



Cloud Services

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.

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

Service availability.....	6
Trust dashboard.....	6
Major problem.....	8
Minor problem.....	8
Notifications.....	8
SLA.....	9
History past 30 days.....	9
Cloud performance.....	9
Maintenance.....	11
Cloud Performance Testing.....	13
Accessing the portal.....	13
Requesting a performance test.....	13
URLS for performance testing.....	14
Testing in the Cloud.....	14
Cross site request forgery.....	15
Available APIs.....	15
API availability across software versions.....	15
Cloud System Management.....	17
Emailing in the Cloud.....	17
Uploading and configuring TMS.....	18
Availability gadget.....	21
Configuring availability reporting.....	23
Availability reporting.....	23
Single Sign On.....	25
Using SAML.....	25
The Planon identity broker solution.....	25

The SSO flow.....	25
Prerequisites - SAML assertion to be sent to Planon.....	27
Activating Keycloak.....	31
Configuring Keycloak.....	32
Replacing the certificate.....	34
Rearranging the mappers.....	34
Service Provider metadata.....	35
Custom domain allowance.....	36
Logging out of Planon Cloud.....	37
KeyCloak secure configuration considerations.....	38
Logging out from Planon Cloud.....	40
Logging out from Planon Cloud but not from IDP.....	41
Logging out from all used components.....	42
Testing the solution.....	43
SSO troubleshooting.....	44
Planon authentication.....	45
Overview.....	45
Configuring Planon User federation.....	47
Recommendations.....	50
Limitations.....	50
Logging.....	51
Security logging.....	51
Logging for anonymization.....	51
What is logged?.....	51
Software health check.....	55
Index.....	56

Service availability

Cloud SLA

Planon is working hard to ensure best customer satisfaction and offers an optimal working environment for its customers.

Availability of Production	99,5% based on 7x24x365 (excluding planned maintenance)
Recovery Time Objective (RTO)	8 hours
Recovery Point Objective (RPO)	24 hours



The environments that are in hibernation can be activated by accessing the provided URL. The instance will take a short while before it comes online. Only Production environments can have an SLA.

RPO of two hours

As a licensed feature for Premium Cloud only, it is possible to have a recovery point objective of 2 hours. An RPO of 2 hours is only possible for a disaster situation. A disaster is any unplanned interruption of Planon's operations (technical down-time not caused by human interaction).

This means that when a disaster occurs, Planon ensures that a maximum of 2 hours of data is lost.

Example

Disaster	RTO	RPO
12:00 AM	20:00 PM	10:00 AM

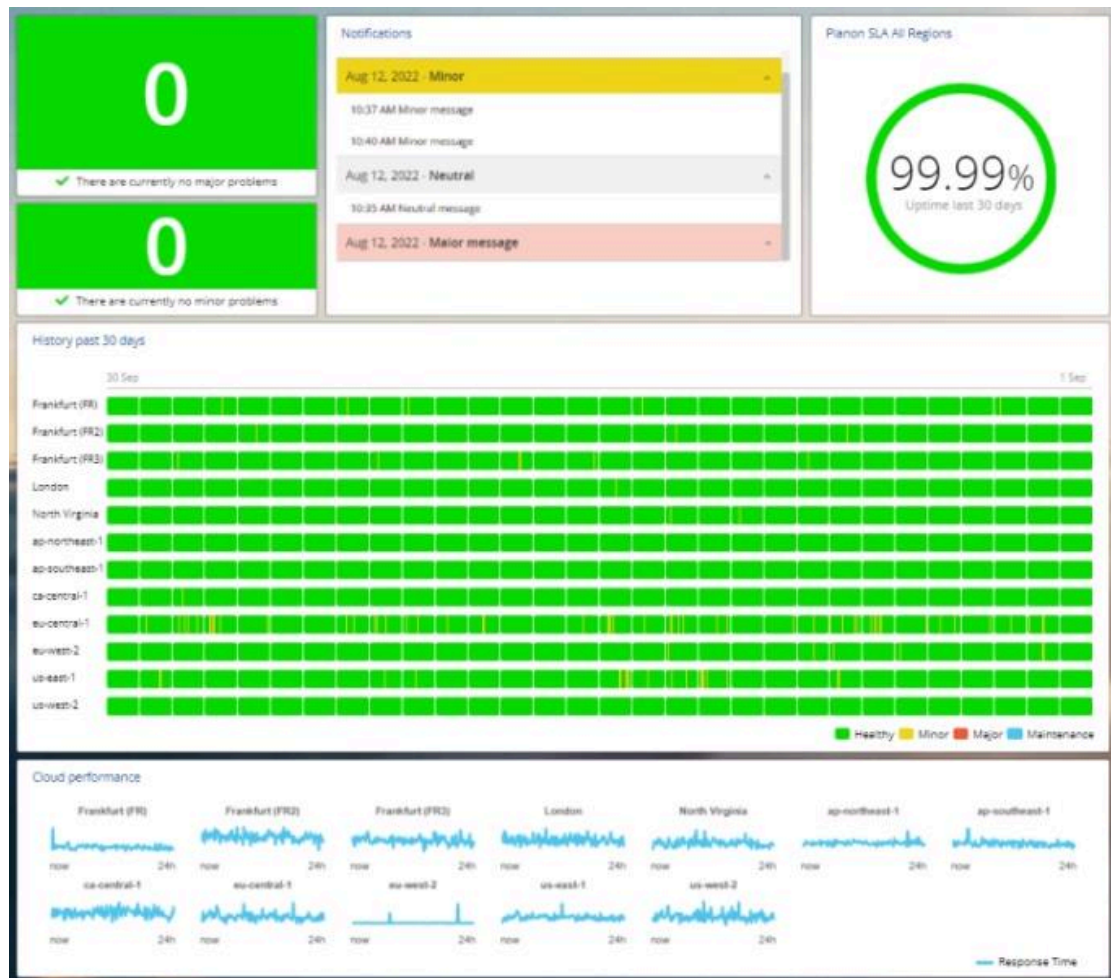
Trust dashboard

Planon wants to ensure maximum customer satisfaction and offer an optimal working environment for its customers.

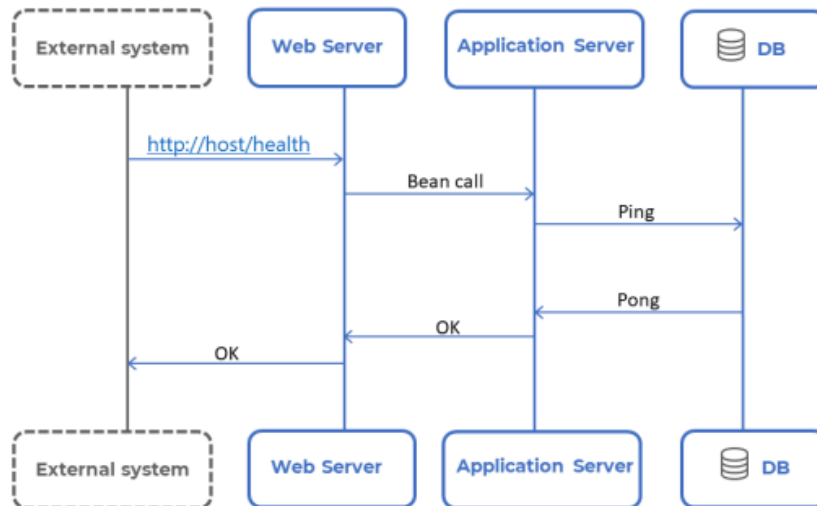
Therefore, Planon is committed to making sure that the customers' production environments are operational at least 99,5% (excluding planned maintenance).

For transparency, Planon publishes a [Trust dashboard](#) that is available online (24*7). The dashboard displays:

- The average uptime over 30 days
- The number of major and minor problems
- Notifications panel, showing:
 - Planned maintenance slots
 - Information about incidents (major/neutral/minor)
- The uptime history per region
- Cloud performance per region



To be able to build the Trust dashboard, Cloud environments are continuously monitored, as shown in the following image:



SLA

Cloud performance

Major problem

The definition of a major problem is:

At least 10 customer environments in a region are down, and this comprises more than 10% of the customer environments in this region.

When this happens, the **Major problem** block will turn red and will display the number of major problems. In addition, the **History** block on the Trust dashboard will be updated.

Minor problem

The definition of a minor problem is:

An individual customer is down.

The **Minor problem** block will turn orange and will display the number of Minor problems. In addition, the **History** block on the Trust dashboard will be updated.

Notifications

The **Notifications** panel will display information that is important for customers to know.

SLA

The Planon SLA part will display the average SLA of all customers of the past 30 days.

When hovering your mouse over the number that is shown, a precision of 6 digits behind the decimal point is displayed.

While the Trust dashboard displays the average SLA of all customers, each individual customer can consult their own production SLA via their **Availability** gadget.



Customer contracts younger than 30 days are not included when calculating the average SLA. The SLA service is only available for Production environments.

[Availability gadget](#)

[Trust dashboard](#)

History past 30 days

The **History past 30 days** part displays the history of problems of the past 30 days.

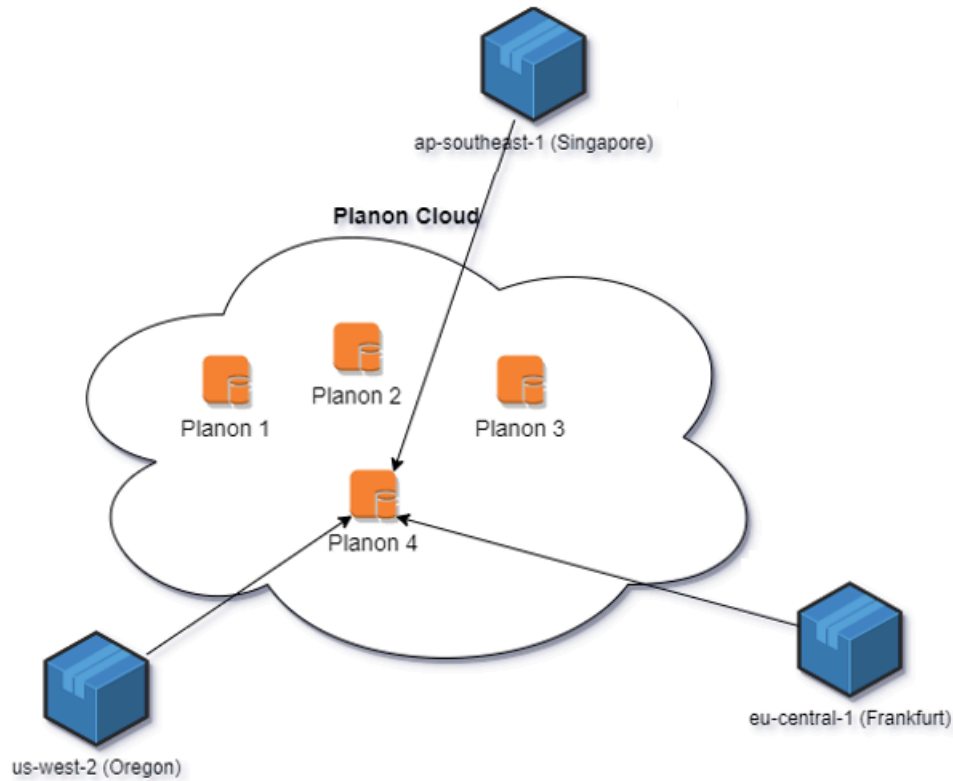
Time line

- The thickness of the line is determined by the duration of the incident or of grouped incidents. The minimum is 1 pixel. Example: A 15 minutes downtime for a customer, will display the minimum of 1 pixel on the day block
- Mouseover on a day shows all the incidents of that day.
- Incidents at the same time window are grouped in lines that are displayed (thicker line). Incidents that occurred at different times, will display multiple vertical lines.
- Mouseover on a day that contains multiple major/minor incidents shows the appropriate values.
- Solved incidents stay the same color, but the mouseover pop-up box indicate that the problem is resolved (resolved date is filled in)
- The pop-up box on mouseover shows the start date, start time, end time and current status of the problem: *Solved* or *Working on it*.
- The legend explains the meaning of the colors used.

Cloud performance

Every five minutes, three agents located in different parts of the world ping each customer environment.

This feature is used to determine if there is a problem with a customer and to determine the performance of the environment.



As shown earlier, a ping will go through different layers.

If, for example, one component is very busy, this will have an effect on the ping outcome. This way, you will get an indication of the performance of the Planon environment

The ping results of the three agents will be stored and an average of these three results is calculated. A higher standard average, does not mean that the performance is poor. The distances between the agents could be further away. Any spikes, however, may indicate performance problems.

[Availability gadget](#)

[Trust dashboard](#)

Maintenance

Planon distinguish two types of maintenance: Planned Maintenance and Unplanned Maintenance.



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.

Unplanned maintenance

Unplanned Maintenance (Emergency Maintenance) is maintenance that cannot be scheduled regularly because of its nature. Either urgent security fixes or urgent IT-related fixes will be done in this window.

Planned maintenance

Planned Maintenance distinguishes two types:

- General maintenance for all Planon Cloud Customers.

General maintenance is a maintenance window covering the IT related maintenance of the Planon Cloud. This window affects all customers simultaneously in a selected region. Average the duration of this maintenance is 90 minutes.

- Maintenance for Planon Cloud customers without Upgrade Control.

Maintenance for Planon Cloud Customers without Upgrade Control is a maintenance window where the Planon Application is being upgraded to the latest version. Average window of this maintenance is 4 hours, where the down-time of the application is 75 minutes.

If the window of this planned maintenance is inconvenient to business operations, the customer can manually start the update via the Environment Management gadget at a time that is convenient and the environment will not be affected by the maintenance.

Please note that a Planned Maintenance will always have a notice period of at least 12 hours. The Planned Maintenance will be performed between Monday to Friday outside working hours. Working hours are: 08:00 AM through 06:00 PM local data-center location time.

Emergency number

For urgent issues, the Planon Cloud Center team is available 24/7/365. You can contact us via the telephone number listed on the [customer portal](#) > **Cloud** > **Cloud Maintenance** (credentials required) when there is a:

- Production stand-still situation, where the customer is unable to continue its work within the Planon application due to technical reasons falling under the responsibility of the Planon Cloud Center team.




For all other issues (such as non-Production stand-stills or projects that are not notified to the Planon Cloud Center team), please contact [Planon Support](#).

Cloud Performance Testing

This document provides an overview of the possibilities, processes and restrictions for performance testing in the Planon Cloud.

For a complete overview of Planon performance tuning, please refer to the Planon Performance Tuning Reference Guide.

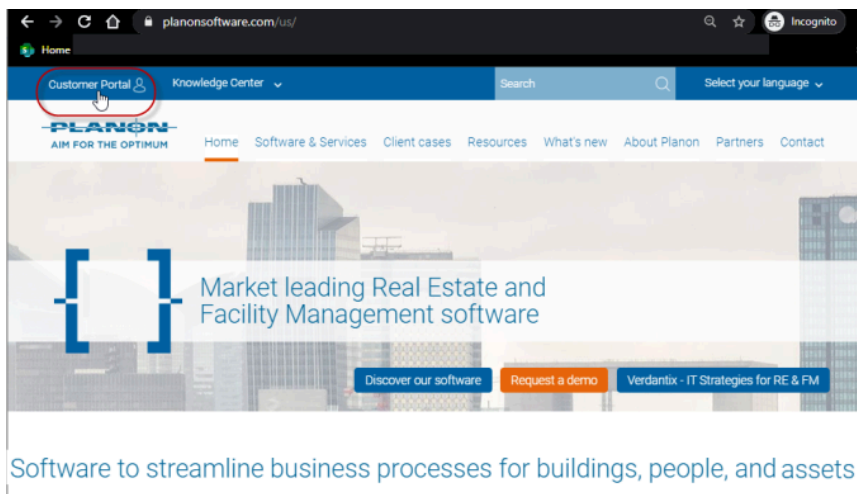
 This document is delivered in the documentation set that is part of your Planon installation or can be obtained from the Planon Customer Portal.

Accessing the portal

To access this portal, you will need to log in using your customer credentials.

Procedure

1. Go to planonsoftware.com and click Customer Portal.




2. Log in using your credentials.
3. Go to Downloads > Live > Documentation > 1. Before you start > Planon Performance Tuning Guide.pdf

Here, you can download the document.

Requesting a performance test

The Planon Cloud team requires an official customer request to execute a performance test of a Planon Cloud environment.

The reason for this request is that performance tests might impact the performance of other environments. Therefore, the performance test will have to be monitored closely to ensure that other customers are not affected by it.

 The Planon Cloud team may interrupt and stop the performance test if issues occur.

Creating a request

1. On the Customer Portal, create a ticket for Planon support to request a performance test.
2. Provide the following information:
 - a. Cloud environment to be tested.
 - b. Start date / time of the test.
 - c. End date / time of the test.
 - d. An indication of the expected load.
 - e. Test target and test tool.
3. The request will be assessed internally and the customer will be notified of the decision.

The request can be approved or rejected. Reasons for rejection can be:

- The test could be disruptive for other environments.
- The Cloud infrastructure is in maintenance at the requested time window.
- A planned upgrade is scheduled at the requested time window.


URLS for performance testing

For reasons of security and data protection, access to the Planon Cloud application is restricted.

However, the following web endpoints can be made available for performance testing.

The Planon ProCenter application (web application):

- <https://<cloud name>.planoncloud.com/>
- Custom domain (if configured)

 For information about URLs available in the Cloud, see [Environment Delivery Information](#).

Testing in the Cloud


After obtaining approval as communicated via Planon support, the tests can be conducted.

Every action that regular users can perform in a Cloud environment can thus be tested.

Such tests can either be performed manually or by automatically executing user actions via scripting. Often, these scripts enable mocking multiple concurrent users.

It is important to understand that it is possible to test all actions that can (manually) be performed in the user interface. However, scripts that mimic users by sending HTTP requests have some limitations (see the next section)

The Cloud team can assist the team doing the performance test by providing relevant operational data.

 The Planon built-in performance monitoring functionality provides performance insight into Planon processes. To enable this and to see which processes are monitored, please see the information available in the [Planon WebHelp](#).

Cross site request forgery

Performance tests are often conducted to verify response times and hardware resource usage when a high number of concurrent users is using the system.

To be able to mimic many concurrent users without having to open a lot of browser windows, a performance tool often simply sends HTTP requests that would typically be sent when performing actions in a browser.


Restriction

The Planon application is protected against *cross site request forgery* (CSRF). This protection dynamically encrypts endpoints, which virtually makes it impossible to 'predict' the URLs.

Consequently, it is not possible to use automated performance tools that mimic browser users by sending HTTP requests, as such tool cannot circumvent dynamically encrypted URLs.

Available APIs

CSRF protection is disabled for (non-webclient) APIs such as the PMFS API and Web services API.

 Consequently, this makes it possible to apply automated performance tools for testing these APIs and to mimic multiple concurrent users by sending HTTP requests.

API availability across software versions

Please note that although it is possible to mimic users by sending HTTP requests to (non-public) APIs, these APIs are not guaranteed to be stable across Planon software versions.



This means that when upgrading to a newer Planon software version, the endpoints may have changed. Consequently, customers may need to update their scripts in order to run automated performance tests.

Cloud System Management

The following information is meant for the system administrator.

Introduction

One of the main principles of the Planon Cloud is that the customer is in control without being dependent on Planon staff.

In addition to maintaining the physical aspects of your Planon Cloud environment, it is also possible to customize email and deploy your own TMS.

Emailing in the Cloud

By default, a mail server is configured for your Planon Cloud environment. This mail server is managed by Planon Cloud Center.

SPF

To enable this mail server to send mails from your own domain name, the server address needs to be included in the domain SPF record. Planon has created a DNS record for this to easily include the correct server: `spf.planoncloud.com`

An example SPF record for `example.com` will look like this:

```
example.com TXT 300 "v=spf1 include:spf.planoncloud.com -all"
```

DKIM

Planon enables DKIM signing for Planon Cloud mail servers. To set up DKIM, the following information is required:

- DKIM Selector: Planon
- DKIM Public Key:

```
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDdv88v7tCclW  
+Le2+dDoMcNrfQ4x2Cml
```

```
/55uW0Q7dxiiSe3w0kj7zbD9iwlz9kNAJQoeu4O1935s8O+N62JbrlpVkzxxZgtskvjrmH
```

```
cW1sE7xZuGti9dqYx0/aVq5iPc4sGphyOpkP  
+qPwRSJBSpKutZgKRg40Cn2Hqyr3Gpy4jQIDAQAB
```



Make sure that the Public Key is one line and that there are no spaces in it when adding the DNS record!

ESMTP with TSL support

Extended Simple Mail Transfer Protocol or ESMTP is a protocol used for sending and receiving email over IP networks. ESMTP includes additional functionality that SMTP does not support, such as Transport Layer Security (TLS). Planon provides ESMTP with TLS support over port 587.

i Emails sent over the public internet are already encrypted with TLS. The ESMTP setup mentioned here refers to the communication between your Planon application and the Planon SMTP server.

To set this up, enter the following values in these fields:

- ESMTP with TLS: Yes
- SMTP with SSL: No

* Email catcher on?	<input type="radio"/> Yes	<input type="radio"/> No
* ESMTP with TLS	<input checked="" type="radio"/> Yes	<input type="radio"/> No
* SMTP with SSL	<input type="radio"/> Yes	<input checked="" type="radio"/> No
* Log successful emails	<input checked="" type="radio"/> Yes	<input type="radio"/> No

Uploading and configuring TMS

In Planon Cloud, customers are empowered to upload and configure TMS themselves.

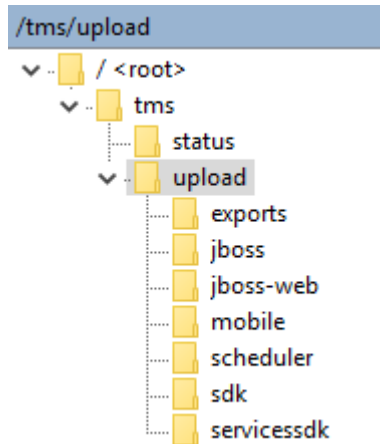
To access and upload TMS, you must use the credentials obtained via the Environment management gadget corresponding with the Cloud instance.

i For regular file access (File Explorer) to the TMS upload server, you can use tools such as WinSCP.

Procedure

1. Log on to the TMS upload server by clicking the URL provided.
2. On the **Login** screen, enter your user name and password.
The user name and password can be obtained via the [Environment management gadget](#).
3. Click **OK**. You are logged on to the TMS upload server.

The following screenshot shows the folder structure of the TMS upload server:



Status

The **status** folder includes the 'TMS-deployed.out' file, which gives an overview of the deployed TMS bundles.

Upload

The **upload** folder contains different subfolders in which you can upload your bundles:

- **exports**: This folder contains two subfolders: **jboss** and **jboss-web**. These folders each contain an `export.packages` file which you need to edit in order to add your TMS solutions.
- **jboss**: Here you can place your standard SX bundles, Enterprise Talk (PEET) TMS workers and query builders.
- **jboss-web**: Here you can place your extended actions bundles.
- **mobile**: Here you can place your custom bar code bundles.
- **scheduler**: Here you can place your alerts, scheduled tasks, and so on.
- **sdk**: Here you can place all bundles that use the SDK for business process integration.
- **servicessdk**: Here you can place your SDK bundles that use the Web client authentication method. Everything that has end user implementation.

Deploy

After uploading the bundles to the correct place, complete the following procedure to deploy them:

1. Click the URL provided to log on to the Planon Web Client.
2. Open the **Environment Management Overview**.
3. Click the **Danger zone** tab and select the correct instance.
4. Click **Reload TMS**.
5. For webclient user extensions (WCX) you need to re-login to activate the extension.



All files in the TMS folder are now loaded as TMS. This includes the **hidden files**! Make sure hidden files are visible in your file explorer, e.g. WinSCP. In WinSCP, the setting is: **Preferences > Panels > Show hidden files**.

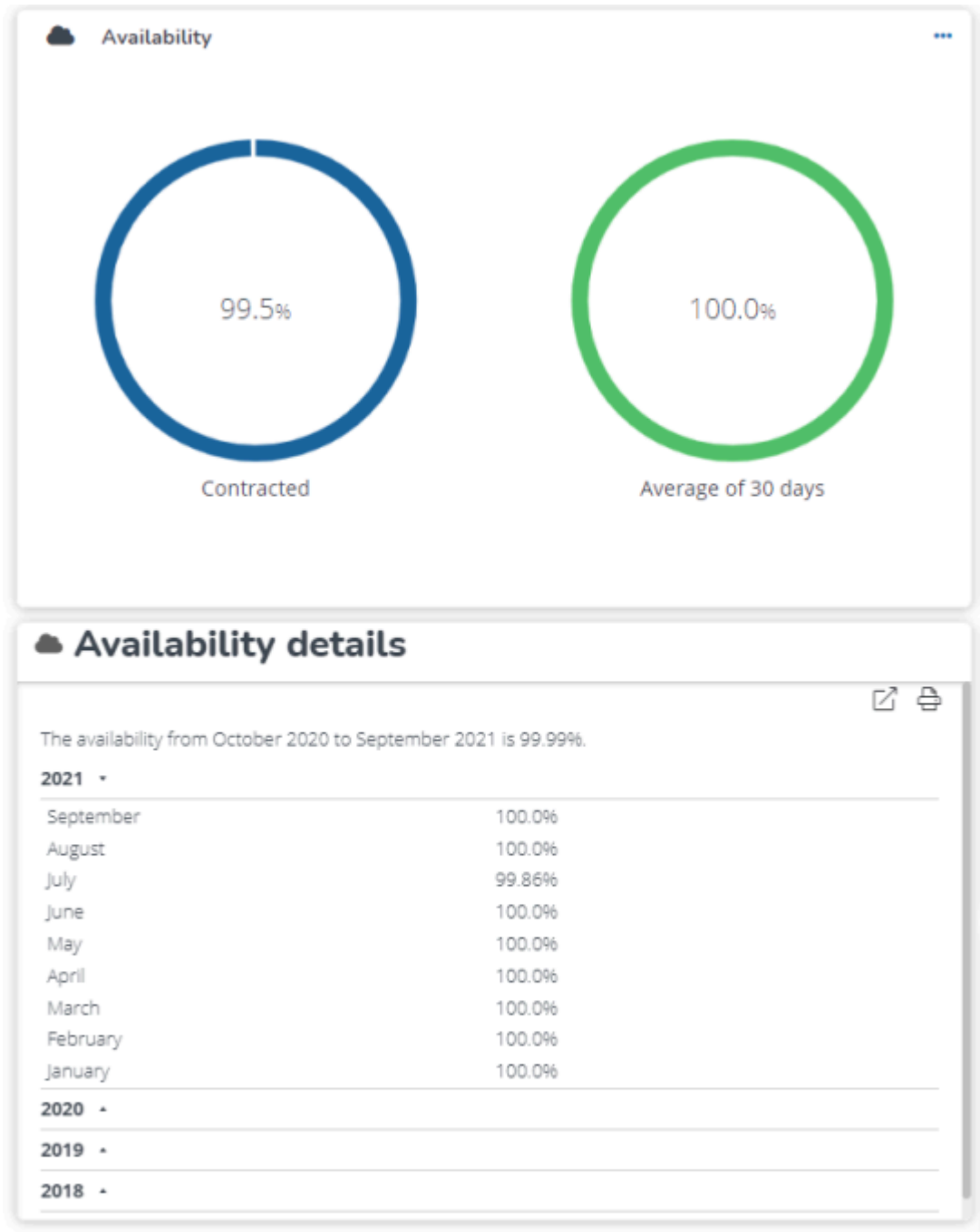


Do not forget to register the solution extension in Planon.

Availability gadget

On the homepage, the **Availability** gadget displays the up-time over the previous 30 days.

To support customers in reporting the Planon Cloud availability over a longer period of time, the **Availability** gadget features a **Details** level.



i The **Availability** gadget is only available in Production mode.

SLA

Cloud performance

Configuring availability reporting

Since this is a new feature, existing customers who want to use this feature need to complete the following configuration.



This is a one-time action only!

1. Go to TSIs > ProCenter modules - Web configuration (Web UI Manager) and set it to Under construction.
2. Go to TSI > Web definitions and click Add selection steps on the action panel.
3. Add the Trust step and click OK.
4. Go back to the All TSIs level and set the TSI back to Completed.
5. In your navigation panel, go to Web configuration and select the Availability definition (Trust) in your list of definitions.
6. Click Add Trust details and fill out the required fields.

For Code, make sure to enter *pcc_trust_details*. When done, Save your new definition.

This code will automatically appear as the Gadget details in your Availability definition (Details page > Actions tab).

You have linked details to your availability gadget. The details are now available to the Availability gadget on your homepage.

Availability reporting

Contractually, customers need to be able to report about the availability of the Planon Cloud over a period of time, typically, a year.

The **Availability** gadget contains details about the up-time.

1. On the Availability gadget, click the elipsis points (...) button on the right.

The Availability Details screen appears.

The availability from October 2017 to September 2018 is 99.5%

2018

September	100.0%
August	97.0%
July	97.0%
June	100.0%
May	100.0%
April	100.0%
March	100.0%
February	100.0%
January	100.0%

2017

The screenshot shows a window titled 'Availability Details' with a close button (X) in the top right corner. Below the title bar, there are two icons: a document with a download arrow and a printer. The main content area displays a summary line: 'The availability from October 2017 to September 2018 is 99.5%'. Below this, the data is grouped by year. The year '2018' is expanded, showing a list of months from September to January with their respective availability percentages. The year '2017' is collapsed. The table for 2018 shows: September (100.0%), August (97.0%), July (97.0%), June (100.0%), May (100.0%), April (100.0%), March (100.0%), February (100.0%), and January (100.0%).

On the top it lists the availability over the last 12 months.

Subsequently, it lists the availability per month clustered by year.

2. On the top right, click Export as CSV to download a CSV file containing the listed details.

The file will be downloaded to your browser's download location.

Alternatively, click Print all to print the file to a printer device or to PDF.

Single Sign On

This chapter describes how to configure and implement Single Sign On for Planon Cloud.

Using SAML

The following sections describe how to configure SAML SSO.

The Planon identity broker solution

Planon Cloud supports Single Sign On (SSO) based on SAML2, a process that allows users to authenticate themselves against an external customer side Identity Provider (IdP) rather than obtaining and using a separate user name and password handled by Planon Cloud.

Currently, only Service Provider initiated SSO is supported in the Planon Cloud.

To enable the customer to configure the SSO setup, Planon Cloud introduces an Identity Broker solution. The login information for this Identity broker solution will be provided to you by your Planon contact person.

For each Planon Cloud environment (Development, Test, Acceptance, Production), a separate Identity Broker solution is available.

The SSO feature is provided as a self service.

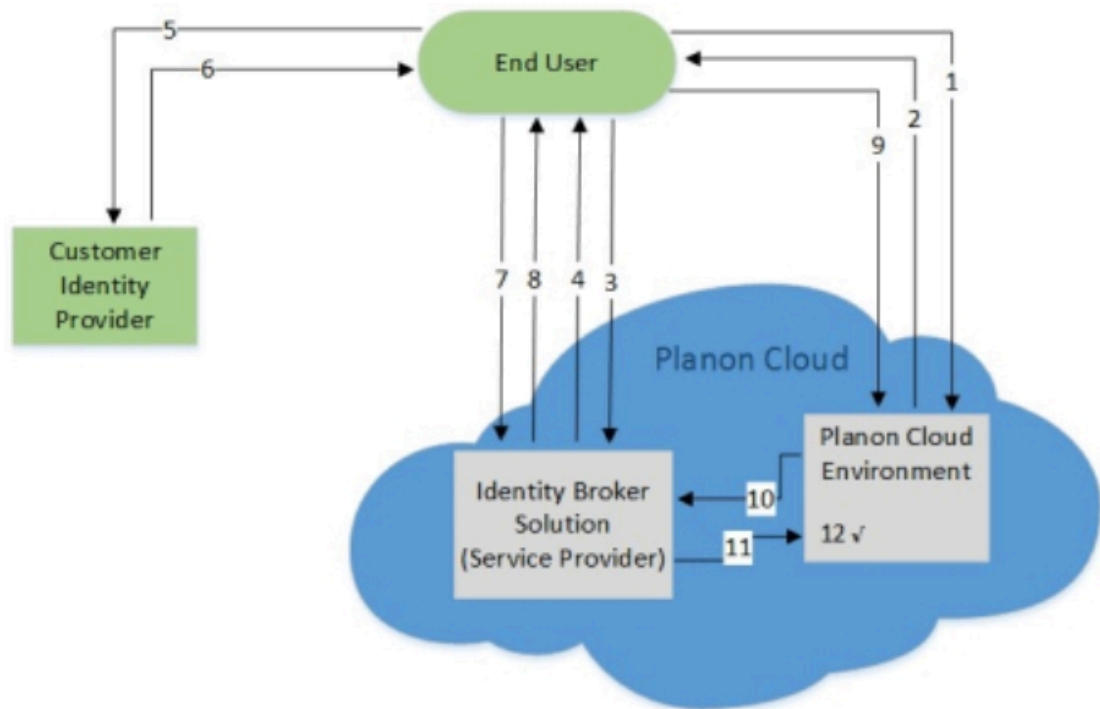
The customer can turn off/on and configure this feature at will. Planon recommends to check with a consultant /ICC person.

The SSO flow

A Single-Sign-On-enabled Planon Cloud environment consists of various components.

- End user
- Planon Cloud environment
- Identity Broker solution
- Customer Identity Provider (IdP)

The following image describes the connection between these various components in Planon Cloud:



The numbers in the diagram correspond with the steps below.

i In this process, the end user is a browser.

Only a few of these actions will result in something that an actual end user will see. These steps are marked with an * and a short explanation is given on what the end user could experience.

1. End users request a resource from the Planon Cloud The service provider performs a security check on behalf of the target resource. (If a valid security context at the Identity Broker (service provider) already exists, skip steps 2–9).

End user experience: enter the Planon URL in the browser or click on a link that points to the Planon Cloud.

2. Planon Cloud Environment responds with a redirect to the Identity Broker solution.
3. End user requests login Identity Broker solution*.

End user experience: If manual login is enabled (default for all non-prod environments), the user can log in with the initial Planon supervisor account (credentials can be obtained via the [Environment management gadget](#)), or the user can click on the link to be redirected to IDP (step 4). If SAML Identity Provider is default login method automatically redirect to IDP (step 4).

4. The Identity Broker responds with a redirect to the Identity Provider.
5. The end user requests login from the Identity Provider*.

End user experience: User views the login page or is automatically logged in to the Identity Provider, depending on the configuration at the customer.

6. After a successful login at the Identity Provider, the end user is redirected to the Identity Broker.
7. The end user visits the Identity Broker with a SAML post.
8. The Identity Broker responds with a redirect to the Planon Cloud.
9. Post configured attribute to Planon Cloud.
10. Planon Cloud checks if user session is valid at Identity Broker solution.
11. Identity Broker solution confirms, when the session is valid.
12. Only after the valid session confirmation, the user can access the requested resource.

End user experience: The user sees the requested resource at Planon Cloud. If the user name is unknown in the Planon Cloud Environment, an access failed message will be displayed.

Prerequisites - SAML assertion to be sent to Planon

The Identity Broker Solution requires a SAML response that contains the following two components:

A **NameID** (including a mandatory format description).

A separate **SAML attribute** that contains the identifier to map to Planon. (so not the NameID itself!)

In the example below, these mandatory components appear in bold.

The following excerpt is an anonymized sample of a SAML post to Planon:

```
<samlp:Response ID="_0216c6ce-7f8c-4e22-b6ca-d4cb9c6fc431"
  InResponseTo="ID_dbe02f23-e90a-4b04-a8ab-8af19632c7b5" Version="2.0"
  IssueInstant="2015-09-01T20:55:33.525Z"
  Destination="https://xx-yyy.planoncloud.com/"
  xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" >
  <saml:Issuer
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">urn:xyz:saml:idp</s
    aml:Issuer>
    <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo>
    <CanonicalizationMethod
```

```

Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
<SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"
/>
<Reference URI="#_0216c6ce-7f8c-4e22-b6ca-d4cb9c6fc431">
<Transforms>
<Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
<Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
<InclusiveNamespaces PrefixList="#default samlp saml ds xs xsi"
2001/10/xml-exc-c14n#" />
</Transform>
</Transforms>
<DigestMethod
xmlns="http://www.w3.org/Algorithm="http://www.w3.org/2000/09/xmldsig#sh
a1" />
<DigestValue>WrxQ8DfeSzygwXgKFbLLuK/iPvI=</DigestValue>
</Reference>
</SignedInfo>
<SignatureValue>...</SignatureValue>
<KeyInfo>
<X509Data>
<X509Certificate>...</X509Certificate>
</X509Data>
</KeyInfo>
</Signature>
<samlp:Status>
<samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
</samlp:Status>
<saml:Assertion Version="2.0" ID="_e6db33a1-0724-4474-bdde-a9628e8223e0"
IssueInstant="2015-09-01T20:55:33.525Z"

```

```

xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
<saml:Issuer>urn:xyz:saml:idp</saml:Issuer>
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
  <SignedInfo>
    <CanonicalizationMethod
      Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
    <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"
      />
    <Reference URI="#_e6db33a1-0724-4474-bdde-a9628e8223e0">
      <Transforms>
        <Transform
          Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
        <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
          <InclusiveNamespaces PrefixList="#default saml ds xs xsi"
            org/2001/10/xml-exc-c14n#" />
        </Transform>
      </Transforms>
      <DigestMethod
        xmlns="http://www.w3.org/2000/09/xmldsig#"
        Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"
        />
      <DigestValue>Y1ksPiFQl6Mzh0nJrMNO2OMDtEI=</DigestValue>
    </Reference>
  </SignedInfo>
  <SignatureValue>...</SignatureValue>
  <KeyInfo>
    <X509Data>
      <X509Certificate>...</X509Certificate>
    </X509Data>
  </KeyInfo>
</Signature>

```

```

<saml:Subject>
  <saml:NameID Format="urn:oasis:names:tc:SAML:2.0:nameidformat:
  persistent">username</saml:NameID>
  <saml:SubjectConfirmation
    Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
    <saml:SubjectConfirmationData NotOnOrAfter="2015-09- 01T20:58:33.541Z"
      Recipient="https://xx-yyy.planoncloud.com/"
      InResponseTo="ID_dbe02f23-e90a-4b04-a8ab-8af19632c7b5" />
  </saml:SubjectConfirmation>
</saml:Subject>
<saml:Conditions NotBefore="2015-09-01T20:52:33.525Z"
  NotOnOrAfter="2015-09-01T20:58:33.525Z">
  <saml:AudienceRestriction>
    <saml:Audience>https://xyyyy.
    planoncloud.com/auth/realms/environment-test</saml:Audience>
  </saml:AudienceRestriction>
</saml:Conditions>
<saml:AuthnStatement AuthnInstant="2015-09-01T20:55:33.541Z"
  SessionIndex="_e6db33a1-0724-4474-bdde-a9628e8223e0">
  <saml:AuthnContext>
    <saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:Passwo
    rd</saml:AuthnContextClassRef>
  </saml:AuthnContext>
</saml:AuthnStatement>
<saml:AttributeStatement>
  <saml:Attribute Name="email">
    <saml:AttributeValue
      xsi:type="xs:string"xmlns:xs="http://www.w3.org/2001/XMLSchema"xmlns:xsi
      ="http://www.w3.org/2001/XMLSchema-instance">USERNAME@email.com</saml:At
      tributeValue>

```

```
</saml:Attribute>
</saml:AttributeStatement>
</saml:Assertion>
```

For more information on how to check a SAML assertion, please see [SSO troubleshooting](#).

Activating Keycloak



The following Keycloak configuration is an example only. No rights can be derived. Screenshots and example may differ from your situation. If you need assistance in setting up your local specific configuration of keycloak, please contact your account manager.

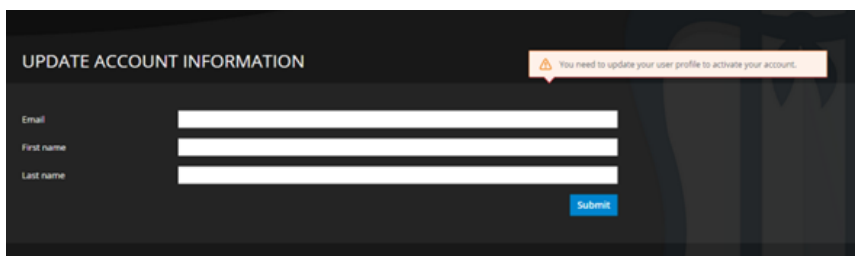
Take the following steps to activate Keycloak.

1. Turn on SSO by using the Environment Management gadget, save the URL and user name/password.
2. Open the URL saved in step 1 and log in with the initial credentials.



3. At the first login, you will be prompted to complete your profile.

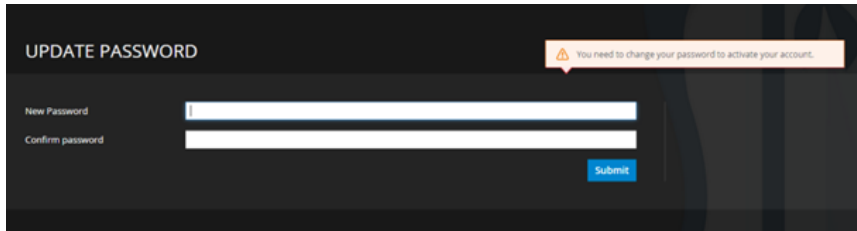
Provide a valid email address. A verification email will be sent to you to enable your account.



4. You will be prompted to change your password.



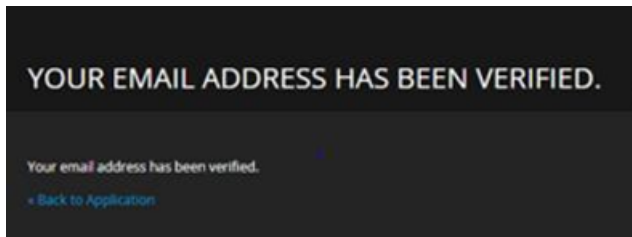
You can use the password saved at step 1 as the **New Password**. This way the password can always be looked up in the **Environment Management** gadget.



A verification email will be sent to you to the email address you have provided. This email contains an activation link for your account.

Note that the link in this email will expire within 5 minutes.

5. After verifying the email address, you can log in to the Planon Cloud Identity Broker solution.



Configuring Keycloak



The following Keycloak configuration is an example only. No rights can be derived. Screenshots and example may differ from your situation. If you need assistance in setting up your local specific configuration of keycloak, please contact your account manager.

Take the following steps to configure Keycloak.

1. In the menu on the left panel, select **Identity Providers (IdP)**.
2. Select SAML in the list to modify the preconfigured settings.
3. Modify the details in the data section, you can configure the settings here (the Redirect URI is automatically set for you):

~ SAML Config

- Single Sign-On Service URL
- Single Logout Service URL
- Backchannel Logout
- NameID Policy Format
- HTTP-POST Binding Response
- HTTP-POST Binding for AuthnRequest
- HTTP-POST Binding Logout
- Want AuthnRequests Signed
- Want Assertions Signed
- Want Assertions Encrypted
- Signature Algorithm
- SAML Signature Key Name
- Force Authentication
- Validate Signature
- Validating X509 Certificates

Save Cancel

4. The information for the fields under SAML Config need to be provided by the customer.

These are the details of the Identity Provider (IDP) on the Production environments (and recommended on Non-Production environments):

- **Want Assertions Signed** must be **ON**
- **Validate Signature** must be **ON**.

5. Click **Save** to add the configuration to the **Identity Broker solution**.

6. Click the **Mappers** tab. Click on **attributetoplanon**.

Identity Providers > salesforce > Identity Provider Mappers > attributetoplanon

Identity Provider Mapper attributetoplanon

- ID: c26991bc-caed-404c-9e6d-bcb8e3e4725c
- Name: attributetoplanon
- Mapper Type: Attribute Importer
- Attribute Name: please change this
- Friendly Name:
- User Attribute Name: user.attributes.plnuid

7. Modify the **Attribute Name** with the correct IDP SAML attribute.

This will also be provided by the customer.

Do not fill the field **Friendly Name** and do not modify the field **User Attribute Name**.

8. Click **Save** to activate the updated attribute mapper to the configuration.

Replacing the certificate

For enhanced control over their own Cloud environments, customers can further tweak single-sign-on configuration.



The following Keycloak configuration is an example only. No rights can be derived. Screenshots and example may differ from your situation. If you need assistance in setting up your local specific configuration of keycloak, please contact your account manager.

1. In the Environment Management gadget > SSO tab, log on to Keycloak by clicking the Identity broker URL.

The Keycloak console appears.

2. In the left panel, select Identity Providers (IdP).
3. Select SAML in the list to modify the preconfigured settings.
4. Create a backup of the data in the fields Single Sign-On Service URL and Validating X509 Certificates.
5. Replace the values in these fields with the *Single Sign-On Service URL* and *X509 Certificate* provided by the Identity Provider.
6. Click Save.

The changes are active directly and can be tested immediately. To do this, close the browser completely and open a new session to validate the login.



For more information on configuring Keycloak, see Keycloak's [Server Administration Guide](#).

Rollback

Should the credentials provided in the fields **Single Sign-On Service URL** and **Validating X509 Certificates** not function correctly for any reason and the previous values need to be reinstated, replace the values with those you backed up earlier. This will reactivate the former settings.

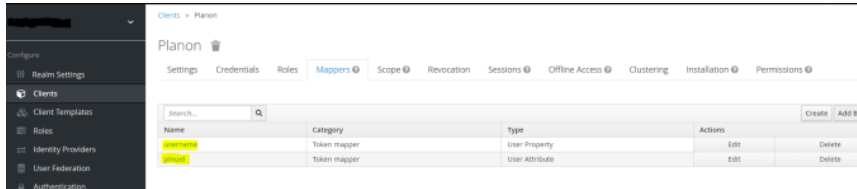
Rearranging the mappers

After configuring the identity provider, please make sure the mappers for the Planon client are in the correct order.

To find and check the current order of mappers, proceed as follows:


1. Click on Clients in the left panel, and click on the Planon client.
2. Open the Mappers tab, and make sure the order is:
 - username
 - plnuid

Example



If these mappers are not in the correct order, delete and recreate them in the correct order. (You may need to do this a couple of times to get it right).

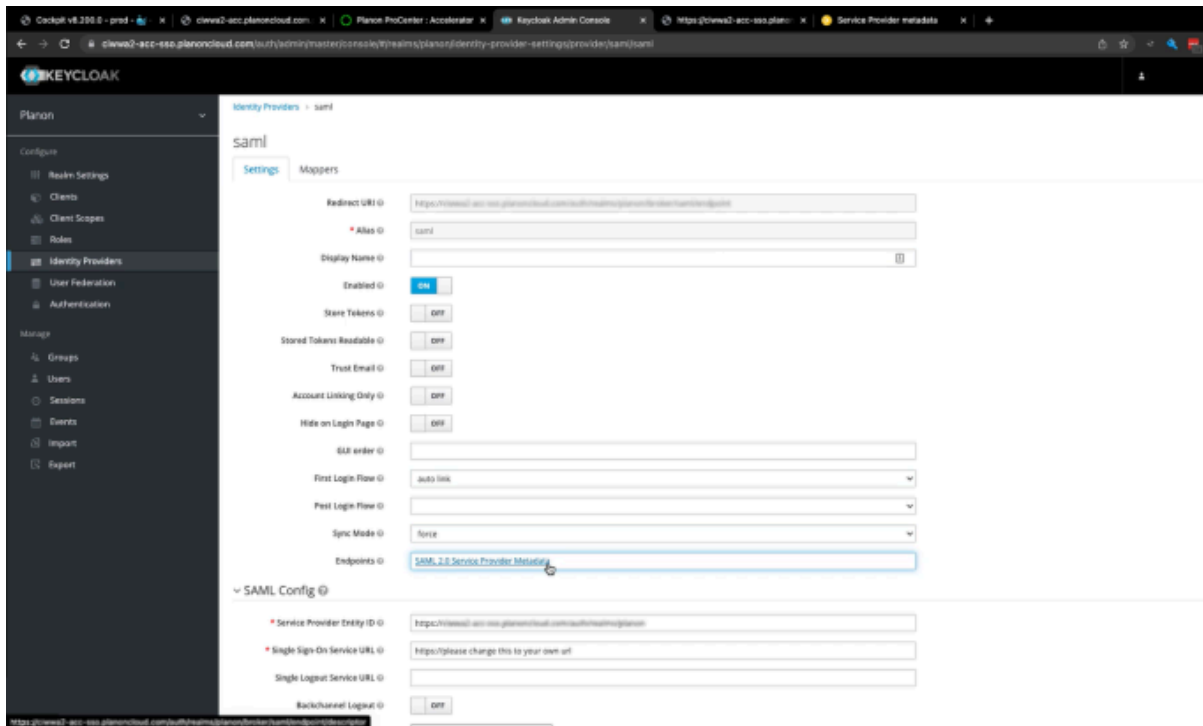
Service Provider metadata

 The following Keycloak configuration is an example only. No rights can be derived. Screenshots and example may differ from your situation. If you need assistance in setting up your local specific configuration of keycloak, please contact your account manager.

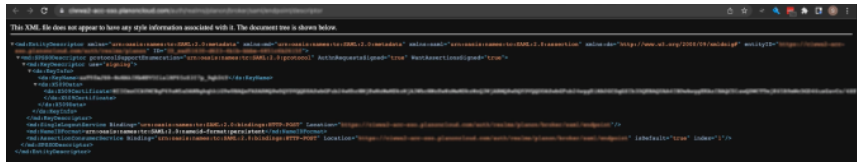
You must also send some details on SSO - the Service Provider Metadata - to the customer. If there are any configuration changes in the metadata, they can be exported via the Identity Broker solution.

1. In the menu on the left panel, select **Identity Providers (IDP)**.
2. Select the Identity Provider just created.
3. Click the link in the **Endpoints** field.

It may not directly be apparent that this is a link, but if you hover over the field, the URL will be displayed at the bottom of your browser.



Clicking the link opens the metadata page in your browser:



4. Share this URL with the customer IDP administrator to establish a trusted relation between IDP and the Service Provider.

If the logon page is enabled, you can still automatically be redirected to the desired IDP by adding the following parameters to the URL:

?kc_idp_hint=<IDP Alias>

Example

https://customer-prod.planoncloud.com/?kc_idp_hint=saml

If a redirect to the default IDP is enabled, you can go to the login page by entering a different value.

Example

https://customer-prod.planoncloud.com/?kc_idp_hint=lmas

Custom domain allowance

When adding a custom domain to your Planon Cloud environment additional configuration needs to be done in Keycloak to be able to use Planon via the custom domain in combination with Single Sign on.

Take the follow steps to configure Keycloak.

Procedure

1. In the menu on the left panel select **Clients**.
2. In the list that is displayed, select **Client ID** Planon.
3. Add the Custom Domain URL in the **Valid Redirect URIs** by typing the URL followed by /*

Clients > Client details

Planon OpenID Connect

Clients are applications and services that can request authentication of a user.

Settings | Keys | Credentials | Roles | Client scopes | Sessions | Advanced

General Settings

Client ID *

Name

Description

Always display in UI Off

Access settings

Root URL

Home URL

Valid redirect URIs

[Add valid redirect URIs](#)

Jump to section

- General Settings
- Access settings
- Capability config
- Login settings
- Logout settings

- Click **Save** to add the redirect URL.

Logging out of Planon Cloud

This URL makes a user log off from Planon, sends a log off request to the Identity Broker solution and redirects the user to the given redirect URL.

The redirect URL must be configured in Identity Broker solution.

Procedure

- Login to the Identity Broker solution.
- On the left side, select **Clients**.
- Select **Planon**.
- Add the value of the redirect URL in the **Valid Redirect URIs** by typing the URL followed by /*

Clients > Planon

Client Planon

Settings | Credentials | Roles | Mappers | Scope | Revocation | Sessions | Clustering | Installation

Client ID: Planon

Name: Planon

Enabled: ON

Consent Required: OFF

Direct Grants Only: OFF

Client Protocol: openid-connect

Access Type: confidential

* Valid Redirect URIs:

- https://<name>.planoncloud.com/*
- http://www.planonsoftware.com

Base URL: https://<name>.planoncloud.com

Admin URL:

Web Origins: https://<name>.planoncloud.com/*

Save Cancel

5. Click **Save** to add the redirect URL.

i Note that [Logging out from Planon Cloud](#) but not from IDP only works if you do not configure a Single Logout Service URL on the Identity Provider page.

KeyCloak secure configuration considerations

This section lists a number of security considerations that can enhance your security level when using Planon Single Sign On (SSO).

! Please be aware that these configuration settings are considerations that highly depend on the customers' requirements, their Identity Provider and the security policies within the customers' organization. Only IT staff that is trained in these configurations should deploy these considerations or contact Planon for consultancy.

Authentication

External identity provider

When delegating authentication to an external identity provider (IdP) you should consider the following:

Subject	Description
Local account password	When a user logs in using an external identity provider, KeyCloak will create an account in it's local store.

Subject	Description
Forcing external IdP login	<p>By default, it is possible for users to set a password on this account and use the user name and the KeyCloak local password to login.</p> <p>As this bypasses the external identity provider, this may be undesired.</p> <p>This behavior can be disabled at two places:</p> <ul style="list-style-type: none"> • Configure > Authentication > Required actions and disable Update password. When this is disabled, users can no longer set the password on the local KeyCloak account. • Configure > Authentication > Flows > Browser and disable the forms. When this is disabled, the password screen can no longer be used. Please be aware that this option will also disable all local keycloak accounts just as supervisor. <p>What also could be considered is to make the login via an external IdP mandatory in the browser flow by setting the Identity Provider Redirector to required; this way, you cannot authenticate against other sources than your own IdP.</p> <p>This can be configured by going to: Configure > Authentication > Browser and configure the Identity Provider Redirector as Required.</p>

Using Planon user federation

It is possible to authenticate using the Planon system as an authentication source. Credentials entered in the KeyCloak user name and password fields are validated against the Planon credential store.

Subject	Description
Local account password	<p>When a user logs in using the Planon user federation, KeyCloak will create an account in it's local store. By default, it is possible for users to set a password on this account and use the user name and the KeyCloak local password to login. This bypasses the Planon user federation check so this may be undesired.</p> <p>This can be configured by going to: Configure > Authentication > Required actions and disable Update password.</p>

Subject	Description
	When this is disabled, users can no longer set the password on the local KeyCloak account.

KeyCloak local account password

Subject	Description
Password policy	<p>When using the local KeyCloak passwords, it is advised to set a password policy. This can be done in:</p> <p>Configure > Authentication > Policies > Password policy.</p> <p>Here, you can add policies for the different aspects of the passwords. Planon recommends setting the password policy in accordance with your organization's security policies.</p>
Brute force protection	<p>Brute force detection will be enabled by default. However, customers can set up their own metrics if desired.</p> <p>The Brute force detection settings can be found under:</p> <p>Configure > Realm settings > Security defences > Brute force detection</p>

General settings

Subject	Description
Multi-factor admin	<p>We strongly recommend to set up multi-factor authentication on the admin account. This can be done by:</p> <p>User name (top right of your screen) > Manage account > Account security > Signing in > Two-factor authentication</p>
Security headers	<p>Customers can set up their own security headers if desired.</p> <p>The security headers settings can be found under:</p> <p>Configure > Realm settings > Security defences > Header</p>

Logging out from Planon Cloud

Logging out from the Planon Cloud can be achieved in two ways.

- Log out from the Planon Cloud, but the user is not logged out of the Identity Provider (default configured).
- Log out of Planon Cloud and the user is logged out from all the used components.

For this, the Identity Provider must support Single Log Out.

Logging out from Planon Cloud but not from IDP

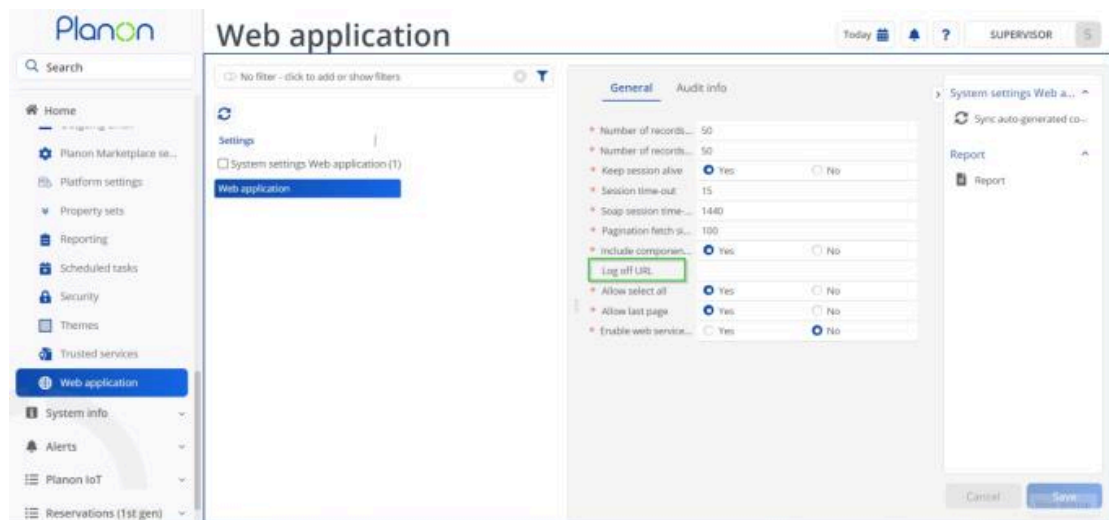
If the used Identity Provider does not support single logout or the project team decides not to have the end user log out at the Identity Provider, the following configuration steps should be followed:

A user is being logged out in Planon and the Identity Broker solution is redirected to another web page.

This makes logging out work only partly, the logout only works visual. The session in Planon and the Identity Broker solution are ended but session at IDP is not ended.

If the user visits Planon again within the SSO session timeout, the user will be logged in again automatically.

In a Planon Cloud environment, a logout URL must be configured in **System settings > Web application > Log off URL**.



The correct URL is the **entityID** that is mentioned in the metadata followed by:

```
/protocol/openid-connect/logout?client_id=Planon&post_logout_redirect_uri=Customer chosen URL
```

Example

If no custom domain is configured:

`https://customer-test.planoncloud.com/auth/realms/planon/protocol/openid-connect/logout?client_id=Planon&post_logout_redirect_uri=https://www.planonsoftware.com/`

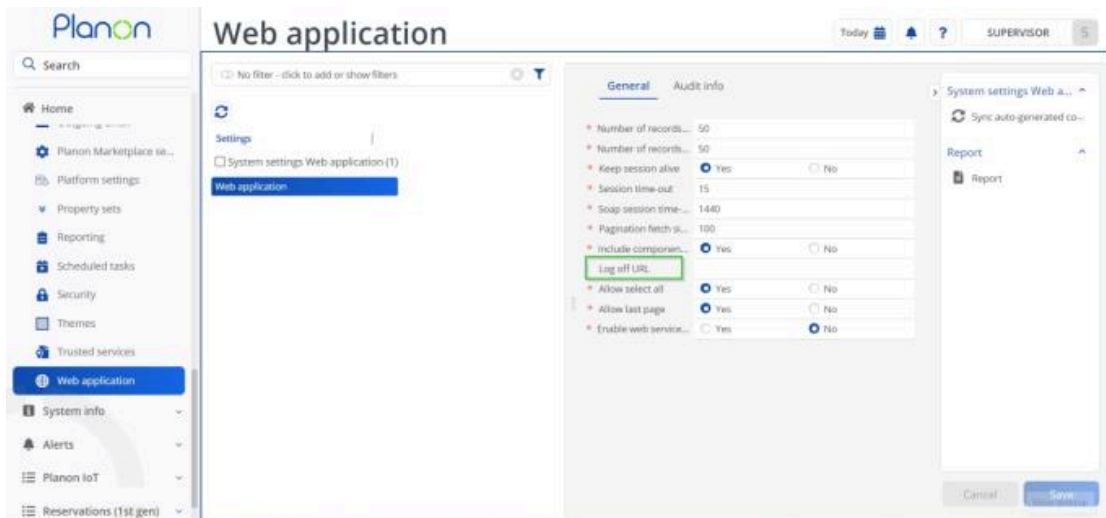
If a custom domain is configured (example custom domain is `facilities.customer.com`):

`https://facilities.customer.com/auth/realms/planon/protocol/openid-connect/logout?client_id=Planon&post_logout_redirect_uri=https://www.planonsoftware.com/`

Logging out from all used components

 To enable this feature, the Identity Provider must support Single Log Out (SLO).

In the Planon Cloud environment a log out URL must be configured in **System settings > Web Application > Log off URL**.



The correct URL is the **entityID** that is mentioned in the metadata followed by `/protocol/openid-connect/logout`

Example

If no custom domain is configured:

`https://customer-test.planoncloud.com/auth/realms/planon/protocol/openid-connect/logout`

If a custom domain is configured (example custom domain is `facilities.customer.com`):

<https://facilities.customer.com/auth/realms/planon/protocol/openid-connect/logout>

This URL logs off the user in Planon and sends a log off request to the Identity Broker solution.

The Identity Broker solution will send a single log out request to the Identity Provider.

1. Log in to the Identity Broker solution.
2. On the Left, select **Identity Providers**.
3. In the right panel select your identity provider.
4. Enter the given Identity Provider's Single Logout URL in the Single Logout field.
5. Subsequently, the session will be closed as soon as the end-user logs out from Planon software.

Testing the solution

Prerequisite

Ensure that the UID for the test user is present as an account in the Planon Cloud environment for a full working test.

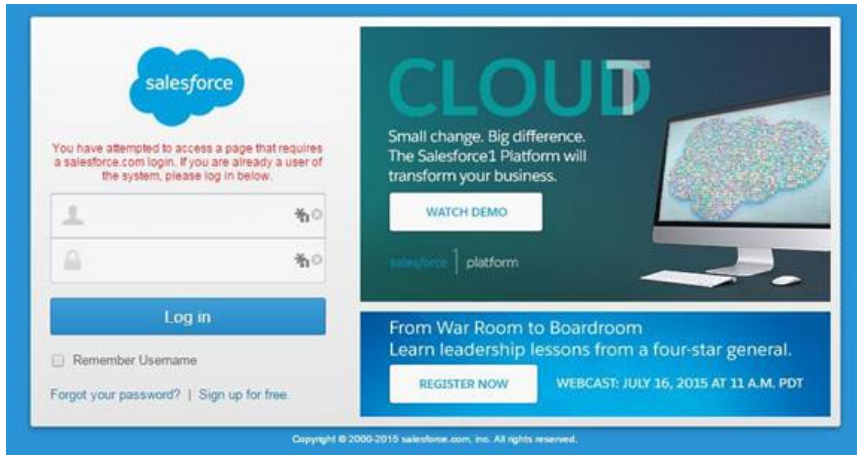
Procedure

1. Visit the main URL of the Planon Cloud environment. The default login page is being replaced by the Identity Broker login page.

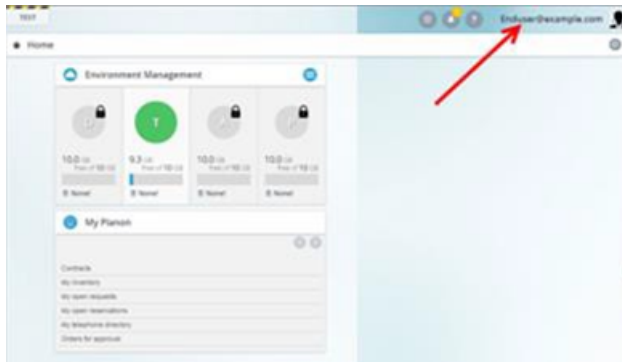
For production, the configured IDP will be configured as default and no manual login will be possible. The users will be automatically redirected to the IDP page.



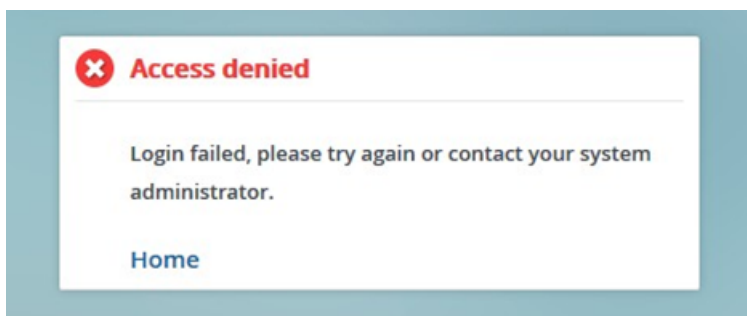
2. To check the SSO solution, click on the alias you configured in the Identity Broker (only for environments other than Production). You will be redirected to the configured IDP (in this example, Salesforce).



Once you log on to the Identity Provider, you will be logged in to Planon with the configured UID (in the example, the user e-mail address).



If you do not see the Planon screen, but an Access denied message, it means that the SSO login was successful but the users UID could not be resolved as a Planon Cloud account.



SSO troubleshooting

For troubleshooting the SSO configuration, Planon recommends to use Mozilla Firefox in combination with the add-on **SAML Tracer**. This add-on lets you read the messages being sent between the end user (browser), the Identity Broker (Service Provider) and the IDP (Identity provider at customer side).

Make sure the SAML Tracer is enabled when visiting the Planon Cloud environment. All http messages will be recorded. If a message contains a SAML request, it is highlighted and the SAML request can be viewed in the SAML tab. Please ensure that the SAML assertion sent by the Identity Provider meets the prerequisites.

Common issues:

- No format in **NameID**
- No separate SAML attribute present (this is not needed when the **NameID** is used as the identifier)

Planon authentication

It is possible to configure KeyCloak to validate the entered user name and password against the accounts stored in the Planon database.

Having this in place renders a Planon Cloud environment suitable for OpenID Connect authentication without having to use an external authentication source (IDP).

Prerequisites

Before configuring this feature, please note the following requirements:

- This feature is currently only available on Planon Cloud environments.
- The environment must have Keycloak enabled (**SSO** tab in the [Environment management gadget](#)).
- The Planon version must be L92 or later.

Overview

When a Cloud environment is delivered, the following way of authentication is the default configuration.



This configuration is also the default **on-premise** configuration; it uses form authentication for the Planon environment.



Keycloak

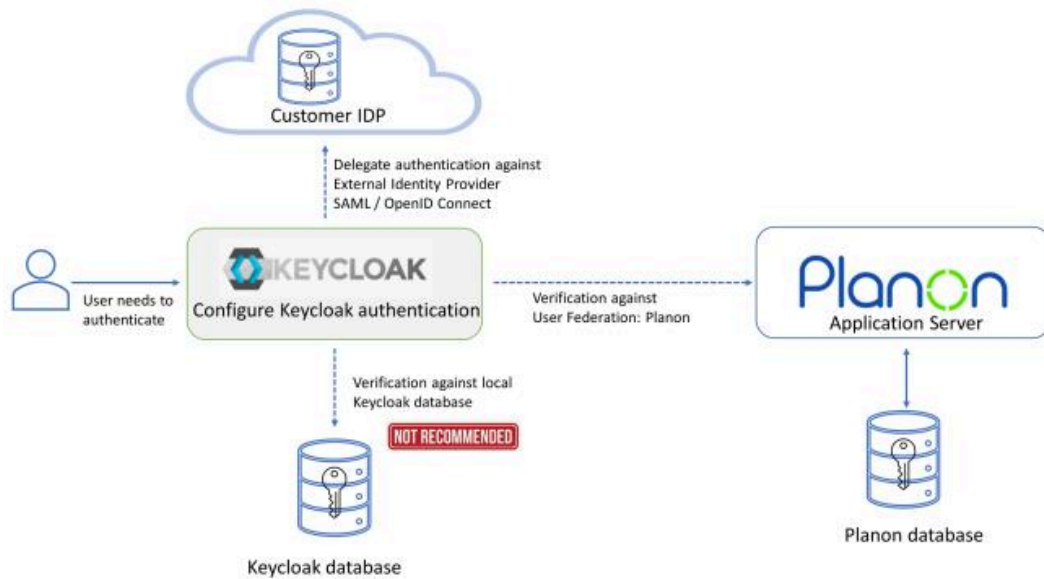
Enabling Single Sign On (**SSO**) on a Cloud environment introduces Keycloak authentication. Keycloak can be configured to use different authentication *sources*.

By default, the authentication via Keycloak is configured as follows.

i This configuration needs to be adjusted by the customer according to the customer's specific (security) requirements. The default configuration only contains the supervisor user to be able to log in to Planon.



The following diagram shows the possible configuration options for authenticating users. This includes the configuration that needs to be applied by the customer.



The customer can choose to:

- Add accounts to the Keycloak database for users to authenticate against Keycloak.

i This is not recommended!

- Add Planon provider in Keycloak under User federation.
This way, users authenticate against the account in Planon database via Keycloak
- Add a external IDP under Identity Providers in Keycloak.
This way, users authenticate against the external IDP of the customers choice via Keycloak.

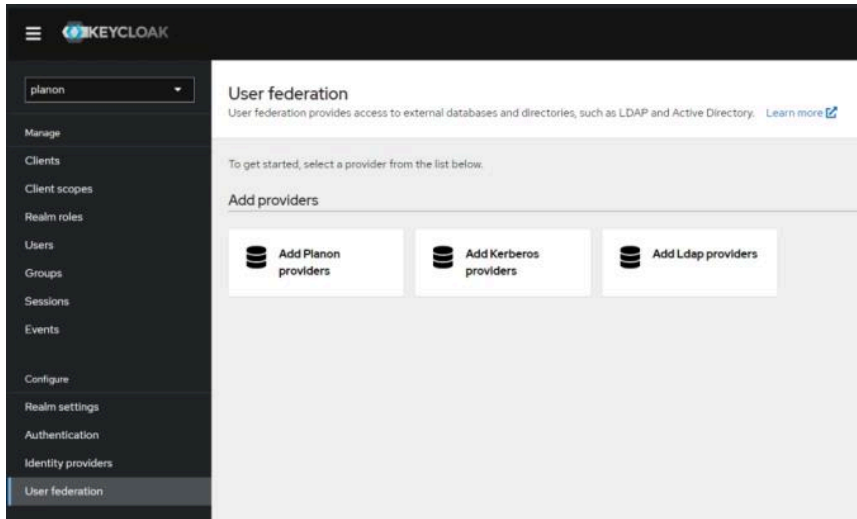
i This is the recommended solution.

Configuring Planon User federation

Proceed as follows to configure User Federation: Planon.

Procedure

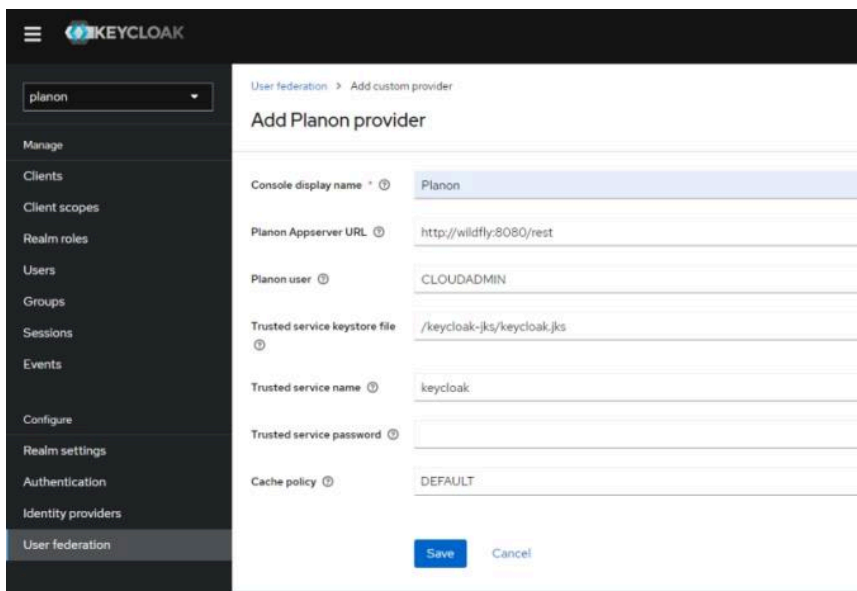
1. Add a **Planon provider** in the section User Federation of KeyCloak.



2. Fill out the settings.

In a Planon Cloud environment only the Console display name needs to be entered, all other fields are pre-configured.

Most of them are initialized correctly for Cloud environments so they need not be changed.



The following table provides a description of the required settings:

Field	Description
Console display name	The name of the user federation in the Keycloak configuration.

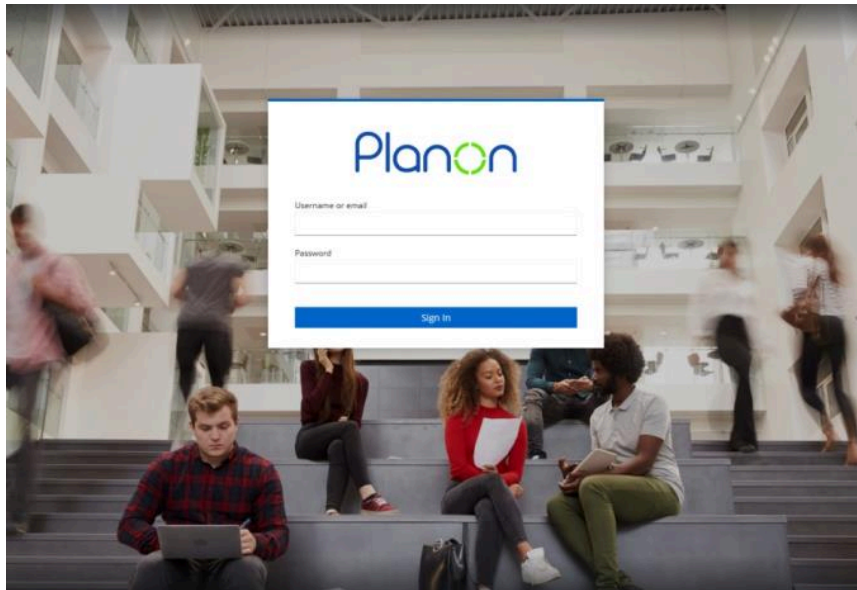
Field	Description
Planon AppServer URL	The location of the Planon backend that can handle user validation. For Cloud, the default value is fine.
Planon user	The user that is used to perform queries to the Planon backend. This should be an active user.
Trusted service keystore file	The user federation uses a trust between Keycloak and the Planon backend. This file contains the keys. For Cloud, you can leave this as is.
Trusted service name	The user federation uses a trust between Keycloak and the Planon backend. This is the name of that trusted service. For Cloud, you can leave this as is.
Trusted service password	The user federation uses a trust between KeyCloak and the Planon backend. This field can override the password. For Cloud, you can leave this as is.
Cache policy	Sets the caching policy. Default should be fine.

3. Click **Save** to apply your settings.

A check with the configured backend is carried out to verify that all configured values are correct. When a mismatch is detected, the save will fail and an error with specific error information will be displayed.

If saving is successful, the user federation is activated.

End users can now log in via Keycloak with the user name and password that are stored in the Planon backend.



Managing users can still be done through the Planon **Accounts** TSI. For more information, see the [Planon Webhelp](#).

Recommendations

- It is not recommended to combine the Planon user federation and Keycloak local password verification. For this reason, we recommend to disable the **Update password** required action on the authentication section of the Keycloak configuration.
- It is recommended to switch to the OpenID Connect authentication method for applications that support this as is described in the [Planon Webhelp](#)


Limitations

- It is not possible to use Planon's [Forgotten password](#) functionality together with Planon user federation.
- Planon user federation is currently only available on Cloud environments.

Logging

The following topics describe how to enable logging and provide information about what is logged.


Security logging

-  If you want to log the login and logout timings of the users (in the selected user group), go to the **User groups** TSI > **User groups** and enable the **Additional security logging** field by selecting **Yes**. This data will be stored in the security logging file. To enable this feature, you must first make the security logging settings. For more information, refer to **Authorization > Security logging**.
- The **Additional security logging** setting is not enabled by default because it comes with a performance penalty. If you start logging for each user, this will create a considerable overhead. Only enable this setting if you need the information to retrieve more detailed information for analyzing issues.

Logging for anonymization

When an account is anonymized, an entry describing this action will be included in the audit log. The log will display a date-time stamp, the name of the account that performed the action and the name of the account that was anonymized.

```
12-01-2018:09:00 ~|~LABOUT-Lars Bout~|~Account anonymized~|~PAWIFI-Patrick Wifian~|~NULL~|~
```

-  This feature allows system administrators to check the status of accounts and find out what action was undertaken and by whom.

What is logged?

Events that are logged

- Licensing changes
 - Linking or unlinking a solution license to a user group.
- Authentication changes

- Adding/deleting a user
- Adding/deleting a user group
- Adding/deleting users from a user group
- Resetting or changing a user's password
- Adding/deleting a product from a user group
- Updating a user group
- (Failed) user actions
 - Failure to log on by a user
 - When a user tries to log on and his/her account is locked
 - First time user login
 - Failed user login (inactive start / end date)
 - When an account is locked (multiple wrong logins, end date, password expired)
- Password settings
 - Changing the password strength
 - Changing password settings
- Logging in/out Planon administrators
 - Logging of login/log off of users linked to the Planon administrator group



• If you want to log the login and logout timings of the users (in the selected user group), go to the **User groups** TSI > **User groups** and enable the **Additional security logging** field by selecting **Yes**. This data will be stored in the security logging file. To enable this feature, you must first make the security logging settings.

For more information, refer to **Authorization > Security logging**.

- The **Additional security logging** setting is not enabled by default because it comes with a performance penalty. If you start logging for each user, this will create a considerable overhead. Only enable this setting if you need the information to retrieve more detailed information for analyzing issues.

- Authorization changes
 - Switching on/off authorization
 - Switching on/off business object authorization
 - Changes to user group permissions:
 - Adding/deleting/updating action filters
 - Updating authorization filters (when linked to user group)
 - Adding/deleting/updating authorization links
 - Updating function profiles (when linked to a user group)
 - Adding/deleting field rights
 - Updating field rights

- Adding/deleting actions
- Adding/deleting status transitions
- Adding/deleting extended actions
- Changing the permission type of BORight
- Changing the function profile default permission type

Environment Management gadget

In the Cloud, the following events are logged:

- **Disk**
 - Changing disk space allocation
- **Customize**
 - Changing the welcome image
 - Changing the welcome image to default
 - Changing the favicon image
 - Changing the favicon image to default
 - Changing the error page URL
- **Backups**
 - Creating manual backup
 - Restoring backup (including backup ID, destination and with or without resetting user password)
 - Deleting a backup
 - Converting a backup from *incremental* to *full*
 - Changing a backup name
 - Changing a backup expiry date
 - Changing a backup comment
 - Changing retention period
 - Changing **Save disk space** (toggle for: incremental full backups)
- **Danger zone**
 - Restarting
 - Scheduling a restart
 - Canceling a scheduled restart
 - Upgrading
 - Scheduling an upgrade

- Canceling a scheduled upgrade
- Reloading TMS
- Changing the WebDAV password
- Resetting NYX credentials
- Importing a clone
- Creating a clone voucher
- Importing Accelerator
- **IP whitelisting**
 - Enabling IP whitelist
 - Disabling IP whitelist
 - Changing IP whitelist settings
- **SSO**
 - Enabling the SSO realm
 - Enabling SSO
 - Disabling SSO
 - Resetting the SSO Admin password
- **Domain settings**
 - Changing the domain alias setting
 - Changing mutual SSL settings
 - Changing portal URL settings

Software health check

The URL endpoint `/health` allows you to verify if your servers are up and running. A round-trip is executed from webserver to application server and database server, and back. The endpoint `/health` page returns **OK** if everything is up and running, and if that is not the case, **NOK** is returned.

Procedure

1. Make sure that there has been a valid login on the webserver. The `/health` URL only functions properly after one valid login on the webserver. Each time the webserver is restarted, one login is needed to have the URL work properly again.



If there has been no valid login on the webserver, the `/health` URL returns **OK** but *no* round-trip is done and no check is performed!

2. Go to the endpoint `/health`.

The check is now performed.

Index

A

- Accessing the customer portal 13
- Activating Keycloak 31
- APIs across software versions 15
- Availability gadget 21
- Availability reporting 23
- Availability reporting: configuration 23

C

- Cloud performance 9
- Cloud testing 14
- Configuration 18
- Configuring Keycloak 32
- credentials 13
- CSRF 15
- Custom barcode 18
- Custom domain allowance 36

D

- DKIM 17
- Dynatrace 14

E

- Email 17
- Environment Management
 - Logging 51
- ESMTP with TLS support 17

F

- File upload 18

H

- History past 30 days 9
- http requests 15
- HTTP requests 15

I

- Identity Broker Solution 25, 41
- Identity provider 25

K

- Keycloak
 - Limitations 50
 - Recommendations 50

L

- Logging
 - Cloud 51
- Logging for anonymization 51
- Logging out 40
- Logging out - SLO 42
- Logging out of Planon Cloud 37
- Log-off URL 41

M

- Mail server 17
- Maintenance 11
- Major problem 8
- Mappers 34
- Minor problem 8

N

- NameID 27
- Non-public APIs 15
- non-webclient APIs 15
- Notification 8

O

- OpenID Connect
 - Planon database 45

P

- Performance testing 13
- Planned maintenance 8
- PMFS API 15

R

- Replace certificate 34
- Requesting procedure 13
- RPO 6
- RTO 6

S

- SAML 25, 27, 34
- SAML attribute 27
- SAML post 27
- SAML2 25
- Secure configuration
 - Considerations 38
- Security logging: switch on 51
- Service availability 6
- Service Provider metadata 35
- Single log out 42
- Single Sign On 25

SLA 9
Software health check 55
SPF 17
SSO 44
SSO flow 25

T

Testing the solution 43
TMS
 Upload 18
Troubleshooting 44
Trust dashboard 6

U

UID 43
Up-time 21
URLs
 Performance testing 14
User federation
 Planon 47

V

Valid Redirect URI 36

W

Web Services API 15
What is logged 51