Configure Correlation Policy on FMC

Contents

Introduction

This document describes the procedure to configure a Correlation Policy to connect events and detect anomalies on your network.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these products:

- Secure Firewall Management Center (FMC)
- Secure Firewall Threat Defense (FTD)

Components Used

The information in this document is based on these software and hardware versions:

- Firepower Threat Defense for VMware version 7.6.0

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Correlation Policies are used to identify potential security threats on your network by configuring different types of events, and are used for remediation, conditional alerts, and traffic policies.

Configure

Configure Correlation Rules

Step 1. Navigate to **Policies** > **Correlation** and select **Rule Management**.

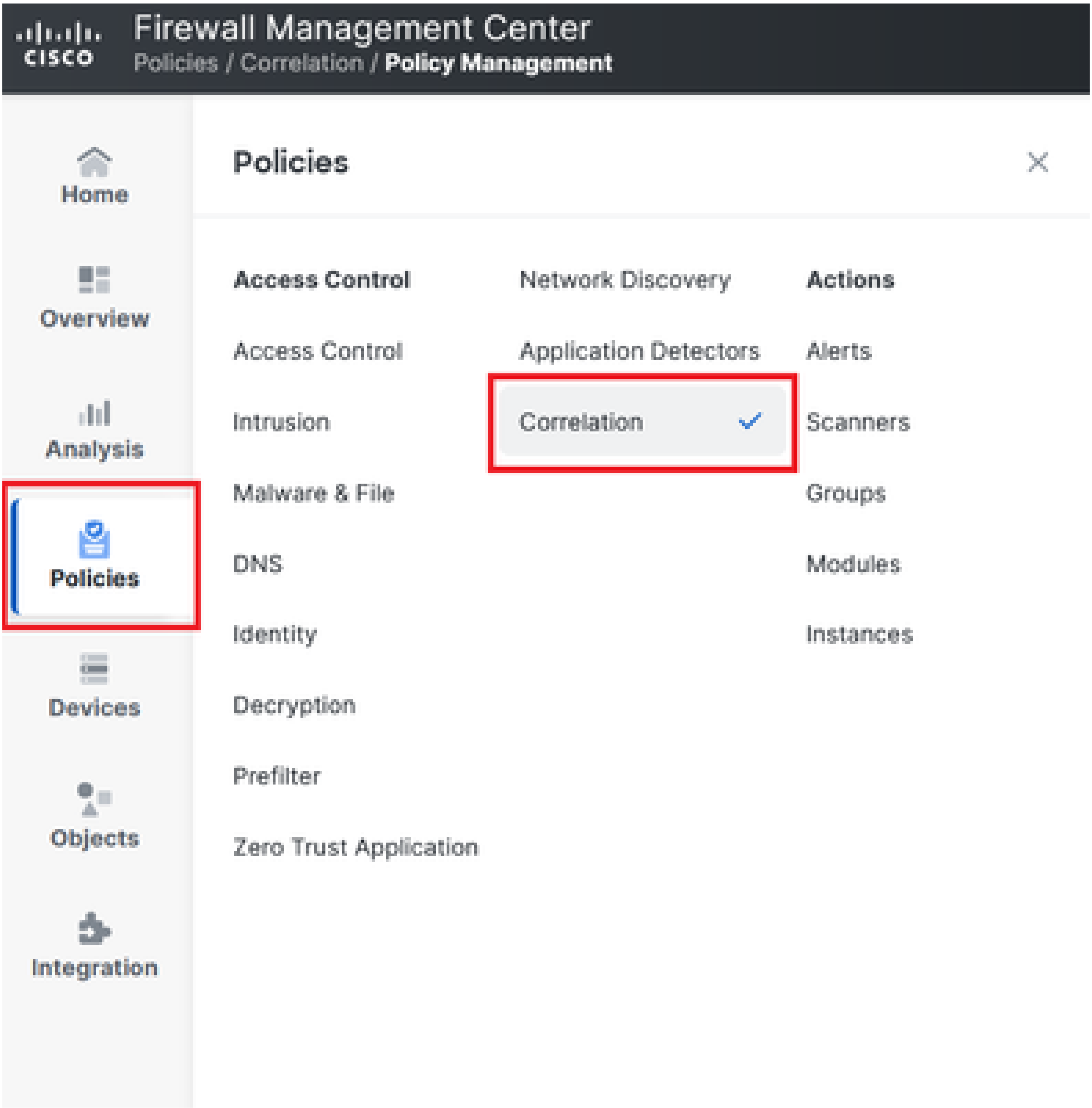
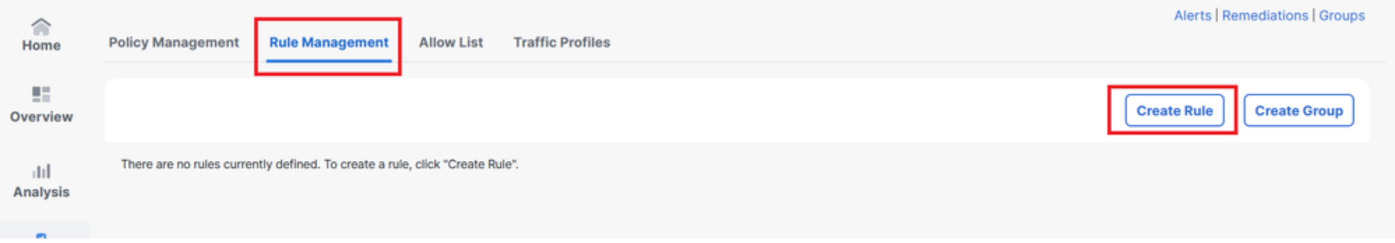


Image 1. Navigation to Correlation Policy Menu

Step 2. Create a new rule by selecting **Create Rule**.

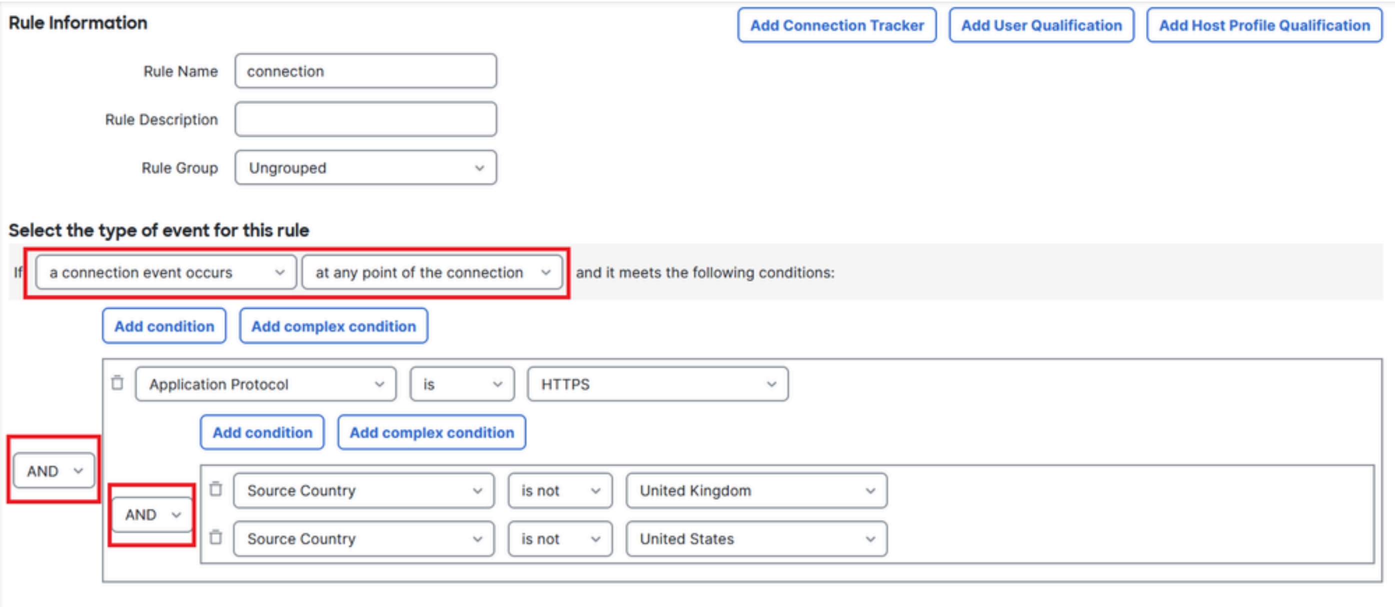


There are no rules currently defined. To create a rule, click "Create Rule".

Image 2. Rule Creation on Rule Management Menu

Step 3. Select an event type and the conditions to match the rule.

When your rule contains multiple conditions, you must link them with **AND** or an **OR** operator.



Rule Information

Rule Name: connection

Rule Description:

Rule Group: Ungrouped

Select the type of event for this rule

If a connection event occurs at any point of the connection and it meets the following conditions:

Application Protocol is HTTPS

AND

Source Country is not United Kingdom

AND

Source Country is not United States

Image 3. Rule Creation Menu

Note: Correlation Rules must not be generic, if the rule is constantly triggered by normal traffic, this can consume additional CPU and affect FMC performance.

Configure Alerts

Step 1. Navigate to **Policies** > **Actions** > **Alerts**.

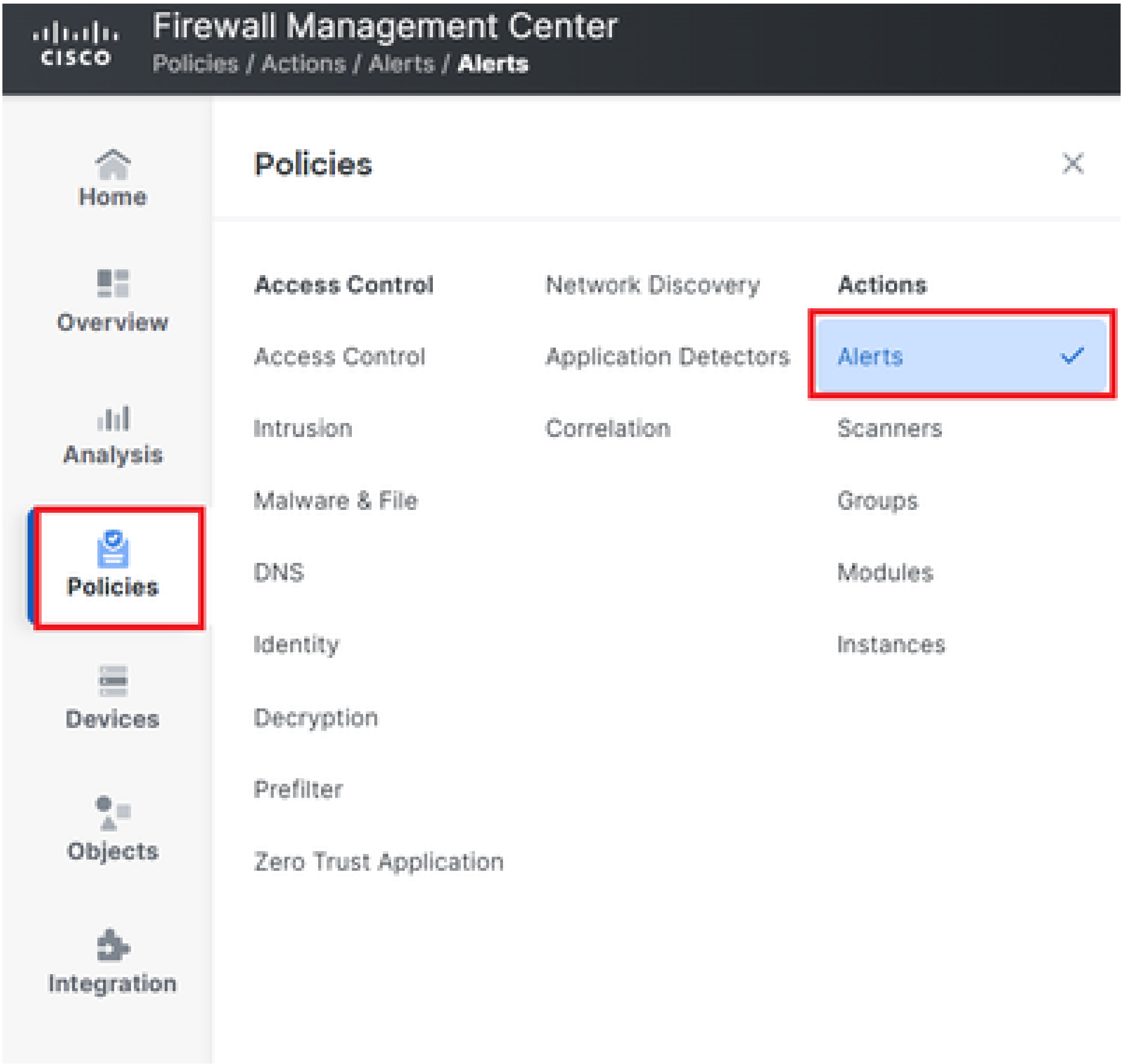
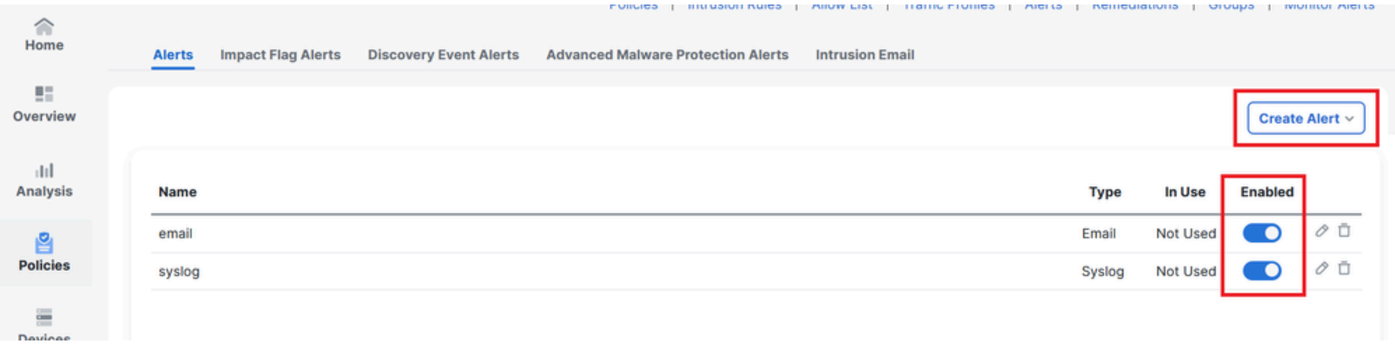


Image 4. Navigation to Alerts Menu

Step 2. Select **Create Alert** and create either a **Syslog**, **SNMP** or **email alert**.


Policies | Intrusion Rules | Allow List | Traffic Profiles | Alerts | Remediations | Groups | Monitor Alerts
Home
Overview
Analysis
Policies
Devices
Alerts
Impact Flag Alerts
Discovery Event Alerts
Advanced Malware Protection Alerts
Intrusion Email
Create Alert

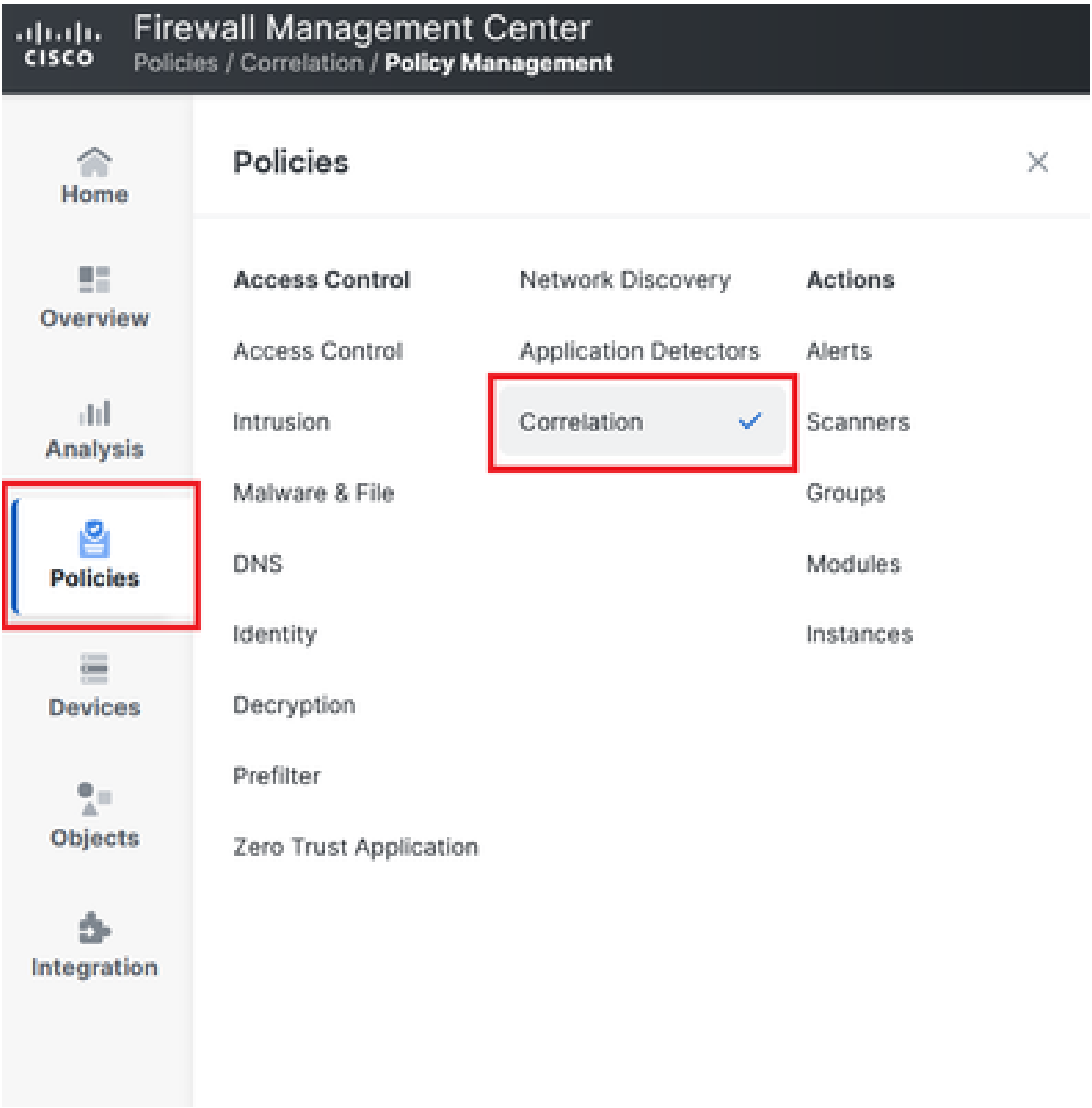
Name	Type	In Use	Enabled
email	Email	Not Used	●
syslog	Syslog	Not Used	●

Image 5. Create Alert

Step 3. Verify the alert is enabled.

Configure Correlation Policy

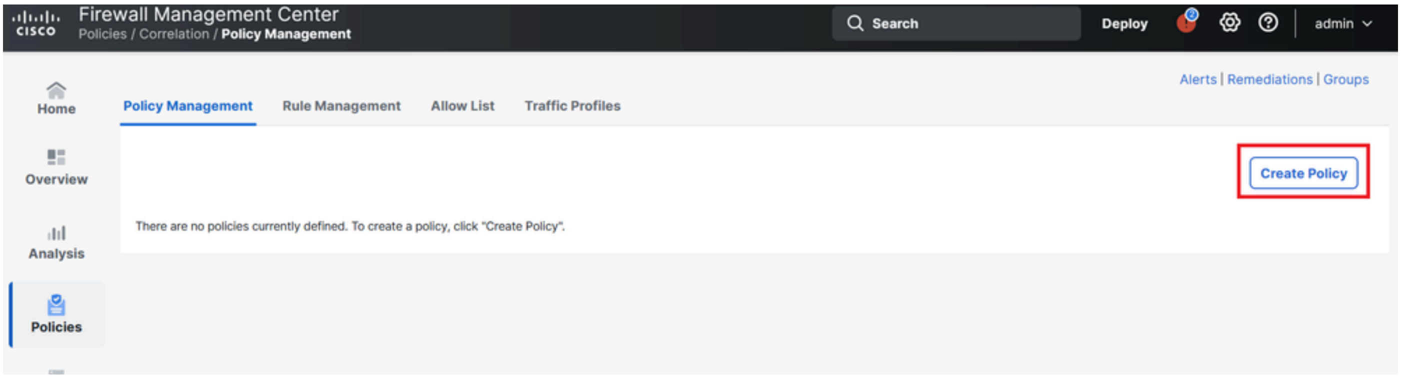
Step 1. Navigate to **Policies** > **Correlation**.



Navigation to Correlation Policy Menu

Image 6. Navigation to Correlation Policy Menu

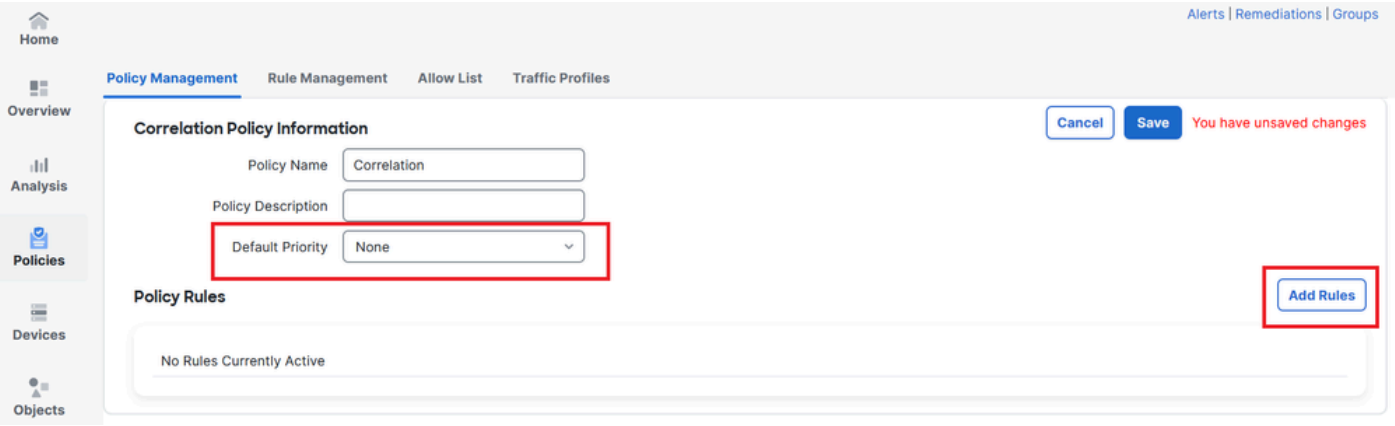
Step 2. Create a new **Correlation Policy**. Select the **default priority**. Use **None** to use the specific rules' priorities.



There are no policies currently defined. To create a policy, click "Create Policy".

Image 7. Create New Correlation Policy

Step 3. Add rules to the policy by selecting **Add Rules**.



Correlation Policy Information

You have unsaved changes

Policy Name: Correlation

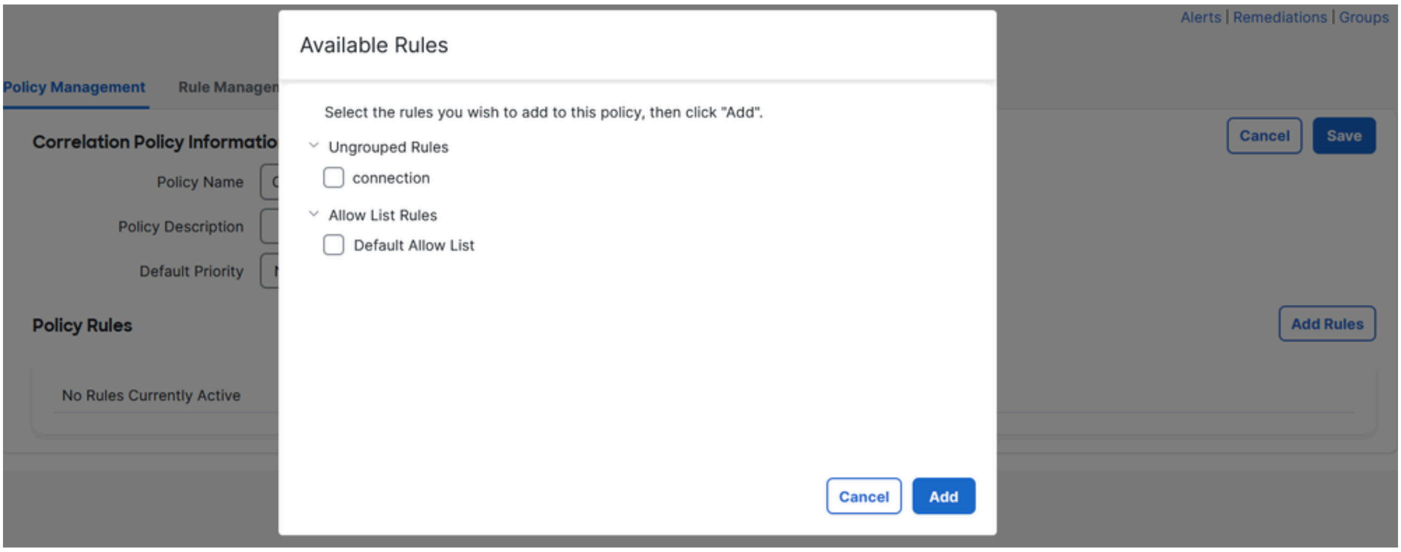
Policy Description:

Default Priority: None

Policy Rules

No Rules Currently Active

Image 8. Add Rules and Select Priority for Correlation Policy



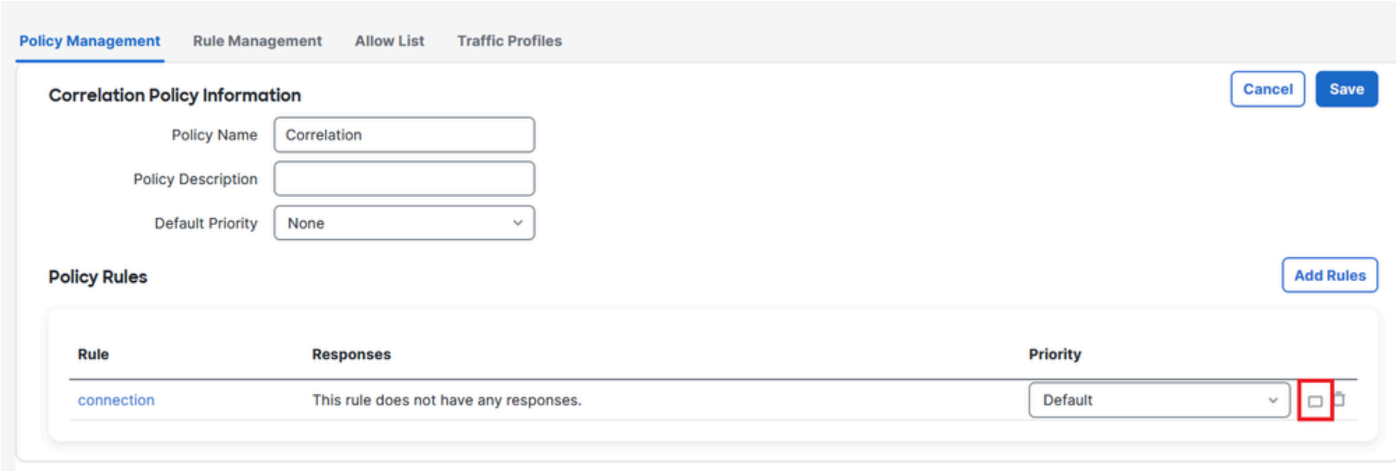
Available Rules

Select the rules you wish to add to this policy, then click "Add".

- Ungrouped Rules
  - □ connection
- Allow List Rules
  - □ Default Allow List

Image 9. Select Rules to Add to the Correlation Policy

Step 4. Assign a **response** to the rule from the alerts you created, so whenever it is triggered, it sends the selected alert type.



Correlation Policy Information

Policy Name: Correlation

Policy Description:

Default Priority: None

Policy Rules

Rule	Responses	Priority
connection	This rule does not have any responses.	Default

Image 10. Add Responses' Button

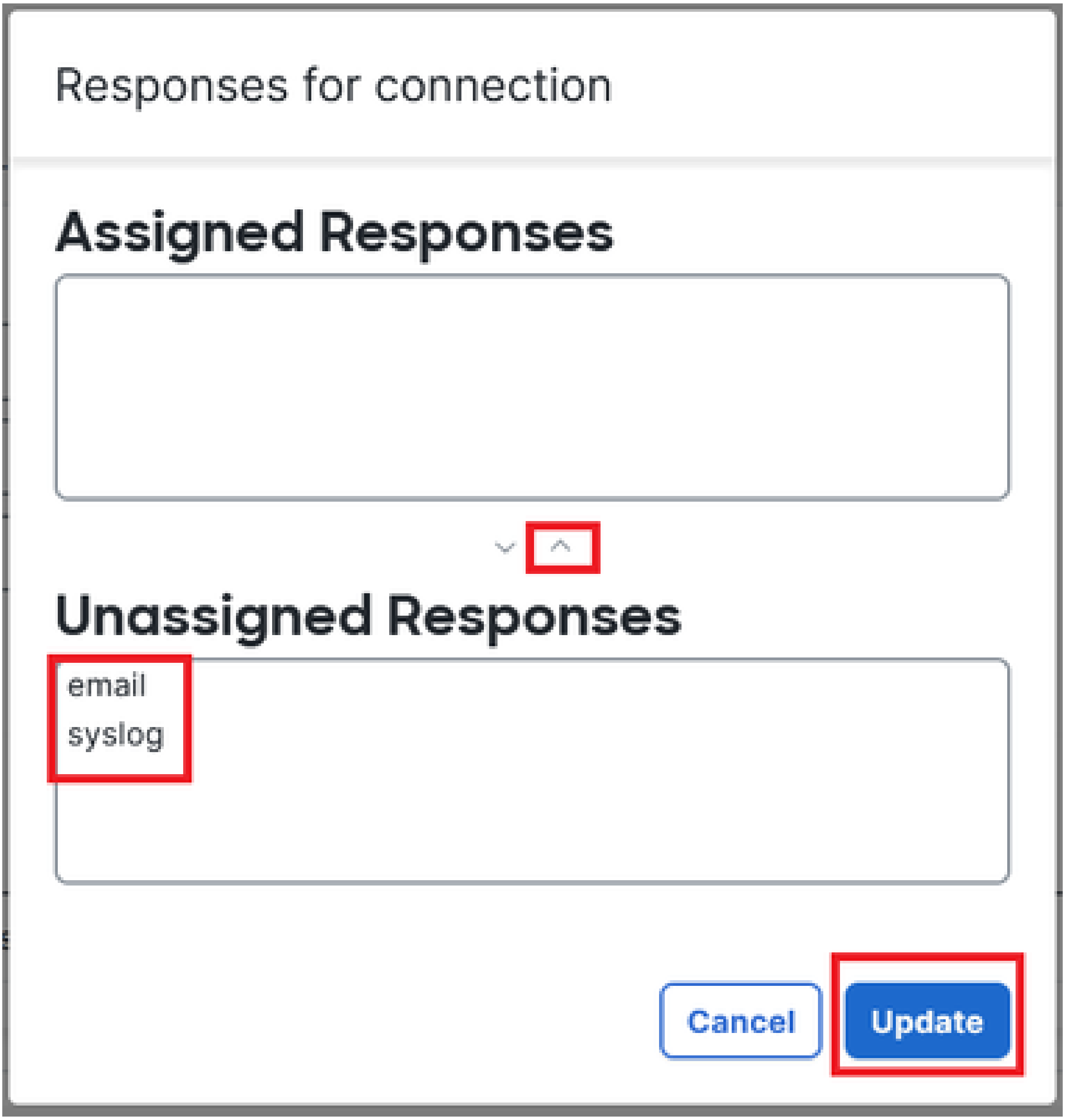
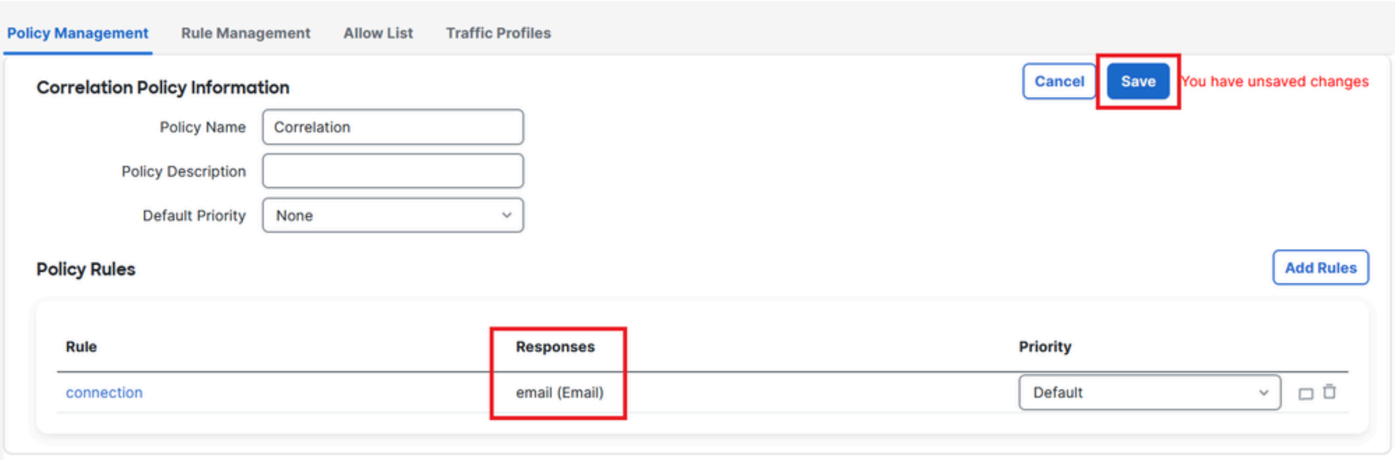


Image 11. Assign Responses to Correlation Rule

Step 5. Save and enable your **Correlation Policy**.



Correlation Policy Information

Policy Name: Correlation

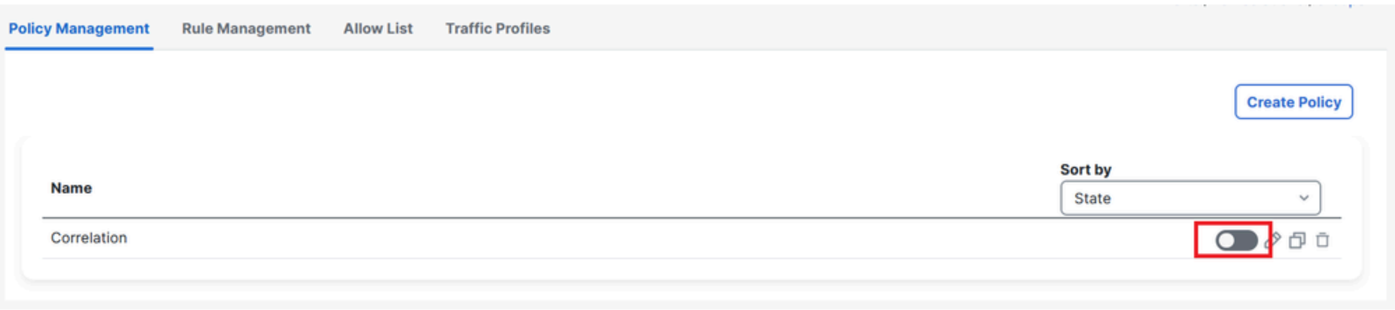
Policy Description:

Default Priority: None

Policy Rules

Rule	Responses	Priority
connection	email (Email)	Default

Image 12. Response Added Correctly to the Correlation Rule



Sort by: State

Name
Correlation

Image 13. Enable Correlation Policy