Australian Government

Consumer Data Right

CDR Service Management Portal user guide

Australian Competition and Consumer Commission

User guide

Version 2

September 2026

Contents

Terms of use

By voluntarily reporting incidents through the Consumer Data Right (CDR) Service Management Portal, each participant agrees that it:

- will not report or include any information that it considers confidential
- is responsible for complying with the Service Management Portal's privacy and information-handling obligations, including
  - Part IVD of the *Competition and Consumer Act 2010* (Cth)
  - the *Privacy Act 1988* (Cth)
  - 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 about the use of such information

Further, each participant accepts that the Australian Competition and Consumer Commission may use reported incident information for compliance and enforcement purposes. This may include making publicly available data on the number and severity of incidents and the time taken to resolve them. Data may also be made available as set out in the ACCC/AER information policy.

Thanks for your ongoing support of CDR. Please direct any questions to the Technical Operations inbox: cdrtechnicaloperations@accc.gov.au.

1. CDR Service Management Portal overview

The Consumer Data Right (CDR) Service Management Portal (SMP) is provided by the Australian Competition and Consumer Commission (ACCC) for CDR participants to raise, manage, and communicate technical incidents with each other and with the CDR Technical Operations team. The CDR Technical Operations team takes a ‘monitoring’ approach to aid resolution of issues and promote a healthy and effective CDR ecosystem.

The CDR SMP can be accessed here: cdrservicemanagement.atlassian.net/servicedesk

1.1 Gaining access

To request access:

- Ask your organisation's CDR representative to submit a service request; or
- Email: cdrtechnicaloperations@accc.gov.au.

1.2 Role types

The CDR Service Management Portal allows for 2 types of roles, ‘agent’ and ‘customer’. Each participant can have 1 agent license and up to 5 customer licences for each organisation.

Role type	Description
Customer	Has restricted access, can raise new incidents & service requests, as well as view and comment on incidents that are shared with them. Tickets cannot be assigned to Customer users.
Agent	Has a higher level of access, can access queues to create, process, and manage incidents & service requests. Agents can have tickets assigned to themselves, progress incidents through workflows, reassign them to other teams, and add customer-facing comments.

Note

The options and information available in the SMP and visible on your screen depend on your role – customer or agent.

Additional licences can be requested by raising a service request in the CDR Service Management Portal or by emailing the CDR Technical Operations team via cdrtechnicaloperations@accc.gov.au. Requests will be reviewed based on demonstrated business need.

1.3 Severity and priority classification

The priority and severity criteria assess incidents and issues for impact and urgency. This gives a consistent measurement of incidents and issues that may impact a single participant or the ecosystem.

1.3.1 Severity

Category/ impact	CDR ecosystem	Business/consumer
Major	CDR ecosystem is unavailable or ecosystem functionality is severely degraded	• Many CDR consumers are affected and/or acutely disadvantaged in some way • Major reputational/financial impacts for multiple CDR participants • Unavailability of service(s) stops critical business functions
Significant	One or more CDR providers cannot share data	• A moderate number of CDR consumers are affected and/or disadvantaged in some way • Moderate reputational/financial impacts for CDR participants • Partial impact on critical services that stops or limits business functions
Minor	Degradation of a service affecting an accredited data recipient, a data holder or the CDR Register	• A limited number of CDR consumers are affected and/or disadvantaged but not in a significant way • No or minor reputational/financial impact for CDR participants • Impact on availability of non-critical service(s)

1.3.2 Priority

Category/ impact	CDR ecosystem	Business/consumer
High	Critical risk to the CDR ecosystem and no workaround is available Consumer data cannot be shared	• Critical risk to the business of the reporting organisation, and no workaround is available • The damage caused by the incident increases rapidly • Most users are affected
Significant	Medium risk to the CDR ecosystem and no workaround is available Most consumer data cannot be shared	• Medium risk to the business of the reporting organisation and no workaround is 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 is available Some consumer data cannot be shared	• Low risk to the business of the reporting organisation and a workaround is available • The damage caused by the incident only marginally increases over time • Single user impact

1.4 Incident categories

The incident categories and subcategories will enable the ACCC CDR team 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 revoking 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, completeness and consistency, and to 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 profiles in the CDR ecosystem. **Note:** This does not include incidents related to security events such as data breaches
Consumer Experience	Incidents caused by nonconformance to Consumer Experience (CX) Standards and Guidelines in the CDR ecosystem
Admin API (Get Metrics)	Incidents related to lack or noncompliance of data from the Get Metrics API
Other	Incidents that fall outside of the above-mentioned categories

Note

The following table provides subcategory definitions.

1.5 Incident subcategories

Subcategories are available for each incident category. This enables more precise classification of incidents reported in the CDR ecosystem.

Categories	Subcategories	Subcategory 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 (one-time password)
	Amending an existing consent	Incidents related to modifying an existing consent (authorisation) with a data holder brand	Consumer unable to extend the consent
	Revoking an existing consent	Incidents related to removing an existing consent (authorisation)	Data holders not notifying the accredited data recipient that

Categories	Subcategories	Subcategory definition	Examples
			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	Incomplete 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
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 (compared to the established standards) shared by the participants
System/ Service Availability	System/Service Availability	Incidents related to participants' system or services availability	Failed 5xx response from participants' systems or 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	Slower response times for API requests, which do not meet the defined performance standards
	Throttling	Incidents related to non-conformance to the traffic thresholds defined in Consumer Data Standards	Failed responses due to use of throttling limits
CDR Rules / Standards Interpretation	Implementation Error	Incidents related to issues caused by 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 or insufficient documentation of CDR Rules and Standards	Incidents raised due to discrepancy between Consumer Data Standards and other normative references

Categories	Subcategories	Subcategory definition	Examples
Security Profile (Information Security)	Certificate Error	Incidents related to authentication errors 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 and claims	An invalid claim error is encountered
	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 recycling
Consumer Experience	Consumer Experience	Incidents caused by non-conformance to CX Standards and Guidelines in the CDR ecosystem	Nonconformance with user interface 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 noncompliance of Get Metrics Data	Data returned by Get Metrics indicates that the solution is classed as non-functional
Other	Other	Incidents that fall outside of the above-mentioned categories	

CX = consumer experience; DCR = Dynamic Client Registration

Note: A 5xx response is a category of error codes returned by webservers. It is similar to the well-known 404 error.

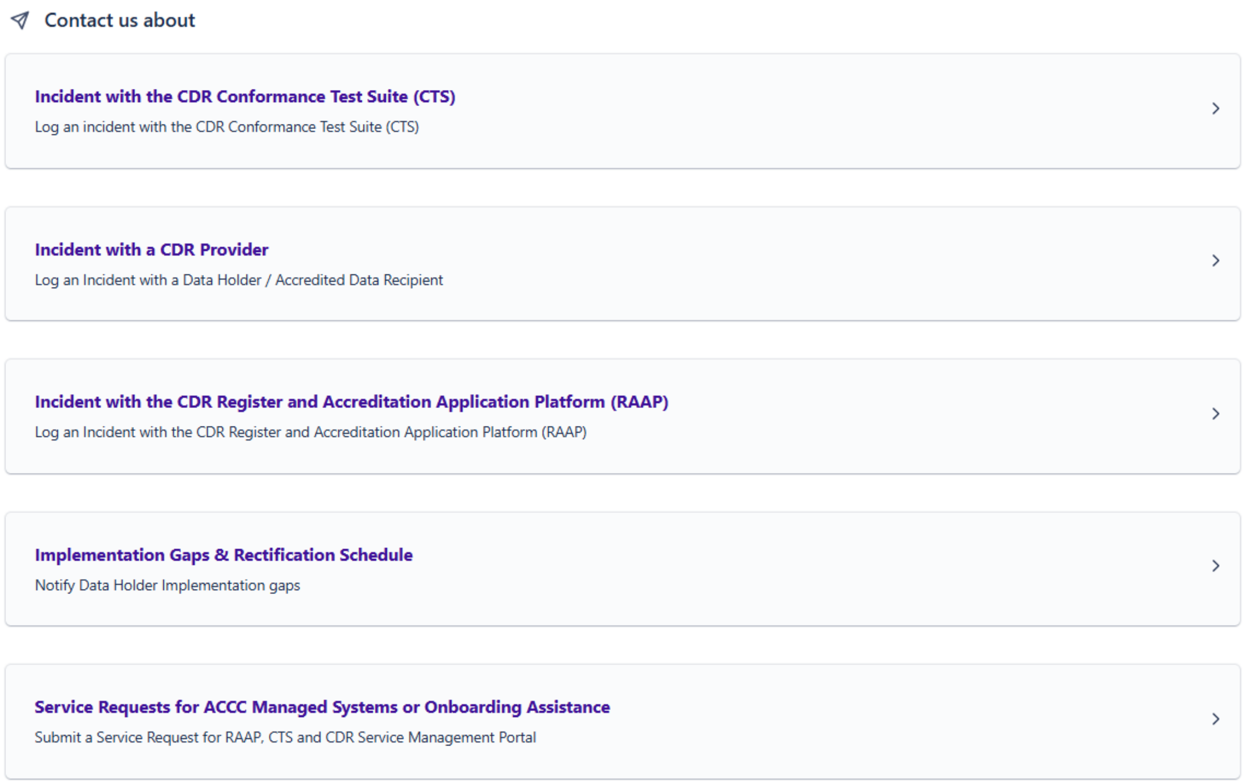
2. CDR Service Management Portal: customer view

2.1 Logging an incident or request

The CDR SMP is at cdrservicemanagement.atlassian.net/servicedesk.

2.2 Logging an incident or request: service catalogue

Participants are presented with a service catalogue when entering from the CDR SMP. From here, a variety of issues and requests can be raised. Technical incidents may be shared between participants. In some scenarios, the CDR Technical Operations team can be included if required. Participants can also submit tickets in the CDR SMP if they believe a CDR system is the cause of an incident.



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

After a ticket is logged, a notification email is generated and sent to the requestor, the recipient and anyone the ticket has been shared with.

> **Selecting a request type**
>
> To raise a ticket, select the request type closest to your requirement to ensure your request gets to the right team.

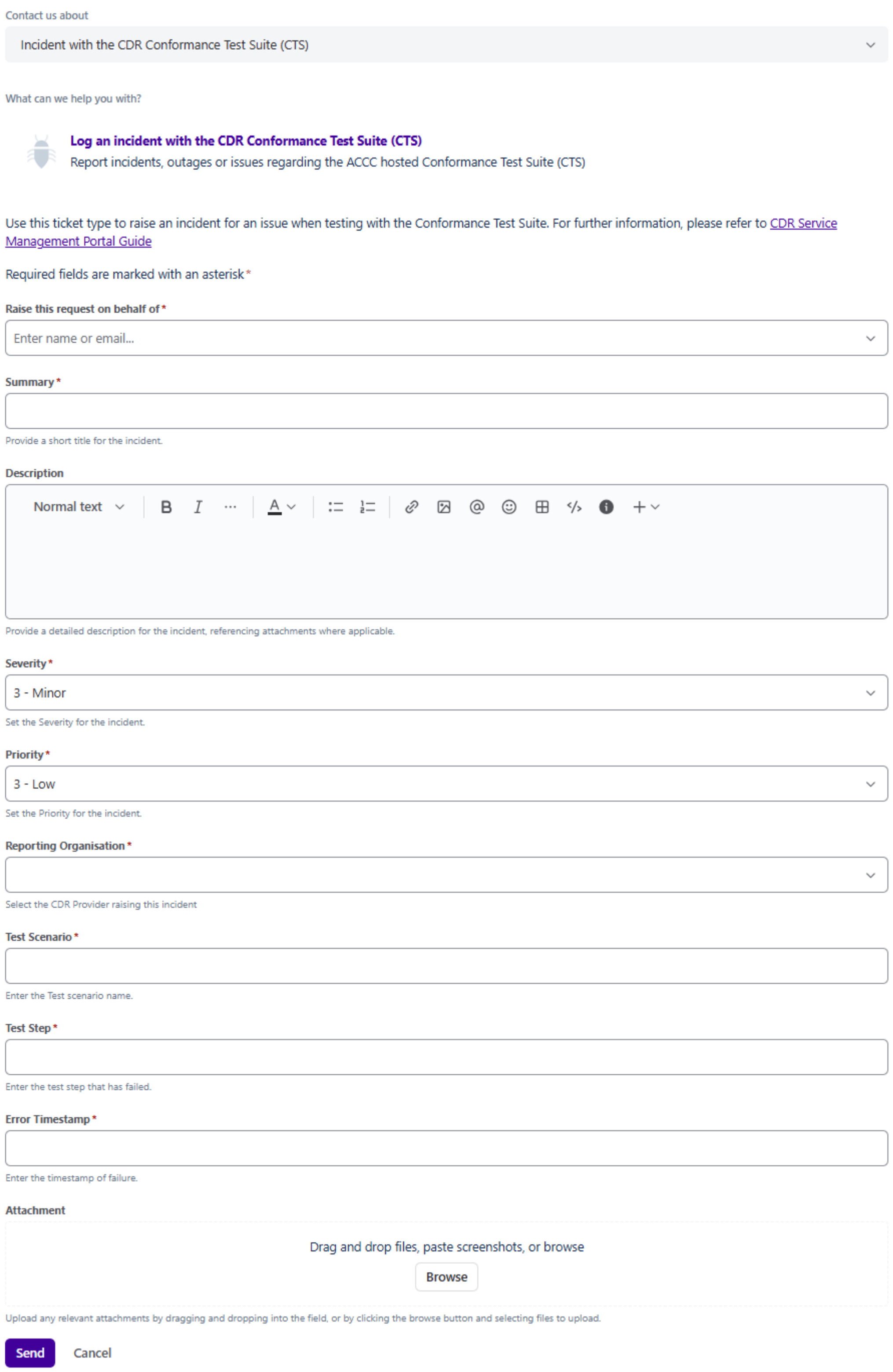
2.3 Types of incidents and requests

Below are some of the issues and services managed through the CDR SMP.

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 CTS
Incident with a CDR Provider	Used by a participant to raise a technical incident with a CDR participant, when the resolving party is another data holder or accredited data recipient
Incident with the CDR Register and Accreditation Application Platform (RAAP)	Used by participants to raise an incident with the CDR team when 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 Onboarding Assistance	Used by participants to raise requests or queries relating to the onboarding process, RAAP, CTS or CDR SMP Examples include specifying or updating participant configuration information and requesting information or access to RAAP, CTS or the CDR SMP

2.3.1 Incident with the CDR Conformance Test Suite (CTS)

After choosing this option, you will be presented with the following form.



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 *

Enter name or email...

Summary *

Provide a short title for the incident.

Description

Normal text

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

Test Scenario *

Enter the Test scenario name.

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

Browse

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

Send

Cancel

Filling out the form

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 in Section 1.3.)

Priority: Set the priority for the incident. (See guide in Section 1.3.)

Reporting Organisation: Select the CDR provider you are representing.

Test Scenario ID: Enter the test scenario ID.

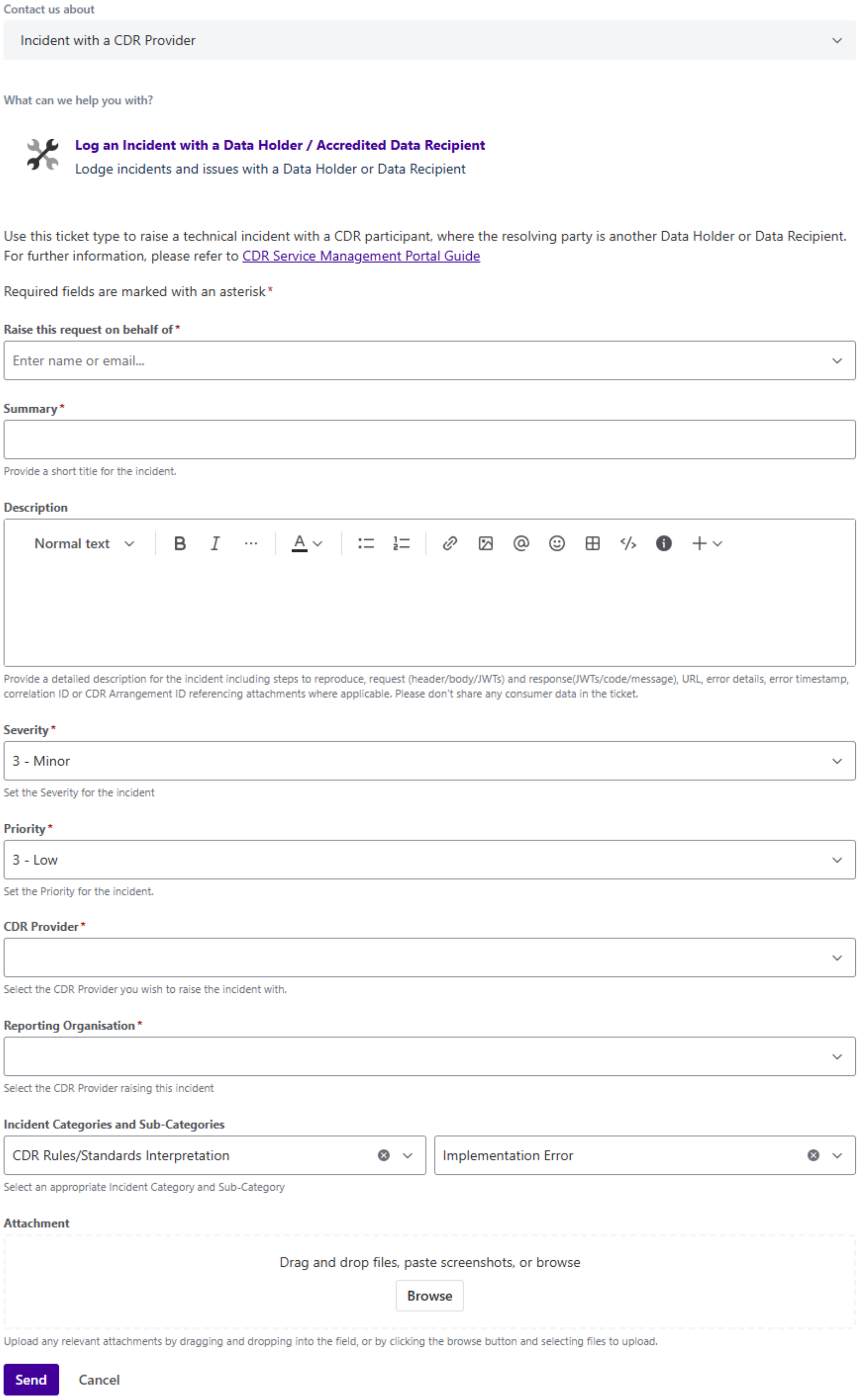
Test Step: Enter the test step that has failed.

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 include logs and screenshots.

2.3.2 Incident with a CDR Provider

After choosing this option, you will be presented with the following form.



Contact us about

Incident with a CDR Provider

What can we help you with?

Log an Incident with a Data Holder / Accredited Data Recipient

Lodge incidents and issues with a Data Holder or Data Recipient

Use this ticket type to raise a technical incident with a CDR participant, where the resolving party is another Data Holder or Data Recipient. For further information, please refer to CDR Service Management Portal Guide

Required fields are marked with an asterisk*

Raise this request on behalf of*

Enter name or email...

Summary*

Provide a short title for the incident.

Description

Normal text B I ··· A

Provide a detailed description for the incident including steps to reproduce, request (header/body/JWTs) and response(JWTs/code/message), URL, error details, error timestamp, correlation ID or CDR Arrangement ID referencing attachments where applicable. Please don't share any consumer data in the ticket.

Severity*

3 - Minor

Set the Severity for the incident

Priority*

3 - Low

Set the Priority for the incident.

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 Error

Select an appropriate Incident Category and Sub-Category

Attachment

Drag and drop files, paste screenshots, or browse

Browse

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

Send

Cancel

Filling out the form

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 in Section 1.3.)

Priority: Set the priority for the incident. (See guide in Section 1.3.)

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

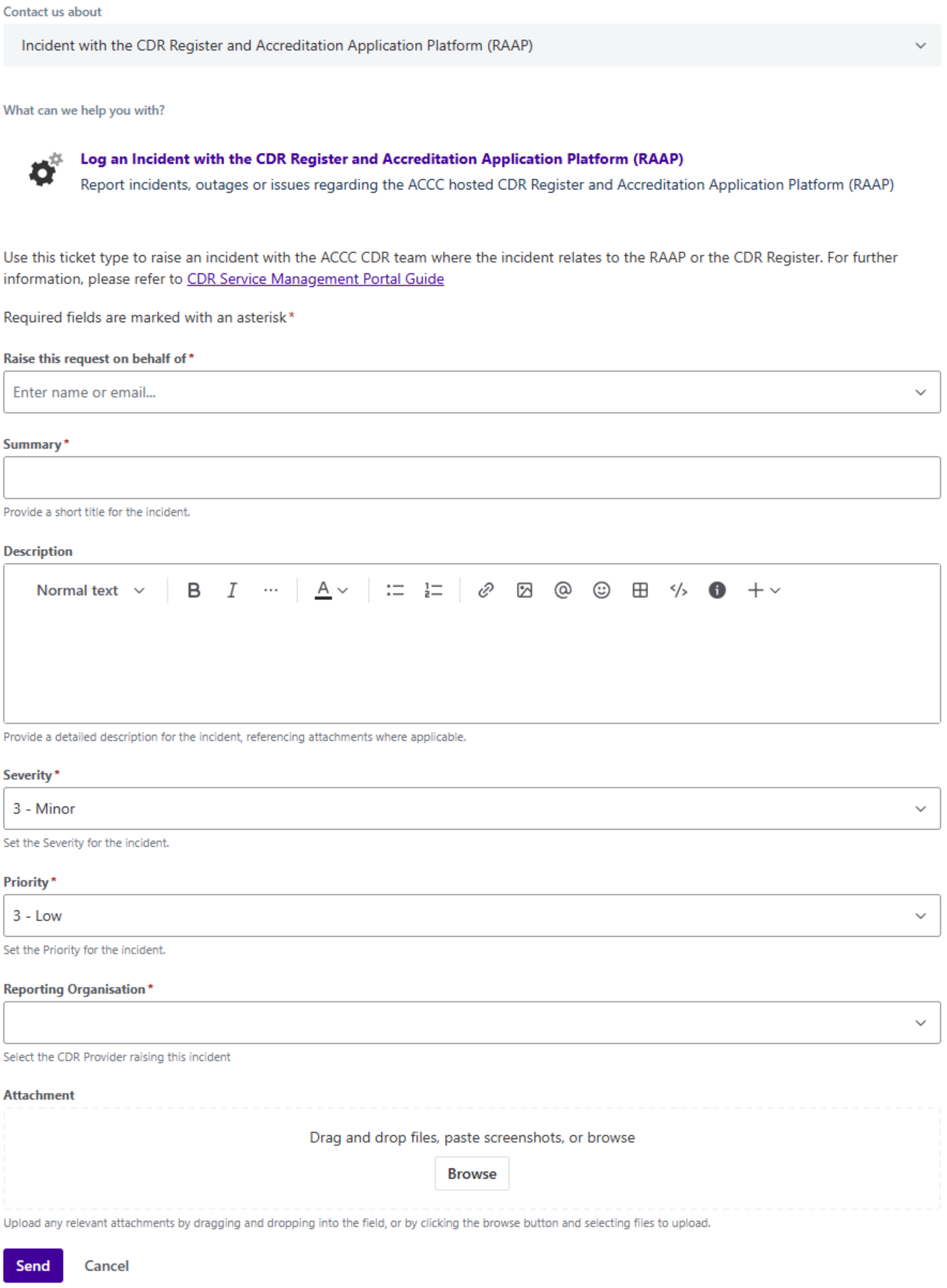
Reporting Organisation: Select the CDR provider you are representing.

Incident Categories and Sub-Categories: Choose the appropriate incident category and subcategory to categorise the issue. (See the guides in Section 1.4 and Section 1.5 for detailed definitions.) Note that 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.

2.3.3 Incident with the CDR Register and Accreditation Application Platform (RAAP)

After choosing this option, you will be presented with the following form.



Contact us about

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

What can we help you with?

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

Use this ticket type to raise an incident with the ACCC CDR team where the incident relates to the RAAP or the CDR Register. For further information, please refer to CDR Service Management Portal Guide

Required fields are marked with an asterisk*

Raise this request on behalf of*

Enter name or email...

Summary*

Provide a short title for the incident.

Description

Normal text

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

Browse

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

Send Cancel

Filling out the form

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 in Section 1.3.)

Priority: Set the priority for the incident. (See guide in Section 1.3.)

Reporting Organisation: Select the CDR provider 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.

2.3.4 Implementation Gaps & Rectification Schedule

This request type allows a data holder to notify the ACCC of any CDR implementation gaps. We expect data holders to promptly rectify any noncompliance. If they do not, they face possible enforcement 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 noncompliance with their obligations. We also expect participants to proactively notify us of updates to existing rectification schedule items. This includes 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 for 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 before submission.

The form to notify the ACCC of implementation gaps is presented in 2 sections. The first section describes the nature of the implementation gap(s) in the submission.

Contact us about

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.

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.

Required fields are marked with an asterisk*

Raise this request on behalf of*

Enter name or email...

Summary*

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

Issue Description

Normal text B I ··· A

Implementation Gap	Proposed Resolution Date	Additional Details

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

Filling out the form

Summary: Provide a short title for your request.

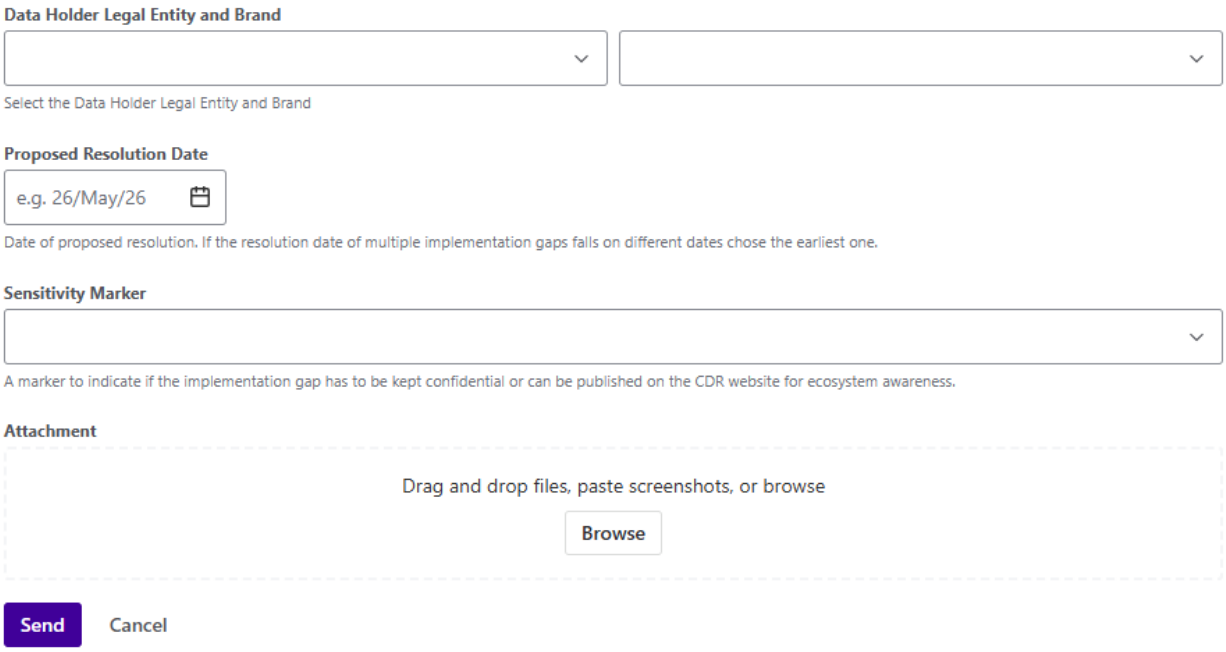
Issue Description: Fill in the table included; add more rows if required. Provide a detailed description for your request, referencing attachments where applicable.

In detail:

- Provide a description of the implementation gap in column 1.
- Include a proposed resolution date in column 2. Use the dd/mm/yy date format.
- Optionally, provide additional details in column 3.

Ensure that the description is clear enough to let third parties, such as accredited data recipients, understand the impact of the disclosed implementation gap.

The second section of the form allows the identification of the data holder brand and the sensitivity marker.



Filling out the form

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

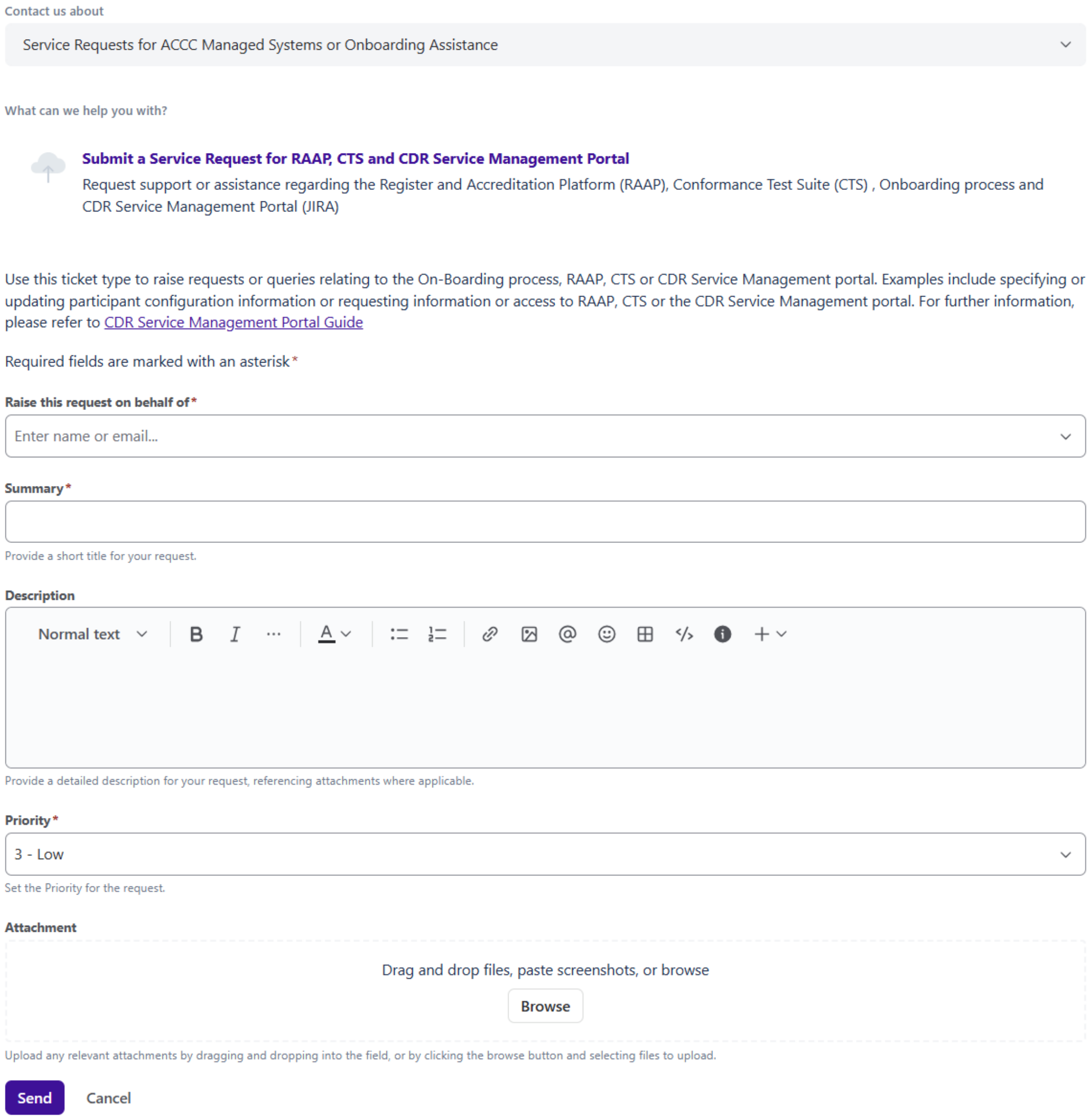
Proposed Resolution Date: Select the earliest date if multiple gaps are being declared.

Sensitivity Marker: Indicate if the material in columns 1 and 2 is suitable for publication or confidential. Material in column 3 will not be published. If you consider that information entered in column 1 or 2 is not suitable for publication, email accc-cdr@accc.gov.au for further guidance.

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

2.3.5 Service Requests for ACCC Managed Systems or Onboarding Assistance

A service request can ask a CDR team to perform an action on behalf of an organisation that you are associated with. Examples of actions include updating endpoints and user management.



Filling out the form

Summary: Provide a short title for your request.

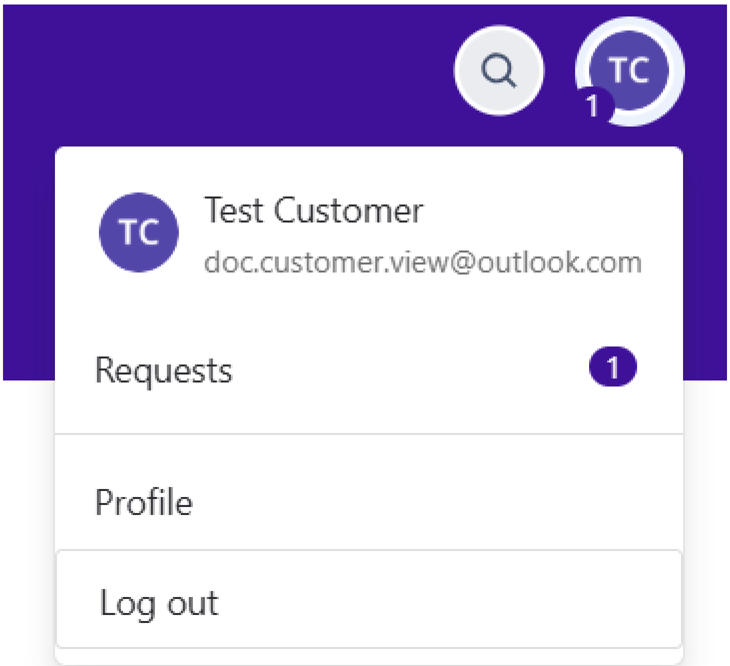
Description: Provide a clear and detailed description for your request, referencing attachments where applicable.

Priority: Set the priority for the request. (See Section 1.3.)

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

2.4 Tracking requests

Users can track requests by logging in to the CDR Service Management Portal as a customer and clicking on the **Requests** button in the top-right corner of the window.



Fields in this menu

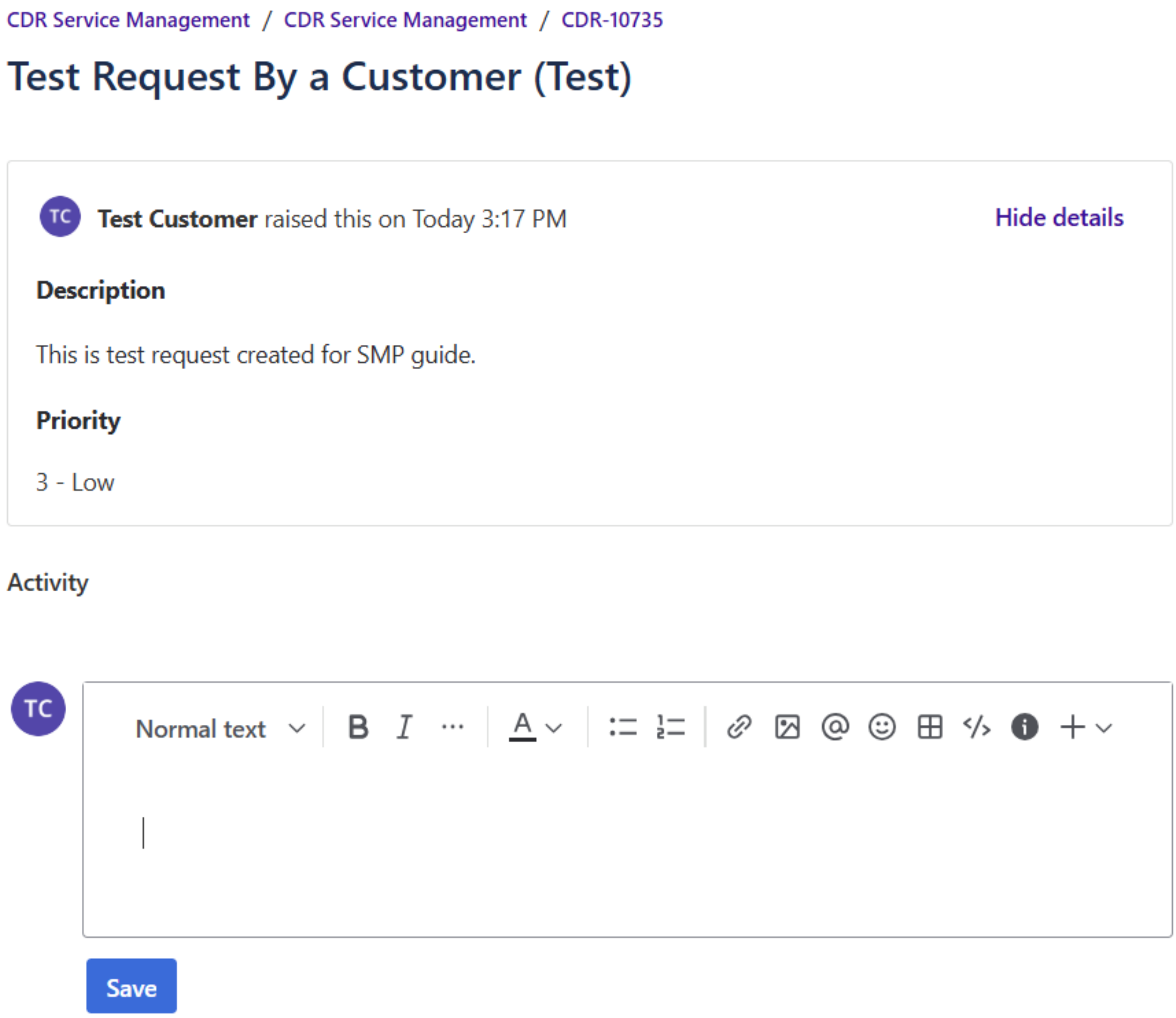
Requests: View incidents/requests created by you or shared with you.

Profile: Shows your profile from where you can manage your account and edit account preferences.

Log Out: Logs you out from your Atlassian account.

2.5 Updating or commenting on requests

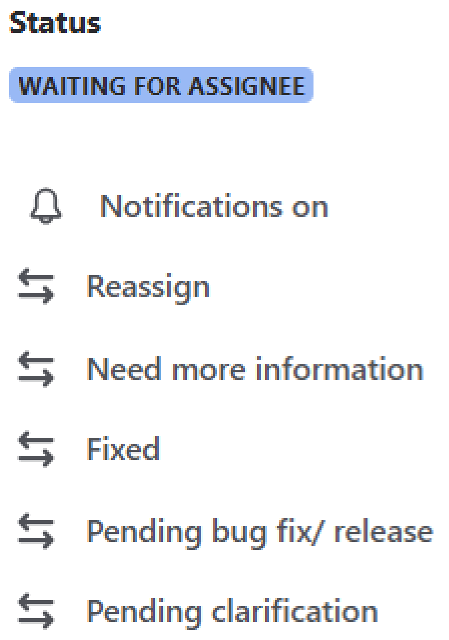
In your **Requests** view, users can select a request and add comments or updates.



> **Filling out the form**
>
> Add your comments by clicking in the comments field and typing.
>
> Click **Save** to submit your comment or update.

2.6 Progressing through workflows

After an incident has been submitted, users can progress the incident through the various workflow states.



Filling out the form

When you click on any of the states, you will be prompted to enter extra information.

Notifications on: Click this option if you want to turn notifications on or off.

Reassign: Enter additional information, then click **Reassign**. This will reassign the ticket back to the current assignee.

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

Fixed: Enter the required information and click **Fixed** if issue has been resolved.

Pending bug-fix/release: Enter the details and click **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 and Standards clarification. It will set the status to **Pending Clarification**.

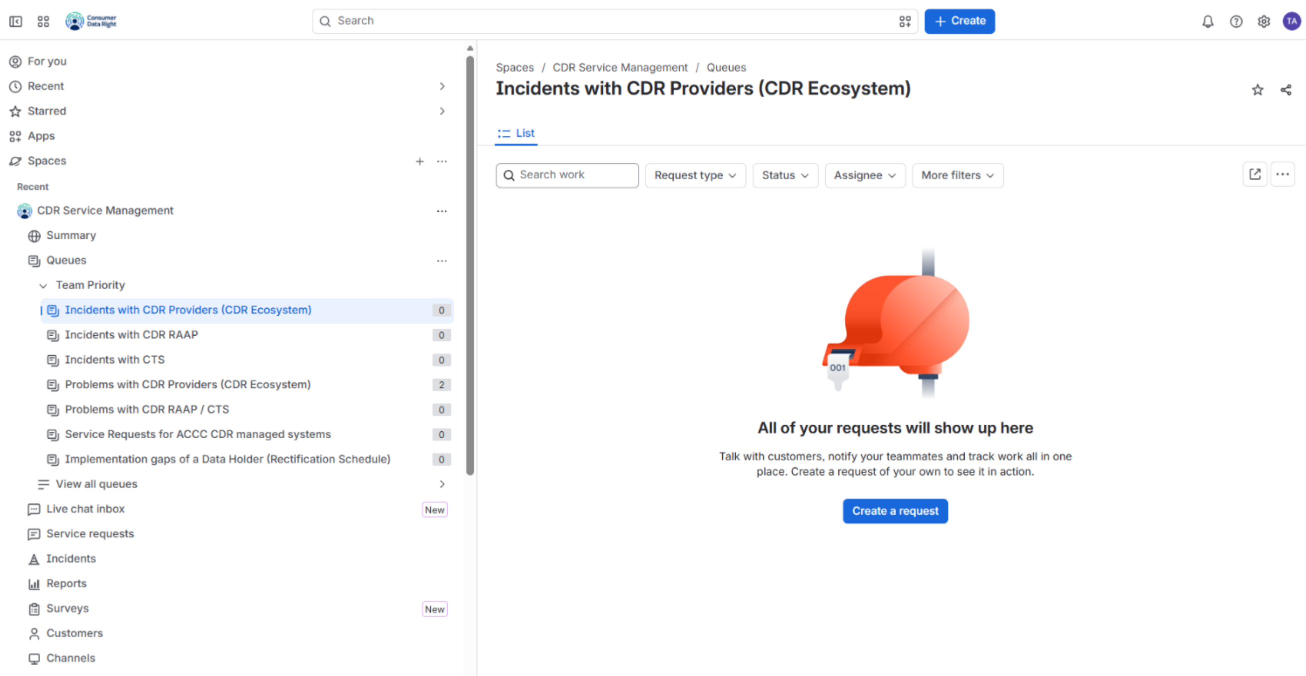
3. CDR Service Management Portal: agent view

3.1 Agent role

An agent can access queues and raise and process incidents and service requests. That is, they can move incidents through workflows, reassign incidents to other teams and make customer-facing comments. When an agent logs in to cdrservicemanagement.atlassian.net, they will see the project view as shown below.

An agent can navigate between existing incidents and service requests from the left-hand panel. They can create new incidents and service requests from the top menu bar.

As an agent, you will only see incidents and service requests that are assigned to you and/or reported by you.



Navigating the page

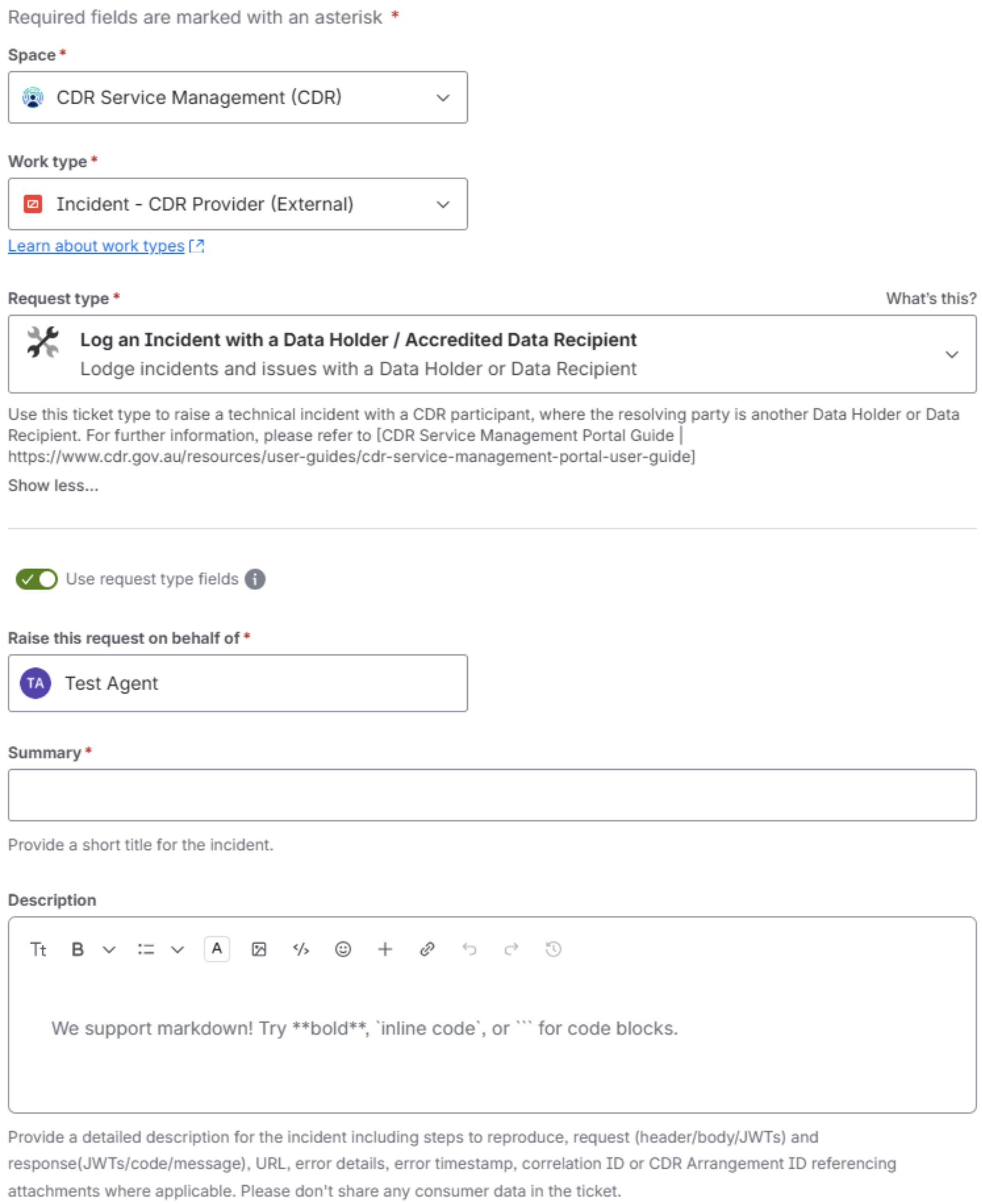
Click the **Create** button (top menu) to create a new incident or request.

Select **Queue** (left menu) to navigate between service requests and incidents within your configured queues.

When **Queue** is selected, a list of queues is provided. The queue for participants is ‘Incidents with CDR Providers (CDR Ecosystem)’. All other queues are for internal ACCC use.

3.2 Creating incidents and service requests

Fill out the **Create issue** form. It is shown here in 2 parts, corresponding to the upper and lower halves of the screen.



Filling out the form (Part 1)

Space: This is set to CDR Service Management by default.

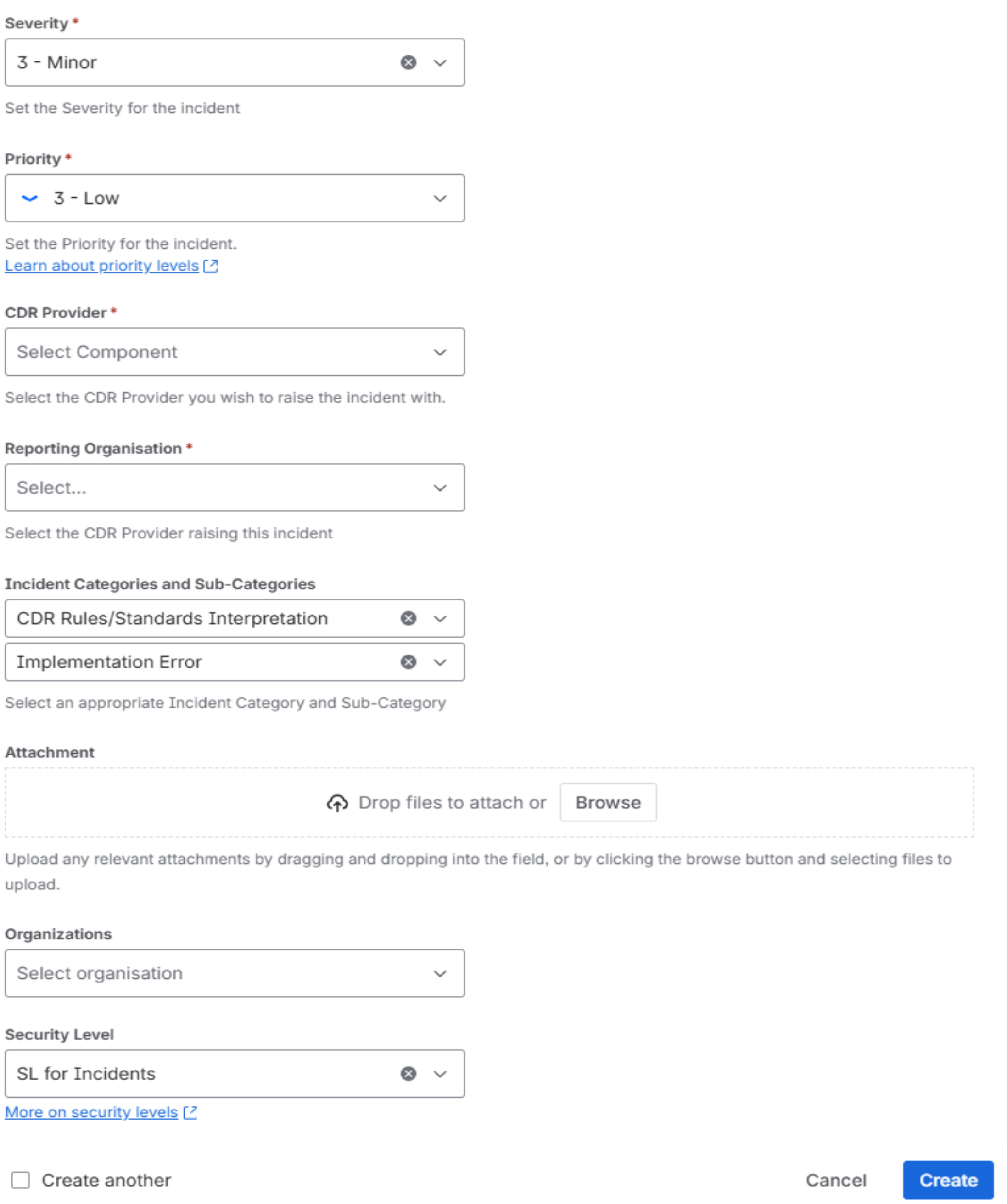
Request type: Select the incident or service request type.

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.

The second part of the form allows extra information to be added.


Severity *
3 - Minor
Set the Severity for the incident
Priority *
3 - Low
Set the Priority for the incident.
Learn about priority levels
CDR Provider *
Select Component
Select the CDR Provider you wish to raise the incident with.
Reporting Organisation *
Select...
Select the CDR Provider raising this incident
Incident Categories and Sub-Categories
CDR Rules/Standards Interpretation
Implementation Error
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 organisation
Security Level
SL for Incidents
More on security levels
Create another
Cancel
Create

Filling out the form (Part 2)

Severity: Set the severity for the request. (See guide in Section 1.3.)

Priority: Set the priority for the request. (See guide in Section 1.3).

CDR Provider: Select the CDR provider you are reporting the incident to using the drop-down list.

Reporting Organisation: Select the CDR provider you are representing.

Incident Categories and Sub-Categories: Choose the appropriate incident category and subcategory to categorise the issue. (See the guides in Section 1.4 and Section 1.5 for detailed definitions.) Note that 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.

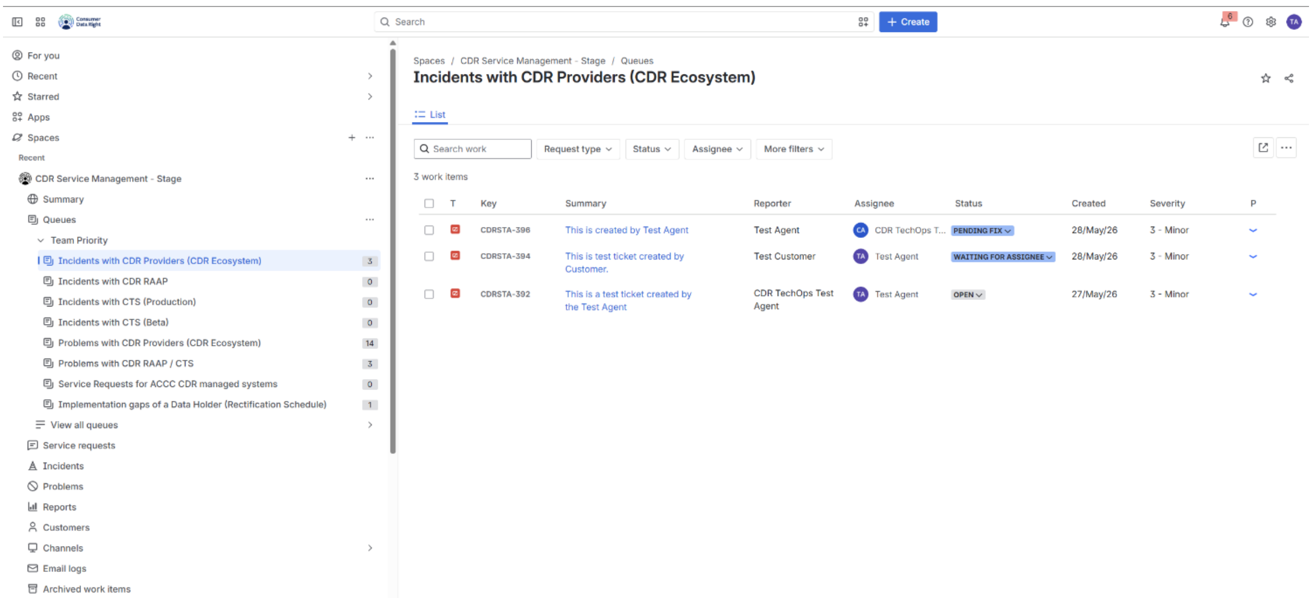
Security Level (no action needed): This is reset by the system after the record is created.

3.3 Managing incidents

On navigation to the service request or incident view, users can manage tickets by clicking on the relevant ticket in the view.

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

Incidents raised with a CDR provider can only be viewed by the ACCC, the reporter and the assignee in the queue. An incident that is shared with other users and/or organisations will be viewable by those users when they are acting as a customer.

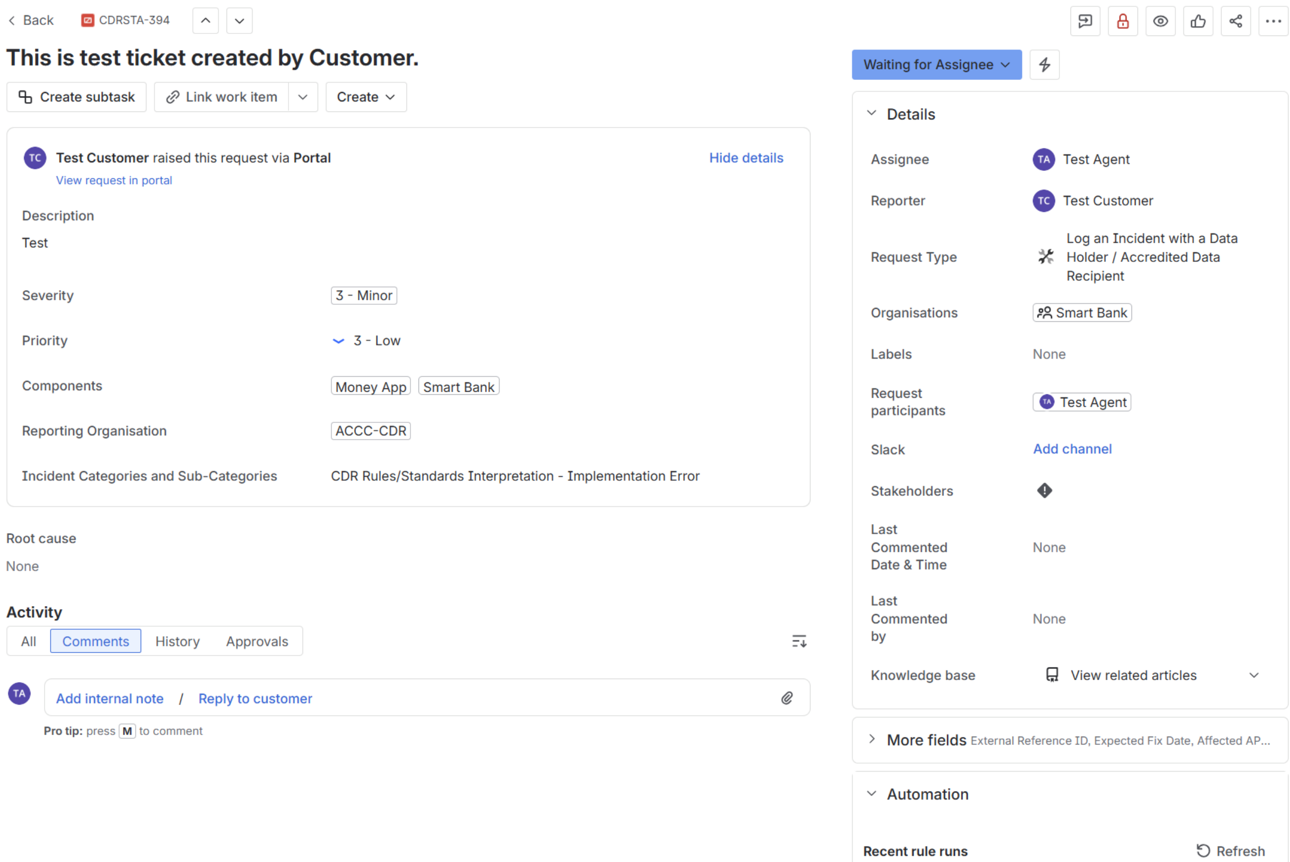


Navigating the page

Click the title of the ticket in the **Summary** column to open and edit it.

3.4 Incident view

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



Note

Internal notes are visible only to the reporter and assignee. To share comments with users who have access to the ticket, select 'Reply to customer' instead of adding an internal note.

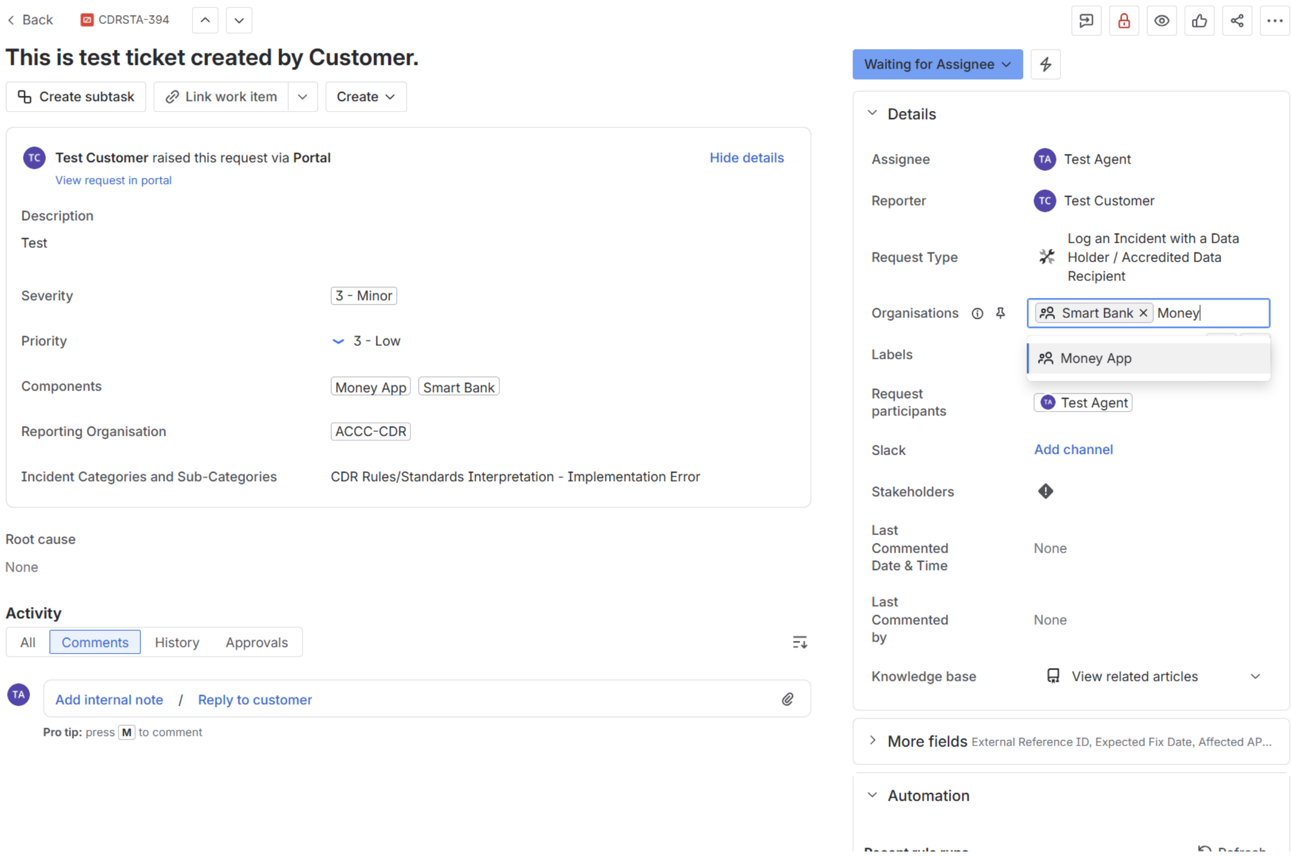
Incidents raised with a CDR provider can only be viewed by the ACCC, the reporter and the assignee in the queue. Incidents shared with other users and/or organisations are shown in the customer view.

3.5 Sharing 'incident with a CDR provider' with another CDR provider

After you have opened the incident with a CDR provider, you can share it with another user or organisation.

> **Note**
>
> A problem with a CDR provider can be viewed by ***all*** agent users in the CDR SMP, including agent users from organisations other than your own.

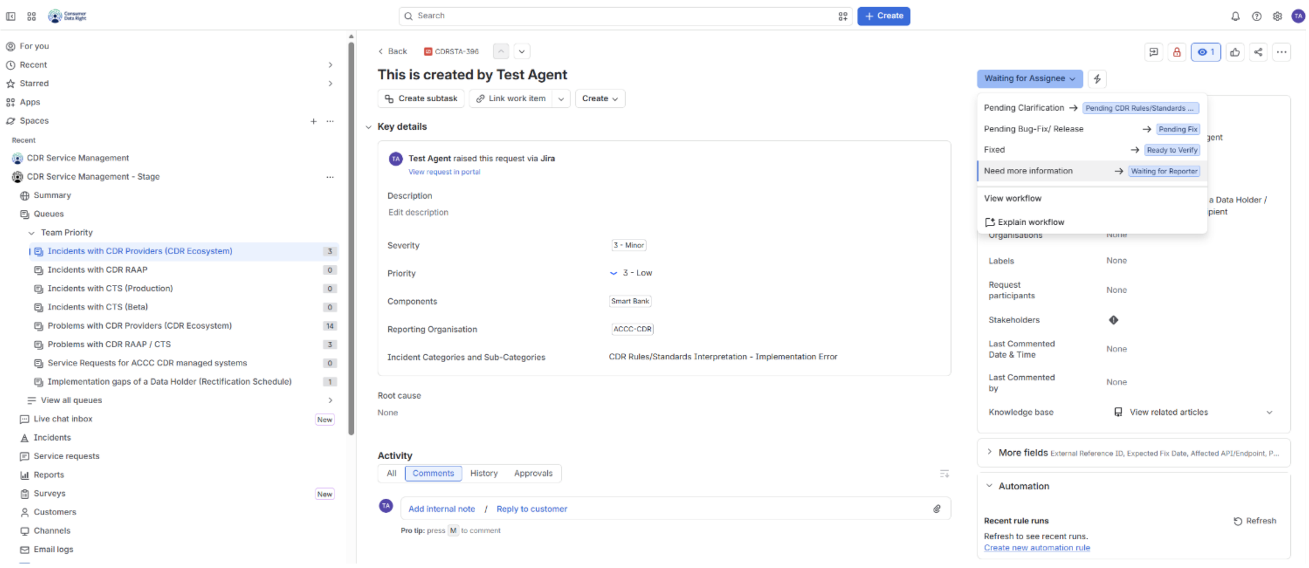
If you reassign an incident to another user, you will no longer have agent access to the ticket. However, you can continue to view and comment on the ticket as a customer if it is shared with you or your organisation.



> **Navigating the page**
>
> Choose the user with whom the incident is to be shared. Do this using the **Request participants** field on the right-hand pane.
>
> Choose the organisation with which the incident is to be shared. Do this using the **Organisations** field on the right-hand pane.

3.6 Moving through workflows

When viewing an incident, users can click on the incident status (for example, ‘open’, ‘pending fix’, ‘resolved’) for a given incident to go to the next state in the workflow. For example, in the image above, on the right the incident status is set to the green ‘resolved’ state. In the image below, it is in the blue ‘waiting for assignee’ state.



Progressing the incident

Click the incident status button to see the next states in the workflow. In this example, the status of the incident is ‘waiting for assignee’.

Then select the relevant state to progress the ticket.

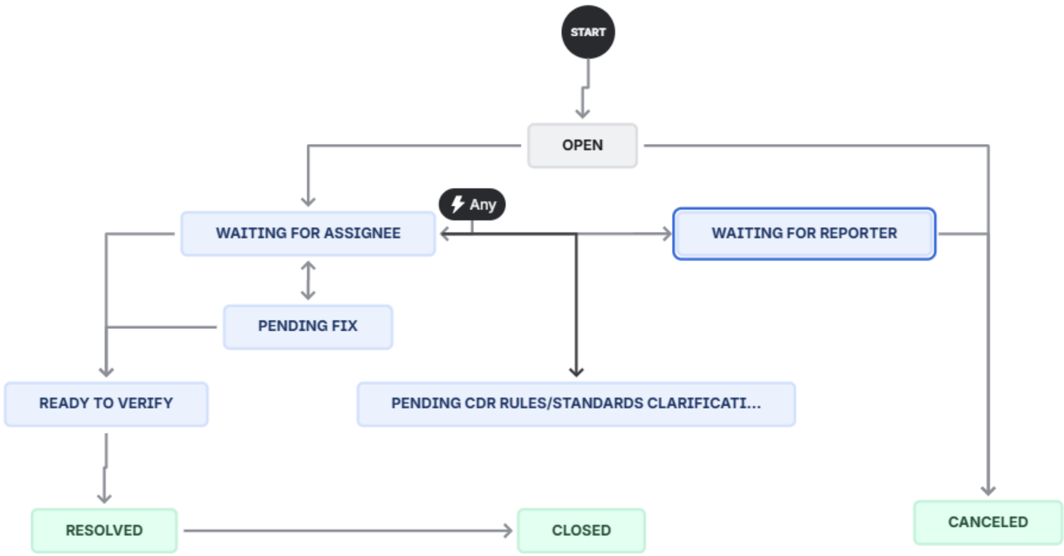
if you are waiting for more information from the incident reporter, users should change the status from ‘waiting for assignee’ to ‘waiting for reporter’.

Section 3.7 shows an example of the workflow for progressing an incident.

3.7 Incident lifecycle management for CDR provider

Note

It is very important for the participants to adhere to the incident life cycle management process, which is shown here.



Stages in this lifecycle:

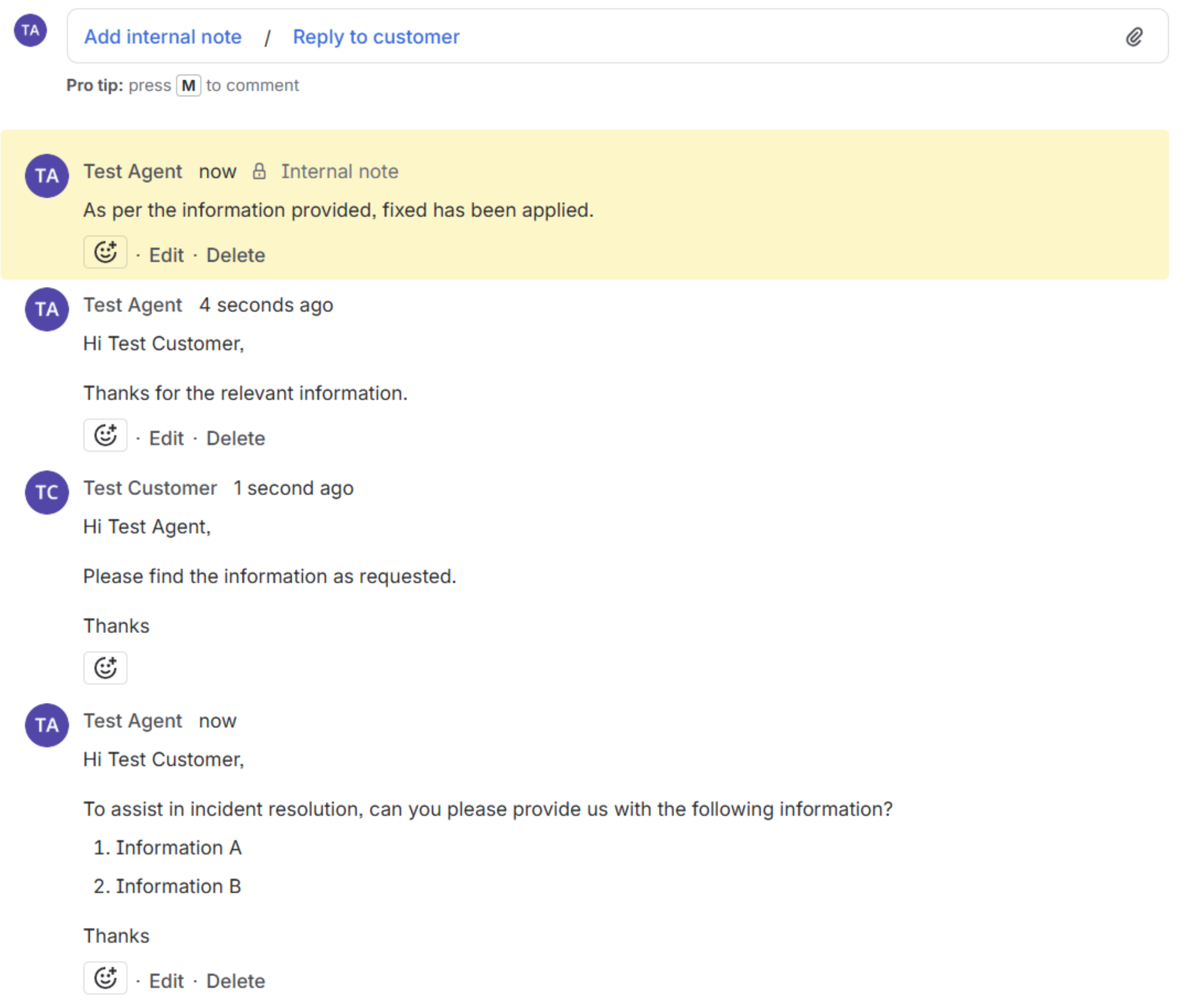
- **Open:** The incident will be in an ‘open’ state when it has been raised by the participant.
- **Waiting for assignee:** The incident is awaiting assessment by the assigned participant. The assignee should review the incident and move it to the appropriate next status.
- **Waiting for reporter:** The ticket is waiting for the incident reporter to provide input.
- **Pending fix:** The incident has been investigated, and a resolution has been identified. The assignee is implementing, testing, or scheduling the fix
- **Ready to verify:** The assignee sets the status to 'Ready to verify' once they have implemented the fix, asking the participant who raised the incident to verify it
- **Pending CDR Rules / Standard clarification:** The incident cannot progress until clarification is received regarding the interpretation or application of the CDR Rules or Consumer Data Standards.
- **Resolved:** The reporter or affected participant has verified the incident is resolved and can change the state to ‘resolved’ if no further action is required. The state must be set to ‘assigned’ if the incident is not resolved on verification.
- **Closed:** The incident has been resolved, verification has been completed, and no further action is required. The CDR Technical Operations team will review the incident and close the ticket.
- **Cancelled:** The incident is no longer required to be progressed. On mutual agreement between the reporter and the assignee, the incident can be changed to ‘cancelled’ by the participant who raised the ticket.

3.8 Internal and customer-facing comments

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

Add internal note is viewable only by other agents assigned to the ticket (reporter and assignee) and is not visible in the customer view (see Section 1.2).

Reply to customer Reply to customer comments are visible to all users who have access to the ticket, including shared users and assigned agents, this option is recommended for maximum visibility of updates.



Navigating the page

Click on the **Reply to customer** hyperlink. This will allow you to add and save a comment. Note you can press the **M** key to comment.

You can also edit and delete your notes and comments if you have made a mistake.

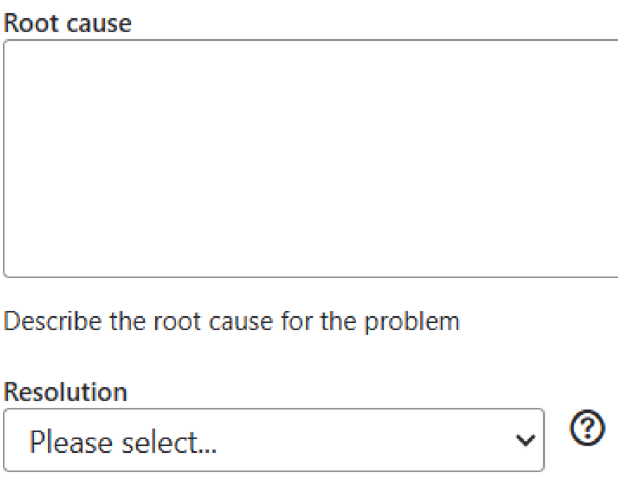
Then select the relevant state to progress the ticket.

3.9 Fixing and verifying incidents

An incident can be moved to 'Ready to Verify' (see the lifecycle flow chart in Section 3.7) once the resolving participant has investigated the issue, deployed a fix, and requested that the affected participant verify the resolution. When transitioning the incident to this status, the resolving participant should also provide details of the root cause and the implemented fix.

Note

It is very important for the participants to progress the incident to the ‘ready to verify’ state as soon as the fix has been deployed to ensure verification is completed promptly.

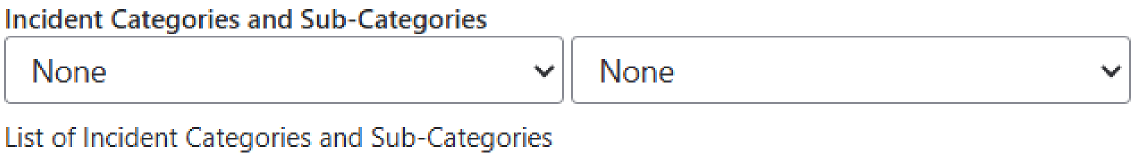


Navigating the page

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

Resolution: Select the relevant resolution from the drop-down box.

Next, provide some information about the incident categories.



> **Navigating the page**
>
> **Incident Categories and Sub-Categories:** Choose the appropriate incident category and subcategory. (See the guides in Section 1.4 and Section 1.5 for detailed definitions.)
>
> This field is mandatory when incident status is changed from ‘fixed’ to ‘ready to verify’.

Last, indicate the affected API. After that is selected, a drop-down containing relevant endpoints becomes available.

> **Navigating the page**
>
> **Affected API/Endpoint:** Select the primary affected API and endpoint for the issue.

3.10 Resolving and closing incidents

An incident can be transitioned to ‘resolved’ when the affected participant confirms the incident is fixed.

The incident may be marked ‘closed’ by the CDR Technical Operations team when all affected participants agree the incident has been resolved and all outstanding actions have been completed.

Background and more information

More information on the topics covered in this user guide is available in the following resources.

- CDR Service Management Portal user guide supplement for energy data holders
- CDR compliance and enforcement policy (ACCC and Office of the Australian Information Commissioner)
- ACCC/AER information policy (ACCC and Australian Energy Regulator)

CDR provides consumers with greater control over their data. It gives consumers the power to require a data holder to safely share their data with a service provider, so they can get better deals and services.

The key compliance requirements of CDR are established by:

- Part IVD of the *Competition and Consumer Act 2010*
- the Competition and Consumer (Consumer Data Right) Rules 2020
- the Consumer Data Standards.

The CDR information map is a topic-based listing of CDR information published by the Australian Competition and Consumer Commission (ACCC), the Australian Office of the Information Commissioner (OAIC), Treasury and the Data Standards Body (DSB). A glossary of CDR terms can be found on the CDR website.

The CDR Support Portal includes guidance on commonly queried CDR topics. It can also be used to submit questions about the CDR Rules and Standards for CDR agencies to respond to directly.

The ACCC and DSB facilitate the CDR implementation call. It provides a forum for participants and other stakeholders to ask questions about their obligations and receive updates on the CDR system.

Further contact

For questions about using the SMP, please contact the ACCC's CDR Technical Operations team via email to cdrtechnicaloperations@accc.gov.au.