User Adds Resource

Before a request is made, the user has acquired an authentication token from the proper source as a manager. The user then creates an html packet with the authentication in the header. The user then adds the proper data into the request for a new resource. The user then sends the html packet to the REST API server. The server then verifies authorization token with authorization API. If the authentication token is invalid, refer to Extension: Invalid Authentication Token. After the token if verified the server adds the new resource to the database. The server then sends a success code to the user.

User Deletes Resource

Before a request is made, the user has acquired an authentication token from the proper source as a manager. The user then creates an HTML packet with the authentication in the header. The user includes the identifier of the resource to be deleted in the request body or URL. The user then sends the HTML packet to the REST API server. The server verifies the authorization token with the authorization API. If the authentication token is invalid, refer to Extension: Invalid Authentication Token. After the token is verified, the server removes the specified resource from the database. The server then sends a success code to the user.

User Updates Resource

Before a request is made, the user has acquired an authentication token from the proper source as a manager. The user then creates an HTML packet with the authentication in the header. The user includes the updated data and the identifier of the resource to be modified in the request. The user then sends the HTML packet to the REST API server. The server verifies the authorization token with the authorization API. If the authentication token is invalid, refer to Extension: Invalid Authentication Token. After the token is verified, the server updates the resource in the database with the new data. The server then sends a success code to the user.

User Query's for Data by location

Before a request is made, the user has acquired an authentication token from the proper source as an employee or manager. The user then creates an HTML packet with the authentication in the header. The user includes the location parameter in the request. The user then sends the HTML packet to the REST API server. The server verifies the authorization token with the authorization API. If the authentication token is invalid, refer to Extension: Invalid Authentication Token. After the token is verified, the server queries the database for resources associated with the specified location. The server then sends the query results to the user.

User Query's for Data by employee

Before a request is made, the user has acquired an authentication token from the proper source as an employee or manager. The user then creates an HTML packet with the authentication in the header. The user includes the employee identifier in the request. The user then sends the HTML packet to the REST API server. The server verifies the authorization token with the authorization API. If the authentication token is invalid, refer to Extension: Invalid Authentication Token. After the token is verified, the server queries the database for resources assigned to the specified employee. The server then sends the query results to the user.

User Query's for Data by resource

Before a request is made, the user has acquired an authentication token from the proper source as an employee or manager. The user then creates an HTML packet with the authentication in the header. The user includes the resource identifier in the request. The user then sends the HTML packet to the REST API server. The server verifies the authorization token with the authorization API. If the authentication token is invalid, refer to Extension: Invalid Authentication Token. After the token is verified, the server queries the database for data related to the specified resource. The server then sends the query results to the user.

User Query's for Data by date assigned

Before a request is made, the user has acquired an authentication token from the proper source as an employee or manager. The user then creates an HTML packet with the authentication in the header. The user includes the date or date range in the request. The user then sends the HTML packet to the REST API server. The server verifies the authorization token with the authorization API. If the authentication token is invalid, refer to Extension: Invalid Authentication Token. After the token is verified, the server queries the database for resources assigned on the specified date. The server then sends the query results to the user.

Invalid Authentication Token

This use case is an extension that occurs after a user's authentication token is sent to the authentication API. The authentication API returns either a bad token or expired token. The server then sends a bad request error to the user.

User request is invalid

This use case is an extension that occurs after a user is authenticated and the request is sent to the database. The database returns an error code to the server. The server then sends a bad request to the user.