



Planon product changes introduced by Google third-party cookie deprecation



Portal integration

- With the upcoming deprecation of third-party cookie support by Google the Planon portal integration support will become deprecated from January 1st 2024.

It is no longer possible to use Planon functionalities within another website via an iframe, unless the Portal url is configured to allowed in the browser of the user.



Fix portal instructions



Portal integration

Adjust your website by no longer using an iframe for showing the desired Planon functionalities, but in a new browser window instead.

This allows you to continue to offer the same functionality to your users but accessed in a technically different way.

If you want to continue using iFrames make sure the portal url that contains the iframe links must be added to the allowed to use third-party cookies sites in the browser of all endusers.

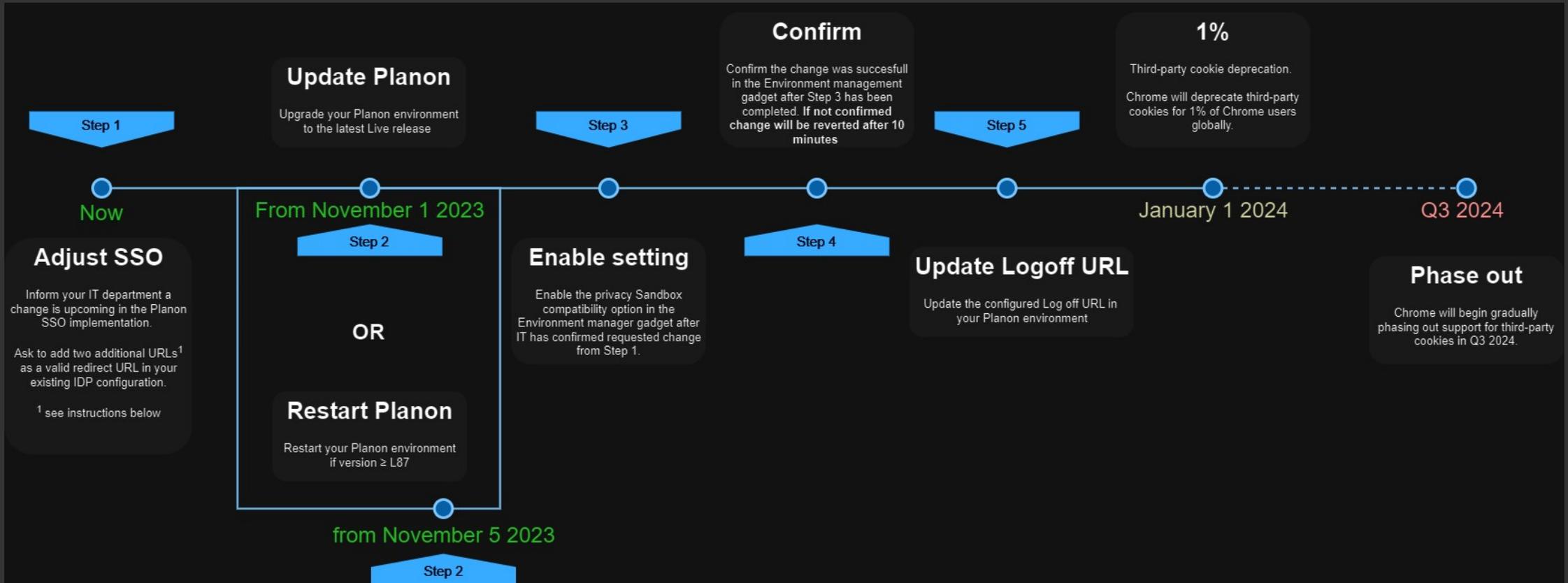


What to do if you use Planon ProCenter across different domains?

This presentation contains instructions to apply the fix to your Planon environment

- On-premise installation: please contact [Planon Support](#)
- Planon Cloud installation in combination with Custom Domain functionality and Single Sign-On configuration, follow the steps in the diagram on the next page.

Steps to become third-party cookie proof





Fix ProCenter instructions

Step 1 – Extend IDP SSO configuration with additional redirect URLs

Ask your IT department to expand the current IDP SSO configuration for your Planon environment(s) to add two additional redirect URLs. This is in addition to the existing permitted redirect URL.

- Example (urls may be different in your environment):

Custom domain	facilities.customer.com
Current redirect URL in IDP configuration	https://customerenvironment-prod-sso.planoncloud.com/auth/realms/planon/broker/saml/endpoint
1 st additional redirect URL	https://customerenvironment-prod.planoncloud.com/auth/realms/planon/broker/saml/endpoint
2 nd additional redirect URL	https://facilities.customer.com/auth/realms/planon/broker/saml/endpoint



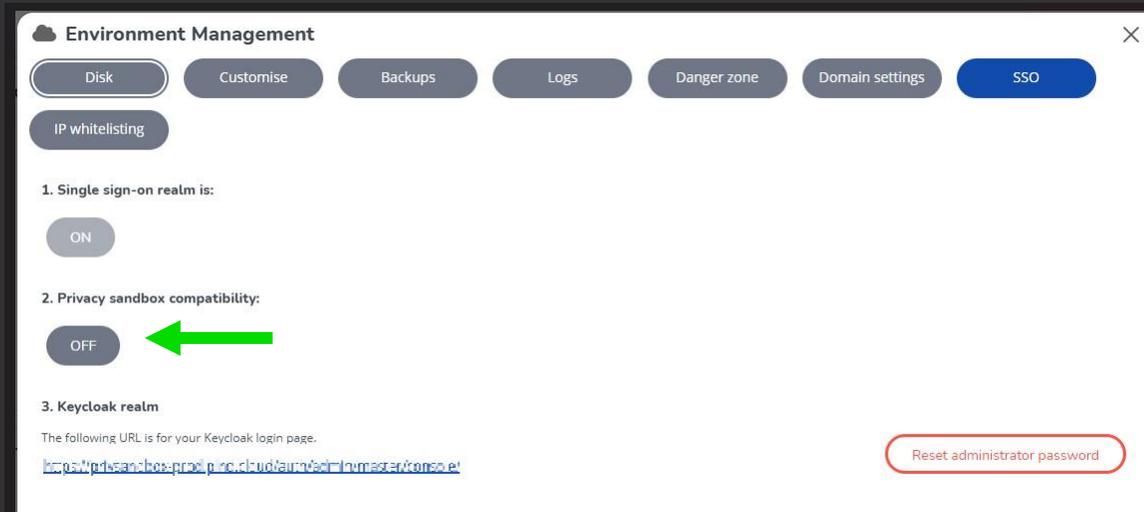
Step 2 – Upgrade to latest Planon Live release

If your environment is still running on a Planon release older than L87, ensure that you upgrade to the latest Planon Live release.

If you are using a Planon Live release of L87 or higher, restart your environment to ensure the installation of the latest hotfix.

Step 3a – Planon Environment Manager Gadget – SSO Settings

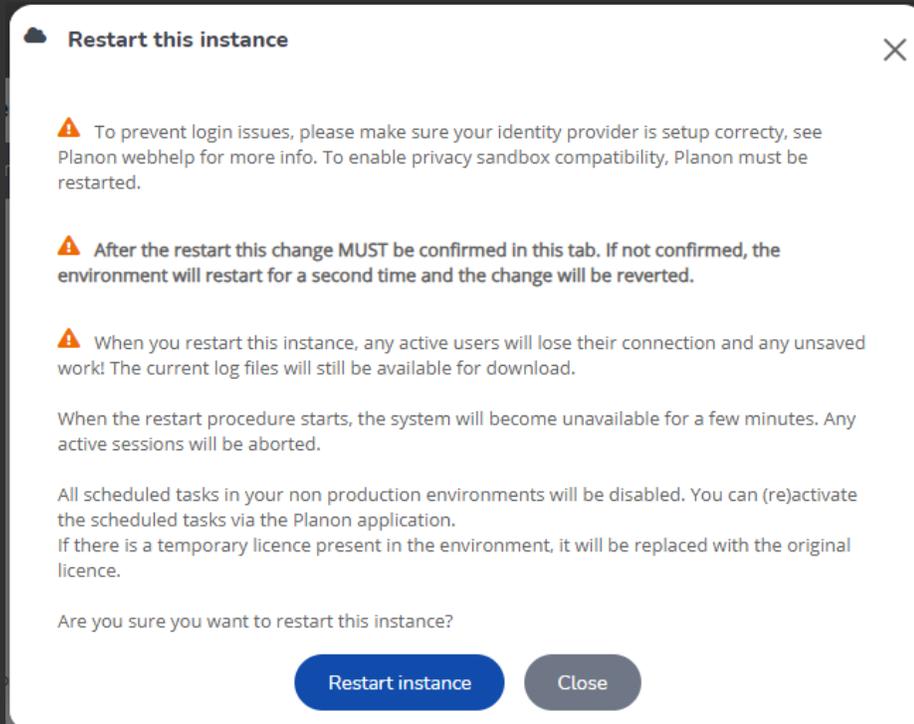
- Ensure that you have successfully finished steps 1 and 2
- Go to the Planon Environment Management Gadget
- Select Tab SSO



- #2. Privacy sandbox compatibility > switch this setting to ON

Step 3b – Enable Privacy Sandbox compatibility

After the previous click, the following window will appear:

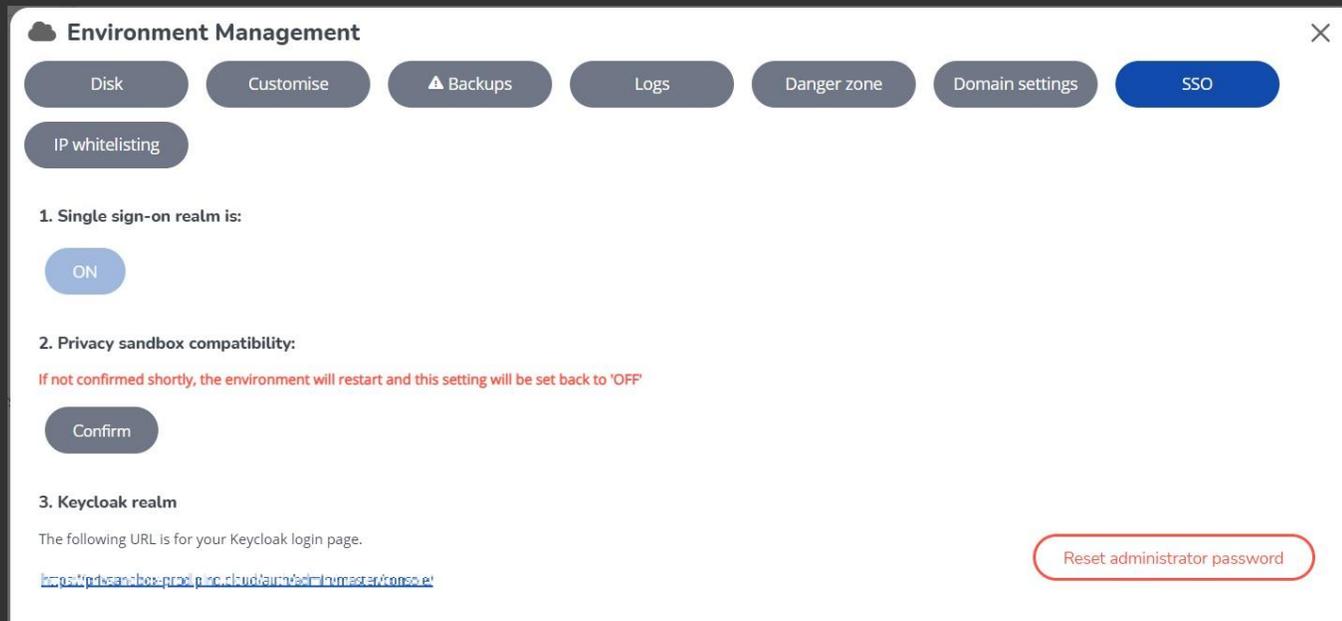


- Click [Restart instance], the environment will restart

Step 4a – Confirm change in SSO setting **within 10 minutes!**

After the restart of the environment, within 10 minutes:

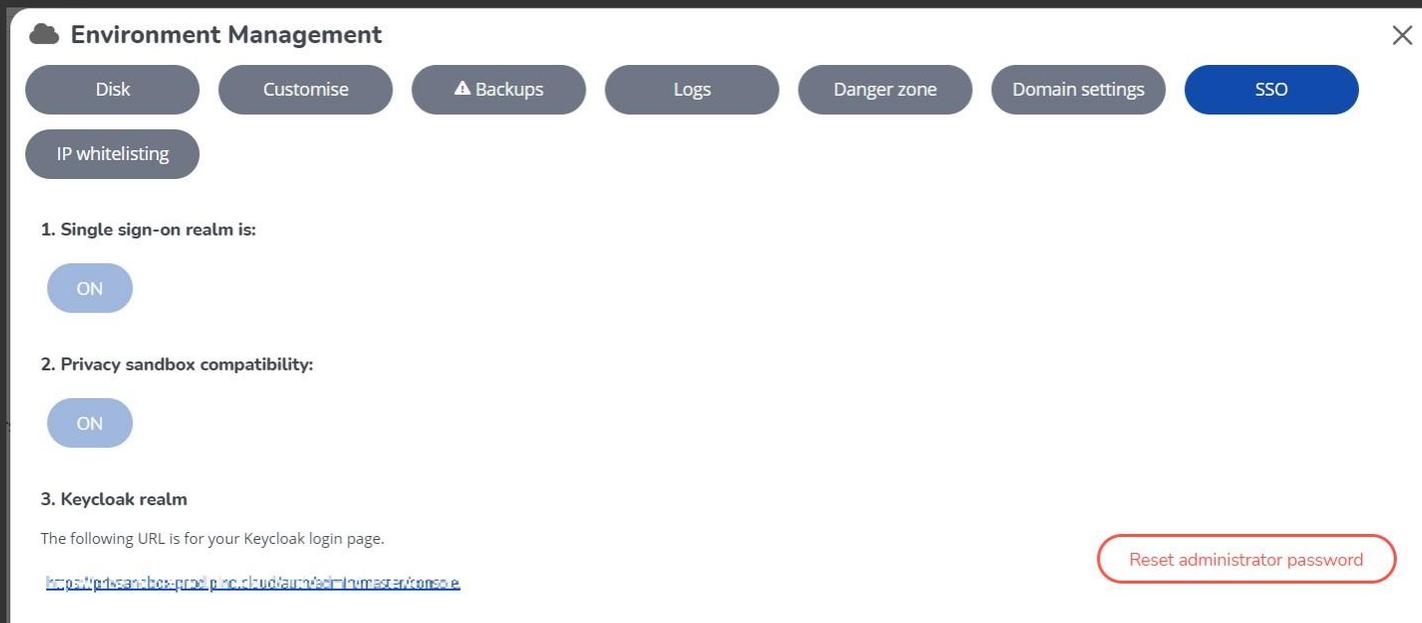
- Log in to your environment via Single Sign On (not as supervisor)
- Go to the Planon Environment Management gadget
- Select Tab SSO
- Confirm the change: #2. Privacy sandbox compatibility to save this.



The screenshot shows the 'Environment Management' interface with the 'SSO' tab selected. The 'Single sign-on realm' is set to 'ON'. Under 'Privacy sandbox compatibility', there is a red warning: 'If not confirmed shortly, the environment will restart and this setting will be set back to 'OFF''. A 'Confirm' button is visible. At the bottom, there is a 'Reset administrator password' button and a Keycloak realm URL: <https://planon-hes-prod-poc.cloud.sap.net/planon-admin-console/>.

Step 4b – Check Privacy sandbox compatibility - setting

After the confirmation of the Privacy sandbox compatibility setting, you will notice that this cannot be disabled anymore.



The screenshot shows 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, there is a section for 'IP whitelisting'. The main content area is divided into three sections:

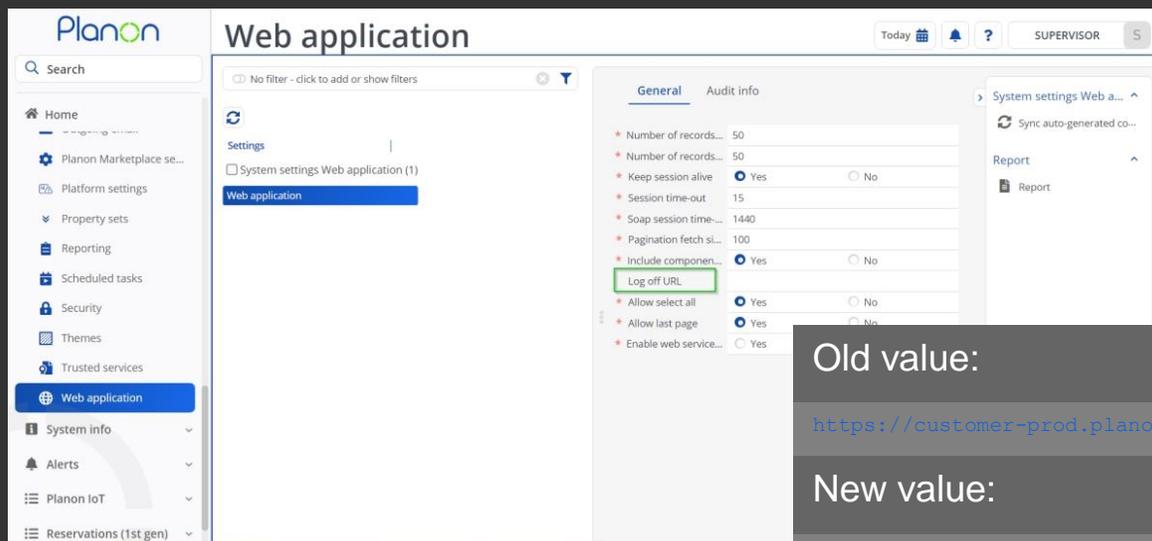
- 1. Single sign-on realm is:**
ON
- 2. Privacy sandbox compatibility:**
ON
- 3. Keycloak realm**
The following URL is for your Keycloak login page.
<https://privacy-sandbox-prod.pnc.cloud/aura/identity/master/console>

At the bottom right, there is a button labeled 'Reset administrator password'.

Step 5 – Update log off URL

In Planon ProCenter update the configured Log off URL

- Go to TSI **System settings** > **Web Application** > **Log off URL**.
- Adjust the hostname to match the custom domain

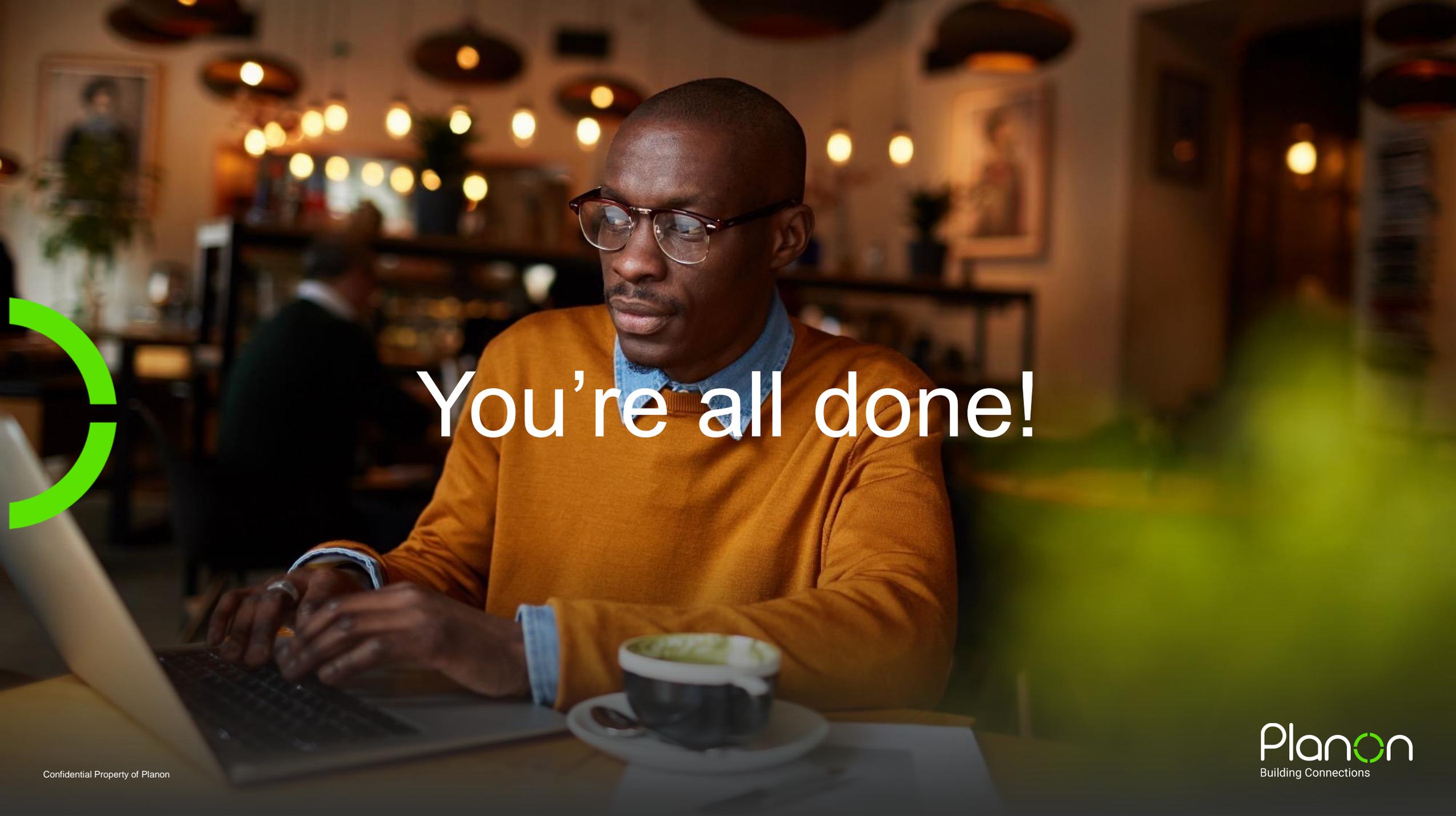


The screenshot shows the 'Web application' settings page in Planon ProCenter. The 'Log off URL' field is highlighted with a green box. A callout box shows the old value and the new value.

Old value:
<https://customer-prod.planoncloud.com/auth/realms/planon/protocol/openid-connect/logout>

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

If you have successfully completed the above steps, your Planon Cloud environment will be future-proofed for the phasing out of third-party cookies.

A man with glasses and a mustache, wearing a yellow sweater over a blue collared shirt, is sitting at a table in a cafe. He is looking at a laptop screen and has his hands on the keyboard. A cup of coffee with a white lid is on the table in front of him. The background is a warm, dimly lit cafe with string lights and framed pictures on the wall. A large green graphic element, resembling a stylized 'C' or a partial circle, is on the left side of the image.

You're all done!