Validate and Categorize the Incident

At A Glance

Incident Management Process

Log a Incident → Categorize a Incident → Investigate and Diagnose → Resolve and Recover → Validate and Close

Validate and Categorize the Incident

Purpose

Validating Incident information ensures that all required information has been provided and documented properly in the record in order to allow timely investigation and diagnosis of the issue. Incidents that are accurately categorized become useful future input element for various IT service management processes (e.g. Problem Management and Knowledge Management).

1. Validate All Incident Information

- Special Handling Notes
- Priority
- Component
- EUDP Restriction
- Attachment

2. Create Service Request (if necessary)

2a Create Service Request record via Incident

2b Fill in mandatory fields in the Service Request record

2c Save the record

Available in future release

Notes

An Escalation record can be attached to a Incide in the situation of a case escalation.

The trigger of case escalation management process can be done at later stages of Incident management too.

When validating an incident, it may be necessary to document how to reproduce the issue. How to reproduce the issue reported (if necessary) can be found at this LINK

1. Validate All Incident Information

Incident Management

Notes

Special Handing notes can be viewed but not modified.

Special handling notes

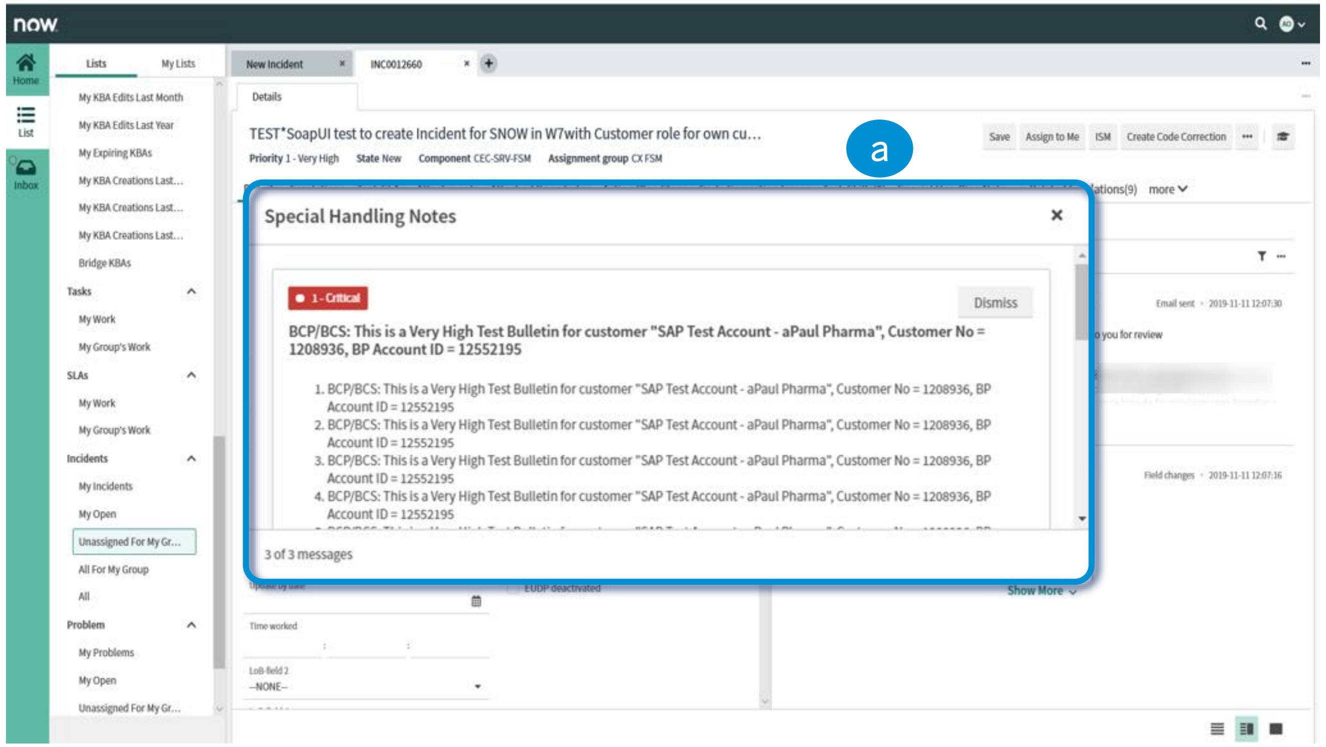
Whenever the Incident record is opened, the Special Handling Notes are displayed in the pop-up window. These notes provide specific requirements or agreements regarding the requestor, system installation, handling restrictions, etc. that are relevant for the incident handling.

Step 1

Scroll to check all messages for additional instructions on the special handling of this Incident. You may also check the information in the **Special Handling Notes** tab.

Option A: Check Special Handling Notes in the pop-up window

All special handling notes are listed in the pop-up window.



TEST*SoapUI test to create Incident for SNOW in W7with Customer role for own cu...

Priority 1 - Very High State New Component CEC-SRV-FSM Assignment group CX FSM

Special Handling Notes

● 1 - Critical

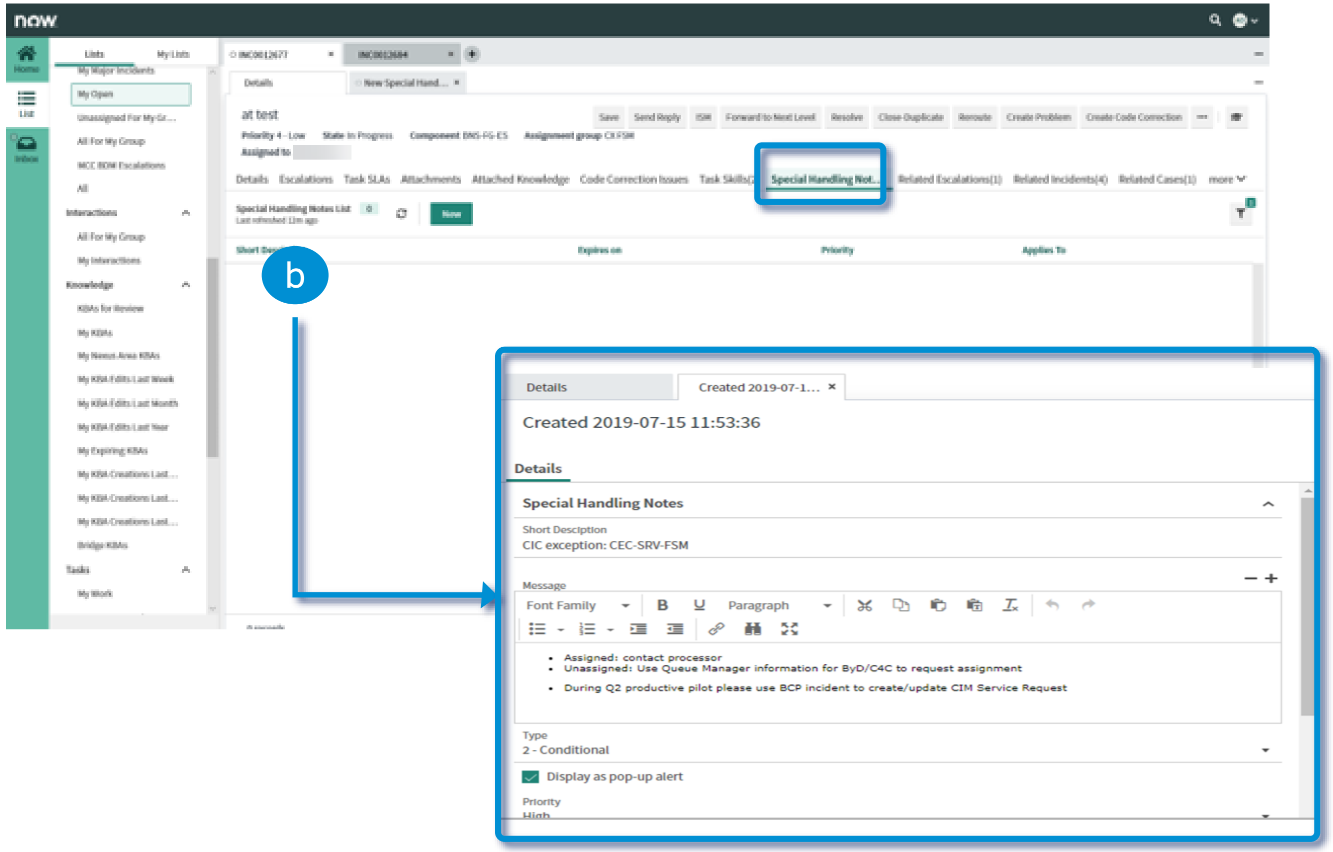
BCP/BCS: This is a Very High Test Bulletin for customer "SAP Test Account - aPaul Pharma", Customer No = 1208936, BP Account ID = 12552195

1. BCP/BCS: This is a Very High Test Bulletin for customer "SAP Test Account - aPaul Pharma", Customer No = 1208936, BP Account ID = 12552195
2. BCP/BCS: This is a Very High Test Bulletin for customer "SAP Test Account - aPaul Pharma", Customer No = 1208936, BP Account ID = 12552195
3. BCP/BCS: This is a Very High Test Bulletin for customer "SAP Test Account - aPaul Pharma", Customer No = 1208936, BP Account ID = 12552195
4. BCP/BCS: This is a Very High Test Bulletin for customer "SAP Test Account - aPaul Pharma", Customer No = 1208936, BP Account ID = 12552195

3 of 3 messages

Option B: Check Special Handling Notes the Special Handling Notes tab

Click each of the special handling notes listed down in the **Special Handling Notes** tab to view the individual content.



Created 2019-07-15 11:53:36

Details

Special Handling Notes

Short Desciption
CIC exception: CEC-SRV-FSM

Message

- Assigned: contact processor
- Unassigned: Use Queue Manager information for ByD/C4C to request assignment
- During Q2 productive pilot please use BCP incident to create/update CIM Service Request

Type
2 - Conditional

☑ Display as pop-up alert

Priority
High

1. Validate All Incident Information

Incident Management

Priority

When the Incident has a Priority of 1 – Very High or 2 – High, Be sure to verify the priority from the Description field.

Description field is only editable during creation. Once the incident is created it is not possible to add any comment into the Description.

Notes

Priority is the urgency of the issue reported in the Incident. It is determined and assigned by the incident Creator. However, Priority can be changed by the reporter or the Support Engineer if necessary.

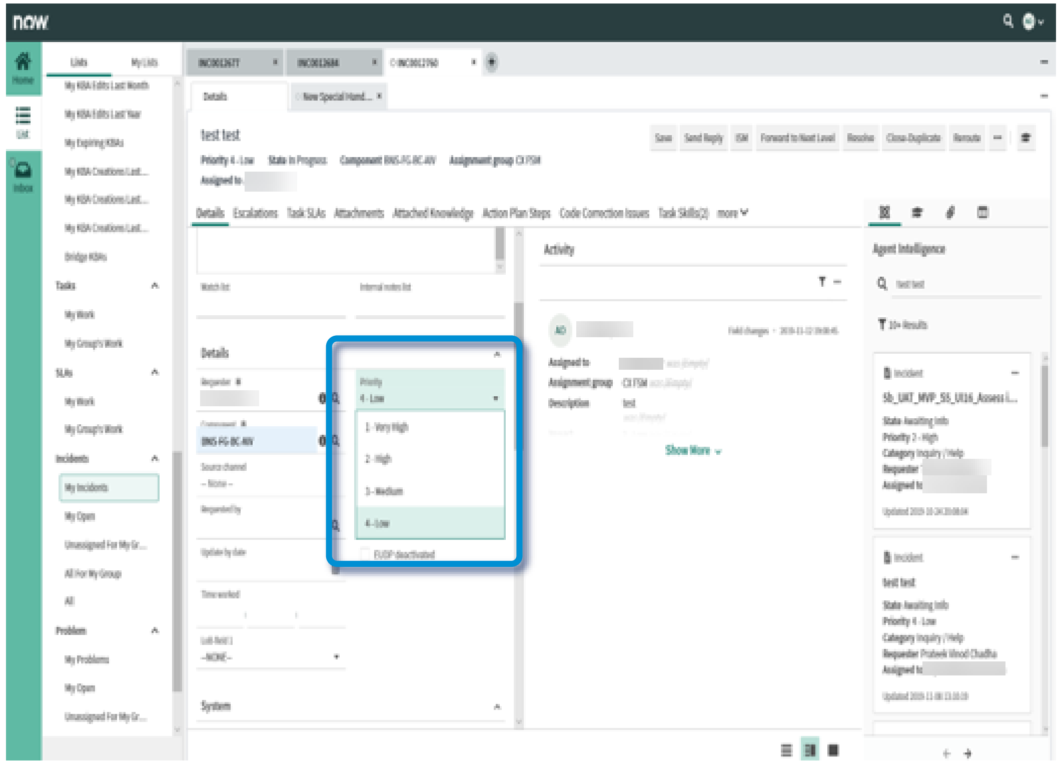
Priority is categorized in 4 levels:

- 1 – Very High
- 2 – High
- 3 – Medium
- 4 – Low

More information regarding priority levels can be found in next two slides

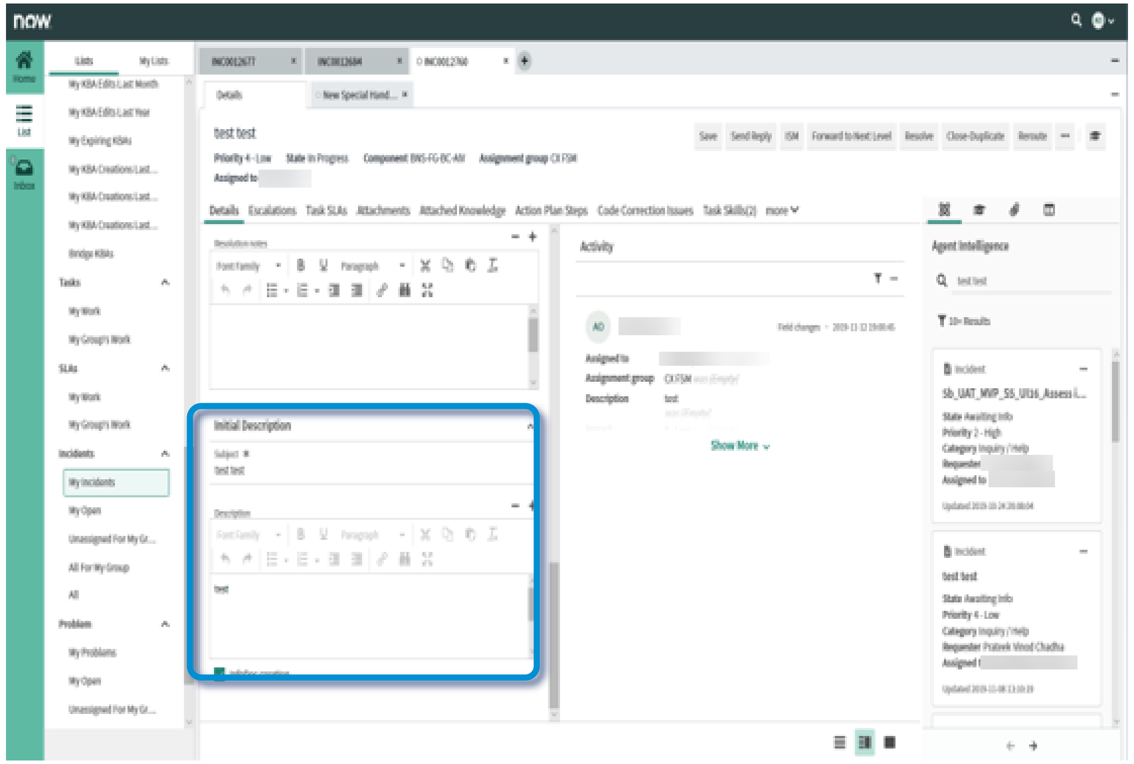
Step 1

Check the **Priority**.



Step 2

Read the **Initial Description** to understand the issue. Validate that the appropriate priority is set.



1. Validate All Incident Information

Incident Management

What is Priority?

Priority is the urgency of the issue reported in the Incident. It is determined and assigned by the Incident Creator. However, Priority can be changed by the reporter or the Incident Processor if necessary.

What are the 4 levels of Priority?

1 – Very High

- Problem with **very serious consequences** for normal business processes or IT processes related to **core business processes**.
- **Urgent** work cannot be performed.
- This is generally caused by one of more of the following circumstances:
  - A productive system is completely down;
  - The imminent system go-live or upgrade of a production system cannot be completed;
  - The customer's or requestor's core business processes are seriously affected;
  - A workaround is not possible for each of the circumstances mentioned above.
- The issue **requires immediate processing** because the malfunction **may cause serious losses**.
- In case of go-live or upgrade, the reason to delay go-live or upgrade must be one that would cause serious losses if not resolved beforehand.

2 – High

- **Normal** business processes are **seriously** affected.
- **Necessary** tasks cannot be performed.
- Issue is caused by incorrect or inoperable functions in the SAP system that **are required immediately**.
- The issue is **to be processed as quickly as possible** as a continuing malfunction can **seriously disrupt** the entire productive business flow.

3 – Medium

- **Normal** business processes are affected.
- The problem is caused by incorrect or inoperable functions in the SAP system.

4 – Low

- The problem has **little or no effect** on normal business processes.
- The problem is caused by incorrect or inoperable functions in the SAP system that are **rarely used or not required daily**.

1. Validate All Incident Information

Incident Management

What scenarios are considered as 1 – Very High?

Scenario / Business Impact	Explanation
A productive system is completely down	▪ The entire system is technically down and cannot be brought back up ▪ System goes down multiple times a day requiring restarts resulting in disruption of the core business process ▪ Core business process is down without any feasible workaround.
The imminent system go-live or upgrade of a production system (as relates to an SAP system) can't be completed	▪ Key Milestone (including Go / No Go decision for a project phase) is to happen in the next 5 business days and the customer is losing money as a result of a potential delay to the project. ▪ For test and quality systems very high priority will only be justified in the situations where they can jeopardize a production system ▪ Customers/Requestor should be given the benefit of doubt and any ambiguity around the imminent Go-live definition should be addressed to the responsible person in the region where the customer/requestor is located
The customer's core business processes are seriously affected	▪ A business process that can result in significant financial loss or legal ramifications if it cannot be executed on time (example: Shipping, Billing, Payroll)
And for each circumstance a feasible workaround is not available	▪ A workaround is considered feasible if it requires only minimal level of manual intervention from the customer for the short term ▪ An example of this would be utilizing a different business process to achieve the same end result, rescheduling the job to a different server/time of the day, etc. ▪ A workaround is not considered feasible if it requires the use of processes outside of an SAP system

1. Validate All Incident Information

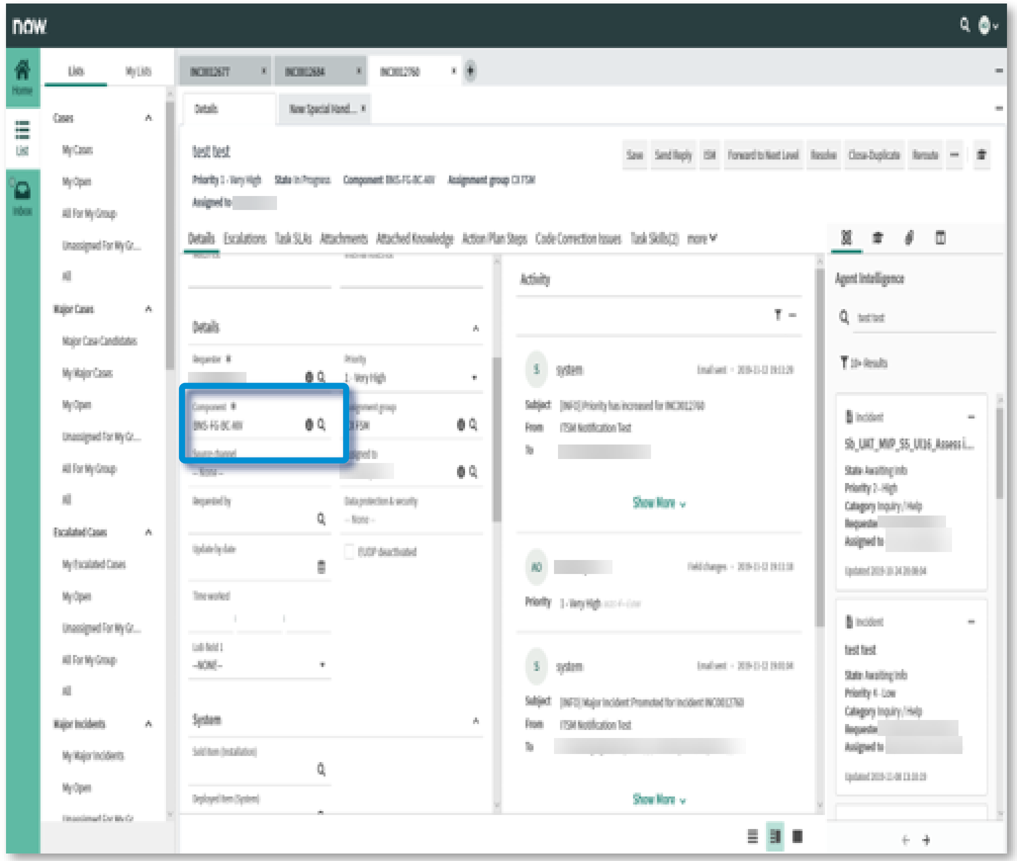
Incident Management

Component

1a Check the original component provided by the requestor and prepare handover information if adjustment is needed

Step 1

Based on the information provided in the Incident check whether the correct component has been chosen by the requestor.



test test

Priority 1 - Very High State In Progress Component BNS-FG-BC-AIV Assignment group CX FSM

Assigned to

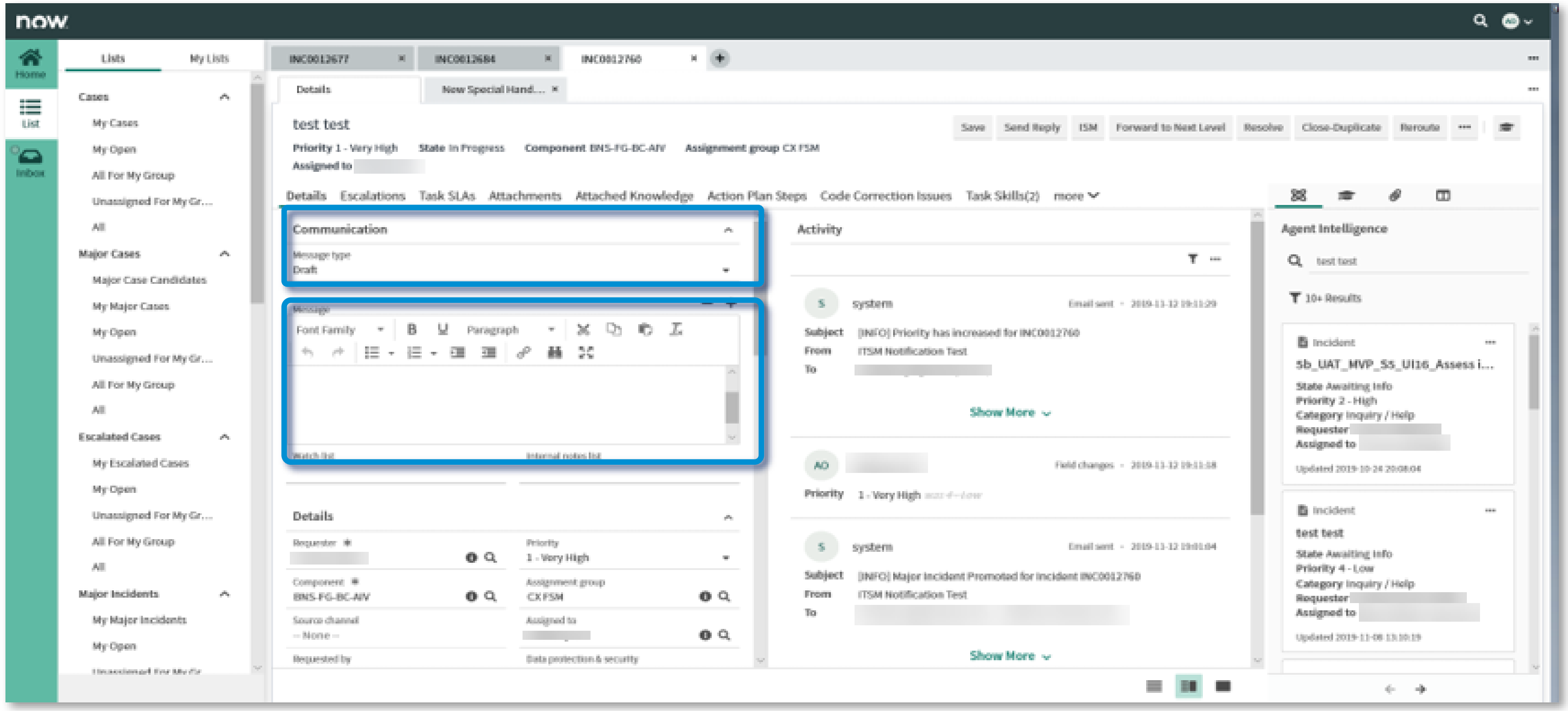
Component BNS-FG-BC-AIV

Step 2 (if applicable)

Based on the initial analysis, if the Incident processor decides that the component needs to be changed, Incident processor should document the findings in the **Message** field and choose the **Message type** as **Internal Info**.

Recommendation is to provide at least the following information :

- Issue description in your own words
- System details (where available or already documented in Incident)
- Recreate previous steps to analyze/ reproduce the issue



test test

Priority 1 - Very High State In Progress Component BNS-FG-BC-AIV Assignment group CX FSM

Assigned to

Message type: Draft

system — Email sent • 2019-11-12 19:11:29
Subject [INFO] Priority has increased for INC0012760
From ITSM Notification Test
To

AO — Field changes • 2019-11-12 19:11:18
Priority 1 - Very High

system — Email sent • 2019-11-12 19:01:04
Subject [INFO] Major Incident Promoted for Incident INC0012760
From ITSM Notification Test
To

Requester
Priority 1 - Very High
Component BNS-FG-BC-AIV
Assignment group CX FSM
Source channel -- None --
Assigned to
Requested by
Data protection & security

Incident
5b_UAT_MVP_S5_UI16_Assess i...
State Awaiting Info
Priority 2 - High
Category Inquiry / Help
Requester
Assigned to
Updated 2019-10-24 20:08:04

Incident
test test
State Awaiting Info
Priority 4 - Low
Category Inquiry / Help
Requester
Assigned to
Updated 2019-11-08 13:10:19

1. Validate All Incident Information

Incident Management

Component

1b Adjust the component

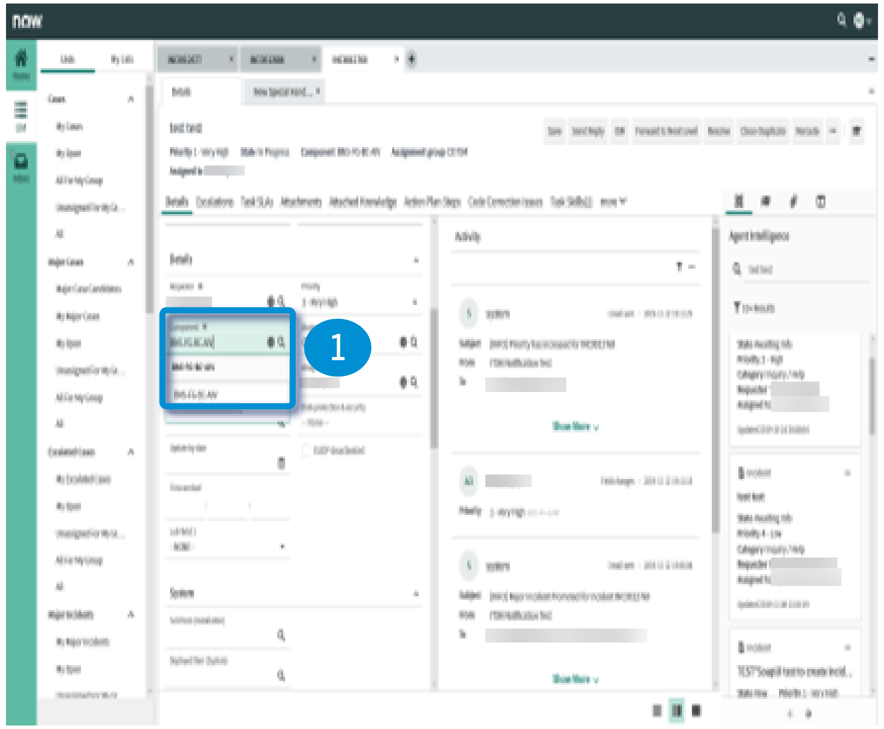
Step 1

Manually change the component to reassign the incident. This can be done either by directly typing the component name in the **Component** field, or by searching via the component list.

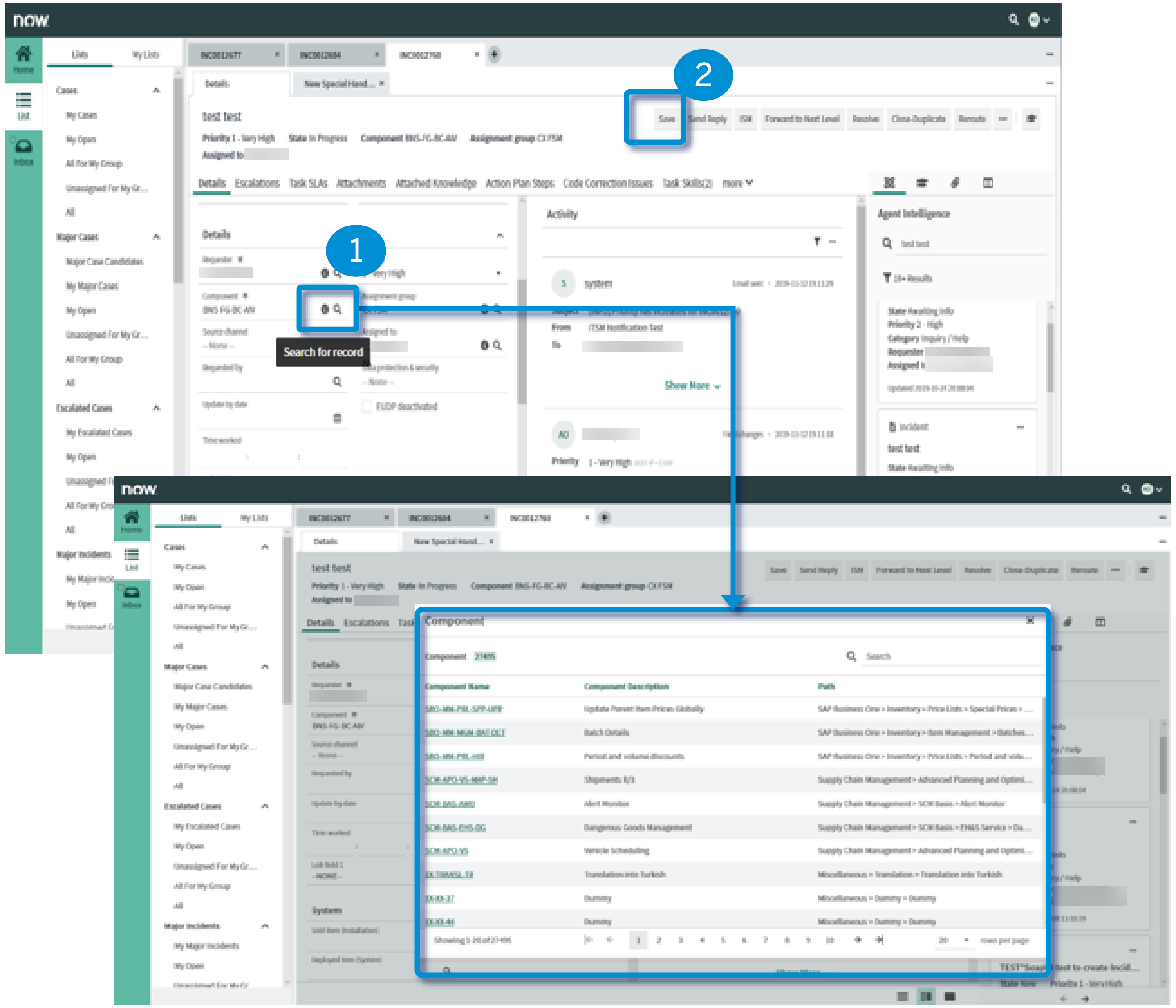
Step 2

Click **Save** to update the record. The **Assignment group** is automatically updated based on pre-defined routing rules.

Option A: Change component by typing the name in the field



Option B: Change component by searching via component list



Component

Component 27495

Component Name	Component Description	Path
SBO-MM-PRL-SPP-UPP	Update Parent Item Prices Globally	SAP Business One > Inventory > Price Lists > Special Prices > ...
SBO-MM-MGM-BAT-DET	Batch Details	SAP Business One > Inventory > Item Management > Batches...
SBO-MM-PRL-HIR	Period and volume discounts	SAP Business One > Inventory > Price Lists > Period and volu...
SCM-APO-VS-MAP-SH	Shipments 8/3	Supply Chain Management > Advanced Planning and Optimi...
SCM-BAS-AMO	Alert Monitor	Supply Chain Management > SCM Basis > Alert Monitor
SCM-BAS-EHS-DG	Dangerous Goods Management	Supply Chain Management > SCM Basis > EH&S Service > Da...
SCM-APO-VS	Vehicle Scheduling	Supply Chain Management > Advanced Planning and Optimi...
XX-TRANSL-TR	Translation into Turkish	Miscellaneous > Translation > Translation into Turkish
XX-XX-37	Dummy	Miscellaneous > Dummy > Dummy
XX-XX-44	Dummy	Miscellaneous > Dummy > Dummy

Showing 1-20 of 27495 · 1 2 3 4 5 6 7 8 9 10 · 20 rows per page

1. Validate All Incident Information

Incident Management

EUDP Restriction

EUDP Remote Access restrictions do NOT apply to employees that are physically located within the EU and EFTA areas.

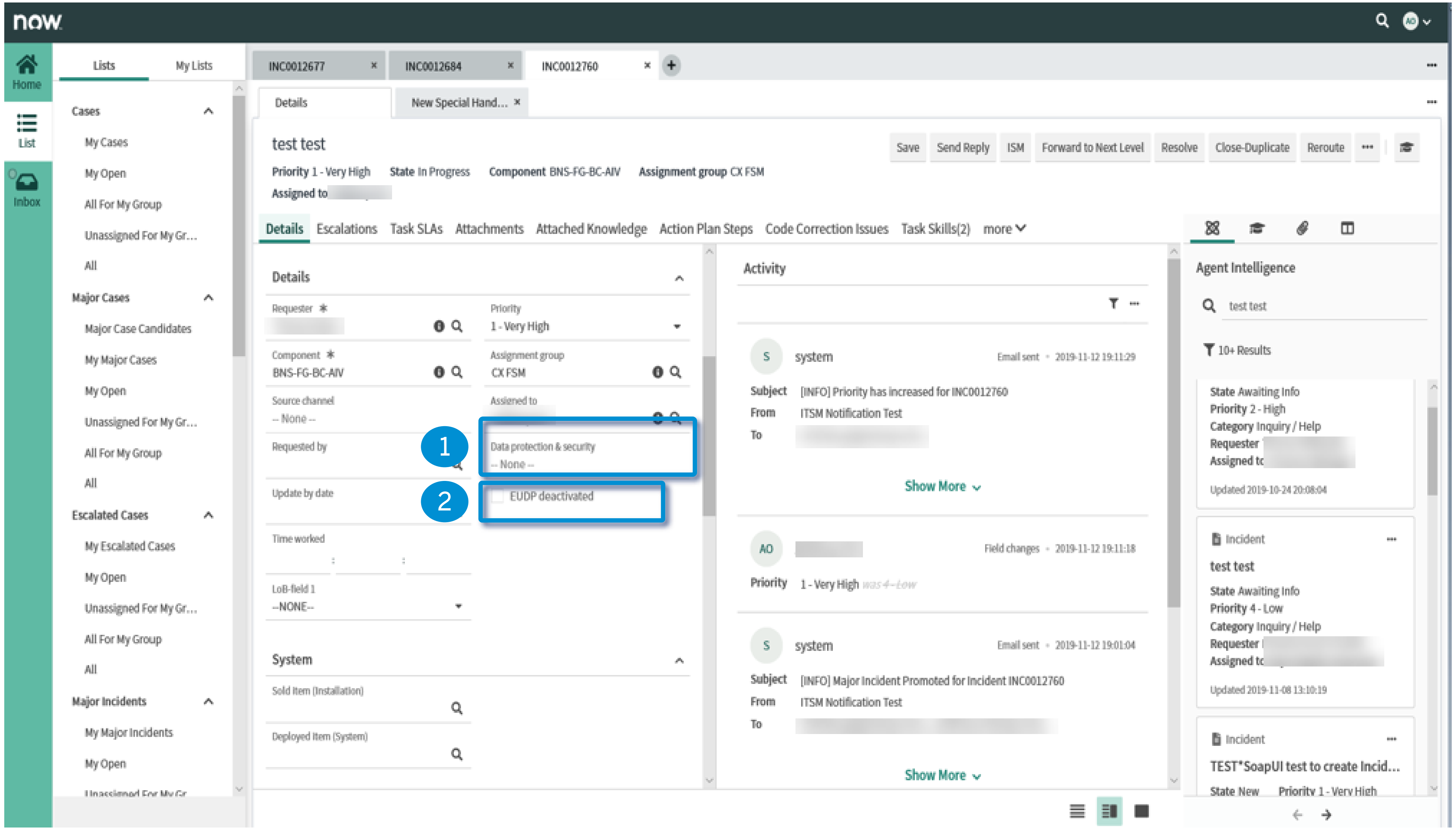
Step 1

The type of **Data protection & security** is displayed in the **System** section and is prefilled by the Installation.

Step 2 (if necessary)

In case of emergency and the requestor requires immediate support, the Incident processor can request the requestor deactivate the EUDP restriction.

Once the requestor deactivates the restriction, the **EUDP deactivated** box will be automatically checked.



test test

Priority 1 - Very High State In Progress Component BNS-FG-BC-AIV Assignment group CX FSM

Assigned to [redacted]

Details

Requester * [redacted]

Priority: 1 - Very High

Component * BNS-FG-BC-AIV

Assignment group: CX FSM

Source channel: -- None --

Assigned to

Requested by

Data protection & security: -- None --

Update by date

□ EUDP deactivated

Time worked

LoB-field 1: --NONE--

System

Sold Item (Installation)

Deployed Item (System)

Activity

S system — Email sent • 2019-11-12 19:11:29
Subject [INFO] Priority has increased for INC0012760
From ITSM Notification Test
To [redacted]

AO [redacted] — Field changes • 2019-11-12 19:11:18
Priority 1 - Very High ~~was 4 - Low~~

S system — Email sent • 2019-11-12 19:01:04
Subject [INFO] Major Incident Promoted for Incident INC0012760
From ITSM Notification Test
To [redacted]

Agent Intelligence

test test

10+ Results

State Awaiting Info
Priority 2 - High
Category Inquiry / Help
Requester [redacted]
Assigned to [redacted]
Updated 2019-10-24 20:08:04

Incident
test test
State Awaiting Info
Priority 4 - Low
Category Inquiry / Help
Requester [redacted]
Assigned to [redacted]
Updated 2019-11-08 13:10:19

Incident
TEST*SoapUI test to create Incid...
State New Priority 1 - Very High

Notes

As the Incident processor does not communicate with the customer for CASEs, then If the EUDP needs to be deactivated, the Incident processor would need to ask the Case processor to ask the customer for that

1. Validate All Incident Information

Incident Management

EUDP Restriction

Country Whitelist for Remote and Attachment Access

European Free Trade Association (EFTA) states (green):

- Liechtenstein
- Iceland
- Norway
- Switzerland

Member states of the European Union (blue):

- Austria
- Belgium
- Bulgaria
- Croatia
- Cyprus
- Czech Republic
- Denmark
- Estonia
- Finland
- France
- Germany
- Greece
- Hungary
- Ireland
- Italy
- Latvia
- Lithuania
- Luxembourg
- Malta
- The Netherlands
- Poland
- Portugal
- Romania
- Slovakia
- Slovenia
- Spain
- Sweden
- ~~United Kingdom~~

Notes

- EU DP Remote Access restrictions do basically not apply to employees physically located in one of the above countries.
- **Since the Brexit on January 31st 2020 the UK is not part of the EU anymore. However until Dec 31st 2020 the UK is in a transition period in which the remote access - & attachment handling rules keep the same for UK-based engineers.**

1. Validate All Incident Information

Incident Management

Attachment

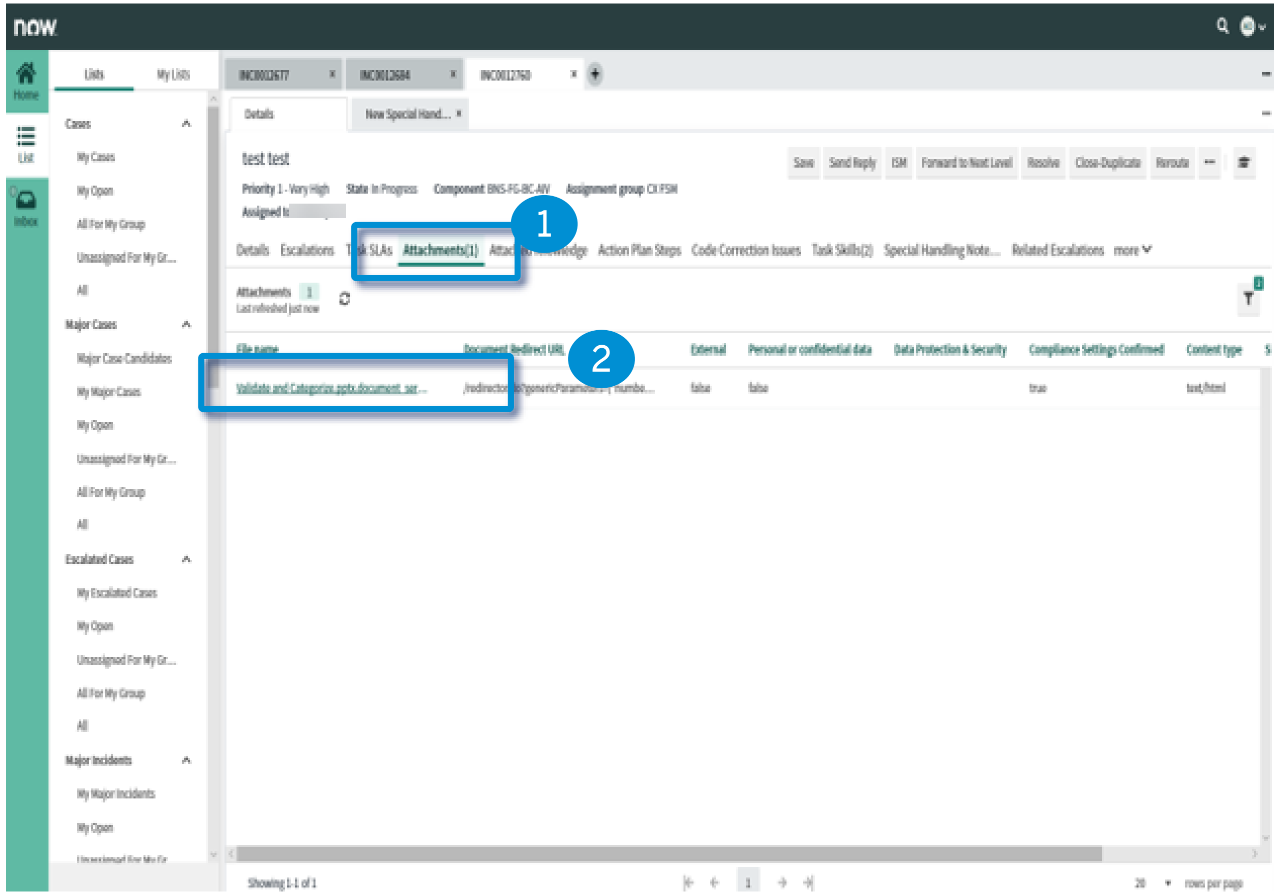
Files can be attached when creating the Incident to provide more information of the issue reported. The Incident processor needs to ensure that the attachments have been correctly classified.

GDPR Compliance

Please DO NOT use the attachment icon on the sidebar to download any file, as this does not require the data protection checkpoint through this path.

Step 1

Go to **Attachments** tab and click the **File name** to open the details of the attachment.



test test

Priority 1 - Very High State In Progress Component BNS-FG-BC-AIV Assignment group CX FSM

Assigned to [redacted]

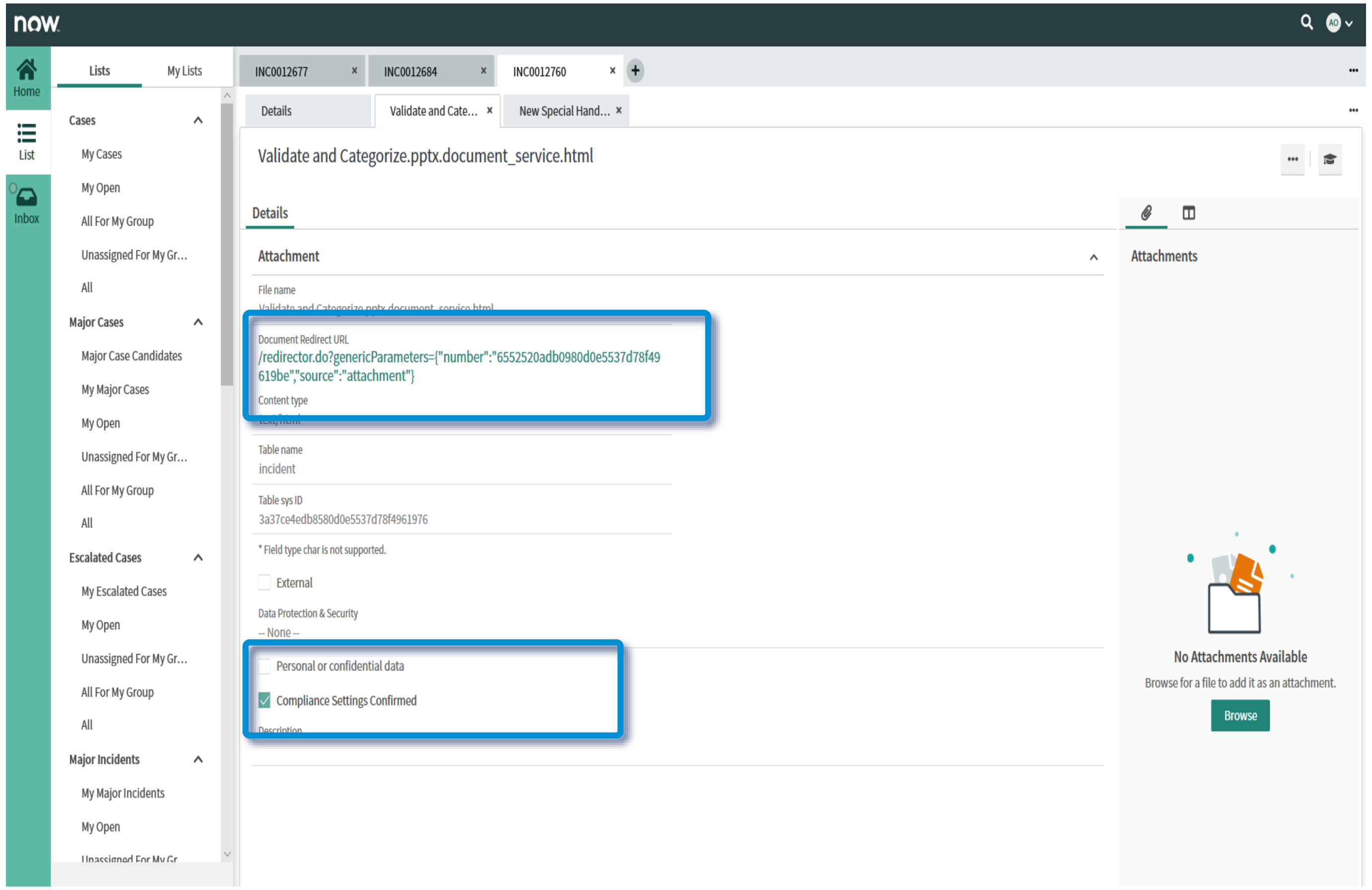
Attachments 1
Last refreshed just now

File name	Document Redirect URL	External	Personal or confidential data	Data Protection & Security	Compliance Settings Confirmed	Content type
Validate and Categorize.pptx.document_ser...	/redirector.do?genericParameters={"numbe...	false	false		true	text/html

Step 2

Click **Document Redirect URL** to open the attachment.

NOTE: Pay attention to the classification of **Personal or confidential data** and **Data Protection & Security** setting.



Validate and Categorize.pptx.document_service.html

Attachment

File name
Validate and Categorize.pptx.document_service.html

Document Redirect URL
/redirector.do?genericParameters={"number":"6552520adb0980d0e5537d78f49619be","source":"attachment"}

Content type
text/html

Table name
incident

Table sys ID
3a37ce4edb8580d0e5537d78f4961976

* Field type char is not supported.

□ External

Data Protection & Security
-- None --

□ Personal or confidential data

☑ Compliance Settings Confirmed

Description

2. Create Service Request (if necessary)

Incident Management

What is Service Request?

Service request is a formal request from a user for routine business function such as information and advice, standard change (e.g. password reset, workstation installation for new user), and access to IT services, using a predefined service catalog with approval steps. Service request does not include configuration change in the application.

Detailed work instructions on how to create Service Request will be available soon

Change Log

Case Management – Validate Information and Categorize the Case

What is a change log?

What you are reading is official SAP process documentation. Stringent version control is required for Compliance purposes. Thus, this **change log** is a record of who made what changes to this content & when, in case further follow up is needed.

Please send any questions or concerns to

Blanca Serrano, Madrid
Process Manager

Change Log

Version	Changed by	Date	Description of changes	Status
1.0.0	Anthony Orr	November 10, 2019	▪ WIPS 4.0 initial document -WIPS 4.0 Golden Standard Baseline Document	Released
1.0.1	Nádia Xavier	January 30, 2020	▪ Page 9: Added Brexit relevant information, updated the country whitelist and the map picture.	Released