



TRACELINK UNIVERSITY

Home

Resources

TraceLink University

What's new in the system 2026.2.0 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 17 Sep 2026 and Production on 13 Oct 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
16 Jul 2026	01	Initial version.
10 Aug 2026	02	The following updates have been made since the previous revision was distributed: • The Validation date in Release information is updated to 17 Sep 2026. • The Production date in Release information is updated to 13 Oct 2026.
25 Aug 2026	03	The following updates have been made since the previous revision was distributed: • 2 system features are added: ◦ Search and Simplify B2B Integration Link Settings. ◦ Automatically Use Default Transform Versions in Transform Sets.
17 Sep 2026	04	The following updates have been made since the previous revision was distributed: • 1 system feature is added. ◦ Configure and Simplify Password Requirements. • 7 issues are added to Resolved Issues. • 2 issues are added to Known Issues.

Date	Revision	Description
24 Sep 2026	05	The following updates have been made since the previous revision was distributed: • Issue information of Administration, version 26.2.1 patch is added: ◦ 1 issue is 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.

Administrators Can View User Roles

Company Administrators can now view all roles assigned to a user directly from the Company Users page. The new User Roles table provides a consolidated view of user roles across Applications and Networks. This enhancement improves visibility into user access and simplifies user management by allowing Company Administrators to quickly review assigned roles without navigating to multiple areas of the platform.

Impact analysis

The impacts for these features are the same as Administrators Can View User Roles feature in the Administration, solution version 13.0.0 release.

Enhanced B2B Connection Association Management

The existing Connection Association page has been split into separate Inbound Connection Rules and Outbound Connection Rules pages to simplify B2B connection management.

- The Inbound Connection Rules page displays all existing B2B Connections by default and allows users to update the associated Company or Location

through a simplified interface.

- The Outbound Connection Rules page organizes outbound routing into Default Company Connection, Default Connections for Locations, and Override Default Settings, while enforcing unique routing rules to prevent duplicate configurations.

These changes simplify inbound and outbound connection management and provide a more intuitive user experience.

Impact analysis

The impacts for these features are the same as Enhanced B2B Connection Association Management feature in the Administration, solution version 13.0.0 release.

Generate API Keys for Integration Principal Users

System administrators can now generate API keys for Integration Principal users directly from the Integration Principal details page to simplify the setup of machine-to-machine integrations. Previously, administrators had to rely on manual processes outside the UI to generate API keys, making integration setup more time-consuming. When an Integration Principal is created, TraceLink automatically generates an API key and displays it on the Integration Principal details page. Each API key includes an access key and a private key. For security reasons, the private key can be viewed and copied only within 5 minutes of being generated. After the private key expires, a new API key must be generated.

Impact analysis

The impacts for these features are the same as Generate API Keys for Integration Principal Users feature in the Administration, solution version 13.0.0 release.

User Access Management Through User Groups

This release introduces User Groups, which enable System Administrators to manage network memberships and role assignments for multiple users at once. Previously, administrators had to assign network access and roles individually for each user. Now, they can assign access once at the group level and apply it to multiple users.

User Groups also strengthen governance by preventing duplicate or conflicting network access assignments. Users cannot receive access to the same network through both an individual membership and a User Group membership, or through multiple User Groups. Memberships inherited through a User Group are clearly identified and can be managed only through the associated User Group.

This enhancement reduces administrative effort, improves consistency, and helps ensure secure and predictable access management across the platform.

Impact analysis

The impacts for these features are the same as User Access Management Through User Groups feature in the Administration, solution version 13.0.0 release.

Business Teams for Applications

Administrators can now create and manage Business Teams for Applications (Links) in US Compliance and Serialized Operations Manager (SOM) applications to control partner visibility for owner users. Previously, Business Teams were supported only for Networks in Multienterprise Information Network Tower (MINT) and Process Orchestration, Execution, and Tracking (POET) applications, and owner users had visibility into all partner data within a service. Administrators can now assign service links to Business Teams and associate them with user network memberships, allowing users to access only the partners assigned to their Business Team. Users without a Business Team continue to have access to all partners.

This enhancement provides more granular access control, enables organizations to restrict partner visibility where needed, and delivers a consistent Business Team access model across both Process Networks and Services.

Impact analysis

- Interface options:
 - Processing
- Business segment impacts:
 - All business segments for Owners

Additional Identifiers in B2B Integration Link Settings

Company Administrators can now add multiple company and location identifiers in the Additional Identifiers section of B2B Integration Link Settings. Previously, Link Settings supported only a single company or location identifier, limiting customers who needed additional identifiers for specific integration scenarios. This enhancement provides more flexible B2B integration configuration by supporting multiple identifiers where needed.

Impact analysis

The impacts for these features are the same as Additional Identifiers in B2B Integration Link Settings feature in the Administration, solution version 13.0.0 release.

Support for Managing Company Locations

OPUS Administration now includes a dedicated Manage Locations experience that enables **Track and Trace Services (TTS)** Administrators and System Administrators to search, view, and maintain company location information. This experience provides the same location management capabilities available in the TTS Manage Locations screen through a centralized interface in OPUS Administration. Administrators can:

- Locate company locations.
- Update location details, including the location name, address, participation in TraceLink applications, and Info Exchange configuration.
- Export location records.

These capabilities help administrators efficiently manage location information while providing a consistent administration experience across OPUS.

Impact analysis

The impacts for these features are the same as Support for Managing Company Locations feature in the Administration, solution version 13.0.0 release.

Support for Managing Company Partners

OPUS Administration now includes a dedicated Manage Partners experience that enables TTS Administrators to search, view, and maintain partner information associated with their company. This experience provides the same partner management capabilities available in the **Track and Trace Services (TTS)** Manage Partners screen through a centralized interface in OPUS Administration. Administrators can:

- Locate partner records.
- Update partner details, including the company name and partner type.
- Manage partner identifiers.

These capabilities help administrators maintain partner information while providing a consistent administration experience across OPUS.

Impact analysis

The impacts for these features are the same as Support for Managing Company Partners feature in the Administration, solution version 13.0.0 release.

Single Sign-On Settings Identity Provider Controls

Company Administrators can now switch between **Company SSO** and **TraceLink SSO** on the Single Single Sign-On Settings page without losing the configured Identity Provider (IdP) settings. Previously, switching from Company SSO to TraceLink SSO removed the configured IdP settings, requiring administrators to reconfigure the Identity Provider before re-enabling Company SSO. This enhancement preserves the existing IdP configuration when IdP authentication is disabled and requires an explicit administrative action to remove the configuration. As a result, administrators can switch between SSO authentication methods more efficiently while retaining existing IdP settings.

Impact analysis

The impacts for these features are the same as Single Sign-On Settings Identity Provider Controls feature in the Administration, solution version 13.0.0 release.

Search and Simplify B2B Integration Link Settings

Company Administrators can now search and filter Link Settings on the B2B Integration Link Settings screen to quickly locate specific B2B connection configurations. Previously, Company Administrators had to manually scroll through the Link Settings list to locate a specific configuration.

This enhancement also simplifies the New Link Settings page by displaying only the General section during initial creation. The Connection Type Information and IDoc Transaction Details sections remain available when viewing or editing a Link Setting after it is created.

Impact analysis

The impacts for these features are the same as Search and Simplify B2B Integration Link Settings feature in the Administration, solution version 13.0.0 release.

Automatically Use Default Transform Versions in Transform Sets

Transform Sets in Administration can now automatically use the transform version designated as Default in Integration Catalog. Previously, users had to select a specific version and manually update each Transform Set to use a newer version. When the Default version changes in Integration Catalog, Transform Sets configured to use the Default version automatically use the new version. Transforms with a Default version display (**Default**) for easy identification.

Impact analysis

- Interface options:
 - Processing
- Business segment impacts:
 - All business segments for Owners

Configure and Simplify Password Requirements

System Administrators can now configure **Minimum Password Length** and **Minimum Number of Special Characters** directly in Single Sign-On Settings. Previously, these password requirements could only be configured through backend settings. The configured requirements automatically apply when users create, change, or reset passwords, making password policy management simpler and more efficient.

Impact analysis

The impacts for these features are the same as Configure and Simplify Password Requirements feature in the Administration, solution version 13.0.0 release.

Resolved issues

Administration, version 2026.2.1

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-44365: Incorrect Roles Display for Process Networks Using Company-Specific or Marketplace Solutions	Processing	Assigning user roles for a Process Network configured with a company-specific or Marketplace solution displayed roles from the base standard solution instead of the solution attached to the Process Network. The Roles drop-down in Users, New Network Membership now displays the correct solution-specific roles for assignment. This issue is resolved.

Administration, version 2026.2.0

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
TL-102599: Network and App Administrators Can View Unauthorized Applications and Networks	Processing	Network and App Administrators could view all company applications and networks in drop-down menus across Network Members, Network and Apps, Links, and Business Teams , regardless of their administrative permissions. The drop-down menus now display only the applications and networks that the Network and App Administrator is authorized to manage. This issue is resolved.
CMCP-43838: Bulk Partner Link Upload Fails for Unmatched Master Data Identifiers	Processing	Bulk partner link CSV uploads failed with a technical error when an identifier had no matching Master Data record. The upload now skips unmatched identifier rows, continues processing valid partner links, and displays clear error details for affected rows. This issue is resolved.

ID	Interface	Issue Description
CMCP-108523: Company User Exports Include Inactive Users	Processing	Company User CSV exports included users with inactive company memberships even though they were hidden from the UI. Detailed and Import-Compatible CSV exports now include only users with active company memberships, aligning exported data with the Company Users screen. This issue is resolved.
TL-111103: Application Owner Filter Does Not Update Message Settings Results	Processing	The Message Settings table did not refresh results when filtering by Application (Owner) . The correct results are now displayed. This issue is resolved.
CMCP-41703: Search Results Exceed Selected Rows-Per-Page Limit	Processing	Search result tables displayed more records than the selected rows-per-page limit across Network and Apps, Network Links, Failed Links, Business Teams, Message Settings , and Integration Principals . The tables now display the correct selected number of rows per page. This issue is resolved.
CMCP-43124: Network Members Search Fails with a Gateway Timeout	Processing	Searching or filtering Network Members could fail due to excessive backend queries. The search is now optimized to reduce unnecessary backend requests and load results reliably. This issue is resolved.
CMCP-43304: Single Sign-On Configuration Updates Fail When Login Attempts Value Is Missing	Processing	Saving Single Sign-On configuration or certificate updates failed when the failed login attempts value was missing. The value is now optional, allowing SSO updates to save successfully when it is not provided. This issue is resolved.

Known issues

Administration, version 2026.2.1

There are no known issues in this release.

Administration, version 2026.2.0

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
TL-115318: Default Outbound Identifier Updates Delayed in TTS UI	Processing	When the Default Outbound Identifier Type or Default Outbound Identifier Value is updated in Manage Locations in OPUS Administration UI, the updated value does not immediately appear in Track and Trace Services (TTS) UI due to a cache synchronization delay. The updated value appears after approximately one minute or when the TTS UI page is refreshed.
TL-114059: Manage Location update fails for Default Outbound Identifier Type	Processing	Users may encounter a validation error when updating location attributes in OPUS Administration if the location has a Default Outbound Identifier Type that is supported by the TraceLink Network but not recognized by OPUS . This prevents any changes to the location from being saved. Contact TraceLink support to edit attributes for an affected location.

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](#)