Detection list management APIs

Overview

You can manually manage users in the Departing Employees list (https://support.code42.com/Administrator/Cloud/Code42_console_reference/Departing_Employees_reference) and High Risk Employees list (https://support.code42.com/Administrator/Cloud/Code42_console_reference/High_Risk_Employees_reference) from the Code42 console. To automate the process of managing users in these detection lists, you can write scripts that use the Detection List Management APIs (https://developer.code42.com/api/#tag/Detection-Lists). This article provides an introduction to the APIs.

Code42 Developer Portal

This article applies to non-Incydr product plans. If you have an Incydr product plan (https://support.code42.com/Terms_and_conditions/Code42_customer_support_resources/Code42_product_plans), see the Code42 Developer Portal (https://developer.code42.com/) for API documentation and resources. The portal provides:

- A single request URL (https://developer.code42.com/api/#section/Getting-started/Request-URLs) for Code42 API calls to each cloud instance
- API reference documentation (https://developer.code42.com/api/) as well as guides that describe how to use the APIs

Considerations

- The tasks in this article require use of the Code42 API (https://support.code42.com/Administrator/Cloud/Monitoring_and_managing/Code42_API_resources/Introduction_to_the_Code42_API).
  - If you are not familiar with using Code42 APIs, review Code42 API syntax and usage (https://support.code42.com/Administrator/Cloud/Monitoring_and_managing/Code42_API_resources/Code42_API_syntax_and_usage).
  - For assistance with using the Code42 API, contact your Customer Success Manager (CSM) to engage the Code42 Professional Services team. Or, post your question to the Code42 community (https://success.code42.com) to get advice from other Code42 security practitioners.
- To perform tasks in this article, you must:
Have the Customer Cloud Admin role.

Obtain an authentication token and a tenant ID.

Create a detection list profile for a user for each user you want to manage in a detection list.

Manage users

Use the api/v2/user/ resource to manage users in the detection lists. For the commands available in the /user/ resource, see the API summary section below. The following sections demonstrate how to perform some basic tasks with this API resource.

Create a detection list profile for a user

Before you can manage a Code42 user with the detection management list APIs, you must create a detection list profile for the user. This profile is for an existing Code42 user and contains the details needed to manage that user on the Departing Employees and High Risk Employees lists. It includes information about the user specifically for use in detection lists, such as notes, risk attributes, and cloud user names. When you add the user to any detection list, the profile accompanies them.

When you create a detection list profile for a user, the information is associated with the user's UID. You must submit the user's UID whenever you run any subsequent APIs to manage the user in a detection list.

Keep in mind that a detection list profile is created automatically when you add Code42 users to detection lists using the Code42 console. You only have to create a detection list profile for a user if one has not been created yet.

Check if a detection list profile already exists

Before attempting to create a detection list profile for a user, check to see if a profile already exists by running the api/v2/user/getbyusername API or api/v2/user/getbyid API. If a profile already exists, attempting to create a profile for the user results in an error.

To create a detection list profile, use the api/v2/user/create API command as shown in the following example.

- Replace <RequestURL> with the request URL of your Code42 cloud instance, for example, https://ecm-default.prod.ffs.us2.code42.com/svc/api/v2/user/
- Replace <AuthToken> with the authentication token.
- Replace <SampleTenant> with the tenant ID you obtained in the Get a tenant ID section.
- Replace <Code42Username> with the Code42 username. The username is assigned when the user is added to Code42.
- Replace <UsernameInCloudService> with the username of the user in a cloud service (such as Google Drive) if the username is different than the Code42 username.
curl -X POST <requestURL>/create \
-H 'content-type: application/json' \
-H "authorization: Bearer <AuthToken>" \
-d '{"tenantId": "<SampleTenant>", "userName": "<Code42Username>", "notes": "This is an example user note.", "riskFactors": ["FLIGHT_RISK", "HIGH_IMPACT_EMPLOYEE"], "cloudUsernames": ["<UsernameInCloudService>"]}'

An excerpt of an example successful response:

{"type$":"USER_V2","tenantId":"1233456","userId":"123456789424242","userName":"john.doe@example.com","displayName":"John Doe","notes":"This is an example user note.","cloudUsernames": ["john.doe@gmail.com","john.doe@example.com"],"riskFactors": ["FLIGHT_RISK","HIGH_IMPACT_EMPLOYEE"]}

Get the detection list profile for a user

If you need to get a user's detection list profile to find information about the user, use the api/v2/user/getbyusername API or the api/v2/user/getbyid API.

For example, if you don't know a user's UID, you can find it by running the api/v2/user/getbyusername API command as shown in the following example.

- Replace <RequestURL> with the request URL of your Code42 cloud instance, for example, https://ecm-default.prod.ffs.us2.code42.com/svc/api/v2/user/
- Replace <AuthToken> with the authentication token (https://support.code42.com/Administrator/Cloud/Monitoring_and_managing/Code42_API_resources/Code42_API_authentication_methods).
- Replace <SampleTenant> with the tenant ID you obtained in the Get a tenant ID section.
- Replace <Code42Username> with the Code42 username of the user. The username is assigned when the user is added to Code42 (https://support.code42.com/Administrator/Cloud/Configuring/Add_users_from_the_Code42_console#Add_users_manually).

curl -X POST <requestURL>/getbyusername \
-H 'content-type: application/json' \
-H "authorization: Bearer <AuthToken>" \
-d '{"tenantId": "<SampleTenant>", "username": "<Code42Username>"}'}

A successful response returns the user ID and other information:
Some available actions

Following are some of the actions you can perform using the Detection List Management APIs (https://developer.code42.com/api/#tag/Detection-Lists). For a complete list of actions you can perform with the APIs, see the API summary section below.

Add a user to a detection list

You can add a user to the Departing Employees list using the api/v2/departingemployee/add API, or add a user to the High Risk Employees list using the api/v2/highriskemployee/add API.

Bulk add users to a detection list
To leverage these APIs to add multiple users at once, see Introduction to the Code42 command-line interface (https://support.code42.com/Administrator/Cloud/Monitoring_and_managing/Introduction_to_the_Code42_command-line_interface).

Add a departing employee

The following example demonstrates how to add a user to the Departing Employees list using the api/v2/departingemployee/add API.

In the following example:

- Replace <RequestURL> with the request URL of your Code42 cloud instance, for example, https://ecm-default.prod.ffs.us2.code42.com/svc/api/v2/departingemployee
- Replace <AuthToken> with the authentication token (https://support.code42.com/Administrator/Cloud/Monitoring_and_managing/Code42_API_resources/Code42_API_authentication_methods).
- Replace <SampleTenant> with the tenant ID you obtained in the Get a tenant ID section.
- Replace <ID> with the user's UID.

```bash
curl -X POST <RequestURL>/add \
-H 'content-type: application/json' \
-H "authorization: Bearer <AuthToken>" \
-d '{ "tenantId": "<SampleTenant>", "userId": "<ID>", "departureDate": "2020-04-07" }'
```

An excerpt of an example successful response:

https://support.code42.com/Administrator/Cloud/Monitoring_and_managing/Code42_API_resources/Detection_list_management...
Add a high risk employee

The following example demonstrates how to add a user to the High Risk Employees list using the api/v2/highriskemployee/add API.

In the following example:

- Replace <RequestURL> with the request URL of your Code42 cloud instance, for example, https://ecm-default.prod.ffs.us2.code42.com/svc/api/v2/highriskemployee
- Replace <AuthToken> with the authentication token (https://support.code42.com/Administrator/Cloud/Monitoring_and_managing/Code42_API_resources/Code42_API_authentication_methods).
- Replace <SampleTenant> with the tenant ID you obtained in the Get a tenant ID section.
- Replace <ID> with the user's UID.

Copy to Clipboard

```
curl -X POST <RequestURL>/add \
-H 'content-type: application/json' \
-H "authorization: Bearer <AuthToken>" \
-d '{ "tenantId": "<SampleTenant>", "userId": "<ID>" }'
```

An excerpt of an example successful response:
```
{"type$":"HIGH_RISK_EMPLOYEE_V2","tenantId":"123456","userId":"123456789424242","userName":"john.doe@example.com","displayName":"John Doe","notes":"This is an example user note.","createdAt":"2020-03-31T19:35:49.4400509Z","status":"OPEN","cloudUsernames":[]}"}
```

Obtain a listing of all users in a detection list

You can obtain a list of all users in the Departing Employees list using the api/v2/departingemployee/search API, or obtain a list of all users in the High Risk Employees list using the api/v2/highriskemployee/search API.

Obtain a list of departing employees

Obtain a list of departing employees in Code42 by running the api/v2/departingemployee/search API.
In the following example:

- Replace `<RequestURL>` with the request URL of your Code42 cloud instance, for example, [https://ecm-default.prod.ffs.us2.code42.com/svc/api/v2/departingemployee](https://ecm-default.prod.ffs.us2.code42.com/svc/api/v2/departingemployee).
- Replace `<AuthToken>` with the authentication token ([https://support.code42.com/Administrator/Cloud/Monitoring_and_managing/Code42_API_resources/Code42_API_authentication_methods](https://support.code42.com/Administrator/Cloud/Monitoring_and_managing/Code42_API_resources/Code42_API_authentication_methods)).
- Replace `<SampleTenant>` with the tenant ID you obtained in the Get a tenant ID section.

```bash
curl -X POST <RequestURL>/search  \
-H 'content-type: application/json' \
-H "authorization: Bearer <AuthToken>" \
-d '{ "tenantId": "<SampleTenant>", "filterType": "OPEN", "pgSize": "20", "pgNum": "1", "srtKey": "DISPLAY_NAME", "srtDirection": "ASC" }'
```

An excerpt of an example successful response:

```
{"type$":"DEPARTING_EMPLOYEE_SEARCH_RESPONSE_V2","items":[{"type$":"DEPARTING_EMPLOYEE_V2","tenantId":"123456","userId":"123456789424242","userName":"john.doe@example.com","displayName":"John Doe","notes":"This is an example user note.","createdAt":"2020-03-31T19:22:18.5651920Z","status":"OPEN","cloudUsernames":["john.doe@gmail.com","john.doe@example.com"],"departureDate":"2020-04-07"},"totalCount":1,"rollups":[{"type$":"DEPARTING_EMPLOYEE_FILTER_ROLLUP_V2","filterType":"OPEN","totalCount":1},{"type$":"DEPARTING_EMPLOYEE_FILTER_ROLLUP_V2","filterType":"LEAVING_TODAY","totalCount":0},{"type$":"DEPARTING_EMPLOYEE_FILTER_ROLLUP_V2","filterType":"EXFILTRATION_24_HOURS","totalCount":0},{"type$":"DEPARTING_EMPLOYEE_FILTER_ROLLUP_V2","filterType":"EXFILTRATION_30_DAYS","totalCount":0}],"filterType":"OPEN","pgSize":20,"pgNum":1,"srtKey":"DISPLAY_NAME","srtDirection":"ASC"}
```

**Obtain a list of high risk employees**

Obtain a list of high risk employees in Code42 by running the `api/v2/highriskemployee/search` API.

In the following example:

- Replace `<RequestURL>` with the request URL of your Code42 cloud instance, for example, [https://ecm-default.prod.ffs.us2.code42.com/svc/api/v2/highriskemployee](https://ecm-default.prod.ffs.us2.code42.com/svc/api/v2/highriskemployee).
- Replace `<AuthToken>` with the authentication token ([https://support.code42.com/Administrator/Cloud/Monitoring_and_managing/Code42_API_resources/Code42_API_authentication_methods](https://support.code42.com/Administrator/Cloud/Monitoring_and_managing/Code42_API_resources/Code42_API_authentication_methods)).
- Replace `<SampleTenant>` with the tenant ID you obtained in the Get a tenant ID section.

```bash
curl -X POST <RequestURL>/search  \
-H 'content-type: application/json' \
-H "authorization: Bearer <AuthToken>" \
-d '{ "tenantId": "<SampleTenant>", "filterType": "HIGH", "pgSize": "20", "pgNum": "1", "srtKey": "RISK", "srtDirection": "ASC" }'
```
curl -X POST <RequestURL>/search \
-H 'content-type: application/json' \
-H "authorization: Bearer <AuthToken>" \
-d '{ "tenantId": "<SampleTenant>", "filterType": "OPEN", "pgSize": "20", "pgNum": "1", "srtKey": "DISPLAY_NAME", "srtDirection": "ASC" }'

An excerpt of an example successful response:

```
{"type$":"HIGH_RISK_SEARCH_RESPONSE_V2","items": [{"type$":"HIGH_RISK_EMPLOYEE_V2","tenantId":"123456","userId":"123456789424242","userName":"john.doe@example.com","displayName":"John Doe","notes":"This is an example note.","createdAt":"2020-03-31T19:35:49.440500Z","status":"OPEN","cloudUsernames":["john.doe@gmail.com","john.doe@example.com"],"riskFactors": ["FLIGHT_RISK","HIGH_IMPACT_EMPLOYEE"]}],

{"type$":"HIGH_RISK_EMPLOYEE_V2","tenantId":"123456","userId":"987654321424242","userName":"jane.smith@example.com","displayName":"Jane Smith","notes":"This is an example note.","createdAt":"2020-03-31T19:45:30.3092900Z","status":"OPEN","cloudUsernames": ["jane.smith@gmail.com", "jane.smith@example.com"], "managerUid": "Jack.Shep", "managerUsername": "Jack.Shep@example.com", "managerDisplayName": "Jack Shep", "title": "People Person", "division": "Acme", "department": "Human Resources", "employmentType": "Full Time", "city": "The Island", "state": "MN", "country": "US", "riskFactors": ["FLIGHT_RISK", "HIGH_IMPACT_EMPLOYEE"]},

totalCount: 2,"rollups": [{"type$": "HIGH_RISK_FILTER_ROLLUP_V2","filterType": "OPEN","totalCount": 2},{"type$": "HIGH_RISK_FILTER_ROLLUP_V2","filterType": "EXFILTRATION_24_HOURS","totalCount": 0},{"type$": "HIGH_RISK_FILTER_ROLLUP_V2","filterType": "EXFILTRATION_30_DAYS","totalCount": 0}],

totalCount: 2,"rollups": [{"type$": "HIGH_RISK_FILTER_ROLLUP_V2","filterType": "OPEN","pgSize": 20,"pgNum": 1,"srtKey": "DISPLAY_NAME","srtDirection": "ASC" ]
```

View details of a user in a detection list

You can view details of a user in the Departing Employees list using the `api/v2/departingemployee/get` API, or view details of a user in the High Risk Employees list using the `api/v2/highriskemployee/get` API.

The commands to view the details of a departing or high risk employee are similar. The following example shows how to view the details of a high risk employee using the `api/v2/highriskemployee/get` API.

In the following example:

- Replace `<RequestURL>` with the request URL of your Code42 cloud instance, for example, https://ecm-default.prod.ffs.us2.code42.com/svc/api/v2/highriskemployee

- Replace `<AuthToken>` with the authentication token (https://support.code42.com/Administrator/Cloud/Monitoring_and_managing/Code42_API_resources/Code42_API_authentication_methods).

- Replace `<SampleTenant>` with the tenant ID you obtained in the Get a tenant ID section.

- Replace `<ID>` with the user's UID.
curl -X POST <RequestURL>/get \
-H 'content-type: application/json' \
-H "authorization: Bearer <AuthToken>" \
-d '{ "tenantId": "<SampleTenant>", "userId": "<ID>" }'

An excerpt of an example successful response:

```json
{"type$":"HIGH_RISK_EMPLOYEE_V2","tenantId":"123456","userId":"123456789424242","userName":"john.doe@example.com","displayName":"John Doe","notes":"This is an example note.","createdAt":"2020-03-31T19:35:49.4400500Z","status":"OPEN","cloudUsernames":[]}]
```

**Enable or disable alerts for all users in a detection list**

You can enable or disable alerts for all users in a detection list using the api/v2/departingemployee/setalertstate API or the api/v2/highriskemployee/setalertstate API.

The commands to enable or disable alerts for all departing or high risk employees are similar. The following example shows how to enable alerts for all high risk employees using the api/v2/highriskemployee/setalertstate API.

In the following example:

- Replace <RequestURL> with the request URL of your Code42 cloud instance, for example, https://ecm-default.prod.ffs.us2.code42.com/svc/api/v2/highriskemployee
- Replace <AuthToken> with the authentication token (https://support.code42.com/Administrator/Cloud/Monitoring_and_managing/Code42_API_resources/Code42_API_authentication_methods).
- Replace <SampleTenant> with the tenant ID you obtained in the Get a tenant ID section.

```bash
curl -X POST <RequestURL>/setalertstate \
-H 'content-type: application/json' \
-H "authorization: Bearer <AuthToken>" \
-d '{ "tenantId": "<SampleTenant>", "alertsEnabled": true }'
```

To disable alerts, run the command with the alertsEnabled value set to false.

To verify that the alerts setting is changed as desired, select Alert Settings in the Departing Employees list or High Risk Employees list (https://support.code42.com/Administrator/Cloud/Monitoring_and_managing/How_to_create_a_security_alert#Enable_or_disable_default_rules).

https://support.code42.com/Administrator/Cloud/Monitoring_and_managing/Code42_API_resources/Detection_list_management...
Remove a user from a detection list

You can remove a user from the Departing Employees list using the `api/v2/departingemployee/remove` API, or remove a user from the High Risk Employees list using the `api/v2/highriskemployee/remove` API.

Bulk remove users from a detection list

To leverage these APIs to remove multiple users at once, see [Introduction to the Code42 command-line interface](https://support.code42.com/Administrator/Cloud/Monitoring_and_managing/Introduction_to_the_Code42_command-line_interface).

The commands to remove a user from the Departing Employees or High Risk Employees lists are similar. The following example shows how to remove a user from the High Risk Employees list using the `api/v2/highriskemployee/remove` API.

In the following example:

- Replace `<RequestURL>` with the request URL of your Code42 cloud instance, for example,
  ```plaintext
  https://ecm-default.prod.ffs.us2.code42.com/svc/api/v2/highriskemployee
  ```
- Replace `<AuthToken>` with the authentication token ([Code42_API_resources/Code42_API_authentication_methods](https://support.code42.com/Administrator/Cloud/Monitoring_and_managing/Code42_API_resources/Code42_API_authentication_methods)).
- Replace `<SampleTenant>` with the tenant ID you obtained in the [Get a tenant ID](https://support.code42.com/Administrator/Cloud/Monitoring_and_managing/Code42_API_resources/Get_a_tenant_ID) section.
- Replace `<ID>` with the user's UID.

```plaintext
curl -X POST <RequestURL>/remove \
-H 'content-type: application/json' \
-H "authorization: Bearer <AuthToken>" \
-d '{ "tenantId": "<SampleTenant>", "userId": "<ID>" }'
```

To verify that the user is removed, generate a listing of all users in the detection list as shown above.

Detection list management API structure and syntax

**Summary**

- **Request URL**
  - United States:
    - If you sign in to the Code42 console at https://console.us.code42.com/console (US1), use:
      ```plaintext
      https://ecm-east.us.code42.com/svc/api/v2/<resource>
      ```
    - If you sign in to the Code42 console at https://console.us2.crashplan.com/console (US2), use:
      ```plaintext
      https://ecm-default.prod.ffs.us2.code42.com/svc/api/v2/<resource>
      ```
• If you sign in to the Code42 console for the Code42 federal environment at https://console.gov.code42.com/console (US3), use:

https://ecm-default.gov.code42.com/svc/api/v2/<resource>

• Ireland:

• If you sign in to the Code42 console at https://console.ie.code42.com/console (EU1), use:

https://ecm-default.ie.code42.com/svc/api/v2/<resource>

Code42 console URL for US2

Code42 console URL console.us2.crashplan.com was formerly www.crashplan.com/console. For more information, see Changes to server URLs (https://support.code42.com/Terms_and_conditions/Product_lifecycle_policy/Changes_to_server_URLs).

• Resources

  • User API:

    /user/

    • addcloudusernames: Add cloud user names to a user
    • addriskfactors: Add a list of risk factors to a user
    • create: Create a user profile
    • getbyid: Get a user profile by user ID
    • getbyusername: Get a user profile by Code42 username
    • refresh: Refresh SCIM attributes for a user
    • removecloudusernames: Remove cloud user names from a user
    • removeriskfactors: Remove risk factors from a user
    • updatenotes: Update notes for a user

  • Departing employee:

    /departingemployee/

    • add: Add a departing employee
    • get: View the details of a specific departing employee
    • remove: Remove a departing employee
    • search: Obtain a list of departing employees
    • setalertstate: Enable alerts for all departing employees
    • update: Update a departing employee's details

  • High risk employee:

    /highriskemployee/

    • add: Add a high risk employee
    • get: View the details of a specified high risk employee
• **remove**: Remove a high risk employee
• **search**: Obtain a list of high risk employees
• **setalertstate**: Enable alerts for all high risk employees

- **Authentication method**: Include an authentication token ([https://support.code42.com/Administrator/Cloud/Monitoring_and_managing/Code42_API_resources/Code42_API_authentication_methods](https://support.code42.com/Administrator/Cloud/Monitoring_and_managing/Code42_API_resources/Code42_API_authentication_methods)) in the request header
- **API documentation**: For additional API documentation, see [https://developer.code42.com/api/#tag/Detection-Lists](https://developer.code42.com/api/#tag/Detection-Lists).

### Get a tenant ID

The APIs require that you provide the unique ID of your organization (or tenant) in the Code42 cloud. To obtain the tenant ID, use your Code42 administrator credentials to submit a **GET** request to:

- **United States**:
  - If you sign in to the Code42 console at https://console.us.code42.com/console (US1), use:
    ```
    https://console.us.code42.com/c42api/v3/customer/my
    ```
  - If you sign in to the Code42 console at https://console.us2.crashplan.com/console (US2), use:
    ```
    https://console.us2.crashplan.com/c42api/v3/customer/my
    ```
  - If you sign in to the Code42 console for the Code42 federal environment at https://console.gov.code42.com/console (US3), use:
    ```
    https://console.gov.code42.com/c42api/v3/customer/my
    ```
- **Ireland**: If you sign in to the Code42 console at https://console.ie.code42.com/console (EU1), use:
  ```
  https://console.ie.code42.com/c42api/v3/customer/my
  ```

In the following example, replace `<AuthToken>` with the authentication token ([https://support.code42.com/Administrator/Cloud/Monitoring_and_managing/Code42_API_resources/Code42_API_authentication_methods](https://support.code42.com/Administrator/Cloud/Monitoring_and_managing/Code42_API_resources/Code42_API_authentication_methods)) you obtained and replace `console.us.code42.com` with the URL of your Code42 cloud instance:

```
```

A successful response returns the `tenantUid`:

```json
{"data":{"name":"My Org","registrationKey":"4s42ukut7pwmpwr4c","deploymentMode":"PUBLIC","maintenanceMode":false,"tenantUid":"42b42dfe-4242-4242-428a-8a1dfd352f2f","masterServicesAgreement":{"accepted":true,"acceptanceRequired":false}},"error":null,"warnings":null}
```
Related topics

- Add departing employees (https://support.code42.com/Administrator/Cloud/Monitoring_and_managing/Add_departing_employees)
- Add high-risk employees (https://support.code42.com/Administrator/Cloud/Monitoring_and_managing/Add_high-risk_employees)
- Introduction to the Code42 command-line interface (https://support.code42.com/Administrator/Cloud/Monitoring_and_managing/Introduction_to_the_Code42_command-line_interface)
- Code42 API syntax and usage (https://support.code42.com/Administrator/Cloud/Monitoring_and_managing/Code42_API_resources/Code42_API_syntax_and_usage)
- Code42 API authentication methods (https://support.code42.com/Administrator/Cloud/Monitoring_and_managing/Code42_API_resources/Code42_API_authentication_methods)