



TRACELINK UNIVERSITY

Home

Resources

TraceLink University

What's new in the system 2026.3.0 release

Explore what's new in the Administration, version 2026.2.0 release. What's new in the user interface.

Release information

This document describes the TraceLink capabilities included in the Administration, version 2026.2.0 release, which is available on Validation on 27 Oct 2026 and Production on 24 Nov 2026.

The following apps are impacted by this release and will be updated to the version listed:

- Administration, version 2026.2.0

Solutions supported by this app version:

- Administration, solution version 13.0.0

The features below are in order of functional relevance (i.e. the typical order in which a user executes a function or task).



These release notes are subject to change based on the deployment of the

release. In the event of changes, the release notes and any related documentation will be updated within one week of release deployment. Deployment completion can be confirmed in the TraceLink Release Notice email.

Patch releases

The following patch is released for this version:

- Administration, version 2026.2.1 is available on Validation on 24 Sep 2026 and Production on 13 Oct 2026.

These patches are cumulative, and the most recent patch release includes functionality from all previous versions.

Revisions

Date	Revision	Description
29 Sep 2026	01	Initial version.
27 Oct 2026	02	The following updates have been made since the previous revision was distributed: • 3 issues are added to Resolved Issues. • 0 issues are added to Known Issues.

API features

There is no new or updated API functionality included in this release.

System features

The following new or updated system functionality is included in this release.

Enhanced Password Policy Configuration

This release adds security controls for password requirements and privileged users. **System Administrators** can configure password requirements for their company. **System Administrators** and **User Administrators** can designate users as **Privileged Users**.

Enhanced Password Validation Controls

When **System Administrators** select Use TraceLink security to authenticate users as the Authentication Method in Single Sign-On Settings, they can now configure the following security controls:

- Breached Password Check – Prevents users from setting passwords found in known breach databases.
- Username Similarity Check – Prevents users from setting passwords that conflict with supported username-based password validation rules.

Privileged User Password Requirements

Companies can now designate users as Privileged User when those accounts must follow stricter password requirements.

In the General section of the Users, Company Users, User Details screen, **System Administrators** and **User Administrators** can now:

- Privileged User – Designate a user as a **Privileged User** to apply the privileged-user password policy. This designation does not grant additional application roles, permissions, or administrative access.

In Single Sign-On Settings, when Use TraceLink security to authenticate users is selected as the Authentication Method, **System Administrators** can now:

- Minimum Password Length for Privileged Users – Set a separate minimum password length for users designated as **Privileged Users**. This setting allows companies to require longer passwords for privileged accounts without changing the minimum password length for other users. If no value is

configured, the standard Minimum Password Length applies.

The privileged user password requirements apply when users set their initial password, change their password, or reset a forgotten password. Existing passwords remain valid until the next password rotation, expiration, or reset.

These enhancements provide greater flexibility and help companies enforce stronger, more consistent password security requirements.

Impact analysis

The impacts for these features are the same as Enhanced Password Policy Configuration feature in the Administration, solution version 14.0.0 release.

Enhanced Session Security with IP Address Restriction

This release introduces Restrict Sessions by IP Address, a company-level setting in the General section of Single Sign-On Settings. **System Administrators** can use Restrict Sessions by IP Address to associate an active user session with the IP address used to establish the session.

If the IP address changes during an active session, the user may be required to authenticate again. Restrict Sessions by IP Address gives **System Administrators** greater control over session security and helps prevent active sessions from being used from a different IP address.

Impact analysis

The impacts for these features are the same as Enhanced Session Security with IP Address Restriction feature in the Administration, solution version 14.0.0 release.

Resolved issues

Administration, version 2026.3.0

The following issues are resolved in this release. The prefixes are for internal

TraceLink tracking purposes and do not mean anything to customers.

ID	Interface	Issue Description
CMCP-44401: Transaction types not loading in Message Settings	Processing	The Transaction Type drop-down did not display available transaction types when editing Message Settings. Administrators can now view all available transaction types and successfully save Message Settings without errors. This issue is resolved.
TL-121771: Company Logo Not Saving in My Network Company	Processing	Saving a company logo in My Network Company resulted in a version conflict error and prevented the logo from being saved. Company logos can now be uploaded and saved successfully without errors. This issue is resolved.
CMCP-40818: Company Information Updates Result in Version Conflict	Processing	Updating company profile details in My Network Company caused a version conflict that prevented subsequent updates to company information in Life Sciences Cloud (LSC). Company profile data now remains synchronized, allowing company information to be updated in both OPUS Administration and LSC without errors. This issue is resolved.

Known issues

Administration, version 2026.3.0

There are no known issues in this release.

The following known issues are included in this release and will be fixed in a future patch release. The prefixes are for internal TraceLink tracking purposes and do not mean anything to customers.

ID	Interface	Issue Description

Related Content



Troubleshoot a problem in OPUS Solution Environment

This topic answers some common troubleshooting scenarios.

[View More](#)



Troubleshoot a problem in Administration

If the company owns Opus apps, users must go to opus.tracelink.com to log in to the Opus Platform or through an IdP that routes to opus.tracelink.com.

[View More](#)



What's new in Extensible TraceLink Transfer, version 2024.3

Explore what's new in the Extensible TraceLink Transfer, version 2024.3 release.

[View More](#)



What's new in the Solution Builder, version 2024.4.0 release

Explore what's new in the Solution Builder, version 2024.4 release.

[View More](#)



What's new in the Opus Solution Environment, version 4.0.0 release

Explore what's new in the OPUS Solution Environment, version 10.0.0 release.

[View More](#)



What's new in the Solution Builder, version 2024.5.0 release

Explore what's new in the Solution Builder, version 2024.5.1 release.

View More