## Use Case 1: Adding a record

### Targeted Release

Initial Release

### Main Success Scenario

An “Add Record” request is received by the system. The request data is validated and sanitized. The security token is extracted from the request. The security token is sent to the Authentication Server for validation. The system receives a response from the Authentication Server. The requester’s system role is identified using information received from the Authentication Server. If the requester is an Administrator or Contributor, a new record is added to the database using the data contained in the request.

### Alternate Scenarios

If the request contains invalid data, an error response is returned to the requester.

If the Authentication Server is not reachable or times out, an error response is returned to the requester.

If the security token does not exist, is not valid, or is expired, an error response is returned to the requester.

If the requester is not an Administrator or Contributor, an error response is returned to the requester.

If the addition of the record to the database is not successful, an error response is returned to the requester.

## Use Case 2: Deleting a Record

### Targeted Release

Initial Release

### Main Success Scenario

A “Delete Record” request is received by the system. The request data is validated and sanitized. The security token is extracted from the request. The security token is sent to the Authentication Server for validation. The system receives a response from the Authentication Server. The requester’s system role is identified using information received from the Authentication Server. The target record is found in the database. If the requester is an Administrator or the Contributor that created the target record, the target record is removed from the database.

### Alternate Scenarios

If the request contains invalid data, an error response is returned to the requester.

If the Authentication Server is not reachable or times out, an error response is returned to the requester.

If the security token does not exist, is not valid, or is expired, an error response is returned to the requester.

If the requester is not an Administrator or the Contributor that created the target record, an error response is returned to the requester.

If the deletion of the record from the database is not successful, an error response is returned to the requester.

## Use Case 3: Listing all records

### Targeted Release

Initial Release

### Main Success Scenario

A “List All Records” request is received by the system. The request data is validated and sanitized. The security token is extracted from the request. The security token is sent to the Authentication Server for validation. The system receives a response from the Authentication Server. The requester’s system role is identified using information received from the Authentication Server. If the requester possesses a system role, all the records in the database are retrieved, validated, sanitized, and returned to the requester.

### Alternate Scenarios

If the request contains invalid data, an error response is returned to the requester.

If the Authentication Server is not reachable or times out, an error response is returned to the requester.

If the security token does not exist, is not valid, or is expired, an error response is returned to the requester.

If the requester does not possess a system role, an error response is returned to the requester.

If the records cannot be retrieved from the database, an error response is returned to the requester.

If the data retrieved from the database is invalid, an error response is returned to the requester.

## Use Case 4: Commenting on a Record

### Targeted Release

Initial Release

### Main Success Scenario

An “Add Comment” request is received by the system. The request data is validated and sanitized. The security token is extracted from the request. The security token is sent to the Authentication Server for validation. The system receives a response from the Authentication Server. The requester’s system role is identified using information received from the Authentication Server. The targeted record is found in the database and a new comment is added to it using the data contained in the request.

### Alternate Scenarios

If the request contains invalid data, an error response is returned to the requester.

If the Authentication Server is not reachable or times out, an error response is returned to the requester.

If the security token does not exist, is not valid, or is expired, an error response is returned to the requester.

If the requester does not possess a system role, an error response is returned to the requester.

If the targeted record could not be retrieved from the database, an error response is returned to the requester.

If the new comment could not be added to the record, an error response is returned to the requester.

## Use Case 5: Deleting a Comment

### Targeted Release

Initial Release

### Main Success Scenario

A “Delete Comment” request is received by the system. The request data is validated and sanitized. The security token is extracted from the request. The security token is sent to the Authentication Server for validation. The system receives a response from the Authentication Server. The requester’s system role is identified using information received from the Authentication Server. If the requester is an Administrator or the Contributor that created the comment, the targeted comment is found in the database is deleted.

### Alternate Scenarios

If the request contains invalid data, an error response is returned to the requester.

If the Authentication Server is not reachable or times out, an error response is returned to the requester.

If the security token does not exist, is not valid, or is expired, an error response is returned to the requester.

If the requester is not an Administrator or the Contributor or Commenter that created the comment, an error response is returned to the requester.

If removing the targeted comment from the database fails, an error response is returned to the requester.

## Use Case 6: Editing a Record

### Targeted Release

Upcoming Release

### Main Success Scenario

An “Edit Record” request is received by the system. The request data is validated and sanitized. The security token is extracted from the request. The security token is sent to the Authentication Server for validation. The system receives a response from the Authentication Server. The requester’s system role is identified using information received from the Authentication Server. If the requester is an Administrator or the Contributor that created the record, the edits defined in the request are applied to the target record.

### Alternate Scenarios

If the request contains invalid data, an error response is returned to the requester.

If the Authentication Server is not reachable or times out, an error response is returned to the requester.

If the security token does not exist, is not valid, or is expired, an error response is returned to the requester.

If the requester is not an Administrator or the Contributor that created the record, an error response is returned to the requester.

If editing the targeted record in the database fails, an error response is returned to the requester.

## Use Case 7: Editing a Comment

### Targeted Release

Upcoming Release

### Main Success Scenario

An “Edit Comment” request is received by the system. The request data is validated and sanitized. The security token is extracted from the request. The security token is sent to the Authentication Server for validation. The system receives a response from the Authentication Server. The requester’s system role is identified using information received from the Authentication Server. If the requester is the Contributor or Commenter that created the comment, the edits defined in the request are applied to the target comment.

### Alternate Scenarios

If the request contains invalid data, an error response is returned to the requester.

If the Authentication Server is not reachable or times out, an error response is returned to the requester.

If the security token does not exist, is not valid, or is expired, an error response is returned to the requester.

If the requester is not the Contributor or Commenter that created the comment, an error response is returned to the requester.

If editing the targeted comment in the database fails, an error response is returned to the requester.

## Use Case 8: Searching for a Record by Tags

### Targeted Release

Upcoming Release

### Main Success Scenario

A “Search by Tag” request is received by the system. The request data is validated and sanitized. The security token is extracted from the request. The security token is sent to the Authentication Server for validation. The system receives a response from the Authentication Server. The requester’s system role is identified using information received from the Authentication Server. All records matching the tag in the request are retrieved from the database, validated, sanitized, and returned to the user.

### Alternate Scenarios

If the request contains invalid data, an error response is returned to the requester.

If the Authentication Server is not reachable or times out, an error response is returned to the requester.

If the security token does not exist, is not valid, or is expired, an error response is returned to the requester.

If the requester does not possess a system role, an error response is returned to the requester.

If searching by the tag in the database fails, an error response is returned to the requester.

If the data retrieved from the database are invalid, an error response is returned to the requester.

## Use Case 9: Searching for a Record by Creator

### Targeted Release

Upcoming Release

### Main Success Scenario

A “Search by Creator” request is received by the system. The request data is validated and sanitized. The security token is extracted from the request. The security token is sent to the Authentication Server for validation. The system receives a response from the Authentication Server. The requester’s system role is identified using information received from the Authentication Server. All records created by the target user are retrieved from the database, validated, sanitized, and returned to the user.

### Alternate Scenarios

If the request contains invalid data, an error response is returned to the requester.

If the Authentication Server is not reachable or times out, an error response is returned to the requester.

If the security token does not exist, is not valid, or is expired, an error response is returned to the requester.

If the requester does not possess a system role, an error response is returned to the requester.

If retrieving the records created by the target users from the database fails, an error response is returned to the requester.

If the data retrieved from the database is invalid, an error response is returned to the requester.

## Use Case 10: Searching for a Record by Phrase

### Targeted Release

Upcoming Release

### Main Success Scenario

A “Search by Phrase” request is received by the system. The request data is validated and sanitized. The security token is extracted from the request. The security token is sent to the Authentication Server for validation. The system receives a response from the Authentication Server. The requester’s system role is identified using information received from the Authentication Server. All records containing the phrase in the request are retrieved from the database, validated, sanitized, and returned to the user.

### Alternate Scenarios

If the request contains invalid data, an error response is returned to the requester.

If the Authentication Server is not reachable or times out, an error response is returned to the requester.

If the security token does not exist, is not valid, or is expired, an error response is returned to the requester.

If the requester does not possess a system role, an error response is returned to the requester.

If searching by the phrase in the database fails, an error response is returned to the requester.

If the data retrieved from the database is invalid, an error response is returned to the requester.

## Use Case 11: Requesting the history of a record

### Targeted Release

Upcoming Release

### Main Success Scenario

A “Resource History” request is received by the system. The request data is validated and sanitized. The security token is extracted from the request. The security token is sent to the Authentication Server for validation. The system receives a response from the Authentication Server. The requester’s system role is identified using information received from the Authentication Server. If the requester is an Administrator, the history records of the targeted record are retrieved from the database, validated, sanitized, and returned to the requester.

### Alternate Scenarios

If the request contains invalid data, an error response is returned to the requester.

If the Authentication Server is not reachable or times out, an error response is returned to the requester.

If the security token does not exist, is not valid, or is expired, an error response is returned to the requester.

If the requester does not possess a system role, an error response is returned to the requester.

If retrieving the record history records the database fails, an error response is returned to the requester.

If the data retrieved from the database is invalid, an error response is returned to the requester.