EUROPEAN UNION AGENCY
FOR CYBERSECURITY

CRA Single Reporting Platform – AR User Manual

SEPTEMBER 2026

Document History

Date	Version	Modification
09/09/2026	v1.0	First version

Table of Contents

List of Tables

SECTION 1

Introduction

1. Introduction

1.1 Purpose of the AR User Manual

The Cyber Resilience Act (CRA) Single Reporting Platform (SRP) is an online tool developed and operated by ENISA to support the reporting of actively exploited vulnerabilities (AEVs) and severe incidents (SIs) having an impact on the security of products with digital elements. Designed to simplify EU reporting obligations, the SRP enables relevant notifications to be submitted through a single platform and communicated to the relevant authorities.

This user manual provides practical guidance for Assigned Representatives (ARs) of manufacturers and, once applicable, open-source software stewards on how to access the platform, navigate the interface, complete forms, and perform the main workflows required for registration, notification submission, notification updates, manufacturer and AR association management, viewing of reminders and alerts and dashboard monitoring. The manual is intended to help users understand what actions they can perform through the platform and how to complete them correctly, using step-by-step scenarios and screenshots. It focuses on the user-visible functionalities and operational workflows available to ARs through the platform interface.

1.2 Scope of the Platform

The SRP is the online reporting platform established under the CRA to support manufacturers in fulfilling their mandatory reporting obligations for AEVs and SIs having an impact on the security of products with digital elements. The corresponding reporting obligations for open-source software stewards apply once Article 24(3) of the CRA becomes applicable.

From 11 September 2026, the SRP supports mandatory notifications by manufacturers under Article 14 of the CRA. **Voluntary reporting under Article 15 is not available in the initial release of the platform and will be introduced in a future phase.**

Through the SRP, an AR submits a notification to the relevant CSIRT designated as coordinator (CDaC). Once submitted, the notification is simultaneously made available to ENISA, while the designated CSIRT is responsible for disseminating the information to other relevant CSIRTs in Member States where the affected product is also available, subject to the applicable CRA provisions.

The initial implementation of the SRP delivers the core functionalities required for mandatory reporting. The platform is designed to facilitate coordination among relevant stakeholders while ensuring compliance with regulatory requirements and alignment with operational needs. ENISA will continue to maintain and enhance the platform and its functionalities as necessary following launch.

The SRP is operational from 11 September 2026, when the CRA reporting obligations for manufacturers under Article 14 become applicable.

The SRP is available at: https://portal.cra-srp.enisa.europa.eu.

1.3 Target Audience

This user manual is intended for Assigned Representatives (ARs) acting on behalf of manufacturers and, once applicable, open-source software stewards who access the platform to submit, review, and update notifications, manage manufacturer and AR associations, and conduct other user-administration activities available to their role.

For the purposes of the SRP, an AR is the individual who submits notifications on behalf of a manufacturer or, once applicable, an open-source software steward. Different platform functionalities are available depending on whether the user acts as a Primary AR or Secondary AR.

1.4 How to Use the Manual

This manual is designed to guide ARs through the relevant platform procedures step-by-step. It first introduces the SRP and its scope, then explains registration and access, login and logout, AR role-specific scenarios, notification workflows, common platform functionalities, and Frequently Asked Questions (FAQs).

The manual is organized as follow:

- Section 2 explains the registration process for ARs, including registration as a Primary AR and invitation-based registration as a Secondary (Backup) AR. It also explains how a Primary AR can invite a Secondary AR to become associated with a manufacturer.
- Section 3 describes login and logout procedures.
- Section 4 provides step-by-step guidance for AR scenarios, including profile and manufacturer management, AR association management, dashboard use, notification submission, and notification updates.
- Section 5 presents other functionalities available on the platform, including reminders and alerts.
- Section 6 provides FAQs addressing common issues related to platform access, AR roles, notification submission, validation, and notification statuses.

1.5 Acronyms and Definitions

Table 1 – Acronyms

Acronym	Meaning
72hrs	72-hour Notification as per Art. 14.2(b) and 14.4(b) of the CRA
AEV	Actively Exploited Vulnerability
AR	Assigned Representative
CC	Concerned CSIRT
CDaC	CSIRT Designated as a Coordinator
CRA	Cyber Resilience Act
CRG	Cybersecurity-Related Grounds

Acronym	Meaning
CSIRT	Computer Security Incident Response Team
ENISA	European Union Agency for Cybersecurity
EW	Early Warning as per Art. 14.2(a) and 14.4(a) of the CRA
FR	Final Report as per Art. 14.2(c) and 14.4(c) of the CRA
IdP	Identity Provider
PEC	Particular Exceptional Circumstances
SI	Severe Incident
SRP	Single Reporting Platform

Table 2 – Definitions

Term	Definition
72-hour Notification	Follow-up notification submitted within the applicable 72-hour timeframe after an Early Warning.
Actively Exploited Vulnerability	A vulnerability that is being actively exploited and may require notification through the SRP.
Assigned Representative	User acting on behalf of a manufacturer or open-source software steward in the SRP.
Secondary (Backup) AR	Assigned Representative invited by a Primary AR to support submission and handling of notification for the manufacturer and able to request elevation to Primary AR.
Concerned CSIRT	CSIRT that may receive access to disseminated notification information, where applicable.
CSIRT Designated as a Coordinator (CDaC)	Designated CSIRT responsible for reviewing a notification or manufacturer association and coordinating related dissemination actions.
Cybersecurity-Related Grounds	Grounds used by a CDaC to support controlled dissemination of full or partial information as per Art. 16.2 of the CRA and Delegated Act.
Early Warning	Initial notification submitted by an AR for an actively exploited vulnerability or severe incident.
Final Report	Final report submitted by the AR to complete the reporting sequence.

Term	Definition
Particular Exceptional Circumstances	Circumstances that may justify delaying dissemination, subject to justification and CSIRT decision.
Primary AR	Main Assigned Representative for the manufacturer in the SRP, who can manage the manufacturer association, invite or remove Secondary ARs, submit, review and update notifications, and perform other administrative functions available to that role.
Secondary AR	Secondary (or backup) Assigned Representative, who can submit, view and update notifications for the manufacturer and claim the Primary AR role – subject to review and approval by the designated CSIRT, but does not have the same administrative permissions as the Primary AR.
Severe Incident	Cybersecurity incident that may require notification through the SRP.
Single Reporting Platform (SRP)	Centralised online platform supporting CRA notification workflows for AR, CSIRT, and ENISA users.
SRP Website/Portal	https://portal.cra-srp.enisa.europa.eu

CRA SRP Glossary

Please refer to the SRP Glossary for a detailed explanation of SRP data fields, completion instructions, examples, expected formats, timeline, and applicability: https://www.enisa.europa.eu/cra-srp-glossary

SECTION 2

AR User Registration

2. User Registration (AR)

This section explains how Assigned Representatives register on the SRP, either as a Primary AR through the standard registration flow or as a Secondary (Backup) AR through an invitation sent by a Primary AR.

General notes

- AR users authenticate through **EU Login** when registering on the SRP. Authentication steps carried out within EU Login are not described in this manual. Further information on EU Login is available through the official EU Login guidance at: https://trusted-digital-identity.europa.eu/index_en.

EU login

An EU Login account with multi-factor authentication (MFA) is needed in order to access the platform.

ARs that have already an EU Login account with no MFA enabled should enable MFA before their first access to the platform.

- Validation by the CSIRT Designated as Coordinator (CDaC) of whether an AR is authorised to submit notifications on behalf of a specific manufacturer takes place after registration and is not a prerequisite for submitting a notification. Validation takes place in parallel with the reporting process. Specific validation procedures may vary between CSIRTs and remain the responsibility of the relevant CSIRT.
- Manufacturers and open-source stewards are advised to register and initiate the validation process only when they need to submit a specific notification, rather than registering pre-emptively.

2.1 Register as a Primary AR and associate with a manufacturer

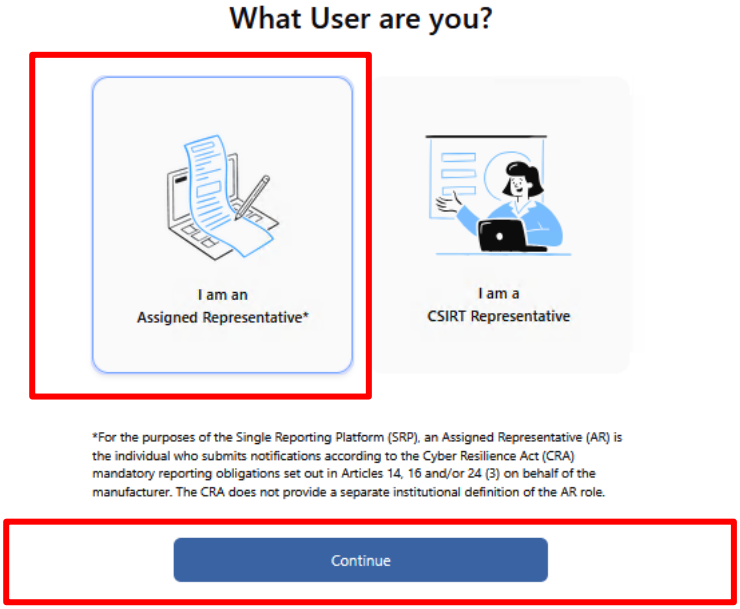
Purpose: Follow this procedure to register on the SRP as a Primary Assigned Representative (Primary AR) and create an association with a manufacturer.

Pre-conditions:

- You are not yet registered as an SRP user.
- You have an active EU Login account with MFA enabled.

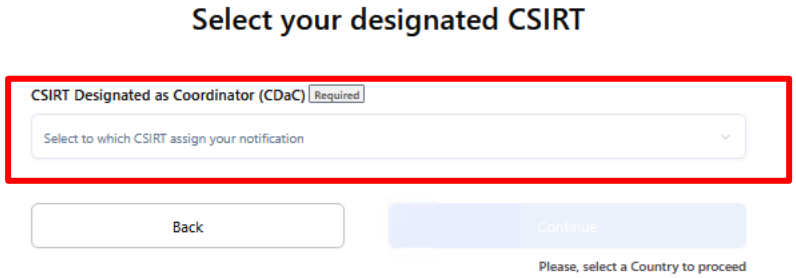
Steps:

1. **Open the SRP website**, select the AR role, and click “Continue”.



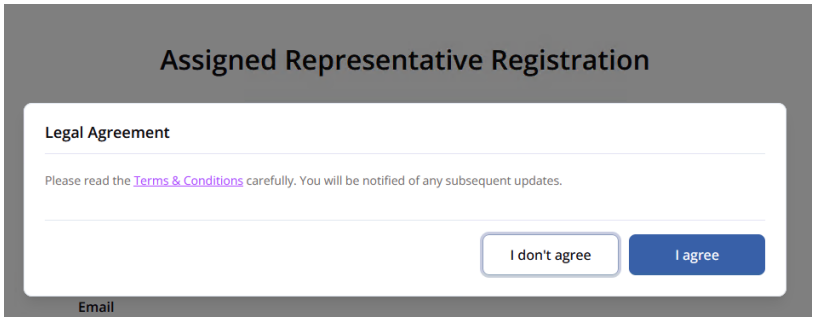
2. **Select the CSIRT Designated as Coordinator (CDaC)** from the drop-down menu and click "Continue".

Note: The manufacturer is responsible for identifying the correct CDaC in accordance with Article 14(7) of the CRA.



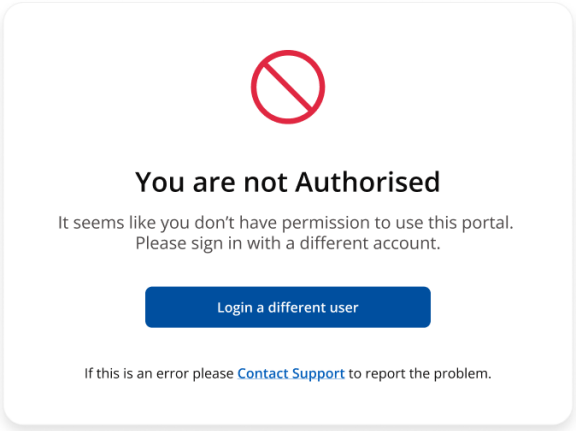
3. **Authenticate through EU Login**.

4. **Read and accept the legal agreement.**

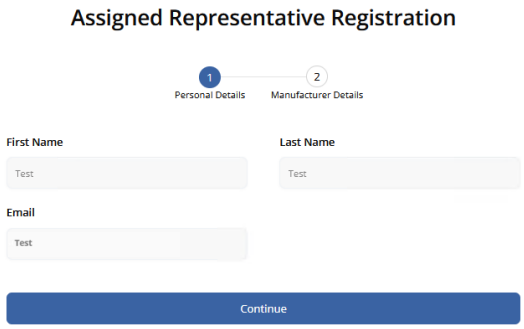


Exceptions and error handling:

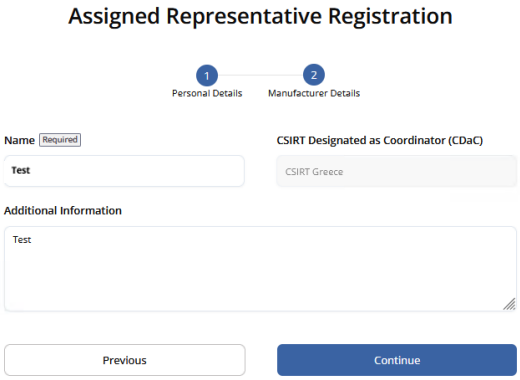
- If authentication fails, the SRP redirects you to a "**Not Authorised**" page.

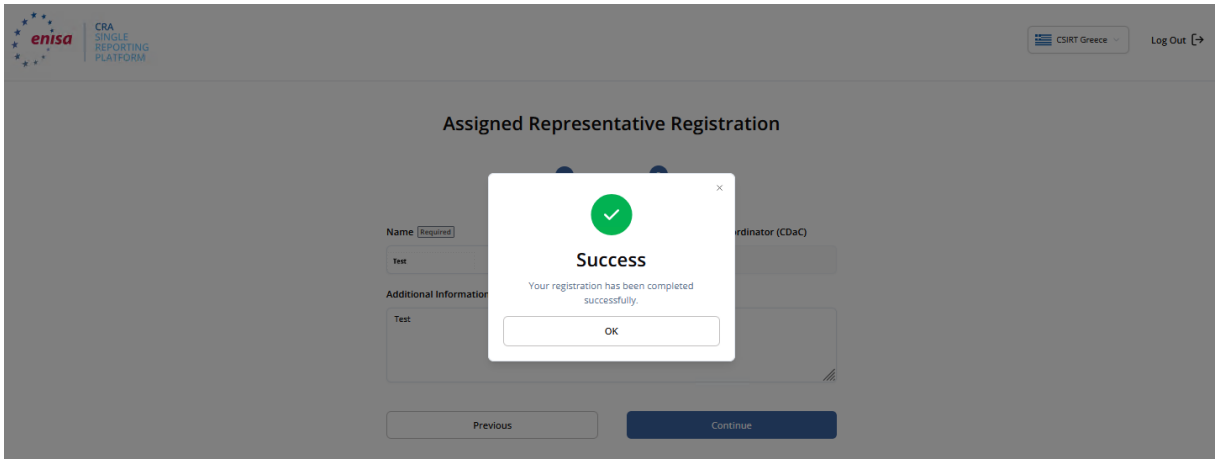


5. **Review and confirm the accuracy of your pre-filled personal details**, including First Name, Last Name, Email, then click "Continue". These fields are retrieved from EU Login and cannot be edited in the SRP.



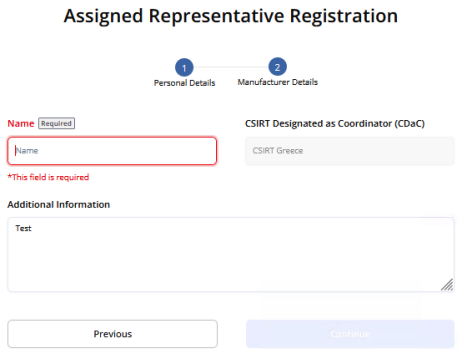
6. **Enter the manufacturer details**, including Manufacturer Name and Additional Information (optional), then click "Continue".





Exceptions and error handling:

- If required manufacturer information is missing, such as Manufacturer Name, the SRP displays an error and the “Continue” button remains disabled.



Expected result and system outcome: Registration is completed and the user account becomes “Active” with the “AR Primary User” role. The manufacturer entity is created in the SRP based on the information provided, and the AR-manufacturer association is submitted for validation by the CSIRT. The system sends a confirmation email to the user.

The AR may start submitting notifications while validation of the AR–manufacturer association is pending. The system will allow up to 20 submissions while a user is not yet verified.

2.2 Register as a Secondary AR via invitation

Purpose: Follow this procedure to register on the SRP as a Secondary AR using an email invitation sent by the Primary AR.

Pre-conditions:

- You are not already registered as an SRP user
- You have an active EU Login account with MFA enabled
- **You have received a valid SRP email invitation initiated by a Primary AR**
    - **The feature to invite a Secondary AR is available only to a “Verified” Primary AR**

Steps:

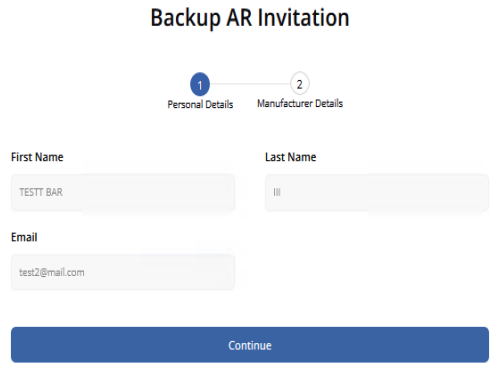
1. **Click the link in the email invitation** and authenticate **through EU Login**.

Exceptions and error handling:

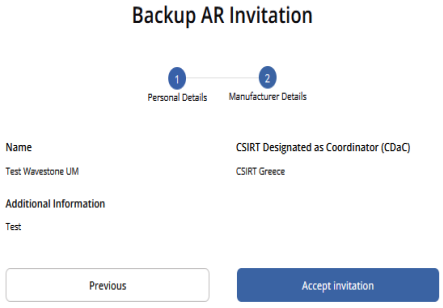
- If the invitation link has expired because more than 7 days have passed since the SRP sent the invitation, you will be redirected to a page displaying an error message.

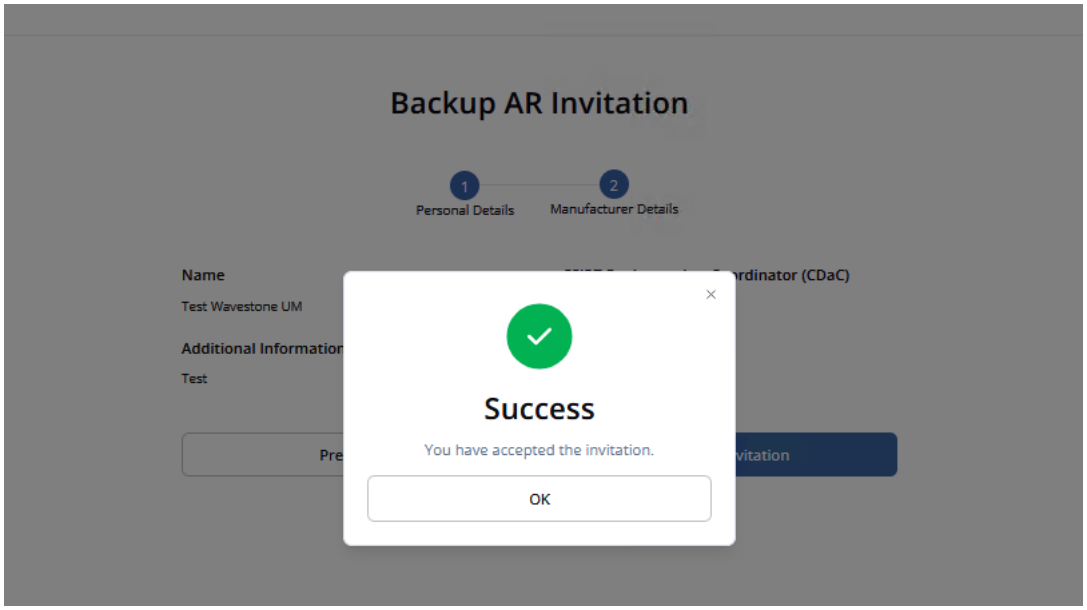
- If you click on the link but use the wrong EU Login account, you will not be associated with the manufacturer.

2. **Review and confirm the accuracy of your pre-filled personal details**, including First Name, Last Name, Email, then click “Continue”. These fields are retrieved from EU Login and cannot be edited in the SRP.



3. **Review and confirm the accuracy of the pre-filled manufacturer details** for the manufacturer associated with the Primary AR who initiated the invitation, then click “Accept invitation”.





Expected result and system outcome: Registration is completed and you become a Secondary AR for the relevant manufacturer. Your system role is displayed as “AR Backup User” and your status is set to “Active”.

If registration is not completed within 7 days of the invitation being sent, the invitation expires and the user status becomes “Invitation Expired” in the SRP.

2.3 Accept a Secondary AR association invitation as an existing SRP user

Purpose: Follow this procedure if you are already a registered AR and receive an email invitation to become associated with an additional manufacturer.

Pre-conditions:

- You are already registered as an SRP user and are associated with at least one other manufacturer
- You have an active EU Login account with MFA enabled
- **You have received a valid SRP email invitation from the Primary AR of the relevant manufacturer**

Steps:

1. **Click the link in the email invitation** and authenticate through EU Login.

2. **Review and confirm the accuracy of your pre-filled personal details**, including First Name, Last Name, Email, then click “Continue”. These details are retrieved from EU Login and cannot be edited in the SRP.

3. **Review and confirm the accuracy of the pre-filled manufacturer details** for the additional manufacturer associated with the Primary AR who sent the invitation, then click “Accept invitation”.

Expected result and system outcome: You are now associated with the relevant manufacturer as a Secondary AR. Your system role is displayed as “AR Backup User” for this additional manufacturer, while your SRP user status remains “Active”.

If you do not accept the Primary AR’s invitation within 7 days of the invitation being sent, the invitation expires and the invitation/association request is displayed as “Invitation Expired” in the SRP. Your existing SRP account, however, remains “Active” and your existing manufacturer association(s) are unaffected.

SECTION 3

AR User Login & Logout

3. AR User Login & Logout

This section explains how registered AR users log in to and log out of the SRP.

General notes

AR users authenticate through **EU Login** when accessing the SRP. The SRP authentication process itself is not described in this manual.

3.1 Log in to the SRP

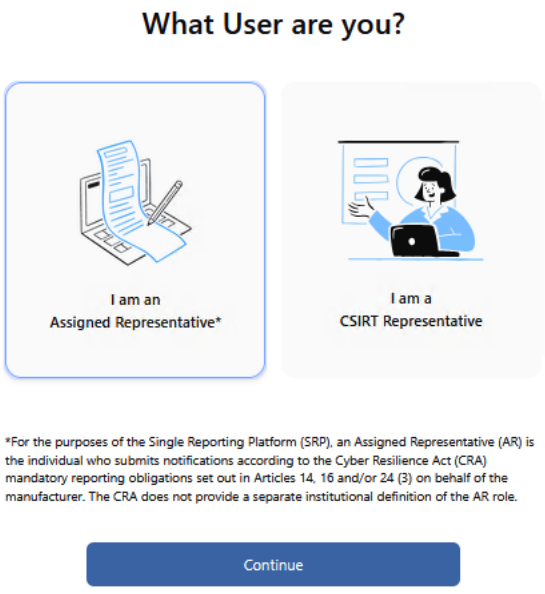
Purpose: Follow this procedure to log in to the SRP as a registered AR user.

Pre-conditions:

- You have an active EU Login account.
- You are already registered as an SRP user and your SRP user status is “Active”.

Steps:

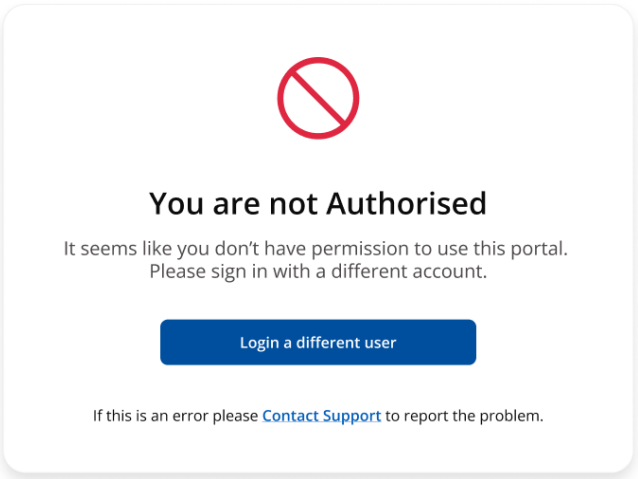
1. Open the SRP, select the Assigned Representative role and click “Continue”.



2. Select the CSIRT Designated as Coordinator (CDaC) from the drop-down list and click “Continue”.

3. Authenticate through EU Login.

Exceptions and error handling: If authentication fails, the SRP redirects you to a **Not Authorised** page.



4. Wait while the SRP verifies that your SRP user account exists and is active.

5. After successful verification, the Dashboard is displayed. For more information on the Dashboard and its available functions, see Section 4.6.1.

Note: If you are not yet registered as an SRP user, you are redirected to the registration process as described in Section 2.

Expected result and system outcome: You are successfully logged in to the SRP and the Dashboard available to your AR role is displayed.

3.2 Log out of the SRP

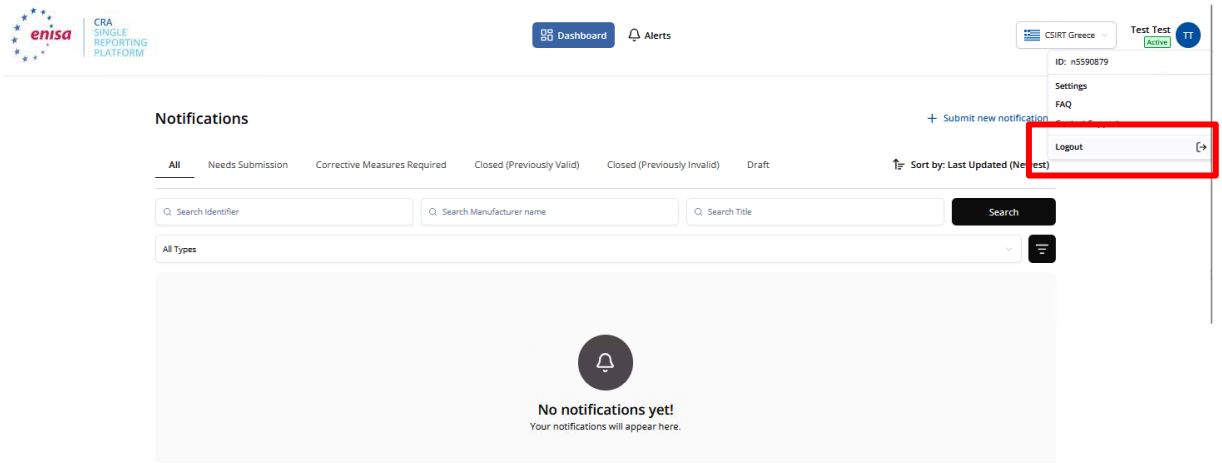
Purpose: Follow this procedure to log out of the SRP securely.

Pre-conditions:

- You are logged in to the SRP.

Steps:

1. Click your user identifier or profile menu and select **Log Out**.



Expected result and system outcome: Your SRP session is terminated, and you are logged out of the platform.

SECTION 4

AR Scenarios

4. AR Scenarios

This section provides step-by-step guidance for the main actions available to ARs in the SRP, including profile and manufacturer management, Secondary AR invitation, manufacturer association management, Primary AR role transition, Dashboard use, notification submission, and notification updates.

Audience

This section is intended for:

- AR users who manage manufacturer associations and submit or update notifications in the SRP.
- Primary AR users who invite Secondary ARs for manufacturers they represent.
- Secondary AR users who request to become the Primary AR for a manufacturer.

General notes

AR users can access the relevant AR scenarios only after successful login, provided that their SRP user status is “Active” and the applicable AR role and manufacturer association requirements are met.

4.1 View Personal Details and Manufacturer Details

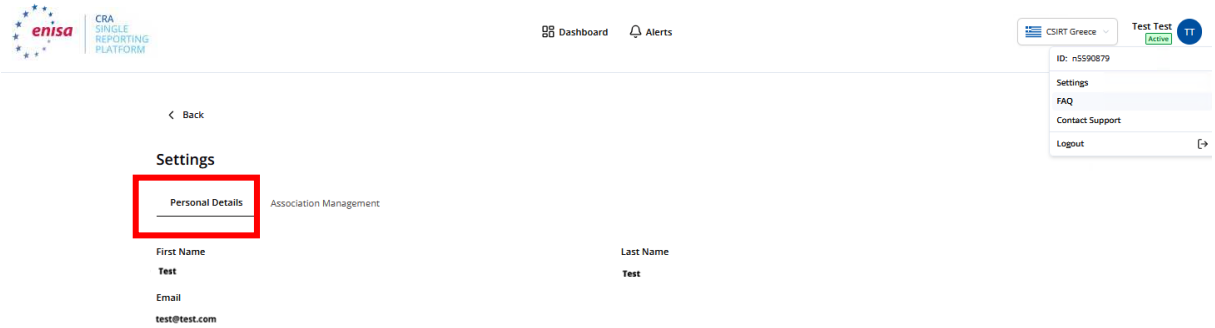
Purpose: Follow this procedure to view your personal details and the details of manufacturers with which you are associated through the Settings menu.

Pre-conditions: Your user status is “Active”, and you are logged in to the platform.

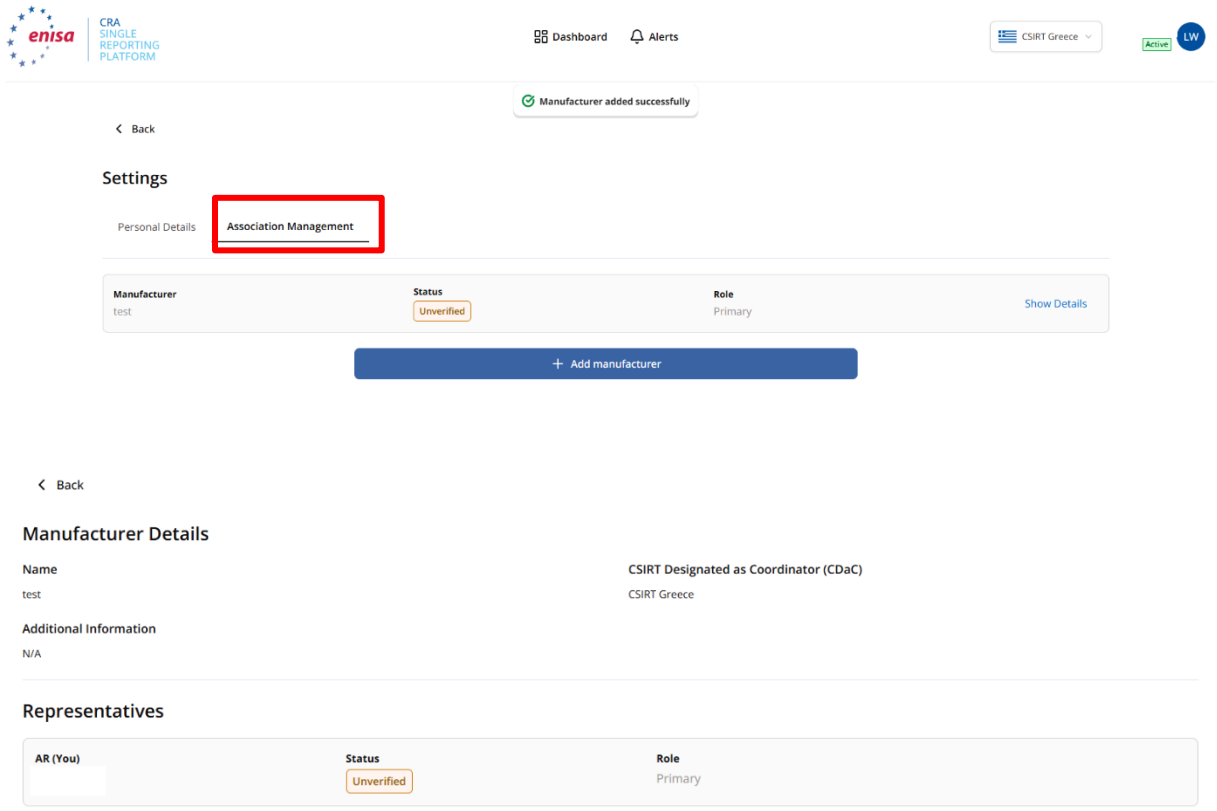
Steps:

1. From the Dashboard, click your profile name, and select “Settings” from the profile drop-down menu.

2. **Personal details:** Review your personal information displayed in the Settings menu.



3. **Manufacturer details:** Select "**Association Management**" to view the manufacturer information and your association with the relevant manufacturer.



Expected result and system outcome: Your personal details and manufacturer details are displayed for review. In the example above, the AR has not yet been validated by the designated CSIRT, and its status will be displayed as "Unverified".

4.2 Invite Secondary AR (by Primary AR)

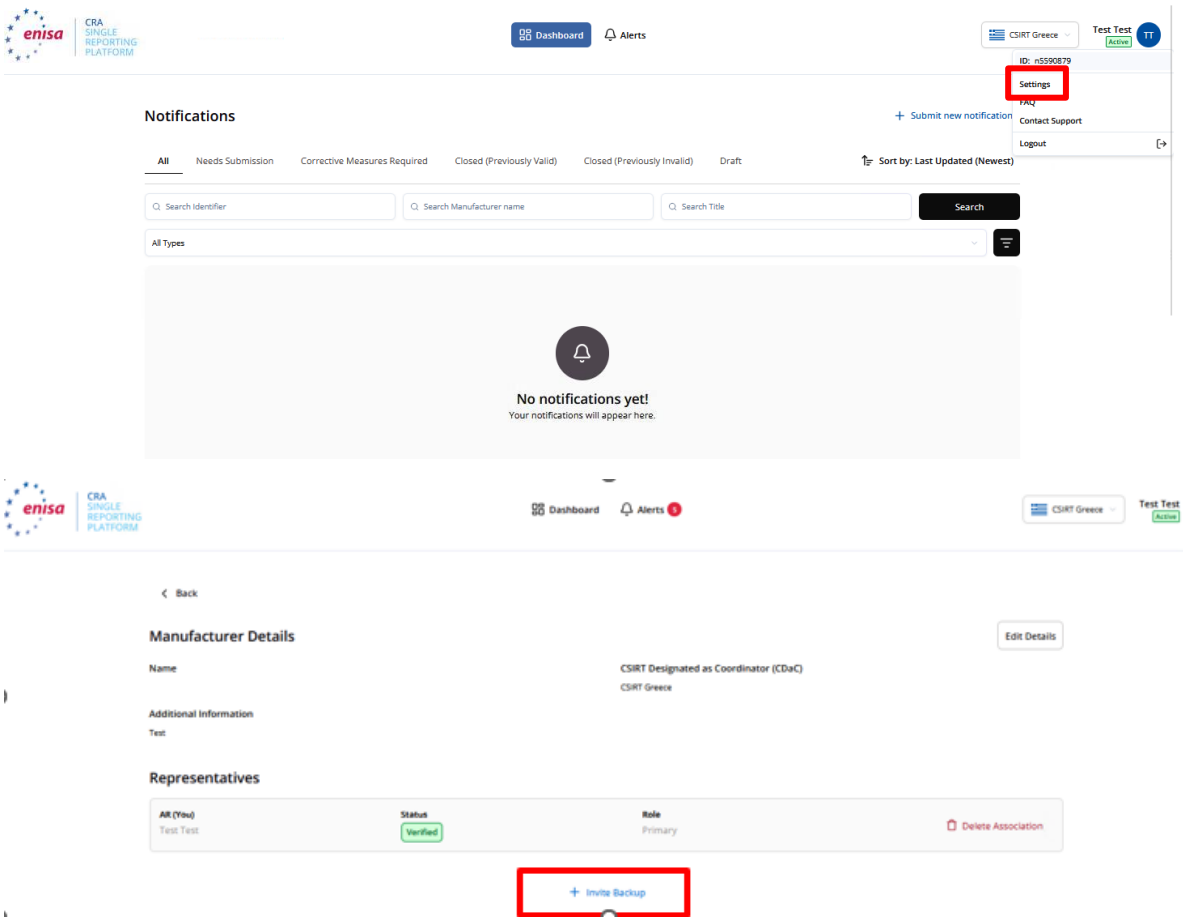
Purpose: Follow this procedure, as a Primary AR, to invite a Secondary AR for a manufacturer you represent.

Pre-conditions:

- Your user status is set to "Active" and you are logged in to the SRP.
- You have the Primary AR role for the relevant manufacturer.
- Your AR-manufacturer association has been validated by the CSIRT Designated as Coordinator (CDaC) and is displayed as "Verified".

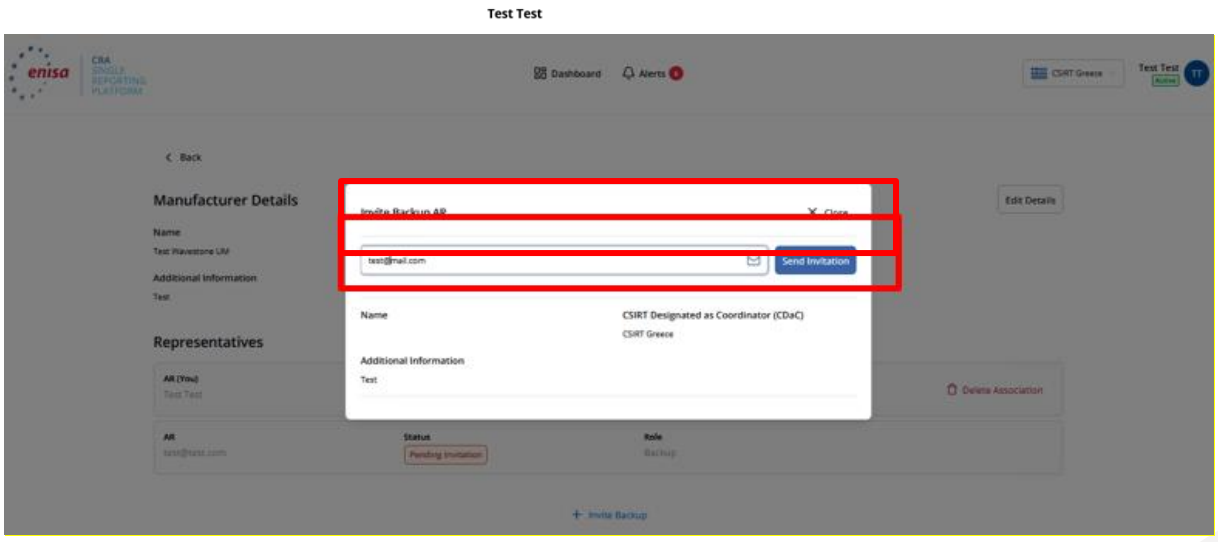
Steps:

1. Open the Settings section and select the option to add a Secondary AR ("Invite Backup") for the manufacturer you represent.



***Note**: You must first have a verified AR-manufacturer association before being able to invite a Secondary AR.*

2. Enter the email address used by the prospective Secondary AR to register on EU Login and click “Send Invitation”.



Confirmation: The SRP displays a pop-up confirming that the invitation has been sent.

Expected result and system outcome: The SRP sends an email invitation to the Secondary AR. A new user record is created in the SRP with the specified email address and corresponding manufacturer details. The user role is assigned once the registration is completed.

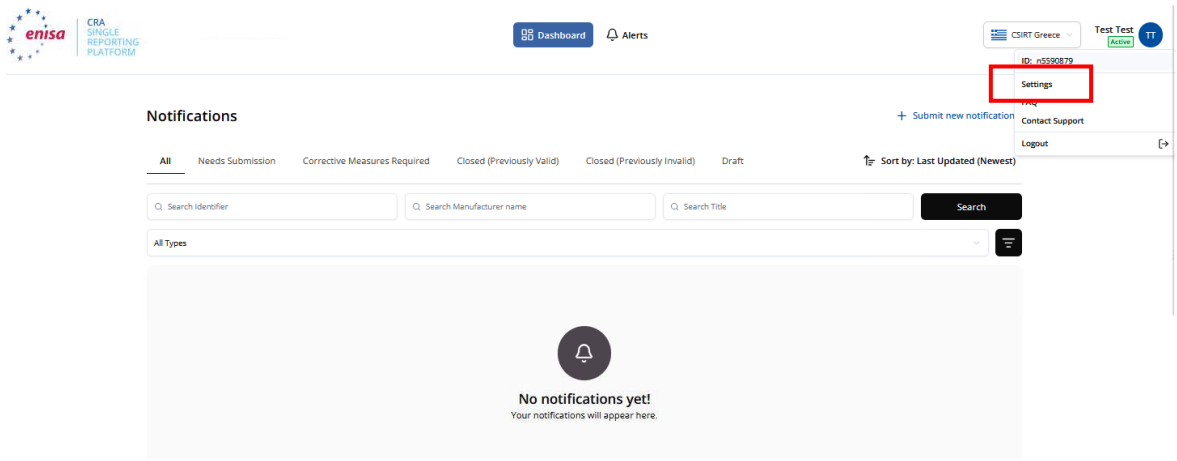
4.3 Add Additional Manufacturer Association via Settings

Purpose: Follow this procedure to request an additional manufacturer association through the Settings menu.

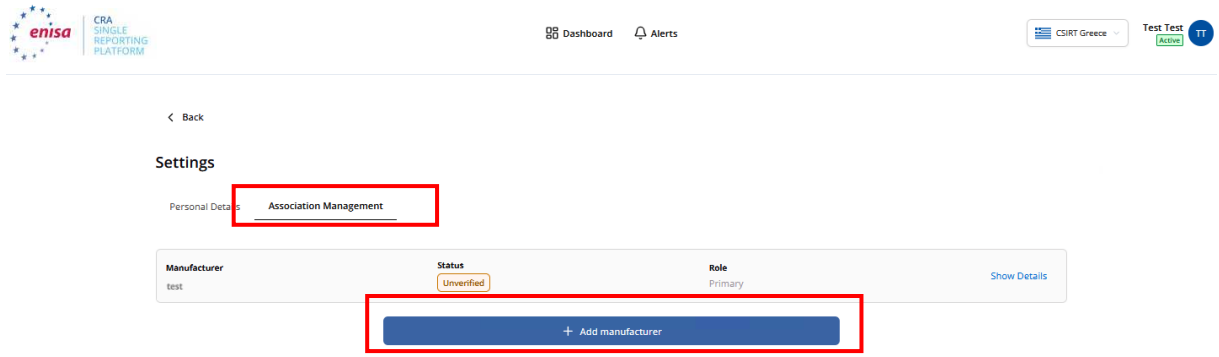
Pre-conditions: Your user status is “Active” and you are logged in to the SRP.

Steps:

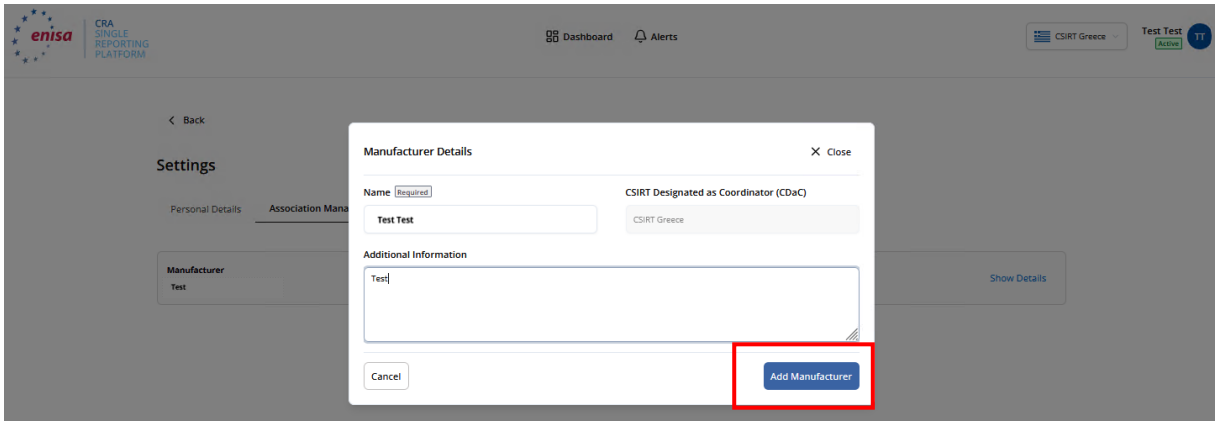
1. Open the Dashboard, click your profile name, and select “Settings” from the profile drop-down list.



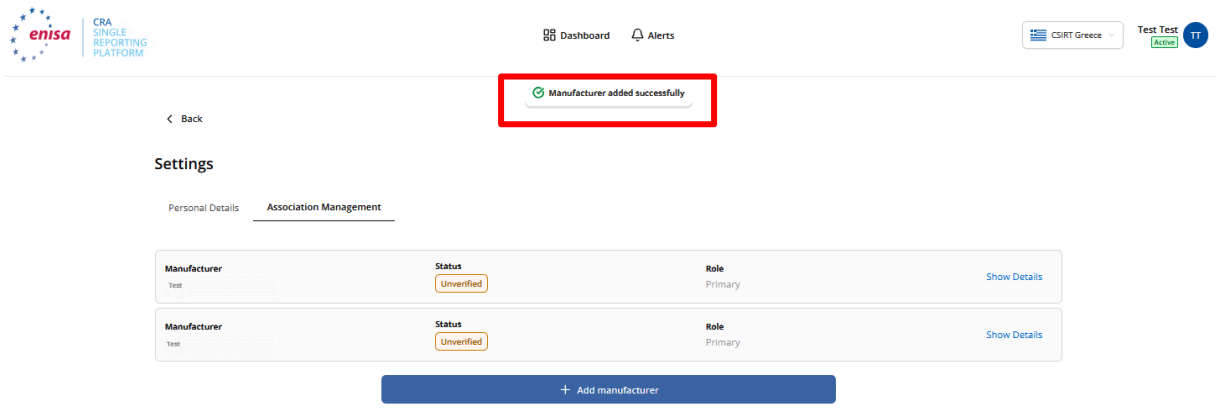
2. Open “Association Management” and click “Add Manufacturer”.



3. Enter the required details for the new manufacturer and click “Save”.

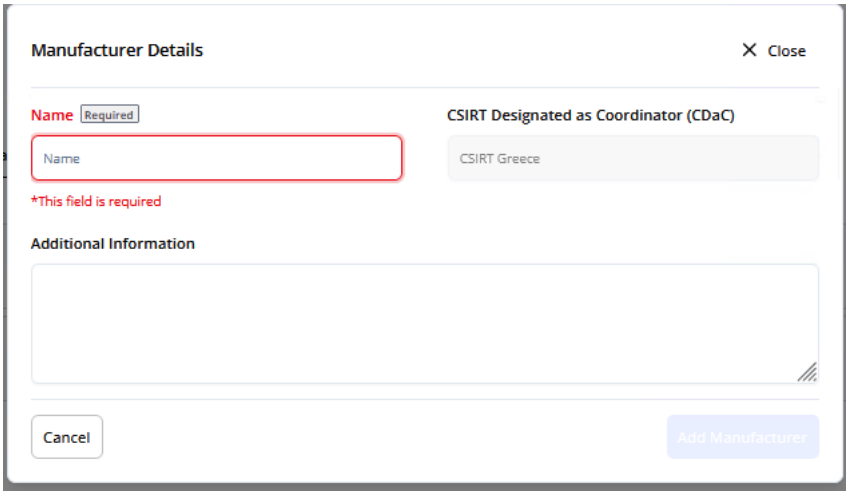


Confirmation: The SRP displays a pop-up confirming that the manufacturer has been created and the association request has been submitted.



Exceptions and error handling:

If required manufacturer details are missing, such as Manufacturer Name, the SRP displays an error and the “Continue” or “Save Edit” button remains disabled.



Expected result and system outcome: The manufacturer record and the AR association with the manufacturer are created in the SRP and submitted to the designated CSIRT for validation. The SRP sends an email confirming the association request. As an "Unverified" AR, you can submit up to 20 notifications.

4.4 Claim Primary AR Role (by Secondary AR)

Purpose: Follow this procedure, as a Secondary AR, to request the Primary AR role for a manufacturer.

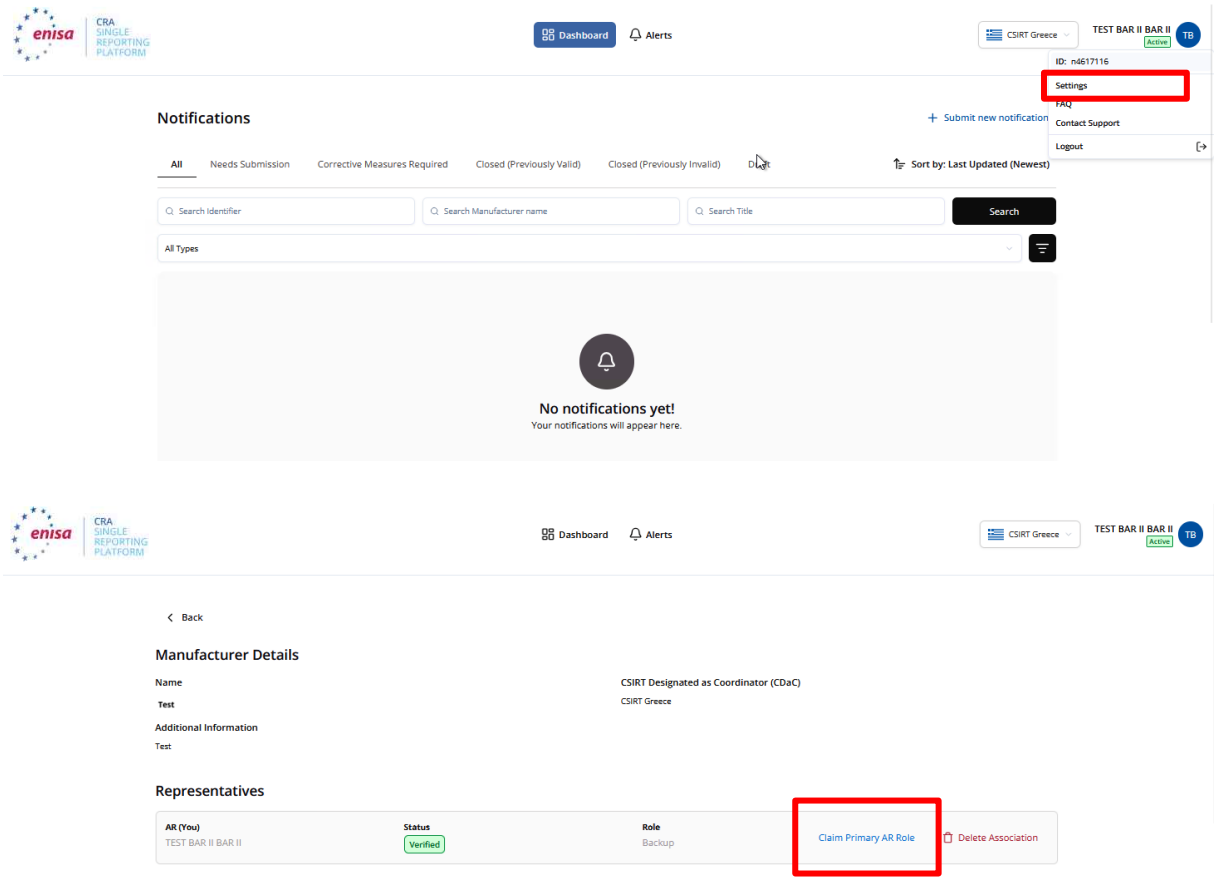
Pre-conditions:

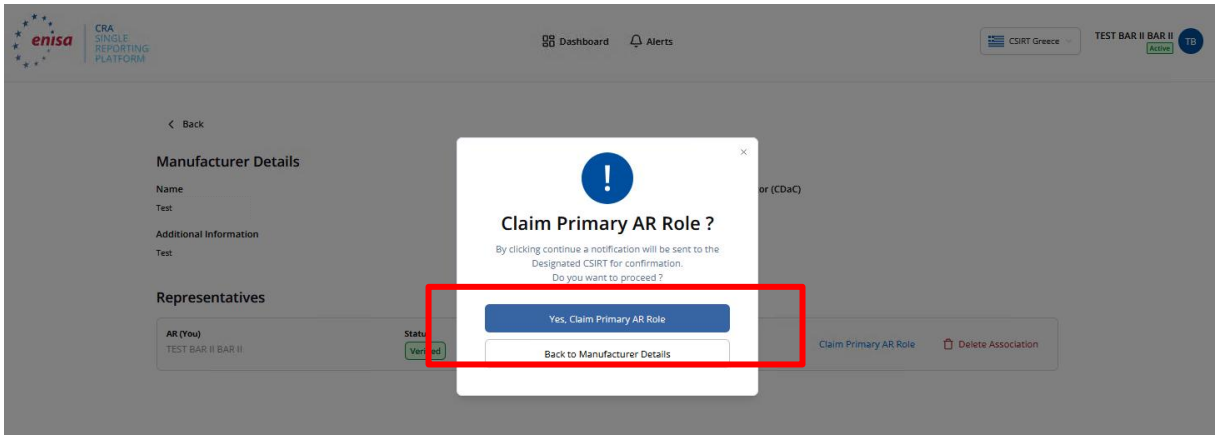
- You are a Secondary AR for the relevant manufacturer.
- Your user status is “Active” and you are logged in to the SRP.

Steps:

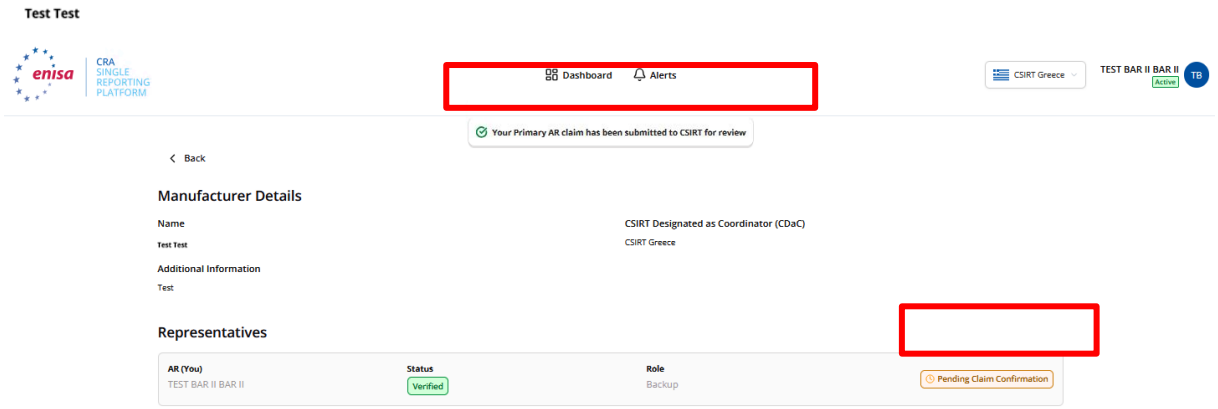
1. Open the Dashboard, click your profile name, and select “Settings” from the profile drop-down list.

2. Select the option to claim the Primary AR role for the relevant manufacturer.





Confirmation: The SRP displays a pop-up asking you to confirm the claim request.



3. Confirm the request.

Expected result and system outcome: The claim request is created and submitted to the designated CSIRT for review and approval. The Secondary AR remains in the existing role until the request is approved.

4.5 Manage Manufacturer Association

Purpose: Follow this procedure to manage the association between AR users and manufacturers, including removal of your own association or, where applicable, the association of a Secondary AR.

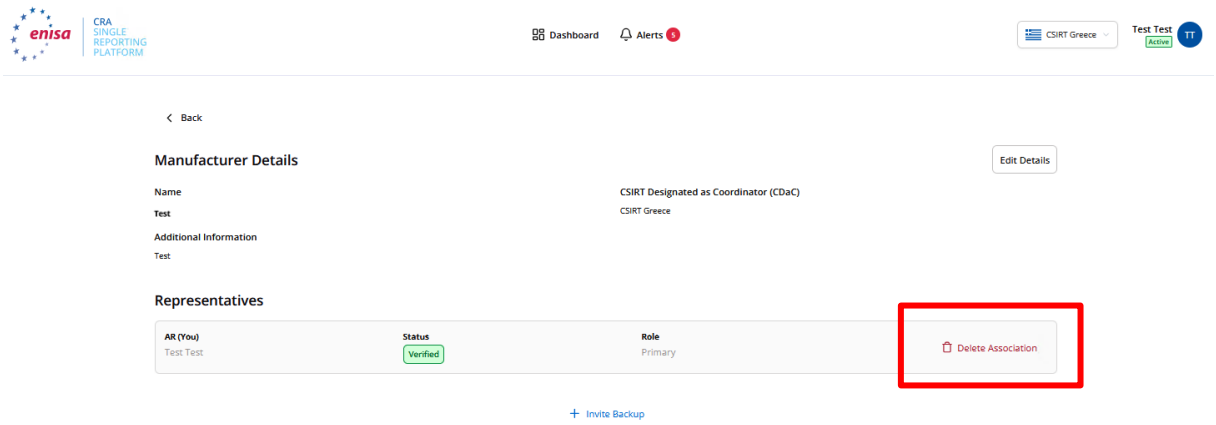
Pre-conditions: Your user status is “Active”, you are logged in to the SRP, and the AR association with the manufacturer has been “Verified”.

Steps:

1. Open the AR Association Management page in the SRP.

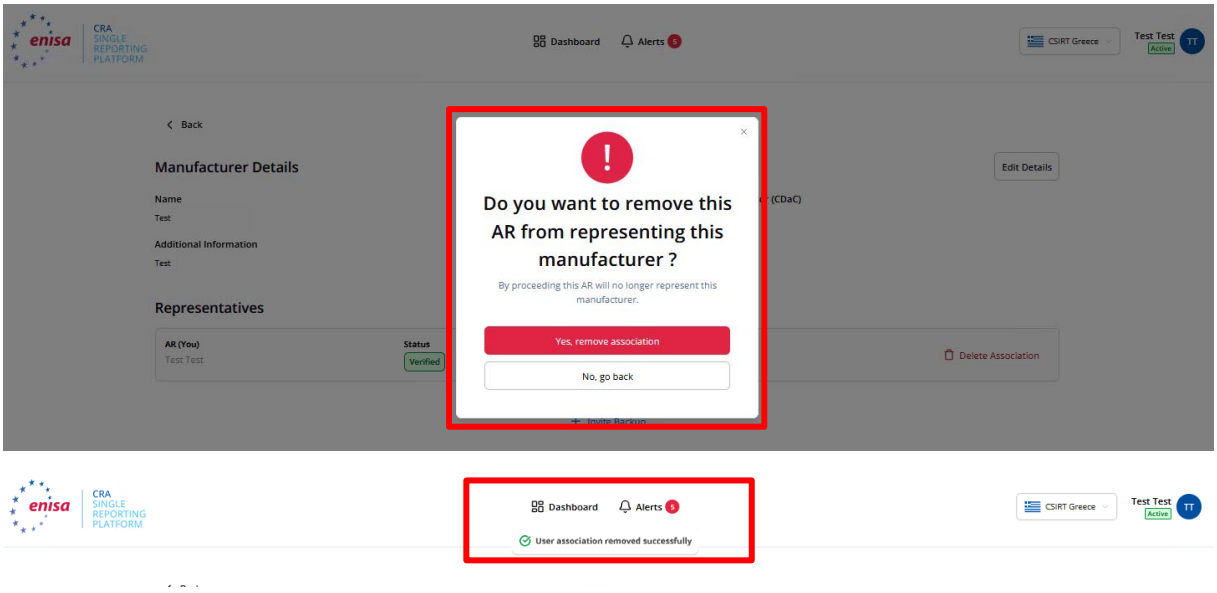
Role-specific options:

As a **Primary AR**, you can remove your own association or remove a Secondary AR association for the manufacturer. As a **Secondary AR**, you can remove your own association.

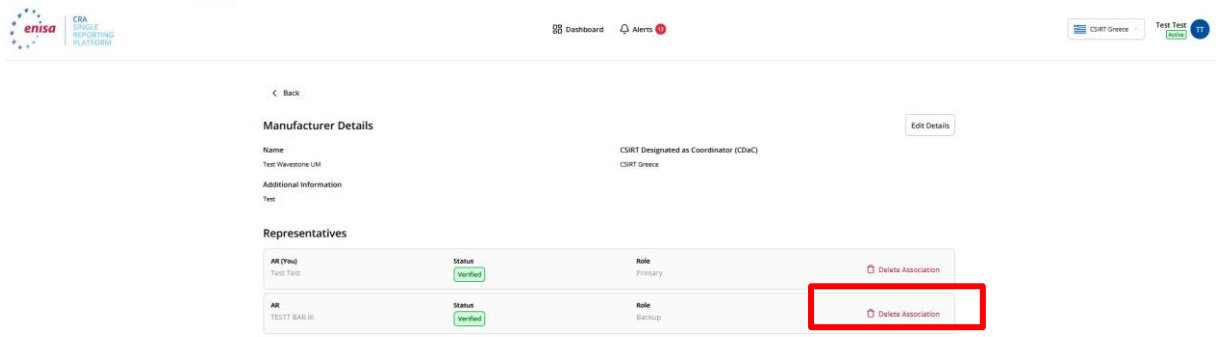


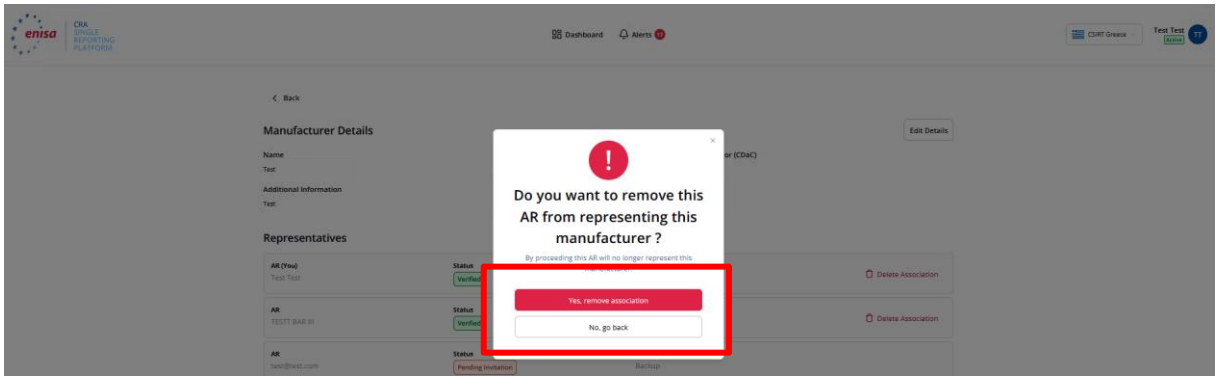
2. Click “Delete Association” for the association to be removed and confirm the action.

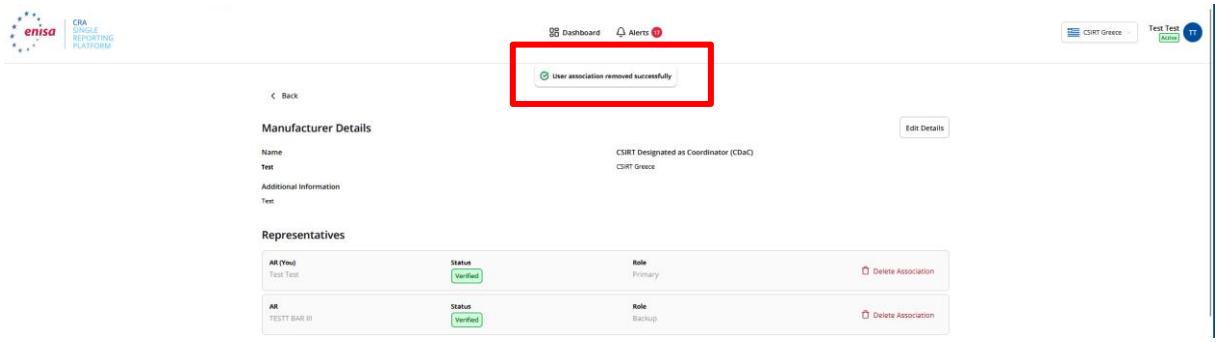
AR removes own association:



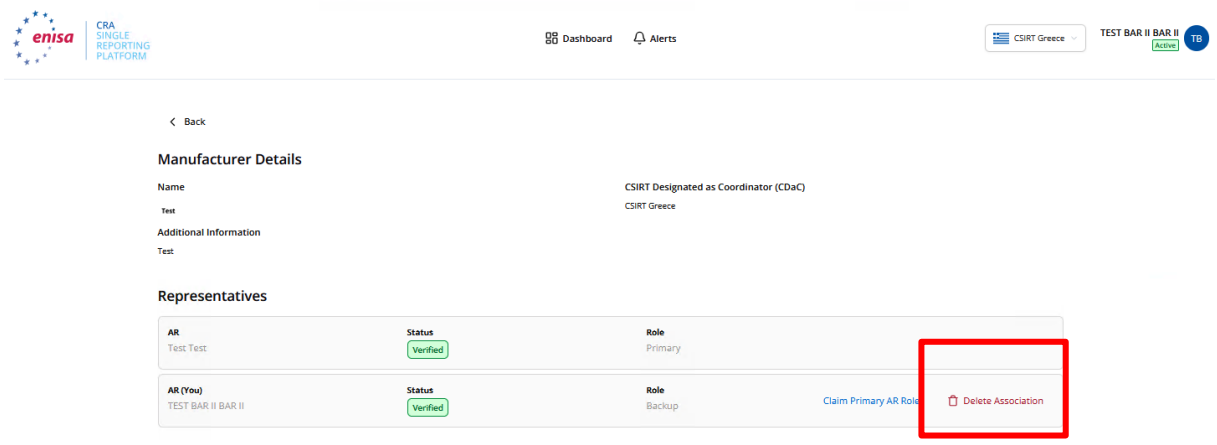
AR removes Secondary AR:

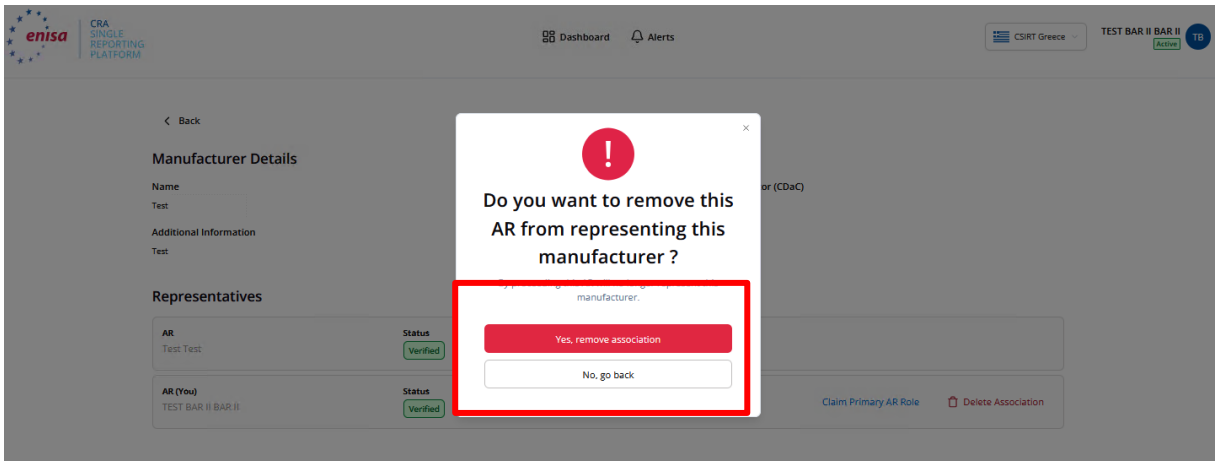






Secondary (Backup) AR removes own association:





Expected result and system outcome: The selected AR association is removed.

4.6 Dashboard

Purpose: Use the Dashboard to view accessible notifications, search, sort and filter records, and open notification details.

Access options:

- Directly after login (section 3).
- By accessing the valid Dashboard URL while logged in.
- By selecting a Notification Alert, where available.

4.6.1 View Dashboard

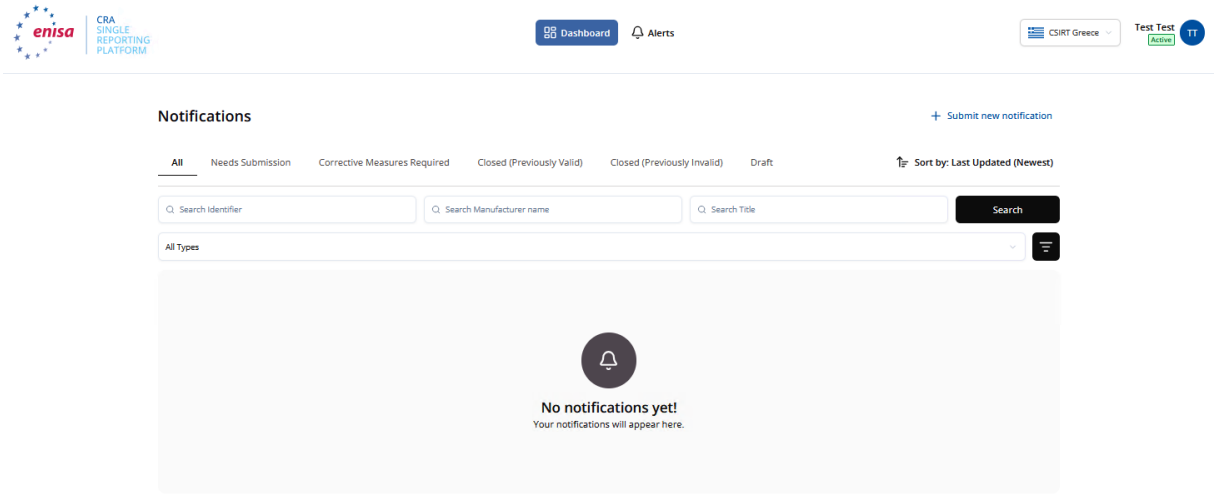
Purpose: Follow this procedure to view the list of notifications accessible to you.

Pre-conditions: Your user status is “Active” and you are logged in to the SRP.

Steps:

1. Open the Dashboard. The content displayed depends on the notifications created by the logged-in AR.

Dashboard at first login for an AR:



Exceptions and access limitations:

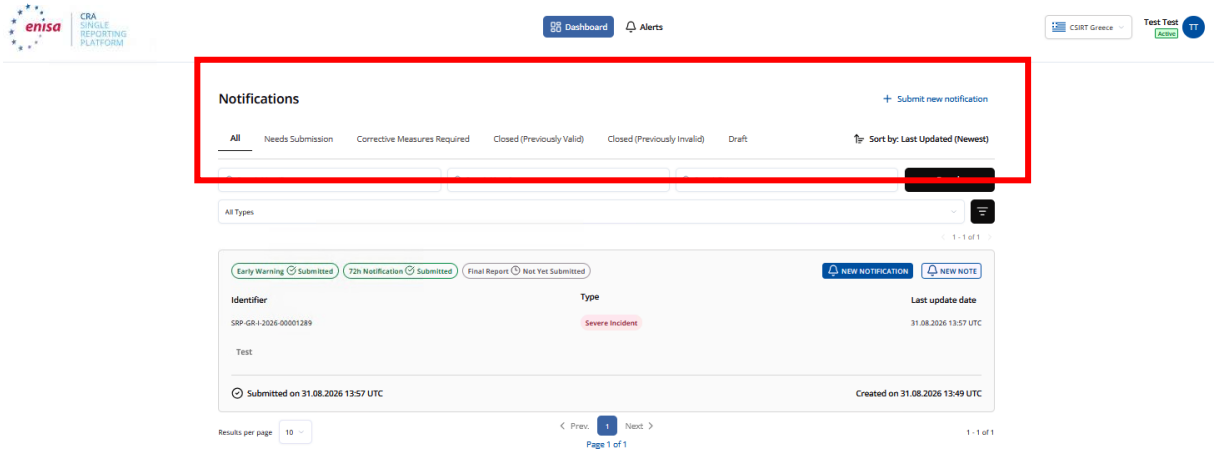
A Primary AR can access all notifications associated with their manufacturer, whereas a Secondary AR can only access notifications they submitted and drafts they created. Secondary ARs cannot view notifications submitted by another AR associated with the same manufacturer.

Expected result and system outcome: The Dashboard is displayed and lists the notifications accessible to you based on your user permissions.

4.6.2 Search, Sort & Filter Notifications

Test

Purpose: Follow this procedure to search, sort, and filter the notifications accessible to you.



The actions that you can perform include:

- Search for notifications.
- Sort notification records.
- Filter results based on specific criteria.

Pre-conditions:

- Your user status is “Active” and you are logged in to the SRP.
- At least one notification has previously been submitted or saved as a draft by you.

Steps:

1. Open the Dashboard and review the default notification sorting.

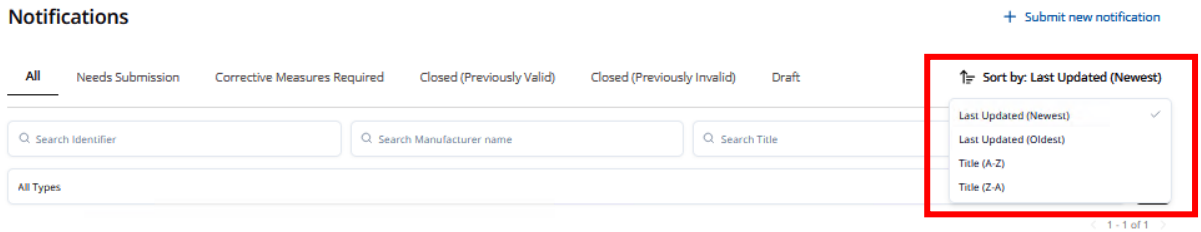
- Last updated date (most recently updated notifications appear first).
- Existence of labels indicating an action is needed: “Report is late”, “Report due soon”, .

2. Use the Search field to search by one of the following criteria:

- Notification ID (free text).
- Manufacturer (free text).
- Title (free text).

3. Sort the notification list by one of the available columns.

- Title: sort alphabetically.
- Last Update: sort by date.



4. Select “All filters” to filter the notification list.

You narrow down the results with one or more of these criteria:

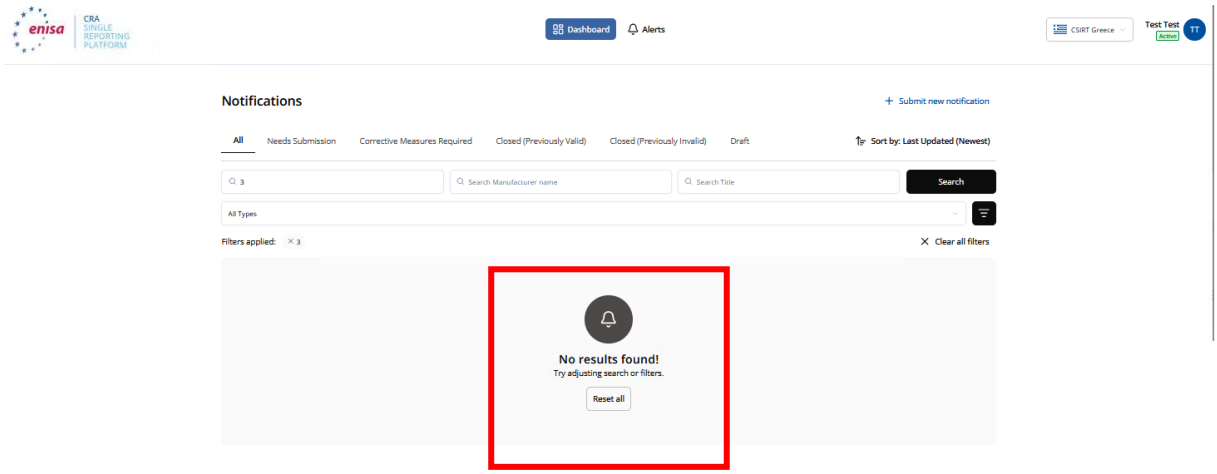
- Member States where the product with digital elements is available.
- Type of submission.

You can select “Action Required” to display only notifications with a pending-action label. These are sorted by:

- Last update date, with the most recently updated appear first.
- Labels, based on the following sequence: Report is late, Report due soon, etc.

5. Select “Clear Filters”, if needed, to remove all applied filters.

Exceptions and error handling: If **no results** are found, the SRP informs you that no notifications match the search or filter criteria.



Expected result and system outcome: The notification list is searched, sorted, and/or filtered according to your selections.

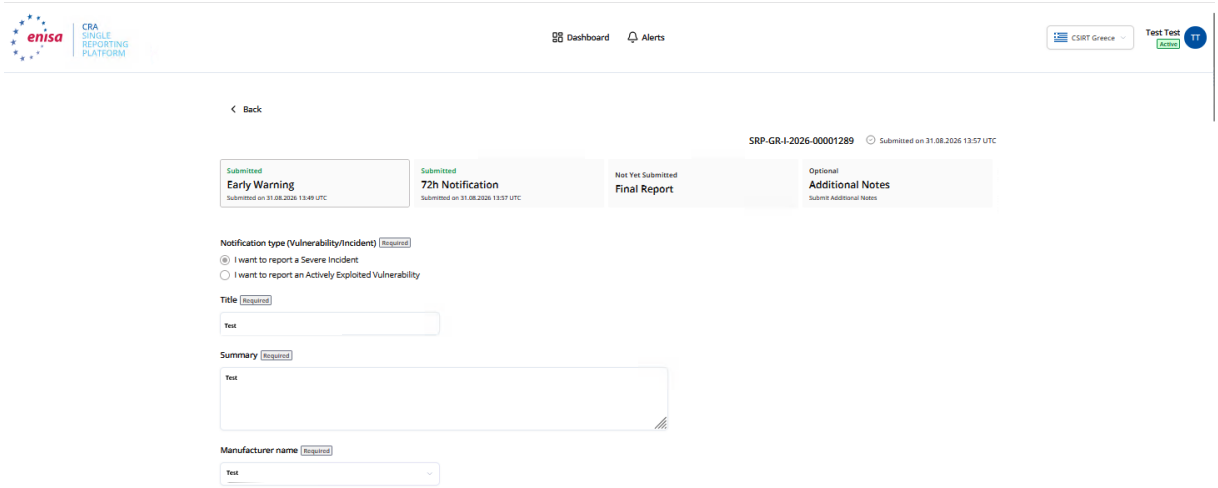
4.6.3 View Notification Details

Purpose: Follow this procedure to view the details of a notification accessible to you.

Pre-conditions: Your user status is “Active”, you are logged in to the SRP, and the notification is accessible from your Dashboard.

Steps:

1. Click a notification in the Dashboard to open its details.



Expected result and system outcome: The notification details are displayed according to your role and permissions.

4.7 Submit New Notification

Purpose: Follow this procedure to submit a new notification for an actively exploited vulnerability (AEV) or severe incident (SI) having an impact on the security of a product with digital elements, so that it can be received and processed through the SRP workflow.

Pre-conditions:

- Your user status is “Active” and you are logged in to the SRP.
- You have an association with the relevant manufacturer
- Your association may be “Verified” or validation may still be pending (“Unverified”) and you are not exceeding the submission limits.

4.7.1 Notification Workflow

A notification in the SRP is submitted progressively through three reporting steps: **Early Warning**, **72-hour Notification**, and **Final Report**. These steps allow the Assigned Representative to provide initial information first, then complete or update the notification as additional information becomes available. The sequence and timing of the reports depend on the applicable CRA reporting obligations and on the type of event being reported.

Table 3 – Notification Submission Steps

Step	Purpose	Typical outcome
Early Warning	Initial report used to notify the designated CSIRT that an AEV or SI has been identified and to provide the first available information.	The notification is submitted to the designated CSIRT and becomes visible according to the platform workflow.
72-hour Notification	Follow-up report used to provide additional details after the Early Warning, where required.	The notification is updated and made available for review and dissemination decisions according to the applicable rules.
Final Report	Final submission used to complete the reporting sequence once the required information is available.	The notification becomes complete from the AR side and is no longer editable by the AR after submission.

Draft versus submission: When a report is saved as a draft, it is stored in the SRP but is not submitted to the designated CSIRT for review. A draft can be reopened and completed later by the AR who created it. When a report is submitted, the SRP changes the notification status, sends the relevant alerts or emails, and makes the information available in accordance with the applicable workflow.

Editing after submission: After the Early Warning or 72-hour Notification is submitted, the AR may still update the notification where the platform allows it and while the notification remains editable. After the Final Report is submitted, the notification is no longer editable by the AR.

Recipients and visibility: Submitted reports are made available to the designated CSIRT for review. The notification is also simultaneously made available to ENISA, except where Particular Exceptional Circumstances (PEC) apply to the 72-hour AEV Notification. Other concerned CSIRTs receive the information following dissemination by the designated CSIRT.

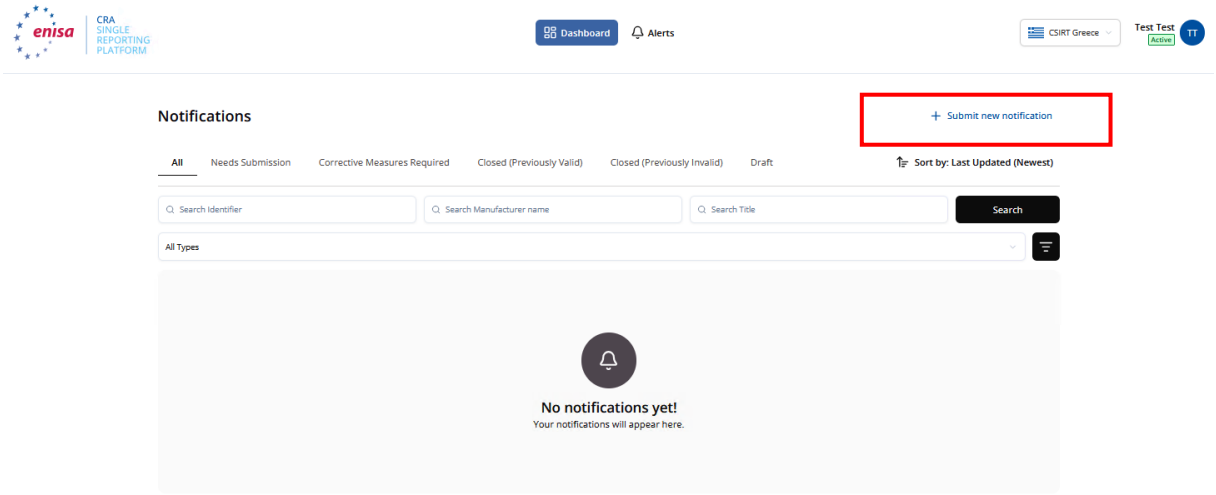
Important: Not all reports necessarily contain the same level of detail. Users should complete all required fields displayed by the SRP and provide additional information where available and relevant. Certain fields are mandatory if the information is available, as required by the CRA. If required information is missing, the SRP displays a validation error and prevents submission until the issue is corrected.

4.7.2 Submit Early Warning

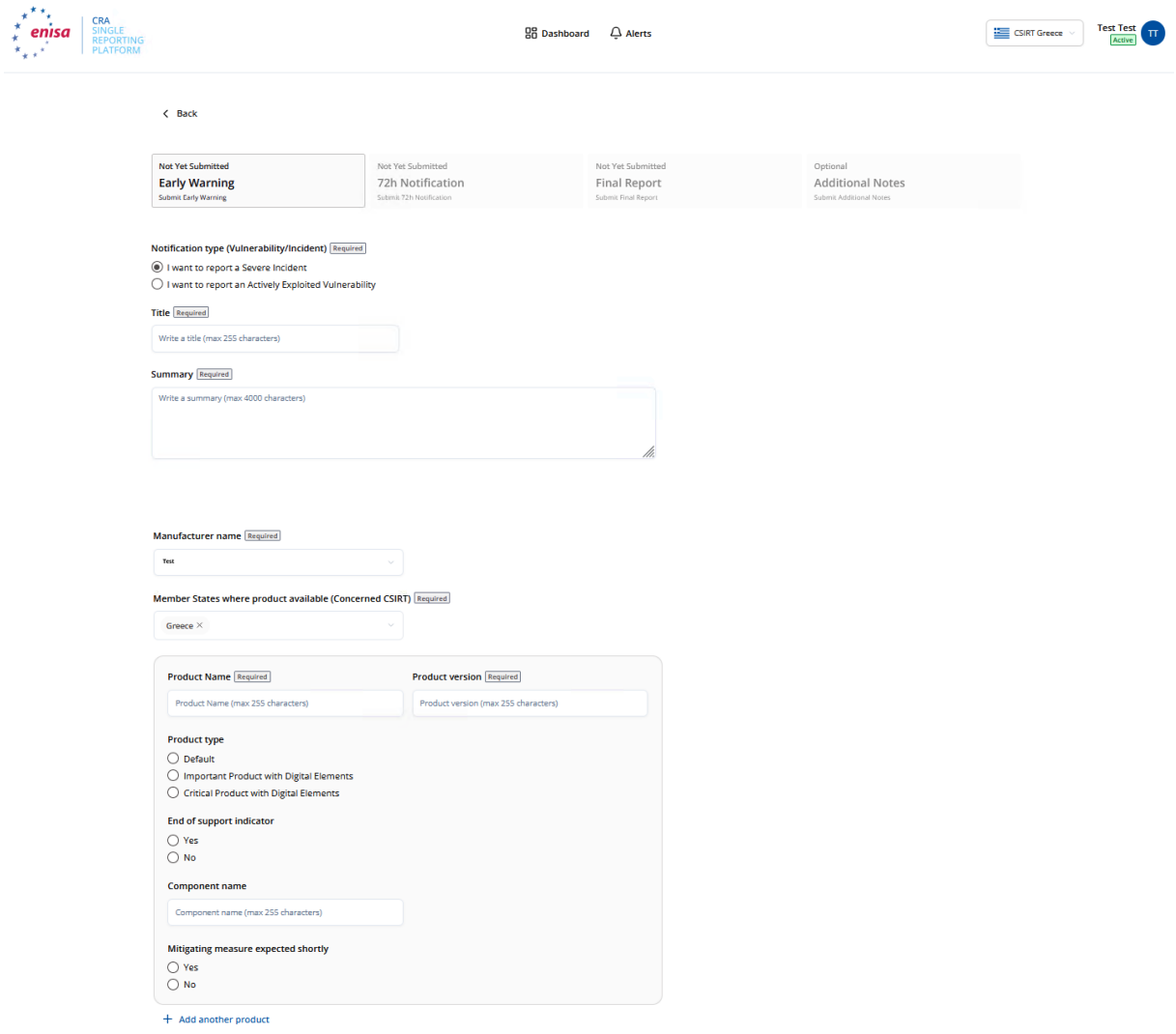
Purpose: Follow this procedure to create and submit the Early Warning report for a new notification.

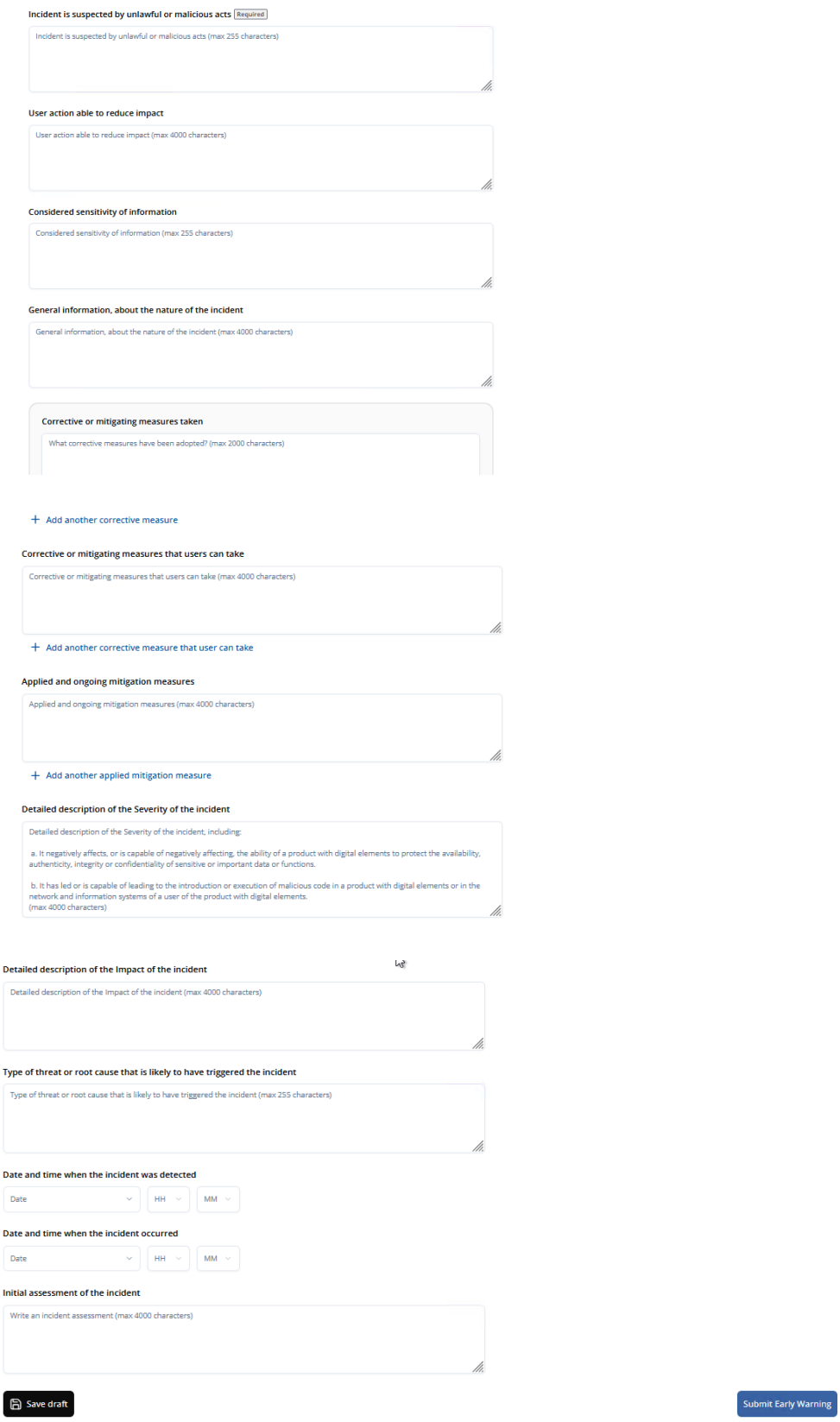
Steps:

1. Click “Submit new notification” from the Dashboard. The SRP creates a new notification and pre-fills the user type as AR.

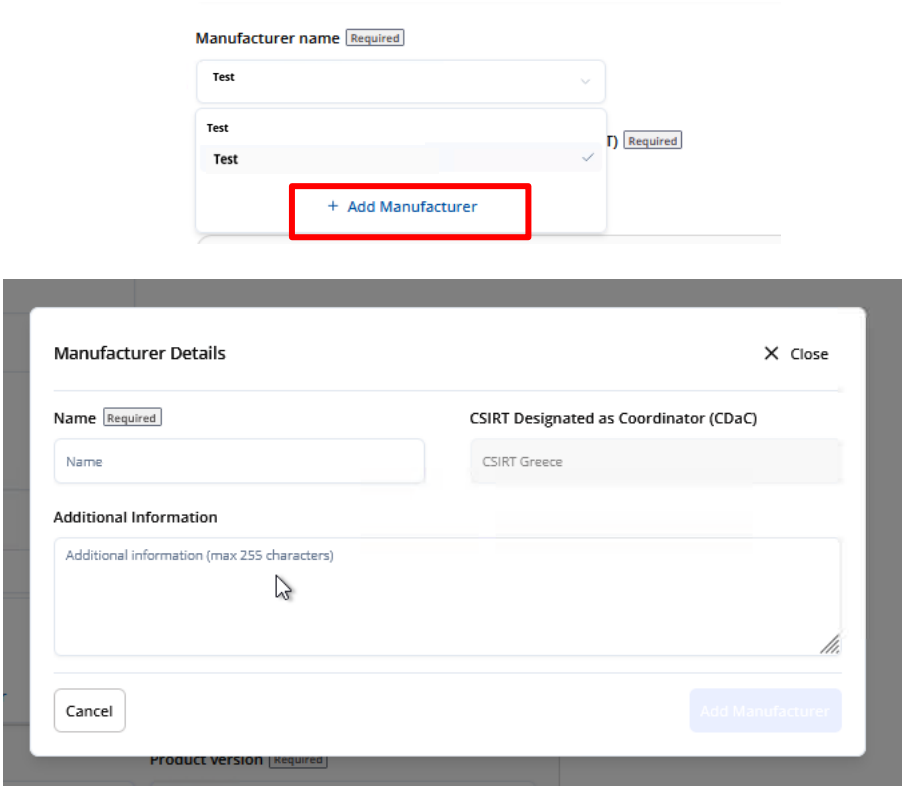


2. Complete the required fields and any relevant optional fields in the Early Warning tab. Fields differ depending on whether you select Actively Exploited Vulnerability or Severe Incident.

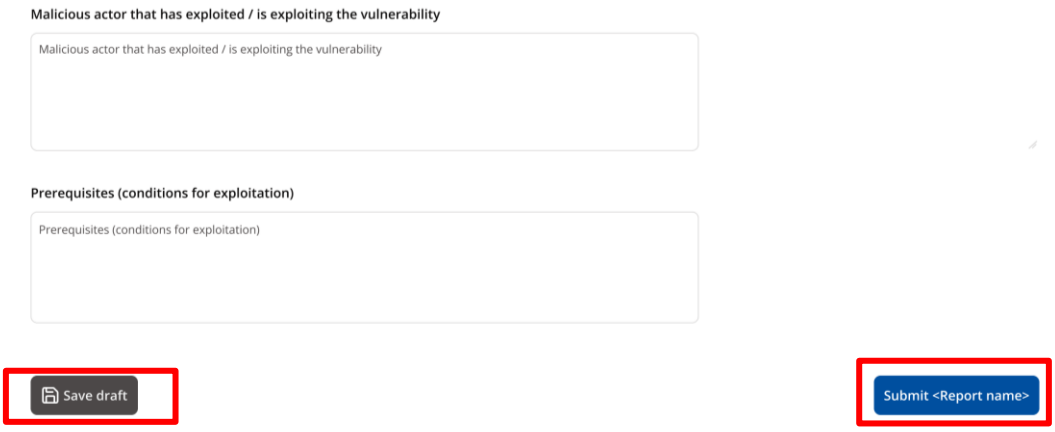



Incident is suspected by unlawful or malicious acts Required
Incident is suspected by unlawful or malicious acts (max 255 characters)
User action able to reduce impact
User action able to reduce impact (max 4000 characters)
Considered sensitivity of information
Considered sensitivity of information (max 255 characters)
General information, about the nature of the incident
General information, about the nature of the incident (max 4000 characters)
Corrective or mitigating measures taken
What corrective measures have been adopted? (max 2000 characters)
Add another corrective measure
Corrective or mitigating measures that users can take
Corrective or mitigating measures that users can take (max 4000 characters)
Add another corrective measure that user can take
Applied and ongoing mitigation measures
Applied and ongoing mitigation measures (max 4000 characters)
Add another applied mitigation measure
Detailed description of the Severity of the incident
Detailed description of the Severity of the incident, including:
a. It negatively affects, or is capable of negatively affecting, the ability of a product with digital elements to protect the availability, authenticity, integrity or confidentiality of sensitive or important data or functions.
b. It has led or is capable of leading to the introduction or execution of malicious code in a product with digital elements or in the network and information systems of a user of the product with digital elements.
(max 4000 characters)
Detailed description of the Impact of the incident
Detailed description of the Impact of the incident (max 4000 characters)
Type of threat or root cause that is likely to have triggered the incident
Type of threat or root cause that is likely to have triggered the incident (max 255 characters)
Date and time when the incident was detected
Date
HH
MM
Date and time when the incident occurred
Date
HH
MM
Initial assessment of the incident
Write an incident assessment (max 4000 characters)
Save draft
Submit Early Warning

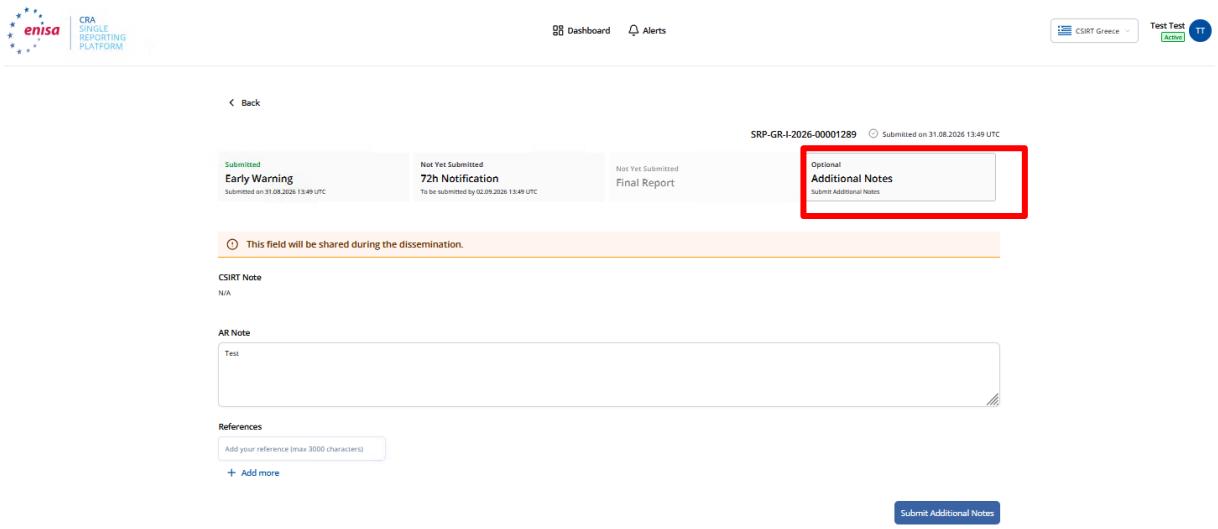
3. Select an existing manufacturer or add a new manufacturer, where permitted.

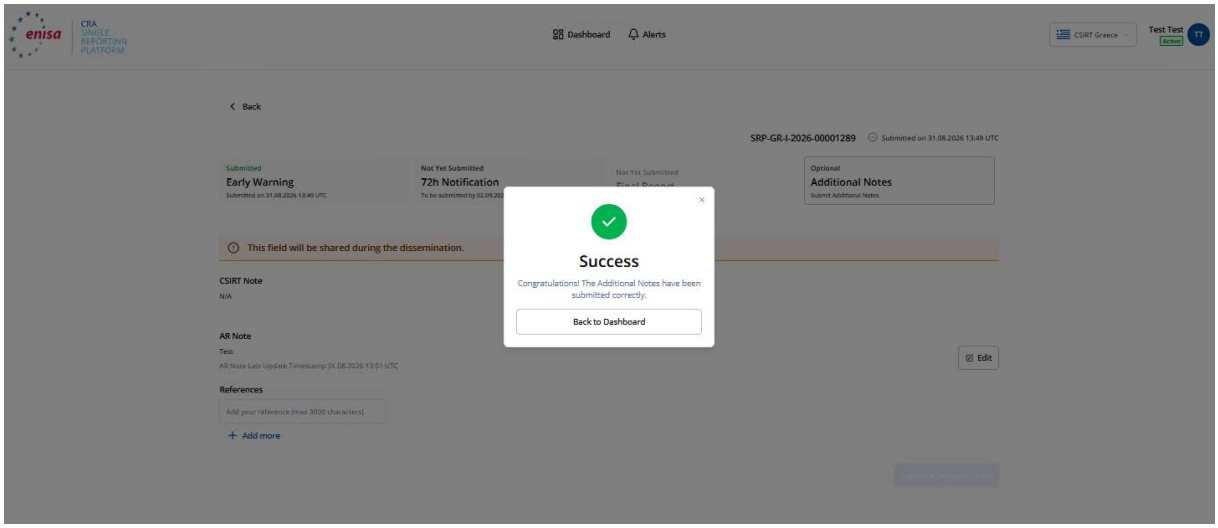


4. Submit the notification or save it as a draft.

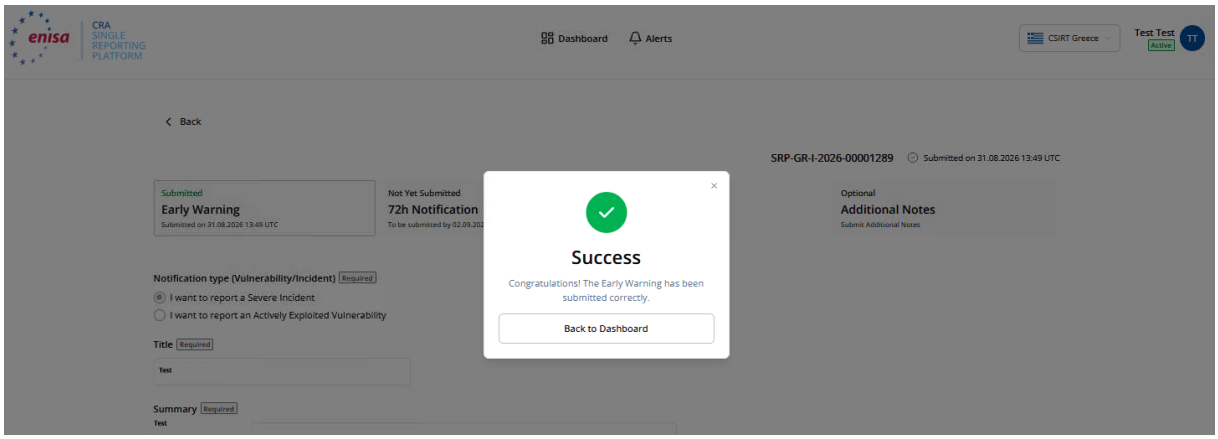


5. Optionally update “Additional Notes”, which are visible to users with access to the notification.

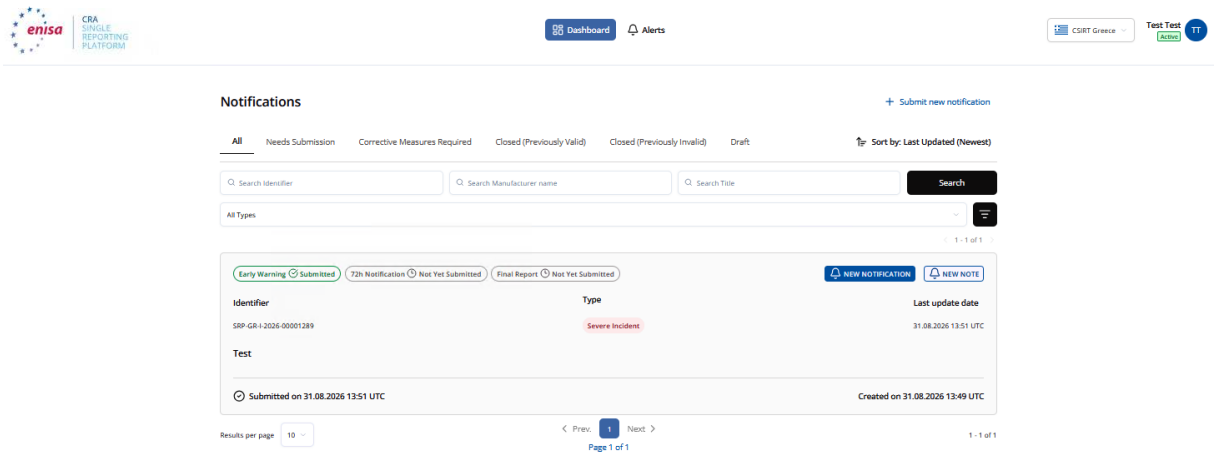




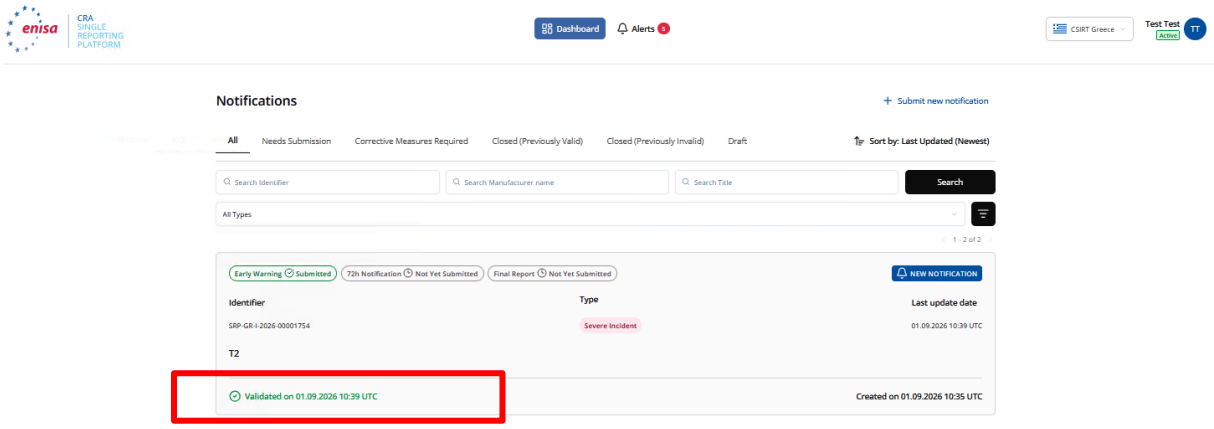
Notification successfully submitted:



The notification is listed in the Dashboard. **Before CSIRT validation**:

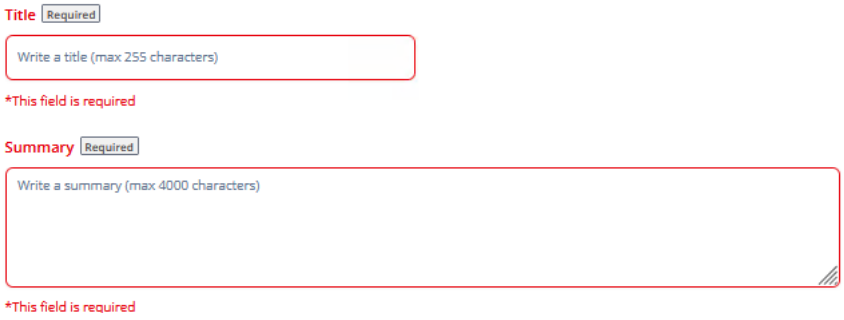


After CSIRT validation:



Exceptions and error handling:

If you omit mandatory data, the SRP will return an **error** informing you which mandatory data are missing and need to be provided.



Expected result and system outcome: The Early Warning is either saved as a draft or submitted. If submitted, it appears in the Dashboard with the corresponding status and is made available according to the SRP workflow.

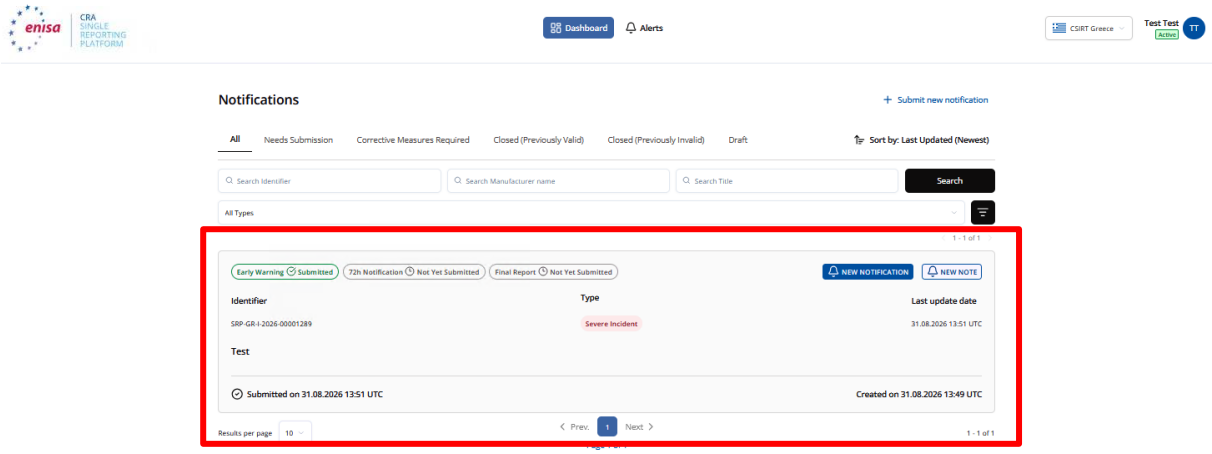
4.7.3 Submit 72-hour Notification

Purpose: Follow this procedure to submit the 72-hour Notification for an existing notification after the Early Warning has been submitted.

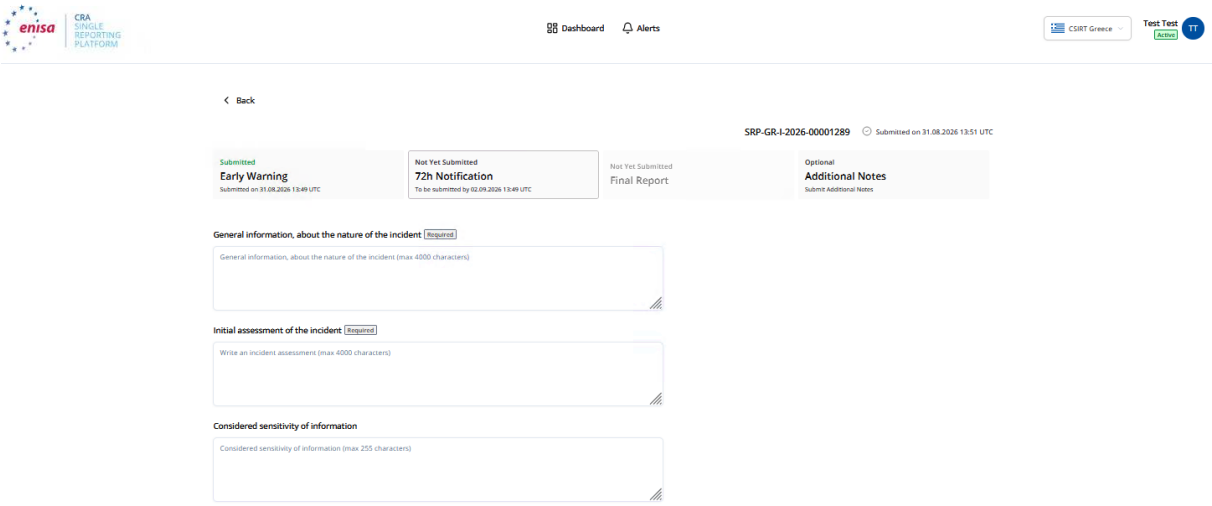
Pre-conditions: An Early Warning has already been submitted for the notification.

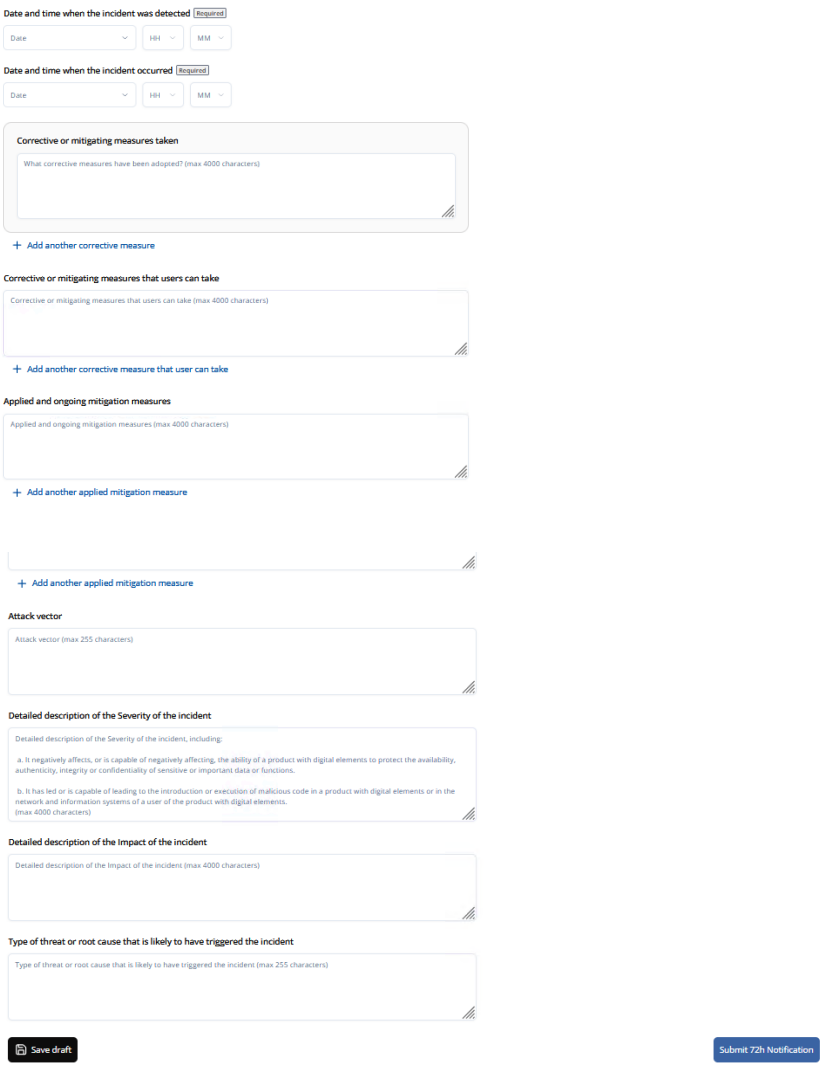
Steps:

1. Open the existing notification from the Dashboard.



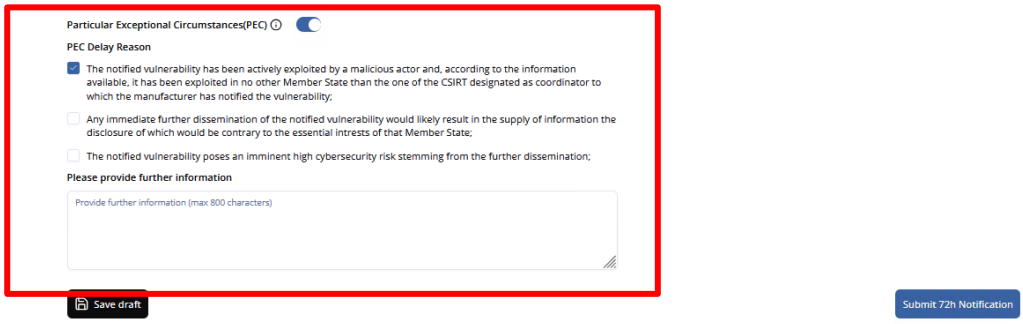
2. Complete the required fields and any relevant optional fields in the 72-hour Notification tab. Please note that some fields that were optional at the Early Warning stage may now be required. Other fields may be mandatory if the information is available.



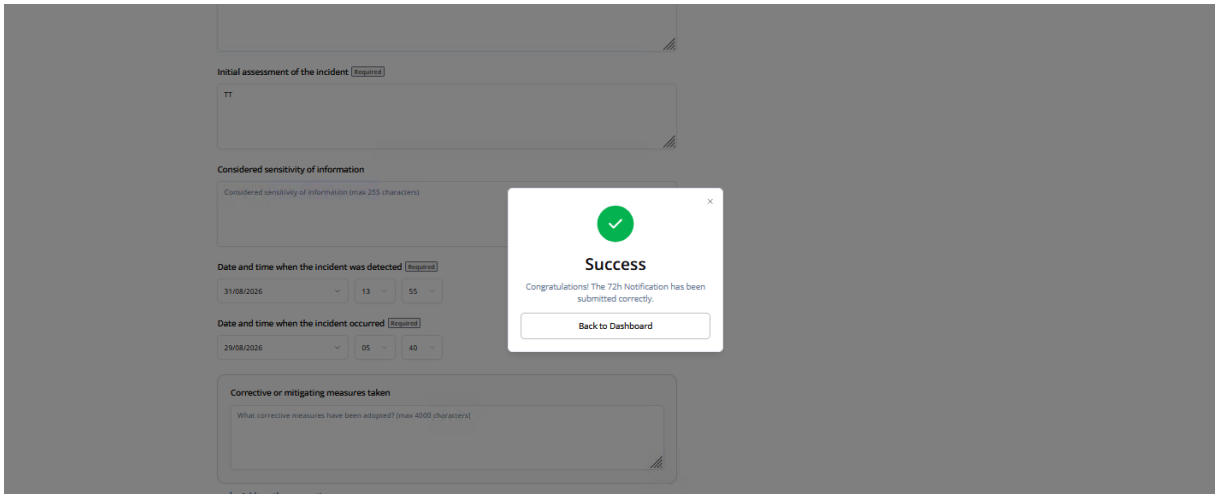


3. Optionally update the Additional Notes.

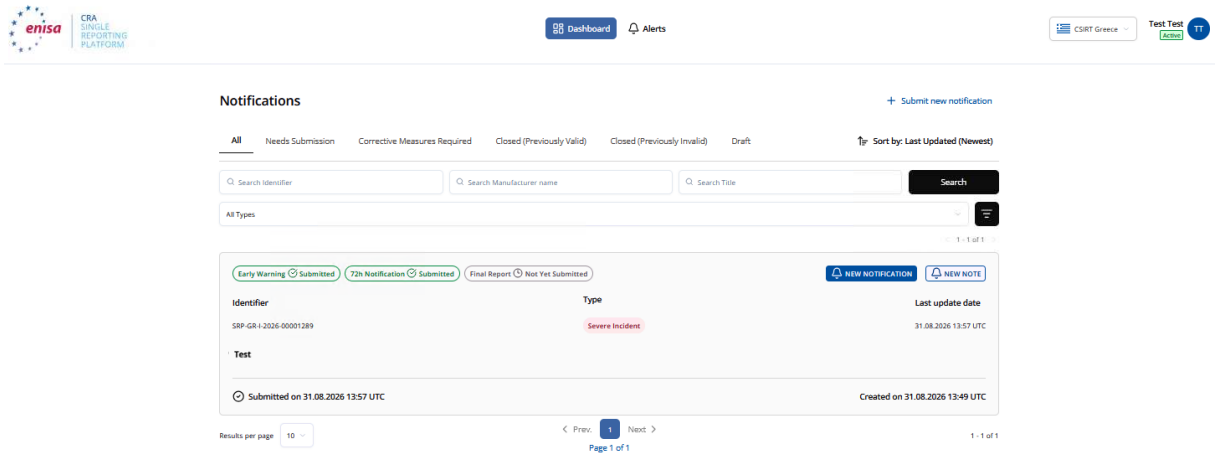
4. For an AEV only, where applicable, indicate whether “Particular Exceptional Circumstances” (PEC) apply. PEC is available only in the 72-hour Notification for an Actively Exploited Vulnerability (AEV).



5. Submit the 72-hour Notification or save it as a draft.



The notification is listed in the Dashboard (to be validated by the CSIRT):



Exceptions and error handling:

If required information is missing, the SRP displays an **error** identifying the information that must be provided before submission.

Expected result and system outcome: The 72-hour Notification is saved as a draft or submitted. If submitted, the notification is updated in the Dashboard and made available for CSIRT review in accordance with the applicable dissemination workflow.

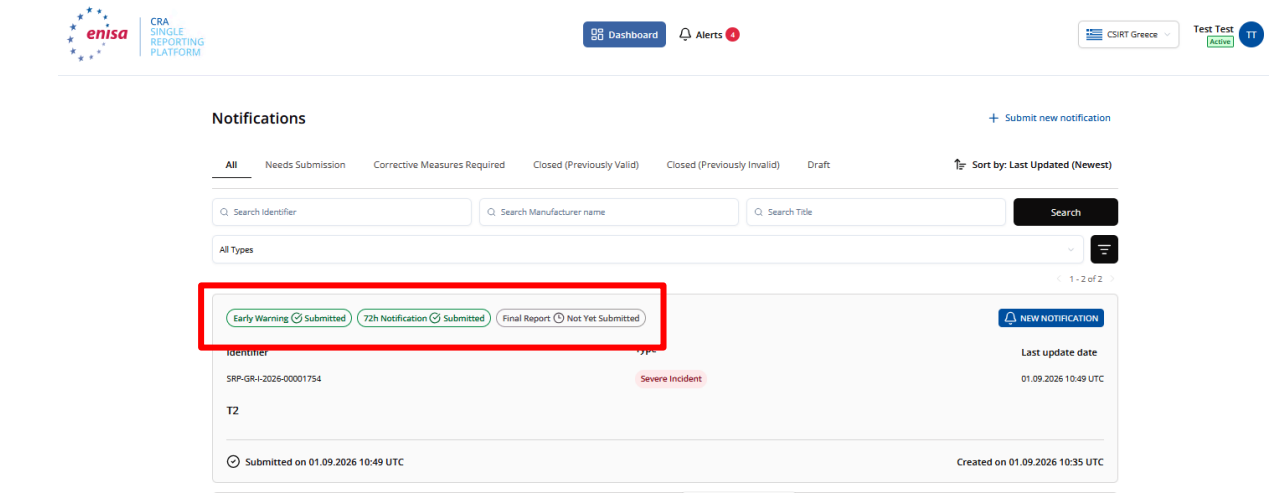
4.7.4 Submit Final Report

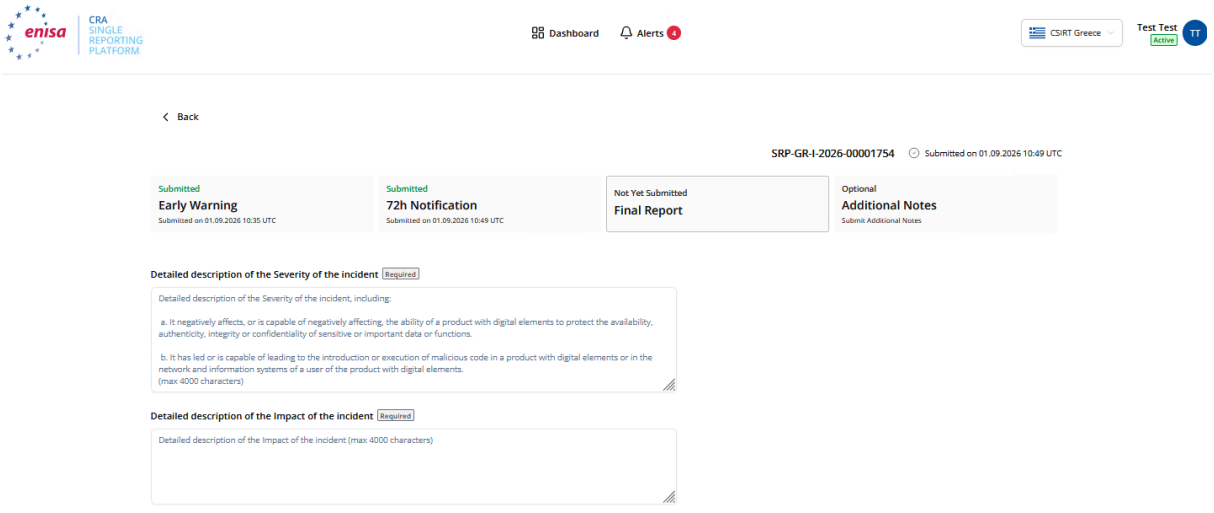
Purpose: Follow this procedure to submit the Final Report for an existing notification after the Early Warning and 72-hour Notification have been submitted.

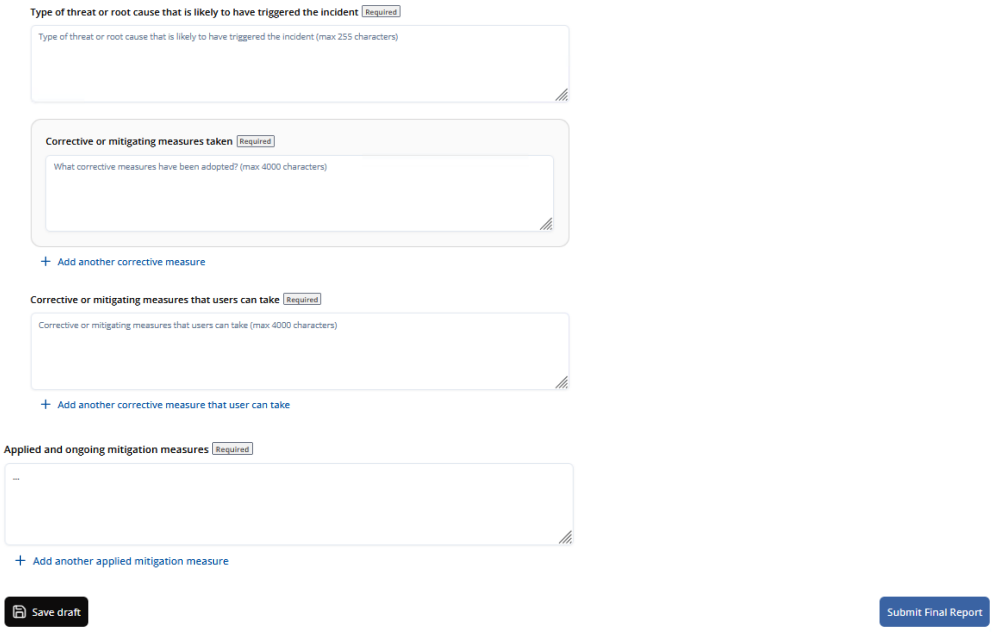
Pre-conditions: An Early Warning and a 72-hour Notification have already been submitted through the SRP.

Steps:

1. Open the existing notification from the Dashboard.



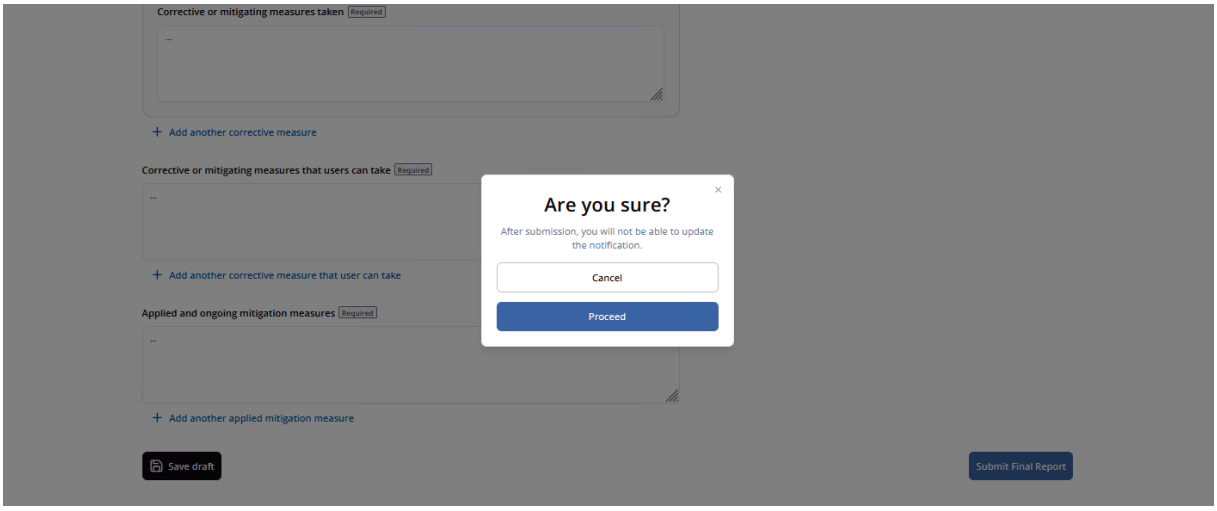


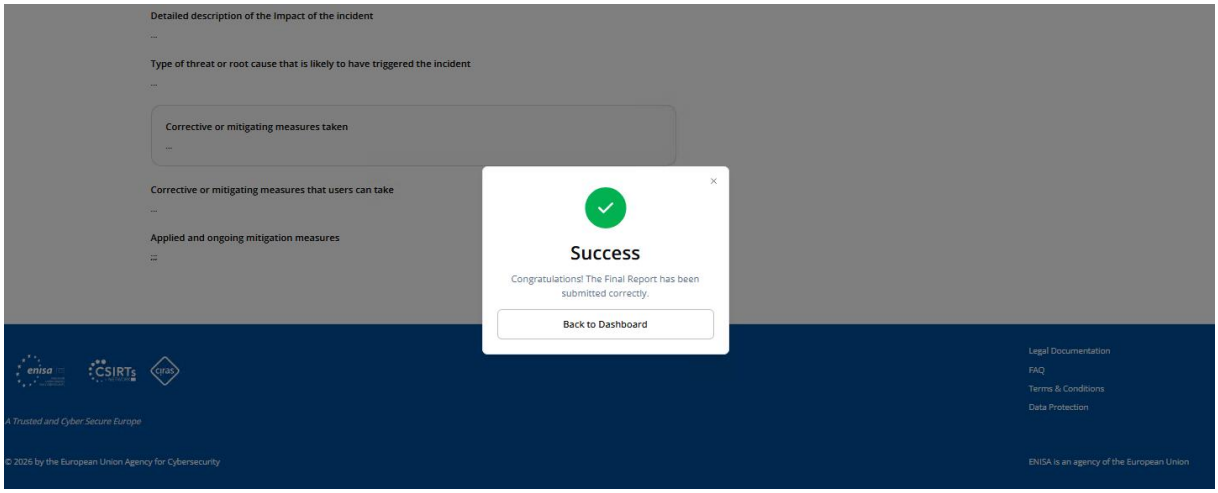


2. Complete the required fields and any relevant optional fields needed in the Final Report tab. Some fields that were optional in the Early Warning and 72hrs Notification stages may now be required or mandatory if the information is available.

3. Optionally update the Additional Notes field.

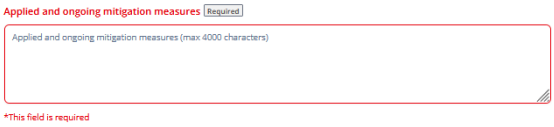
4. Submit the Final Report or save it as a draft.



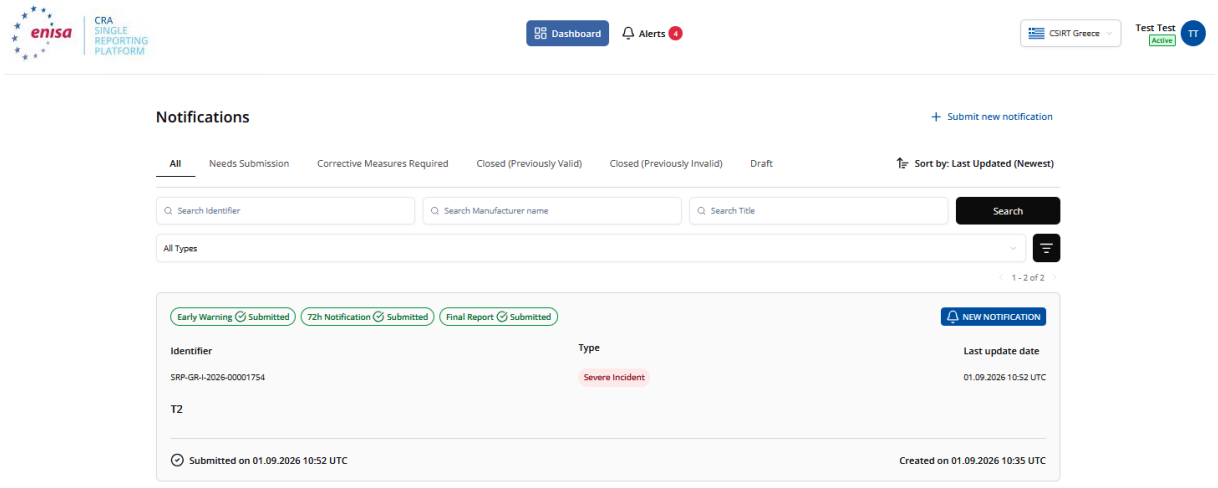


Exceptions and error handling:

If required information is missing, the SRP displays an **error** identifying the information that must be provided before submission.



5. After all reports have been submitted, verify that the progress bar displays the completed icons for each submitted step.



Expected result and system outcome:

- **Draft:** The notification remains in "Draft" status and is visible only to the AR who created it.
- **Early Warning**: Once submitted, the Early Warning is made available to the designated CSIRT for review. The SRP sends an email and alert to the designated CSIRT and a

confirmation email and alert to the submitting AR. The Early Warning is simultaneously made available to ENISA, unless a dissemination delay applies according to the workflow. The notification status is updated to “EW Submitted” and the report sub-state to “Early Warning”.

- **72-hour Notification**: Once submitted, the notification status is updated to “72h Submitted” and the report sub-state to “72h Notification”. The 72-hour Notification is made available to the designated CSIRT for review. ENISA is simultaneously given access to the notification unless PEC has been invoked. Where PEC is invoked, the dissemination status becomes “72h Submitted under PEC”; ENISA receives the PEC reasons, while access to the 72-hour Notification content remains delayed according to the applicable dissemination decision. Other concerned CSIRTs receive access to the 72-hour Notification or to PEC-related information only where this is allowed by the dissemination decision taken by the designated CSIRT.
- **Final Report**: Once submitted, the notification status is updated to “FR Submitted” and the report sub-state to “Final Report”. The Final Report is made available to the designated CSIRT for review and is no longer editable by the AR. ENISA receives access to the Final Report in accordance with the standard SRP workflow, while other concerned CSIRTs receive it following dissemination by the designated CSIRT.

4.8 Update Existing Notification

Purpose: Follow this procedure to update an existing notification for an actively exploited vulnerability (AEV) or severe incident (SI).

Pre-conditions:

- Your user status is “Active” and you are logged in to the SRP.
- A notification has previously been submitted or saved as a draft by you.
- The notification is not closed.
- The Final Report has not been submitted, because the notification becomes non-editable to the AR after Final Report submission.

Steps:

1. Open the notification and update the necessary fields in the applicable report tab.
2. Click “Update” to save the modified notification information.

Exceptions and error handling:

If you omit required information and click “Update”, the SRP displays an **error** identifying the information that must be provided, as described in Sections 4.7.1, 4.7.2, or 4.7.3.

Notifications: The SRP automatically notifies the designated CSIRT via an alert. Where applicable under the dissemination workflow, ENISA and concerned CSIRTs that already have access to the notification are also alerted to the update.

Expected result and system outcome:

Stored Data and “read-only” visibility:

- For **SI Notifications** (regardless of the Notification state, Early Warning, 72h Notification, Final Report):

  - If the Notification has not yet been disseminated by the designated CSIRT, the updated notification data (all fields) are automatically stored only in the SRP National Endpoint Data Layer and remain only visible to the designated CSIRT.
  - If the notification has already been disseminated to concerned CSIRTs by the designated CSIRT, the updated notification data (all fields) are automatically stored in the SRP ENISA Master Data Layer and automatically made visible to ENISA and the concerned CSIRTs.
- For **AEV Notifications**:
  - If the Notification has not yet been disseminated by the designated CSIRT, the updated notification data (all fields) are automatically stored only in the SRP National Endpoint Data Layer and remain only visible to the designated CSIRT.
  - If the notification has already been disseminated by the designated CSIRT, with delay not applied to at least ENISA and/or one concerned CSIRT, please refer to the Disseminate Notification (AEV) by designated CSIRT scenario for additional details.

The state of a successfully submitted notification is updated to "Submitted". An email and an alert are sent to you to inform you of the update. An email and an alert are also sent to the recipient of the notification (designated CSIRT and additional involved parties, if the notification has been disseminated to them) to inform them of the update.

In case the update was cancelled, or required fields were not provided, the information is not stored in the system.

4.9 View Reminders and Alerts

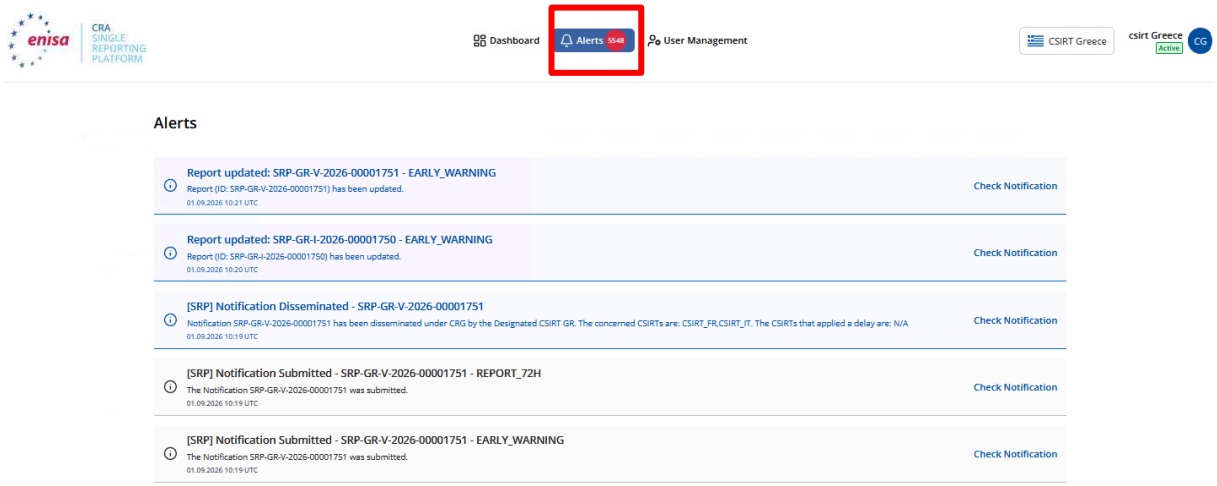
Purpose: Follow this procedure to review reminders and alerts generated by the SRP for actions requiring your attention.

Pre-conditions:

- You have an EU Login account and are registered on the SRP.

Steps:

1. Open the **Alerts** tab.



Notes: Alerts are triggered by actions requiring AR user attention. Light blue alerts are unread. When an alert is opened, it is automatically marked as read and it turns grey. Red alerts appear only for critical actions, such as when a CSIRT invalidates a submission.

Expected result and system outcome: The selected alert is marked as read and its details are displayed for review.

SECTION 5

Frequently Asked Questions

5. Frequently Asked Questions

General SRP FAQs can be found here: https://www.enisa.europa.eu/topics/product-security/single-reporting-platform-srp/frequently-asked-questions

What should I do if I cannot log in?
Verify the selected role and authentication method. If the issue persists, contact support with your role, email address, and error message.

Why can I not see a notification in my Dashboard?
The notification may not be accessible to your role, filters may be applied, or the notification may have been created by another user.

Can a Secondary AR submit notifications?
Yes, if the platform configuration, role, and association status allow it.

What happens when an AR association is pending?
The designated CSIRT must review and approve or reject the association. You will still be able to submit notifications up to a certain limit.

Can a notification be updated after the Final Report?
Notifications become non-editable after Final Report submission by an AR.

Who receives alerts when a notification is submitted or updated?
The submitting AR, the designated CSIRT, ENISA, and, where applicable, concerned CSIRTs receive alerts depending on the notification status and dissemination status.

What is PEC used for?
PEC is used to delay dissemination under particularly exceptional circumstances, subject to justification and CSIRT decision.

What is CRG used for?
CRG supports dissemination decisions based on cybersecurity-related grounds, including full or partial information sharing.

How do I know whether I am Primary AR or Secondary AR?
Your AR role depends on how your association with the manufacturer was created. A Primary AR is the main administrative representative for the manufacturer in the SRP. The Primary AR can manage the manufacturer association, invite or remove Secondary ARs, submit, view and update notifications, and perform other administrative functions available to that role. A Secondary AR is associated with the manufacturer following an invitation from the Primary AR. A Secondary AR may submit and update notifications for the manufacturer but does not have the same administrative permissions as the Primary AR. A Secondary AR may also claim the Primary AR role, subject to review and approval by the designated CSIRT. Both Primary and Secondary ARs can open, review, and edit the notification(s) associated with their manufacturer. You can check your current AR role and manufacturer association status in the Settings > Association Management.

How do I know whether my notification was validated?
Check the notification status in the Dashboard or in the notification details. When the designated CSIRT validates the notification, the status is updated to “Valid”, and the SRP sends the relevant alert or email notification according to the workflow.

What does it mean when a notification is Valid, Invalid, Closed, or Submitted?
“Submitted” means the notification has been sent through the SRP and is available for the next workflow step. “Valid” means the designated CSIRT has reviewed and accepted the notification. “Invalid” means the designated CSIRT has reviewed the notification and marked it as not valid. “Closed” means no further action is expected for that notification in the current workflow.

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14
Chalandri 15231, Attiki, Greece

Brussels Office
Rue de la Loi 107
1049 Brussels, Belgium

enisa.europa.eu

Publications Office
of the European Union