Cisco – SMART Service Desk Integration Scope and Life Cycle – Case Study

Scope: To Integrate **Cisco TAC/Support Case Manager/Cisco Call Manager** with **SMART Service Desk** for Incident tickets created by Managed Service Providers and System Integrators.

Smart Bonding:

Smart Bonding is the process to connect SMART ServiceDesk to Cisco. The Smart Bonding middleware software offers a multitude of connection possibilities, so almost any kind of system with an API can be connected.

Technical Details:

SMART ServiceDesk has 2 way information exchange with Cisco Call Manager. Each party invokes the API provided by the other party.

Authentication:

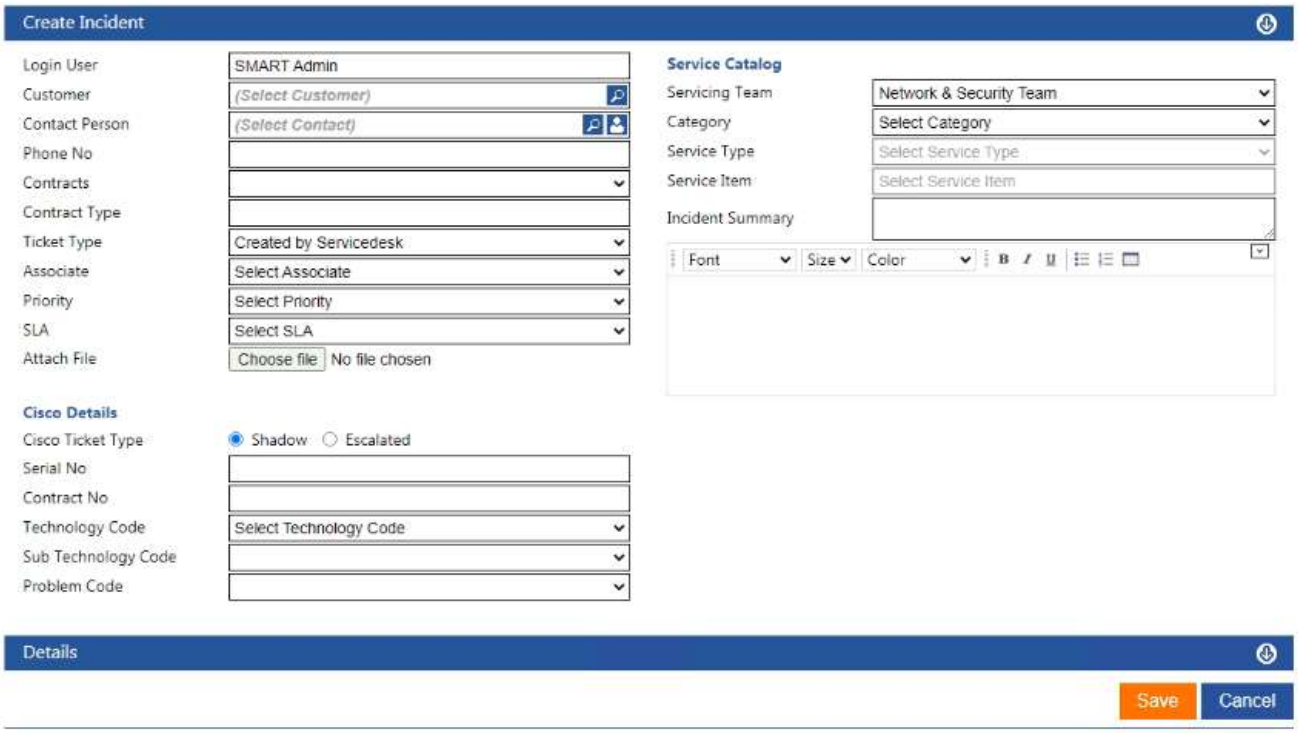
To authenticate with this API Cisco provides a username and password which will then be converted to a base64 encoded string that needs to be used to generate a token. SMART API is also authenticated with a user name and password which Cisco utilises for API access within.

Basic Authentication can be used for API accessing for both parties.

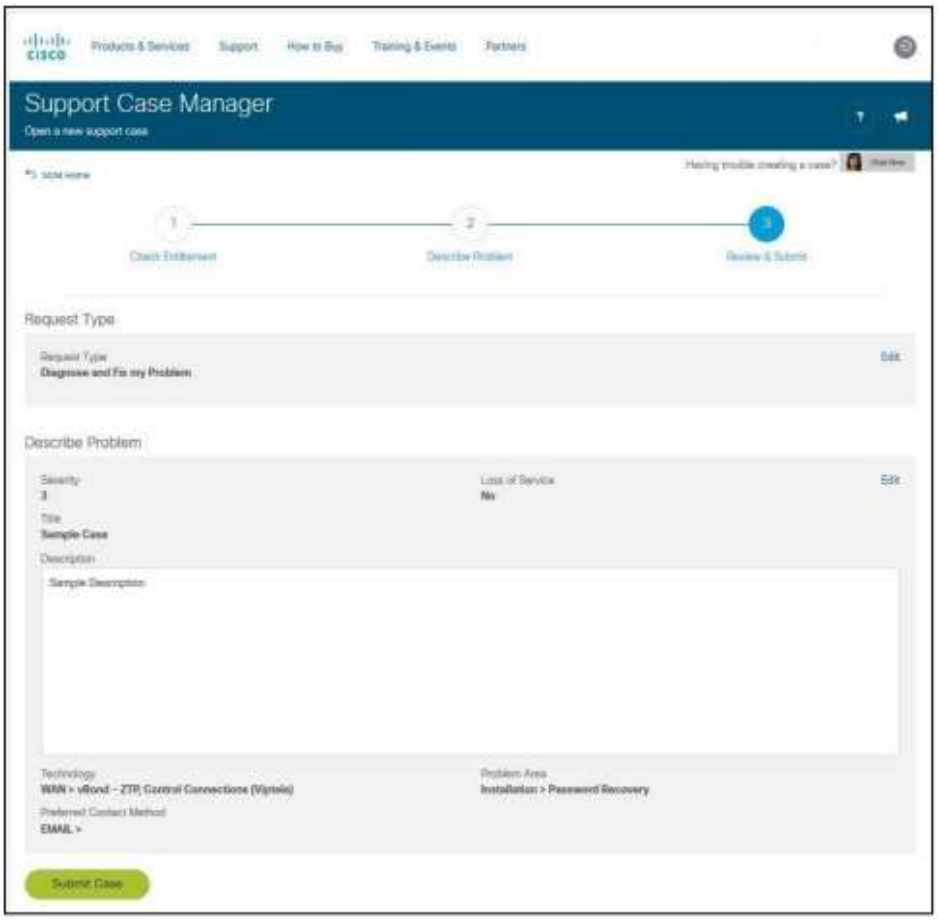
The Life Cycle of Incident ticket is as follows.

Basic Workflow (life cycle) of the ticket:

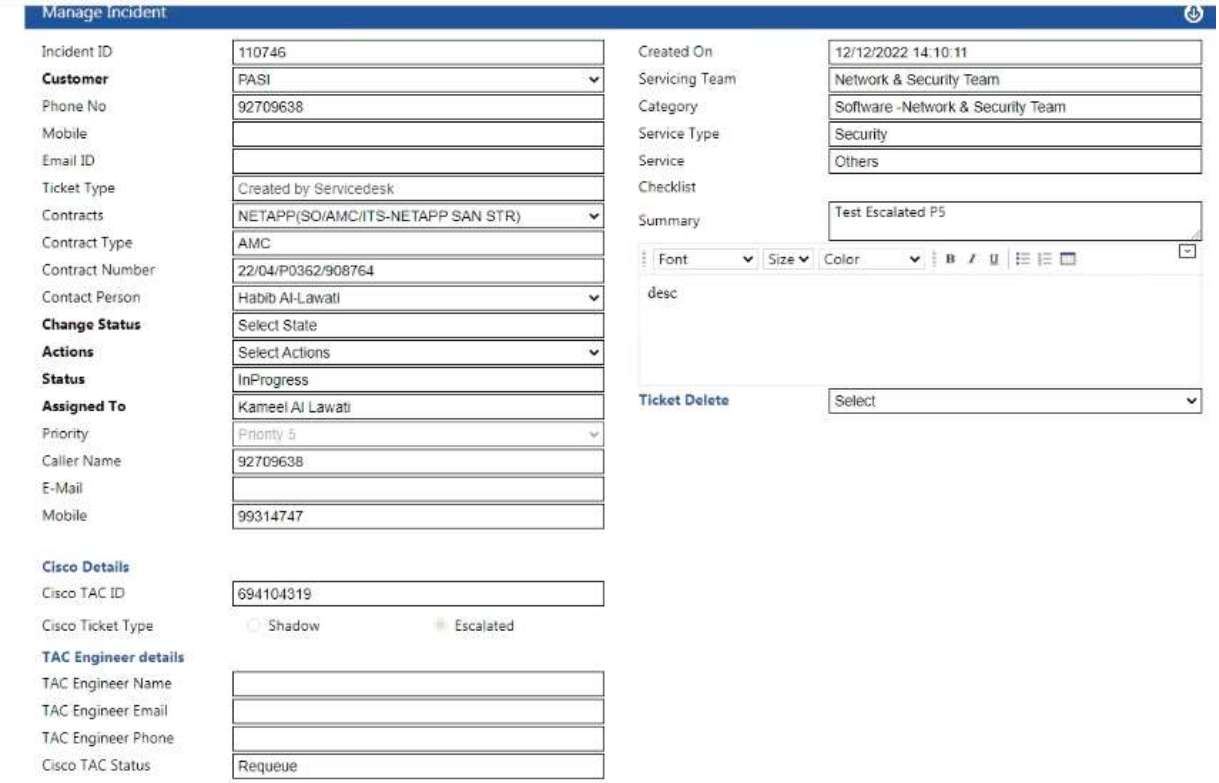
1. Case is escalated (created) in SMARTServiceDesk and pushed to Cisco



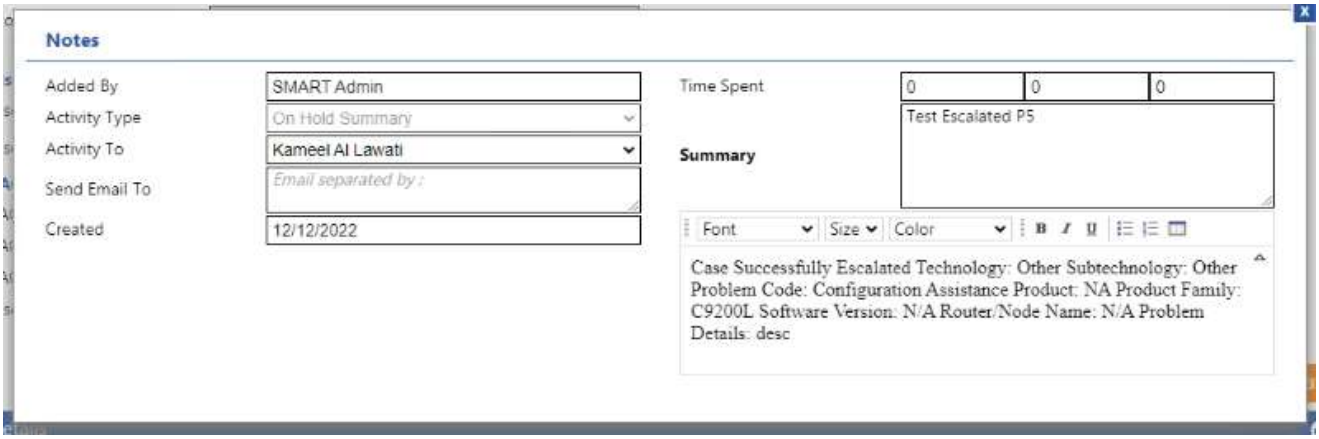
- Shadow or Escalated are the options given and one option can be selected.
- Contract and Serial numbers are mandatory to enter.
- Rest of the fields can be selected depending upon the requirement.
- A message is received as response from Cisco that will state in the remarks 'Message received successfully'.



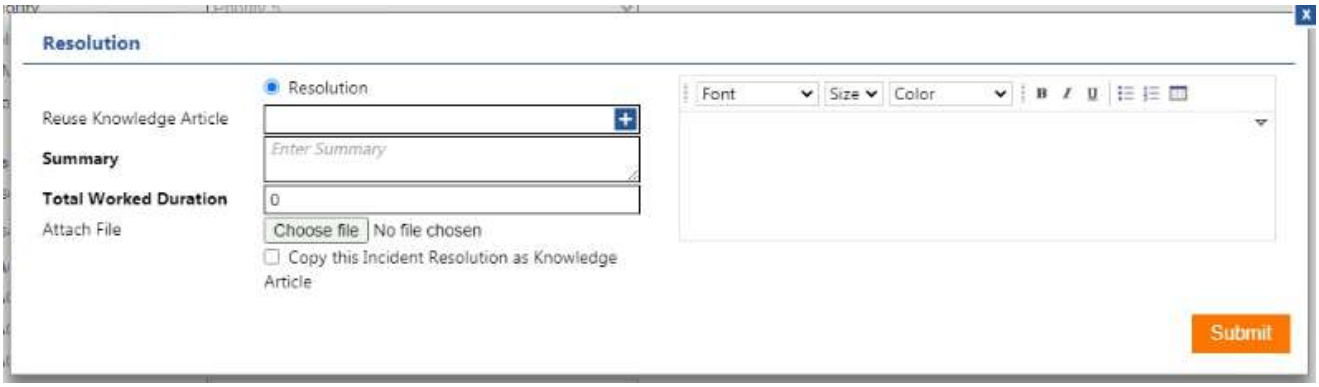
2. Case is set to 'Resolved' in Manage Page after the successful ticket escalation message is received



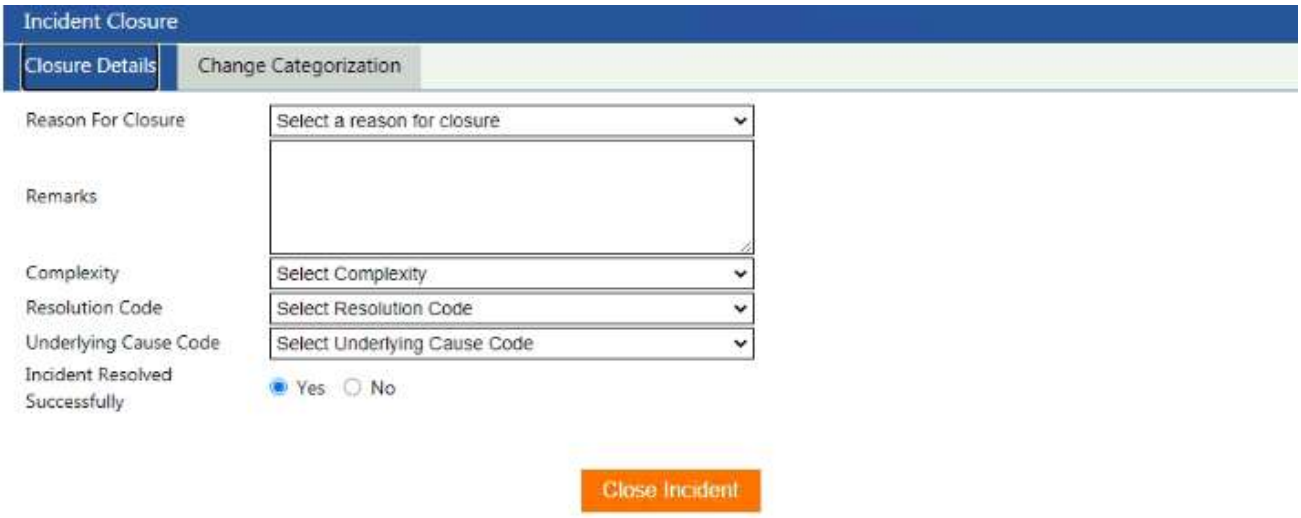
- Cisco updates the TAC ID and other details by utilising the SMART API.
- Engineer details will appear once the ticket is owned by a support member.
- A message will be sent that states 'Case has been set to auto solved - please wait for CE confirmation'
- Another message will be sent that states 'Please allow up to 2 minutes for solve confirmation'
- And finally, the last message in this process will state 'Case has been successfully solved' which means the case has been solved on the Cisco side as well.



- Cisco updates Activity with the ticket details.
- Activity details will be sent to Cisco each time when a non-private activity is added
- Resolution Notes will be sent to Cisco once resolved.



3. After this, the final part of the process will automatically close the ticket.



- Once the ticket has been successfully closed on the Cisco side, you will get a message 'CSOne Update:Closed' and no further updates are allowed to the case."
- Closed details will be sent to Cisco after the ticket is closed.

Test Scenarios

Authentication: Basic (base 64 encoded)

1: SMART Creates Shadow Ticket, Updates, Adds Attachment, Solves, and Closes

Following are the steps to follow for this Test Scenario.

- Case Creation & acknowledgement
- Automatic Case update from Cisco after creation
- SMART sending comment to Cisco
- SMART adding private comment, not sending to Cisco
- SMART adding attachment
- SMART solving case
- SMART closes case

2. SMART Creates Shadow Ticket and Escalates, Cisco Solves and Closes

Following are the steps to follow for this Test Scenario.

- Case Creation & acknowledgement
- Automatic Case update from Cisco after creation
- SMART escalates case
- Cisco solves case
- Cisco closes case

3. SMART Creates Escalated Ticket, Cisco Solves and Closes

Following are the steps to follow for this Test Scenario.

- Case Creation & acknowledgement
- Automatic Case update from Cisco after creation
- Cisco solves case
- Cisco closes case

4. SMART Creates Escalated Ticket P1 or P2, Cisco Solves and Closes

Following are the steps to follow for this Test Scenario.

- Case Creation & acknowledgement
- Automatic Case update from Cisco after creation
- Cisco solves case
- Cisco closes case

5. SMART Pulls TSP Codes List

Following are the steps to follow for this Test Scenario.

- SMART pulls TSP Code List
- Smart Bonding returns TSP Code List to SMART