



Alert Destinations / SIEMs

- [Datadog](#), on page 1
- [Microsoft Sentinel](#), on page 3
- [PagerDuty](#), on page 4
- [ServiceNow](#), on page 6
- [Slack](#), on page 7
- [Webex](#), on page 9
- [Splunk](#), on page 10

Datadog

Once configured, Multicloud Defense alerts will sent to Datadog using the defined Alert Service Profile and Alert Rule.

Create an Alert Profile Service

Before you begin

In order to send alerts to Datadog, the following information is required:

- Datadog account
- API Key



Tip

- To Sign up for a Datadog account, refer to [Datadog Account \(https://www.datadoghq.com/\)](https://www.datadoghq.com/).
 - To create a Datadog API Key, refer to [Datadog API Key \(https://app.datadoghq.com/account/login?next=%2Faccount%2Fsettings#api\)](https://app.datadoghq.com/account/login?next=%2Faccount%2Fsettings#api).
-

Procedure

Step 1 Navigate to **Administration > Alert Profiles > Services**.

- Step 2** Click **Create**.
- Step 3** **Name** - Enter unique name for the alert integration. Example `multicloud defense-Datadog-profile`.
- Step 4** **Description** (optional) - Enter a description for the alert integration.
- Step 5** **Type** - Using the pulldown, choose **Datadog**.
- Step 6** **API Key** - Specify the Datadog API Key used to authenticate the communication.
- Step 7** Click **Save**.

What to do next

Create an alert rule with this new profile.

Create an Alert Rule

Before you begin

In order to send alerts to Datadog, the following information is required:

- Datadog account
- API Key



Tip

- To Sign up for a Datadog account, refer to Datadog Account (<https://www.datadoghq.com/>).
- To create a Datadog API Key, refer to Datadog API Key (<https://app.datadoghq.com/account/login?next=%2Faccount%2Fsettings#api>).

Procedure

-
- Step 1** Navigate to **Settings > Alert Profiles > Alert Rules**.
- Step 2** Click **Create**.
- Step 3** **Profile Name** - Enter unique name for the integration. Example `multicloud defense-Datadog-alert-rule`.
- Step 4** **Description** (optional) - Enter a description for the alert rule.
- Step 5** **Alert Profile** - Using the pulldown, choose a PagerDuty Alert Profile. As example, select profile created above `multicloud defense-Datadog-profile`.
- Step 6** **Type** - Using the pulldown, select either **System Logs** or **Discovery**.
- Step 7** **Sub Type** - For Type **System Logs**, the Sub Type pulldown options are either: **Gateway** or **Account**. For Type **Discovery**, the Sub Type pulldown options: **Insights Rule**.
- Step 8** **Severity** - For selected Type **System Logs**, and using the pulldown, select a Severity level from options: `Info Warning Medium High` or `Critical`. For Type **Discovery**, select a Severity level from options: `Info Medium Critical`.
- Step 9** **Enabled** - Using the checkbox, check to enable this alert profile.

Step 10 Click **Save**.

Microsoft Sentinel

Once configured, Multicloud Defense alerts will sent to Microsoft Sentinel using the defined Alert Service Profile and Alert Rule.

Create an Alert Profile Service

Before you begin

In order to send alerts to Microsoft Sentinel, the following information is required:

- Create an Azure Log Analytics Workspace.
- Define an Azure Log Table.

Procedure

- Step 1** Navigate to **Administration > Alert Profiles > Services**.
- Step 2** Click **Create**.
- Step 3** **Name** - Enter unique name for the alert integration. Example `mcd-mssentinel-profile`.
- Step 4** **Description** (optional) - Enter a description for the alert integration.
- Step 5** **Type** - Using the pulldown, choose **Microsoft Sentinel**.
- Step 6** **API Key** - Specify the Shared Key created in Azure for the Azure Log Analytics Workspace.
- Step 7** **Azure Log Table Name** - Specify the name of the Azure Log defined when creating the Azure Log Analytics Workspace.
- Step 8** **Azure Log Analytics Workspace ID** - Specify the ID of the Azure Log Analytics Workspace.
- Step 9** Click **Save**.
-

What to do next

Create an alert rule with this new profile.

Create an Alert Rule

Before you begin

In order to send alerts to Microsoft Sentinel, the following information is required:

- Create an Azure Log Analytics Workspace.
- Define an Azure Log Table.

Procedure

-
- Step 1** Navigate to **Administration** > **Alert Profiles** > **Alert**.
- Step 2** Click **Create**.
- Step 3** **Profile Name** - Enter unique name for the integration. Example `mcd-mssentinel-alert-rule`.
- Step 4** **Description** (optional) - Enter a description for the alert rule.
- Step 5** **Alert Profile** - Using the pulldown, choose the appropriate profile you previously created. As example, select profile created above `mcd-mssentinel-profile`.
- Step 6** **Type** - Using the pulldown, select either **System Logs** or **Discovery**.
- Step 7** **Sub Type** - For Type **System Logs**, the Sub Type pulldown options are either: **Gateway** or **Account**. For Type **Discovery**, the Sub Type pulldown options: **Insights Rule**.
- Step 8** **Severity** - For selected Type **System Logs**, and using the pulldown, select a Severity level from options: `Info` `Warning` `Medium` `High` or `Critical`. For Type **Discovery**, select a Severity level from options: `Info` `Medium` `Critical`.
- Step 9** **Enabled** - Using the checkbox, check to enable this alert profile.
- Step 10** Click **Save**.
-

PagerDuty

Once configured, Multicloud Defense alerts will sent to a PagerDuty API gateway using the defined Alert Service Profile and Alert Rule.

Create an Alert Profile Service

Before you begin

In order to complete the steps in this guide, you will need:

- A PagerDuty account with an API Key configured.



Tip

- Sign up for a PagerDuty account (<https://www.servicenow.com/my-account/sign-up.html>).
 - Setup the API Key (<https://developer.pagerduty.com/api-reference>).
-

Procedure

-
- Step 1** Navigate to **Administration** > **Alert Profiles** > **Services**.
- Step 2** Click **Create**.
- Step 3** **Name** - Enter unique name for the alert integration. Example `mcd-pagerduty-profile`.

- Step 4** **Description** (optional) - Enter a description for the alert integration.
- Step 5** **Type** - Using the pulldown, choose **PagerDuty**.
- Step 6** **API Key** - Copy the PagerDuty API key generated above, or other PagerDuty API Key as desired.
- Step 7** Click **Save**.
-

What to do next

Create an alert rule with this new profile.

Create an Alert Rule

Before you begin

In order to complete the steps in this guide, you will need:

A PagerDuty account with an API Key configured.



- Tip**
- Sign up for a PagerDuty account (<https://www.servicenow.com/my-account/sign-up.html>).
 - Setup the API Key (<https://developer.pagerduty.com/api-reference>).
-

Procedure

- Step 1** Navigate to **Administration > Alert Profiles > Alert Rules**.
- Step 2** Click **Create**.
- Step 3** **Profile Name** - Enter unique name for the integration. Example `mcd-pagerduty-alert-rule`.
- Step 4** **Description** (optional) - Enter a description for the alert rule.
- Step 5** **Alert Profile** - Using the pulldown, choose a PagerDuty Alert Profile. As example, select profile created above `mcd-pagerduty-profile`.
- Step 6** **Type** - Using the pulldown, select either **System Logs** or **Discovery**.
- Step 7** **Sub Type** - For Type **System Logs**, the Sub Type pulldown options are either: **Gateway** or **Account**. For Type **Discovery**, the Sub Type pulldown option is: **Insights Rule**.
- Step 8** **Severity** - For selected Type **System Logs**, and using the pulldown, select a Severity level from options: `Info Warning Medium High or Critical`. For Type **Discovery**, select a Severity level from options: `Info Medium Critical`.
- Step 9** **Enabled** - Using the checkbox, check to enable this alert profile.
- Step 10** Click **Save**.
-

ServiceNow

Once configured, Multicloud Defense alerts will sent to a ServiceNow API gateway using the defined Alert Service Profile and Alert Rule.

Create an Alert Profile Service

Before you begin

In order to complete the steps in this guide, you will need:

- A ServiceNow account with an Incoming Webhook URL.
- API Key configured.



Tip

- Sign up for a ServiceNow account (<https://www.servicenow.com/my-account/sign-up.html>)
- Setup Webhook and API Key (<https://docs.servicenow.com/search?q=setup%20webhook>)

Procedure

-
- Step 1** Navigate to **Administration > Alert Profiles > Services**.
 - Step 2** Click **Create**.
 - Step 3** **Name** - Enter unique name for the alert integration. Example `mcd-servicenow-profile`.
 - Step 4** **Description** (optional) - Enter a description for the alert integration.
 - Step 5** **Type** - Using the pulldown, choose **ServiceNow**.
 - Step 6** **API Key** - Specify the ServiceNow API key generated above, or other ServiceNow API Key as desired.
 - Step 7** **API URL** - Specify the ServiceNow Webhook URL generated above, or other ServiceNow Webhook URL as desired.
 - Step 8** Click **Save**.
-

What to do next

Create an alert rule with this new profile.

Create an Alert Rule

Before you begin

In order to complete the steps in this guide, you will need:

- A ServiceNow account with an Incoming Webhook URL.

- An API Key configured.

**Tip**

- Sign up for a ServiceNow account (<https://www.servicenow.com/my-account/sign-up.html>)
- Setup Webhook and API Key (<https://docs.servicenow.com/search?q=setup%20webhook>)

Procedure

-
- Step 1** Navigate to **Administration > Alert Profiles > Alert Rules**.
- Step 2** Click **Create**.
- Step 3** **Profile Name** - Enter unique name for the integration. Example `mcd-servicenow-alert-rule`.
- Step 4** **Description** (optional) - Enter a description for the alert rule.
- Step 5** **Alert Profile** - Using the pulldown, choose a ServiceNow Alert Profile. As example, select profile created above `mcd-servicenow-profile`.
- Step 6** **Type** - Using the pulldown, select either **System Logs** or **Discovery**.
- Step 7** Select the **Sub Type**.
- For Type **System Logs**, the options are either **Gateway** or **Account**.
 - For Type **Discovery**, the only option is **Insights Rule**.
- Step 8** Select the **Severity**.
- For selected Type **System Logs**, and using the pulldown, select a Severity level from options: **Info Warning Medium High or Critical**.
 - For Type **Discovery**, select **Info Medium Critical**.
- Step 9** **Enabled** - Using the checkbox, check to enable this alert profile.
- Step 10** Click **Save**.
-

Slack

Once configured, Multicloud Defense alerts will sent to a Slack Incoming Webhook URL using the defined Alert Service Profile and Rule.

Create an Alert Profile Service

Before you begin

In order to complete the steps in this guide, you will need:

- A Slack account with an incoming webhook URL configured.



-
- Tip**
1. Create a Slack account (<https://slack.com/get-started#/create>).
 2. Create an incoming Webhook (<https://slack.com/help/articles/115005265063-Incoming-webhooks-for-Slack#set-up-incoming-webhooks>).
-

Procedure

-
- Step 1** Navigate to **Administration > Alert Profiles > Services**.
- Step 2** Click **Create**.
- Step 3** **Name** - Enter unique name for the alert integration. Example `mcd-slack-profile`.
- Step 4** **Description** (optional) - Enter a description for the alert integration.
- Step 5** **Type** - Using the pulldown, choose **Slack**.
- Step 6** **API URL** - Specify the Slack Webhook URL generated above, or other Slack Webhook URL as desired.
-

What to do next

Create an alert rule with this new profile.

Create an Alert Rule

Before you begin

In order to complete the steps in this guide, you will need:

A Slack account with an Incoming Webhook URL configured.



-
- Tip**
1. Create a Slack account (<https://slack.com/get-started#/create>).
 2. Create an incoming Webhook (<https://slack.com/help/articles/115005265063-Incoming-webhooks-for-Slack#set-up-incoming-webhooks>).
-

Procedure

-
- Step 1** Navigate to **Administration > Alert Profiles > Alert Rules**.
- Step 2** Click **Create**.
- Step 3** **Profile Name** - Enter unique name for the integration. Example `mcd-slack-alert-rule`.
- Step 4** **Description** (optional) - Enter a description for the alert rule.
- Step 5** **Alert Profile** - Using the pulldown, choose a Slack Alert Profile. As example, select profile created above `mcd-slack-profile`.

- Step 6** **Type** - Using the pulldown, select either **System Logs** or **Discovery**.
- Step 7** **Sub Type** - For Type **System Logs**, the Sub Type pulldown options are either: **Gateway** or **Account**. For Type **Discovery**, the Sub Type pulldown options are: **Insights Rule**.
- Step 8** **Severity** - For selected Type **System Logs**, and using the pulldown, select a Severity level from options: Info Warning Medium High or Critical. For Type **Discovery**, select a Severity level from options: Info Medium Critical.
- Step 9** **Enabled** - Using the checkbox, check to enable this alert profile.
- Step 10** Click **Save**.
-

Webex

Once configured, Multicloud Defense alerts will sent to a Webex API gateway using the defined Alert Service Profile and Alert Rule.

Create an Alert Profile Service

Use the following procedure to create an alert profile for the Webex service:

Before you begin

In order to complete the steps in this guide, you will need:

- A Webex account with an Incoming Webhook URL.
- API Key configured.



- Note**
1. Create or access a [Webex account](#).
 2. Create a [Webex Incoming Webhook](#).
 3. Accept the Incoming Webhook permissions.
 4. Provide a Name and select a Webex Space.
 5. Copy the Webex Webhook URL to use in the configuration of the Alert Service Profile.
-

Procedure

- Step 1** Navigate to **Administration > Alert Profiles > Services**.
- Step 2** Click **Create**.
- Step 3** **Name** - Enter unique name for the alert integration.
- Step 4** (Optional) **Description** - Enter a description for the alert integration.
- Step 5** **Type** - Using the pulldown, choose **Webex**.

Step 6 **API URL** - Specify the Webex Webhook URL generated as part of the prerequisites, or other Webex Webhook URL as desired.

What to do next

Create an alert rule with this new profile.

Create an Alert Rule

Procedure

Step 1 Navigate to **Administration > Alert Profiles > Alert Rules**.

Step 2 Click **Create**.

Step 3 **Profile Name** - Enter unique name for the integration. An example is `mcd-servicenow-alert-rule`.

Step 4 (Optional) **Description** - Enter a description for the alert rule.

Step 5 **Alert Profile** - Using the pulldown, choose a **Webex Alert Profile**. As example, select profile created above `mcd-servicenow-profile`.

Step 6 **Type** - Using the pulldown, select either **System Logs** or **Discovery**.

Step 7 Select the **Sub Type**.

- For Type System Logs, the options are either **Gateway** or **Account**.
- For Type Discovery, the only option is **Insights Rule**.

Step 8 Select the **Severity**.

- For selected Type System Logs, and using the pulldown, select either **Info Warning Medium High** or **Critical**.
- For Type Discovery, select **Info Medium Critical**.

Step 9 **Enabled** - Using the checkbox, check to enable this alert profile.

Step 10 Click **Save**.

Splunk

Once configured, Multicloud Defense alerts will sent to an API gateway using the defined Alert Service Profile and Alert Rule.

Create a Splunk Profile Service

Use the following procedure to create an alert profile for the Splunk service:

Before you begin

You must have the following configured and ready:

- Create an API Key in Multicloud Defense and store both the key and secret. See [Create an API Key in Multicloud Defense](#) for more information.
- Set up the HTTP Event Collector (HEC) in Splunk Web. See [Configure HTTP Event Collector on Splunk Cloud](#) for more information.
- Your Splunk HEC must have the following configured:
 - HEC must be **enabled**.
 - You must have at least one active HEC token available.
 - You must use an active token to authenticate into HEC.
 - You must format the data that goes to HEC in a certain way. See [Format events for HTTP Event Collector](#).

Procedure

- Step 1** Navigate to **Administration > Alert Profiles > Services**.
- Step 2** Click **Create**.
- Step 3** **Name** - Enter unique name for the alert integration.
- Step 4** **Description** (optional) - Enter a description for the alert integration.
- Step 5** **Type** - Using the pulldown, choose **Splunk**.
- Step 6** **API Key** - Copy the Splunk API key generated above, or other PagerDuty API Key as desired.
- Step 7** Check the **Skip Verify Certificate** box if your server doesn't have certificates with SAN field matching with domain. If your server does have certificates with SAN fields matching the domain, leave this unchecked.
- Step 8** **Index**(**default - main**) is Splunk's default index where all the processed data is stored. This is provided when you configure the Splunk HEC.
- Step 9** Enter the **API URL** for the Splunk HTTP Event Collector. We recommend this URL
`https://<host>:<port>/services/collector` .
- Step 10** Click **Save**.
-

What to do next

Create an alert rule with this new profile.

Create a Splunk Rule

Use the following procedure to create a rule containing the splunk alert service:

Procedure

- Step 1** Navigate to **Administration > Alert Profiles > Alert**.
- Step 2** Click **Create**.
- Step 3** **Profile Name** - Enter unique name for the integration. Example `mcd-mssentinel-alert-rule`.
- Step 4** **Description** (optional) - Enter a description for the alert rule.
- Step 5** **Alert Profile** - Using the pulldown, choose the appropriate profile you previously created. As example, select profile created above `mcd-splunk-rule`.
- Step 6** **Type** - Using the pulldown, select either **System Logs** or **Discovery**.
- Step 7** **Sub Type** - For Type **System Logs**, the Sub Type pulldown options are either: **Gateway** or **Account**. For Type **Discovery**, the Sub Type pulldown options: **Insights Rule**.
- Step 8** **Severity** - For selected Type **System Logs**, and using the pulldown, select a Severity level from options: `Info` `Warning` `Medium` `High` or `Critical`. For Type **Discovery**, select a Severity level from options: `Info` `Medium` `Critical`.
- Step 9** **Enabled** - Using the checkbox, check to enable this alert profile.
- Step 10** Click **Save**.
-