



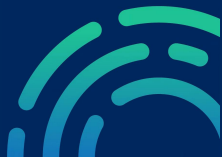
Australian Government



Consumer
Data Right

CDR Service Management Portal

Guide for Participants



Contents

Overview

3. CDR Service Management Tool Overview
4. Getting the Right Information
5. Types of Incidents and Requests
6. Getting Prioritisation Right
7. Post Incident Reviews

Customer Portal

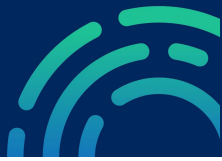
8. Customer Portal: Logging an Incident or Request
9. Customer Portal: Selecting Request Type
10. Customer Portal: Service Request - Example
11. Customer Portal: Incident with a CDR Provider- Example
12. Customer Portal: Incident Categories
13. Customer Portal: Incident Sub-Categories
16. Customer Portal: Sharing of 'Incident with a CDR Provider' with another CDR Provider user or organisation
17. Customer Portal: Incident with the CDR Register and Accreditation Platform (RAAP) - Example
18. Customer Portal: Incident with the Conformance Test Suite (CTS) – Example
19. Customer Portal: Notify Data Holder Implementation Gaps
22. Customer Portal: Tracking Requests

Agent View

23. Agent Role: Overview
24. Agent: Creating Incidents and Service Requests
26. Managing Incidents
27. Agent: Incident View
28. Agent: Sharing of 'Incident with a CDR Provider' with another CDR Provider user or organisation
29. Agent: Progressing Through Workflows
30. Agent: Incident Lifecycle Management for CDR Provider Incidents
31. Agent: Adding Comments – Differences between Internal and Customer Facing Comments
32. Agent: Fixing and Verifying Incidents
33. Agent: Resolving and Closing Incidents

For further information contact:

CDRtechnicaloperations@acc.gov.au



CDR Service Management Tool Overview

The CDR Service Management Portal is provided by the ACCC for CDR participants to communicate technical incidents between each other, or with the ACCC CDR Technical Operations team. The CDR Technical Operations team undertake a ‘monitoring’ approach to facilitate effective resolution of issues and promote a healthy and effective CDR ecosystem.

The CDR Service Management Portal can be found here:
<https://cdrservicemanagement.atlassian.net/servicedesk>

Gaining Access

During the CDR On-Boarding process, an Authorised CTS Tester and a Primary IT Contact from each participant will be granted access to the CDR Service Management Portal. Other users who wish to have access, can request access by asking their organisation’s CDR representative to raise a Service Request or by emailing the CDR Technical Operations and Participant Support team (CDRTechnicalOperations@acc.gov.au).

Role Types

The CDR Service Management Tool has two types of roles, the ‘Agent’, and the ‘Customer’. Each participant is limited to a total of 2 Agents and 5 Customers:

Role Type	Description
Customer	Has restricted access that allows this role to raise new incidents and service requests, view and comment on incidents that are shared with them.
Agent	Can access queues, raise and process incidents and service requests (i.e. move incidents through workflows, reassign incidents to other teams and make customer-facing comments).

For further information contact:

CDRtechnicaloperations@acc.gov.au



Getting the Right Information

When logging an incident or request for service please ensure that all fields provided are completed, and attach any related files, logs, or screenshots that may be helpful to speed the resolution of any incidents or requests.

Please Note: Each participant in voluntarily reporting incidents through CDR Service Management portal, agrees to do so on the understanding that each participant:

- should not report or include any information that it considers confidential;
- is responsible for complying with its privacy or information handling obligations including under Part IVD of the *Competition and Consumer Act 2010* (Cth), the *Privacy Act 1988*, and the Consumer Data Rules;

accepts that the information it reports or includes will be available to the intended participants and that participants are not subject to any confidentiality obligations regarding the use of such information. In addition, in relation to reported incident information, each participant accepts that the ACCC may use information for Compliance and Enforcement (C&E) purposes, including by making publicly available data regarding the number, ageing (how long for resolution), severity (including no of each) of incidents overall, and for each named participant, and otherwise as set out in the ACCC/AER Information Policy (<https://www.accc.gov.au/publications/accc-aer-information-policy-collection-and-disclosure-of-information>).

Thanks for your ongoing support of the CDR. Please direct questions to the Technical Operations Inbox. CDRTechnicalOperations@acc.gov.au

The CDR Service Management Portal can be found here:
<https://cdrservicemanagement.atlassian.net/servicedesk>

For further information contact:

CDRtechnicaloperations@acc.gov.au



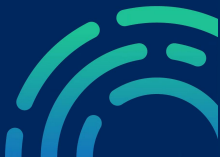
Types of Incidents and Requests

The CDR Service Management Portal can be used to assist participants in a variety of activities. Below are some of these issues and services managed through the CDR Service Management Portal:

Request Types	Usage
Incident with a CDR Provider	Used to raise a technical incident with a CDR participant, where the resolving party is another Data Holder or Data Recipient.
Incident with the CDR Register and Accreditation Platform (RAAP)	Used by participants to raise an incident with the ACCC CDR team where the incident relates to the RAAP or the CDR Register.
Service Requests for ACCC Managed Systems or On-boarding Assistance	Used by participants to raise requests or queries relating to the On-Boarding process, RAAP, CTS or CDR Service Management portal. Examples include specifying or updating participant configuration information or requesting information or access to RAAP, CTS or the CDR Service Management portal.
Incident with the CDR Conformance Test Suite (CTS)	Used by a participant to raise an incident for an issue they are facing when testing in the Conformance Test Environment.
Notify Data Holder Implementation gaps	Used by Data Holders to notify the ACCC of CDR solution implementation gaps and the proposed rectification schedule.

For further information contact:

CDRtechnicaloperations@acc.gov.au



Getting Prioritisation Right

The Prioritisation and Severity criteria assesses incidents/issues from an Impact and Urgency perspective to gain a consistent measurement of incidents/issues that may impact either a single participant or the ecosystem.

Severity

Category / Impact	CDR Ecosystem	Business / Consumer
Major	<ul style="list-style-type: none"> CDR ecosystem is unavailable, or the ecosystem functionality is severely degraded. 	<ul style="list-style-type: none"> A large number of CDR consumers are affected and/or acutely disadvantaged in some way. Major reputational/ financial impact for multiple CDR participants. Unavailability of service(s) that stops critical business functions.
Significant	<ul style="list-style-type: none"> One or more of CDR providers are not able to share data. 	<ul style="list-style-type: none"> A moderate number of CDR consumer are affected and/or disadvantaged in some way. Moderate reputational/ financial impact for CDR participants. Partial impact to critical services that stops or limits business functions.
Minor	<ul style="list-style-type: none"> Degradation of a service impacting an ADR, a DH or the CDR Register. 	<ul style="list-style-type: none"> A limited number of CDR consumers are affected and/or disadvantaged but not in a significant way. No/minor reputational/financial impact for CDR participants. Impact to availability of non-critical service(s).

Priority

Category / Urgency	CDR Ecosystem	Business / Consumer
High	<ul style="list-style-type: none"> Critical risk to CDR ecosystem and no workaround available. Consumer data cannot be shared. 	<ul style="list-style-type: none"> Critical risk to the business of the reporting organisation with no workaround available. The damage caused by the Incident increases rapidly. Most users are affected.
Moderate	<ul style="list-style-type: none"> Medium risk to CDR ecosystem and no workaround available. Most Consumer data cannot be shared. 	<ul style="list-style-type: none"> Medium risk to the business of the incident reporting organisation with no workaround available. The damage caused by the Incident increases considerably over time. Moderate number of users are affected.
Low	<ul style="list-style-type: none"> Low risk to CDR ecosystem and workaround available. Some Consumer data cannot be shared. 	<ul style="list-style-type: none"> Low risk to the business of the incident reporting organisation with a workaround available. The damage caused by the Incident only marginally increases over time. Single user impact.

For further information contact:

CDRtechnicaloperations@acc.gov.au



Post Incident Reviews

Some incidents require a Post Incident Review (a PIR). Reviews into the cause of incidents can be helpful to assist in understanding underlying issues, problems or ‘bug’s that exist in the collective CDR ecosystem. Often, the information that is learned from an incident, and any subsequent PIR, can be turned into helpful knowledge articles for the benefit of all current and future participants.

The focus of a Post Incident Review is to learn from the incident(s) and reduce the likelihood of re-occurrence. Information contributed to a PIR should follow the guidance set out on [page 4](#) of this guide.

1. Incident Summary Information

Incident No(s):		Date & Time of Incident occurred:	
Incident Title:			
Prepared by:			
Severity:	Choose an item.	Priority:	Choose an item.
Resolving Participant(s):		Date & Time of Incident Resolved/Workaround in place:	
Impacted Participant(s):		No. Customer Impacted: (<10, <100, <1000, most, all)	Choose an item.
Repeated Incident (Yes/No)?	Choose an item.	Past Incident No(s):	
Raised a Problem Ticket (Yes/No)?	Choose an item.	Problem Ticket No.:	

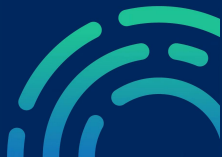
2. Business Impact

3. Incident Description - Technical Perspective

4. Tactical Solution / How was Incident Resolved?

For further information contact:

CDRtechnicaloperations@acc.gov.au



Customer Portal: Logging an Incident or Request

Participants are presented with a **service catalogue** when entering the portal. From here workflows are available to raise a variety of issues and requests. Technical incidents may be between participants and can include ACCC CDR Technical Operations and Participant Support team if required. Participants can also generate tickets with the ACCC CDR if they believe a ACCC CDR system is the cause of an incident.

Note that once a ticket is logged, a notification email is generated for the requestor, the recipient and anyone that the ticket is shared with.

Contact us about

Incident with the CDR Conformance Test Suite (CTS)

Log an incident with the CDR Conformance Test Suite (CTS)



Incident with a CDR Provider

Log an Incident with a Data Holder / Accredited Data Recipient



Incident with the CDR Register and Accreditation Platform (RAAP)

Log an Incident with the CDR Register and Accreditation Platform (RAAP)



Implementation Gaps & Rectification Schedule

Notify Data Holder Implementation gaps



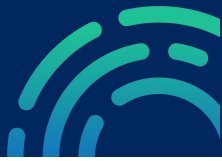
Service Requests for ACCC Managed Systems or On-boarding Assistance

Submit a Service Request for RAAP, CTS and CDR Service Management Portal



For further information contact:

CDRtechnicaloperations@acc.gov.au



Customer Portal: Selecting Request Type

To raise a ticket, select the request type most aligned to your requirement to ensure your request gets to the right team.

Contact us about

Incident with the CDR Conformance Test Suite (CTS) >

Log an incident with the CDR Conformance Test Suite (CTS)

Incident with a CDR Provider >

Log an Incident with a Data Holder / Accredited Data Recipient

Incident with the CDR Register and Accreditation Platform (RAAP) >

Log an Incident with the CDR Register and Accreditation Platform (RAAP)

Implementation Gaps & Rectification Schedule >

Notify Data Holder Implementation gaps

Service Requests for ACCC Managed Systems or On-boarding Assistance >

Submit a Service Request for RAAP, CTS and CDR Service Management Portal

For further information contact:

CDRtechnicaloperations@acc.gov.au



Customer Portal: Service Request- Example

Contact us about

Service Requests for ACCC Managed Systems or On-boarding Assistance

What can we help you with?

Submit a Service Request for RAAP, CTS and CDR Service Management Portal
Request support or assistance regarding the Register and Accreditation Platform (RAAP), Conformance Test Suite (CTS) , On-boarding process and CDR Service Management Portal (JIRA)

A Service Request can be used to request for an ACCC CDR team to perform an action on behalf of an organisation that you are associated with. Examples of the type of actions include: Updating endpoints, user management etc.

Raise this request on behalf of*

CDR Technical Operations & Participant Support

Summary*

Provide a short title for your request.

Summary: Provide a short title for your request.

Description

Provide a detailed description for your request, referencing attachments where applicable.

Description: Provide a clear and detailed description for your request, referencing attachments where applicable.

Priority*

3 - Low

Set the Priority for the request.

Priority: Set the Priority for the request. (See guide on [page 6](#))

Attachment

Drag and drop files, paste screenshots, or browse

Upload any relevant attachments by dragging and dropping into the field, or by clicking the browse button and selecting files to upload.

Attachment: Upload any relevant attachments by dragging and dropping into the field, or by clicking the browse button and selecting files to upload.

The CDR Service Management Portal can be found here:
<https://cdrservicemanagement.atlassian.net/servicedesk>

For further information contact:
CDRtechnicaloperations@acc.gov.au



Customer Portal: Incident Categories

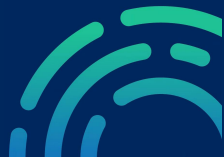
The Incident categories/sub-categories will enable the CDR and providers to quickly identify incident types for more efficient resolution and provide greater insight into the types of incidents being reported in the CDR ecosystem.

Incident Categories	Definitions
Consent (Authorisation) Management	Issue related to establishing, amending and revocation of consent.
Dynamic Client Registration	Issues related to a software product registering with a data hold brand.
Data Quality	Incidents related to data accuracy, data completeness, consistency and compliance of consumer data in the CDR ecosystem.
System/Service Availability	Incidents related to participant system or services availability.
Performance	Incidents related to degradation of performance of participant systems or services in their interaction with the CDR ecosystem.
CDR Rules / Standards Interpretation	Incidents related to the interpretation of CDR Rules and Consumer data standards.
Security Profile (Information Security)	Incidents related to information security profile in the CDR ecosystem. <i>Note: This does not include incidents related to security events such as data breaches etc.</i>
Consumer Experience	Incidents caused by non-conformance to consumer experience standards and guidelines in the CDR ecosystem.
Admin API (Get Metrics)	Incidents related to non-provision or non-compliance of data from the Get Metrics API.
Other	Incidents that fall outside of the above-mentioned categories.

Note: Sub-Category definitions are provided in the following pages.

For further information contact:

CDRtechnicaloperations@acc.gov.au



Customer Portal: Incident Sub-Categories

A number of sub-categories are available for each incident category which enable further classification of incidents reported in the CDR ecosystem.

Categories	Sub Categories	Sub Category Definition	Examples
Consent (Authorisation) Management	Establishing a new consent	Incidents related to establishing a new consent with a data holder brand.	Incidents related to issues with authentication (OTP).
	Amending an existing consent	Incidents related to modifying an existing consent with a data holder brand.	Unable to extend the consent etc.
	Revocation of an existing consent	Incidents related to removing an existing consent.	Data holders not notifying the data recipient that consent had been revoked on the Data holder's end.
Dynamic Client Registration	Create Registration	Failure to establish Dynamic Client Registration (DCR).	Errors encountered during DCR.
	Modify Registration	Failure to modify existing registration.	Modification request rejected by data holder brands.
Data Quality	Data Accuracy	Incidents related to accuracy of consumer data in the CDR ecosystem.	Incorrect consumer data in CDR ecosystem when compared to the source data holder systems.
	Data Completeness	Incidents related to completeness of consumer data in the CDR ecosystem.	Missing consumer data shared by the Data holders in the CDR ecosystem.
	ID Permanence	Incidents related to non-compliance with ID permanence standards by the participants in the CDR ecosystem.	Varying ID for the same resource when queried by the participants in the CDR ecosystem.

For further information contact:

CDRtechnicaloperations@acc.gov.au



Customer Portal: Incident Sub-Categories

A number of sub-categories are available for each incident category which enable further classification of incidents reported in the CDR ecosystem.

Categories	Sub Categories	Sub Category Definition	Examples
Data Quality	Data Consistency	Incidents related to inconsistency of consumer data across the ecosystem.	Varying consumer data being shared by the data holders when queried by the participants in the CDR ecosystem.
	Data Compliance	Incidents related to non-conformance of data definitions like type, size and format in the CDR ecosystem.	Incorrect format of data shared by the participants against the established stand
System/ Service Availability	System/Service Availability	Incidents related to participant system or services availability.	Failed 5XX response from participant systems/services.
Performance	Data Latency	Incidents related to response times in data presented via CDR API endpoints from the receipt of request to delivery of response.	Higher response times from API requests failing to meet the defined performance threshold standards.
	Throttling	Incidents related to non-conformance to traffic thresholds defined in consumer data standards.	Failed responses due to implementation of throttling limits.
CDR Rules / Standards Interpretation	Implementation Error	Incidents related to issues faced due to incorrect implementation of CDR Rules and Standards.	Failed response due to non-conformance with CDR Rules and Standards.
	Ambiguity in standards/rules	Incidents related to lack of clarity/insufficient documentation of CDR Rules and Standards.	Incidents raised due to discrepancy between consumer data standards and other normative references.

For further information contact:

CDRtechnicaloperations@acc.gov.au

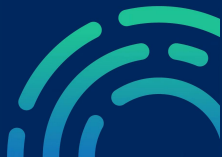


Customer Portal: Incident Sub-Categories

A number of sub-categories are available for each incident category which enable further classification of incidents reported in the CDR ecosystem.

Categories	Sub Categories	Sub Category Definition	Examples
Security Profile (Information Security)	Certificate Error	Incidents related to authentication error due to incorrect certificate configuration in the CDR ecosystem.	Failure in handshake between servers due to certificate issues.
	Scopes & Claims	Incidents related to issues with scopes & claims.	Encountered an Invalid claim error.
	Client Authentication	Incidents related to issues in client authentication methods in the CDR ecosystem.	Authentication failure during retrieval of access token from Data Holder.
	Tokens	Incidents related to issues with retrieval of ID, access and refresh tokens in the CDR ecosystem.	Failure in refresh token re-cycling.
Consumer Experience	Consumer Experience	Incidents caused by non-conformance to consumer experience standards and guidelines in the CDR ecosystem.	Non-conformance with UI standards defined under CX guidelines.
Admin API (Get Metrics)	Non-provision of Get Metrics Data	Incident caused by Non-provision of Get Metrics Data	Failure to provide Get Metrics response due to a system error.
	Non-compliance of Get Metrics Data	Incident caused by Non-compliance of Get Metrics Data	Data returned by Get Metrics indicates that the solution is not meeting the non-functional requirements.
Other	Other	Incidents that fall outside of the above-mentioned categories.	

For further information contact:
CDRtechnicaloperations@acc.gov.au



Customer Portal: Sharing of 'Incident with a CDR Provider' with another CDR Provider user or organisation

CDR Service Management / Consumer Data Right Service Management - Stage / CDRSTA-261

Sharing Information with another user in My organisation

AJ Arun Janardhanan raised this on Today 2:31 PM [Hide details](#)

Description
This issue is shared with my organisation, so another user from my organisation can see the ticket as well

Severity
3 - Minor

Priority
3 - Low

CDR Provider
Smart Bank

Incident Categories and Sub-Categories
Other - Other

Status
OPEN

[↔](#) Cancel

Request type
 Log an Incident with a Data Holder / Accredited Data Recipient

Shared with

- AJ** Arun Janardhanan
Creator
- Smart Bank
- Money App x Ada x

Add Cancel

Activity

CO

Share with: Choose the user or organisation to which the incident needs to be shared with and click on Add button.

The CDR Service Management Portal can be found here:
<https://cdrservicemanagement.atlassian.net/servicedesk>

Note: Problem with a CDR Provider will be visible for all the users and/or organisations in the CDR Service Management Portal.

For further information contact:
CDRtechnicaloperations@acc.gov.au



Customer Portal: Incident with the CDR Register and Accreditation Platform (RAAP) - Example

Contact us about

Incident with the CDR Register and Accreditation Platform (RAAP) ▾

What can we help you with?

Log an Incident with the CDR Register and Accreditation Platform (RAAP)
Report incidents, outages or issues regarding the ACCC hosted CDR Register and Accreditation Platform (RAAP)

Raise this request on behalf of *

Enter name or email... ▾

Summary *

Provide a short title for the incident.

Description

Normal text ▾ **B** *I* ... ▾

Provide a detailed description for the incident, referencing attachments where applicable.

Severity *

3 - Minor ▾

Set the Severity for the incident.

Priority *

3 - Low ▾

Set the Priority for the incident.

Reporting Organisation *

▾

Select the CDR Provider raising this incident

Attachment

Drag and drop files, paste screenshots, or browse

Upload any relevant attachments by dragging and dropping into the field, or by clicking the browse button and selecting files to upload.

Share with *

Share with ACCC-CDR ▾

Summary: Provide a short title for your incident.

Description: Provide a detailed description for your incident, referencing attachments where applicable.

Severity: Set the Severity for the incident. (See guide on [page 6](#))

Priority: Set the Priority for the incident. (See guide on [page 6](#))

Reporting Organisation: Select the CDR Provider that you are representing.

Attachment: Upload any relevant attachments by dragging and dropping into the field, or by clicking the browse button and selecting files to upload.

Share with: Select the Organisation that you want to share this ticket with.

The CDR Service Management Portal can be found here:
<https://cdrservicemanagement.atlassian.net/servicedesk>

For further information contact:
CDRtechnicaloperations@acc.gov.au



Customer Portal: Incident with the Conformance Test Suite (CTS) - Example

Contact us about
Incident with the CDR Conformance Test Suite (CTS)

What can we help you with?
Log an incident with the CDR Conformance Test Suite (CTS)
 Report incidents, outages or issues regarding the ACCC hosted Conformance Test Suite (CTS)

Raise this request on behalf of

Summary
 Provide a short title for the incident.

Description
 Normal text | **B** *I* ... | | | | | | |

Provide a detailed description for the incident, referencing attachments where applicable.

Severity
 3 - Minor

Set the Severity for the incident.

Priority
 3 - Low

Set the Priority for the incident.

Reporting Organisation
 Select the CDR Provider raising this incident

CTS Test Phase
 Conformance Testing - Production
 Conformance Testing - Beta

Enter the CTS Test Phase for the incident. Select "Conformance Testing - Beta" only if you have enrolled for the CTS Beta program.

Test Scenario ID
 Enter the Test scenario ID.

Test Step
 Enter the test step that has failed.

Error Timestamp
 Enter the timestamp of failure.

Attachment
 Drag and drop files, paste screenshots, or browse

Upload any relevant attachments by dragging and dropping into the field, or by clicking the browse button and selecting files to upload.

Share with

Summary: Provide a short title for your incident.

Description: Provide a detailed description for your request, referencing attachments where applicable.

Severity: Set the Severity for the incident. (See guide on [page 6](#))

Priority: Set the Priority for the incident. (See guide on [page 6](#))

Reporting Organisation: Select the CDR Provider that you are representing.

CTS Test Phase: Select "Conformance Testing - Production" unless advised otherwise

Test Scenario ID: Enter the test scenario ID.

Test Step: Enter the test step that has failed.

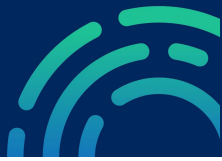
Error Timestamp: Enter the timestamp of failure.

Attachment: Upload any relevant attachments by dragging and dropping into the field, or by clicking the browse button and selecting files to upload. Examples can include logs, screenshots etc.

Share with: Select the Organisation that you want to share this ticket with.

The CDR Service Management Portal can be found here:
<https://cdrservicemanagement.atlassian.net/servicedesk>

For further information contact:
CDRtechnicaloperations@acc.gov.au



Customer Portal: Notify Data Holder Implementation Gaps

Please Note: This request type allows data holders to notify the ACCC of CDR solution implementation gaps. We expect data holders to promptly rectify their non-compliance or face possible enforcement consideration in line with the ACCC/OAIC Compliance and Enforcement Policy for the Consumer Data Right. Listing an issue on a rectification schedule does not preclude the ACCC from pursuing compliance or enforcement action in-line with this policy.

We also expect participants to notify us of non-compliance with their obligations. We also expect participants to proactively notify us of updates to existing rectification schedule items, including when an issue is resolved or if there will be a delay in meeting a proposed resolution date.

The ACCC may contact you via this ticket seeking clarification of information provided. We ask that you regularly check for such updates until the information has been published on the CDR website.

Submissions of this type must be authorised by the appropriate person within a given organization using the appropriate [Sensitivity Marker](#). Submissions should be made by a representative of the data holder legal entity, rather than a third party (such as a service provider), unless otherwise agreed with the ACCC prior to submission.

For further information contact:

CDRtechnicaloperations@acc.gov.au




Customer Portal: Notify Data Holder Implementation Gaps (continued)

Contact us about

Implementation Gaps & Rectification Schedule

Contact us about: Select 'Implementation Gaps & Rectification Schedule'.

What can we help you with?

 **Notify Data Holder Implementation gaps**
Lodge implementation gaps in a Data Holder solution and the proposed rectification schedule.

What can we help you with: Click on 'Notify Data Holder Implementation gaps'.

Please submit a new notification each time you wish to add, remove, or alter an implementation gap published on the rectification schedule. Please note that you do not need to submit new notifications for existing implementation gaps.

Raise this request on behalf of*

Ada

Raise this request on behalf of: Nominate the primary contact person for this request.

Summary*

Summary: Provide a short title for your request.

Provide the Data Holder Brand Name and a brief summary of the implementation gap

Issue Description

Aa B I ... A @ ☺ ☒ <> ⓘ ” + v

Implementation Gap	Proposed Resolution Date	Additional Details

Issue Description: Fill in the table included, add more rows if required. Provide a detailed description for your request, referencing attachments where applicable. Use the dd/mm/yyyy date format in the date column.

Provide detailed description of the implementation gap and proposed resolution date.

Note: Please provide a description of the implementation gap in Column 1 and provide a proposed resolution date in Column 2. If you wish to do so, you may provide additional details in Column 3. Please ensure that the implementation gap description is sufficient that third parties, such as accredited data recipients, will be able to meaningfully interpret the impact of the disclosed implementation gap.

For further information contact:

CDRtechnicaloperations@acc.gov.au



Customer Portal: Notify Data Holder Implementation Gaps (continued)

Data Holder Legal Entity and Brand

Select the Data Holder Legal Entity and Brand

Data Holder Legal Entity and Brand: Select the Data Holder Brand that you are providing the notification for. Please submit one ticket per brand.

Proposed Resolution Date

Date of proposed resolution. If the resolution date of multiple implementation gaps falls on different dates chose the earliest one.

Proposed Resolution Date: Select the earliest date if multiple gaps is being declared.

Sensitivity Marker

A marker to indicate if the implementation gap has to be kept confidential or can be published on the CDR website for ecosystem awareness.

Sensitivity Marker: Indicate if the material in Column 1 & 2 is suitable for publication or confidential. Material in Column 3 will not be published

Attachment

Drag and drop files, paste screenshots, or browse

Attachment: Upload any relevant attachments by dragging and dropping into the field, or by clicking the browse button and selecting files to upload.

Powered by Jira Service Management

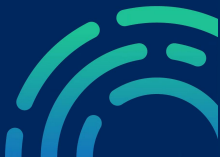
Note: Please indicate that material is suitable for publication by selecting the appropriate sensitivity marker.

Material provided in Column 1 (Implementation Gap) and Column 2 (Proposed Resolution Date) will be published on the CDR website.

Information provided in Column 3 will not be published. If you consider that information entered into Column 1 or 2 is not suitable for publication, please email acc-cdr@acc.gov.au for further instructions.

For further information contact:

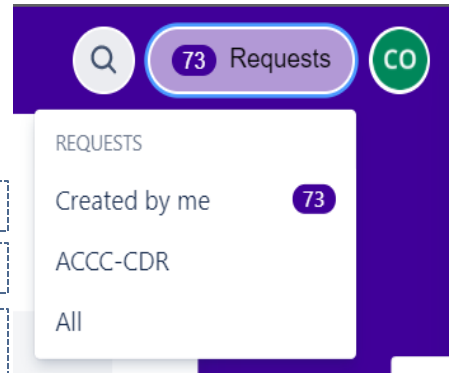
CDRtechnicaloperations@acc.gov.au



Customer Portal: Tracking Requests

You can track your requests by logging into the JIRA Customer Portal and clicking on the requests button in the top right-hand corner of the Jira window.

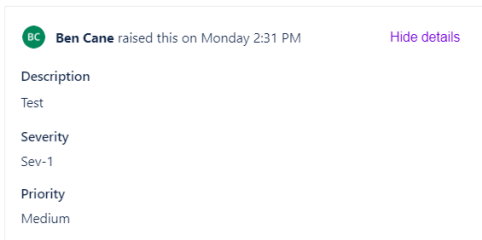
- Created by me:** View Incidents created by the user.
- Organisation:** View Incidents shared with your organisation.
- All:** View all the Incidents shared with the user including the ones created by the user and shared with your organisation.



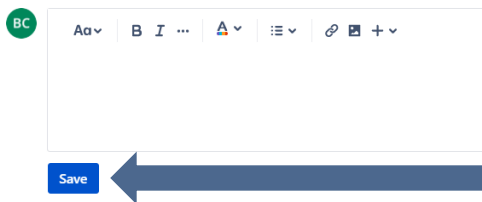
Updating or Commenting on Requests

Consumer Data Right / CDR Service Management / CDRSTA-17
[Test] CTS AUD Claim failure

In your requests view, you can select the relevant request and add comments or updates.



Activity



Click in the comments field and start typing.

Click save to submit your comment or update.

The CDR Service Management Portal can be found here:
<https://cdrservicemanagement.atlassian.net/servicedesk>

For further information contact:
CDRtechnicaloperations@acc.gov.au



Agent Role: Overview

The Agent role can access queues, raise and process incidents and service requests (i.e. move incidents through workflows, reassign incidents to other teams and make customer-facing comments). When an Agent logs in to <https://cdrservicemanagement.atlassian.net> they will see the project view as per below.

Agents can navigate between existing incidents and service requests from the left-hand panel, and also create new incidents and service requests from the top menu bar.

Click the Create button to create a new incident or request.

Select Queue to navigate between Service Requests or Incidents within your configured queues.

The Queue available to participants is Incident with a CDR Provider (CDR Ecosystem). All other queues are for internal ACCC use.

Key	Summary	Reporter	Assignee	Status	Created
CDRSTA-78	Clarification of the Certificate issuance process	Callan Witnitz	CDR Technical Operati...	OPEN	26/Feb/21

- CDR Service Management - Stage Service project
- Back to project
- All tickets
- STARRED
- OTHER
- Service Requests for CDR RAAP (0)
- Onboarding Assitance (1)
- Access Requests for CDR Systems (0)
- Access Requests for JIRA (0)
- Incident with a CDR Provider (CDR Ecosystem) (2)
- Incident with CDR RAAP (0)
- Incident with CTS (0)

For further information contact:
CDRtechnicaloperations@acc.gov.au



Agent: Creating Incidents and Service Requests

Create issue

Import issues ...

Project *

CDR Service Management (CDR) ▼

Project: By default this is set to CDR Service Management.

Issue type *

Incident - CDR Provider (External) ▼

Issue type: (no action needed) - This is the underlying Issue type behind the Request type. Please use the Request type field to make your selection instead of this field.

[Learn more](#)

Request type *

What's this?

Log an Incident with a Data Holder / Accredited Data Recipient
Lodge incidents and issues with a Data Holder or Data Recipient ▼

Request type: Select the incident or service request type. These are the same as what's in the Service Catalogue.

Give feedback

Raise this request on behalf of *

CDR Technical Operations & Participant Sup...

Raise this request on behalf of: Nominate the primary contact person for this request.

Summary

Summary: Provide a short title for your request.

Provide a short title for the incident.

Description

Aa ▼ | **B** | *I* | ... | **A** ▼ | | | | | @ | | | | | + ▼

Press Ctrl + / to learn time-saving keyboard shortcuts.

Description: Provide a detailed description for your request, referencing attachments where applicable.

Provide a detailed description for the incident, referencing attachments where applicable.

For further information contact:

CDRtechnicaloperations@acc.gov.au



Agent: Creating Incidents and Service Requests (continued)

Severity *

3 - Minor ✕ ▼

Set the Severity for the incident

Severity: Set the Severity for the request. (See guide on [page 6](#))

Priority *

3 - Low ▼

Set the Priority for the incident. [Learn more](#)

Priority: Set the Priority for the request. (See guide on [page 6](#))

CDR Provider

▼

Select the CDR Provider you wish to raise the incident with.

CDR Provider: Select the CDR provider that you are reporting the incident to using the dropdown list.

Reporting Organisation *

▼

Select the CDR Provider raising this incident

Reporting Organisation: Select the CDR Provider that you are representing.

Incident Categories and Sub-Categories

CDR Rules/Standards Interpretation ✕ ▼
Implementation ✕ ▼

Select an appropriate Incident Category and Sub-Category

Incident Categories & Sub-categories: Choose the appropriate Incident Category and Sub-category to categorise the issue. (See guide from [page 12](#) to [15](#) for detailed definitions). *Note: This is an optional field when raising the incident*

Attachment

Drop files to attach or [browse](#)

Upload any relevant attachments by dragging and dropping into the field, or by clicking the browse button and selecting files to upload.

Attachment: Upload any relevant attachments by dragging and dropping into the field, or by clicking the browse button and selecting files to upload.

Organizations

Select organization ▼

Organisations: Select the organisation(s) that you wish to share the ticket with.

Security Level

SL for Incidents ✕ ▼

Security Level: (no action needed) This is reset by the system after the record is created.

[Learn more](#)

Create another issue

Cancel

Create

For further information contact:
CDRtechnicaloperations@acc.gov.au



Agent: Managing Incidents

Once you've navigated to either the service request or incident view, you can manage your own tickets by clicking on the relevant ticket in the view.

The screenshot shows the 'CDR Service Management - Stage' interface. On the left is a sidebar with navigation options like 'All tickets', 'STARRED', and 'OTHER'. The main area displays a table of incidents under the heading 'Incidents with CDR Providers (CDR Ecosystem)'. The table has columns for 'T', 'Key', 'Summary', 'Reporter', 'Assignee', 'Status', and 'Created'. One row is highlighted in grey, and a blue arrow points to its 'Summary' cell, which is enclosed in a dashed box with the text 'Click the ticket link to open and edit.'

T	Key	Summary	Reporter	Assignee	Status	Created
<input type="checkbox"/>	CDRSTA-83	CLONE - CLONE - Test Data Holder Incident	CDR Technical Operations	Ben Cane	OPEN	27/Feb/21
<input type="checkbox"/>	CDRSTA-81	Test Data Holder Incident	CDR Technical Operations	Ben Cane	ASSIGNED	27/Feb/21
<input type="checkbox"/>	CDRSTA-79	Poor data quality from Participant Bank Example	Callan Witmitz	Ben Cane	RESOLVED	26/Feb/21
<input type="checkbox"/>	CDRSTA-77	Test Incident shared	johnson.ip	Ashlea Silcock	OPEN	26/Feb/21

Note: Incidents raised with a CDR Provider can only be viewed by ACCC, the Reporter and the Assignee in the queue. Incident that is shared with other users and/or organisations will be presented in the Customer Portal.

For further information contact:
CDRtechnicaloperations@acc.gov.au



Agent: Incident View

In the incident or request view, you're able to progress the ticket through the workflow, request other participants to join the ticket, add internal notes and reply to customer. You can also edit and change other fields, such as priority, severity, incident categories, root cause and expected fix date etc.

← Back
CDRSTA-79

View request in portal

Description
When reviewing customer data, it has been identified that the data is of poor quality, information between columns are being transposed.

Severity 2 - Significant

Priority ^ 1 - High

Components Smart Bank

Incident Categories and Sub-Categories Data Quality - Data Accuracy

Root cause
Data was corrupted prior to uploading.

Activity

CS

Add internal note / Reply to customer

📎

Pro tip: press **M** to comment

🔊
👁️ 1
👍
🔗
⋮

Reporting Organisation
ACCC-CDR

Last Commented Date & Time
None

Last Commented by
None

Automation
⚡ Rule executions

More fields ^

External Reference ID
None

Expected Fix Date
26 Feb 2021

Linked alerts
[View](#)

Created 26 February 2021 at 14:24

Note: Only the Assignee and Reporter can see the internal notes, if you want those whom the ticket is shared with to view the comments in the Customer Portal, please use Reply to customer when commenting on the ticket.

For further information contact:

CDRtechnicaloperations@acc.gov.au



Agent: Sharing of ‘Incident with a CDR Provider’ with another CDR Provider user or organisation

Once you’ve opened the Incident with a CDR Provider, you can share it with another user or organization.

Projects / CDR Service Manage... / CDRSTA-79

Poor data quality from Participant Bank Example

Create subtask Create major incident Link issue

Callan Witmitz raised this request via Portal

Description: When reviewing customer data, it has been identified that the data is of poor quality, information between columns are being transposed.

Severity: 2 - Significant

Priority: 1 - High

Components: Smart Bank

Root cause: Data was corrupted prior to uploading.

Activity: Add internal note / Reply to customer

Ben Cane 26 February 2021, 17:01: Hi Callan.

Resolved Done

Details

Assignee: Ben Cane

Reporter: Callan Witmitz

Request Type: Log an Incident with a Data Holder / Accredited Data Recipient

Organizations: Smart Bank

Labels: Monev App

Request participants: ad

Automation: Ada

Choose the user to which the incident needs to be shared with.

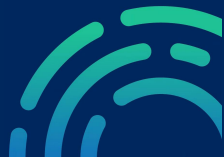
Choose the organisation to which the incident needs to be shared with.

Note: Problem with a CDR Provider will be visible to all the agent users in the CDR Service Management Portal.

If you reassign an incident ticket to another user, you will no longer have visibility of the ticket in the Agent view. You will still be able to see it in the Customer Portal if the ticket is shared with you/or your organisation.

For further information contact:

CDRtechnicaloperations@acc.gov.au



Agent: Progressing Through Workflows

Waiting for Assignee ▾

Pending Clarification → PENDING CDR RULES/STANDARDS...

Pending Bug-Fix/ Release → PENDING FIX

Fixed → READY TO VERIFY

Need more information → WAITING FOR REPORTER

View workflow

Assignee

CA CDR TechOps Test Agent

Assign to me

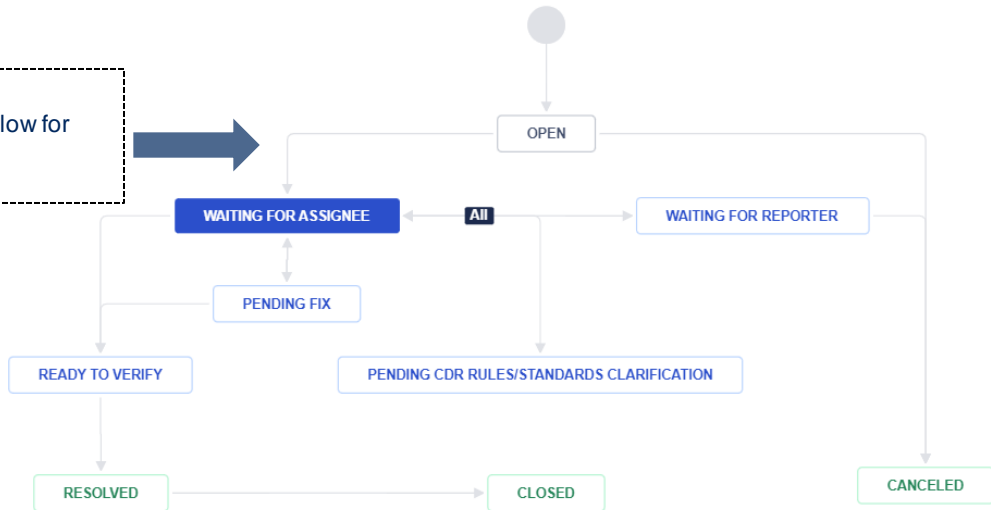
Reporter

A Ada

Click the incident status button to see the next stages of workflow and select the relevant stage to progress the ticket.

Note: It is advised to change the state from “Waiting for Assignee” to “Waiting for Reporter” if you are waiting for more information from the incident reporter.

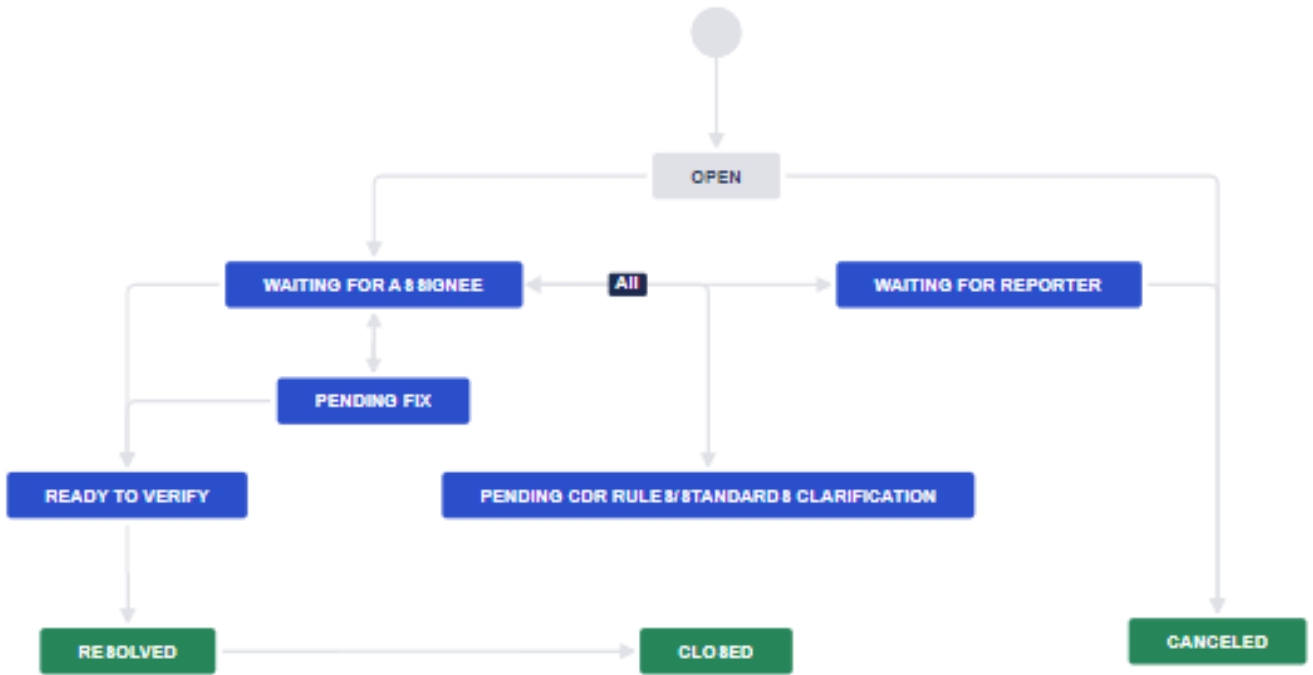
This is an example of the workflow for progressing an incident.



For further information contact:
CDRtechnicaloperations@acc.gov.au



Agent: Incident Lifecycle Management for CDR Provider Incidents



OPEN: The incident will be in an “OPEN” state when it has been raised by the participant.

PENDING CDR RULES/STANDARD CLARIFICATION: The incident requires clarification before it can proceed

CANCELLED: The incident will need to be changed to “CANCELLED” state by the participant raising the ticket on mutual agreement.

WAITING FOR ASSIGNEE: The participant who the ticket is assigned to will need to triage the incident and transition it to another state.

PENDING FIX: The incident is waiting on the assignee to provide a solution.

RESOLVED: Once the participant has verified the incident, they can change the state to “RESOLVED” if the incident has been fixed. The state needs to be changed to “ASSIGNED” if the incident is not resolved on verification.

WAITING FOR REPORTER: The ticket is waiting for the incident reporter to provide input.

READY TO VERIFY: The incident will need to be progressed to “READY TO VERIFY” state and reply back to the participant raising the incident and ask them to verify.

CLOSED: CDR Technical Operations team will review the incident and change it to “CLOSED” state once the incident has been resolved.

Note: It is very important for the participants to adhere to the above-mentioned incident life cycle management process.

For further information contact:

CDRtechnicaloperations@acc.gov.au



Agent: Adding Comments - Differences between Internal and Customer Facing Comments

In the incident or request view, you can reply to the customer or add an internal note.

Reply to customer is visible to both the people who you had shared this ticket and the agents assigned to the ticket. To ensure that the note is visible to all interested parties, by default, you should select Reply to customer when commenting on the ticket.

Internal note is viewable only by other agents assigned to the ticket (Reporter / Assignee) and is not visible in the Customer Portal.

Inform stakeholders is not currently in use, ignore this option.

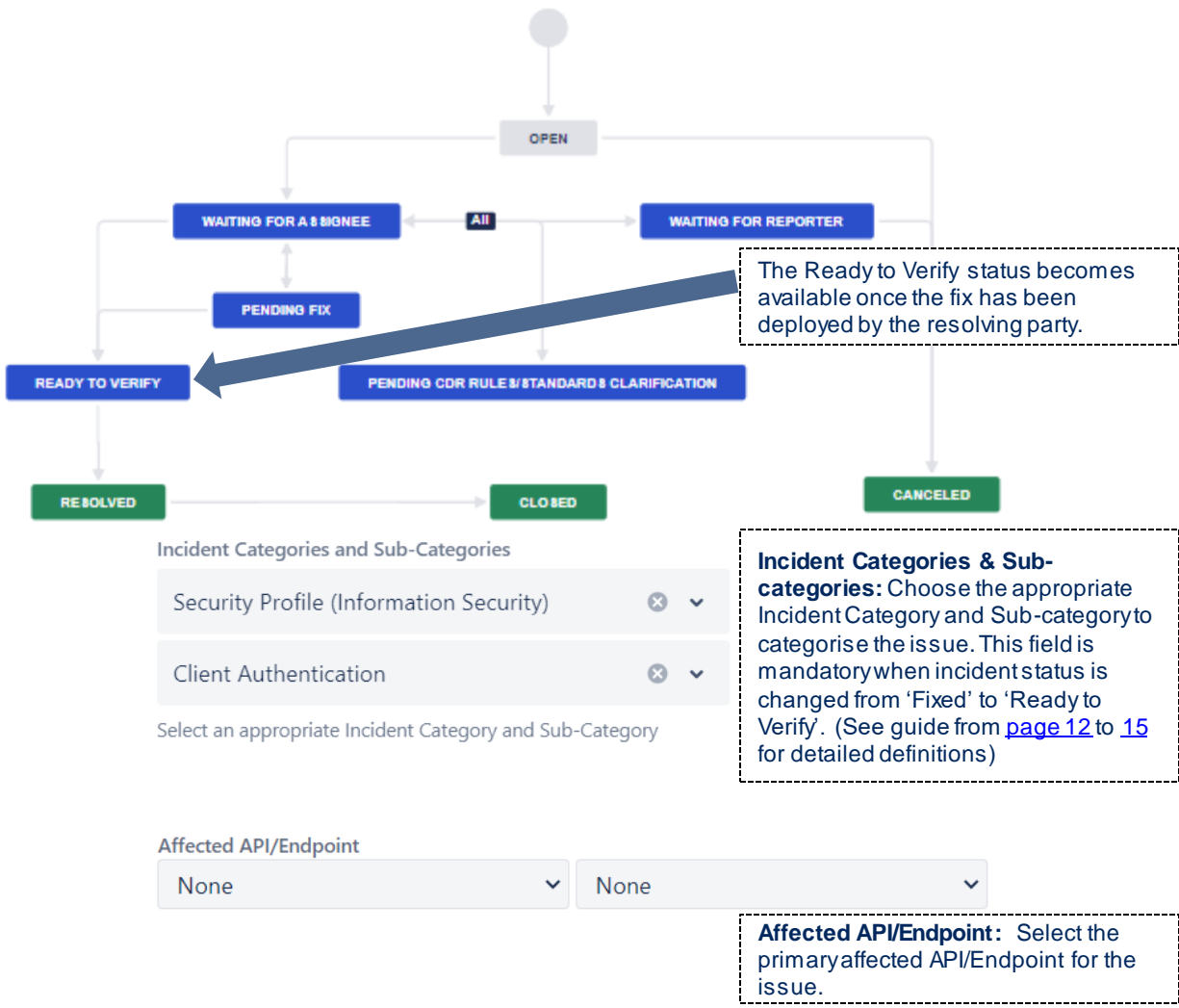
The screenshot shows a ticket comment interface with three comment entries. The top entry is a public comment from 'Ada' at 16 March 2023 at 14:29. The middle entry is an internal note from 'Ada' at 16 March 2023 at 14:20, highlighted in yellow. The bottom entry is a public comment from 'Ada' at 16 March 2023 at 14:18. A callout box points to the 'Reply to customer' option in the top comment's header, stating: 'Click on the Reply to customer hyperlink to add a comment. You can also edit and delete your notes and comments if you've made a mistake.' Another callout box points to the 'Internal note' header, stating: 'Note: The internal note is hidden on the Customer Portal'. A third callout box points to the bottom comment, which is a public comment.

For further information contact:
CDRtechnicaloperations@acc.gov.au



Agent: Fixing and Verifying Incidents

An incident is *fixed* when the resolving participant has investigated and fixed the issue. The incident can be changed to *Ready to Verify* and a reply sent to the impacted participant informing them to conduct verification.



Incident Categories and Sub-Categories

- Security Profile (Information Security) [x] v
- Client Authentication [x] v

Incident Categories & Sub-categories: Choose the appropriate Incident Category and Sub-category to categorise the issue. This field is mandatory when incident status is changed from 'Fixed' to 'Ready to Verify'. (See guide from [page 12](#) to [15](#) for detailed definitions)

Affected API/Endpoint

None v None v

Affected API/Endpoint: Select the primary affected API/Endpoint for the issue.

Note: It is very important for the participants to progress the incident to "Ready to Verify" state as soon as the fix has been deployed.

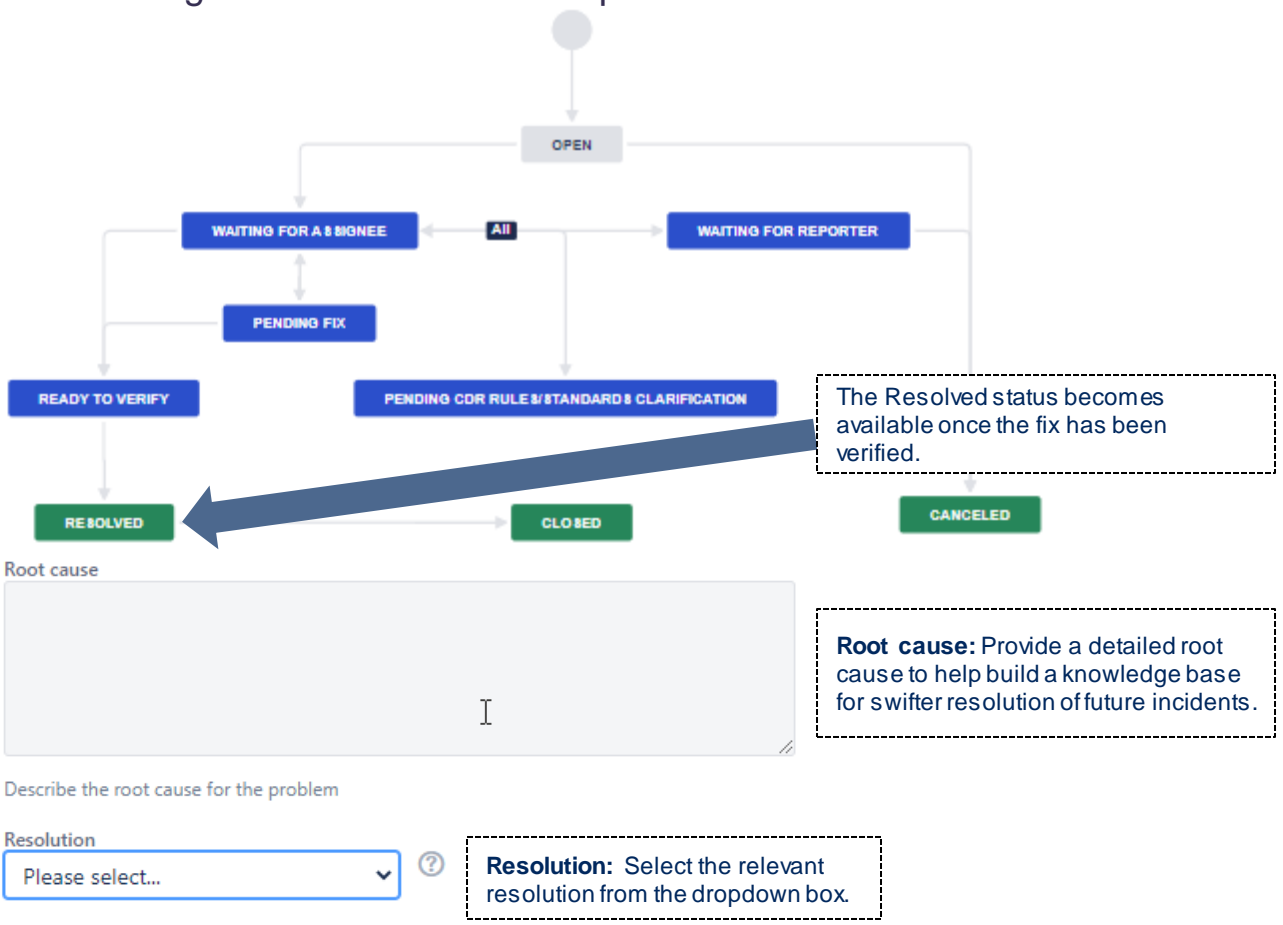
For further information contact:
CDRtechnicaloperations@acc.gov.au



Agent: Resolving and Closing Incidents

An incident is *resolved* when the impacted participant confirms the incident is resolved.

The incident can be *closed* by the CDR Technical Operations team when all impacted participants agree the incident has been resolved and all outstanding actions have been completed.



Note: It is very important for the participants to progress the incident to “Resolved” state as soon as it has been fixed and verified.

For further information contact:
CDRtechnicaloperations@acc.gov.au