Management

The **Administration** page offers opporutnities to watch the state of your account and the overall status of the cloud service providers affiliated with your account.

Management

The **Administration** page offers opporutnities to watch the state of your account and the overall status of the cloud service providers affiliated with your account.

API Keys

Navigate to **Administration** > **Management** > **API Keys** to view this page.

Search

Use the search bar to seek or filter the list of API keys with key words. You must use at least three characters for the search to qualify.

API Key Table and Actions

This table lists all the API keys that are created by Multicloud Defense components for your cloud service providers. View the role, key ID, the date the key was added to Multicloud Defense, and the date the key expires.

From here you can create or delete API keys. Note that these keys are generated by Multicloud Defense and not related to the keys your cloud service provider might create to maintain communication. Continue reading for more information.

Create an API Key in Multicloud Defense

Use the following procedure to create an API Key:

Procedure

Step 1 Navigate to Navigate to **Administration** > **Management** > **API Keys**.

Step 2 Click **Create API Key**.

Step 3 Enter a unique **Name**.

Step 4 Confirm the **Email Address** that Multicloud Defense automatically generates. You cannot change this option.

Step 5 Use the drop-down menu to select one of the key roles:

- **admin_read_only** - This role restricts interactions so you cannot modify or action anything, and can only "view" the available data.
- **admin_read_rw** - This role allows you to read and modify available data.

Step 6 Enter an appropriate value for **API Key Lifetime (days)**. The deafult value is 365 days.

Step 7 Click **Save**.

Delete an API Key from Multicloud Defense

Use the following procedure to delete a API Key:

Procedure

Step 1 Navigate to **Administration** > **Management** > **API Keys**.

Step 2 Select the API Key from the table and check the box so it is highlighted.

Step 3 Click **Delete**.

Step 4 Confirm you want to delete the key and click **Yes**. The key is immediately removed from Multicloud Defense.

Account Level Settings

This page displays some of the tags used in Multicloud Defense, including application tags and custom tags. Continue reading for more information.

Application Tags

The application tag is a string of characters and is used as one of the classification criteria for the automatic classification of processes or threads. Tagging allows you to group apps based on your unique requirements so that you can search for apps and find vulnerabilities. Note that not all cloud service providers support the use of application tags.

Note You can only create one appication tag at a time. If you need to create a new tag, you **must** delete the existing tag and then create a new application tag.

Create an Application Tag

Use the following procedure to create an application tag. Note that these tags are for internal use only and may not be recognized or available from your cloud ervice provider's interface.

Procedure

Step 1 Navigate to **Administration** > **Management** > **Account**.

Step 2 In the **Application Tag** table, click **Create**.

Step 3 The type of application tag is `APPLICATION_TAG_KEYS` by default.

Step 4 Enter a brief **Description** of the tag. This can help identify or differentiate between other tags that might have a similar name or concept.

Step 5 Enter at least one **Value**. Hit `Enter` after each value to create more than one. Note that these values are case sensitive.

Step 6 Click **Save**. The tag is created and available in the table.

Edit an Application Tag

Use the following procedure to edit an existing application tag that has been created in Multicloud Defense. You cannot use this procedure to modify tags that were created in your cloud service provider's interface.

Procedure

Step 1 Navigate to **Administration** > **Management** > **Account**.

Step 2 In the **Application Tag** table, locate the application tag you want to edit and check its box on the left so it is highlighted.

Step 3 Click **Edit**.

Step 4 Modify the following parameters:

- **Description** - You can edit or delete the description.
- **Tag Values** - You can add or remove tags here.

Step 5 Click **Save**. Alternatively, you can cancel at any time without saving changes.

Delete an Application Tag

Use the following procedure to delete an existing application tag:

Procedure

Step 1 Navigate to **Administration** > **Management** > **Account**.
Step 2 In the **Application Tag** table, locate the application tag you want to edit and check its box on the left so it is highlighted.
Step 3 Click **Delete**.
Step 4 Confirm you want to delete the application tag and click **Yes**.

Custom Tags

Custom tags are simple pieces of data that provide details about an item and make it easy to locate related items that have the same tag. You can use a tag to easily identify or differentiate an object, policy, rule, and more.

Create a Custom Tag

Use the following procedure to create a custom tag in Multicloud Defense. Note that these tags are for internal use only and may not be recognized or available from your cloud ervice provider's interface.

Procedure

Step 1 Navigate to **Administration** > **Management** > **Account**.
Step 2 In the **Custom Tag** table, click **Create**.
Step 3 Enter the **Value** of the tag. This can help identify or differentiate between other tags that might have a similar name or concept
Step 4 Enter at least one **Value**.
Step 5 Click **Save**. The tag is created and available in the table.

Edit a Custom Tag

Use the following procedure to modify an existing custom tag:

Procedure

Step 1 Navigate to **Administration** > **Management** > **Account**.
Step 2 In the **Custom Tag** table, locate the application tag you want to edit and check its box on the left so it is highlighted.
Step 3 Click **Edit**.
Step 4 Modify the following parameters:

- Key.
- Values.

Step 5 Click **Save**. Alternatively, you can cancel at any time without saving changes.

Delete a Custom Tag

Use the following procedure to delete an existing custom tag:

Procedure

Step 1 Navigate to **Administration** > **Management** > **Account**.
Step 2 In the **Custom Tag** table, locate the application tag you want to edit and check its box on the left so it is highlighted.
Step 3 Click **Delete**.
Step 4 Confirm you want to delete the application tag and click **Yes**.

System

The **System** page is a historical document that catalogues at least a year's worth of updates. You can use these details for general knowledge, locating the correct Release Notes version, and when you contact Cisco Support for product help. The following information collections are displayed here:

Component

This section displays the current versions for both the Multicloud Defense Controller and the user interface. Note that you cannot force an update or rollback to a previous version from this page.

Gateway Images

The gateway images table denotes when your Multicloud Defense Gateway was upgraded, which version of the gateway was in place and for how long, and what time zone the gateway is established in.

Talos/Network Intrusion

This table displays all the updates from Cisco's Talos Intelligence Group. These updates are pushed to Cisco products separate from a normal product software release.

Web Protection

This table displays all the Web Application Firewall (WAF) core and trustwave rule updates against the latest Web application vulnerabilities and threats.

Metering

The **Metering** page displays graphs of usage, both for the overall useage of Multicloud Defense and the gateway instances created for your cloud service providers.

Filters

Use the filters located at the top of the page to determine the data displayed in the page. You can change this view by selecting the month and year. You can use these filter settings to generate a usage report.

Generate a Usage Report

You can generate a usage report for either of the two options from this page. Navigate to **Administration** > **Mangement** > **Metering** and expand the **Download** drop-down option in the **Filter** section of the page to select either usage or instances. The file is downloaded locally as an .csv file. Use the filtering options to determine the timespan the report should generate from.

Usage Records

The **Usage Records** table details the number of accounts associated with your tenant, how many hours the accounts were interacted with, and on what days of the month selected in the Filter section. You can determine from the usage/month ratio what days were the most active.

Instance Records

The **instance Records** table displays the following instance statistics:

- Account Name.
- Account type by cloud service provider.
- Instance ID.
- Instance Type.
- Availablilty zone.
- Gateway.
- Started - When the gateway instance was created.
- Ended - When the gateway instance expired or was terminated.

Alert Profiles

Access the following Management views by navigating to **Administration** > **Alert Profiles**.

Both the **Services** and **Alerts** page focus on alerts from Multicloud Defense. The **Alerts** page focuses on *where* alerts are sent to and the **Alerts** page details *what* alerts are sent to the endpoints configured. For ideal configuration, spend time setting up entries in both pages to successfully and wholly optimze the alert opportunity within the dashboard.

Services

Navigate to **Administration** > **Management** > **Service** to view this page.

Services focuses on **where** you want to send alerts to. Note that you must provide criteria from the third-party application in order to successfully configure any options on this page.

Search

Use the search bar to seek or filter the list of services with key words. You must use at least three characters for the search to qualify.

Services Table and Actions

This table lists all the services that are created by Multicloud Defense components for your cloud service providers. View the name, type of service, the date the service was updated.

From here you can create or delete services. Note that these services are generated by Multicloud Defense and not related to the services your cloud service provider might provide.

Create a Service

Use the following procedure to create a service:

Before you begin

You must have service notifications or integrations enabled or allowed on your third party messaging application.

Procedure

Step 1 Navigate to Navigate to **Administration** > **Management** > **Services**.

Step 2 Click **Create**.

Step 3 Enter a unique **Name**.

Step 4 (Optional) Enter a **Description**. This may help differentiate between other services that may have a similar name.

Step 5 Use the drop-down menu to select the service **Type**:

- Pager Duty.
- ServiceNow.
- Slack.
- Datadog.
- Microsoft Sentinel.
- Microsoft Teams.
- Webex.
- Splunk.

Step 6 Depending on the service type, complete the following entries when prompted:

- API Key.
- API URL.
- Azure Log Table Name.
- Azure Log Analytics Workspace ID

- (Optional for Splunk) Index.

Step 7 Click **Save**.

Edit a Service

Use the following procedure to edit an existing service:

Procedure

Step 1 Navigate to Navigate to **Administration** > **Management** > **Services**.
Step 2 Locate and select the service within the table so it is highlighted.
Step 3 Expand the Actions drop-down menu and click **Edit**.
Step 4 Modify the following aspects of the service:

- Name.
- Description.
- Type.
- Type-specific configuration criteria.

Step 5 Click **Save** to confirm the changes. At any point, click **Cancel** to close the window and cancel the changes.

What to do next

You may have to **Refresh** the page to see any changes.

Clone a Service

Use the following procedure to clone an existing service:

Procedure

Step 1 Navigate to Navigate to **Administration** > **Management** > **Services**.
Step 2 Locate and select the service within the table so it is highlighted.
Step 3 Expand the Actions drop-down menu and click **Clone**.
Step 4 A clone of the service is generated. By default, only the service **Type** and any service-specific configuration criteria is retained.
Step 5 Enter a unique **Name**.
Step 6 (Optional) Enter a description.

Step 7 Click **Save** to confirm the changes. At any point, click **Cancel** to close the window and cancel the changes.

What to do next

You may have to **Refresh** the page to see changes or additions to the table.

Export a Service

Use the following procedure to export an existing service:

Procedure

Step 1 Navigate to Navigate to **Administration** > **Management** > **Services**.

Step 2 Locate and select the service within the table so it is highlighted.

Step 3 Expand the Actions drop-down menu and click **Export**.

Step 4 Multicloud Defense generates an export wizard.

Step 5 Either click **Download** to download the terrform locally or click **Copy Code** to copy the JSON resource to manually paste into the terroform script.

Step 6 Within the terrform prompt, execute the command provided in the lower half of the window: `terraform import "ciscomcd_alert_profile". "servicename" <number in table>`

Step 7 Follow the prompts within terraform to complete the task. There are no more steps in the dashboard.

Delete a Service

Use the following procedure to delete an existing service:

Procedure

Step 1 Navigate to Navigate to **Administration** > **Management** > **Services**.

Step 2 Locate and select the service within the table so it is highlighted.

Step 3 Expand the Actions drop-down menu and click **Delete**.

Step 4 Confirm you want to delete the service and click **Yes**.

Step 5 The service is removed from Multicloud Defense.

Alerts

The Alerts page focuses on **what** alerts are sent to the third-party endpoints.We strongly recommend configuring both alerts and services to take advantage of the alerts opportunity.

Create an Alert

Use the following procedure to create an alert:

Procedure

Step 1 Navigate to Navigate to **Administration** > **Management** > **Services**.

Step 2 Click **Create**.

Step 3 Enter a unique **Name**.

Step 4 (Optional) Enter a **Description**. This may help differentiate between other services that may have a similar name.

Step 5 Select the **Alert Profile**. At this time, `Pagerduty` is the only option available.

Step 6 Use the drop-down menu to select the alert **Type**.

- System Logs.
- Audit Logs.
- Discovery.

Step 7 (Optional) Use the drop-down menu to select the **Sub Type**. Note that these options may change or may not be available depending on the Type you selected in step 6:

- Gateway.
- Account.
- Controller.
- Insights Rule.

Step 8 Use the drop-down menu and select the level of **Severity**:

- Info.
- Warning.
- Medium.
- High.
- Critical.

Step 9 The **Enabled** checkbox is checked by default. This option designates whether the alert profile is active and usable or not. If it is disabled, Multicloud Defense does not include it when issuing alerts.

What to do next

Services to designate where these alerts are sent to.

Edit an Alert

Use the following procedure to edit an existing alert:

Procedure

Step 1 Navigate to Navigate to **Administration** > **Management** > **Alert**.

Step 2 Locate and select the alert within the table so it is highlighted.

Step 3 Expand the Actions drop-down menu and click **Edit**.

Step 4 Edit any of the fields and selections of the alert proile. Note that some of the available fields may change depending on the selections you make.

Step 5 Click **Save** to confirm the changes. At any time, click **Cancel** to cancel the changes and close out the edit window.

Clone an Alert

Use the following procedure to clone an existing alert:

Procedure

Step 1 Navigate to Navigate to **Administration** > **Management** > **Alert**.

Step 2 Locate and select the alert within the table so it is highlighted.

Step 3 Expand the Actions drop-down menu and click **Edit**.

Step 4 A clone of the alert is generated. By default, only the **Alert Profile** and **Type** is retained.

Step 5 Edit any of the remaining fields and selections of the alert. Note that some of the available fields may change depending on the selections you make.

Step 6 Click **Save** to confirm the changes. At any time, click **Cancel** to cancel the changes and close out the edit window.

Export an Alert

Use the following procedure to export an existing alert:

Procedure

Step 1 Navigate to Navigate to **Administration** > **Management** > **Alert**.

Step 2 Locate and select the alert within the table so it is highlighted.

Step 3 Expand the Actions drop-down menu and click **Export**.

Step 4 Multicloud Defense generates an export wizard.

Step 5 Either click **Download** to download the terraform locally or click **Copy Code** to copy the JSON resource.

Step 6 Manually paste into the terraform script.

Step 7 Within the terraform prompt, execute the command provided in the lower half of the window: `terraform import "ciscomcd_alert_rule"."alertname" <number in table>`

Step 8 Follow the prompts within the terraform prompt to complete the task. **Close** the export window in Multicloud Defense. There are no more steps in the dashboard.

Delete an Alert

Use the following procedure to delete an existing alert:

Procedure

Step 1 Navigate to Navigate to **Administration** > **Management** > **Alert**.

Step 2 Locate and select the alert within the table so it is highlighted.

Step 3 Expand the Actions drop-down menu and click **Delete**.

Step 4 Confirm you want to delete the service and click **Yes**.

Step 5 The alert is removed from Multicloud Defense.