

Configure Tags on Cisco Intersight Resources

Contents

[Introduction](#)

[Background Information](#)

[Account Resource Tags](#)

[Requirements](#)

[via the UI](#)

[Via the API](#)

[Infrastructure Service Resource Tags](#)

[via the UI List View](#)

[Organization Resource Tags](#)

[Via API](#)

[Device Registration Resource Tags](#)

[Via the API](#)

Introduction

This document describes the steps required to add tags to Cisco Intersight resources.

Background Information

A tag is a generic piece of key/value metadata which can be applied to resources within Cisco Intersight. These resources can vary from Server endpoints, to Accounts, and more.

As a user, tags can be used to group Cisco Intersight resources which will allow for querying of resources based on these tag values.

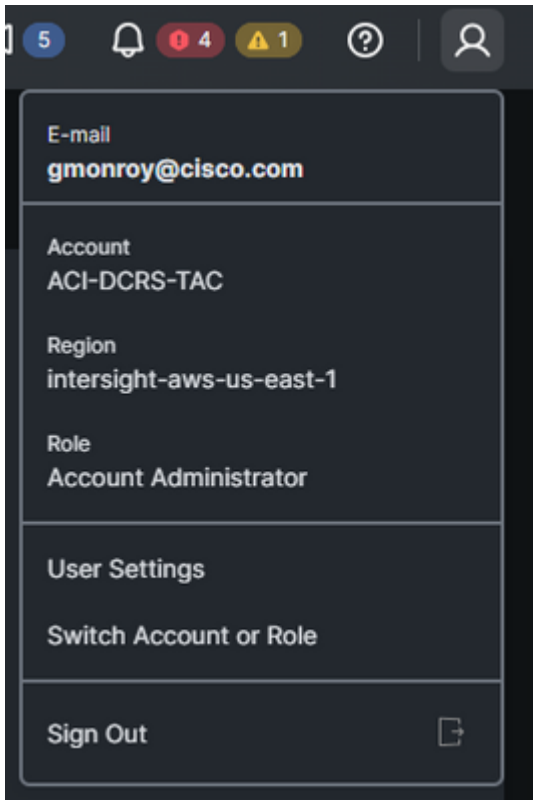
Within Cisco, there are various programs that rely on Cisco Intersight resource tags to enable/disable specific featuresets. Please refer to the documentation of the specific program for more information on those features and functionality.

Account Resource Tags

Requirements

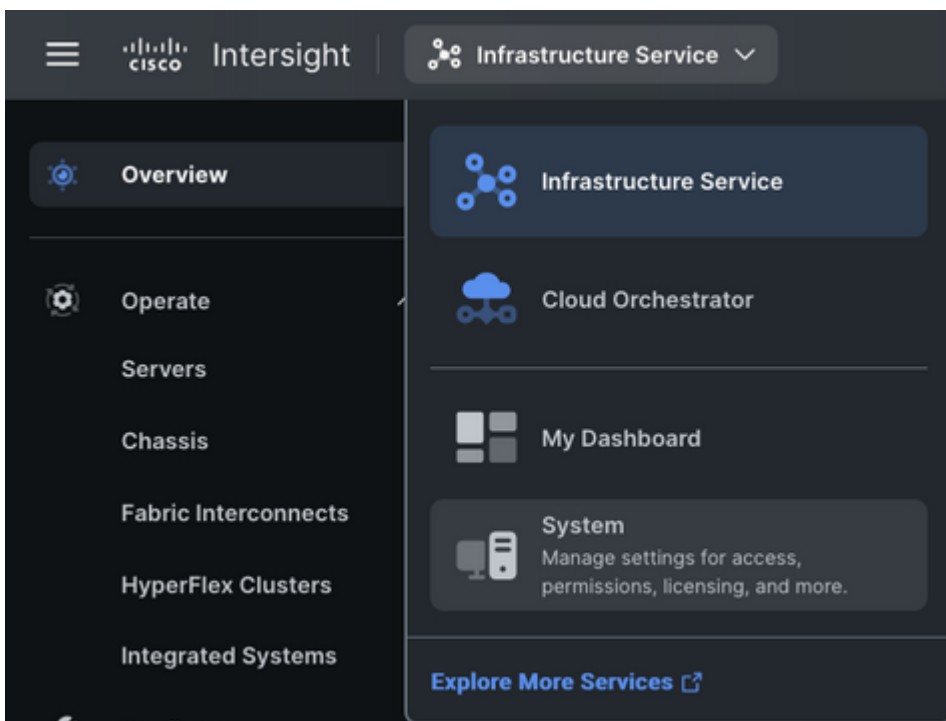
- Account Administrator role for the account to be modified
- Access to the [iam.Account API endpoint](#)

When logged in via the UI, click the profile menu in the top right of the UI to show the logged-in **Account** and **Role**.



via the UI

1. Click the Services Selector
2. Select "**System**"



3. From the **Settings > Account Details** view, Click "Configure".

The screenshot shows the Cisco Intersight Settings page. The top navigation bar includes the Cisco logo, the word "Intersight", a "System" dropdown menu, and a search bar. The left sidebar contains a "Settings" menu with a gear icon, and an "Admin" section with a shield icon and an upward arrow. The "Admin" section lists: Targets, Software Repository, Tech Support Bundles, Audit Logs, Sessions, and Licensing. The main content area is titled "Settings" and is divided into two columns. The left column contains a list of settings categories: GENERAL (Account Details, Access Details, Notifications), AUTHENTICATION (Single Sign-On, Domain Names, Cisco ID, Trusted Certificates), ACCESS & PERMISSIONS (IP Access Management, Security & Privacy, Users, Groups, Roles, Organizations, Resource Groups), and API (API Keys, OAuth2 Tokens, Webhooks). The right column is titled "Account Details" and displays a table of account information.

Field	Value
Account Name	WW-SV-RTP
Account ID	5981c48f3e95200001fdf5d7
Access Link	https://5981c48f3e95200001fdf5d7 https://ww-sv-rtp.intersight.com/
Region	intersight-aws-us-east-1
Created Time	Aug 2 2017 8:24 AM
Default Idle Timeout	30m
Maximum Concurrent Sessions per User	32 sessions
Default Session Timeout	16h
Audit Log Retention Period	48 Months
Tags	-

4. From the "Configure Account Settings" popup, a **key:value** pair can be submitted to add a new tag.

5. Once entered, click "Configure" to submit

Configure Account Settings



Account Name *

WW-SV-RTP

Default Idle Timeout (Seconds)

1800



300 - 18000

Default Session Timeout (Seconds)

57600



300 - 31536000

Maximum Concurrent Sessions per User (Sessions)

32



2 - 32

Audit Log Retention Period (Months)

48



6 - 48

Set Tags

AutoRMAEmail kmccabe2@cisco.com, sttardy@cisco.com



Cancel

Configure

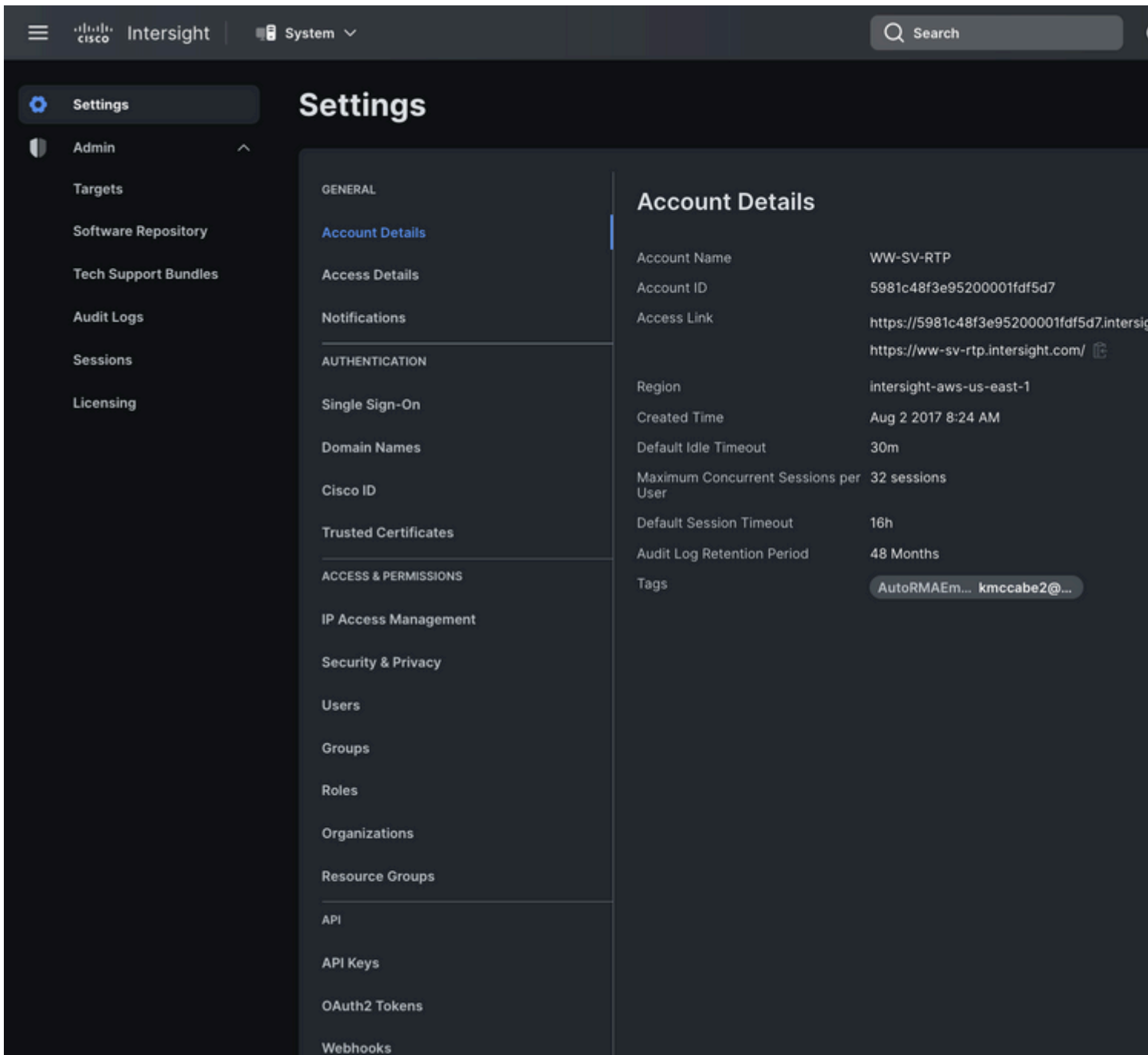
The tag must be entered with a in "key:value" format. For example above we entered:

AutoRMAEmail: kmccabe2@cisco.com, sttardy@cisco.com

This will create a tag on the Account resource with a key of AutoRMAEmail and a value of kmccabe2@cisco.com, sttardy@cisco.com.

Note: When adding a net-new tag, the auto-helper prediction will not show any options. Enter the net-new tag exactly as documented, then hit **enter** to submit.

6. Configured Tags can be validated form the Account Details view



The screenshot shows the Cisco Intersight Settings page. The left sidebar contains a navigation menu with items: Settings, Admin, Targets, Software Repository, Tech Support Bundles, Audit Logs, Sessions, and Licensing. The main content area is titled 'Settings' and is divided into two columns. The left column lists various settings categories: GENERAL (Account Details, Access Details, Notifications), AUTHENTICATION (Single Sign-On, Domain Names, Cisco ID, Trusted Certificates), ACCESS & PERMISSIONS (IP Access Management, Security & Privacy, Users, Groups, Roles, Organizations, Resource Groups), and API (API Keys, OAuth2 Tokens, Webhooks). The right column is titled 'Account Details' and displays the following information:

Account Name	WW-SV-RTP
Account ID	5981c48f3e95200001fdf5d7
Access Link	https://5981c48f3e95200001fdf5d7.intersight.com/
Region	intersight-aws-us-east-1
Created Time	Aug 2 2017 8:24 AM
Default Idle Timeout	30m
Maximum Concurrent Sessions per User	32 sessions
Default Session Timeout	16h
Audit Log Retention Period	48 Months
Tags	AutoRMAEm... kmccabe2@...

Via the API

1. [HTTP GET the iam.Account resource](#) to find the Moid of the specific Account resource (AccountMoid)

to be updated. Any existing Tags to be kept should be documented.

```
<#root>
```

```
GET /api/v1/iam/Accounts
```

```
RESPONSE:
```

```
{
  "ObjectType": "iam.Account.List",
  "Results": [
    {
      "
```

```
AccountMoid
```

```
": "5eb2e1e47564612d307xxxxx",
  "
```

```
Moid
```

```
": "5eb2e1e47564612d307xxxxx",
  ...snip...
  "
```

```
Tags
```

```
": [{
  "Key": "existingKey",
  "Value": "existingVal"
}]
}]
}
```

2. [HTTP POST the specific iam.Account resource by Moid](#) and include the new and existing Tags in the request payload.

Note: If the Account Resource has existing Tags, they must be included in the POST to be retained. If they are not included in the POST, they will be deleted from the Account Resource.

```
<#root>
```

```
POST /api/v1/iam/Accounts/5eb2e1e47564612d307xxxxx
```

```
PAYLOAD:
```

```
{
  "
```

```
Tags
```

```
": [{
  "Key": "existingKey",
  "Value": "existingVal"
}, {
  "Key": "ACIProactive",
  "Value": "brvarney@cisco.com"
}]
```

}

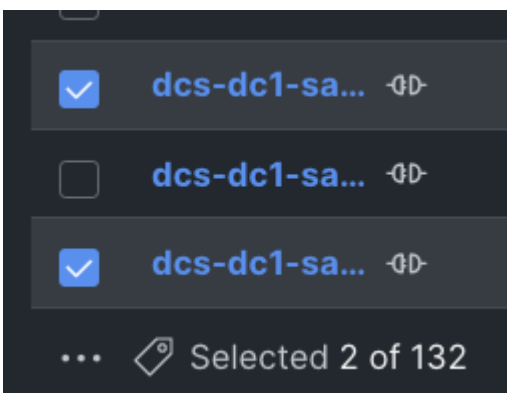
Infrastructure Service Resource Tags

via the UI List View

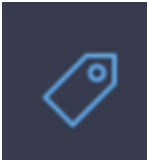
Resources that are displayed within a list view via the Infrastructure Service can be tagged. For Example, Servers, Clusters, Fabric Interconnects, Chassis, etc.

Note: Proactive RMA does not support any features enabled via Infrastructure Service resource Tags. Do not use the below steps to configure **Proactive RMA** tags.

1. Within a list view, check the box of the resources to be tagged

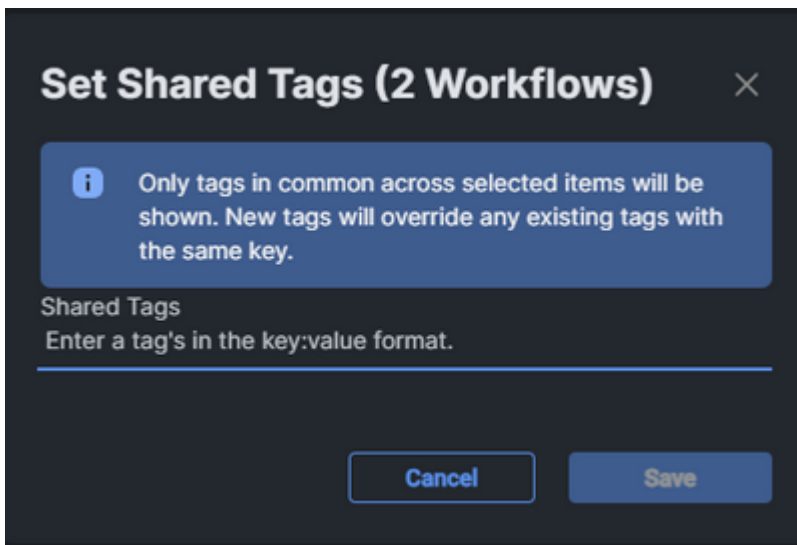


2. Press the tag button located next to the ellipsis



3. Within the "Set Shared Tags" popup, enter the **key:value** tag to be applied to all selected objects

4. Hit "**Save**" to submit



Note: When adding a net-new tag, the auto-helper prediction will not show any options. Enter the net-new tag exactly as documented, then hit **enter** to submit.

Organization Resource Tags

Via API

1. Open API Docs for Organizations

Navigate to the api doc page for [Organizations](#).

Note: If using the Connected Virtual Appliance, navigate to [https://\[FQDN_of_appliance\]/apidocs/apirefs/organization/Organizations/model/](https://[FQDN_of_appliance]/apidocs/apirefs/organization/Organizations/model/) instead

2. Identify Organization you wish to update.

Please see the [Intersight API Query Guide](#) for reference.

Users can simply use the GET endpoint to list all Organizations with no parameters. If there are too many organizations in your account to easily view in one output, users can use a \$select query parameter to limit the fields shown, but ensure to include Tags in the \$select statement eg:

The screenshot displays the Cisco Intersight Developer Center API Reference for the 'organization.Organizations' resource. The left sidebar lists various methods: POST (Create), GET (Read), POST (Update), PATCH (Update), DELETE (Delete), and GET (Read). The main content area shows the GET method details, including a REST Client interface with a 'Send' button and a '200 Success' status. The response text is shown in a dark-themed editor, displaying a JSON object with the following structure:

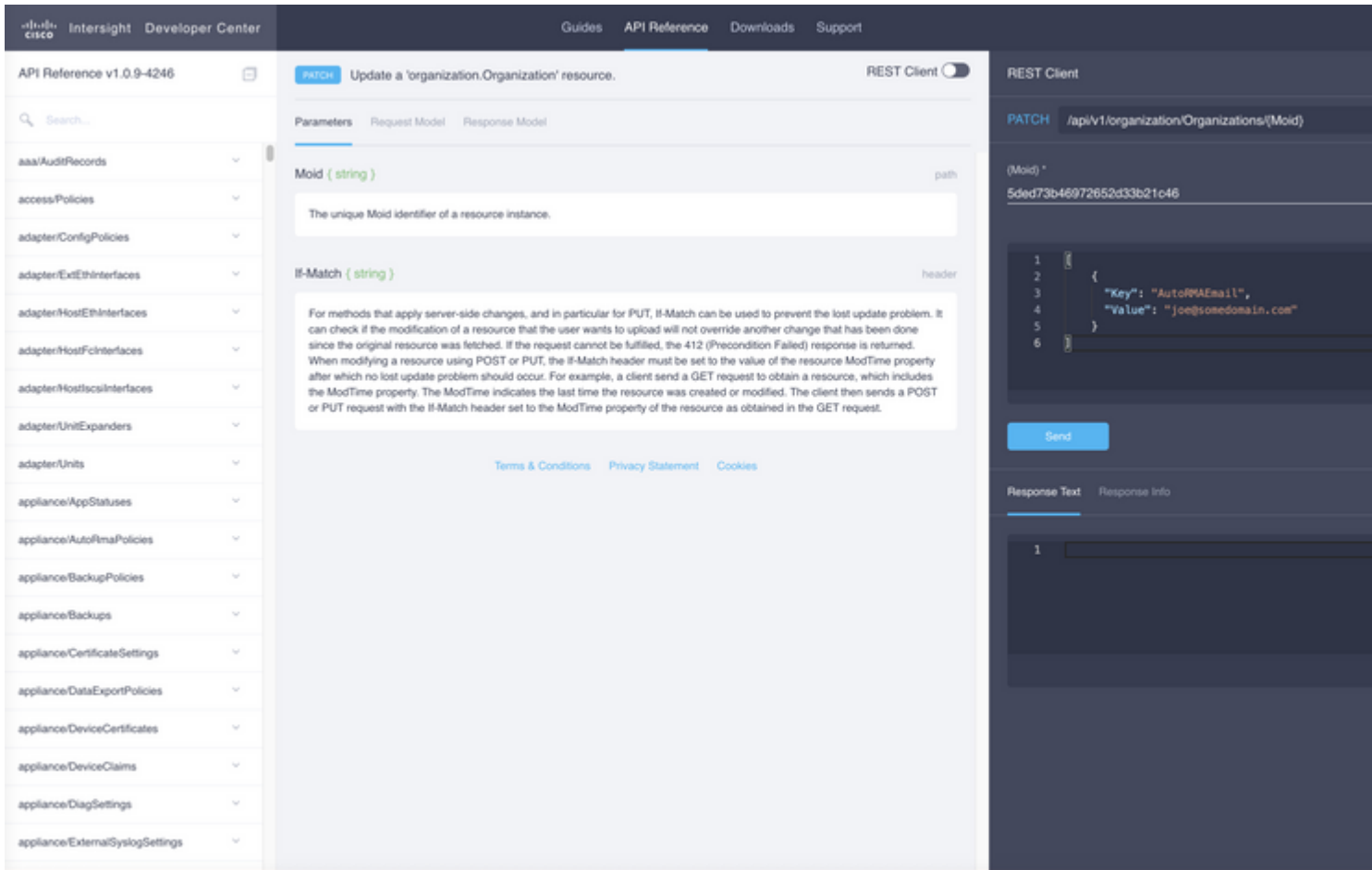
```

1  {
2    "ObjectType": "organization.Organizations",
3    "Results": [
4      {
5        "ClassId": "organization.Organizations",
6        "Moid": "5ddea34a6972652d3353b21...",
7        "Name": "default",
8        "ObjectType": "organization.Organizations",
9        "Tags": [
10       {
11         "Key": "hello",
12         "Value": "world"
13       }
14     ]
15   },
16   {
17     "ClassId": "organization.Organizations",
18     "Moid": "5ded73b46972652d33b21...",
19     "Name": "kMcCabe2",
20     "ObjectType": "organization.Organizations",
21     "Tags": [
22     {
23       "Key": "AutoRMAEmail",
24       "Value": "joe@somedomain.com"
25     }
26   ]
27   },
28 ]
29 }

```

From the API output the field we need is the Moid field, this is a unique identifier for this organization in intersight and will be used in the next step, we also need to get any tags that are in there for the next step.

3. Update the Organization's Tags with the [Organization PATCH API](#) endpoint against the Organizations Moid. Ensure you re-enter existing tags gathered in the body field, or else they will be removed.



The body for the sample PATCH call above:

```
{ "Tags": [ { "Key": "AutoRMAEmail", "Value": "joe@somedomain.com" } ] }
```

Any existing tags that are on the registered can be added into the array of tags.

Please note: if you are following this procedure for to configure Proactive RMA, the email address(s) in here need to be correlative to a CCO Account.

Device Registration Resource Tags

Via the API

1. Open API Docs for Registered Devices

Navigate to the API doc page for [Registered Devices](#)

If using the Connected Virtual Appliance, navigate to [https://\[FQDN_of_appliance\]/apidocs/apirefs/asset/DeviceRegistrations/model/](https://[FQDN_of_appliance]/apidocs/apirefs/asset/DeviceRegistrations/model/) instead

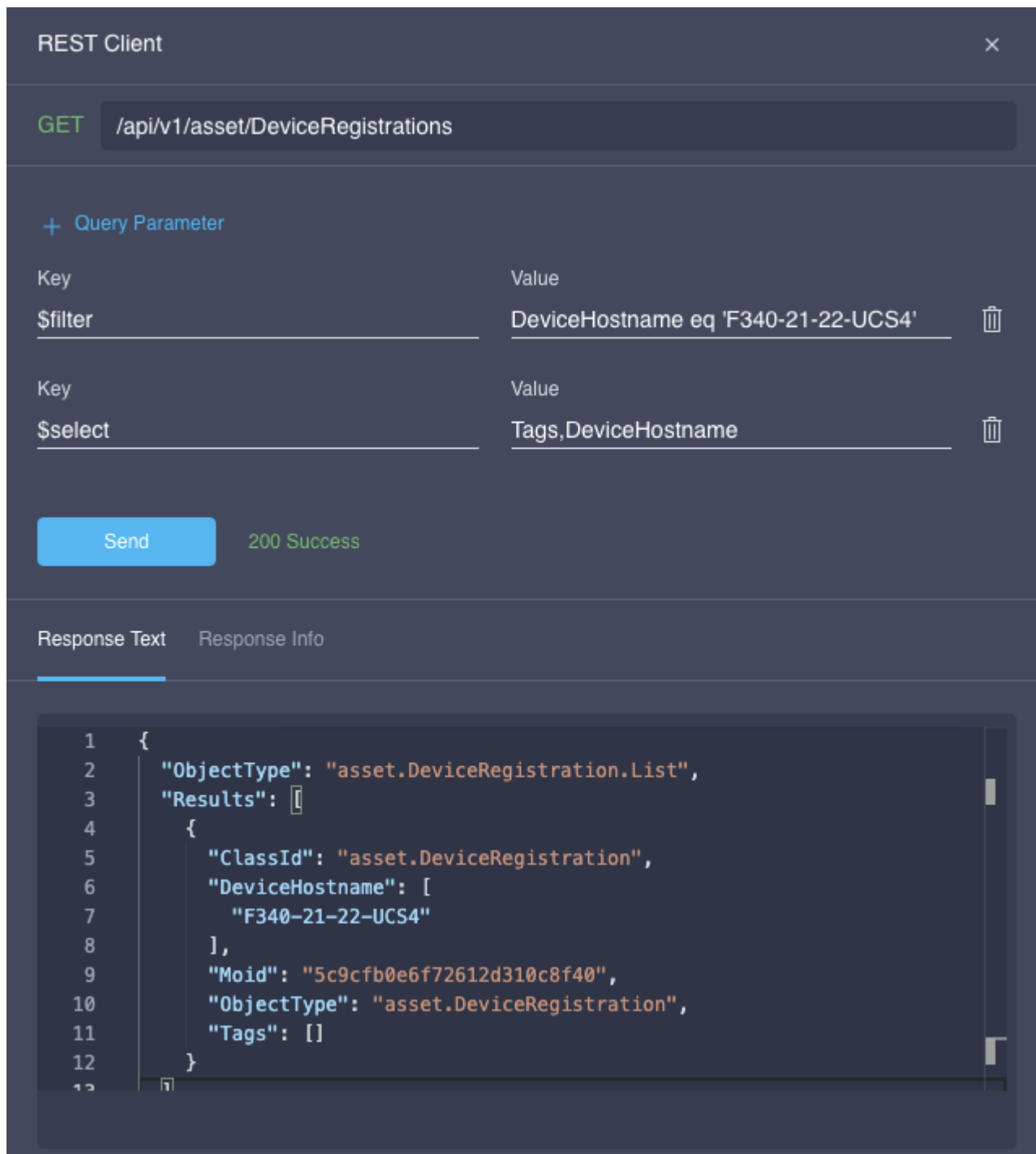
2. Identify the Registered Device which needs to be updated

Please see the [Intersight API Query Guide](#) for reference

One of the easiest ways to query is by hostname, to do this, a query could be crafted like:

```
DeviceHostname eq 'F340-21-22-UCS4'
```

Leveraging \$filter and \$select we see a more manageable output:



The screenshot shows the REST Client interface. The request is a GET to `/api/v1/asset/DeviceRegistrations`. Two query parameters are defined:

Key	Value
<code>\$filter</code>	<code>DeviceHostname eq 'F340-21-22-UCS4'</code>
<code>\$select</code>	<code>Tags,DeviceHostname</code>

The response status is `200 Success`. The response text is a JSON object:

```
1  {
2    "ObjectType": "asset.DeviceRegistration.List",
3    "Results": [
4      {
5        "ClassId": "asset.DeviceRegistration",
6        "DeviceHostname": [
7          "F340-21-22-UCS4"
8        ],
9        "Moid": "5c9cfb0e6f72612d310c8f40",
10       "ObjectType": "asset.DeviceRegistration",
11       "Tags": []
12     }
13   ]
}
```

3. Use the PATCH API to update tags

Extract any tags that are already on the registered device as well as the moid of the device. Navigate to the [PATCH endpoint](#), paste in the Moid in the top moid entry For example:

The screenshot shows a REST Client interface. At the top, the title is "REST Client". Below it, the HTTP method is "PATCH" and the URL is "/api/v1/asset/DeviceRegistrations/{Moid}". The path parameter "{Moid}" is replaced with the value "5c9cfb0e6f72612d310c8f40".

The request body is a JSON object: `{ "Tags": [{ "Key": "AutoRMAEmail", "Value": "joe@somedomain.com" }] }`.

A "Send" button is visible, and the status is "200 Success".

Below the request, there are two tabs: "Response Text" (selected) and "Response Info". The response text is a JSON object: `{ "Moid": "5c9cfb0e6f72612d310c8f40", "ObjectType": "asset.DeviceRegistration", "ClassId": "asset.DeviceRegistration", "CreateTime": "2019-03-28T16:49:18.745Z", "ModTime": "2021-05-17T18:57:57.275966714Z", "Tags": [{ "Key": "AutoRMAEmail", "Value": "joe@somedomain.com" }] }`.

The body for the sample PATCH call above:

```
{ "Tags": [ { "Key": "AutoRMAEmail", "Value": "joe@somedomain.com" } ] }
```

Any existing tags that are on the registered can be added into the array of tags.

Please note: if you are following this procedure for to configure Proactive RMA, the email address(s) in here need to be registered with a valid Cisco Account Username/CCO ID.