Fermilab Service Desk

Incident Management

Recording new Incident work instructions

Software tools: Remedy 7.1x

OVERVIEW

Incident recording:

As the starting point for the Incident Management process; accurately recording new incidents is a key activity in identifying disruption in IT services provided by Fermilab Computing Division to its customers and user community. The Incident recording process will capture and record incident details like customer information, configuration item (CI), classification, and incident description. It is vital to the restoration services and management of these services that information recorded into an incident is complete and accurate. This document identifies key areas of the incident recording process that are essential for meeting these objectives.

General

Description	This document establishes the procedures for recording a New Incident within Remedy.		
Purpose	These procedures provide the necessary steps and details to accurately record a new Remedy Incident.		
Disclaimer	This document is intended to be used by Service Providers using approved software and having access to relevant databases.		
Applicable to	All Service Providers using the Incident Management software tool Remedy.		
Supersedes	N/A		
Document Owner	Fermilab Service Desk	**Owner Org**	Computing Division
Author/s	Allen Forni, Thomas Bozonelos		

VERSION HISTORY

Version	Date	Author(s)	Change Summary
1.6	09/30/2010	Allen Forni	Updated section 7 and added standard header
1.7	10/05/2010	Allen Forni	Changed overview statement and added text section 4, 5 & 6
1.8	10/13/2010	Allen Forni	Updating section 6 and 7

TABLE OF CONTENTS

1.0 REMEDY AR SYSTEM	
Description	Fermilab Computing Division Incident management approved recording software tool.
Purpose	The proper starting point for Incident recording

1. Starting an Incident Management console session:
   a. Enter the following web address into supported[1] web browser
      https://ar-mt1.fnal.gov/arsys/shared/login.jsp?/arsys/
   b. OR start the proprietary (MS-Windows Only) client software
      Instruction to start this application are not supported in this document
2. Logon using your username and password (the one you use for Fermi Time and Labor).
3. Under the Welcome Quick Links
   a. Click on the **Incident Management Console** quick link to start the console.
   b. Proceed to section 2.0 Creating a New Incident

2.0 CREATING A NEW INCIDENT	
Description	Entering Incident information into new a ticket
Purpose	To properly open and record a new Incident and when available use a template to assist in the recording process. *Templates are used to populate the incident with consistent information that is regularly entered. Each service provider can have unique templates for their use. The Service Desk can create templates as requested.*

1. Incident Management Console:
   a. Under the **General Functions** links
      i. Click on **New Incident**
   b. On the Incident Request form; under Quick Links click on **Select Template**
      i. From the **Incident Template Selection** pop-up box; select a template that matches the type of incident you are recording (e.g. Hardware Service Request, Network Install/Repair,..).
         1. If there are no templates found, then click Close and continue with section 3.0 Customer Information.
      ii. Click the Template Name to highlight the template of choice
      iii. Click the **Select** button to apply the template
   c. Proceed to section 3.0 Customer Information

1 Review Service Desk Support Staff FAQ document for a list of Web browsers. https://cd-docdb.fnal.gov:440/cgi-bin/ShowDocument?docid=3185

3.0 CUSTOMER INFORMATION	
Description	Entering Customer information and secondary contact information.
Purpose	To correctly record customer and secondary contact information into a new Incident request using the Remedy IM Console (web interface console or thick console clients).

1. Click the **Customer** Tab to view the fields.
    a. Enter Customer unique last name (portion of) or a Fermi ID number.
        i. Names are case-sensitive and Fermi ID consists of 5 numbers and a trailing alpha character (N, V, C). Example: last name = Forni, Fermi ID = 02596N
        ii. The entry may return a list of similar names
            1. Scroll through the list and click on the correct name
            2. Click the **Select** button to complete the entry process
    b. Confirm with the Customer their contact **Phone Number*+**
        i. If different, click the Edit Phone Number icon (pencil icon to the right side) 
        ii. Update the phone number according to the customer supplied information and click the OK button
2. Proceed to section 4.0 Customer Incident Statement.

4.0 CUSTOMER INCIDENT STATEMENT	
Description	Recording Incident statement and setting priority
Purpose	To correctly record customer Incident statement and priority. The Incident priority is determined by setting the Impact and Urgency values. This document contains excerpts of the Impact and Urgency matrixes. The full matrixes are in document CD DocDB 3064.

1. Within the Incident Request Information area – see image above.
   a. Click the button on the right side of the **Notes** field to expand the dialog box.
      i. If a template was used: Query the customer to obtain the information requested by the template.
      ii. If no template was used: Query the customer to obtain Incident information. *Information should be clearly stated and realistically detailed as to the reported issue.*
      iii. Click the OK button to close the dialog box.
   b. Click the button on the right side of the **Summary*** field to expand the dialog box.
      i. If a template was used you may not need to modify this field. Otherwise, enter a summary statement (<40 character) that best describes the reported incident.
2. Click the down arrow to the right side of the field **Impact*** and **Urgency***; then choose a values according to policies stated in the Incident Management document (CD DocDB 3064).
   a. **Impact Matrix** (*extracted from CD DocDB 3064)*

Extensive/ Widespread	Major Business Impact: Outage with no workaround resulting in complete loss of core business systems to customer.
Significant/ Large	Significant Business Impact: Outage with no workaround resulting in significant loss or degraded system services to customer; however operations can continue in a restricted mode.
Moderate/ Limited	Batch/on-line/hardware problems resulting in minimal impact to system and system availability.
Minor/ Localized	Single points of failure resulting in impact to: Single customers, Single devices, Non-critical peripherals.

   b. **Urgency Matrix** (*extracted from CD DocDB 3064)*

Critical	Restoration is and time is of the essence.
High	Restoration requirement is high and time is of the essence.
Medium	Restoration requirement is medium but time is less critical.
Low	Restoration requirement is low or not required.

5.0 CLASSIFICATION INFORMATION	
Description	Entering Incident Classification information
Purpose	To correctly record Incident classification for Service Type, Reported Source, Reported Date/Time, Product and Operational Categorization. *If a template was used, the following settings may have predetermined values and care should be taken when modifying as the new values may impact how the ticket is assigned.*

Click the **Classification** tab to view the fields – see image above

1. Under the **Incident Service Type** section
   a. From the drop-down menu, select the correct **Service Type** based on the user reported incident.

Incident Service Types			
Submitted by:			
Customer or User	**Automatic or Event**	**Type**	**Definition**
X	---	**User Service Restoration**	A loss or reduction of service that has impacted the user (e.g. system slow when reading or sending email, computer will not start,…)
X	---	**User Service Request**	A request from a user (e.g. information, advice, password reset, access to a supported service,...)
---	X	**Infrastructure Restoration**	An Incident that impacts an individual configuration item of a larger service and the user is not impacted (e.g. a server goes down and jobs failover to other servers.)
---	X	**Infrastructure Event**	A loss or reduction of a service that is detected via automatic event monitoring systems (e.g. BlueArc disk space nearing capacity, but users are not impacted).

2. Under the **Reporting Information** section
   a. From the drop-down menu, select the **Reporting Source** value.

Reporting Source	Definition
Direct Input	The service provider is recording the incident. It may or may not be a service they support.
External Escalation	A 3rd party vendor supporting an on-site service.
Email, Fax, Phone, Voice Mail, Walk In, Web	Self-explanatory
System Management, Other	Do Not use!

   b. Click the icon box to the right side of the **Reported Date+** field to open the dialog box. Enter the corresponding date and time when the incident was initially reported. *(Used when backfilling incidents that were created from Fax, Voice Mail or other delayed entry methods).*

3. **Product Categorization**: - used to identify the Service that is thought to be involved with the reported Incident. The three tier settings are based on a hierarchy with Tier 1 being the highest.
   a. From the drop-down menu for Tier 1, 2 & 3; select the appropriate product categorization that best matches the reported Incident.

Tier	Description	Ticket Requirement
1	Typically the base service provided (e.g. Hardware).	**Required**
2	Typically the sub-service provided (e.g. Workstation; peripheral).	**Required**
3	Typically the sub-sub-service provided (e.g. Desktop; Laptop; Network Printer).	Optional

4. **Operational Categorization**: - used to identify the activity or state of the product categorization.
   a. From the drop-down menu for Tier 1, 2; select the appropriate operational categorization that best matches the reported Incident.

Tier	Description	Ticket Requirement
1	Typically the base activity or state as it relates to the Product categorization.	**Required**
2	Typically the modifier that relates to tier 1.	**Required**

6.0 RELATIONSHIP INFORMATION	
Description	Entering Incident Relationship Information
Purpose	To correctly record relationships with other Incidents, Configuration Items (CI) and other request types.

Relationship Type	**Description**		
Original of	The primary Incident in the Incident to Incident relationship. This Incident is the one that gets updated (worked). Resolving the Original of Incident will resolve all linked Incidents		
Duplicate of	The Incident that is related to the primary (Original of) incident. This Incident will get its resolution from the primary (Original of) Incident.		
Related to	The Incident is NOT a duplicate, but has a dependency with other Incidents. This Incident and the relate Incident need to be resolved independently.		
Configuration Item (CI)	An asset that has been identified as being involved in the Incident or Request.		
	Examples	when to relate	My computer system is running slow! I would like to increase the memory on my computer system!
		when NOT to relate	Please reset my email password! I can't login to file system xyz!

General Procedures:

1. Click on the **Relationships** tab to view current related items or to add new related items.
2. From the **Request Type** drop-down list, select the type of relationship record you wish to create.
   Request Type*: Defines the type of relationship the current incident will have with an additional database item. Items in the database include but are not limited to: Incidents, Configuration Items (CI), CI Unavailability, Infrastructure Change, Problem Investigation, and Solution Database.*
3. Click the **Search** button to bring up the search dialog box.
   The dialog box fields will vary with the type of record you have chosen from the ***Request Type*** *drop-down list.*
4. On the *Search Criteria* dialog box **Search** tab;
   a. Enter key attribute/s of the database item you are looking to find.
      i. Adding more key attributes to the search criteria will reduce the number of returned records.
   b. Click on the **Search** button to execute the search criteria.
   c. From the search results listing, select (highlight) the result record that you want to create the relationship with.
   d. From the **Relationship Type** drop-down list, select the type of relationship you want to create.
   e. Click on the **Relate** button to complete the relationship process.
      i. An information message window will pop-up, giving confirmation.
      ii. Click the **OK** button to close this window
5. The search dialog box should be closed now and your related item should be visible in the incident relationships table.

Example #1 and #2 covers relating Incident to Configuration Item (CI) and Incident to Incident

Example 1 – Relating an Incident to Configuration Item (CI)

1. Click on the **Relationships** tab to view current related items or to add new related items.
2. From the **Request Type** drop-down list, select the **Configuration Item** from the list.
3. Click the **Search** button to open the CI Relationships Search dialog box.
4. On the *Search Criteria* dialog box **Search** tab;
   a. Enter key attribute/s of the Configuration Item (CI) you are looking to find.

Field name	Classification
Tag Number:	property tag
CI Name:	node name
CI ID:	network system number
Serial Number:	serial number

5. Click the Search button to retrieve the CI asset information.
6. If the CI is found, then under the **Relationship Type** drop-down choose **Relate to**
   a. If there is no matching CI, then
      i. Click the Close button to continue working the incident without a related CI.
      ii. Open a new ticket requesting the Asset manager to add the missing CI to the Remedy CMDB database.
7. Click the **Relate** button to complete the relationship process.
8. Go back to step (2) if there are multiple CI's to relate.

Example 2 – Relating an Incident to Incident:

1. Click on the **Relationships** tab to view current related items or to add new related items.
2. From the **Request Type** drop-down list, select **Incident** from the list.
3. Click the **Search** button to open the Incident Relationship Search dialog box.
4. On the *Search Criteria* dialog box **Search** tab;
   a. Enter the Incident ID number into the **Incident ID+** field and execute the search. See table below for allowable Incident ID values and execute options.

		To execute search use option A or B	
	Incident ID+ value	**Option A**	**Option B**
Fully defined	INC000000054897	On the keyboard, click the Enter key after the last entered character.	Click the Search button.
Partly defined	54897	On the keyboard, click the Enter key after the last entered character.	----

5. If the Incident is found, then under the **Relationship Type** drop-down choose **Relate to**
   a. If there is no matching Incident, then review the data and make corrections as needed to obtain the search results you are looking for.
6. Click the **Relate** button to complete the relationship process.
7. Go back to step (2) if there are multiple Incidents to relate. Otherwise proceed with 7.0 Assignment Information.

7.0 ASSIGNMENT INFORMATION	
Description	Entering Assignment information
Purpose	To set the proper Incident Assignee prior to saving the recorded Incident. The Incident Assignee is the IT Support Group for the reported impacted Service.

Beware!! *Incident auto assignment has been enabled for some Service Providers. Incident auto assignment process is based off of the product categorization settings and the Incident Assignee information being left blank prior to saving the recorded Incident. A manually entered Incident assignment value will supersedes the auto entered values of the product categorization.*

Within the Assignment tab, the Incident Assignee area has three (3) required fields (see bolded field names in the image below) that are used in conjunction with each other. When these fields are set properly the Incident will be auto-routed to a support group when the Incident is saved.

1. Click the **Assignment** tab to view the Incident Assignee fields.
   When using an Incident template the Incident Assignee may have a predetermined support group setting. Care should be given when manually overriding these settings as changes in Incident Assignee settings will alter Incident routing.
   a. If the Incident Assignee fields are not blank
      Usage of a template has set the values to a predetermined support group.
      i. To except these values, proceed to step 2.
      ii. To alter these values, proceed to step (1b).
   b. If the Incident Assignee fields are blank
      i. From the drop-down list for **Support Company***, select Fermilab
      ii. From the drop-down list for **Support Organization***, select the Fermilab organization that manages the Service being reported on (e.g. Computing Division).
      iii. From the drop-down list for **Assigned Group*+**, select the Service Provider group name.
2. Click the **Save** button at the bottom of the form to complete the recording of the Incident.