



Australian Government



Consumer
Data Right

CDR Service Management Portal Guide for Participants

Version 6.3

March 2025





Contents

Portal Overview.....	1
Disclaimer.....	2
CDR Service Management Portal.....	3
Severity and Priority Classification	4
Incident Categories.....	5
Incident Sub-Categories	6
Customer View.....	9
Logging an Incident or Request - Portal	10
Logging an Incident or Request – Service Catalogue.....	11
Types of Incidents and Requests	12
Incident with the Conformance Test Suite (CTS).....	13
Incident with a CDR Provider.....	14
Incident with the CDR Register and Accreditation Application Platform (RAAP)	15
Sharing ‘Incident with a CDR Provider’ with another CDR Provider	16
Implementation Gaps & Rectification Schedule	17
Service Requests	20
Tracking Requests.....	21
Updating or Commenting on Requests.....	21
Progressing through workflows.....	22
Agent View.....	23
Agent Role.....	24
Creating Incidents and Service Requests.....	25
Managing Incidents.....	27
Incident View	28
Sharing ‘Incident with a CDR Provider’ with another CDR Provider	29
Progressing Through Workflows.....	30
Incident Lifecycle Management for CDR Provider	31
Internal and Customer Facing Comments	32
Fixing and Verifying Incidents.....	33
Resolving and Closing Incidents.....	34



CDR Service Management Portal Portal Overview





Disclaimer

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* (Cth), and the Competition and Consumer (Consumer Data Right) Rules 2020.
- accepts that the information it reports or includes will be available to the intended participants.
- accepts that participants are not subject to any confidentiality obligations regarding the use of such information.
- 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, time taken to resolve and severity of incidents, 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 any questions to the Technical Operations inbox CDRTechnicalOperations@acc.gov.au .



CDR Service Management Portal

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 and raise and process incidents and service requests (i.e. move incidents through workflows, reassign incidents to other teams and make customer-facing comments).



Severity and Priority Classification

The Priority 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	CDR ecosystem is unavailable, or the ecosystem functionality is severely degraded.	<ul style="list-style-type: none"> Many 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	One or more CDR providers are not able to share data.	<ul style="list-style-type: none"> A moderate number of CDR consumers are affected and/or disadvantaged in some way. Moderate reputational/ financial impact for CDR participants. Partial impact on critical services that stops or limits business functions.
Minor	Degradation of a service impacting an accredited data recipient, a data holder 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 on availability of non-critical service(s).

Priority

Category / Impact	CDR Ecosystem	Business / Consumer
High	Critical risk to the 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.
Significant	Medium risk to the 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.
Minor	Low risk to the 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.



Incident Categories

The Incident categories/sub-categories will enable the ACCC 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	Incidents related to establishing, amending and revocation of consent (authorisation).
Dynamic Client Registration	Incidents related to a software product registering with a data holder's 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.



Incident Sub-Categories

A number of sub-categories are available for each incident category which enables 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 (authorisation) with a data holder brand.	Incidents related to issues with authentication (OTP).
	Amending an existing consent	Incidents related to modifying an existing consent (authorisation) with a data holder brand.	Unable to extend the consent etc.
	Revocation of an existing consent	Incidents related to removing an existing consent (authorisation).	Data holders not notifying the accredited 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 data holder's source 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.



Incident Sub-Categories (cont.)

A number of sub-categories are available for each incident category which enables 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 standards.
System/ Service Availability	System/Service Availability	Incidents related to participants' system or services availability.	Failed 5XX response from participants' 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.



Incident Sub-Categories (cont.)

A number of sub-categories are available for each incident category which enables 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 and 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 (CX) Standards and guidelines in the CDR ecosystem.	Non-conformance with User Interface (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.	



Consumer
Data Right

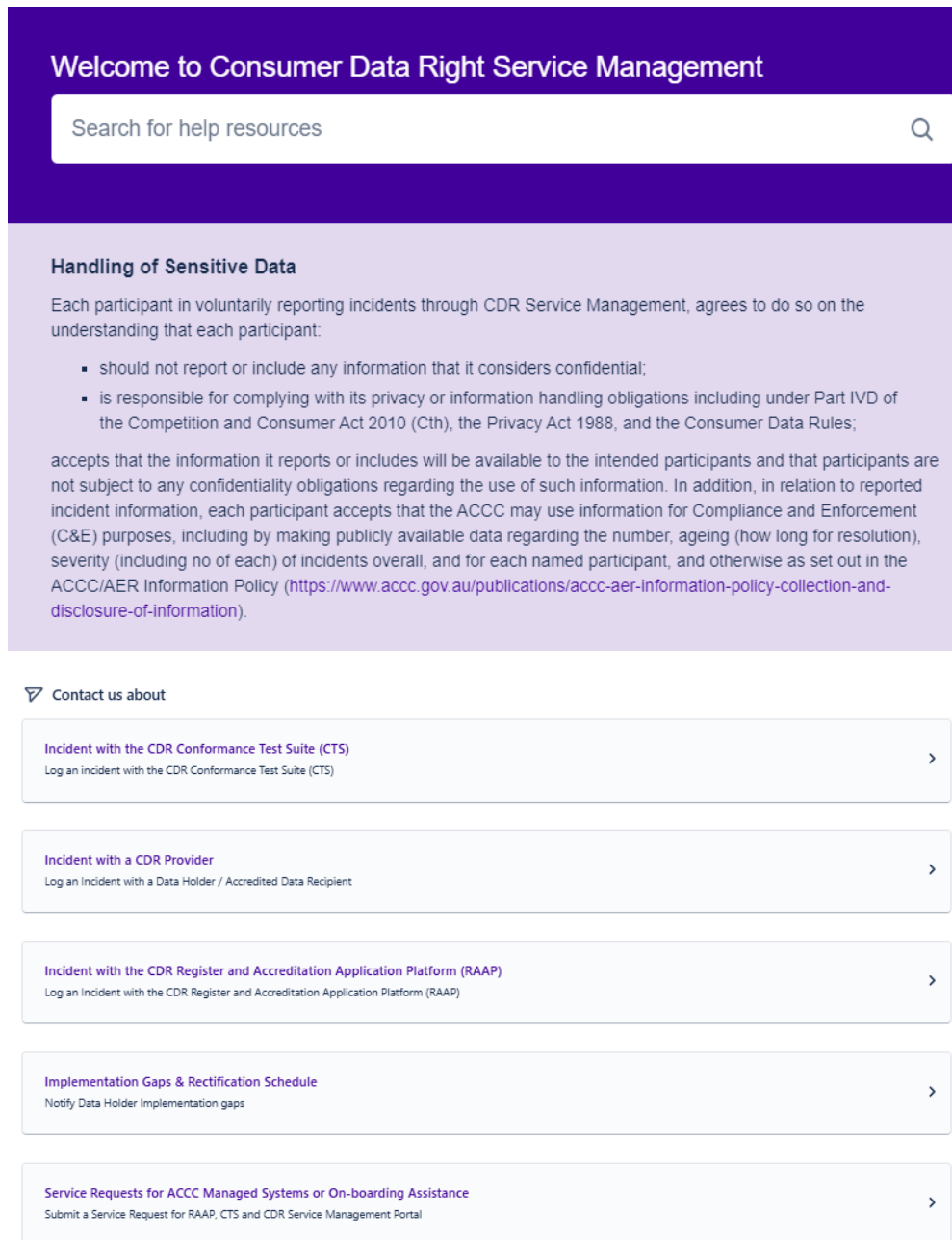
CDR Service Management Portal Customer View





Logging an Incident or Request - Portal

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



Welcome to Consumer Data Right Service Management

Search for help resources

Handling of Sensitive Data

Each participant in voluntarily reporting incidents through CDR Service Management, 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>).

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



Logging an Incident or Request - Service Catalogue

Participants are next presented with a **service catalogue** when entering from the [customer portal](#). From here service offerings are available to raise a variety of issues and requests. Technical incidents may be shared between participants. In certain scenarios, the ACCC CDR Technical Operations team can be included if required. Participants can also submit tickets with the ACCC CDR if they believe an ACCC CDR system is the cause of an incident.

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

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

Select Request Type

To raise a ticket, select the [request type](#) most aligned to your requirement to ensure your request gets to the right team.



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 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 Suite.
Incident with a CDR Provider	Used to raise a technical incident with a CDR participant, where the resolving party is another data holder or accredited 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.
Implementation Gaps & Rectification Schedule	Used by Data Holders to notify the ACCC of CDR implementation gaps and the proposed rectification schedule.
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 Conformance Test Suite (CTS)

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)







Use this ticket type to raise an incident for an issue when testing with the Conformance Test Suite. For further information, please refer to [CDR Service Management Portal Guide](#)

Required fields are marked with an asterisk *

Raise this request on behalf of *

Summary *

Provide a short title for the incident.

Description
 B *I* ...       +

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

Severity *

Set the Severity for the incident.

Priority *

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

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

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 4](#)).

Priority: Set the Priority for the incident. (See guide on [page 4](#)).

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.



Sharing 'Incident with a CDR Provider' with another CDR Provider

Access the CDR Service Management Portal via this link:
<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.

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

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

Activity

CO



Implementation Gaps & Rectification Schedule

This request type allows data holders to notify the ACCC of any CDR implementation gaps. We expect data holders to promptly rectify any 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 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 organisation 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.



Notify Data Holder Implementation Gaps (cont.)

Data Holder Legal Entity and Brand

Select the Data Holder Legal Entity and Brand

Proposed Resolution Date



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

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.

Attachment

Drag and drop files, paste screenshots, or browse

Browse

Send Cancel

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

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

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

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 in Column 1 or 2 is not suitable for publication, email acc-cdr@acc.gov.au for further guidance.

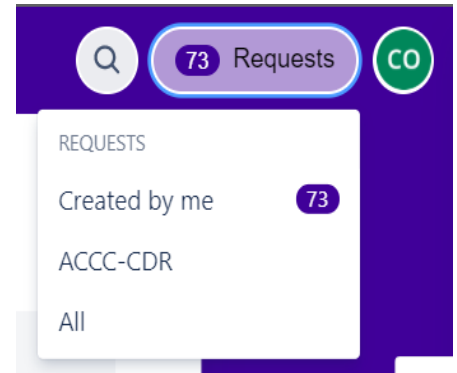
Tracking Requests

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 you.

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.



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

BC Ben Cane raised this on Monday 2:31 PM [Hide details](#)

Description
Test

Severity
Sev-1

Priority
Medium

Activity

BC

Aa B I ... [Rich Text Editor Icons]

Save

Updating or Commenting on Requests

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

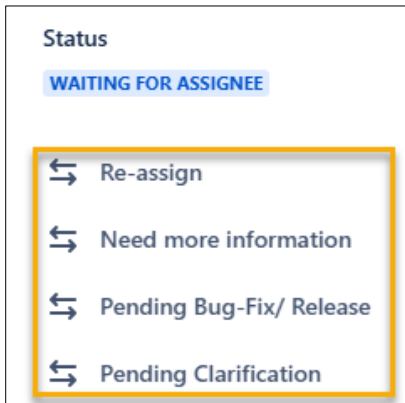
Type your comments by clicking in the comments field.

Click **Save** to submit your comment or update.



Progressing through workflows

When an incident has been submitted you will have the options to progress the incident to the following workflow stages.



The screenshot shows a 'Status' dropdown menu with the current status 'WAITING FOR ASSIGNEE'. Below it, a list of four workflow stages is displayed, each with a double-headed arrow icon: 'Re-assign', 'Need more information', 'Pending Bug-Fix/ Release', and 'Pending Clarification'. The entire list is enclosed in a yellow rectangular border.

When you click on any of the stages, you will be prompted to enter additional information.

Re-assign

Enter additional information, then click **Re-assign** and this will reassign the ticket back to the current assignee.

Need more information

Enter the information required and click **Need more information**.

Pending Bug-Fix/Release

Enter the details and click on **Pending Bug-Fix/Release**. Example, the fix for this incident is reliant on a bug-fix planned for release in Jan 2025...

Pending Clarification

Use this status to indicate that your ticket is pending CDR Rules/Standards Clarification. It will set the stage to **Pending Clarification**.



Consumer
Data Right

CDR Service Management Portal Agent View





Agent Role

The Agent role can access queues and 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 into <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 create new incidents and service requests from the top menu bar.

Note: You will only see incidents and/or service requests that are assigned to yourself and/or reported by yourself.

Projects / CDR Service Management / Queues
Incidents with CDR Providers (CDR Ecosystem)

276 issues

T	Key	Severity	P	Summary	Reporter	Assignee	Status
<input type="checkbox"/>	CDR-...	3 - Minor	▼				WAITING FO
<input type="checkbox"/>	CDR-...	3 - Minor	▼				WAITING FO
<input type="checkbox"/>	CDR-...	3 - Minor	▼				WAITING FO
<input type="checkbox"/>	CDR-...	3 - Minor	▼				WAITING FO
<input type="checkbox"/>	CDR-...	3 - Minor	▼				WAITING FO
<input type="checkbox"/>	CDR-...	3 - Minor	▼				WAITING FO
<input type="checkbox"/>	CDR-...	2 - Significant	▲				WAITING FO

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.

Priority group

Team Priority
8 queues

Incidents with CDR Providers (CDR Ecosystem)	256
Incidents with CDR RAAP	26
Incidents with CTS (Production)	4
Incidents with CTS (Beta)	0
Problems with CDR Providers (CDR Ecosystem)	9
Problems with CDR RAAP / CTS	1
Service Requests for ACCC CDR managed systems	15
Implementation gaps of a Data Holder (Rectification Schedule)	2



Creating Incidents and Service Requests

Create issue

[Import issues](#) ⋮

Project*

CDR Service Management (CDR) ▼

Issue type*

Incident - CDR Provider (External) ▼

[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

[Give feedback](#)

Raise this request on behalf of*

CDR Technical Operations & Participant Sup...

Summary

Provide a short title for the incident.

Description

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

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

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

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

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

Select the incident or service request type. These are the same as what is in the Service Catalogue.

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

Summary: Provide a short title for your request.

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



Creating Incidents and Service Requests (cont.)

Severity *

3 - Minor

Set the Severity for the incident

Priority *

3 - Low

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

CDR Provider

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

Reporting Organisation *

Select the CDR Provider raising this incident


Incident Categories and Sub-Categories

CDR Rules/Standards Interpretation

Implementation

Select an appropriate Incident Category and Sub-Category

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.

Organizations

Select organization

Security Level

SL for Incidents

[Learn more](#)

Create another issue

Cancel

Create

Severity: Set the Severity for the request. (See guide on [page 4](#)).

Priority: Set the Priority for the request. (See guide on [page 4](#)).

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

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

Incident Categories & Sub-categories: Choose the appropriate Incident Category and Sub-category to categorise the issue. (See guide from [pages 5 to 8](#) for detailed definitions). *Note: This is an optional field when raising the incident*

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

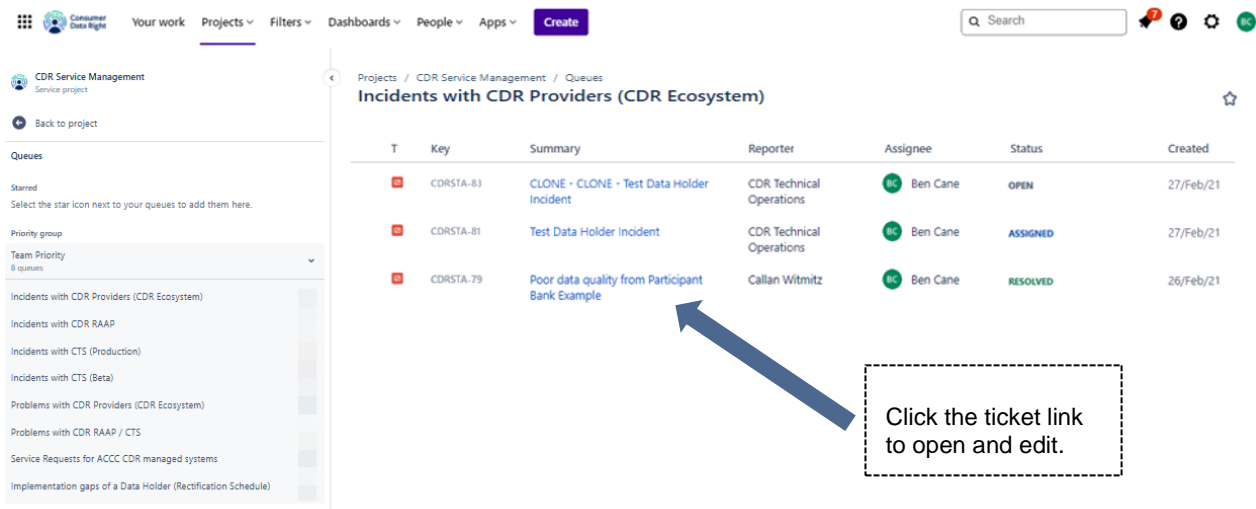
Organisations: Select the organisation(s) that you wish to share the ticket with.

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

Managing Incidents

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

Note: You will only see incidents and/or service requests that are assigned to yourself and/or reported by yourself.



The screenshot shows the 'Incidents with CDR Providers (CDR Ecosystem)' view. The table contains the following data:

T	Key	Summary	Reporter	Assignee	Status	Created
	CDRSTA-83	CLONE - CLONE - Test Data Holder Incident	CDR Technical Operations	Ben Cane	OPEN	27/Feb/21
	CDRSTA-81	Test Data Holder Incident	CDR Technical Operations	Ben Cane	ASSIGNED	27/Feb/21
	CDRSTA-79	Poor data quality from Participant Bank Example	Callan Witmitz	Ben Cane	RESOLVED	26/Feb/21

A callout box with a dashed border and an arrow pointing to the link 'Poor data quality from Participant Bank Example' contains the text: 'Click the ticket link to open and edit.'

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.



Incident View

In the incident or request view, you are 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, use **Reply to customer** when commenting on the ticket.

Sharing 'Incident with a CDR Provider' with another CDR Provider

Once you have opened the Incident with a CDR Provider, you can share it with another user or organisation.

Projects / CDR Service Management / CDRSTA-79

Poor data quality from Participant Bank Example

Create subtask Create major incident Link issue

Callan Witmitz raised this request via Portal [View request in portal](#) [Hide details](#)

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 None

Root cause
Data was corrupted prior to uploading.

Activity
Show: All Comments History
Newest first

[Add internal note](#) / [Reply to customer](#)
Pro tip: press **M** to comment

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 x mon

Labels Money App

Request participants ada

Automation Ada

More fields

External Reference ID None
Expected Release Date None
Linked Tickets View

Created 26 February 2021, 14:24
Updated 26 February 2021, 18:01
Resolved 26 February 2021, 18:00

Configure

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.



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

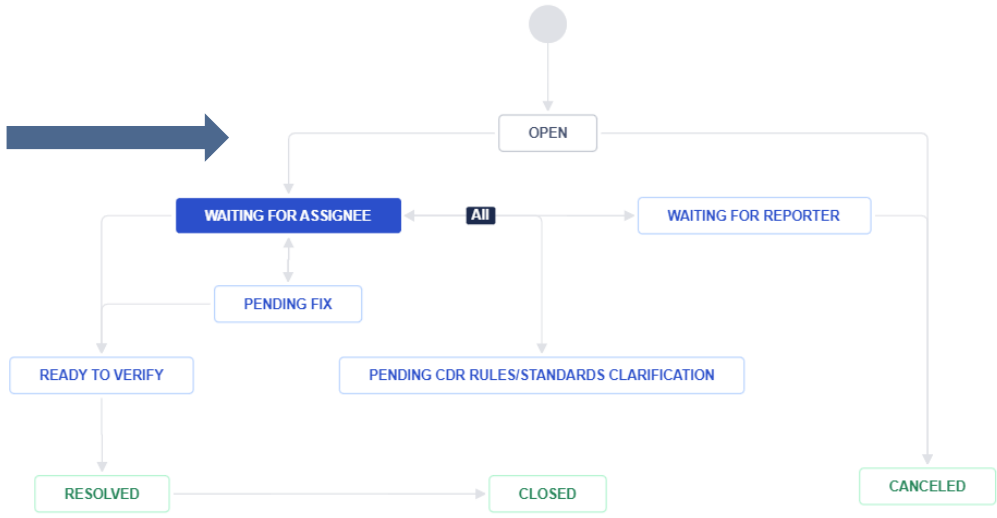
Reporter

- A Ada

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

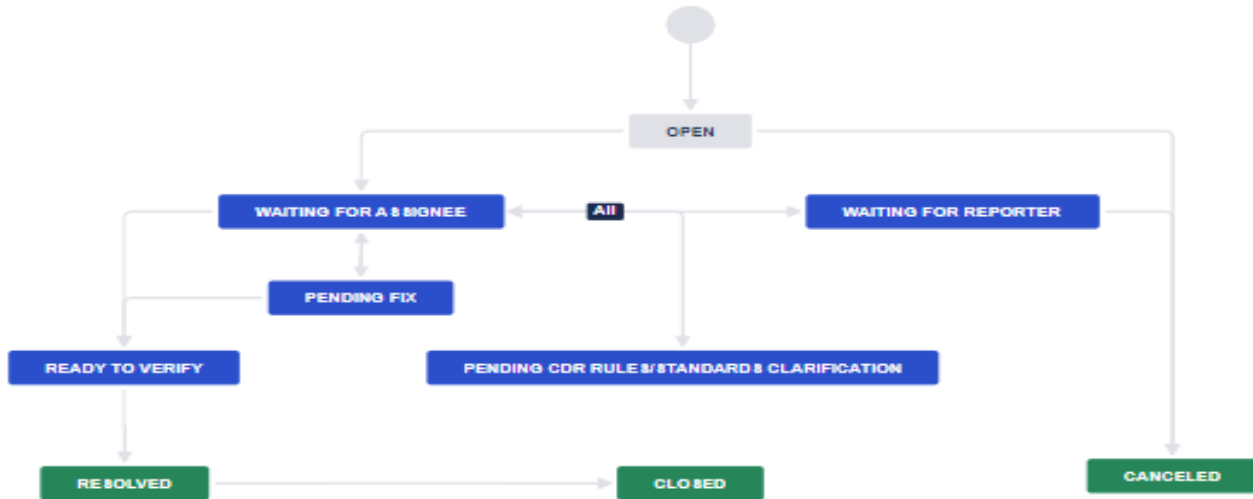
Note: It is advised to change the state from **Waiting for Assignee** to **Waiting for Reporter** if you are waiting for more information from the incident reporter.

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





Incident Lifecycle Management for CDR Provider



Incidents

<p>OPEN: The incident will be in an “OPEN” state when it has been raised by the participant.</p>	<p>WAITING FOR ASSIGNEE: The participant who the ticket is assigned to will need to triage the incident and transition it to another state.</p>	<p>WAITING FOR REPORTER: The ticket is waiting for the incident reporter to provide input.</p>
<p>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.</p>	<p>PENDING FIX: The incident is waiting on the assignee to provide a solution.</p>	<p>PENDING CDR RULES/STANDARD CLARIFICATION: The incident requires clarification before it can proceed.</p>
<p>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.</p>	<p>CLOSED: CDR Technical Operations team will review the incident and change it to “CLOSED” state once the incident has been resolved.</p>	<p>CANCELLED: The incident will need to be changed to “CANCELLED” state by the participant raising the ticket on mutual agreement.</p>

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



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.

A Add internal note / Reply to customer / Inform stakeholders

Pro tip: press **M** to comment

A Ada 16 March 2023 at 14:29
Hi Participant X,
Just following up on the last comment.
Edit · Delete · 🗨️

A Ada 16 March 2023 at 14:20 Edited · Internal note
Hi Participant X,
Information A provided was incomplete, can you send it again so that we can work on it.
Edit · Delete · 🗨️

A Ada 16 March 2023 at 14:18 Edited
Hi Participant X,
To assist in incident resolution, can you provide the following information:

- Information A
- Information B

Edit · Delete · 🗨️

A Ada Today 2:18 PM
Hi Participant X,
To assist in incident resolution, can you provide the following information:

- Information A
- Information B

A Ada Today 2:29 PM
Hi Participant X,
Just following up on the last comment.

A Add a comment

*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.*

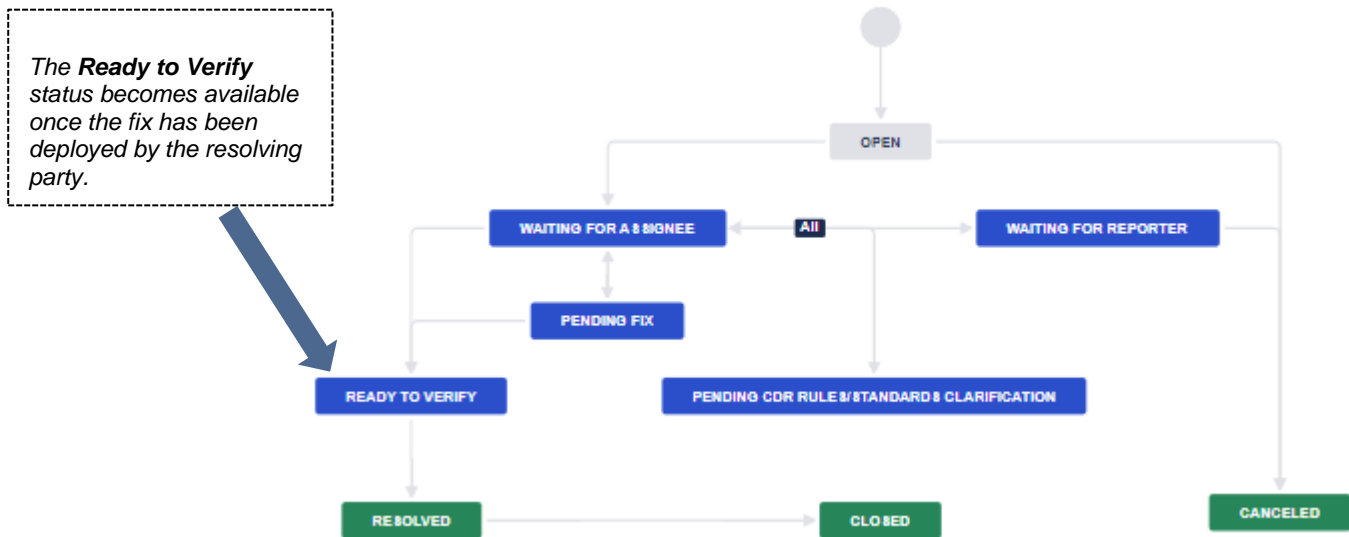
*Note: The **internal note** is hidden on the Customer Portal*



Fixing and Verifying Incidents

An incident is *fixed* when the resolving participant has investigated and fixed the incident.

The incident can be changed to **Ready to Verify** and a reply sent to the impacted participant informing them to conduct verification.



The **Ready to Verify** status becomes available once the fix has been deployed by the resolving party.

Root cause

Root cause: Provide a detailed root cause to help build a knowledge base for swifter resolution of future incidents.

Describe the root cause for the problem

Resolution

Resolution: Select the relevant resolution from the dropdown box.

Incident Categories and Sub-Categories

Security Profile (Information Security)

Client Authentication

Incident Categories & Sub-categories: Choose the appropriate Incident Category and Sub-category to categorise the issue (See guide from [pages 5-8](#) for detailed definitions). This field is mandatory when incident status is changed from **Fixed** to **Ready to Verify**.

Select an appropriate Incident Category and Sub-Category

Affected API/Endpoint

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

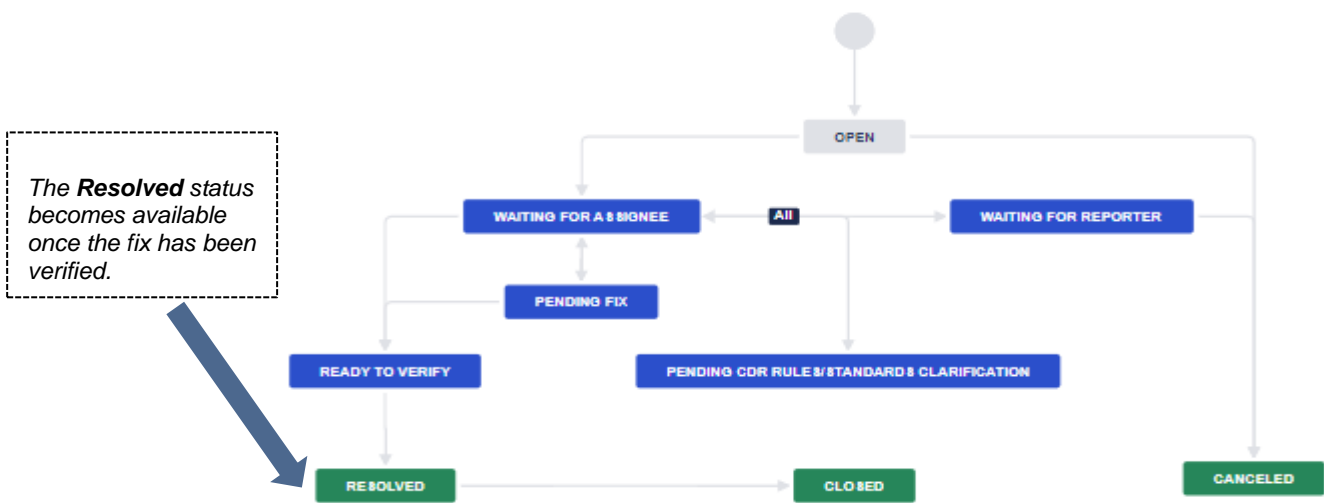
Note: It is very important for the participants to progress the incident to **Ready to Verify** state as soon as the fix has been deployed.



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 **Ready to Verify** state as soon as the fix has been deployed.