

[Read about the latest CXone Expert release](#)

SUPPORT



- HOME
- GETTING STARTED
- RELEASE NOTES
- FAQs
- APIs
- SYSTEM STATUS

IX-Edit



INDEX

Home > Archive > Archived by DOC-12685 - Manage alerts with the Code42 API

Live

This page is published. There is no draft for this page.



[Page settings](#)

Archived by DOC-12685 - Manage alerts with the Code42 API

Last updated: Feb 24, 2022, 1:28 PM by Amy Dohlman Page restriction: Private

Table of contents

Overview

Considerations

Manage alert notifications

- Search for alert notifications by alert filter criteria

Who is this article for?

- Incydr Professional, Enterprise, Horizon, and Gov F2
- Incydr Basic, Advanced, and Gov F1

Find your product plan in the Code42 console on the [Account menu](#).

Search for multiple alert notifications by alert IDs

Search for a single notification by alert ID

Add a note to an alert notification

Dismiss alert notifications

Reopen dismissed alert notifications

Manage alert rule user lists

Locate alert rule IDs

View an alert rule's user list

Add users to an alert rule

Remove specific users from an alert rule

Remove a user's aliases from an alert rule

Remove all users from an alert rule

Alerts management API structure and syntax

Summary

Filter syntax for the query-alerts API command

Filter syntax for the rules/query-rule-metadata API command

Get your organization's tenant ID

Identify userUIDs

Related topics

Overview

You review alert notifications and manage alert rules using the Alerts menu of the Code42 console. To automate the process of viewing alert notifications, adding notes, or opening or dismissing alert notifications, you can write scripts that use the Alerts management APIs. This article introduces those APIs and shows examples of their use.

Considerations

- The tasks in this article require use of the [Code42 API](#).
 - If you are not familiar with using Code42 APIs, review [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.
- To perform tasks in this article, you must obtain an [authentication token](#) and your organization's [tenant ID](#).
- You can also use the Code42 command-line interface (CLI) to work with alert notifications and rules. For more information, see [Introduction to the Code42 command-line interface](#).

Manage alert notifications

To work with alert notifications, use the API query commands to search for alert notifications. Once you [identify specific alert IDs](#), you can then add a note, dismiss, or reopen those alert notifications.

Search for alert notifications by alert filter criteria

To search for alert notifications using filter criteria and identify alert IDs, use the `api/v1/query-alerts` API command. In the following example:

- Replace <RequestURL> with the [request URL](#) of your Code42 cloud instance, for example, `https://alert-service-default.prod.ffs.us2.code42.com/svc/api/v1/`
- Replace <AuthToken> with the [authentication token](#).

- Replace `<SampleTenant>` with the tenant ID you obtained in the [Get your organization's tenant ID](#) section.
- Replace `<FilterType>` with the filter, `<OperatorValue>` with the operator option, and `<Criteria>` with the search term to use in the search. See [Filter syntax for the query-alerts API command](#) below for details.

 [Copy to clipboard](#)

```
curl -X POST \
"<RequestURL>/query-alerts" \
-H "accept: text/plain" \
-H "Authorization: Bearer <AuthToken>" \
-H "Content-Type: application/json" \
-d '{ "tenantId": "<SampleTenant>", "groups": [ {
"filters": [ { "term": "<FilterType>",
"operator": "<OperatorValue>", "value": "
<Criteria>" } ], "filterClause": "AND" } ],
"groupClause": "OR", "pageSize": "20", "pageNum":
"0", "srtKey": "CreatedAt", "srtDirection":
"DESC" }'
```

A successful response returns basic information about the alert notifications that match your search criteria, including the alert IDs of those notifications (look for the `"id": "value"` entry):

```
{ "type$": "ALERT_SUMMARY", "tenantId": "123456", "type": "FED_END
employee endpoint exfiltration system rule", "description": "System
rule for departing employee endpoint
exfiltration.", "actor": "burt.morales@example.com", "target": "N/A", "seve
Employee", "id": "987654321424242", "createdAt": "2020-04-
03T15:21:44.6139300Z", "state": "OPEN" }, {"totalCount": 1, "problems":
[] }
```

Search for multiple alert notifications by alert IDs

After you've located the alert IDs for specific alerts, use the `/api/v1/query-details` API command to search those IDs and

view more details about those alert notifications. In the following example:

- Replace <RequestURL> with the [request URL](#) of your Code42 cloud instance, for example, `https://alert-service-default.prod.ffs.us2.code42.com/svc/api/v1/`
- Replace <AuthToken> with the [authentication token](#).
- Replace <SampleAlertID1> and <SampleAlertID2> with the IDs of the alert notifications. Enclose each ID in quotation marks and separate them with commas.

[Copy to clipboard](#)

```
curl -X POST \
"<RequestURL>/query-details" \
-H "accept: text/plain" \
-H "Authorization: Bearer <AuthToken>" \
-H "Content-Type: application/json" \
-d '{ "alertIds": [ "<SampleAlertID1>", "
<SampleAlertID2>" ] }'
```

A successful response returns full details about the alert notifications, including a list of files involved in the activity.

```
{ "type$": "ALERT_DETAILS_RESPONSE", "alerts":
[ { "type$": "ALERT_DETAILS", "tenantId": "123456", "type": "FED_ENDPOINT
employee endpoint exfiltration system rule", "description": "System
rule for departing employee endpoint
exfiltration.", "actor": "burt.morales@example.com", "target": "N/A", "seve
Employee", "id": "987654321424242", "createdAt": "2020-04-
08T13:50:25.3644410Z", "state": "OPEN", "observations":
[ { "type$": "OBSERVATION", "id": "112233445566", "observedAt": "2020-
04-
08T13:40:00.0000000Z", "type": "FedEndpointExfiltration", "data": "
{ "type$": "OBSERVED_ENDPOINT_ACTIVITY", "id": "6655443322
[ "Endpoint", "exposureTypes":
[ "ApplicationRead", "CloudStorage", "firstActivityAt": "2020-04-
08T13:40:00.0000000Z", "lastActivityAt": "2020-04-
08T13:45:00.0000000Z", "fileCount": 2, "totalFileSize": 311096, "fileC
[ { "type$": "OBSERVED_FILE_CATEGORY", "category": "Image", }
```

```
{{"type$":{"OBSERVED_FILE"},"eventId":{"998877665544"},"path":{"type$":{"OBSERVED_FILE"},"eventId":{"334455667788"},"path":{"Dropbox"},"sendingIpAddresses":{"192.0.2.0"}}}}
```

Search for a single notification by alert ID

Use the `/api/v1/query-details-aggregate` API command to search for a single alert notification using its alert ID. In the following example:

- Replace `<RequestURL>` with the [request URL](#) of your Code42 cloud instance, for example, `https://alert-service-default.prod.ffs.us2.code42.com/svc/api/v1/`
- Replace `<AuthToken>` with the [authentication token](#).
- Replace `<SampleAlertID>` with the alert ID.

[Copy to clipboard](#)

```
curl -X POST \
  "<RequestURL>/query-details-aggregate" \
  -H "accept: text/plain" \
  -H "Authorization: Bearer <AuthToken>" \
  -H "Content-Type: application/json" \
  -d '{"alertId": "<SampleAlertID>"}'
```

A successful response returns full details about the alert notification with all file activity aggregated into a single Observation value.

```
{"type$":{"ALERT_DETAILS_IN_AGGREGATE_RESPONSE"},"alert":
{"type$":{"ALERT_DETAILS_AGGREGATE"},"tenantId":{"123456"},"type
employee endpoint exfiltration system rule","description":{"System
rule for departing employee endpoint
exfiltration.},"actor":{"burt.morales@c42se.com"},"target":{"N/A"},"severit
Employee","id":{"9876543214242"},"createdAt":{"2020-04-
08T13:50:25.3644410Z"},"state":{"OPEN"},"observation":
{"type$":{"OBSERVATION_AGGREGATE"},"observedAt":{"2020-04-
08T13:40:00.000000Z"},"type":{"FedEndpointExfiltration"},"data":{"
```

```
{
  "type$": "OBSERVED_ENDPOINT_ACTIVITY",
  "id": "1122334455",
  "Endpoint": {
    "exposureTypes": [
      "ApplicationRead",
      "CloudStorage"
    ],
    "firstActivityAt": "2020-04-08T13:40:00.000000Z",
    "lastActivityAt": "2020-04-08T13:45:00.000000Z",
    "fileCount": 2,
    "totalFileSize": 311096,
    "fileCategories": [
      {
        "type$": "OBSERVED_FILE_CATEGORY",
        "category": "Image",
        "files": [
          {
            "type$": "OBSERVED_FILE",
            "eventId": "998877665544",
            "path": "C:\\Users\\User\\AppData\\Local\\Microsoft\\Windows\\Temporary Internet Files\\Content.IE5\\...\\image.png"
          },
          {
            "type$": "OBSERVED_FILE",
            "eventId": "334455667788",
            "path": "C:\\Users\\User\\AppData\\Local\\Microsoft\\Windows\\Temporary Internet Files\\Content.IE5\\...\\image.png"
          }
        ]
      }
    ]
  },
  "sendingIpAddresses": [
    "192.0.2.0"
  ],
  "isRemoteActivity": false
}
```

Add a note to an alert notification

To add a note to an alert notification, first locate its alert ID using one of the queries above. Then use the `/api/v1/add-note` command to add a note to that alert. Be aware that any note you add overwrites any existing note attached to the alert.

In the following example:

- Replace `<RequestURL>` with the [request URL](#) of your Code42 cloud instance, for example, `https://alert-service-default.prod.ffs.us2.code42.com/svc/api/v1/`
- Replace `<AuthToken>` with the [authentication token](#).
- Replace `<SampleTenant>` with the tenant ID you obtained in the [Get your organization's tenant ID](#) section.
- Replace `<SampleAlertID>` with the alert ID.

[Copy to clipboard](#)

```
curl -X POST \
  "<RequestURL>/add-note" \
  -H "accept: application/json" \
  -H "Authorization: Bearer <AuthToken>" \
  -H "Content-Type: application/json" \
  -d '{ "tenantId": "<SampleTenant>", "alertId": "<SampleAlertID>", "note": "This is an example note." }'
```

Dismiss alert notifications

You can dismiss multiple alert notifications at once using the API. To dismiss alert notifications, first locate the alert IDs using one of the queries above. Then use the `/api/v1/resolve-alert` command to dismiss those alerts. In the following example:

- Replace `<RequestURL>` with the [request URL](#) of your Code42 cloud instance, for example, `https://alert-service-default.prod.ffs.us2.code42.com/svc/api/v1/`
- Replace `<AuthToken>` with the [authentication token](#).
- Replace `<SampleTenant>` with the tenant ID you obtained in the [Get your organization's tenant ID](#) section.
- Replace `<SampleAlertID1>` and `<SampleAlertID2>` with the IDs of the alert notifications. Enclose each ID in quotation marks and separate them with commas.
- Be aware that any note you enter overwrites any existing note attached to the alert. If you want to dismiss the alert without adding a note (or want to preserve existing notes), delete the "note" term and sample text from the command.

[Copy to clipboard](#)

```
curl -X POST \  
"<RequestURL>/resolve-alert" \  
-H "accept: application/json" \  
-H "Authorization: Bearer <AuthToken>" \  
-H "Content-Type: application/json" \  
-d '{ "tenantId": "<SampleTenant>", "alertIds": [  
"<SampleAlertID1>", <SampleAlertID2>" ], "note":  
"This is an example note."}'
```

Reopen dismissed alert notifications

You can reopen multiple dismissed alert notifications at once using the API. To reopen alert notifications, first locate the alert IDs using one of the queries above. Then use the `/api/v1/reopen-alert` command to reopen those alerts. In the following example:

- Replace `<RequestURL>` with the [request URL](#) of your Code42 cloud instance, for example,

```
https://alert-service-default.prod.ffa.us2.code42.com/svc/api/v1/
```

- Replace <AuthToken> with the [authentication token](#).
- Replace <SampleTenant> with the tenant ID you obtained in the [Get your organization's tenant ID](#) section.
- Replace <SampleAlertID1> and <SampleAlertID2> with the IDs of the alert notifications. Enclose each ID in quotation marks and separate them with commas.
- Be aware that any note you enter overwrites any existing note attached to the alert. If you want to reopen the alert without adding a note (or want to preserve existing notes), delete the "note" term and sample text from the command.

 [Copy to clipboard](#)

```
curl -X POST \  
"<RequestURL>/reopen-alert" \  
-H "accept: application/json" \  
-H "Authorization: Bearer <AuthToken>" \  
-H "Content-Type: application/json" \  
-d '{ "tenantId": "<SampleTenant>", "alertIds": [ \  
"<SampleAlertID1>", <SampleAlertID2>" ], "note": \  
"This is an example note."}'
```

Manage alert rule user lists

If a rule either applies only to specific users or applies to all users except specific users, you can manage the users in those inclusion or exclusion lists using the API. As with alert notifications, you'll need to identify the rule ID associated with the rule before you can manage the users to which it applies.

Be careful with request URLs

The API commands in this section use different request URLs, so use caution when crafting the calls.

Locate alert rule IDs

Before you can manage the users associated with an alert rule, you

need to view details about alert rules and identify the rule IDs for which you want to manage users. Use the `/api/v1/Rules/query-rule-metadata` API command to locate alert rule IDs.

Rule IDs are also included in alert notification searches

The API commands for alert notification searches described above also include the ID of the rule that generated the alert. Look for the `"ruleID": "<value>"` entry in the details returned by the query.

In the following example:

- Replace `<RequestURL>` with the [request URL](#) of your Code42 cloud instance, for example, `https://alert-service-default.prod.ffs.us2.code42.com/svc/api/v1/`
- Replace `<AuthToken>` with the [authentication token](#).
- Replace `<SampleTenant>` with the tenant ID you obtained in the [Get your organization's tenant ID](#) section.
- Replace `<FilterType>` with the filter, `<OperatorValue>` with the operator option, and `<Criteria>` with the search term to use in the search. See [Filter syntax for the rules/query-rule-metadata API command](#) below for details.

[Copy to clipboard](#)

```
curl -X POST \
  "<Request URL>/Rules/query-rule-metadata" \
  -H "accept: text/plain" \
  -H "Authorization: Bearer <AuthToken>" \
  -H "Content-Type: application/json" \
  -d '{ "tenantId": "<SampleTenant>", "groups": [ {
    "filters": [ { "term": "<FilterTerm>",
      "operator": "<OperatorValue>", "value": "
    <Criteria>" } ], "filterClause": "AND" } ],
    "groupClause": "OR", "pgSize": "20", "pgNum":
    "0", "srtKey": "CreatedAt", "srtDirection":
    "DESC" } '
```

A successful response returns basic information about the alert notifications that match your search criteria, including the rule IDs of those notifications (look for the `"observerRuleId": "value"` entry):

```
{
  "type$": "RULE_METADATA_SEARCH_RESPONSE",
  "ruleMetadata": [
    {
      "type$": "RULE_METADATA",
      "modifiedBy": "Code42",
      "modifiedAt": "2016-04T21:07:03.5417950Z",
      "name": "Exposure on an endpoint",
      "description": "This default rule alerts you when departing employees move data from an endpoint.",
      "severity": "HIGH",
      "isSystem": true,
      "isEnabled": false,
      "ruleScope": "Employee",
      "tenantId": "123456",
      "observerRuleId": "123456789424201-10T12:16:40.7765970Z"
    }
  ],
  "totalCount": 8,
  "problems": []
}
```

View an alert rule's user list

Use the `/api/v1/Rules/query-users` API command to view a list of users that are either included in or excluded from a specific alert rule. The output from this command groups the user email addresses and cloud aliases in the rule's inclusion or exclusion list by the user ID associated with those details (which is generally the `userID` value in Code42). You can then use this user ID to remove specific email addresses and cloud aliases from a rule's inclusion or exclusion list as needed.

In the following example:

- Replace `<RequestURL>` with the [request URL](#) of your Code42 cloud instance, for example, `https://fed-observer-default.prod.ffs.us2.code42.com/svc/api/v1/`
- Replace `<AuthToken>` with the [authentication token](#).
- Replace `<SampleTenant>` with the tenant ID you obtained in the [Get your organization's tenant ID](#) section.
- Replace `<SampleRuleID>` with the ID of the alert rule for which you want to view users.

```
curl -X POST \
```

[Copy to clipboard](#)

```
"<RequestURL>/Rules/query-users" \
-H "accept: text/plain" \
-H "Authorization: Bearer <AuthToken>" \
-H "Content-Type: application/json" \
-d '{ "tenantId": "<SampleTenant>", "ruleId": "
<SampleRuleID>" }'
```

A successful response lists the email addresses and cloud aliases of the users in the alert rule's inclusion or exclusion list, grouped by the user ID value (identified by the "userIdFromAuthority" label) associated with that information. The "usersToAlertOn" label identifies whether the rule applies only to the specified users in an inclusion list (SPECIFIED_USERS), to all users except the specified users in an exclusion list (ALL_USERS_NOT_SPECIFIED), or to all users (ALL_USERS).

```
{"type$":"USERS_IN_RULE_RESPONSE","users":
[{"type$":"USER_BAG","userIdFromAuthority":"9472103784785954
["SCassidy","SeanCassidy","sean.cassidy@example.com"]}], "usersTo
```

If a user ID was not provided when users were added to the alert rule (as is common when users are added using the Code42 command-line interface or manually with Alerts in the Code42 console), the results note that the "userIdFromAuthority" value is null. To work with an alert rule's inclusion or exclusion list if the user ID value is null, use the Alerts screens in the Code42 console to manually add and remove users. You can also use the [/api/v1/Rules/remove-all-users](#) API command to remove all email addresses and aliases from a rule, and then re-add user information to that rule using the [/api/v1/Rules/add-users](#) using the users' userIDs in Code42.

```
{"type$":"USERS_IN_RULE_RESPONSE","users":
[{"type$":"USER_BAG","userIdFromAuthority":"Null
UserIdFromAuthority. These usernames must be edited in
the web app.","userAliasList":
["burt.morales@example.com","astrid.ludwig@example.com"]}], "users
```

Add users to an alert rule

If the rule applies to specific users, or if it applies to all users except specific users, you can add users to those inclusion or exclusion lists with the `/api/v1/Rules/add-users` API command. You cannot add users to rules that monitor all users.

Manage default rule user lists with the Code42 console or Detection List Management APIs

You cannot use these alerts APIs to add or remove users from the inclusion or exclusion lists of default rules created by the Departing Employees list or High Risk Employees list. Instead, users are added to and removed from these lists directly in the [Departing Employees list](#) and [High Risk Employees list](#) or with the [Detection List Management APIs](#).

In the following example:

- Replace `<RequestURL>` with the [request URL](#) of your Code42 cloud instance, for example,
`https://fed-observer-default.prod.ffs.us2.code42.com/svc/api/v1/`
- Replace `<AuthToken>` with the [authentication token](#).
- Replace `<SampleTenant>` with the tenant ID you obtained in the [Get your organization's tenant ID](#) section.
- Replace `<SampleRuleID>` with the ID of the alert rule from which you want to remove users.
- Replace `<SampleUserID>` with a value that uniquely identifies the user you want to add. As a best practice, use the user's `userID` in Code42 for this value. See the [Identify userIDs](#) section to locate these values.
- The `userAliasList` parameter identifies the list of email addresses or cloud aliases to associate with that `<SampleUserID>`. Replace `<SampleAlias1>` and `<SampleAlias2>` with the email addresses or cloud aliases you want to add to the rule's inclusion or exclusion list for that user ID.
 - If you want to enter only one email address or cloud alias, use this construction:
`"userAliasList": ["<SampleAlias1>"]`
 - If you want to enter multiple email addresses or cloud aliases for

that user ID, enclose each ID in quotation marks and separate them with commas.

The aliases that you enter here become the values that are added to the rule's inclusion or exclusion list and used to trigger or filter alert notifications.

[Copy to clipboard](#)

```
curl -X POST \  
"<RequestURL>/Rules/add-users" \  
-H "accept: application/json" \  
-H "Authorization: Bearer <AuthToken>" \  
-H "Content-Type: application/json" \  
-d '{ "tenantId": "<SampleTenant>", "ruleId": "  
<SampleRuleId>", "userList": [ {  
  "userIdFromAuthority": "<SampleUserUID>",  
  "userAliasList": [ "<SampleAlias1>", "  
<SampleAlias2>" ] } ]}'
```

Remove specific users from an alert rule

You can also remove users' email addresses or cloud aliases from an alert rule's inclusion or exclusion list with the [/api/v1/Rules/remove-users](#) API command. This command removes all of the email addresses or cloud aliases associated with the user's ID from the specified rule. You cannot remove users from rules that monitor all users.

Manage default rule user lists with the Code42 console or Detection List Management APIs

You cannot use these alerts APIs to add or remove users from the inclusion or exclusion lists of default rules created by the Departing Employees list or High Risk Employees list. Instead, users are added to and removed from these lists directly in the [Departing Employees list](#) and [High Risk Employees list](#) or with the [Detection List Management APIs](#).

In the following example:

- Replace <RequestURL> with the [request URL](#) of your Code42 cloud instance, for example,
`https://fed-observer-default.prod.ffs.us2.code42.com/svc/api/v1/`
- Replace <AuthToken> with the [authentication token](#).
- Replace <SampleTenant> with the tenant ID you obtained in the [Get your organization's tenant ID](#) section.
- Replace <SampleRuleID> with the ID of the alert rule from which you want to remove users.
- Replace <SampleUserID> with the value that uniquely identifies the alias list of the user you want to remove (such as the [user's userID in Code42](#)).

Results depend on the user ID value

The `/api/v1/Rules/remove-users` API command uses the <SampleUserID> value to identify the user alias list to remove from the rule. This value may not always be supplied when users are added to rules, such as when users are added via the Code42 command-line interface or manually with Alerts in the Code42 console. Therefore, results from using `/api/v1/Rules/remove-users` may not be what you expect: if no <SampleUserID> value exists, the corresponding alias list cannot be identified and no users are removed.

To resolve this issue using the API, use the `/api/v1/Rules/remove-all-users` API command to remove all users from a rule's inclusion or exclusion list, then use the `/api/v1/Rules/add-users` to add user aliases that are associated with a <SampleUserID> value.

[Copy to clipboard](#)

```
curl -X POST \
  "<Request URL>/Rules/remove-users" \
  -H "accept: application/json" \
  -H "Authorization: Bearer <AuthToken>" \
  -H "Content-Type: application/json" \
  -d '{ "tenantId": "<SampleTenant>", "ruleId": "
```

```
<SampleRuleID>", "userIdList": [ "  
<SampleUserUID>" ]}'
```

Remove a user's aliases from an alert rule

Before removing user information from an alert rule's inclusion or exclusion list, use the `/api/v1/Rules/query-users` API command to identify what user information is contained in that list and whether it is associated with a user ID. After identifying the user ID associated with the email addresses or cloud aliases in a rule's inclusion or exclusion list, you can then use the `/api/v1/Rules/remove-user-aliases` API command to remove only that user information from the list.

Requires the user ID

If there are no user IDs associated with the user information in an alert rule's inclusion or exclusion list, you cannot remove specific email addresses or cloud aliases from that list with this API command. Instead, you can use one of these methods to work with a rule's user information:

- Use the Alerts screen in the Code42 console to manually add and remove users
- Use the `/api/v1/Rules/remove-all-users` and `/api/v1/Rules/add-users` API commands to remove all user information and then re-add the email addresses and cloud aliases (associated with a Code42 userUID value) that you want to keep

In the following example:

- Replace `<RequestURL>` with the [request URL](#) of your Code42 cloud instance, for example,
`https://fed-observer-default.prod.ffs.us2.code42.com/svc/api/v1/`
- Replace `<AuthToken>` with the [authentication token](#).
- Replace `<SampleTenant>` with the tenant ID you obtained in the [Get your organization's tenant ID](#) section.

- Replace <SampleRuleID> with the ID of the alert rule from which you want to remove users.
- Replace <SampleUserID> with the value that is associated with the email addresses or cloud aliases that you want to remove.
- The userAliasList parameter identifies the email addresses or cloud aliases associated with that <SampleUserID> that should be removed from the list. Replace <SampleAlias1> and <SampleAlias2> with the email addresses or cloud aliases you want to remove from the rule's inclusion or exclusion list for that user ID.
 - If you want to remove only one email address or cloud alias, use this construction:


```
"userAliasList": [ "<SampleAlias1>" ]
```
 - If you want to remove multiple email addresses or cloud aliases for that user ID, enclose each ID in quotation marks and separate them with commas.
 - If there are multiple email addresses or cloud aliases associated with that user ID but you want to remove only one or two, specify only the values to remove.

 [Copy to clipboard](#)

```
curl -X POST \
"<RequestURL>/Rules/remove-user-aliases" \
-H "accept: application/json" \
-H "Authorization: Bearer <AuthToken>" \
-H "Content-Type: application/json" \
-d '{ "tenantId": "<SampleTenant>", "ruleId": "
<SampleRuleID>", "userList": [ {
"userIdFromAuthority": "<SampleUserID>",
"userAliasList": [ "<SampleAlias1>", "
<SampleAlias2>" ] } ]}'
```

Remove all users from an alert rule

If you do not know the user ID associated with the list of email addresses or cloud aliases for a user, you can use the </api/v1/Rules/remove-all-users> to remove all users from an alert rule's inclusion or exclusion list. You can then use the add-users API command to rebuild those lists using known user IDs.

In the following example:

- Replace <RequestURL> with the [request URL](#) of your Code42 cloud instance, for example,
`https://fed-observer-default.prod.ffs.us2.code42.com/svc/api/v1/`
- Replace <AuthToken> with the [authentication token](#).
- Replace <SampleTenant> with the tenant ID you obtained in the [Get your organization's tenant ID](#) section.
- Replace <SampleRuleID> with the ID of the alert rule from which you want to remove all users.

[Copy to clipboard](#)

```
curl -X POST \  
"<Request URL>/Rules/remove-all-users" \  
-H "accept: application/json" \  
-H "Authorization: Bearer <AuthToken>" \  
-H "Content-Type: application/json" \  
-d '{ "tenantId": "<SampleTenant>", "ruleId": "  
<SampleRuleID>" }'
```

Alerts management API structure and syntax

Summary

- **Request URL**
 - United States alerts
 - If you sign in to the Code42 console at `https://console.us.code42.com` (US1), use:
`https://alert-service-east.us.code42.com/svc/api/v1/<resource>`
 - If you sign in to the Code42 console at `https://console.us2.code42.com` (US2), use:
`https://alert-service-default.prod.ffs.us2.code42.com/svc/api/v1/<resource>`
 - If you sign in to the Code42 console for the Code42 federal environment at `https://console.gov.code42.com` (US3), use:
`https://alert-service-default.gov.code42.com/svc/api/v1/<resource>`

- United States alert rule list management
 - If you sign in to the Code42 console at <https://console.us.code42.com> (US1), use:
`https://fed-observer-east.us.code42.com/svc/api/v1/<resource>`
 - If you sign in to the Code42 console at <https://console.us2.code42.com> (US2), use:
`https://fed-observer-default.prod.ffs.us2.code42.com/svc/api/v1/<resource>`
 - If you sign in to the Code42 console for the Code42 federal environment at <https://console.gov.code42.com> (US3), use:
`https://fed-observer-default.gov.code42.com/svc/api/v1/<resource>`
- Ireland
 - For alerts, if you sign in to the Code42 console at <https://console.ie.code42.com> (EU1), use:
`https://alert-service-default.ie.code42.com/svc/api/v1/<resource>`
 - For alert rule list management, if you sign in to the Code42 console at <https://console.ie.code42.com> (EU1), use:
`https://fed-observer-default.ie.code42.com/svc/api/v1/<resource>`

- **Resources**

- Alerts API commands
 - **resolve-alert**: Dismiss an alert.
 - **reopen-alert**: Reopen an alert.
 - **add-note**: Add a note to an alert.
 - **query-alerts**: Search for alerts using alert filter criteria. See Filter syntax for the query-alerts API command below for details.
 - **query-details**: Search for alerts by alert ID.
 - **query-details-aggregate**: Search for an alert by its alert ID. Details about the alert are aggregated into a single Observation value.
 - **rules/query-rule-metadata**: Search for alert rules in your organization's tenant using filter criteria and view basic rule information. See Filter syntax for the rules/query-rule-metadata below for details.
- Alert list management API commands

- **rules/update-is-enabled**: Enable or disable a list of alert rules.
 - **rules/add-users**: Add users to a rule's inclusion or exclusion list.
 - **rules/remove-users**: Remove users (and all aliases associated with those users) from a rule's inclusion or exclusion list.
 - **rules/remove-user-aliases**: Remove specific user aliases from a rule's inclusion or exclusion list.
 - **rules/remove-all-users**: Remove all users (and all aliases associated with those users) from a rule's inclusion or exclusion list.
 - **rules/query-cloud-share-permissions-rule**: Search for **Cloud share permissions changes** alert rules by rule ID.
 - **rules/query-endpoint-exfiltration-rule**: Search for **Exposure on an endpoint alert** alert rules by rule ID.
 - **rules/query-file-type-mismatch-rule**: Search for **Suspicious file mismatch** alert rules by rule ID.
- **Authentication method**: Include an [authentication token](#) in the request header.
 - **Tenant ID**: Many of the API commands require a tenant ID. See the [Get your organization's tenant ID](#) section below.
 - **API documentation**: For additional documentation, see [Alerts](#) on the Code42 Developer Portal.

Filter syntax for the query-alerts API command

The `query-alerts` API uses these filter types, operators, and criteria values to search for alert notifications.

Filter Type	Operator	Criteria
DateObserved	On On or after On or before	Date the alert was triggered, in YYYY-MM-DD format
Actor	Is Is not Contains Does not contain	The username or cloud alias (actor) of the person who caused the event, or portions thereof

Severity	Is Is not	High, Medium, or Low
RuleName	Is Is not Contains Does not contain	The name of the rule, or portions thereof
Description	Is Is not Contains Does not contain	The description of the rule, or portions thereof
AlertState	Is Is not	Open or Dismissed
AlertID	Is	The ID of a specific alert notification

Filter syntax for the rules/query-rule-metadata API command

The `rules/query-rule-metadata` uses these filter types, operators, and criteria values to search for alert rules.

Filter Type	Operator	Criteria
TenantId	Is	The ID o
ObserverRuleId	Is	The ID o
Type	Is Is not	The rule' <ul style="list-style-type: none"> • Clouc FED_ • Expos FED_ • Suspi FED_

Name	Is Is not Contains Does not contain	The name
Description	Is Is not Contains Does not contain	The description
Severity	Is Is not	High, Medium, Low
IsSystem	Is	True or False default rule list or High priority rule list
IsEnabled	Is	True or False enabled
RuleSource	Is Is not	The source of the rule <ul style="list-style-type: none"> • For rule list: D • For rule list: H
ModifiedAt	On On or after On or before	Date the rule was modified in YYYY-MM-DD format
ModifiedBy	Is Is not Contains Does not contain	Username of the user who modified the rule. For Code42 rules, this is the Code42 user name.

CreatedAt	On On or after On or before	Date the format
CreatedBy	Is Is not Contains Does not contain	Username rule. For Employee Code42

Get your organization's 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> (US1), use:
`https://console.us.code42.com/api/v3/customer/my`
 - If you sign in to the Code42 console at <https://console.us2.code42.com> (US2), use:
`https://console.us2.code42.com/api/v3/customer/my`
 - If you sign in to the Code42 console for the Code42 federal environment at <https://console.gov.code42.com> (US3), use:
`https://console.gov.code42.com/api/v3/customer/my`
- Ireland: If you sign in to the Code42 console at <https://console.ie.code42.com> (EU1), use:
`https://console.ie.code42.com/api/v3/customer/my`

In the following example, replace `<AuthToken>` with the [authentication token](#) you obtained and replace `console.us.code42.com` with the URL of your Code42 cloud instance:

[Copy to clipboard](#)

```
curl -vvv -X GET -H 'Authorization: Bearer
<AuthToken>'
'https://console.us.code42.com/api/v3/customer/my'
```

A successful response returns the **tenantUid**:

```
{ "data": { "name": "My
Org", "registrationKey": "4s42ukut7pwpwr4c", "deployme
4242-4242-428a-
8a1dfd352f2f", "masterServicesAgreement":
{ "accepted": true, "acceptanceRequired": false } }, "erro
```

Identify userUIDs

Each user in Code42 is uniquely identified by a userUID value. You use this userUID with the `/api/v1/rules/add-user` and `/api/v1/rules/remove-user` to associate a list of email addresses or cloud aliases with a specific user, and to add and remove those alias lists in alert rules.

You can locate userUIDs directly in the Code42 console:

- Export a [list of Code42 users to a CSV file](#). The file includes each user's userUID.
- View userUIDs in the [User Backup report](#) and [Device Status report](#).

You can also use the `/api/User` API command to [identify a userUID](#). In the following example:

- Replace `<RequestURL>` with the address you use to access the Code42 console, for example, `https://console.us.code42.com/`
- Replace `<Code42Username>` with the Code42 username of the user whose userUID value you want to view.
- Replace `<AuthToken>` with the [authentication token](#).

[Copy to clipboard](#)

```
curl -X GET '<RequestURL>/api/User?q=
<Code42Username>&active=true' -H "Authorization:
Bearer <AuthToken>"
```

When prompted, enter your Code42 password. A successful response lists information about that user, including the userUID.

```
{ "metadata": { "timestamp": "2020-06-12T19:45:41.962Z", "params": { "q": "astrid.ludwig@example.com", "active": "true" } }, "data": { "totalCount": 1, "users": [ { "userId": 199520, "userUid": "933431721358889954", "status": "Active", "creationDate": "2019-12-23T15:51:01.871Z", "modificationDate": "2019-12-23T15:51:02.057Z", "passwordReset": false, "localAuthenticationOnly": true, "admin": { "securityTools": true } } ] } }
```

Related topics

- [Create and manage alert rules](#)
- [Manage Rules reference](#)
- [Introduction to the Code42 command-line interface](#)
- [Code42 API syntax and usage](#)
- [Code42 API authentication methods](#)

[Back to top](#)

Archived by DOC-12587 on-p...

Archived by DOC-12688 - All...

Was this article helpful?

Yes No Leave feedback

Attachments

Search file names and descriptions.

File <input type="checkbox"/>	Last modified <input type="checkbox"/>	Size <input type="checkbox"/>	Added by <input type="checkbox"/>
-------------------------------	--	-------------------------------	-----------------------------------

No files attached.

