IBM Resilient

Incident Response Platform API

Release Notes v28

Release Date: May 2017

Based on a knowledge base of incident response best practices, industry standard frameworks, and regulatory requirements, the Resilient Incident Response Platform helps make incident response efficient and compliant.

Features and Enhancements

The following enhancements have been made in the v28 release:

- **Artifact types**: The v28 release introduces custom artifact types. As a result, the artifact fields for type and value have been set to read-only. The description and relationship fields remain editable.
- **Search**: Search has been enhanced and a new set of API endpoints and methods have been created.

The following REST endpoints have been added:

- **OrgIncidentArtifactTypeREST**
  - Allows organizations to customize settings about their incident artifact types.
- **SearchExREST**
  - An endpoint for performing full text searches through incidents and incident child objects (tasks, incident comments, task comments, milestones, artifacts, incident attachments, task attachments, and data tables).
- **WorkflowREST**
  - Endpoints for managing workflows.

The following REST endpoints have been modified:

- **IncidentNoteREST**
  - The **query** method was added to provide a filtered list of comments related to a specific incident.
  - The **comments** method now returns a **CommentDTO** instead of an **IncidentCommentDTO**.

Licensed Materials – Property of IBM
© Copyright IBM Corp. 2010, 2017. All Rights Reserved.
US Government Users Restricted Rights: Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

- **TaskAttachmentREST**
    - The **query** method was added to provide a filtered list of attachments related to a specific task.
    - The **move** method was added to move an attachment to another object. Currently, a task attachment can only be moved to the task's parent incident.
- **TaskNoteREST**
    - The **query** method was added to provide a filtered list of comments related to a specific task.
    - The **comments** method now returns a **CommentDTO** instead of a **TaskCommentDTO**.

The following Data Transfer Objects (DTOs) have been created:

- **AttachmentResultsDTO**: Provides the results of a query on attachments.
- **CommentResultsDTO**: Provides the results of a query on comments.
- **MoveDTO**: Represents a move request for moving objects from one parent to another.
- **SearchExInputDTO**: Represents the parameters for performing a search.
- **SearchExResultDTO**: Represents a single result from a search.
- **SearchExResultsDTO**: Represents a list of results from a search.
- **TypedObjectReferenceDTO**: Represents a reference to an object and provides the type and name of the object along with information about child objects.
- **WorkflowContentDTO**: Contains the source content of a workflow (e.g., BPMN XML).
- **WorkflowDTO**: Contains information about a workflow.
- **WorkflowModelProblemDTO**: Provides information about workflow parsing problems.
- **WorkflowStatusDTO**: Indicates the status of a workflow deployment.

The following types have been added:

- **AttachmentType**: Used to indicate the type of an attachment.
- **CommentType**: Used to indicate the type of a comment.
- **ObjectHandleList**: Used to represent a list of ObjectHandle objects. Each item in the list can be either a name (string) or ID (integer).
- **TypeId**: Contains additional information about the type for conditions and notifications.

The following Data Transfer Objects (DTOs) have been modified:

- **AutomaticTaskDTO**
    - The **sort_type** input parameter was added to permit the results to be sorted as specified.
    - The **incident_types** field is deprecated in v28. In v27, incident types are no longer associated with automatic tasks directly. This field was preserved in V28 to provide information about actions that had conditions on incident type. However, attempting to create automatic tasks with incident types results in an error. Use the **ActionREST** endpoint to manage actions and conditions (including incident type conditions).

- **ConstDTO:** The following fields were deprecated:
    - Starting with version 28, **artifact_types** returns only the standard built-in system artifact types. Using this data structure, the **IncidentArtifactTypeDTO** has only the following fields filled in:
        - id
        - name
        - desc
        - reg_exp
        - multi_aware
        - file
    - Use **OrgREST** to get the entire list of artifact types (both system and custom) from **FullOrgDTO.incident_artifact_types**. For create, update, and delete operations on artifact types use the **OrgIncidentArtifactTypeREST** resource.
- **FullOrgDTO:**
    - The **artifact_types** property has changed to be **incident_artifact_types**.
- **IncidentArtifactTypeDTO:** The following fields were added:
    - programmatic_name
    - uuid
    - parse_as_csv
    - use_for_relationships
    - system
    - split_on
    - version
    - enabled
    - export_key
- **NotificationDTO**: Prior to version 28, the template definition and substitution values were provided so the API client can perform substitution. Starting with version 28, the template functionality has been expanded, and substitution is performed on the server and provided back as part of the object. Additionally, the following fields have been deprecated:
    - inc_id
    - inc_training
    - task_name
    - task_id
    - comment_text
    - comment_id
- **TaskDTO**: The following fields were deprecated in v27 and **removed** in v28:
    - src_name
    - auto_task_id

The following DTOs are deprecated in this release.

- **CategorySearchResultDTO**: Please use SearchExResultsDTO instead.
- **IncidentArtifactResultDTO**: Please use the IncidentArtifactDTO instead.
- **IncidentCommentDTO**: Please use the CommentDTO instead.
- **IncidentResultDTO:** Please use IncidentArtifactTypeDTO instead.
- **OrgIncidentArtifactTypeDTO:** Please use IncidentArtifactTypDTO instead.
- **SearchInputDTO**: Please use SearchExInputDTO instead.
- **TaskCommentDTO**: Please use the CommentDTO instead.

The behavior of the following endpoint was modified:

- **/orgs/{org_id}/incident_types/{id}:** DELETE will throw a 400 error if there is a condition that references the incident type being deleted. DELETE and PUT will throw a 400 error if the call attempts to remove or hide an incident type that is reference by a rule..