Platform Tracker User’s Guide

Table of Contents

Introduction

General Overview of the Platform Tracker

Platform Tracker is useful for an organization that comprises of many products on perm or cloud base that can help to track issues and outages in system(s) for future analysis that can lead to new projects to improve product(s) quality and resiliency.

Product highlights:

1) To stakeholders an accurate platform(s).
2) To provide a tracking mechanism, complete with an automated alerting system (Incident → RCA → Response)
3) To help prioritize responses to incidents based on relative bang for the buck of each response
4) To automatically generate Incident Reports, thereby enabling them to become living documents with actively monitored follow-up action items.

This document is meant to be used as a companion to the application itself.

Key Application Entities

Six entities are central to tracking system:

Incidents – These can be failures to a single application function, unacceptable application slowdowns, or outright outages. Incidents trigger downstream actions and can lead to subsequent platform stabilizing projects.

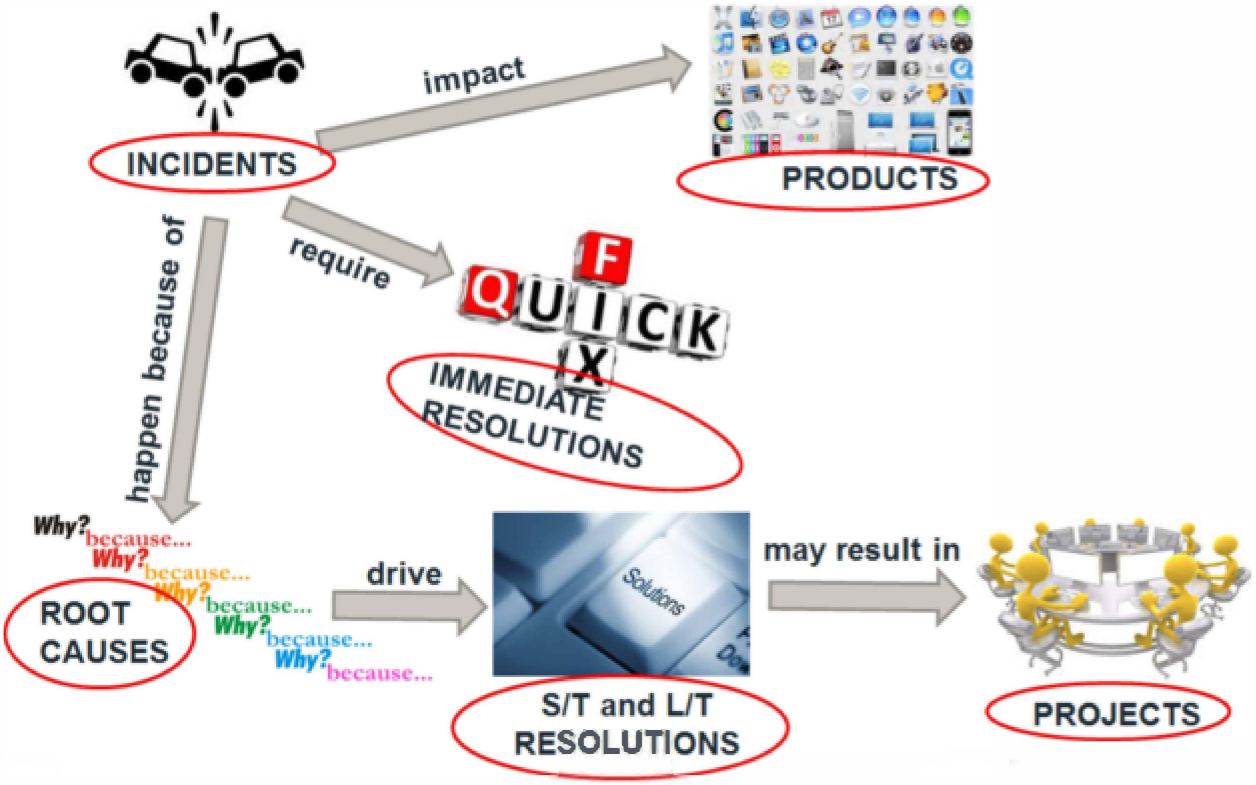
Incidents Groups – These are groups of Incidents that have the same root cause and call for the same set of resolutions. Grouping incidents allows us to more accurate trace problems to solutions.

Root Cause Analyses (RCA) – Some percentage of incidents rise to a level of severity to warrant a formal root cause analysis. As part of its incident-tracing functionality, Platform Tracker captures all related information required for the generation of a Root Cause Analysis (RCA) report.

Resolutions – Incidents are resolved immediately, (say via a reboot), in the short-term, and possibly over the long-term as well (say by adding a process that automatically trims log files before they fill up a disk). Short-term and long-term resolutions are determined after a formal RCA, while immediate resolutions are determined before a formal RCA (the objective of immediate resolutions being restore of service as quickly as possible)

Projects – Incidents or sets of incidents can be deemed so severe that a formal project is embarked upon to mitigate or prevent their recurrence.

Products – Products' service levels are impacted by incidents. The goal of Platform Tracker is to understand the relative financial and end user impact of various incidents on the product set with an eye to prioritizing those resolutions associated with incidents having the largest impact on possible business.


INCIDENTS
impact
PRODUCTS
happen because of
require
QUICK FIX
IMMEDIATE RESOLUTIONS
Why? because... Why? because... Why? because... Why? because... Why? because...
ROOT CAUSES
drive
Solutions
S/T and L/T RESOLUTIONS
may result in
PROJECTS

Basic Navigation

Commands Accessible from the Main Screen

The user can **Create** or **Search** for any of the key entities via the main menu across the top of the welcome screen with 2 exceptions:

1. The user can additionally search for incidents by group, that is, select an incident group and see a list of incidents associated with that group
2. The user cannot create an Incident Group from the main menu. All Incident Groups must be associated with at least one Incident, so incident groups are either implicitly created when the user creates an incident or can be explicitly created from the Incident Detail screen, when a user specifies a new Incident Group for the incident being displayed.

Creating New Records

Records can be created directly from the **Create** options off the main menu, or in several instances, in the context of a related entity. For example, RCA and Resolution records can be created from the Incident Group Detail screen. Naturally the RCA and Resolution records created from the Incident Group Detail screen are associated with the Incident Group being displayed.

Navigating the Search Screens

All Search screens support text string search. Searching for "XXX", for example, will show all records that contain the string "XXX" in any of their fields

All Search screens can be sorted by clicking on column headers. Clicking on the column header first sorts it in ascending order, clicking again sorts it in descending order, and clicking again restores the prior order of the records.

The Resolution, RCA, and Project search screens offer record grouping. This grouping functionality is triggered by dragging the grouping attribute to a band above the column headers. Subgrouping is also possible using the same mechanism.

By default, Incidents, RCA's, and Resolutions are sorted in reverse chronological order, with open RCA's and open Resolutions at the top. Incident Groups, Products, and Projects are sorted alphabetically by name.

Making Editing Changes

The details of any record can be accessed via the Search screens. Clicking on an entity's ID takes the user to its Detail screen. Values of any editable field can be modified and the changes are committed to the database when the Save button is clicked.

Clicking on the Back button takes the user back to the Search screen.

The Incident Management Process

Recording the Incident

When an incident happens, you will go to the Create Incident Screen. For the typical incident, you will fill in the following fields to start:

1. GROUP – You can start typing a keyword and select an existing Incident Group, or you can type a new Incident Group name, or you can leave the field blank, and it will be populated by all or part of the Technical Description field.

2. STATUS – This defaults to "Open". You would set it to "Closed" if the Incident was already resolved.
3. EMAIL RCPT – This determines where the Incident Notification emails will go. There are 3 settings:
    a. Desktop Operations Only
    b. Regular Distribution – It goes to product-specific email distribution lists (determined by the Products chosen below), and to the following email distribution: DesktopSupport@dealertrack.com
    c. Escalated Distribution – If Regular Distribution is chosen, emails don't go to the escalation email distribution list until an incident is over 2 hours old. If Escalated Distribution is chosen, the notification emails are immediately sent to the escalation email distribution list. This option might be chosen if the incident were particularly impactful.
4. START DATE TIME (M) – We use a special "Date time Picker" control to expedite the entering of both dates and times together (which we do for Incident start and end time and for Chronology entries). Clicking on the right-hand section of the control opens up a calendar. At this point, you should see the current date highlighted in gray. You can navigate back and forward in time by clicking on the month and year (displayed at the top), but for this example, let's assume that you are entering an incident on the same day it happened. Next you would click on the highlighted date and up comes a list of each hour, each minute, and AM/PM. Click through to the correct hour and minute or you can type them in by hand. Select AM or PM and you're done.
5. END DATE TIME – You would leave this blank unless you had already resolved the incident.
6. NAME – It is optional but required for producing a complete Incident Report. An example might be "MUMPS DB erroneously reports no space left on device"
7. OWNER – It also is optional but required for producing a complete Incident Report. An example might be "Ken Franco".
8. SEVERITY (M) – Here you can choose P1 (the default) for highest severity to P4 for lowest severity incidents
9. ERROR CONDITION (M) – There is a fixed list of values to choose from that was carried forward from the SLM database.
10. LOCUS (M) – This describes the location of the problem, with 4 possible values:
    a. Internal
    b. Comm – The problem involved the communication network
    c. Sys – The problem was with the system itself.
    d. Internet – The problem involved connection to the Internet
11. BUSINESS DESCRIPTION – This field is used to populate the Incident Summary section of the Incident Report. It provides a description of the Incident from the perspective of the Business Users. It can be left blank.
12. TECHNICAL DESCRIPTION (M) – This field is required and is the central description field for the Incident. It provides a description of the incident from a technical perspective.
13. ASSOCIATED PRODUCTS (M) – provides a dropdown list with all active products and the user must choose at least 1.
14. % OF USERS IMPACTED (M) – This generally will be 100%, but there might be outages impacting only a subset of the user community of a particular product or set of products.
15. TRANSACTION IDS IMPACTED – This should be equal to the number of transactions requiring a rebuild because of the outage. It is defaulted to 0.
16. CALLS RECEIVED – It defaults to 0, but the hope is that we can get accurate calls received data for all incidents, allowing for us to track their frequency over time.
17. ALERTED BY (M) – Dropdown set of options, "End User" is the default.

18. CUSTOMER IMPACT – This is used for the Customer Impact section of the Incident Report. For Customer Impact, you might enter something like "Client services received 292 calls during a 2-hour outage".

After filling in all mandatory fields, the user clicks on Submit to create the new record. Note that an Incident Tag is generated comprised of the impacted product's short name (or the keyword "Multi" if there is more than 1 impacted product) and start date and time. Note also that the user's login name is stored with the Incident.

When the user clicks on Submit, a notification email is also automatically sent out, its list of recipients determined by the setting of the "Email Recipient" field. Note that the screen is designed for rapid completion. To create an incident, the only fields that require user action are the Start Time, Technical Description, and Associated Products.

Providing Incident Updates

As long as an incident remains "Open", in the absence of any user intervention, automated emails will be sent every hour, with a warning notification sent to the desktop notification group after 55 minutes of inactivity.

Activities that reset/disable the timer for these automated emails are the updating of the incident or the closing of the incident. Updating an incident is accomplished by adding an entry to the Incident Chronology, which is available from the "Chronology" tab on the Incident Detail screen.

When you are done adding each entry in the Chronology, you can simply exit back to the Search screen by clicking Cancel/Back or navigate to a different screen.

Each update includes a time stamp, a description, and an updater, all of whom are output in an "Update" email notification when the new Chronology entry is saved.

Closing an Incident

Closing the incident is accomplished by specifying an end time for the incident and setting the incident status to "Closed". That will generate a "Resolution" email notification that will be sent to a list of recipients depending on the incident's elapsed time and the setting of the "Email Recipient" field. No more automated emails will be sent from that point on unless operations updates the incident.

Recording Data for the Incident Report

The Incident Report requires several additional pieces of data in addition to what was captured in the Incident's record.

Adding Corrective Actions by Creating Immediate Resolution(s)

Every Internal incident has an Immediate Resolution, that is, the action or actions performed to restore service. Note that we associate data entered in the Immediate Resolution of an Incident to the "Corrective Actions Taken" section of the Incident Report. The specific fields we use are optionally the Issue field, the Description field (required), and optionally the "Related Actions" field, which correspond to the "Issue", "Immediate Corrective Action" and "Other Actions Taken" subsections respectively of the "Corrective Actions Taken" section of the Incident Report.

Adding Further Actions by Creating Short and Long Term Resolutions

Both the Incident Report and the RCA Report have sections for additional actions. The Incident Report has one section called "Further Action Items" while the RCA Report has 2 sections titled "Short-Term Action Items" and "Long-Term Action Items" respectively. If an Incident requires both Reports, you need only enter each action 1 time, either as a short-term or long-term resolution. Here we use the same "Create Resolution" screen as follows:

1. INCIDENT GROUP NAME – Again, select from a dropdown list the Group Name you previously entered or selected on the Create Incident screen

2. HORIZON – Set to Short-Term or Long-Term depending on how far in the future you expect the action item to be completed.
3. OWNER – The person with the main responsibility for the particular action item, selected from a dropdown list of Platform stakeholders.
4. STATUS – Generally set to Open (that is, the Resolution's actions have not been completed, which should typically be the case for Short –term Resolutions and always the case for Long-Term Resolutions). Note that all Open Resolutions will be tracked by the system, and owners will be alerted to all action items that are past due or coming due in the coming week.
5. ESTIMATED COMPLETION DATE – This should be chosen realistically to give the resolution owner(s) a reasonable probability of completion by the due date
6. ACTUAL COMPLETION DATE – This will get filled out after the action item is completed, at which point the status should change to Closed as well.
7. TYPE – select type of resolution from a dropdown
8. SRI ARTIFACT - <TBD>
9. DESCRIPTION – This is an important field because it will be used by both the Incident Report and the RCA Report for the Incident Group associated with the Incident as well as by email alerts sent to Resolution owners

Recording Data for the Root Cause Analysis Report

If you have already produced an Incident Report for a given Incident, you have already recorded most of the information needed to produce a Root Cause Report. Specifically we will have already gathered data to enable us to load the following RCA Report fields (called Placeholders):

1. The Product field with a comma-delimited list of Products impacted by the Incident
2. The Start and End Time with the Incident Start and End Time. Not that if we are reporting on a group of incidents (typically several in rapid succession), then we would concatenate the start and end times of each individual incident.
3. The Description field with a concatenated list of Incident descriptions, which themselves are comprised of 2 parts: Business Description and Technical Description
4. The Resolution field with the Description field of the Immediate Resolution for the Incident Group – multiple Immediate Corrective Actions are concatenated together
5. The Timeline with the list of Timeline entries for all Incidents in the Incident Group
6. The Short-Term Action Items with any Short-Term resolutions associated with the Incident Group
7. The Long-Term Action items with any Long-Term resolutions associated with the Incident Group

That leaves the following RCA Report fields, which are populated by fields on the RCA Detail screen:

8. The Impact field with the PROBLEM field of the RCA screen
9. Why L1 through Why L5 fields with the WHY fields on the RCA screen
10. The Author field with the OWNER of the RCA screen
11. The Date with the COMPLETION DATE of the RCA screen

Working with Projects

Projects can be used in 2 separate instances:

1. When a resolution or resolutions is sufficiently complex that it requires some degree of management
2. When you have several related threads of work that you want to track as parts of a single whole

Recording Project Information

Naturally you use the Create Project command to create a Project record in PST. A project has the following fields:

1. NAME – This is a short description about the project
2. STATUS – By default, it will be "Open" to start
3. OWNERS - The person or persons with the main responsibility for the Project, selected from a dropdown list of Platform Stability stakeholders.
4. PDLC STATUS – This follows the standard 5 phases of Dealertrack projects and will typically be in the "Propose" phase to start.
5. ECDE ID – TBD
6. RECORDING DATE – Date the Project was entered into Tracker system.
7. STATUS CHANGE DATE – At any PDLC status change, we update this field
8. DESCRIPTION – This should give some contextual information for the project. It can be updated with changes in Project status as the project progresses.
9. DUE DATE – This is the expected completion date. This date should be realistic to prevent unneeded alerting from PST to the Project Owner(s)
10. COMPLETION DATE – The date the project actually completes
11. SOLUTION TYPE – The Platform Tracker approach being taken, chosen from a dropdown list
12. ESTIMATED EFFORT – This is an estimate of the number of person-days the entire project will take. This helps identify bang for buck.
13. ACTUAL EFFORT – The actual number of person-days the project took, to be filled in once it has been completed.
14. CONFLUENCE ID – This is the number of the project given if it is being tracked at the Dealertrack corporate level
15. JIRA ID – This is the link to Jira if the project is being tracked in Jira as well.

Linking Projects to Resolutions

We link Projects to Resolutions to be able to estimate operational impact of each project. The resolutions are tied to Incident Groups, which have customer and revenue impact scores associated with them. Say, for example, that a project would eliminate 2 sets of Incidents in the future (that is, 2 Incident Groups), and each Incident Group had a score of 34, then the operational impact of successfully completing that project would be estimated at 68.

Note that each resolution can only be linked to a single project. If the resolution should be linked to multiple projects, then the resolution should be broken into pieces, each of which could be linked to a single project.

The mechanics for linking resolutions to projects are as follows:

1. Enter the Search Projects screen and click on the target Project ID
2. At the bottom of the screen, click on the Link Resolutions button
3. A window pops open, with a list of all Resolutions
4. Use the Filter box to hone in on the related resolutions. Usually this can be done by using a phrase in the Incident Group Name
5. Check all Resolutions that should be linked
6. Click on the Link command
7. "X" out of the window

Working with Products

Products provide the stake holders with the information we need to assess incident impact, both from a customer and revenue perspective. As a result, 2 of the most important fields for each product it is customer score and revenue score. Those scores are actually percentages, indicating how much of the entire organization revenue or customer pie each product slice takes up. Using that % information, we can compute a normalized score for each incident by multiplying the length of the outage by the % of users or revenue associated with each product impacted. We arbitrarily set the impact score of any day-long outage affecting all products at 100. We will expect the typical single incident score to be in the low single digits, but incident groups might have high scores. Most importantly, we can compare the impact of different incidents or different incident groups, and determine bang for buck for the range of solutions we bring forward to resolve the root cause of various incidents.

Entering a New Product

Here are the specific fields we keep for each Product:

1. PLATFORM – Generation/Version of the Platform that the Product has been built atop. Choose from a dropdown menu. This field lets us look at stability data across generations and potentially track stability across product maturity.
2. SLM NAME – This is not currently used. This can be used as a placeholder reference from external resource.
3. START DATE – Date when this product went live
4. END DATE – Date when this product was retired. Note that a product is retired when the next version of that product goes live
5. CLIENT NAME – This field probably will not be used
6. SHORT NAME – This name is used to form the Incident tag
7. OWNER – This is the Product Owner. It is not currently used.
8. MAX WEEKLY UPTIME – This is used to keep uptime statistics. For instance, if one product has 10,000 minutes of uptime a week while a second product has 5,000 minutes, and both go down for 20 minutes, the second product has twice the % of downtime as the first.
9. REVENUE % - This is the % of total revenue generated by this Product. The sum of all Revenue %'s of all active products should be 100. This number should be refreshed across all products annually after the next year's forecasting numbers are published.
10. USER % - This is the % of total customers who use this Product. The sum of all User %'s of all active products should be 100. This number may be refreshed accordingly.

Modify Product Information

Here are the scenarios that you would require modifying product information:

1. Updates to Revenue and User % - These updates should be updated en mases at the beginning of each year after new revenue projections for each product is done. Each active product should have their revenue and customer %'s updated based on projected revenue and actual customer counts.
2. New generation of Product – Here you need to retire the previous generation by entering an end date, and create a new Product record for the new generation.

Generating Reports

Incident Reporting

Incident Report

The Incident Report can be generated from the Reports menu on the main screen. The user is presented with a search screen and selects the target incident from the results screen. The Report is generated in Word format and displayed on the screen.

Daily Email Report

This email report is generated daily Mondays through Fridays and is sent to <distribution_list>. Monday's email report includes the list of incidents that occurred on Friday through Sunday.

Weekly Report

This report is manually generated from the Reports menu on the main screen. The user is presented with default parameters (all products, prior week) and generates the same weekly report that the SLM application generates.