusable.



After confirmation, please be aware that the option will be permanently enabled and cannot be disabled.



4. If a logoff URL is set for the environment, ensure it is updated to reflect the changes made.

If a custom domain is not used, remove the "-sso" part from the URL.

If a custom domain is configured, adjust the hostname to match the custom domain.

For more information about the logout functionality, please see [Logging out from Planon Cloud \(Cloud Configuration\)](#).

By following these steps, your Planon Cloud environment is future-proofed for the phasing out of third-party cookies.

## IP Whitelisting


IP whitelisting is a security feature for limiting and controlling access only to trusted users.

### IP whitelisting

The screenshot shows the 'Environment Management' interface with a navigation bar containing buttons for 'Disk', 'Customize', 'Backups', 'Logs', 'Danger zone', 'Domain settings', and 'SSO'. The 'IP whitelisting' button is highlighted in blue. Below the navigation bar, the 'IP whitelist' section displays 'Your IP Address: 37.251.24.65' and a note that IP whitelisting uses CIDR notation. There is a checkbox for 'Enable IP whitelist' which is currently unchecked. A text area below contains instructions: 'Please insert your IPs using CIDR notation; use a new line for each IP. For example: 192.168.1.100/32 192.168.2.250/32'. Below the text area is a field for 'Redirect blocked requests to the following url (starting with https:// or https://)', with an example 'https://planonsoftware.com'. A 'Save settings' button is located below the form. At the bottom, there is a table titled 'CIDR examples' with two columns: 'IP' and 'CIDR'.

IP	CIDR
192.168.1.100	192.168.1.100/32
192.168.1.100 & 192.168.2.250	192.168.1.100/32 192.168.2.250/32
192.168.1.*	192.168.1.0/24 192.168.1.100/30 192.168.1.104/29 192.168.1.112/28 192.168.1.128/26 192.168.1.192/29 192.168.1.200/32
192.168.1.100 192.168.1.200	

By specifying an IP addresses, you can grant access to these computers only.

-  To prevent excluding yourself, make sure you include your own IP address.
- Access to both Planon and Keycloak is limited by IP whitelisting.
- IP whitelisting is a licensed feature.

1. Select **Enable IP whitelist** to switch on the feature.

2. Enter the IP address of the computer for which you want provide access.  
The IP address notation should be in Classless Inter-Domain Routing (CIDR) format.
3. Enter a redirect URL to channel blocked requests to.  
Here, customers can provide a customized error page to which user will be redirected when they try to connect to Planon ProCenter via a wrong address. If this field is empty, the default 403 page will be displayed.
4. Click **Save IP settings**.



You have completed whitelisting.

## Alerts

On this tab, you can specify the email addresses of people who should be notified via e-mail if one of the following operations is completed:

- Creating a backup
- Creating a clone
- Restarting the environment
- Upgrading the environment
- Restoring the environment

These operations can take up a considerable time, hence it is useful to notify stakeholders via email once an operation is completed.



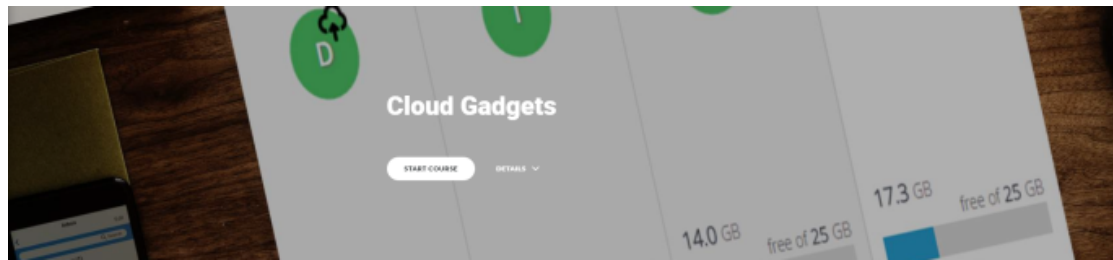
The screenshot shows the 'Alerts' configuration page within the 'Environment Management' interface. At the top, there is a navigation bar with buttons for 'Disk', 'Customise', 'Backups', 'Logs', 'Danger zone', 'Domain settings', and 'SSO'. Below this, the 'Alerts' button is highlighted. The main section is titled 'Email configuration' and contains the instruction: 'Provide one or multiple email address(es) that should be alerted during the following events.' There are five event categories, each with a text input field for email addresses: 'Planon started', 'Backup finished', 'Restore finished', 'Upgrade finished', and 'Clone created'. Each input field has a placeholder text: 'Please enter email addresses separated by comma (e.g. a@example.com, b@example.com)'.

1. Select the event and specify the recipients who should be notified.  
It is recommended to use a mailbox instead of a personal email address.  
You can add multiple recipients, separated by a comma (,).  
You can select all events and specify the recipient(s) or you can select individual events and specify the recipient(s).
2. Click **Save settings** to save your settings.

The recipients that are specified will be notified once the event(s) is/are completed (whether or not successful).

# Cloud e-learning

If you would further like to learn more about Cloud features, an e-learning module is available that touches on some of the features described earlier.



The e-learning provides a concise description of:

- Cloud computing
- The Planon Cloud
- Using Planon Gadgets
- Using the Environment Management Gadget
- (Creating) Backups

Finally, the e-learning includes some practical assignments for testing your understanding of the available Cloud features.

To access the e-learning module:

1. Open the following URL in your browser:
2. Click **Start module**.

# Index

## A

- Acceptance 5, 7
- accessing Planon Cloud Environment gadget 6
- Account credentials 22
- Alerts
  - tab 40
- Alias 28

## B

- Backup - FAQ 17
- Backups in cloud environment 12

## C

- Cloning a cloud environment
  - manual backup required 17
- Cloud e-learning 42
- Cloud environment details 9
- Custom URL 27
- Customize Cloud environment tab
  - favicon image 10
  - Login logo 10
  - service unavailable page URL 10
  - welcome image 10

## D

- Danger zone tab on cloud environment 22
- Development 5, 7
- disk space 9
- Domain 28
- Domain settings in a Cloud environment 26

## E

- Environment credentials 22

## I

- Importing a clone 18
- Improved feature 25
- IP Whitelisting 39

## L

- Logs 19
- Logs:

- garbage collection 20
- security audit 20
- Tomcat 20
- Wildfly 20

## M

- Mutual SSL
  - enable 29

## O

- OpenID Connect 32

## P

- PCC gadget 6, 7
- Portal integration: Cloud 28
- Privacy sandbox compatibility 35
- Production 5, 7

## R

- Reset passwords 22
- Reset service passwords 24
- Restore
  - files from backup 16
- restore backups 12
- Restoring a backup
  - deactivate Platform apps 14
  - disable scheduled tasks 14
- retention days 12

## S

- schedule backup 12
- SSO 30

## T

- Test 5, 7

## U

- Upgrade 25

## W

- Web service console
  - Password reset 24
- WebDAV
  - Password reset 24