TRACELINK UNIVERSITY



# Direct Supplier Incident

Direct supplier incidents are those that occur within suppliers with whom a company has a direct commercial and operational relationship.

## What is a direct supplier incident

Direct supplier incidents allow users at companies that own or link to POET (e.g. supplier relationship managers, quality compliance managers, manufacturing plant managers) to collaborate with their internal locations and external Partners to investigate and resolve problems, as well as update processes to ensure an incident does not happen again. For example, a Supplier might need to report a shortage in raw materials to a Manufacturer, or a CMO might need to report a late or missing shipment from the Supplier to the Manufacturer.

## Types of direct supplier incidents

- **Quality Issues:** Problems with the identity, strength, purity, or labeling of supplied materials that may compromise product quality or patient safety.

- **Deviation Events:** Failures to follow established procedures or maintain required process parameters, often due to equipment or environmental factors.

© TraceLink Inc. 2009 - 2025 All Rights Reserved

- **Delivery and Logistics Failures:** Breakdowns in the timely and accurate supply of materials, impacting production schedules and continuity.

- **Regulatory and Compliance Breaches:** Non-conformance with applicable regulations or quality standards, which may result in citations, warnings, or audit failures.

- **Change Control Failures:** Unapproved changes to processes, materials, or specifications that can affect quality, compliance, or performance.

- **Performance Issues:** Ongoing supplier under-performance that negatively impacts quality, reliability, or service delivery.

- **Data Integrity Issues:** Compromises in the accuracy, completeness, or reliability of records that support quality and compliance.

## How to configure the direct supplier incident marketplace solution

Before using the batch record review marketplace solution, Solution Designers must first configure the solution in Opus Solution Environment (OSE) by following the steps listed below:

### Save the marketplace solution as a company solution in OPUS Solution Environment

Solution Designers must first save the latest version of the marketplace solution from the marketplace catalog as a company solution.

1. Select the Main Menu icon.
2. Select OPUS Solution Environment.
3. Select Catalog from the left menu.

© TraceLink Inc. 2009 - 2025 All Rights Reserved

4. Select Marketplace Solutions.
5. On the Search Solutions page, filter the list of solutions to find the required solution.
6. Find the latest version of the solution and select the Solution Name to open the solution.
7. On the Solution Details page, select Save As.
8. On the Save As panel, fill in the following fields:
    a. Solution Name field – The name of the solution that will be saved as a company solution.
    b. Description field – (Optional) The description of the solution.
9. Select Apply.

    The marketplace will be saved as a company solution in the Available tab on the left menu.

### Create a network for the solution in OPUS Administration

After saving the solution as a Company Solution, Solution designers must create a network for the solution from OPUS Administration.

1. Select the Main Menu  icon.
2. Select Administration.
3. Select Network and Apps from the left menu.
4. Select New.
5. In the Network Information section, fill in the following fields:
    a. Application drop-down – Select the application for which you want to configure the marketplace solution. For e.g. Process Orchestration for Empowered Teams.
    b. Network Name field – The name of the network being created.
    c. Network Description field – (Optional) The description of the network being created.
6. In the Solution section, fill in the following fields:
    a. Standard Solution toggle – This value must be no as the solution for

© TraceLink Inc. 2009 - 2025 All Rights Reserved

which the network is being created is a marketplace solution.

b. Company Solution field – Select the solution that you saved as a company solution in the previous procedure.

7. Select Save.

   The new network is created and the solution is ready for use.

#### Configure roles for the new network in OPUS Administration

After creating a network for the solution, Solution Designers must define roles for accessing the network.

1. Select the Main Menu icon.
2. Select Administration.
3. Select Users from the left menu.
4. Select Network Members from the left menu.
5. On the Search Network Members page, filter the list of network members by the network created in the previous procedure.
6. Select the user email of the user who created the network.
7. Select Edit.
8. In the Roles section, select the role required to access the network.
9. Select Save.

   The role to access the new network is configured.

For more information about configuring or customizing marketplace solutions as per your business needs, see OPUS Solution Environment Help Center.

## Add a direct supplier incident

#### Add a direct supplier incident

By default, a direct supplier incident is created by a set of basic fields, which are widely used. However, depending on your business needs, you may need to include additional fields in the manufacturing incident. To include additional fields,

© TraceLink Inc. 2009 - 2025 All Rights Reserved

edit the direct supplier incident to view all available fields and update the required fields.

1. Select the Main Menu icon.
2. Select My Networks.
3. Select a [POET Network] from the Select your Network drop-down in the header.
4. Select a Partner or location from the Select your Partner or Location drop-down in the header.
5. Select Go.
6. Select Direct Supplier Incident from the left menu.
7. Select New.
8. In the General section fill in the following fields:
    a. Title field – The title of the new direct supplier incident.
    b. Description field – The description of the direct supplier incident.
9. Select Save.
   The direct supplier incident is created in the Draft state.
10. To move the direct supplier incident to To Do state, select Move to.

## Modify a direct supplier incident

### Edit a direct supplier incident

1. Select the Main Menu icon.
2. Select My Networks.
3. Select a [POET Network] from the Select your Network drop-down in the header.
4. Select a Partner or location from the Select your Partner or Location drop-down in the header.
5. Select Go.
6. Select Direct Supplier Incident from the left menu.
7. Select the Display Identifier of the direct supplier incident to edit.

© TraceLink Inc. 2009 - 2025 All Rights Reserved

8. Select Edit.

   In addition to the fields updated when creating the direct supplier incident, additional fields will be displayed which can be updated if required.

9. In the General section update the following fields:
    a. Display Identifier field – The display identifier of the direct supplier incident.
    b. Title field – The title of the direct supplier incident.
    c. Category field – The type of the direct supplier incident. For example: Quality Issues, Deviation Events, Delivery and Logistics Failures, etc.
        i. If you selected Quality Issues in the Category drop-down, add the required sub-category information:
            a. Sub-category field – The sub-category of the selected category. For example: Out-of-Specification (OOS) Results, Contamination, Incorrect Labeling.
            b. Lot Numbers Affected field – The batch or lot affected by the direct supplier incident.
            c. Quality Systems Affected field – The type of deviation for the direct supplier incident.
            d. Additional Testing Needed field – Indicates if retesting is required.
            e. SOPs/Work Instructions to Update field – The list of procedures needing revision.
            f. Validation Required field – Indicates whether re-validation is necessary.
        ii. If you selected Deviation Events in the Category drop-down, add the required sub-category information:
            a. Sub-category field – The sub-category of the selected category. For example: Process Deviation, Equipment Failure, Temperature Excursion.
            b. Equipment or Process Affected field – The description of

© TraceLink Inc. 2009 - 2025 All Rights Reserved

impacted equipment or process.

c. Expected Downtime field – The estimated downtime in hours or days.
d. Deviation Reference Number field – Link to associated deviation record.
e. Root Cause Identified field – Indicates if root cause analysis has been completed.
f. CAPA Linked field – Indicates whether a CAPA has been initiated.

iii. If you selected Delivery and Logistics Failures in the Category drop-down, add the required sub-category information:
   a. Sub-category field – The sub-category of the selected category. For example: Delayed Shipments, Damaged Goods, Incorrect Quantities.
   b. Estimated Delay in Delivery (Days) field – The number of days delayed.
   c. Inventory Impact field – The description of how inventory is affected.
   d. Alternate Routes Available field – Backup logistics options.
   e. Packaging Condition Notes field – Notes on damage or labeling issues.
   f. Carrier Involved field – Name of shipping or logistics provider.
iv. If you selected Regulatory and Compliance Breaches in the Category drop-down, add the required sub-category information:
   a. Sub-category field – The sub-category of the selected category. For example: Form 483, Missing Certificate of Analysis (CoA), Failed Audit.
   b. Regulatory Body Involved field – The regulatory body associated with the breach. For example: FDA, EMA, CDSCO, etc.

© TraceLink Inc. 2009 - 2025 All Rights Reserved

c. Re-approval Required field – Indicates whether new submission is required.
d. Submission Timeline field – The target date for regulatory submission.
e. Documents to Update field – List of impacted regulatory documents.
f. Audit Reference Number field – Link to internal audit record.
g. CAPA Required field – Indicates whether CAPA is mandated by the breach.

v. If you selected Change Control Failures in the Category drop-down, add the required sub-category information:
   a. Sub-category field – The sub-category of the selected category. For example: Form 483, Missing Certificate of Analysis (CoA), Failed Audit.
   b. Change Description field – Describes what was changed without approval.
   c. Date of Change field – The date when the change occurred.
   d. Product Formulation Changed field – Indicates whether formulation was affected.
   e. Regulatory Notification Needed field – Indicates if change requires an external notification.

vi. If you selected Performance Issues in the Category drop-down, add the required sub-category information:
   a. Sub-category field – The sub-category of the selected category. For example: Repeated CAPAs, Poor Audit Scores, Low OTIF (On-Time In-Full).
   b. OTIF % field – The On-Time In-Full performance metric.
   c. CAPA History Summary field – The summary of past CAPAs for this supplier.
   d. Audit Score (%) field – The most recent audit score.

© TraceLink Inc. 2009 - 2025 All Rights Reserved

e. Escalation Required field – Indicates whether issue requires escalation.
f. Performance Review Date field – The last formal performance review.

vii. If you selected Data Integrity Issues in the Category drop-down, add the required sub-category information:
a. Sub-category field – The sub-category of the selected category. For example: Tampered Test Results, Backdated Entries, Incomplete Batch Data.
b. Affected Records field – The description of records/data involved.
c. System Involved field – The systems involved in the incident. For example: LIMS, ERP, MES, etc.
d. Investigation Initiated field – Indicates whether internal investigation has begun.
e. Root Cause Analysis Status field – Indicates the status of the root cause analysis. For example: Not Started, In Progress, Completed, etc.
f. Regulatory Exposure field – Indicates whether this incident has been reported externally.

d. Incident Date field – The date when the direct supplier incident occurred.
e. Due Date field – The due date of the direct supplier incident.
f. Business Priority field – The level of priority for the direct supplier incident. Select from Low, Medium, High, and Critical.
g. Description field – The detailed description of the direct supplier incident.

10. If you require to collaborate with an external partner, enter the details under the Participants section:
a. Initiator Company field – The name of the company that created the direct supplier incident. This field is automatically populated with the logged-in user.

© TraceLink Inc. 2009 - 2025 All Rights Reserved

b. Assignee Company field – The name of the Partner company that is assigned to take action on the direct supplier incident.

11. In the Product Information section, add information about the impacted product in the following fields:
    a. Product Name field – The name of the impacted product.
    b. Item Code Type field – The item code type of the impacted product.
    c. Item Code Value field – The item code value of the impacted product.
    d. Product GTIN field – The GTIN of the impacted product.
    e. Batch/Lot Number field – (Optional) The batch or lot number of the impacted product.
12. In the Locations Affected section, add location information in the following fields:
    a. Business Name field – The business name of the location affected
    b. Identifier Type field – The identifier type of the location affected
    c. Identifier Value field – The identifier value of the location affected
    d. Risk Level field – The level of risk associated with the direct supplier incident. For example: None, Low, Medium, High, Critical.
13. Select Save.
    The direct supplier incident is updated.

Owners can edit the Assignee Details section while the batch record review is in the Draft state. Once the work item moves to the To Do state, the Assignee Details section can be edited only once.

## Direct supplier incidents workflow

The following workflow states are used to track the progress of a direct supplier incident:

© TraceLink Inc. 2009 - 2025 All Rights Reserved

| Base State | Workflow State | Description |
|---|---|---|
| Draft | Draft | The direct supplier incident has been created and is in its initial state. It remains editable by the user who created it until it is submitted for action. |
| To Do | To Do | The direct supplier incident has been assigned for review or action and is awaiting follow-up. When applicable, the relevant supplier partner is notified. |
| In Progress | Under Investigation | The direct supplier incident is actively being investigated. Authorized users can update the record while the issue is assessed, the root cause is identified, and appropriate corrective actions are defined. |

© TraceLink Inc. 2009 - 2025 All Rights Reserved

| Base State | Workflow State | Description |
|---|---|---|
| In Progress | Under Resolution | The required resolution actions are being completed or have been completed and are undergoing verification to confirm the incident has been addressed effectively. |
| Done | Done | The direct supplier incident has been resolved, verified, and formally closed. No further action is required. |

## Monitor direct supplier incident

A high level understanding of the state of all direct supplier incidents that you have access to.

#### View the dashboard (Owner)

1. Select the Main Menu icon.
2. Select My Networks.
3. Select a [POET Network] from the Select your Network drop-down in the header.
4. Select a Partner or location from the Select your Partner or Location drop-down in the header.
5. Select Go.

© TraceLink Inc. 2009 - 2025 All Rights Reserved

6. Select Direct Supplier Incidents Dashboard from the left menu.
   View the widgets in the dashboard, which display pre-defined queries to demonstrate the state of all direct supplier incidents at a high level.

| Metric | Description |
|---|---|
| Status | Direct supplier incidents classified according to workflow status (Draft, To Do, In Progress, Done). |
| Business Priority | Direct supplier incidents classified according to business priority (Critical, high, medium, low) combined with workflow status. |
| Category | Direct supplier incidents classified by exception category. |
| Sub-Category | Direct supplier incidents classified by exception sub-category. |
| CAPA Required | Direct supplier incidents classified by CAPA required or CAPA not required. |
| Incident Aging Report | Direct supplier incidents classified by age (0-7 days, 8-14 days, 15-30 days, >30 days). |
| **Due Date Monitoring** | |
| Direct Supplier Incidents Overdue | Direct supplier incidents past Due Date by currentState. Escalates compliance and execution risks. |
| Direct Supplier Incidents Due in Next 24 Hours | Direct supplier incidents due within 24 hours by currentState. Highlights items requiring immediate executive attention. |
| Direct Supplier Incidents Due in Next 7 Days | Direct supplier incidents due within 7 days by currentState. Supports short-term workload planning. |
| Direct Supplier Incidents Due in Future | Direct supplier incidents due beyond 7 days by currentState. Supports capacity forecasting. |

### View the dashboard (Partner)

1. Select the Main Menu icon.
2. Select My Networks.
3. Select a [POET Network] from the Select your Network drop-down in the header.
4. Select a Partner or location from the Select your Partner or Location drop-down in the header.
5. Select Go.
6. Select Direct Supplier Incidents Dashboard from the left menu.
   View the widgets in the dashboard, which display pre-defined queries to demonstrate the state of all direct supplier incidents at a high level.

© TraceLink Inc. 2009 - 2025 All Rights Reserved

| Metric | Description |
|---|---|
| Business Priority | Direct supplier incidents classified according to business priority (Critical, high, medium, low) combined with workflow status. |
| Status - Open | Direct supplier incidents classified by state (To Do, In Progress). |
| Category | Direct supplier incidents classified by exception category. |
| Sub-Category | Direct supplier incidents classified by exception sub-category. |
| Due Date | Direct supplier incidents classified by due date combined with workflow status. |
| Due Date and Business Priority | Direct supplier incidents classified by due date and business priority. |
| Resolution Time by Category | Direct supplier incidents classified by the time required to resolve incidents grouped by category. |
| **Due Date Monitoring** | |
| Overdue Direct supplier incidents | Direct supplier incidents past Due Date by currentState. Escalates compliance and execution risks. |
| Due in Next 24 Hours | Direct supplier incidents due within 24 hours by currentState. Highlights items requiring immediate executive attention. |
| Due in Next 7 Days | Direct supplier incidents due within 7 days by currentState. Supports short-term workload planning. |
| Due in Future | Direct supplier incidents due beyond 7 days by currentState. Supports capacity forecasting. |

### Search direct supplier incident

1. Select the Main Menu icon.
2. Select My Networks.
3. Select a [POET Network] from the Select your Network drop-down in the header.
4. Select a Partner or location from the Select your Partner or Location drop-down in the header.
5. Select Go.
6. Select Direct Supplier Incident from the left menu.
7. Select Filter.
8. In the Filters panel, fill in one or more of the following fields to filter the results:
    a. Display Identifier field – The display identifier of the direct supplier incident.

© TraceLink Inc. 2009 - 2025 All Rights Reserved

b. Due Date field – The due date of the direct supplier incident.
c. Business Priority field – The business priority of the direct supplier incident.
d. State field – The state of the direct supplier incident.
e. Title field – The title of the direct supplier incident.
f. Category drop-down – The category of the direct supplier incident. For example: Quality Issues, Regulatory, etc.
g. Last Modified Time field – The last modified date and time of the direct supplier incident.
h. Incident Date field – The date when the direct supplier incident occurred.
i. Subcategory drop-down – The sub-category of the direct supplier incident.
j. Initiator Company field – The company which initiated the direct supplier incident.
k. Assignee Company field – The company which was assigned the direct supplier incident.

9. Select Apply.

   All direct supplier incidents matching the filter criteria are displayed.

© TraceLink Inc. 2009 - 2025 All Rights Reserved