How to integrate IBM Control Desk into your BlueMix Service Management toolchain for Incident recording, trending and problem readiness.

[1 Introduction](#_Toc467053811)

[1.1 IBM's Control Desk Features](#_Toc467053812)

[2 Solution Overview](#_Toc467053813)

[2.1 Service Management Architecture Overview](#_Toc467053814)

[2.2 Incident Management Architecture Overview](#_Toc467053815)

[3 Use Cases and Personas](#_Toc467053816)

[4 How-to Use IBM Control Desk](#_Toc467053817)

[4.1 Site Reliability Engineer Reviews Weekly Past Incidents for Trends](#_Toc467053818)

[4.1.1 Other Step/Actions from the Start Center](#_Toc467053819)

[4.2 First Responder works/responds to an incident created through Control Desk](#_Toc467053820)

[4.2.1 Other Step/Actions](#_Toc467053821)

[5 Pre-requisites for setup](#_Toc467053822)

[6 Configuration of Control Desk](#_Toc467053823)

[6.1 Creating and Defining Start Centers](#_Toc467053824)

[6.1.1 Start Centers](#_Toc467053825)

[6.1.2 Creating Queries](#_Toc467053826)

[6.1.3 Creating KPIs](#_Toc467053827)

[6.1 Classification Structure](#_Toc467053828)

[6.2 Escalations](#_Toc467053829)

[6.3 Configuration of fields for Integration to Slack](#_Toc467053830)

[6.4 send a message to Slack when the status of the ticket changes to CLOSED](#_Toc467053831)

[7 How to setup the Integration of NOI with IBM Control Desk](#_Toc467053832)

[7.1 Netcool Operations Insight to Control Desk Integration](#_Toc467053833)

[7.1.1 TSRM gateway installation](#_Toc467053834)

[7.1.2 Basic TSRM gateway configuration:](#_Toc467053835)

[7.1.3 Integration customizations:](#_Toc467053836)

[8 Conclusion](#_Toc467053837)

[9 Glossary of Control Desk Terms](#_Toc467053838)

# Introduction

BlueMix is a Platform as a Service (PaaS) application which provides the ability to rapidly build and deploy and application. Applications may run in native BlueMix or in a hybrid fashion.

There are multiple ways of reducing incidents, issues, outages in BlueMix applications and, once an issue is detected, multiple ways of researching and analyzing and taking steps to reduce or eliminate outages or performance degradation. The purpose of incident recording and trending is to analyze the number, frequency and types of incidents; so-as-to take preventative measures to eliminate or reduce the volume, frequency and severity of the outages or performance degradation to ensure fast and reliable services in BlueMix or in the situation of a Hybrid architecture. These preventative measures may be to leverage official communications to the developers as to what to avoid, or how to tips and solutions for the creating of Run Books to be automated should the issue need to be quickly resolved.

In this guide, we cover the setup of Control Desk so that it can connect with other applications in the middle of the Service Management toolchain and demonstrate the interaction of Control Desk with those other components of the toolchain.

Note: We will not cover standard installation and operation of IBM Control Desk, since this is not unique to the BlueMix environment. Links to references will be provided instead.

## IBM's Control Desk Features

IBM Control Desk unified IT asset and service management software provides a common control center for managing business processes for both digital and physical assets. It enables control, governance and compliance to applications, endpoints and assets to protect critical data and prevent outages.

Control Desk is IT Infrastructure Library (ITIL)-compliant, accessible through mobile devices and integrates with social media and development tools.

IBM Control Desk enables the business to support the user community for the full lifecycle of request, issue and ongoing maintenance and support to systems and infrastructure the users need to do their jobs and to drive revenue for the overall business.

Control Desk enables the IT support and operations to manage user request and support lifecycle from problem detection to fix and helps the business:

1. **Improve operational efficiency** with near real-time and historical analytics.
   * Prioritizes incident response based on business service impact.
   * Speeds problem resolution with a searchable solutions knowledge base and embedded remote diagnostics. Agents can remotely take over workstations and chat with users for faster request fulfillment.
   * Provides ticket templates and pre-populates work order fields with service request information through integration with telephony software.
   * Automatically classifies tickets based on keywords and detail fields.
   * Processes emails into inbound service requests. Service requests can be created, viewed and approved using mobile devices.
2. **Identify incident trends and patterns** with search analytics.
   * Use advanced search, queries and reporting to identify repeat incidents and patterns to focus communication and information to developers and first responders.
   * Provide visibility to first responder, site reliability engineers, incident managers as well as developers.

# Solution Overview

## Service Management Architecture Overview

Cloud based applications need to be available all the time. Proper processes need to be put in place to assure availability and performance. This includes Incident and Problem management to respond to outages, but also the ability to do proper recording of the incidents and problems so-as-to conduct trending, root cause analysis and ensure the elimination of the issue through communication and change management processes to correct the issue.

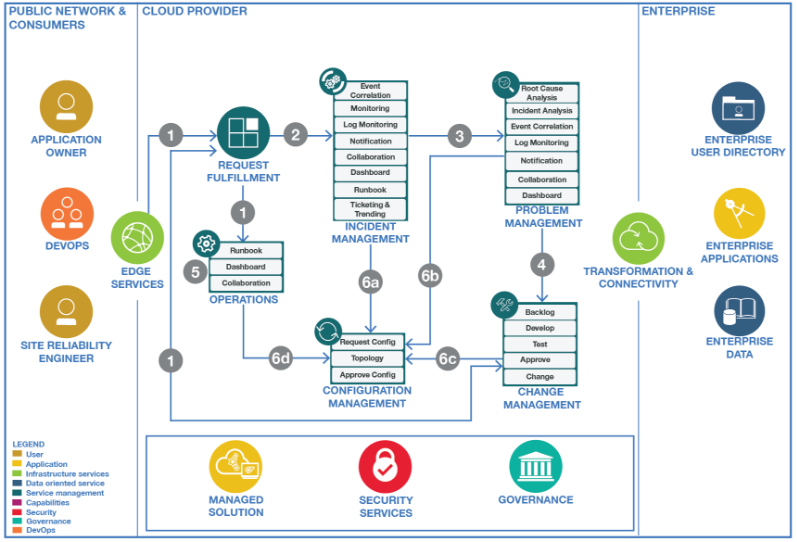


Figure 1 – Service Management Architecture Overview

Diagram can be found at this url - <https://github.com/ibm-cloud-architecture/refarch-cloudnative-csmo>

The following are the runtime flow details of the overall Service Management Architecture image

1. The above flow displays the client or support system reports an incident, request a change or seeks status of an application. Service management users interact with clients to gather more information if needed to diagnose incidents.
2. Incident Management is optimized to restore the service as quickly as possible. This is done through a First Responder team, equipped with Automation and well-defined Runbooks. Sophisticated monitoring is performed to detect issues early, before the service is affected. For complex incidents, subject matter experts collaborate on the investigation and resolution. Stakeholders (e.g. the application owner) are continuously informed about the status of the incident.
3. Once the Service is restored, recording of tickets, and collaborating data enables the roles to prepare for Problem Management to investigate the root cause of the problem leveraging techniques like “5 Whys “. Once it is understood what went wrong, counter measures are taken to prevent the incident from happening again.
4. A change request is created to address the root cause of the incident. The change can be against the application, the infrastructure, or the supporting environment (i.e. skill). Changes are prioritized and approved and put to the backlog to be addressed in an agile manner.
5. Operations handles the integration, usage and delivery of key services to business applications and the enterprise whether it is participating in incident management, architectural patterns, deployment, etc. Operations integrates with, or drives key processes to ensure the enterprise achieves its KPIs.
6. Configuration Management supports these processes (Incident, Problem, Change management) as well as Operations. It maintains knowledge about the contributing components as well as their relationships.

## Incident Management Architecture Overview

Incident management and its operations are key to cloud Service Management. Incident Management is optimized to restore the normal service operations as quickly as, thus ensuring the best possible levels of service quality and availability are maintained. Following figure provides deep dive into Incident Management

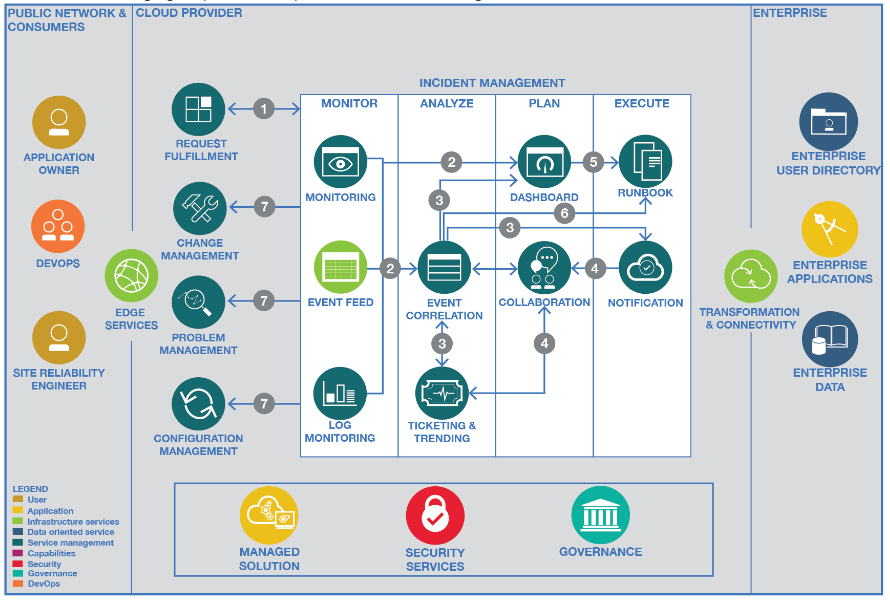


Figure 2 - Incident Management Architecture Overview

Diagram can be found at this URL - <https://github.com/ibm-cloud-architecture/refarch-cloudnative-csmo/blob/master/doc/Incident_Management_Implementation.md>

Following are the flow of the Incident Management Architecture

1. The user or request fulfillment system reports an incident. Stakeholders (e.g., the Application Owner) are continuously informed about the status of the incident.
2. The sophisticated Monitoring and Logging tools, that includes IBM or Third Party tools, connected to the managed solutions detect the issues early and send alerts to the Event Correlation tool and unified Dashboard.
3. The Event Correlation tool is empowered to correlate events from multiple sources and helps identifying and isolating the problem by alerting the Collaboration and Notification systems. First Responder team typically considers correlated events to narrow down the issue instantly. For complex issues the Incident Owner and Subject Matter Experts collaborate on the investigation and resolution.
4. The Notification system creates collaboration channel with alerts specific to an incident allowing Incident Owner and Subject Matter Expert to have records within the incident investigation and mitigation.
5. The Notification system creates an incident with specific details to allow the First responder to resolve using the incident record independent or in collaboration with others in a channel.
6. The Dashboard are preconfigured to provide one single view of various sources of events from Event Correlation and Monitoring systems to guide the First Responder and Subject Matter Experts to isolate and resolve the issues by executing Runbooks.
7. The First Responder Team is equipped with automation and well-defined Runbooks to resolve the issue instantly. The automated process also updates the status of the event so that the dashboard, notification and collaboration channels are synchronized.
8. The Site Reliability Engineer is provided with a set of queries, KPIs and result set to allow for trending and commonalities of records to be found and recorded for trending review and analysis.
9. Once the incident is closed a problem ticket is opened by the Site Reliability Engineer to then determine the root cause of the issue. In case a configuration change is needed the incident, owner opens a ticket in Configuration Management system.

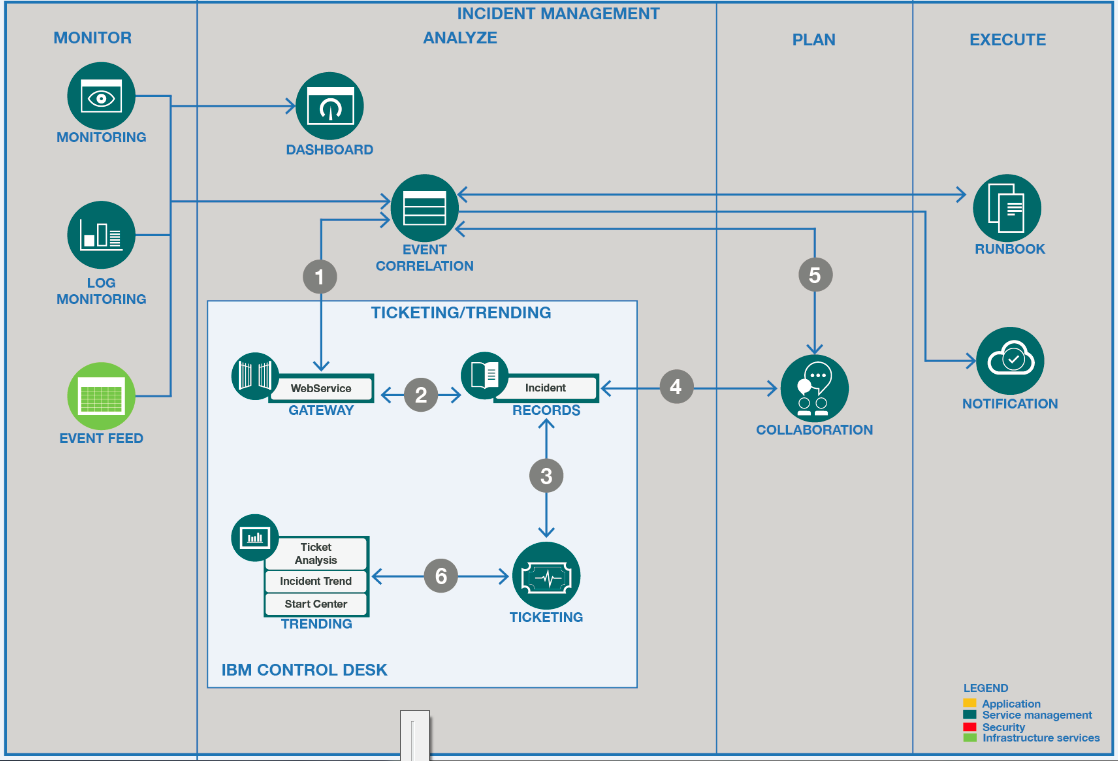


Figure 3 – System Context Diagram for IBM Control Desk

The above figure shows the deep dive of IBM Control Desk and its various components and various integrated tools for incident management and their interactions. One of the key takeaways from the diagram is that the solution supports a strong integration mixture of products and solutions, each feeding or being fed by the central NOI solution.

The following flow describes the setup and operations of this solution in an overall cloud service management space:

1. An event system receives an alert and determines the severity of the issue and creates an incident in IBM Control Desk. At the same time as the incident is being created a collaboration channel is being opened. If the severity of the incident is a one (1) it will be a dedicated collaboration channel and if it is anything lower, it would be set in a general channel.
2. Once the Collaboration Channel is open then the event system will update the Control Desk incident with the details of the channel (URL).
3. The next step in the flow is a decision action. Once the decision is made the flow will follow one or the other path. (Thus a or b)
   1. In this path the users are in the channel collaborating to determine a solution and when the solution is provided the user can type in slack noi resolve and the exact ticket number and the ticket will be set to resolved.
   2. If the flow follows this path then the event system determines if there is a runbook that can be executed to resolve the issue, this can be either manual or automated.
4. Once the runbook has completed the event system is still monitoring to ensure the exact issue is resolved if so the even system updates the incident in Control desk to status resolved.
5. Additionally, the collaboration data from the channel will be retrieved and stored in a work log entry in Control Desk for future use and analysis in trends.

# Use Cases and Personas

The following are common use-cases which involve IBM Control Desk in the Service Management toolchain.

**First Responder** (on call):

1. First Responder receives an alert to support an issue and when in the Slack Channel they want to view in IBM Control Desk if this sort of issue had occurred before and if so what might have been used to resolve the incident.
2. First Responder launches into Control Desk to add a work log of the solution that is found to be the solution to a current incident.
3. First Responder uses the work log from a similar incident to determine who worked on incidents of the same type and may be able to assist more timely now.

**Site Reliability Engineer:**

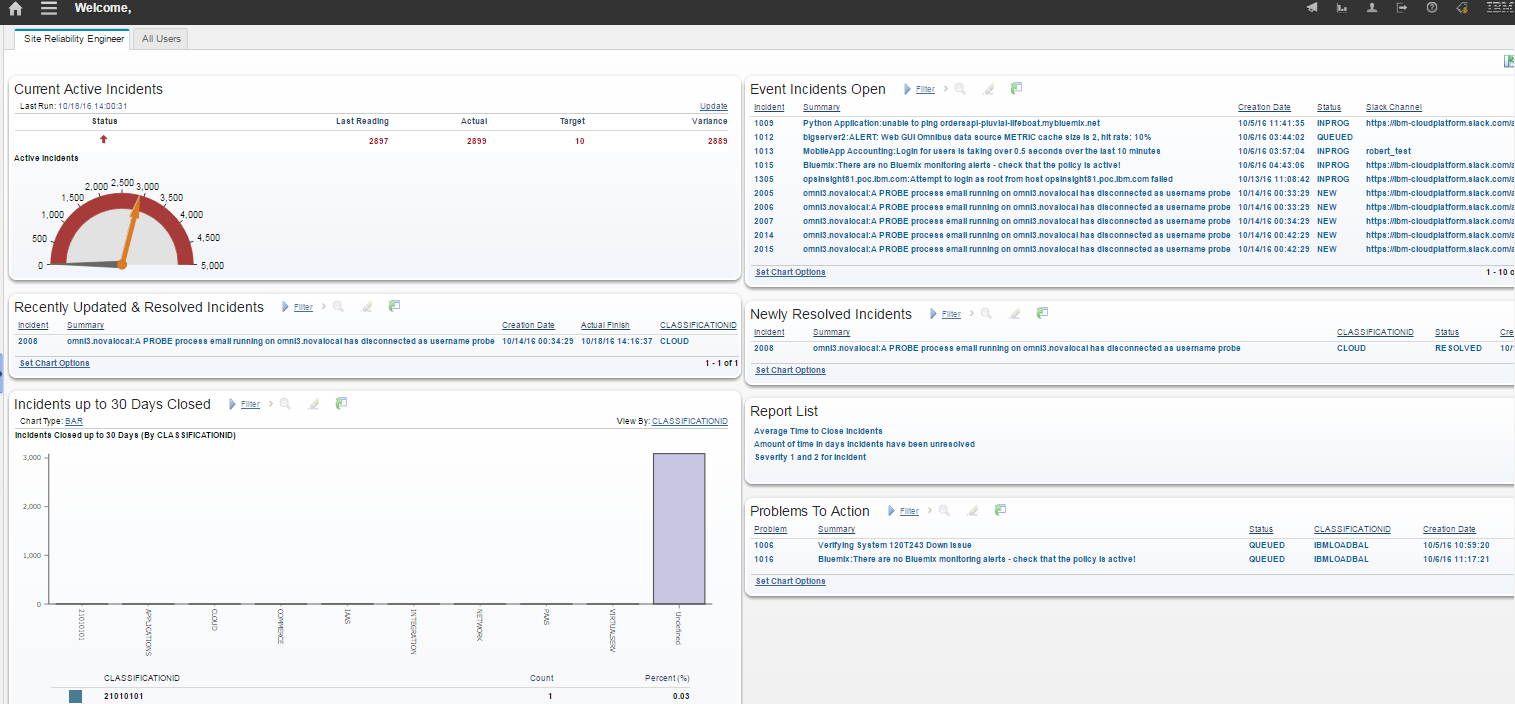
1. Would like to conduct an analysis of the recent incidents to look for trends and frequency changes.
2. Investigates the incidents which are like another incident to solve the current incident faster.
3. To possibly find patterns, and establish problem records for root cause review.
4. To locate resolution to previous incident more timely.
5. To understand who was the team or resources that may have worked an incident before.

# How-to Use IBM Control Desk

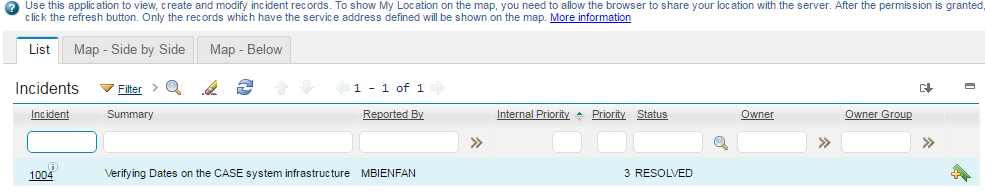
IBM Control Desk is operated though a web based GUI. The exact URL would be retrieved for your instanced based on installation or leveraging a Cloud based solution and is usually of the format http://<servername>/maximo. The following steps provided are focused on a single process in which the site Reliability Engineer or First Responder may perform. As users, they may perform many activities and processes with the data available to them in IBM Control Desk. The additional activities and processes are not fully stepped out in this document.

## Site Reliability Engineer Reviews Weekly Past Incidents for Trends

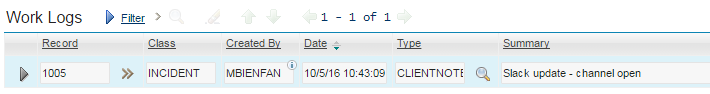
1. Upon login, a site reliability engineer will use the Pre-Created Start Center to view the **Recently Updated & Resolved incidents**. The portlet is created and exists on the lower left corner of the Start Center.



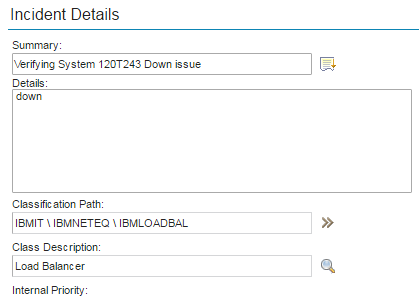
1. The engineer will click on the **Open Results in Application icon** to view the results, this will present all incidents which have a recent updated work log & been set to resolved in the last 24 hours.
2. As the list is presented in the Application list the engineer can scan the list for:
   1. Common summary
   2. Sort by Priority
   3. Take note if the Incident required an owner or owning group to be resolved



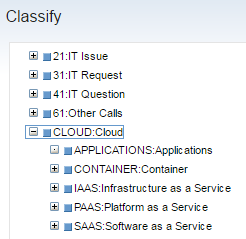
1. The site reliability engineer can further review the incidents by opening them for further details such as
   1. What work log updates were added to give insight as to the run books used
   2. The slack channel conversation
   3. The first responders who may have added a log for a worthy note of detail



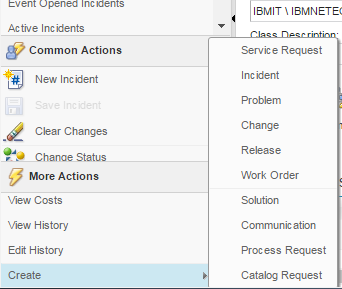
1. As the Engineer reviews the incidents they find of reoccurrence or which they believe should be further researched as a problem record, it may be best to Classify the incident or the problem record for next step or future reporting steps.
2. To Classify the incident, record the Engineer will click on the Double arrows  next to the field Classification Path: and use the dialogue to select a proper classification.



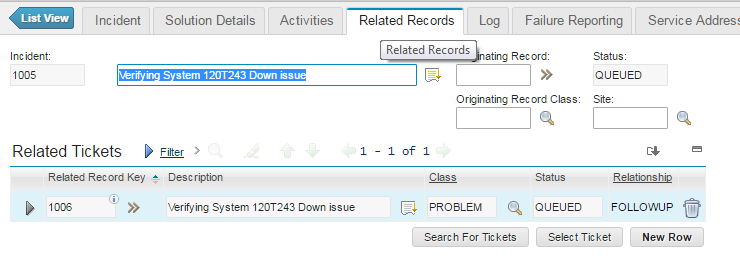
1. When the SRE selects the classification, the engineer will click on the blue box next to the best classification and that will close the dialogue and update the classification field.



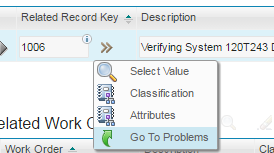
1. Should the Engineer decide to create a problem record for further root cause analysis, the engineer would do so by selecting **Create > Problem** found under **More Actions** on the left-hand navigation panel. Once the problem is created this creation is the bridge from incident management to problem management.



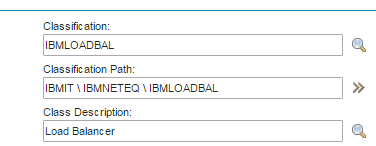
1. Once the problem has been created the Problem record will be viewed by the SRE from the Related Records Tab.

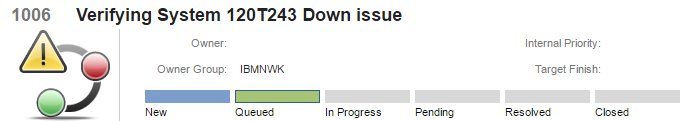


1. The SRE will briefly navigate to the Problem record from the incident to make minor updates to the problem record:
   1. Assign to a person or group
   2. Set Start Dates
   3. Categorize the problem to make it available for full on root cause review by the problem team.
2. The SRE will use the double arrows next to the Related Record Key field and Select **Go to Problems**

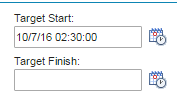


1. The SRE should double check that the Problem record is classified, if the Incident record was Classified before creating the problem record, then the problem record will be classified based on the Classification and auto assigned to an owner group based on classification.



.

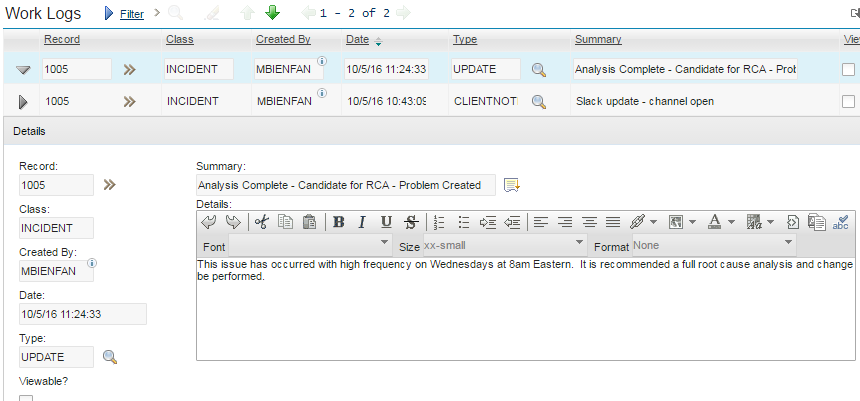
1. If the Classification does not pre-populate the owner group, the SRE can from the left navigation menu under Common actions, click on Select Owner, then search for the group they wish the problem to be reviewed by for root cause.
2. The Engineer may also
   1. choose to set an urgency on the problem record to help prioritize the work to determine root cause through analysis of the problems.
   2. And/or set the Target Start and/or Target Finish to ensure analysis and work are performed timely.



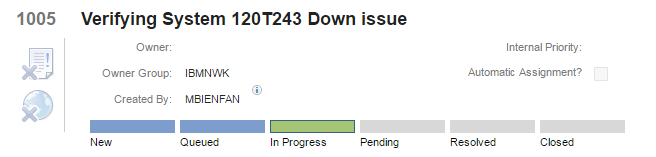
1. To return to the Incident and the trending analysis the engineer would click on the Return button in the upper right hand corner.



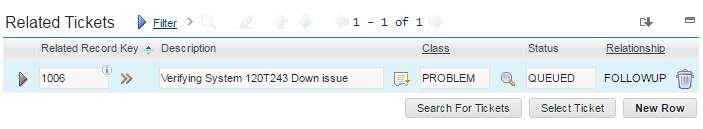
1. The engineer would add a work log by clicking New row on the main incident screen, under work log section. The engineer would record their analysis performed and why this incident or others like it should be reviewed for Root Cause Analysis.



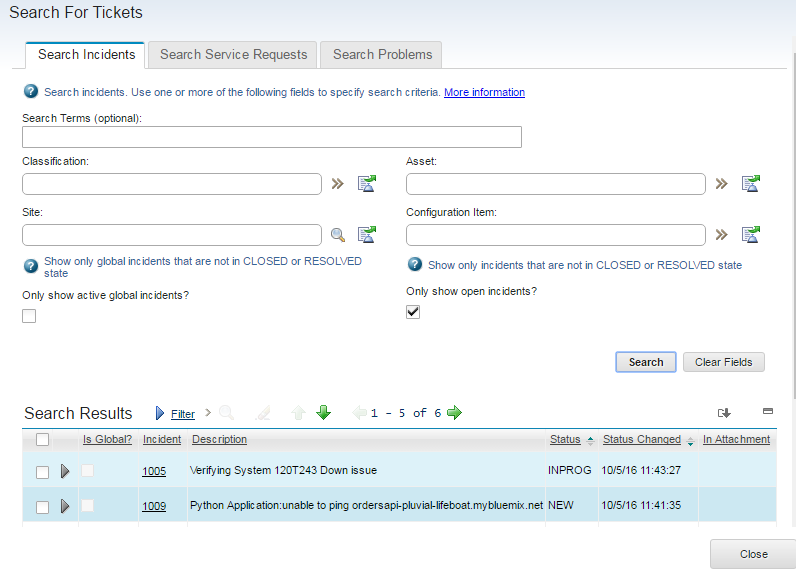
1. After recording the work entry on analysis, then the engineer will set the status to in Progress as the incident can be resolved and closed after root cause is determined and action is being taken, through a change or update.



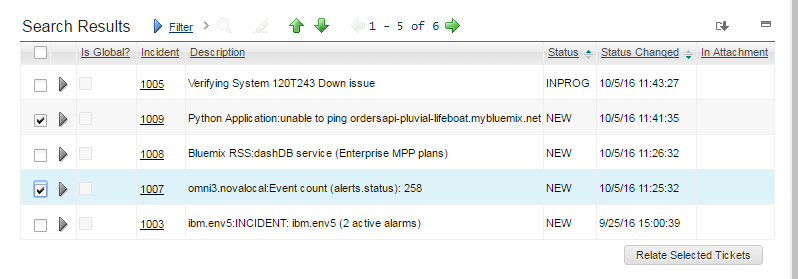
1. Should the Site Reliability Engineer determine several incidents are of the same like kind or could be “related” it is possible to relate the incidents on the Related Records tab.
2. To do the action of relating records, does not cause the records to all be actioned the same, it simply shows that there is some correlation between the events and the incidents that were created.
3. On the Related Records tab the engineer uses the **Select Ticket button,** if they know the ticket numbers to be related. If they wish to search for them then using the **Search for Tickets button** is recommended.



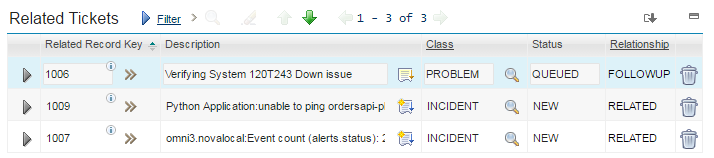
1. When using the **Search for Tickets button** check the box for Only Show Open Incidents and hit search. The results will show in the section of the dialogue for Search Results.
   1. This list can be further filtered using any of the fields at the top of the dialogue before clicking search or
   2. By using the filter row in the Search Results to find tickets in the results.



1. To relate a record, check the box near the record row in the Search results, and then click the box Relate Selected Tickets. Then click Close to return to the record where the related tickets will display.



1. To view the related tickets versus the problem ticket which is a follow-up relationship take a quick look at Related Tickets Section and take note of the Relationships.



1. To return to the original list of incidents that were recently updated and resolved click on the List View Arrow next to Incident header.



### Other Step/Actions from the Start Center

As Control Desk provides an extensive view and set of data the Site Reliability Engineer can take many actions to review trends and conduct incident analysis for the support of Cloud or Hybrid applications. These reviews and analysis conducted can:

* set the stage for problem management
* the understanding for the need for corrective action (runbooks)
* or solutions (documented knowledge)
* or communications (to developers for change of behavior)

To leverage other portlets and data presented in the Start Center the Engineer would

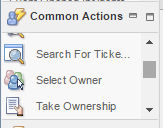
1. Upon login, a site reliability engineer will use the various Start Center portlets to fully review trends occurring and to analyze the data being captured and presented through the Control Desk UI.
2. The other Portlets available to the engineer through their start center would be:
   1. KPI of Current Active Incidents
      1. Enables the engineer and responders to understand the level of volume/impact the current incidents may be having in the infrastructure, if only 5 or 10 incidents should be open at any given time and the current volume is more than this number then they can see they need to take more proactive steps to decreasing incidents.
   2. Incidents up to 30 Days Closed, sorted by Classification
      1. The engineer may want to focus on the incidents he/she has classified as those were likely the incidents that showed interests in the trends occurring recently.
      2. This query view allows for the users to understand the number of incidents being worked and reviewed or analyzed for impact to the overall infrastructure.
   3. Severity 1 Event Incidents
      1. This result set focuses on the top severity of the incidents occurring and are in a status of “active”.
   4. Severity 2,3,4 Event Incidents
      1. These incidents are “active” and not yet resolved through automation or manual steps and are of a lower severity than one.
   5. Newly Resolved Incidents
      1. These incidents have recently been resolved and could be of interests for analysis and trending.
   6. Report List
      1. These are just a few reports which can be launched from the Start Center to aid in the review of data being gathered and assimilated in Control Desk.
   7. Problems to Action
      1. These are records where root because analysis would be performed and corrective changes would be completed.
3. These result sets and portlets can be used directly in the start center or the go to list view icon to work with the data in the list to filter, open and pare down the results to those showing the trends.
4. The Pre-configured start center for the SRE can be further configured to include additional portlets or it is possible to update the configurations to reflect additional parameters, lists and queries.

Further Knowledge of Start Centers can be viewed here

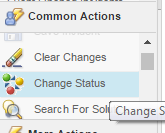
<https://www.ibm.com/support/knowledgecenter/SSWT9A_7.6.0/com.ibm.mbs.doc/startcntr/c_start_center_overview.html>

## First Responder works/responds to an incident created through Control Desk

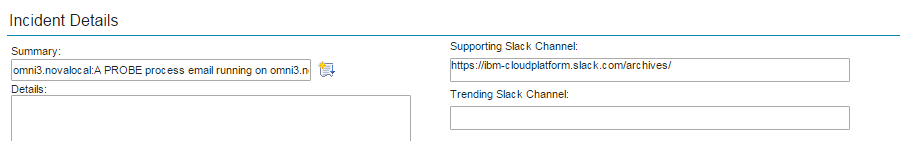
1. Upon login as a first responder, use the Start Center to view the **Event Driven Incidents, or Active Incidents -Assigned to Me**. The portlets allow you to pick up or return to work you have recently worked on.
2. Select an incident from the Event Driven Incidents, click on the record in the result set to open the incident.
3. Once the record is open and you have determined you will work the incident under Common Actions in the left navigation select the Take Ownership action. This will assign the incident to you to work and resolve.



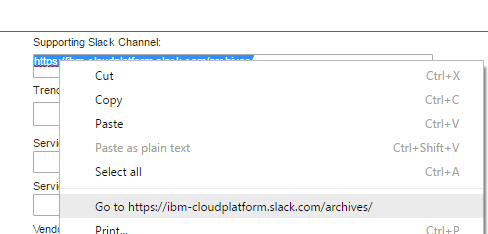
1. The incident will automatically become a status of Queued. To begin work on the incident set the status which is also under Common Actions to a status of in progress.



1. Once in progress, then scroll slightly to the middle of the record and locate the supporting slack channel where others may be in collaboration to resolve.

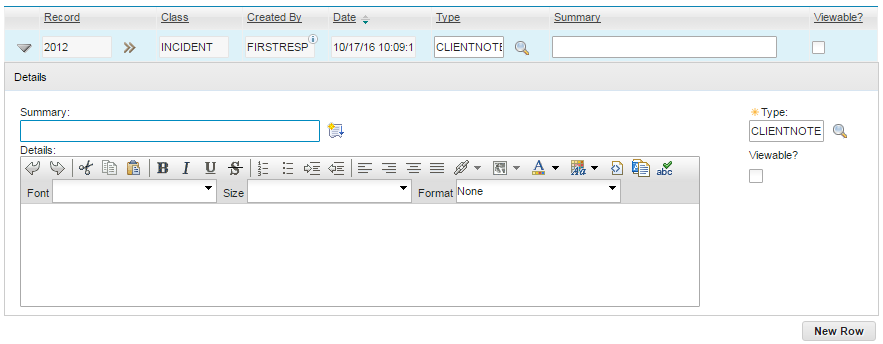


1. Highlight the channel in the field and right click Select the Go to option and you will be taken directly to the slack channel. Read and collaborate for a solution or provide the solution you believe will resolve the issue.



* Note there may also be a trending Slack Channel if the Site Reliability Engineer or other responders are specifically reviewing incidents of a pattern or type and they are in collaboration or discussion in the channel. If there is a trending channel as well it may be of value to review the channel as well.

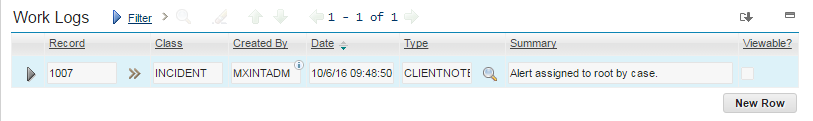
1. To add comments or updates to the incident, then scroll to the section called Work Logs, and click new row. This will create an entry where updates from you can be provided. As these are the notes of the incident activities you may also see entries from the Slack Channel as well as from NOI directly.



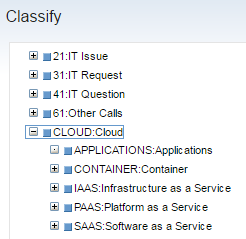
Entry in the Incident recorded by Slack



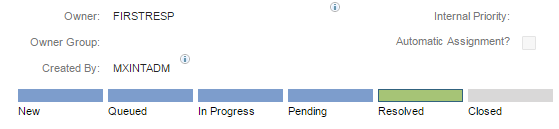
Entry Recorded Update recorded by NOI



1. As an optional task, it is possible for the first responder to Classify the record, if the known issue is identified, recognized and found in the Cloud Classifications structure. Use the double arrows next to Classification Path field and click Classify. To select the classification, use the blue box next to the word. To expand and see more hierarchy use the plus sign.



1. Once the incident issue is resolved, the incident can be set to a status of resolved. This can be done by using the change status under Common Actions in Control Desk or by typing noi resolve in the Slack channel for the incident,



1. Incidents are resolved by writing the following command in SLACK channel:

noi resolve <eventNumber>

1. These are custom slackbots developed as part of the CASE project to integrate the communications of various tools in the overall toolchain.
2. This will work both from the "global" channel - i.e. resolve any event and from the dedicated channel for a specific event.
3. Should the incident be “a global” incident meaning it is affecting many systems the First Responder can set the incident to a global incident and relate other records to it. Such as is identified in these steps.

<https://www.ibm.com/support/knowledgecenter/SSZRHJ/com.ibm.sccd-saas.doc/ticket/c_global.html>

### Other Step/Actions

As Control Desk provides an extensive view and actions the First Responder can take many steps to work, update and review data of incidents that are in support of Cloud or Hybrid applications. These actions and updates can:

* Ensure accurate data for analysis
* Finding faster incidents that have had similar solutions and runbooks
* Ability to return to a slack channel to find past collaborators for resolution or find past actions take for an incident of similar type.
* or communications (to developers for change of behavior)

To leverage other portlets and data presented in the Start Center the First responder would

1. Upon login, the First Responder will use the various Start Center portlets to review active and resolve incidents, take ownership, or find similar incidents/trends occurring and leverage the data being captured and presented through the Control Desk UI to resolve incidents quickly.
2. The other Portlets available to the responder through their start center would be:
   1. Quick Inserts
      1. To create Incidents or problems for future action
   2. Open Incidents – KPI
      1. Enables the engineer and responders to understand the level of volume/impact the current incidents may be having in the infrastructure, if only 5 or 10 incidents should be open at any given time and the current volume is more than this number then they can see they need to take more proactive steps to decreasing incidents.
   3. Average Incident Work Time – KPI
      1. This Key performance indicator is representing how long an incident is worked before it is set to resolved.
   4. Active Incidents Assigned to Me
      1. This would represent and only show incidents the first responder has taken ownership of to ensure no others work this incident or that they have a follow up action or interest.
   5. Severity 1 Incidents – Open
      1. This result set focuses on the top severity of the incidents occurring and are in a status of “active”.
   6. Severity 2, 3, 4, Incidents – Open
      1. These incidents are “active” and not yet resolved through automation or manual steps and are of a lower severity than one.
   7. Newly Created Problems
      1. These are records where root cause analysis would be performed and corrective changes would be completed.
3. These result sets and portlets can be used directly in the start center or the go to list view icon to work with the data in the list view to filter, open and pare down the results to those the responder wishes to work with or review.

Further Knowledge of Start Centers can be viewed here

<https://www.ibm.com/support/knowledgecenter/SSWT9A_7.6.0/com.ibm.mbs.doc/startcntr/c_start_center_overview.html>

# Pre-requisites for setup

The following components of IBM Control Desk, Netcool Operations Insight / Omnibus & Slack are needed for this toolchain integration:

| **Component** | **Purpose** |
| --- | --- |
| IBM Control Desk | IBM Control Desk on Cloud is an integrated service management solution that helps businesses manage a comprehensive range of IT processes, services, and assets.  With IBM Control Desk on Cloud, a business can optimize the performance of their infrastructure and workforce in alignment with overall business objectives. The product features innovative functions that are focused on the following business process areas:  Service desk management, including a self-service center, catalogs for fulfillment, and incident and problem management applications  IT asset and software license management  Change and configuration management  For the First Responders and Site Reliability Engineers to log into Control Desk to perform their work functions.  The solution will allow for the Site Reliability Engineer to review & analyze for trending across incident types, frequency and severity.  The First Responder will be enabled to search for other incidents in the UI to search for quick solutions and re-use solutions that may have been used in the past to resolve an issue. |
| Start Center | A Start Center is a configurable page that gives you quick access to the tools and key performance indicators (KPIs) that you use most often. Each of the security groups that are defined for change management has its own Start Center. When you log on to the product, the Start Center that is mapped to your primary security group is displayed. If you have multiple security group assignments, you can tab to secondary Start Centers. |
| Escalations | Escalations are used to automatically monitor the critical processes in your enterprise. You can also use escalations for events, such as contract expiration, a change in the status of a records, or a change in the ownership of a record. |
| Incident | An incident record is a type of ticket. Other ticket types are service requests and problems. The ticket applications are closely related and share many features, including the ability to define relationships between tickets, link them together for information purposes, and view the linkages and details in the appropriate applications.  For the purposes of this document, especially in the NOI-ICD integration, the use of the word ticket and incident may be interchanged. |
| Script with Launch Action | Creating an automation script with an action launch point to facilitate the development of re-usable actions, that can be configured for use in different object contexts (for example, incidents, tickets). An action launch point associates a script with an action and executes when the specified action occurs. |
| Problem | A problem record is a type of ticket. Other ticket types are service requests and incidents. The Problems, Incidents, and Service Requests applications are closely related and share many features. You can define relationships between tickets, link them for information purposes, and view details for them in the appropriate applications. |
| KPI | Creating key performance indicators to track critical performance variables over time. You can view key performance indicators (KPIs) in the start center or in the KPI Manager application. |
| Reports | There are several predefined reports provided with Control Desk. Use them to gather information about the incidents created for issues in your infrastructure, conduct trending and analyze data based on the incidents and volumes being created. |
| Security | The Security Groups application, you can grant users access to specific applications to refine security measures. Users can have read, insert, save, and delete access to an application. The application access of a security group is linked to site access. You can give a security group access to all sites, access to specific sites, or no access to sites.  Grant user’s specific options within an application. For example, you can grant managers the right to read work order histories, costs, and warranties, but not to insert work orders or service requests. You must configure each application for read access so that administrative users can select additional application access options. |
| Work log |  |
| Netcool Operations Insight (NOI) | An event management and correlation engine which acts as a force-multiplier in the middle of the tool chain, correlating disparate events across applications, services, and infrastructure, and making sure that the most important and business-affecting events are forwarded by suppressing symptomatic events in favor of root-cause events. For the purposes of this document, NOI and Omnibus (the central component of NOI) are interchangeable terms. |
| TSRM Gateway aka ICD Gateway | The NOI component which performs the bi-directional integration between NOI and ICD. Note that TSRM and ICD are synonyms and the gateway's name is TSRM for historical reasons only. |
| Object Server | NOI's central repository of monitoring events. This is an in-memory database that must be extended with new fields as part of the integration. |
| Trigger | An automation within an Object Server that can perform tasks either on a schedule or because of a change in an event. |
| Journal entry | A feature of NOI, allowing operators to information about a given incident. Equivalent to ICD's work logs. |
| Slack | Communications and collaboration platform, improves the capabilities of users to work together to solve issues faster. Also, functions as a ChatOps platform, enabling remote commands and remediation tasks as part of the chat conversation |

1. Installation of IBM Control Desk environment can be done per the standard IBM instructions detailed in the following links and adjusted based on installing in an on-premise solution or a Cloud based solution.

* [Installation of IBM Control Desk - On Premise](https://www.ibm.com/support/knowledgecenter/SSWT9A_7.6.0/com.ibm.sccd-adv.doc/sccd_install/t_ctr_install.html)
* [How to Access IBM Control Desk - On Cloud](https://www.ibm.com/marketplace/cloud/it-service-management/us/en-us?lnk=US_STW_MHP_L1&lnk2=learn_CtrlDesk)

1. Installation of the Omnibus environment can be done per the standard IBM instructions detailed in the following links and adjusted by any local requirements (connections to LDAP, choice of operating system and database, H/A considerations and so on...). The integration of Omnibus into the toolchain is loosely coupled and will function with any (IBM-supported) configuration of Omnibus.

* [Omnibus v8.1 installation documentation](https://www.ibm.com/support/knowledgecenter/SSSHTQ_8.1.0/com.ibm.netcool_OMNIbus.doc_8.1.0/omnibus/wip/install/reference/omn_ins_im_omn_install_overview.html)
* [Netcool Operations Insight v1.4 installation documentation](https://www.ibm.com/support/knowledgecenter/SSTPTP_1.4.0.1/soc/integration/reference/soc_int_quickrefgettingstarted.html)
* [Installation best practices](https://www.ibm.com/developerworks/community/wikis/home?lang=en-us#/wiki/Tivoli%20Netcool%20OMNIbus/page/Best%20Practices)

# Configuration of Control Desk

## Creating and Defining Start Centers

### Start Centers

To Set up the Start Centers used in this business flow it will be necessary to leverage several items; queries, where clauses, KPIs and the activity of create and update a Start Center template.

To support the several user personas defined in this How to Guide there are two start centers that were created, Labeled Site Reliability Engineer and First Responder.

Using the screen shots and layouts in this document along with the queries and KPIs listed you will be able to create the Start centers for reuse.

To start with it is necessary to create a template. To do so follow the standard instructions here.

<https://www.ibm.com/support/knowledgecenter/SSWT9A_7.6.0/com.ibm.mbs.doc/startcntr/t_mng_start_center_templates.html?cp=SSWT9A_7.6.0>

<https://www.ibm.com/support/knowledgecenter/SSWT9A_7.6.0/com.ibm.mbs.doc/startcntr/c_start_center_overview.html>

### Creating Queries

For creating predefined and saved queries to be used for the Start Centers and have them available in the applications, it is possible to follow these steps:

<https://www.ibm.com/support/knowledgecenter/SSWT9A_7.5.1/com.ibm.mbs.doc/workview/t_ctr_work_view_queries.html?cp=SSWT9A_7.6.0>

For instructions and steps for creating where clause queries, follow this link:

<https://www.ibm.com/support/knowledgecenter/SSWT9A_7.6.0/com.ibm.mbs.doc/gp_ui/c_SQL_search.html?cp=SSWT9A_7.6.0>

Several queries were created and define to support the start centers. The queries are provided here for quick and fast recreating.

|  |  |
| --- | --- |
| Recently Resolved Incidents | (status = 'RESOLVED' and upper(externalsystem) = 'EVENTMANAGEMENT') |
| Recently Updated and Resolved Incidents | ticketid in ( select recordkey from worklog where modifydate > current timestamp - decimal(240000,6,0) ) and status in (select value from synonymdomain where maxvalue in ('RESOLVED') and domainid = 'INCIDENTSTATUS') and (current timestamp > actualfinish) order by internalpriority ASC |
| Priority 2,3,4 Incidents | ((status = 'INPROG' or status = 'NEW' or status = 'PENDING' or status = 'QUEUED') and upper(externalsystem) = 'EVENTMANAGEMENT' and (reportedpriority = 2 or reportedpriority = 3 or reportedpriority = 4)) |
| Priority 1 Incidents | ((status = 'INPROG' or status = 'NEW' or status = 'PENDING' or status = 'QUEUED') and upper(externalsystem) = 'EVENTMANAGEMENT' and reportedpriority = 1) |
| Incidents Closed up to 30 Days | (status = 'CLOSED') and actualfinish > (current timestamp - 30 days) order by internalpriority ASC |
| All Event Management Incidents | ((status = 'INPROG' or status = 'NEW' or status = 'PENDING' or status = 'QUEUED') and upper(externalsystem) = 'EVENTMANAGEMENT') |
| Incidents Assigned to Logged in User | ((status = 'INPROG' or status = 'NEW' or status = 'PENDING' or status = 'QUEUED')) and (owner = :USER) |
| Open Problems | (historyflag = 0) and (status in (select value from synonymdomain where maxvalue in ('NEW','PENDING','QUEUED','INPRG') and domainid in ('PROBLEMSTATUS'))) |

### Creating KPIs

Several Key Performance Indicators are used in the creating of the Start Centers for these use cases and the instructions for creating or reuse can be found using this knowledge center URL.

<https://www.ibm.com/support/knowledgecenter/SSWT9A_7.6.0/com.ibm.mbs.doc/mbs_common/t_create_kpis.html?cp=SSWT9A_7.6.0>

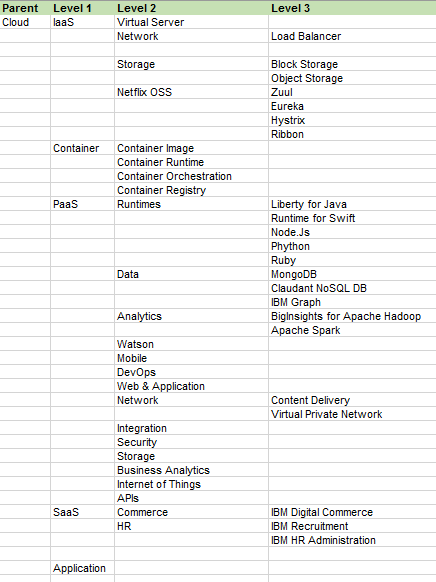
These select statements provide the basis for creating the KPIs leveraged for the Start Centers created for the Start Centers used in this How to Guide.

|  |  |
| --- | --- |
| Open Incidents | select count(\*) from INCIDENT where status in (select value from synonymdomain where maxvalue in ('NEW','QUEUED','PENDING','INPROG')) |
| Average Work Time of Incidents | select avg(TIMESTAMPDIFF(8, char(ACTUALFINISH-ACTUALSTART))) from Incident |

## Classification Structure

To establish a proper Cloud support categorization of the incidents being created in Control Desk by the event monitoring system and by First Responders a new Cloud classification hierarchy has been established. To create classification in IBM Control Desk you will use the Administration > Classification Application.

Imbedded here is the Cloud classification structure recommended for use in the support of cloud infrastructure. It is possible to expand and personalize this classification structure into other classification hierarchies.



## Escalations

Several escalations are used in configuring use escalations to automatically monitor the critical processes in your enterprise. You can also use escalations for events, such as contract expiration, a change in the status of a records, or a change in the ownership of a record.

Several Escalations are used in this implementation for the updating of incident status, or to take an action to send data to integration points.

|  |  |  |  |
| --- | --- | --- | --- |
| Close resolved Incidents after 5 days | STATUS IN (SELECT VALUE FROM SYNONYMDOMAIN WHERE DOMAINID = 'INCIDENTSTATUS' AND MAXVALUE = 'RESOLVED') | Escalation point is 5 days | Action of Incident Close – |
| Process Closed incidents – Slack | STATUS=’CLOSED’ | No Escalation Point | \*Action of Send information to Slack Channel |

*\*Additional details on the script used for the Process closed incidents can be found in section 5.4 of this document*.

Further details and knowledge for escalations can be found at these knowledge center sites.

<https://www.ibm.com/support/knowledgecenter/SSLKT6_7.6.0.5/com.ibm.mbs.doc/escalation/c_ctr_escalation_overview.html>

<https://www.ibm.com/support/knowledgecenter/SSLKT6_7.6.0.5/com.ibm.mbs.doc/escalation/t_work_escalations.html>

<https://www.ibm.com/support/knowledgecenter/SSLKT6_7.6.0.5/com.ibm.mbs.doc/escalation/t_activating_escalations.html>

## Configuration of fields for Integration to Slack

Field additions for Integration to Slack

To interconnect IBM Control Desk and Slack and push and pull data from the systems it is necessary to add fields in Control Desk to display Slack data. To do so follow these steps:

In Database Configuration

1) Add new attribute CASE\_SC\_TRENDING to TICKET table. ALN(300), Trending Slack Channel

2) Add new attribute CASE\_SLACK\_CHANNEL to TICKET table. ALN(300), Supporting Slack Channel.

3) Turn on Admin mode

4) Apply Configuration Changes

5) Turn off Admin mode

In Application Designer

6) Add new attribute INCIDENT.CASE\_SC\_TRENDING and INCIDENT.CASE\_SLACK\_CHANNEL to Incident application above the Service Group.

## send a message to Slack when the status of the ticket changes to CLOSED

To send a message to Slack when the status of the ticket changes to CLOSED

**Create Script with Action Launch Point**

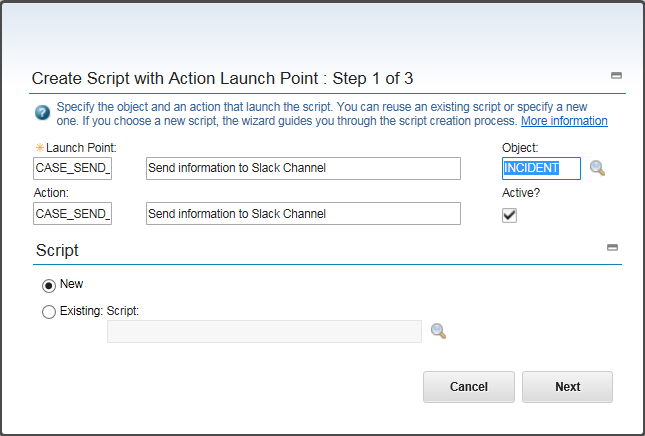
1. Call script SendToSlack.sh (on Linux) with 3 parameters

CASE\_SLACK\_CHANNEL: SlackChannel

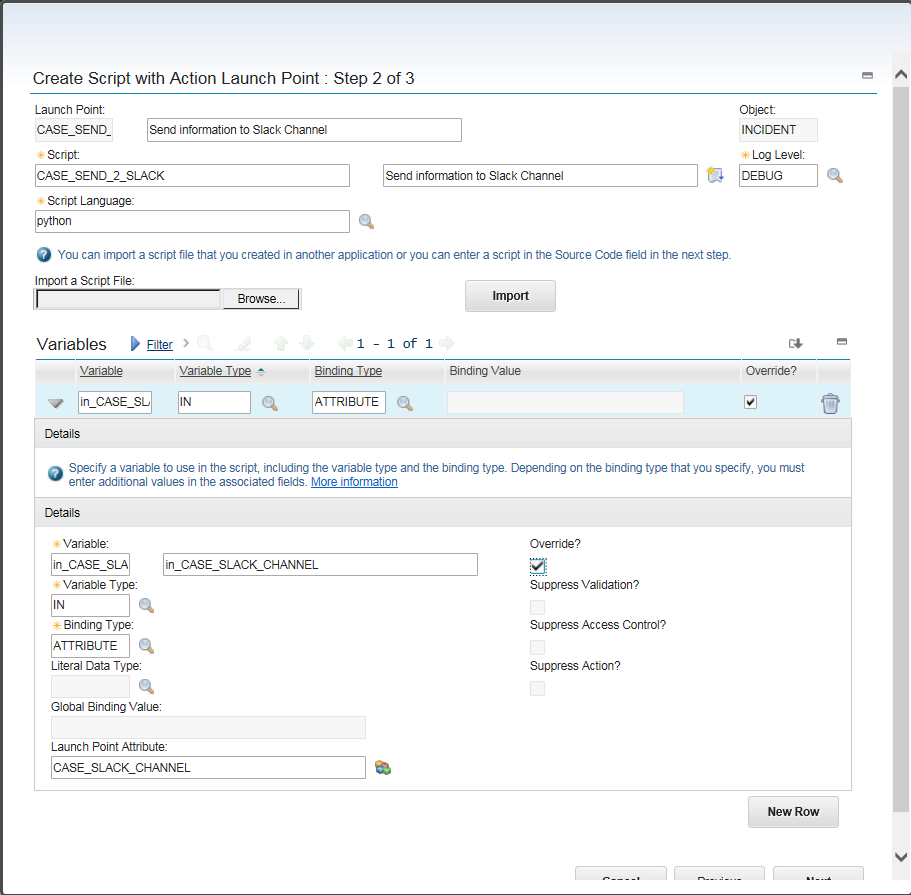
TICKETID: Ticket #

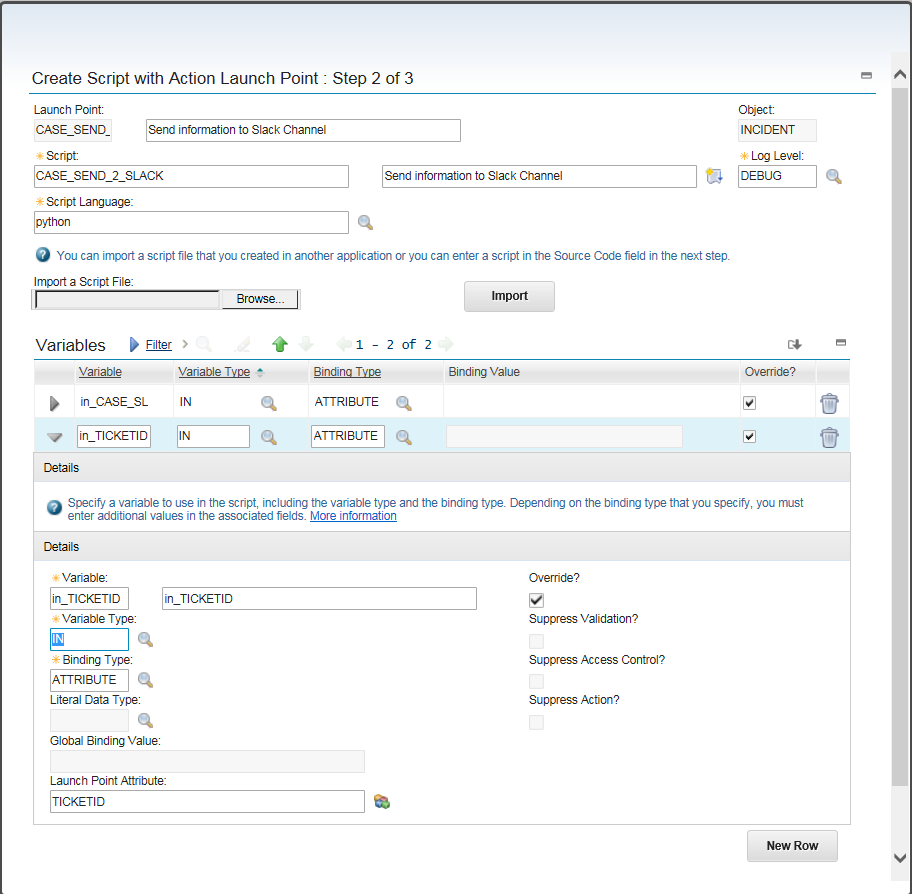
STATUSDATE: Date of closure

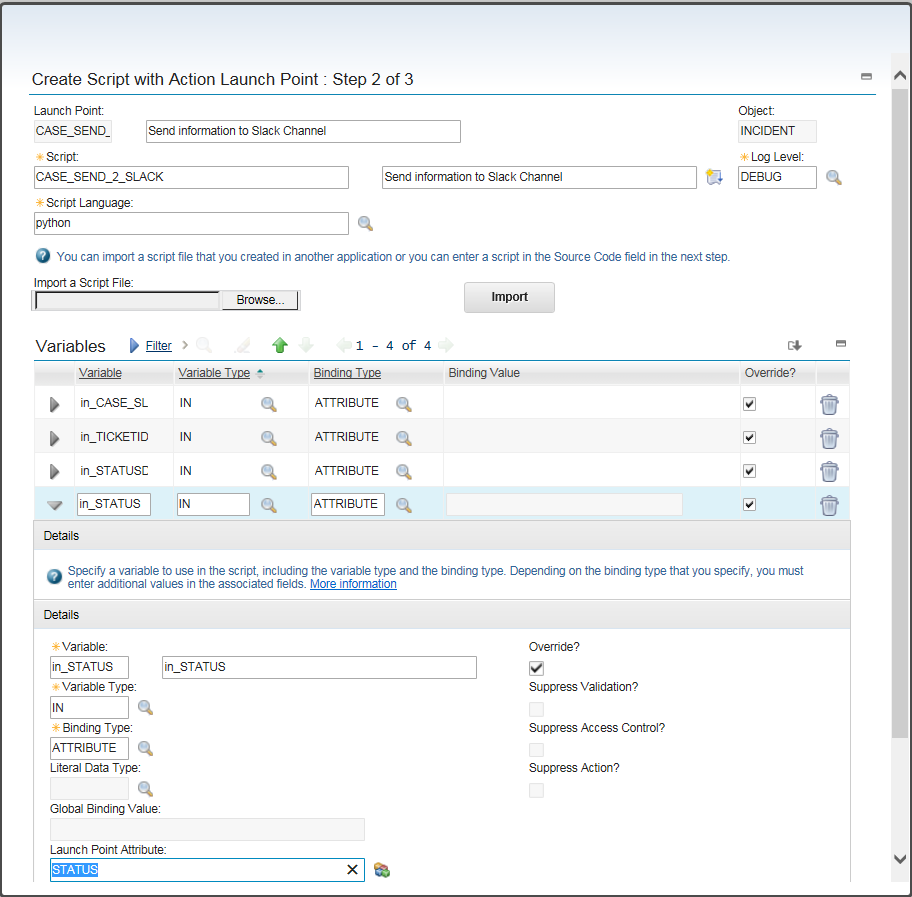
1. Go To -> System Configuration -> Platform Configuration -> Automation Scripts
2. More Action -> Create -> Script with Action Launch Point
3. CASE\_SEND\_2\_SLACK
4. Send information to Slack Channel

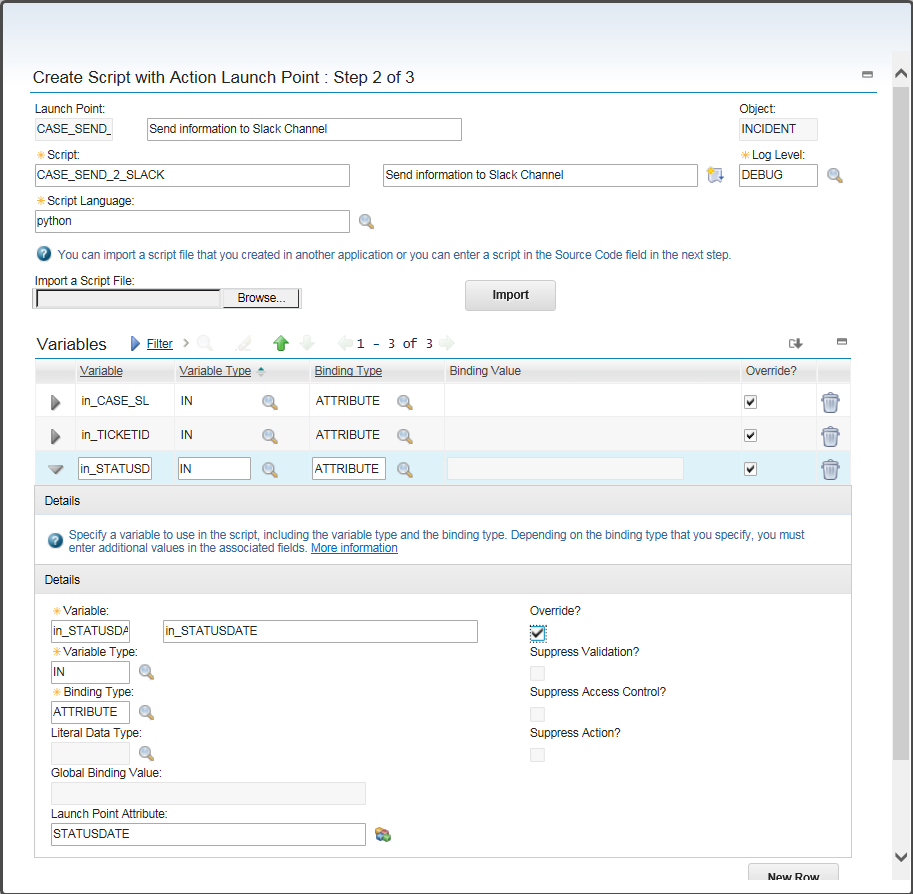


1. To define 4 parameters for the script



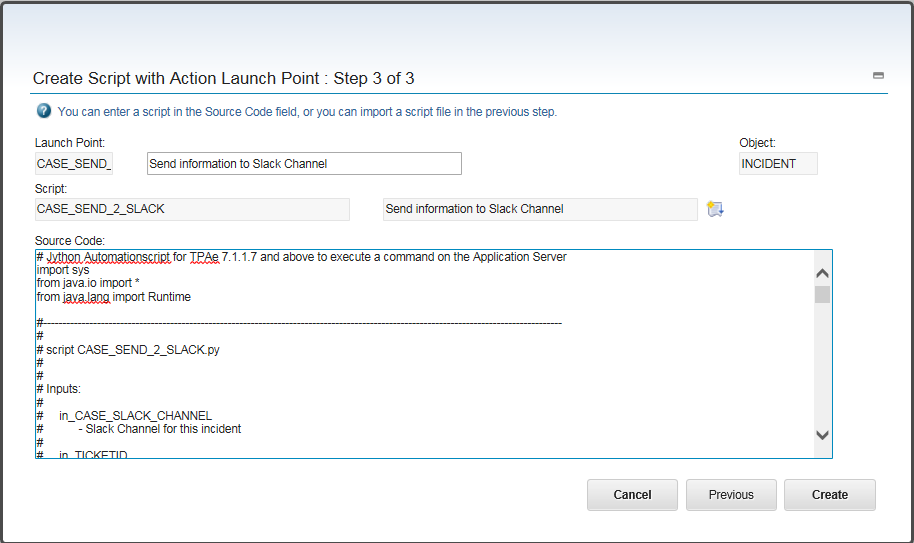






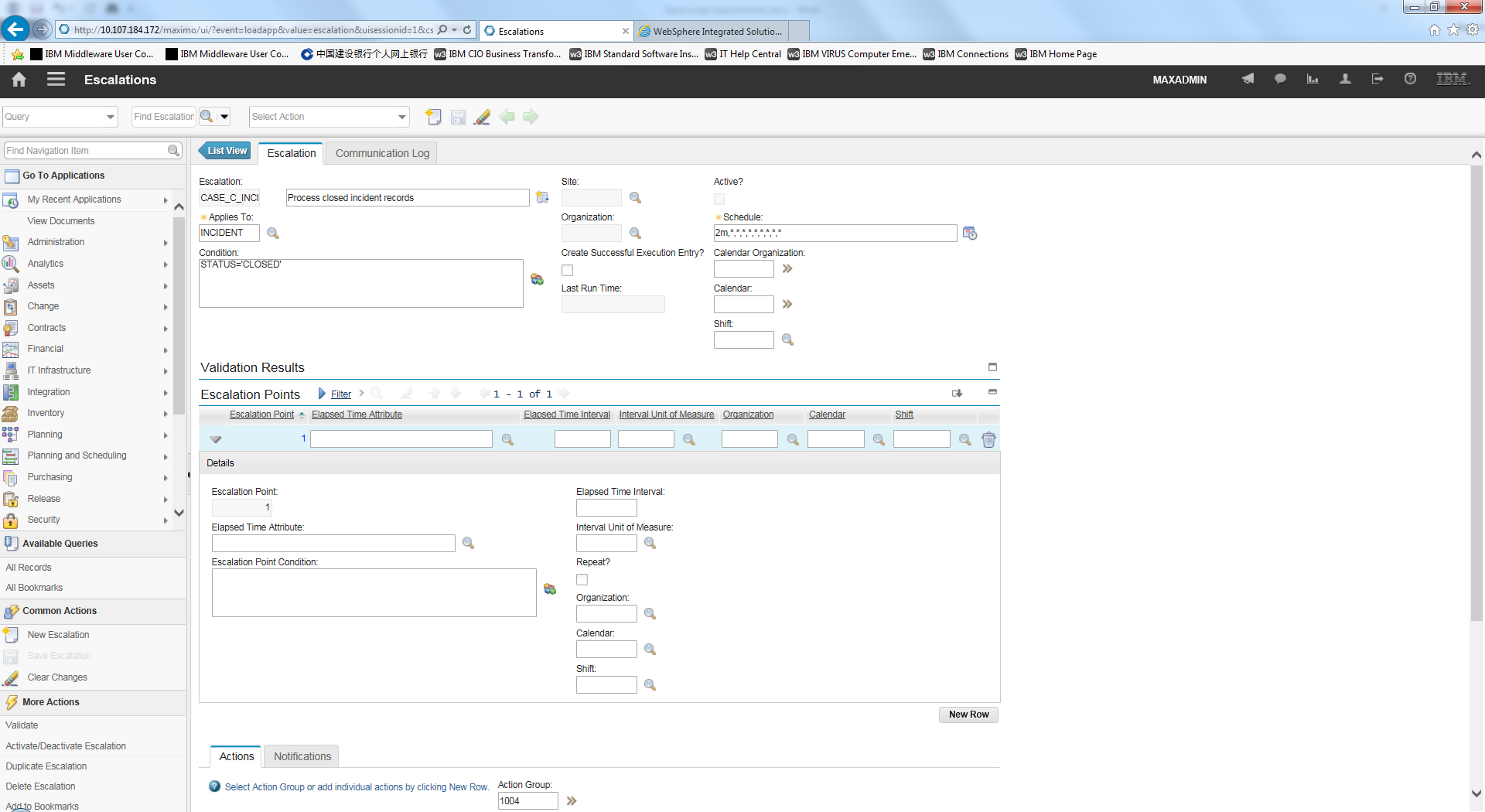
1. Copy and paste the script “Create Script with Action Launch Point” found on GitHub using this URL.

<https://github.com/ibm-cloud-architecture/refarch-cloudnative-csmo/commit/2822d503335dcc43a56007e8299480c54dc6684f>

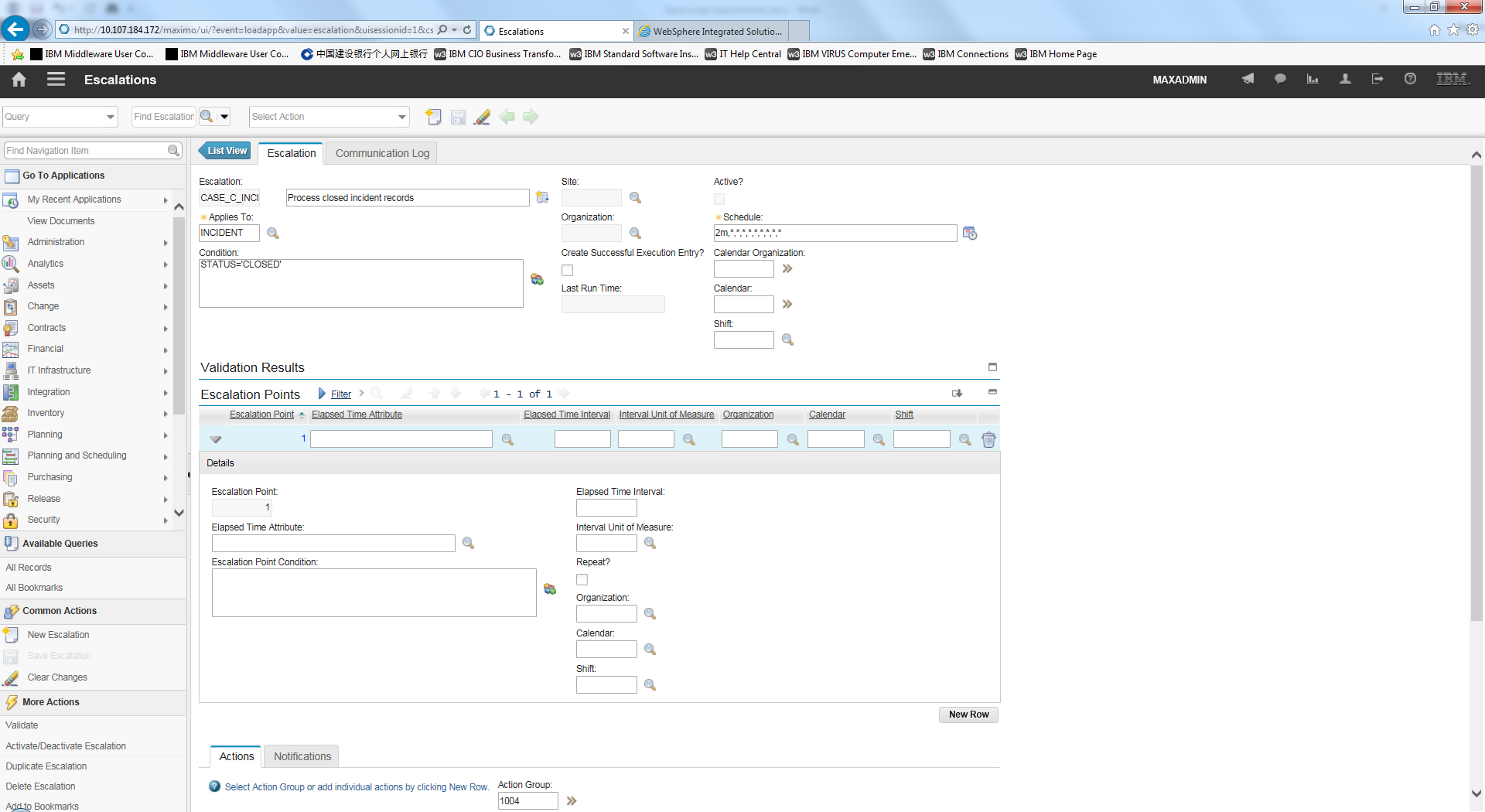


**Creating Escalation**

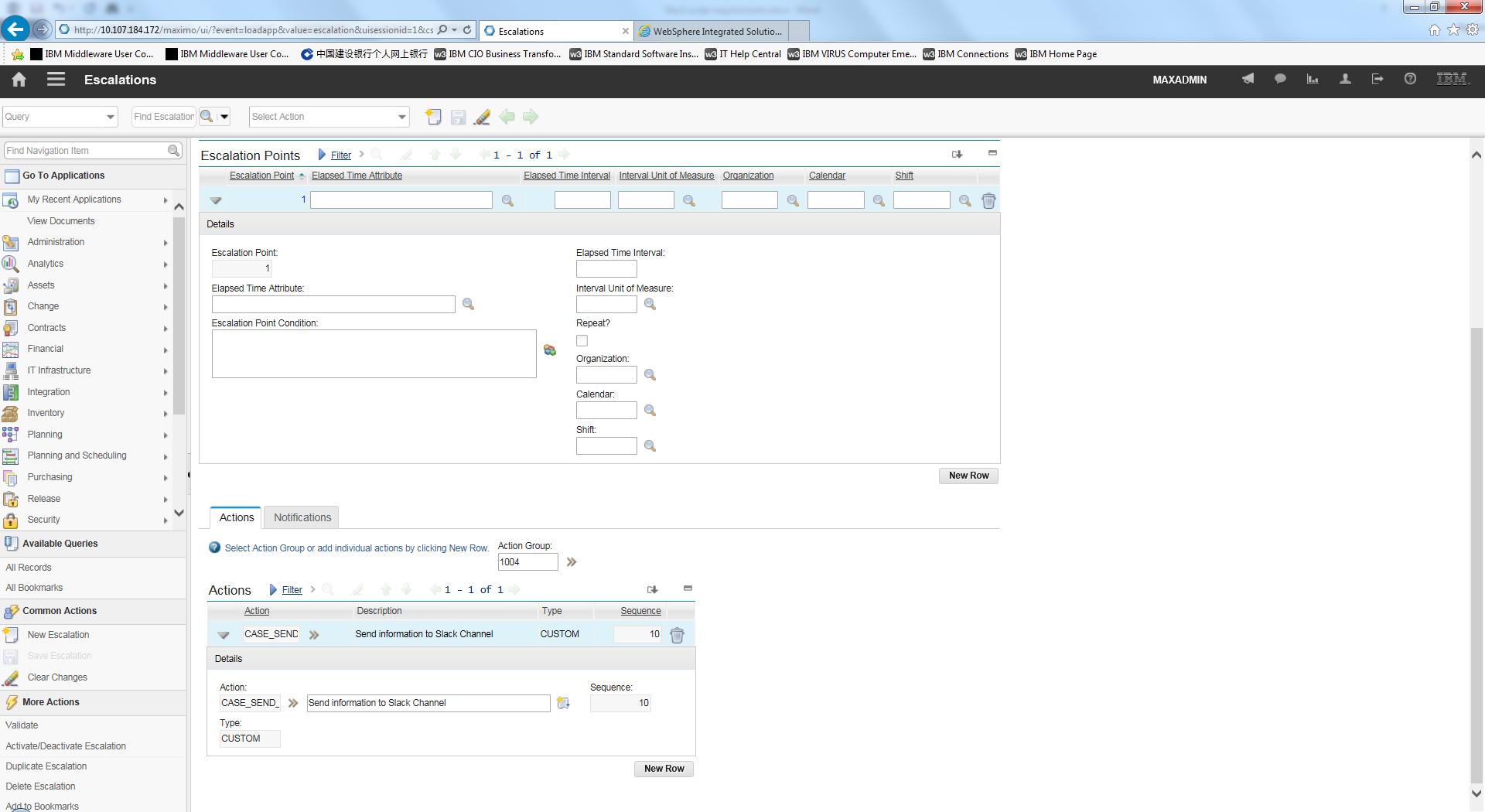
1. Go To -> System Configuration -> Platform Configuration -> Escalations
2. CASE\_C\_INCIDENTS
3. Process closed incident records
4. INCIDENT
5. STATUS=='CLOSED'
6. 2m,\*,\*,\*,\*,\*,\*,\*,\*,\*



1. Add one escalation point



1. Add one Action,
2. CASE\_SEND\_2\_SLACK



1. Validate
2. Activate

# How to setup the Integration of NOI with IBM Control Desk

## Netcool Operations Insight to Control Desk Integration

Please note that, for historical reasons, many of the technical assets are called Maximo, TSRM or SCCD as well as ICD. These all refer to the same product and are functionally synonyms.

### TSRM gateway installation

The integration is based on the TSRM gateway.

Install the TSRM gateway per the standard IBM instructions detailed in the following link and adjusted by any local requirements (H/A considerations, etc...)

[Gateway documentation](http://www.ibm.com/support/knowledgecenter/SSSHTQ/omnibus/gateways/tsrmgw/wip/concept/tsrmgw_intro.html)

[Gateway download instructions](https://www-304.ibm.com/support/docview.wss?uid=swg21610165)

The following videos explain how to perform the basic installation and configuration:

<https://www.youtube.com/watch?v=tb3xNZLwgDo>

<https://www.youtube.com/watch?v=ifK8tq66pug>

### 

### Basic TSRM gateway configuration:

After installing the gateway, configure it to communicate with ICD and test the base configuration before implementing the customizations detailed in section 8.1.3

<http://www.ibm.com/support/knowledgecenter/en/SSSHTQ/omnibus/gateways/tsrmgw/wip/reference/tsrmgw_install_overview.html>

<http://www.ibm.com/support/knowledgecenter/en/SSSHTQ/omnibus/gateways/tsrmgw/wip/reference/tsrmgw_test_connection.html>

#### Journal updates:

To enable NOI to update ICD with any NOI Journal entries or Slack messages, the journal integration must be activated as documented as follows:

<http://www.ibm.com/support/knowledgecenter/SSSHTQ/omnibus/gateways/tsrmgw/wip/reference/tsrmgw_config_tsrm_integrationtoolkit.html>

<https://www.youtube.com/watch?v=UKnP1_hluFY>

#### Optional configurations:

The following configurations are not mandatory for NOI-ICD integration, but many customers implement them.

* [Extend the size of the summary field to match possible long NOI messages](http://www.ibm.com/support/knowledgecenter/en/SSSHTQ/omnibus/gateways/tsrmgw/wip/reference/tsrmgw_config_summary_field.html)
* [Create a custom message object for improved performance](http://www.ibm.com/support/knowledgecenter/en/SSSHTQ/omnibus/gateways/tsrmgw/wip/reference/tsrmgw_config_impr_perf.html)
* [Fine tuning the performance of gateway event processing](http://www.ibm.com/support/knowledgecenter/en/SSSHTQ/omnibus/gateways/tsrmgw/wip/reference/tsrmgw_config_fine_tune.html)

### Integration customizations:

The best practices in this guide depend on the following customizations to the default integration:

For the purposes of this documentation, it is assumed that the gateway has been named G\_ICD.

#### Change Ticket content details

The configuration file $NCHOME/ netcool/omnibus/gates/tsrm/tsrm.mapping contains the translation between NOI field and ICD fields.

The default mapping

|  |
| --- |
| CREATE MAPPING StatusMap  (  'CLASS' = 'INCIDENT',  'DESCRIPTION' = '@Node' + ":" + '@Summary' ON INSERT ONLY,  'REPORTEDBY' = 'NETCOOL' ON INSERT ONLY,  'REPORTDATE' = TO\_TIME('@FirstOccurrence') ON INSERT ONLY,  'REPORTEDPRIORITY' = Lookup('@Severity','SeverityTable') ON INSERT ONLY,  'STATUS' = Lookup('@Severity', 'StatusTable'),  'TTNumber' = '@TTNumber'  );  CREATE MAPPING JournalMap  (  'CLASS' = 'INCIDENT',  'Chrono' = '@Chrono',  'CREATEDATE' = TO\_TIME('@Chrono'),  'DESCRIPTION' = 'NETCOOL JOURNAL ENTRY',  'DESCRIPTION\_LONGDESCRIPTION' = TO\_STRING('@Text1') + TO\_STRING('@Text2') + TO\_STRING('@Text3'),  'ServerName' = STATUS.SERVER\_NAME,  'ServerSerial' = STATUS.SERVER\_SERIAL  ); |

Should be changed to:

|  |
| --- |
| CREATE MAPPING StatusMap  (  'CLASS' = 'INCIDENT',  'DESCRIPTION' = '@Node' + ":" + '@Summary' ON INSERT ONLY,  'EXTERNALSYSTEM' = 'EVENTMANAGEMENT' ON INSERT ONLY,  'REPORTDATE' = TO\_TIME('@FirstOccurrence') ON INSERT ONLY,  'REPORTEDPRIORITY' = Lookup('@Severity','SeverityTable') ON INSERT ONLY,  'STATUS' = Lookup('@Severity', 'StatusTable'),  'TTNumber' = '@TTNumber'  );  CREATE MAPPING JournalMap  (  'CLASS' = 'INCIDENT',  'Chrono' = '@Chrono',  'CREATEDATE' = TO\_TIME('@Chrono'),  'DESCRIPTION' = TO\_STRING('@Text1'),  'DESCRIPTION\_LONGDESCRIPTION' = TO\_STRING('@Text1') + TO\_STRING('@Text2') + TO\_STRING('@Text3'),  'ServerName' = STATUS.SERVER\_NAME,  'ServerSerial' = STATUS.SERVER\_SERIAL  ); |

#### Add Journal entry for new ticket

It can be useful to add automated journal entries to NOI when ICD tickets are created or changed.

The simplest way to implement this is by adding a new trigger to the NOI Object Server.

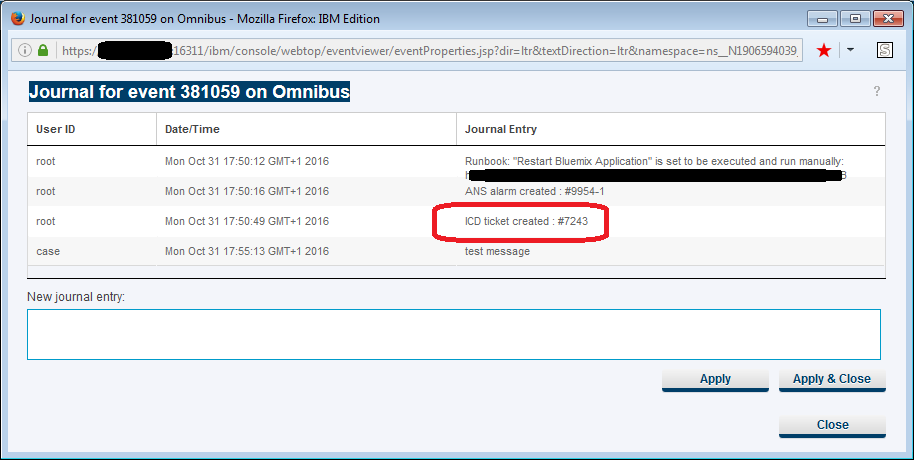
Upload the file CASE\_NOI-ICD-Journal.sql to the OMNIbus server and run the following command:

|  |
| --- |
| $OMNIHOME/bin/nco\_sql -user <username> -password <password> -server <server\_name> < /tmp/CASE\_NOI-ICD-Journal.sql |

Further documentation may be found at: [https://www.ibm.com/support/knowledgecenter/SSSHTQ\_8.1.0/com.ibm.netcool\_OMNIbus.doc\_8.1.0/OMNIbus/wip/admin/task/omn\_adm\_sql\_fw\_startingsqlintintface.html](https://www.ibm.com/support/knowledgecenter/SSSHTQ_8.1.0/com.ibm.netcool_OMNIbus.doc_8.1.0/omnibus/wip/admin/task/omn_adm_sql_fw_startingsqlintintface.html)

If you have multiple ObjectServers, you must run this command multiple times.

The trigger waits for ICD to send an update to NOI with the new ticketID and then writes a journal entry on the event.



If there is integration between NOI and Slack, the journal update will be forwarded to Slack too.

#### Automate Ticket creation

Omnibus triggers can automate many tasks, such as creating ICD tickets for new events.

Two such triggers are CASE\_ICD\_Forward\_NewEvent and CASE\_ICD\_Forward\_UpdatedEvent. The first will create an ICD ticket when a new incoming event matches a specific condition (i.e. severity is 5/Critical) and the second will create a ticket when an event changes to match a specific condition (i.e. an operator or another automation raised the severity of the event).

Make this change by loading the CASE\_NOI-ICD-NewTicketTriggers.sql file into the OMNIbus ObjectServer.

Upload the file to the OMNIbus server and run the following command:

|  |
| --- |
| $OMNIHOME/bin/nco\_sql -user <username> -password <password> -server <server\_name> < /tmp/ CASE\_NOI-ICD-NewTicketTriggers.sql |

You can change the threshold either by modifying the SQL file and re-loading it or by changing the trigger in Omnibus Admin console.

#### Synchronize more fields between NOI and ICD

The file tsrm.map controls which NOI fields are sent to ICD tickets and in what format, as documented in <https://www.ibm.com/support/knowledgecenter/SSWDVU_1.1.0/com.ibm.iteo.doc/install_cfgitsmgate.html>

In order to add more fields, such as the OWNER of the ticket, an extra mapping table must be added to the beginning of the file:

CREATE LOOKUP UserTable (  
 {0 , 'MAXADMIN'},  
 {1 , 'ICDUser #1'},  
 {2 , 'ICDUser #2 },  
 {65534, '' } )

DEFAULT = '' ;

And further on:

CREATE MAPPING StatusMap  
(  
 'CLASS' = 'INCIDENT',   
 'OWNER' = Lookup('@OwnerUID','UserTable'),

Take care to keep the UserTable updated with the relevant mapping between NOI user id numbers and ICD user names.

The file NOI-ICD-modifications.zip includes an example of the modified file.

#### Add new statuses to Ticket status

By default, the only change in status NOI pushes to ICD is RESOLVED when the event status changes to Clear (0). To send more statuses (for example, updating the status to INPROG when a user takes ownership of an event in NOI) we will need to make the following changes:

* Create a new field in the NOI schema, called CASE\_ICD\_Status which will hold the status to be pushed to ICD
* Modify the tsrm.map file so the ICD STATUS field is mapped to CASE\_ICD\_Status and not to Severity
* Add an Omnibus trigger, CASE\_Update\_ICD\_Status, to modify the value of CASE\_ICD\_Status when the owner of a ticket changes or the severity of the ticket changes to 0.
* Add an Omnibus trigger, CASE\_Update\_ICD\_Status\_onDeDup, to make the same modification when the event is changed by an incoming event message instead of by updating an existing message.

The file NOI-ICD-modifications.zip includes the modified files and instructions.

#### Add tools to NOI dashboard

The two tools added here are:

* An operator wishes to open an ICD ticket on an existing event.  
  This is implemented with an SQL tool which runs the following command:  
  update alerts.status set LogTicket =1 where Serial in ( $selected\_rows.Serial );
* An operator wishes to launch into ICD to view the ticket.  
  This is implemented with a script tool which runs the following script:  
  var str = "{@TTNumber}";  
  if (str != "") {   
   window.open ("http://<ICDserver>/maximo/ui/maximo.jsp?event=loadapp&value=incident&additionalevent=useqbe&additionaleventvalue=ticketid=" + str);  
  }  
  else  
  {  
   window.alert("This event has no Control Desk ticket associated");  
  }

The file NOI-ICD-modifications.zip includes the tools and instructions.

#### Update the description of journal/workorders.

If it is setup, then NOI forwards journals entries to work orders that are attached to the Incident. However, by default the description of the work order is hardcoded to NETCOOL JOURNAL ENTRY which means that users must unfurl the work order to see the true description.   
By changing the JournalMap section of the tsrm.map file from

'DESCRIPTION' = 'NETCOOL JOURNAL ENTRY',

to

'DESCRIPTION' = TO\_STRING('@Text1'),

then the proper text is visible much more easily.

Note that you will need to extend the size of the WORKORDER.DESCRIPTION field to accommodate the possible longer length of the journal entry (see section 7.1.2.2 for a similar change done to the ticket's summary field.

The file NOI-ICD-modifications.zip includes a modified tsrm.map file.

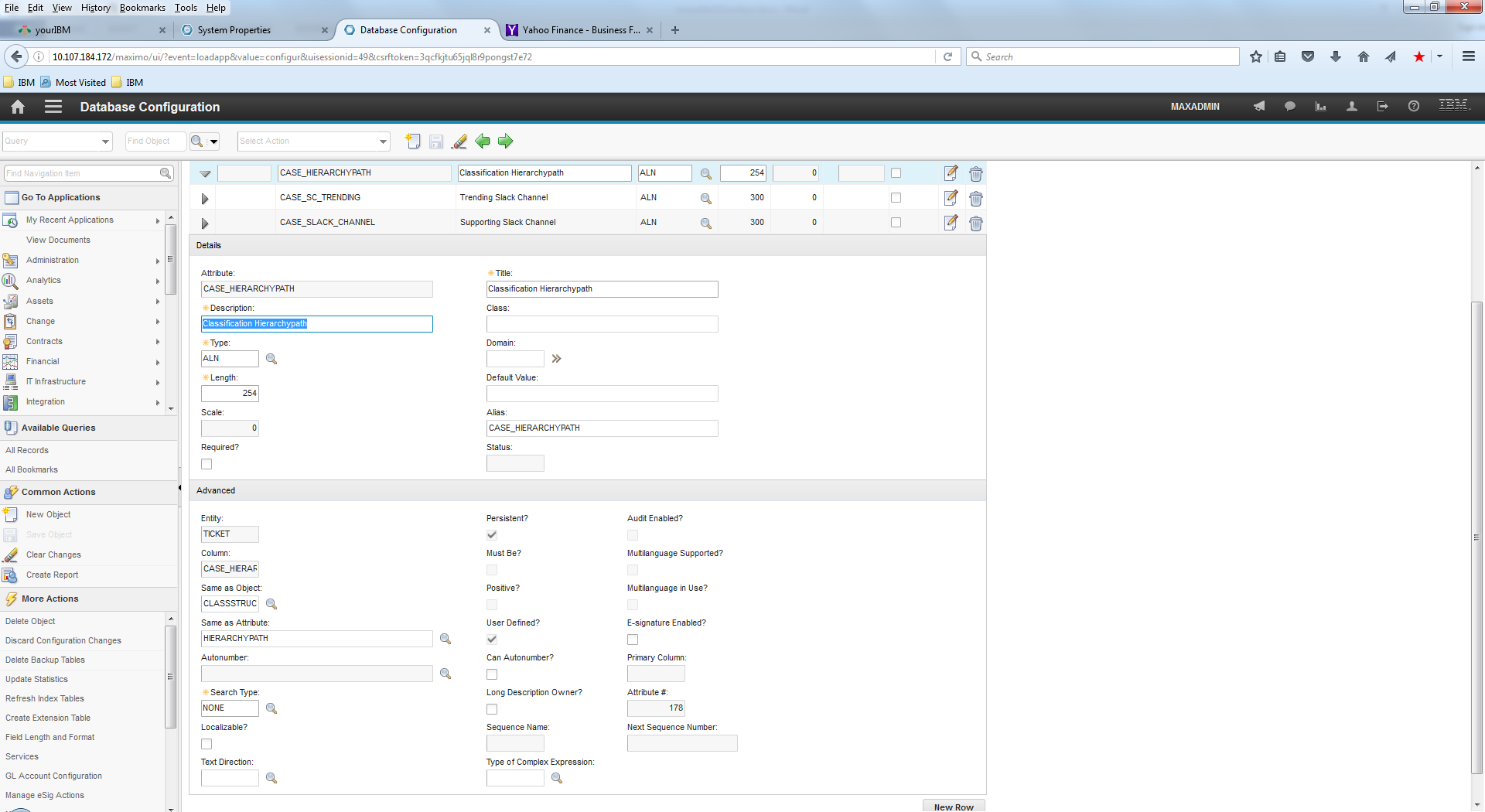
#### Synchronize more fields between ICD and NOI

By default, the only field that is synchronized back to NOI from ICD is the ticket status (field STATUS in ICD and field TicketStatus in NOI). Adding more fields is done by implementing the steps detailed in the following link: <https://www.ibm.com/support/knowledgecenter/SSSHTQ/omnibus/gateways/tsrmgw/wip/reference/tsrmgw_generating_tickets.html>

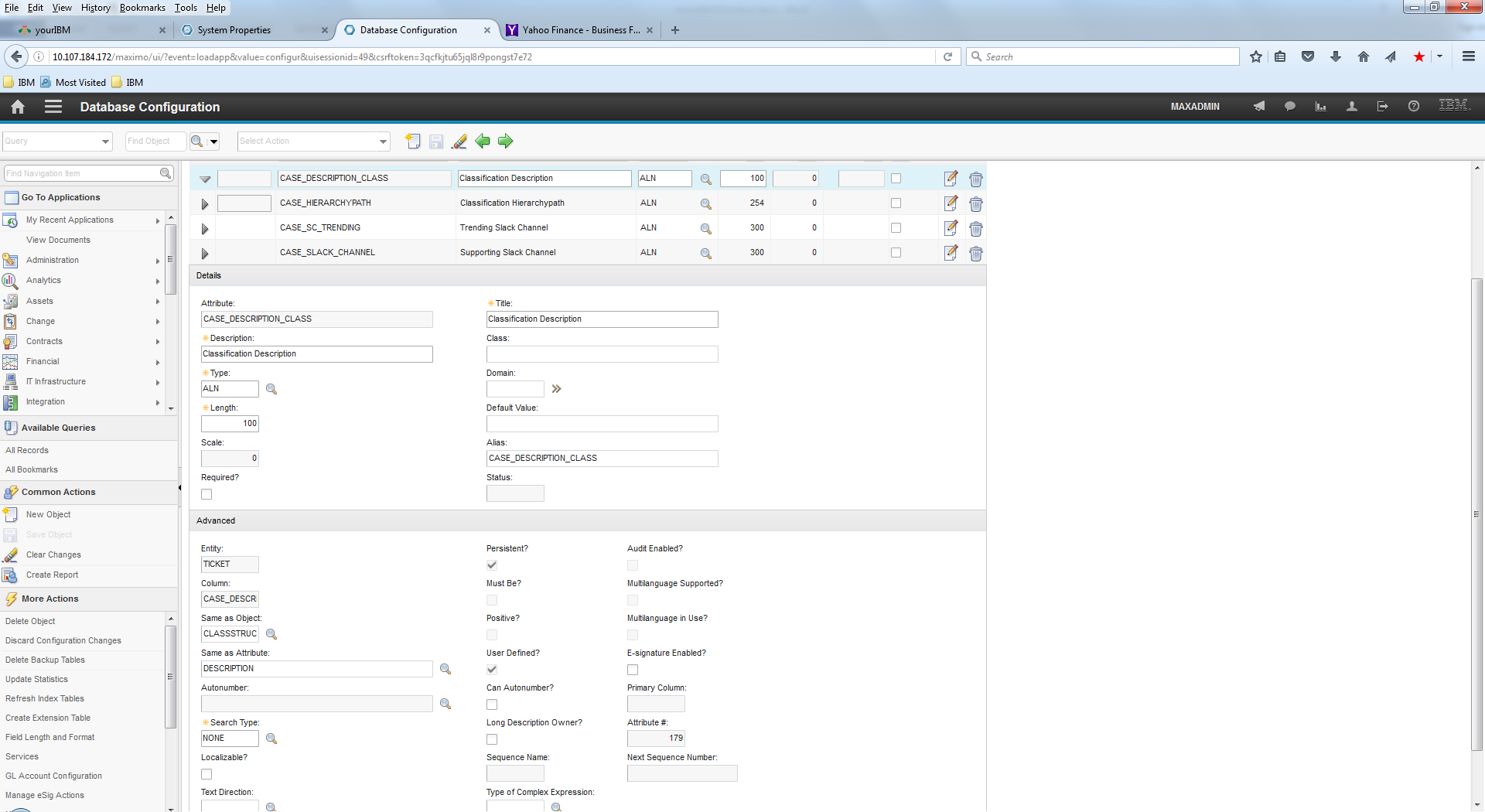
In short, the extra field is configured in **Integration > Object Structures** in ICD and in **$OMNIHOME/gates/tsrm/tsrm.script** in NOI.

One of the most important ticket attributes to synchronize is the DESCRIPTION\_CLASS, the human readable version of the ticket's classification. This field cannot be synchronized using the standard implementation because the attributes HIERARCHYPATH and DESCRIPTION\_CLASS do not reside in Incident record (in its child record CLASSSTRUCTURE), and NOI is not able to sync with the Control Desk system without a configuration change to the Ticket Table.

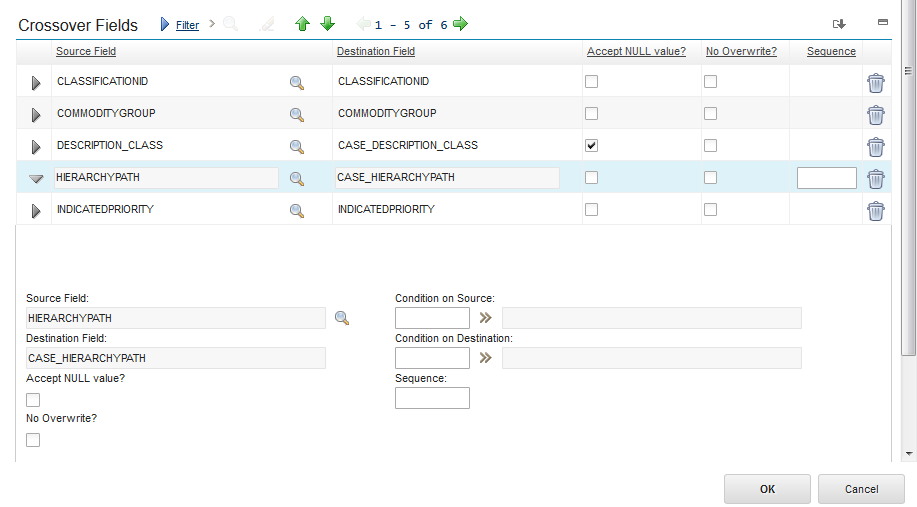
1. Adding attribute CASE\_HIERARCHYPATH to TICKET table

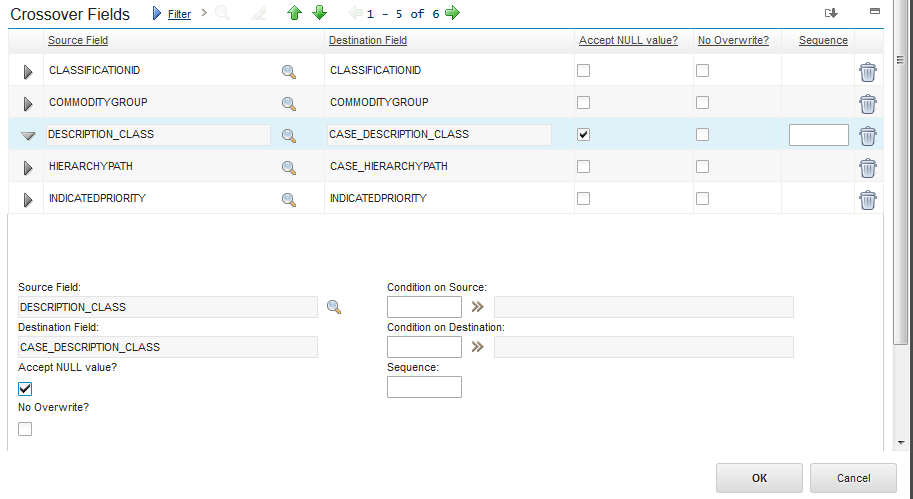


1. Adding attribute CASE\_DESCRIPTION\_CLASS to TICKET table



1. Adding Crossover Fields to domain TSDCLSSTRUCT2TK





The file SynchDescriptionClass\_ICDtoNOI.zip contains the modifications to **$OMNIHOME/gates/tsrm/tsrm.script** and an SQL file to add the field to the NOI schema.

# Conclusion

Hopefully this document assists you in setting up IBM Control Desk, enabling it through an integration with Netcool Operations Insight, and Slack, thus enabling a Service Management toolchain for your applications quickly and efficiently.

For more information about IBM Control Desk see: <http://www-03.ibm.com/software/products/en/control-desk>

# Glossary of Control Desk Terms

|  |  |
| --- | --- |
| Start Center | Dashboard page for first responder and site reliability engineer for when a user enters the UI of control Desk.  The portals and content that users see in the Start Center depends on the Start Center template that is assigned to their security group |
| Portlet | Portlets are segments of data presented on the start center based on queries and presented as lists or graphs. |
| Key Performance Indicators (KPIs) | KPIs are defined as metrics or measurements in Control Desk and presented on the start center as a portlet. |
| Incident | A record in Control Desk created to represent the issue or event occurring which needs resolution through automation or manual steps to resolve.  The incident will be the record where updates from NOI and Slack are recorded to then have a holistic view of the issue: when it occurred and what was the resolution and time frame of the resolution. |
| TSRM Gateway | TSRM Gateway is the terminology used for describing the Gateway used between IBM Control Desk and Netcool Operations Insight. |