tracelink
NETWORK FOR GREATER GOOD

OPUS Administration: Part 2

Table of Contents

Administering TraceLink

Learning Objectives

At the end of this module, you will be able to:

- Manage Network Company Details.
- Configure Single Sign-On.
- Access TTS Administration and Management in OPUS.
- Conduct Company Audit.

Overview

When TraceLink enables your company for TraceLink Single Sign-On (TLSSO) with OPUS (Orchestration Platform for Universal Solutions), it assigns an OPUS System Administrator at your company. The System Administrator is a super user who has access to perform all administration functions in OPUS Administration. If an individual already has the Company Administrator role in TTS, it is best to assign the same individual the System Administrator role in OPUS.

What you learned in previous course?

In the previous course, you learned how to manage your company's Digital Twin within OPUS and oversee its networks, partners, links, and users.

You now understand how to navigate the OPUS administration interface and manage both enterprise and multienterprise network applications to support different business use cases. You learned how to establish secure digital links with partners by connecting digital twins, enabling collaboration and data exchange.

You also gained knowledge of user management, including onboarding users, assigning appropriate roles, and organizing them into Business Teams to control access effectively. In addition, you became familiar with key administrator roles such as System Administrator and Network Apps Administrator and how they govern system configuration and network operations.

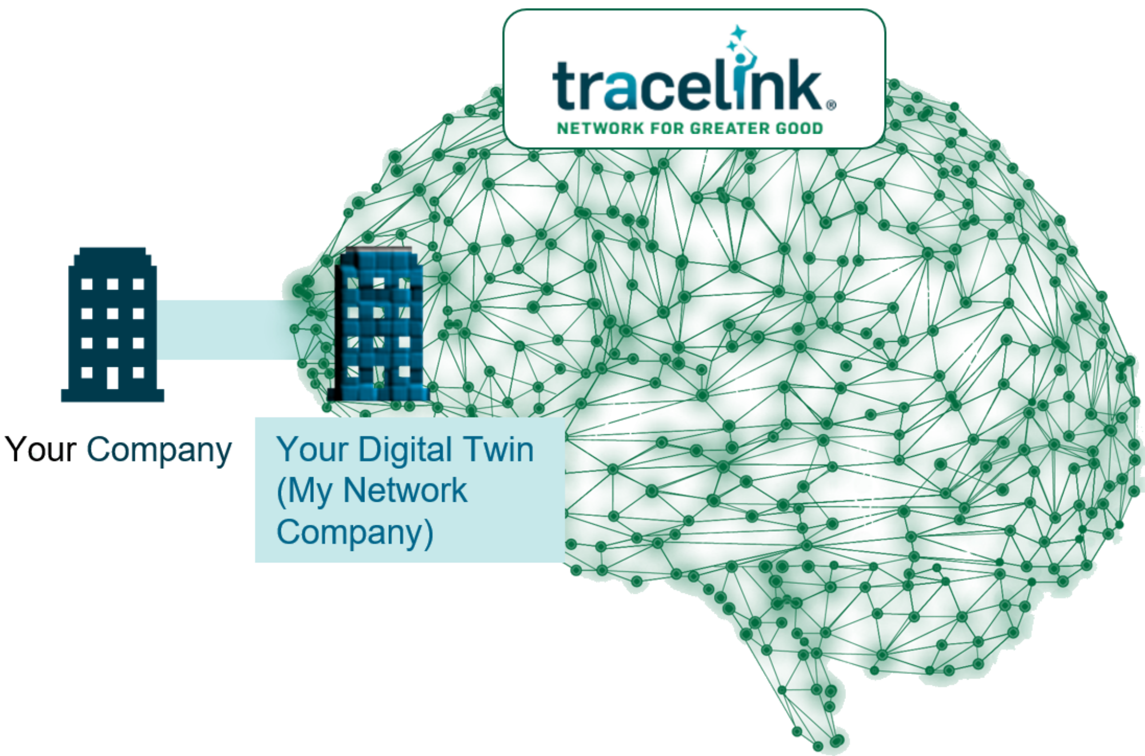
Overall, you learned how to securely configure, manage, and govern your organization's presence and collaborations within the TraceLink network.

Managing Your Network Company Details

Overview

When you connect to TraceLink, TraceLink creates a network profile for your company in the TraceLink ecosystem. This profile serves as a Digital Twin of your organization. A Digital Twin digitally represents your company on the TraceLink network and includes key information of your company.

You manage your network company information on the **My Network Company** page. On this page, System Administrators update company details such as the company profile and logo, headquarters information, and business contact details. The information you enter determines how your company appears in the TraceLink network and how customers and trading partners can view it, based on permission settings.



Only users with the System Administrator role can create or update these company details. This ensures accurate information and proper control over your company's data.

Updating My Network Company Details

As a System Administrator, you can update your network company profile, headquarter details, business contact information and add a logo.

Update My Network Company Details

To update my network company details:

1. Log in to *opus.tracelink.com.*
2. Select **Administration** from the **Main Menu** .
3. In the side menu, select **My Network Company > My Network Company**.
4. Click **Edit**.
5. Under **Profile**, enter details about your company such as its industry and segment.
6. To add or update the logo for your network company, under **Company Logo**, drag-and drop the file or click the field and browse to your logo file, and click **Open**.

   You can upload a .bmp, .jpg, .gif, or .png file. The file size limit is 2 KB.
7. Under **Headquarters**, enter your **Headquarter Address**, as well as the primary phone number and fax.
8. Under **Business Contact** you can enter business name, telephone and email address for your company.

Configuring Single Sign On Details

Overview

The Single Sign-On (SSO) function allows your company to control how users authenticate and access the OPUS platform. In practical terms, it determines what login method your employees use when they navigate to opus.tracelink.com and defines the authentication rules that apply to them.

Through the SSO configuration, administrators can decide whether users log in with standard TraceLink credentials (such as username and password) or through the company's corporate identity provider (such as Microsoft Azure AD, Okta, or another SAML-based system). When SSO is enabled, users typically sign in using their existing corporate credentials, which provides a seamless login experience and aligns with the company's internal security policies.

The SSO settings also control specific login requirements, such as authentication protocols, identity provider configuration, certificate management, and related security parameters. These settings ensure that user access complies with your organization's IT and security standards.

Only users assigned the System Admin role can configure or modify SSO settings. Because SSO operates at the company level, any changes made to these settings apply to all users within the organization. For this reason, administrators should carefully review and validate any updates before applying them to avoid unintended access disruptions.

Configuring Single Sign-On Settings

To ensure security, System Administrators can configure sign-on settings. You can specify settings for timeouts, account lock-out, password expiration, and password reuse.

To Configure Sign-On Settings

1. Log in to *opus.tracelink.com.*
2. Select **Administration** from the **Main Menu** .
3. In the side menu, select **Single Sign-On Settings > Sign-On Settings**.

4. Click **Edit**.

5. To set Authentication Method, under the **General** section:
    a. Select Authentication Method from the drop-down.

        - Tracelink SSO – Select this to authenticate users through the TraceLink's SSO system.

        - Company SSO – Select this to authenticate users through your company's own SSO system.

    b. Enable the multi-factor authentication method by the enabling the switch to use secondary authentication method.

    c. Enter the number of minutes in the **Expire User Session After** field to configure the amount of time before a user's session expires.

If you have selected TraceLink SSO as an authentication method, you can configure the **Failed Login Attempts** and **Password Settings**.

6. To lock users out of their accounts if they exceed login attempts:

    a. Select **Failed Login Attempts**, and specify the number of attempts allowed before the account is locked.

    b. Specify the number of minutes for which the user's account will be locked before they can try again to log in. For this, you have to enable the **Auto-Unlock Account After Specific Duration** toggle switch.

    By default, the account remains locked, users have to reset the password to regain the access.

7. To configure passwords to expire:
    a. Select **Password Settings**.

    b. Specify the number of days before a password will expire. For this, you have to enable the **Password Auto Expires** toggle switch.

    c. To prevent users from reusing previous passwords, enable **Restrict Reuse of Previous Passwords** toggle switch, and also specify the number of previous passwords users cannot reuse.

If you have selected Company SSO as an authentication method, you will have to add the Single Sign-On certificate and URL for your company.

Accessing TTS Administration through OPUS iFrames

Overview

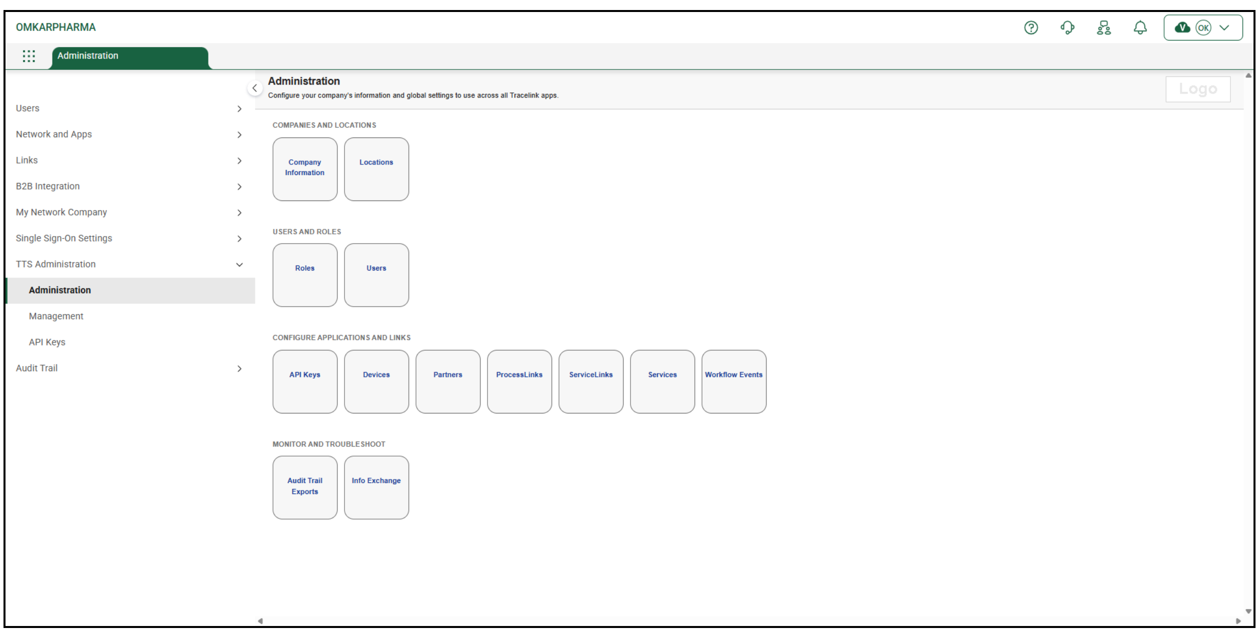
You can administer TTS applications directly in OPUS Administration through an embedded iFrame integration. This setup allows you to access and manage administrative functions of TTS without leaving the OPUS platform. You can also manage API credentials for internal companies and locations through a dedicated API Keys interface within this menu.

To perform these tasks, you must have either the TTS Administrator/TTS Manager role or the System Administrator role. Once you have the appropriate role assigned, you can access the TTS Administration module and perform required configuration and management tasks.

The **TTS Administration** side menu consists of three main sections:

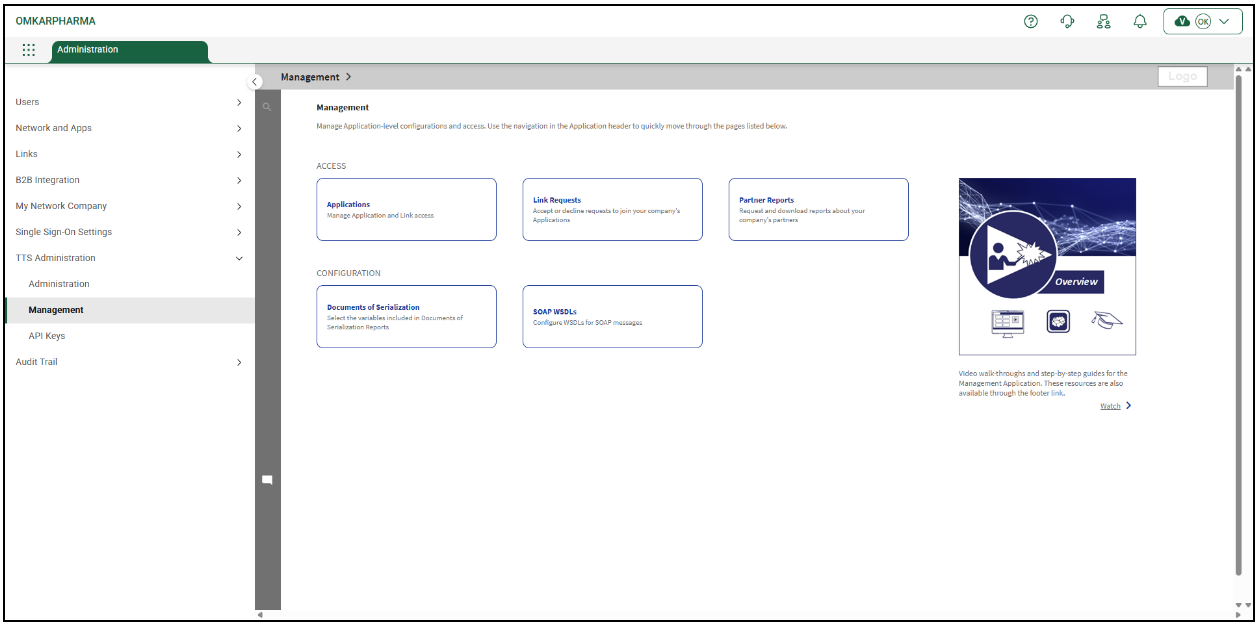
1. Administration

In the Administration section, you configure and maintain the core system environment. You manage users and roles, update company details, configure locations, manage partners, and set up devices for serialization and traceability. This section focuses on system setup and configuration.



2. Management

In the Management section, you handle day-to-day operational activities. You manage applications and access links, request and download partner reports, use compliance tools, set up data rules, and review system messages. This section focuses on daily operations and monitoring.



3. API Keys

You can use the API Keys interface to create, view, activate, and deactivate API keys for internal companies and locations. When you create a key, the private key is shown only once and remains visible for 30 minutes. You must securely copy and store it immediately (e.g., in a password vault). You can centrally manage all keys, monitor their status, and activate or deactivate them as needed to control access. This allows you to securely enable system integrations, enforce lifecycle management, and quickly revoke access if a key is no longer needed or is suspected to be compromised.

Access TTS Administration

As a System Administrator, you can access TTS Administration and Management through OPUS iFrame. Also you can access TTS API Keys.

Access TTS Administration and Management

Note: If you do not have the **System Administrator** role, you need the **TTS Administrator** role to access the Administration sub menu and the **TTS Manager** role to access the Management sub menu in order to perform these steps.

To Access TTS Administration and Management:

1. Log in to *opus.tracelink.com.*
2. Select **Administration** from the **Main Menu** .
3. From the side menu, select **TTS Administration > Administration** or **TTS Administration > Management**.

Access TTS API Keys

As a System Administrator, you can access API Keys function.

Add a new API Key or Update the status of API Key

Note: You need to have the **System Administrator** or **TTS Administrator** role to perform these steps.

To create new API Key:

1. Log in to *opus.tracelink.com.*
2. Select **Administration** from the **Main Menu** .
3. From the side menu, select **TTS Administration > API Keys**.
4. Click **New**.
5. Select the **Company Location**.

The **Identifier Value** and **Identifier Type** associated with the company location will be filled automatically.

6. Click **Save**.

To update the status of API Key.

1. In the **Search API Keys** screen, select the API key you want to update.
2. Click **Update Status**.
3. In the side panel, select **Apply** to change the status from Active to Inactive or from Inactive to Active.

Conducting Audit

Overview

You can use the Audit Trail function in OPUS to view and review changes made in the system.

The Audit Trail shows you the exact date and time a change was made, which user made the change, what data was updated, and where the change occurred (for example, in a specific application or through the user interface).

You can search, filter, and export this information to help track activity, investigate issues, and maintain transparency and compliance.

Note: Only users assigned the **System Administrator** or **Audit Manager** roles are authorized to create and export company and SSO audit reports for further review.

Requesting an Audit Trail Export for Company and SSO Audit

Using the **Administration > Audit Trail** page, you can request an audit trail for your Company and SSO data. You need to have System Administrator or Audit Manager role to perform these steps.

To Request and View an Audit Trail Export for Company and SSO Audit

To request an audit trail export for Company Audit:

1. Log in to *opus.tracelink.com.*
2. Select **Administration** from the **Main Menu** .
3. In the side menu, select **Audit Trail > Company Audit**.
4. Click **New**.
5. Type or select the From Date and time.
6. Type or select the To Date and time.

7. Select the **Export File Type** from the drop-down.

8. Click **Save**.

The report is generated asynchronously and may take several minutes to complete. Once the process is finished, you can download the report in **PDF** or **CSV** format.

9. Click **Download** icon to download the report in selected format.

To request an audit trail export for SSO Audit:

1. Log in to *opus.tracelink.com.*

2. Select **Administration** from the **Main Menu** ⁝⁝⁝.

3. In the side menu, select **Audit Trail > SSO Audit**.

4. Click **New**.

5. Type or select the From Date and time.

6. Type or select the To Date and time.

7. Select the **Export File Type** from the drop-down.

8. Click **Save**.

The report is generated asynchronously and may take several minutes to complete. Once the process is finished, you can download the report in **PDF** or **CSV** format.

9. Click **Download** icon to download the report in selected format.