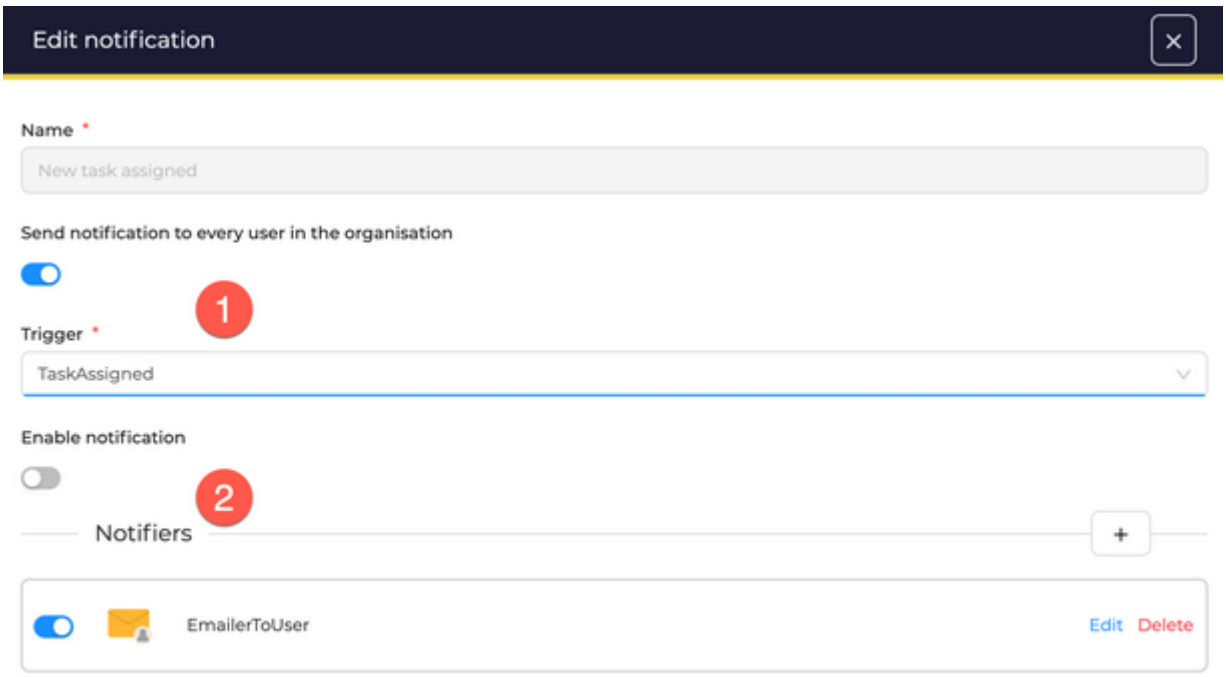
Bildirimler ve Uç Noktalar

Giriş

Bir bildirim şu şekilde tanımlanır:

- Bir Tetikleyici
- Bir veya daha fazla Bildirimci



Tetikleyiciler

Her bildirim yalnızca bir tetikleyiciyle ilişkilendirilir. TheHive, Vakalar, Uyarılar, Görevler, Gözlemlenebilirler ve İşler üzerinde birkaç önceden tanımlanmış tetikleyici ile birlikte gelir. Özel tetikleyiciler de Filtrelenmiş Olay ile tanımlanabilir.

Başka bir tetikleyici, HerhangiBirOlaylar seçildiğinde herhangi bir olayda bildirimleri çalıştırmanıza olanak tanır.

Vakalar için Tetikleyiciler:

- VakaKapatıldı (**CaseClosed**): Bir Vaka kapatıldığında bir eylemi çalıştır
- VakaOluşturuldu (**CaseCreated**): Bir Vaka oluşturulduğunda bir eylemi çalıştır

- VakaPaylaşıldı (**CaseShared**): Bir Vaka paylaşıldığında bir eylemi çalıştır

Uyarılar için Tetikleyiciler:

- UyarıOluşturuldu (**AlertCreated**): Bir Uyarı oluşturulduğunda bir eylemi çalıştır
- UyarıAlındı (**AlertImported**): Bir Uyarı içe aktarıldığında (bir Uyarıdan bir Vaka oluşturulur veya bir Uyarı mevcut bir Vakaya eklenirken) bir eylemi çalıştır

İşler için Tetikleyiciler:

- İşTamamlandı (**JobFinished**): Bir İş başarıyla veya başarısızlıkla sonuçlandığında bir eylemi çalıştır

Gözlemlenebilirler için Tetikleyiciler:

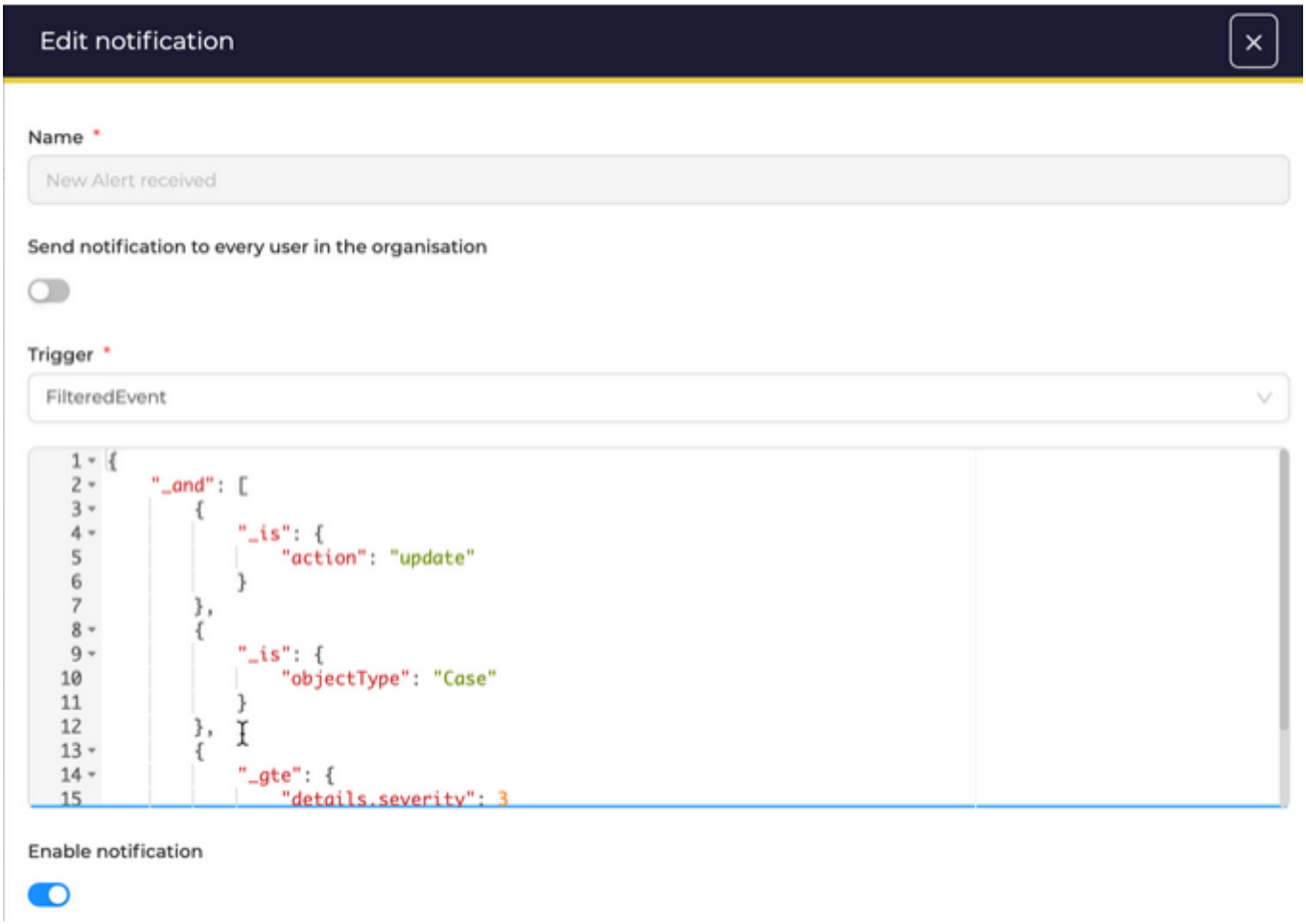
- GözlemOluşturuldu (**ObservableCreated**): Bir Gözlem oluşturulduğunda bir eylemi çalıştır

Görevler için Tetikleyiciler:

- GirişGörevim (**LoginMyTask**): Bir Görevin yeni bir Günlük aldığında bir eylemi çalıştır
- GörevAtandı (**TaskAssigned**): Bir Görev atandığında veya atanmış kişi güncellendiğinde bir eylemi çalıştır
- GörevKapatıldı (**TaskClosed**): Bir Görev kapatıldığında bir eylemi çalıştır

Filtrelenmiş Olay:

Filtrelenmiş Olay seçildiğinde, TheHive, yapılandırılmış bir JSON filtresi yazmanıza izin verir. Bu filtre, uygulamadaki belirli olayları eşleştirmeyi amaçlar ve bildiriciler tarafından tanımlanan bir veya daha fazla eylemi tetikler.



Birbirinden Farklı Bildiriciler

EmailToUser: geçerli Organizasyondaki tüm kullanıcılara bir e-posta gönderir
EmailToAddr : belirli bir e-posta adresine e-posta gönderir
HTTP İsteği: seçilen bir HTTP uç noktasına veri gönderme
Mattermost: seçilen bir Mattermost uç noktasına veri gönderir
Slack: seçilen bir Slack uç noktasına veri gönderme
MS Teams: seçilen bir Microsoft Teams uç noktasına veri gönderme
Webhook: seçilen bir webhook uç noktasına veri gönderme
Kafka: seçilen bir Kafka kuyruğuna veri gönderme
Redis: seçilen bir Redis uç noktasına veri gönderme

Bunlardan ikisi Cortex Analizörleri ve Yanıtlayıcıları çalıştırmak için ayrılmıştır:

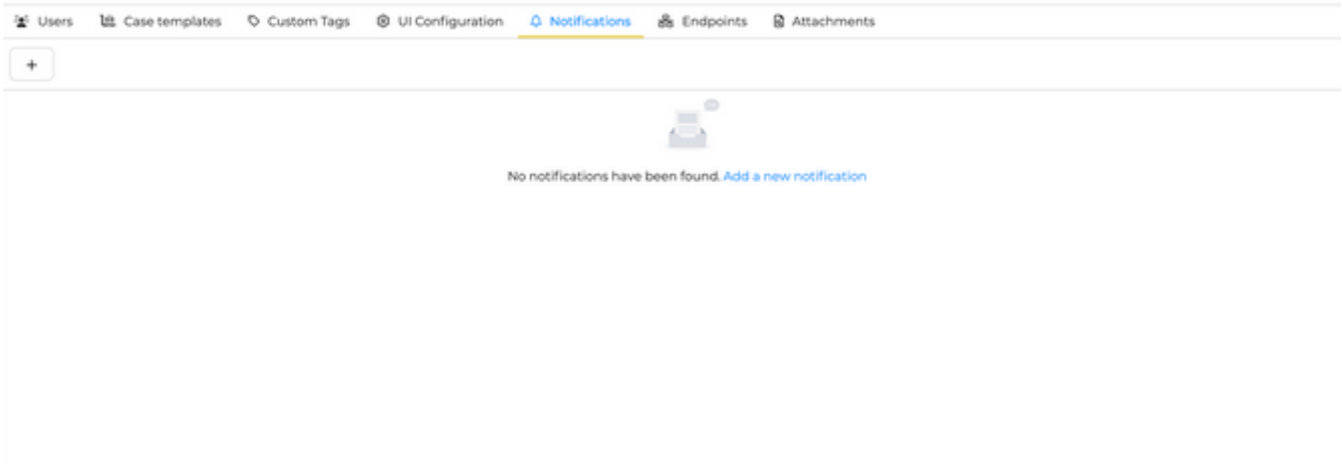
RunAnalyzer: seçili Analizörleri çalıştır
RunResponder: seçili Yanıtlayıcıları çalıştır

Bildirimci Yapılandırması

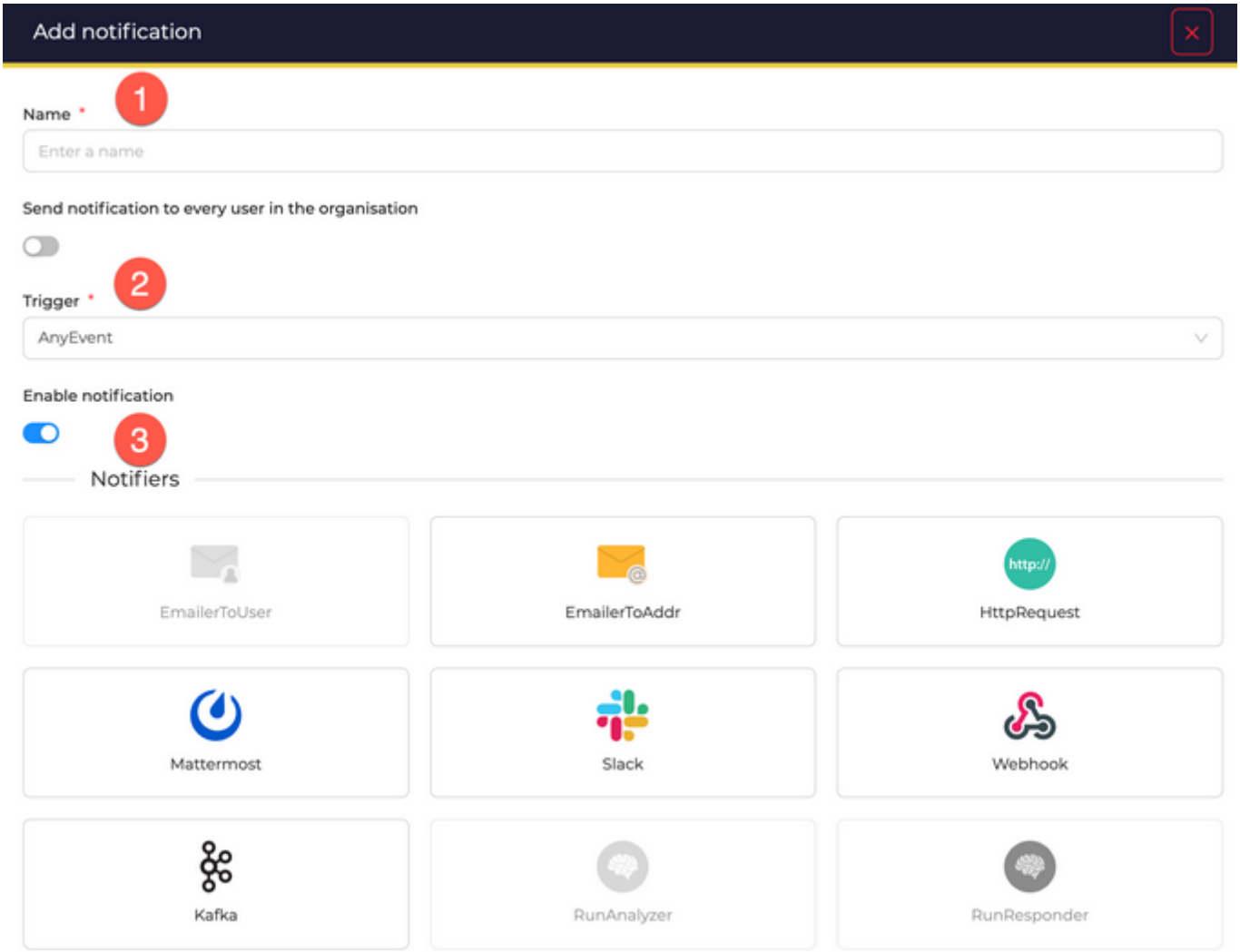
Mattermost Yapılandırması

Bir EnpointOluştur

Organizasyon menüsünü açarak ve Bildirimler sekmesini seçerek Bildirimler listesine erişebilirsiniz.



Bildirim eklemek için "+" düğmesine tıklayın.



Bir bildirim oluşturun:

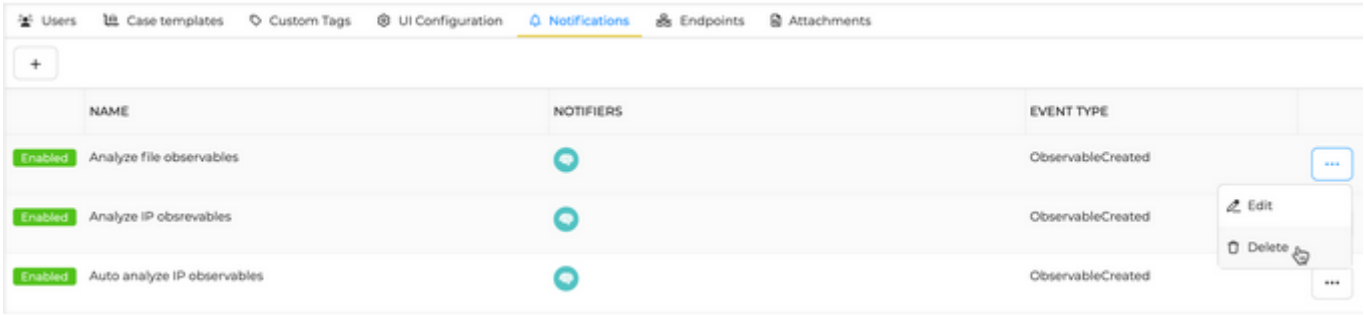
- Bildirime benzersiz bir ad verin
- Bir tetikleyici seçin
- Bir bildirici seçin ve yapılandırın

Daha sonra bildirimi kaydetmek için "Onayla"ya tıklayın.

Bildirimler Üzerinde İşlemler

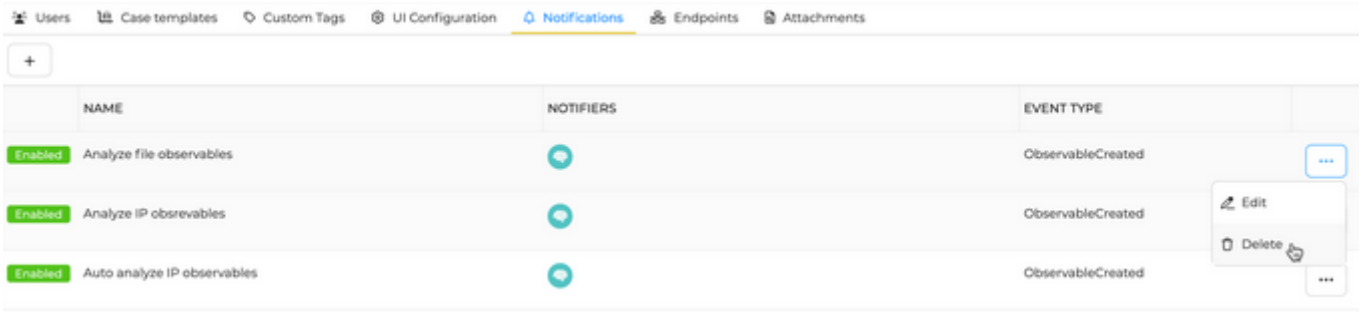
Bir Bildirimi Sil

Bildirim listesinde sil seçeneğine tıklayın:

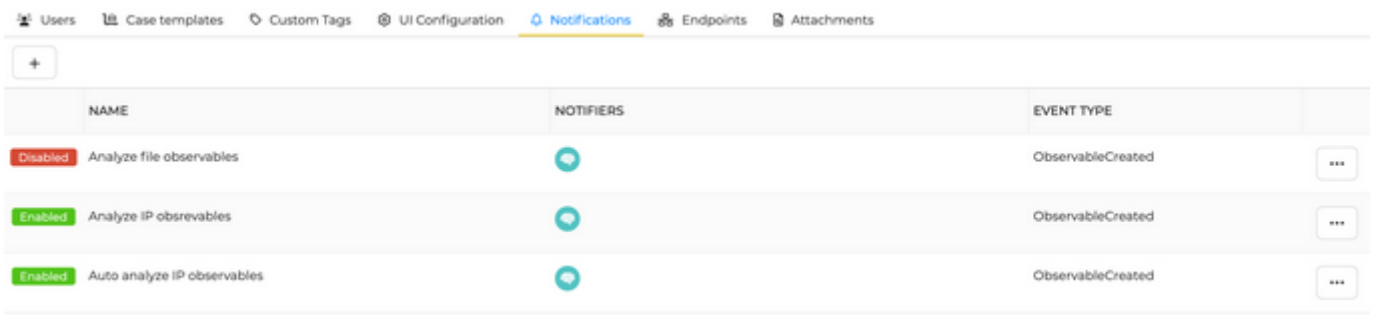


Bir Bildirimi Devre Dışı Bırakma

Bildirimler listesinde, devre dışı bırakmak istediğiniz bildirimi düzenleyin:



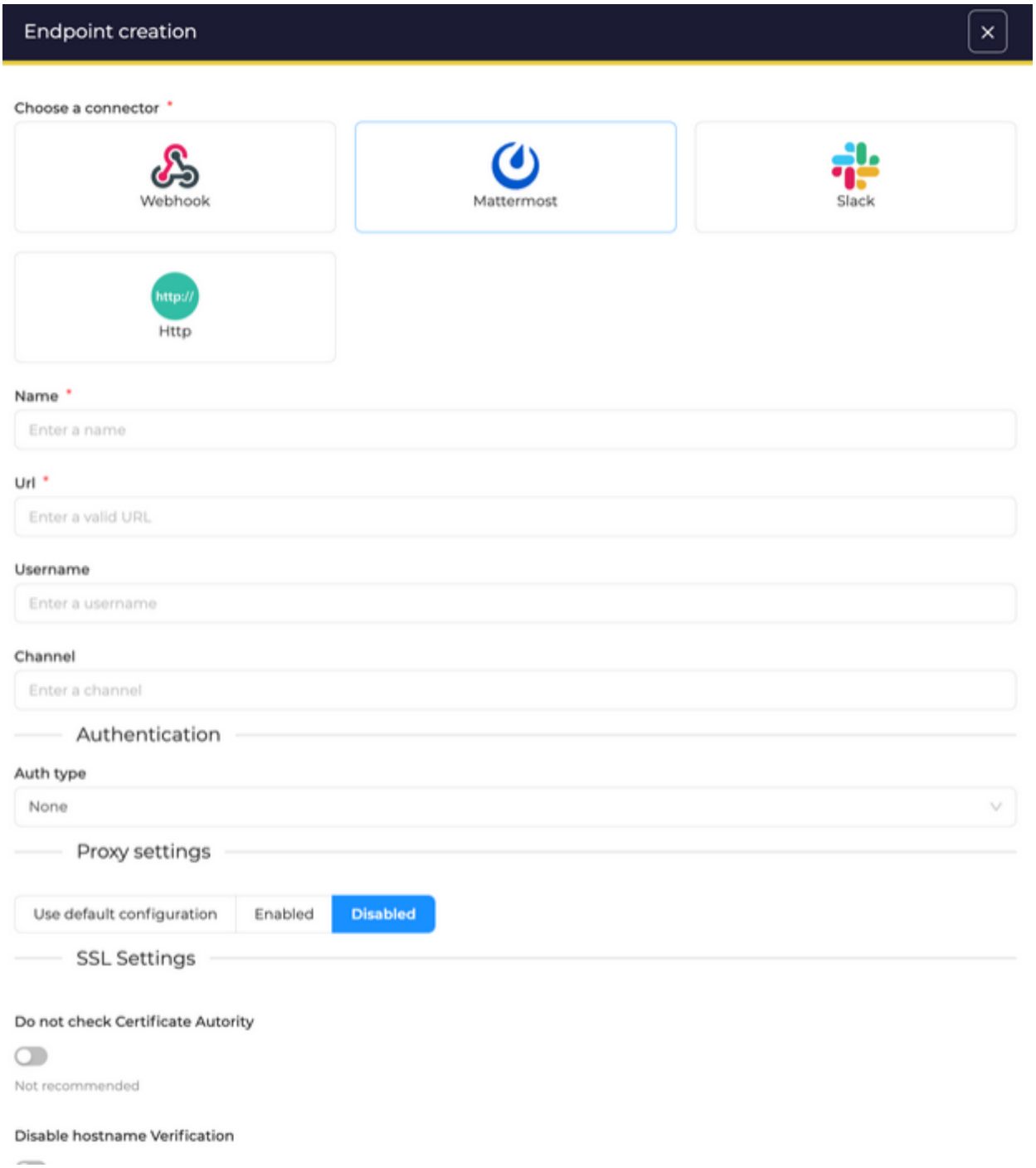
Sonucu Bildirimler listesinde belirtin.



Bildiriciler

Enpoint yapılandırması

Mattermost'u seçin ve gerekli bilgileri doldurun.



Mattermost Uç Noktası Yapılandırması:

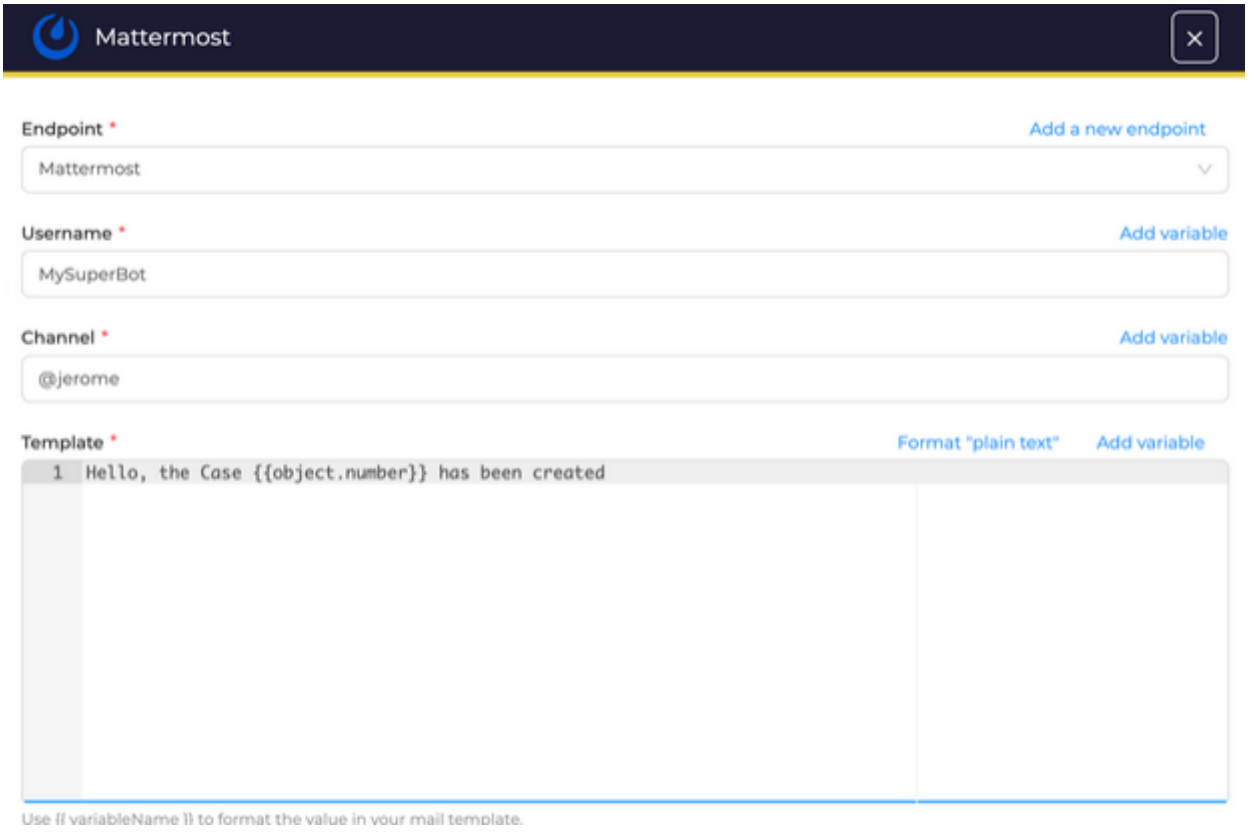
- Ad: Uç noktaya benzersiz bir ad verin
- URL: Mattermost örneğinize bağlanmak için URL'yi belirtin

- Kullanıcı Adı: Veri göndermek için kullanılan varsayılan kullanıcı adı
- Kanal: Veri göndermek için kullanılan varsayılan kanal
- Kimlik Doğrulama Türü: Bu uç noktaya bağlanmak için Temel kimlik doğrulamasını kullanın veya Anahtar veya Taşıyıcı yöntemini kullanın
- Proxy Ayarları: Bu uç noktaya bağlanmak için bir web proxy kullanmayı seçin
- Sertifika Yetkilileri: Gerekirse özel Sertifika Yetkilileri ekleyin (PEM biçiminde)
- SSL Ayarları: Sertifika Yetkilisi kontrolünü devre dışı bırakın ve/veya ana bilgisayar adlarında kontrolleri devre dışı bırakın

Daha sonra, uç noktayı oluşturmak için "Onayla"ya tıklayın.

Bildirim Yapılandırması

Bir Bildirim oluştururken Bildirimci olarak Mattermost'u seçin ve formu doldurun.



Mattermost'u Seçin

TheHive, giriş verileriyle şablonları oluşturmanıza olanak tanımak için Handlebars kullanır, ve bu çoğu form alanında kullanılabilir:

- Uç Nokta: Kullanılacak uç noktayı seçin
- Kullanıcı Adı: Bir kullanıcı adı seçin. Giriş verilerinden bir bilgi kullanmak istiyorsanız, değişken eklemek için tıklayın. Bu, uç noktada yapılandırılmış varsayılan kullanıcı adını geçersiz kılacaktır.

- Kanal: Verilerin gönderileceği Mattermost'taki hedef kanalı seçin. Giriş verilerinden bir bilgi kullanmak istiyorsanız, değişken eklemek için tıklayın. Bu, uç noktada yapılandırılmış varsayılan kanalı geçersiz kılacaktır.
- Şablon:
  - Kullanılabilir formatlar: JSON, Markdown ve Düz metin
  - Şablona eklenecek bir değişken seçmek için Değişken Ekle'ye tıklayın

Daha sonra bu Bildiriciyi kaydetmek için "Onayla"ya tıklayın.

MS Teams Yapılandırması

Microsoft Teams'i Bildirimci olarak kullanmak için en az bir uç nokta oluşturmak gerekir. Bu uç nokta, TheHive'ın MS Teams'e nasıl bağlanacağını tanımlar.

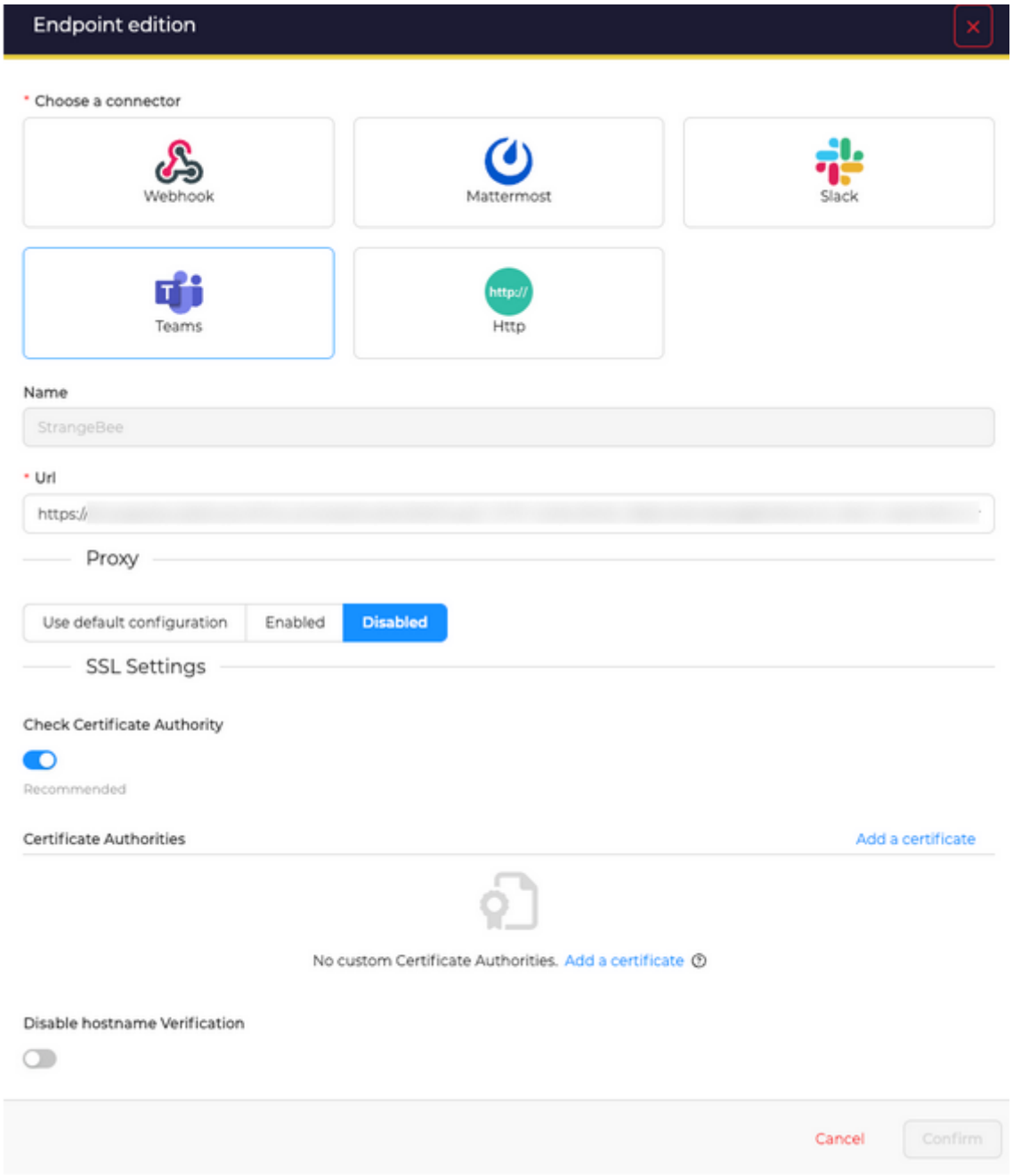
Bir Enpoint oluşturun

Kuruluş yapılandırma görünümünde Uç Noktalar sekmesini açın. Ardından, şuna tıklayın düğmesine basarak yeni bir Bildirici oluşturun.



Enpoint yapılandırması

Takımları seçin ve gerekli bilgileri doldurun.

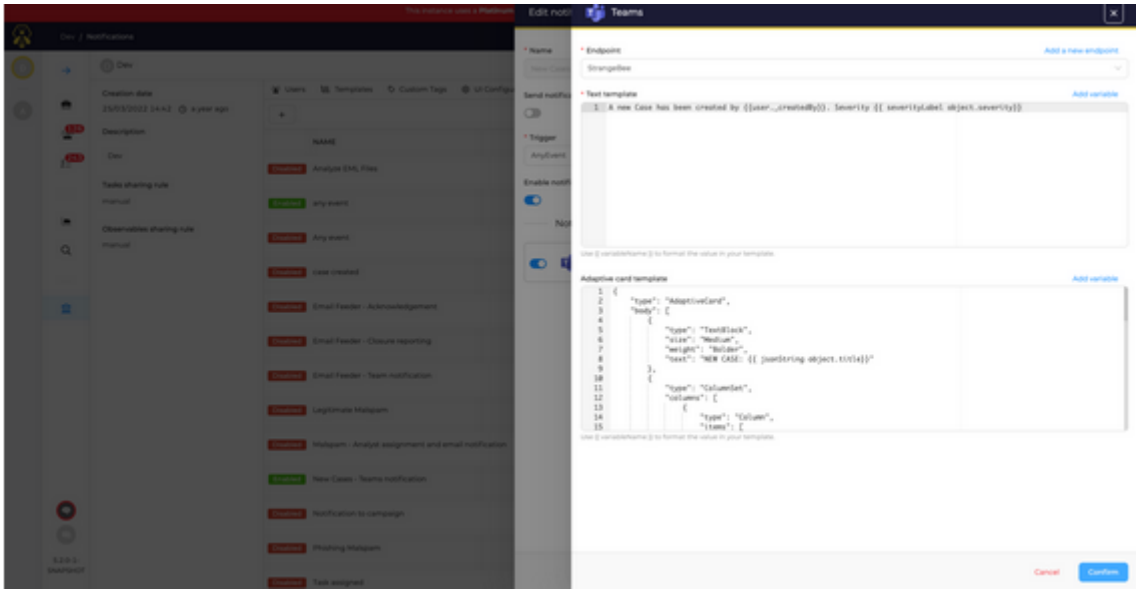


Ad (**Name**:): uç noktaya benzersiz bir ad verin
URL: MS Teams'inize bağlanmak için URL'yi belirtin; Bu, Teams'de gelen web kancası oluşturulurken kopyalanan URL'dir
Kimlik Doğrulama Türü (**Auth Type**): Bu uç noktaya bağlanmak için Temel kimlik doğrulamayı kullanın veya Anahtar veya Taşıyıcı yöntemini kullanın
Proxy ayarları (**Proxy settings**): bu uç noktaya bağlanmak için bir web proxy kullanmayı seçin
Sertifika yetkilileri (**Certificate authorities**): Gerekirse özel Sertifika Yetkilileri ekleyin (PEM biçimi)
SSL ayarları (**SSL settings**): Sertifika Yetkilisi kontrolünü ve/veya ana bilgisayar adları kontrollerini devre dışı bırakın

Ardından, uç noktayı oluşturmak için onayla'ya tıklayın.

Bildirim yapılandırması

Bir Bildirim oluştururken Bildirimci olarak Teams/ENDPOINT (ENDPOINT oluşturulan uç noktanın adı olacak şekilde) öğesini seçin ve formu doldurun.



TheHive, giriş verileriyle şablonlar oluşturmanıza izin vermek için Handlebars kullanır ve bunu formun çoğu alanında kullanabilirsiniz:

- Uç Nokta **(Endpoint):** Kullanılacak uç noktayı seçin
- Metin Şablonu (**Text template**:): Bu zorunludur, hatta bir uyarlanabilir kart şablonu doldurulmuş olsa bile. Bu, özet bölümünde, bildirimlerde kullanılır. Biçim düz metindir.
- Uyarlanabilir Kart Şablonu (**Adaptive card template**:):
  - Mevcut formatlar: JSON, Markdown ve Düz metin
  - Şablon içine eklemek için bir değişken seçmek için "Değişken Ekle"ye tıklayın.

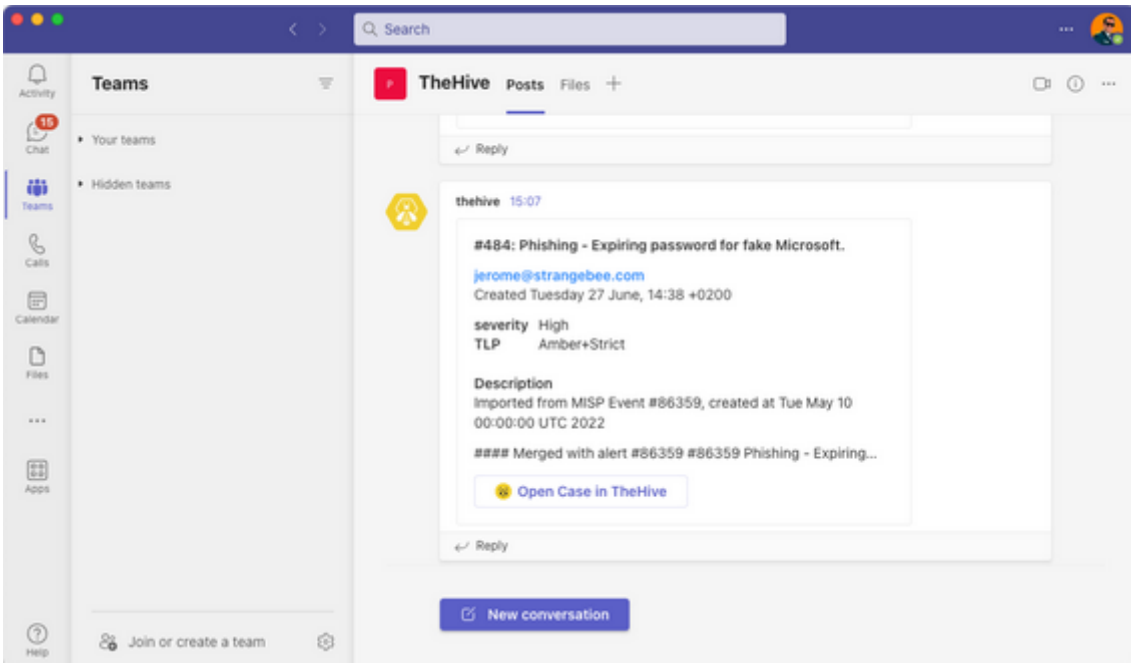
Example: template used to display notification when a new Case is created

```
{
"type": "AdaptiveCard",
"body": [
   {
   "type": "TextBlock",
   "size": "Medium",
   "weight": "Bolder",
   "text": "#{{object.number}}: {{object.title}}",
   "horizontalAlignment": "Left",
   "spacing": "None",
   "wrap": true
   },
```

```
    {
    "type": "ColumnSet",
    "columns": [
        {
        "type": "Column",
        "items": [
            {
            "type": "TextBlock",
            "weight": "Bolder",
            "text": "{{object._createdBy}}",
            "fontType": "Default",
            "color": "Accent",
            "spacing": "None"
            },
            {
            "type": "TextBlock",
            "spacing": "None",
            "text": "Created {{dateFormat object._createdAt "EEEE d MMMM, k:m Z" locale="en"
tz="Europe/Paris"}}",
            "isSubtle": true,
            "wrap": true,
            "fontType": "Default",
            "weight": "Default",
            "size": "Default"
            }
        ]
        }
    ]
    },
    {
    "type": "FactSet",
    "facts": [
        {
        "title": "severity",
        "weight": "Bolder",
        "value": "{{ severityLabel object.severity}}"
        },
        {
        "title": "TLP",
        "weight": "Bolder",
```

```
        "value": "{{ tlpLabel object.tlp}}"
        }
    ]
    },
    {
    "type": "TextBlock",
    "weight": "Bolder",
    "text": "Description",
    "spacing": "Large",
    "wrap": true,
    "horizontalAlignment": "Left"
    },
    {
    "type": "TextBlock",
    "text": "{{object.description}}",
    "spacing": "None",
    "wrap": true,
    "horizontalAlignment": "Left",
    "maxLines": 3
    }
],
"actions": [
    {
    "type": "Action.OpenUrl",
    "title": "Open Case in TheHive",
    "iconUrl": "https://docs.strangebee.com/images/thehive.png",
    "url": "{{url}}",
    "style": "positive"
    }
],
"$schema": "http://adaptivecards.io/schemas/adaptive-card.json",
"version": "1.5"
}
```

Oluşturulan tetikleyici Case ile birlikte kullanıldığında, bu şablon Microsoft Teams'de buna benzer bir kart oluşturacaktır:



İpuçları
MS Teams aktif Kartlarını yazın#

Uyarlanabilir kartınızı tasarlamak için başlangıç noktası olarak https://adaptivecards.io/designer/ adresini kullanın
Tarihleri biçimlendir#

TheHive, tarihleri okumak için işleyici çubukları dize yardımcılarını kullanır
Bildirimlerde tarih ve saati biçimlendirmek için özel Java kalıplarının kullanılması gerekir

TheHive#'dan diğer özel verileri biçimlendirme

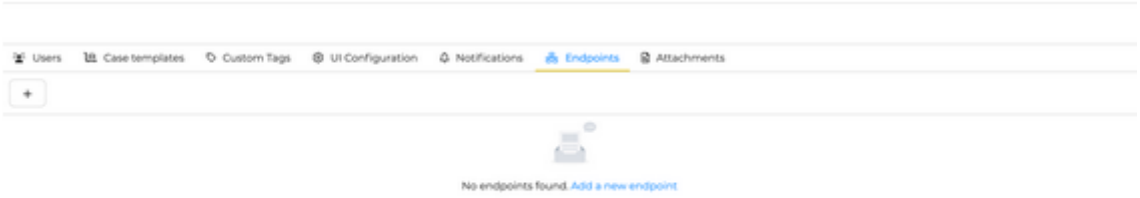
TheHive'a özel birkaç veri, bildirimlerdeki nesne verileriyle birlikte özel dize işleyicileri kullanılarak düzgün bir şekilde görüntülenebilir:

TLP değerini görüntülemek için tlpLabel (örnek: {{tlpLabel object.tlp}})
PAP değerini görüntülemek için papLabel (örnek: {{papLabel object.pap}})
şiddet değerini görüntülemek için severityLabel (örnek: {{severityLabel object.severity}})

Slack kanallarına bildirim gönderme

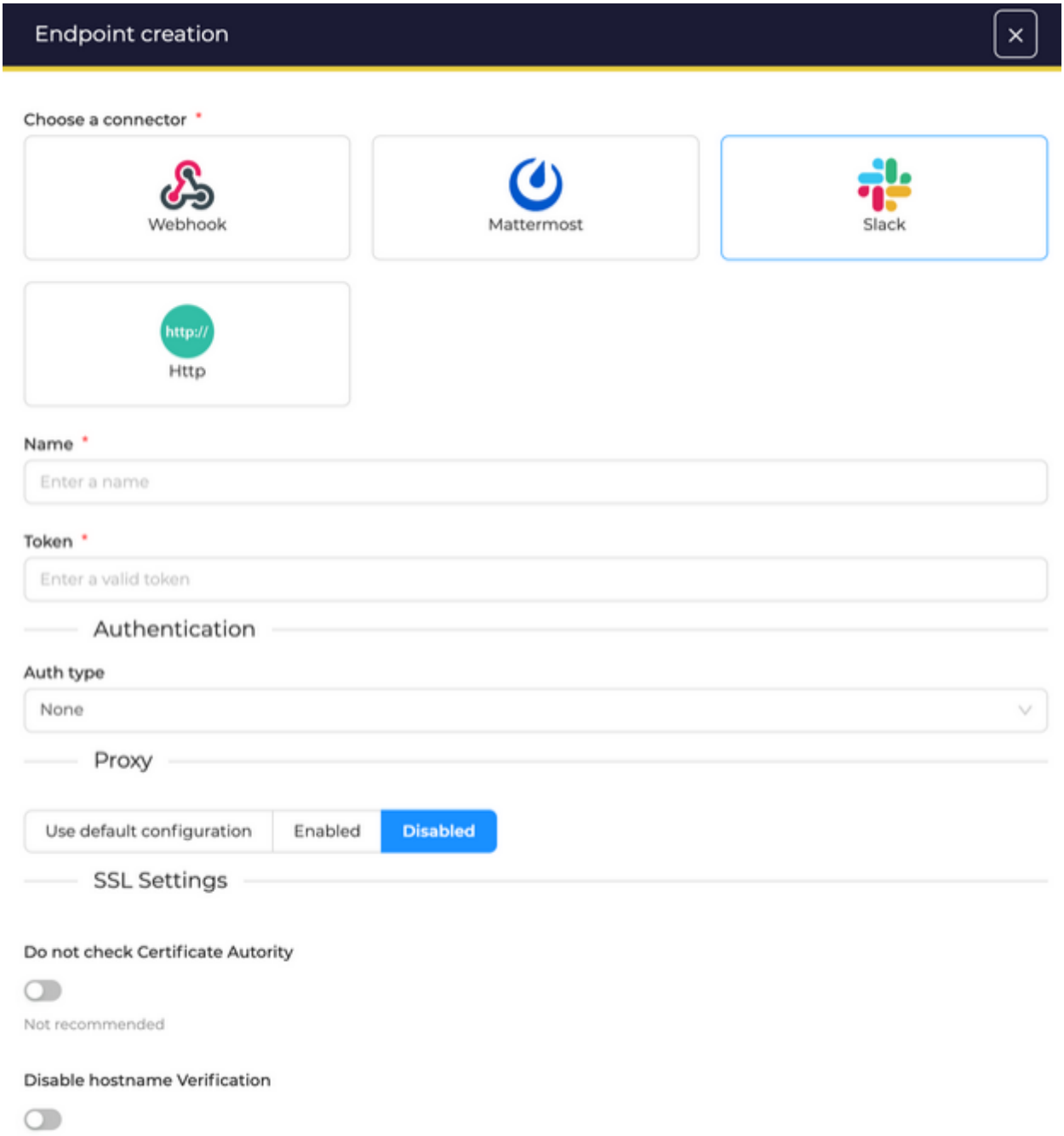
Slack kanallarına bildirim göndermek için TheHive'da en az bir uç nokta oluşturmanız gerekmektedir. Bu uç nokta, TheHive'in Slack'e nasıl bağlanacağını tanımlar. Uç nokta oluşturun#

Organizasyon yapılandırma görünümünde, Uç Noktaları sekmesini açın. Ardından, yeni bir Bildirim Oluşturucu oluşturmak için "+" düğmesine tıklayın.



Enpoint yapılandırması

Slack'i seçin ve gerekli bilgileri doldurun.



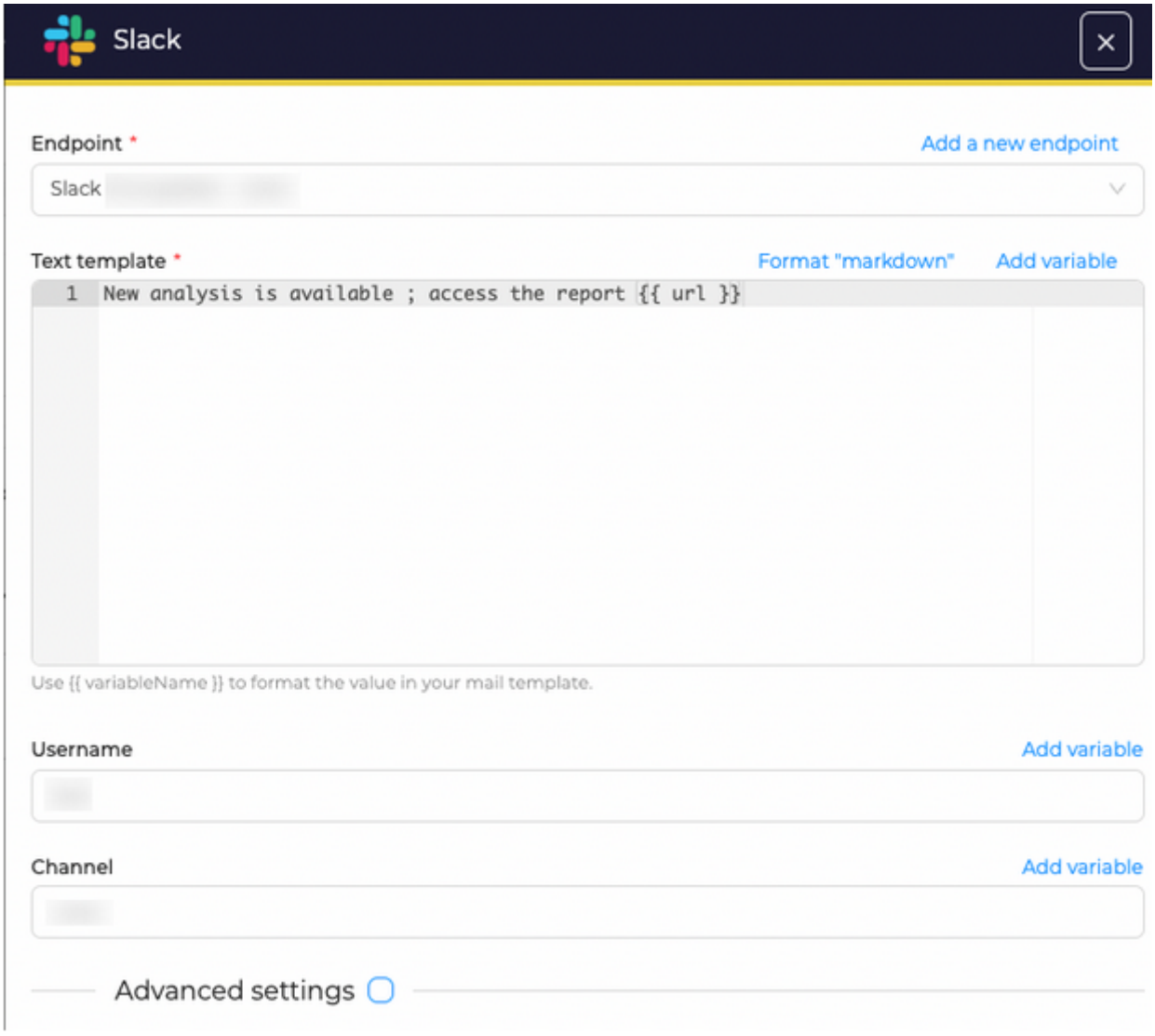
- Ad: uç noktaya benzersiz bir ad verin
- Belirteç: hizmete bağlanmak için kullanılacak belirteci belirtin

- Kimlik Doğrulama Türü: Bu uç noktaya bağlanmak için Temel kimlik doğrulamayı kullanın veya Anahtar veya Taşıyıcı yöntemini kullanın
- Proxy ayarları: bu uç noktaya bağlanmak için bir web proxy kullanmayı seçin
- Sertifika yetkilileri: Gerekirse özel Sertifika Yetkilileri ekleyin (PEM biçimi)
- SSL ayarları: Sertifika Yetkilisi kontrolünü ve/veya ana bilgisayar adları kontrollerini devre dışı bırakın

Ardından, uç noktayı oluşturmak için onayla'ya tıklayın.

Bildirim yapılandırması

Bir Bildirim oluştururken Bildirimci olarak Slack'i seçin ve formu doldurun.



Slack'i seçin

TheHive, girdi verileriyle şablonlar oluşturmanıza izin vermek için Handlebars'ı kullanır ve bu, çoğu form alanında kullanılabilir:

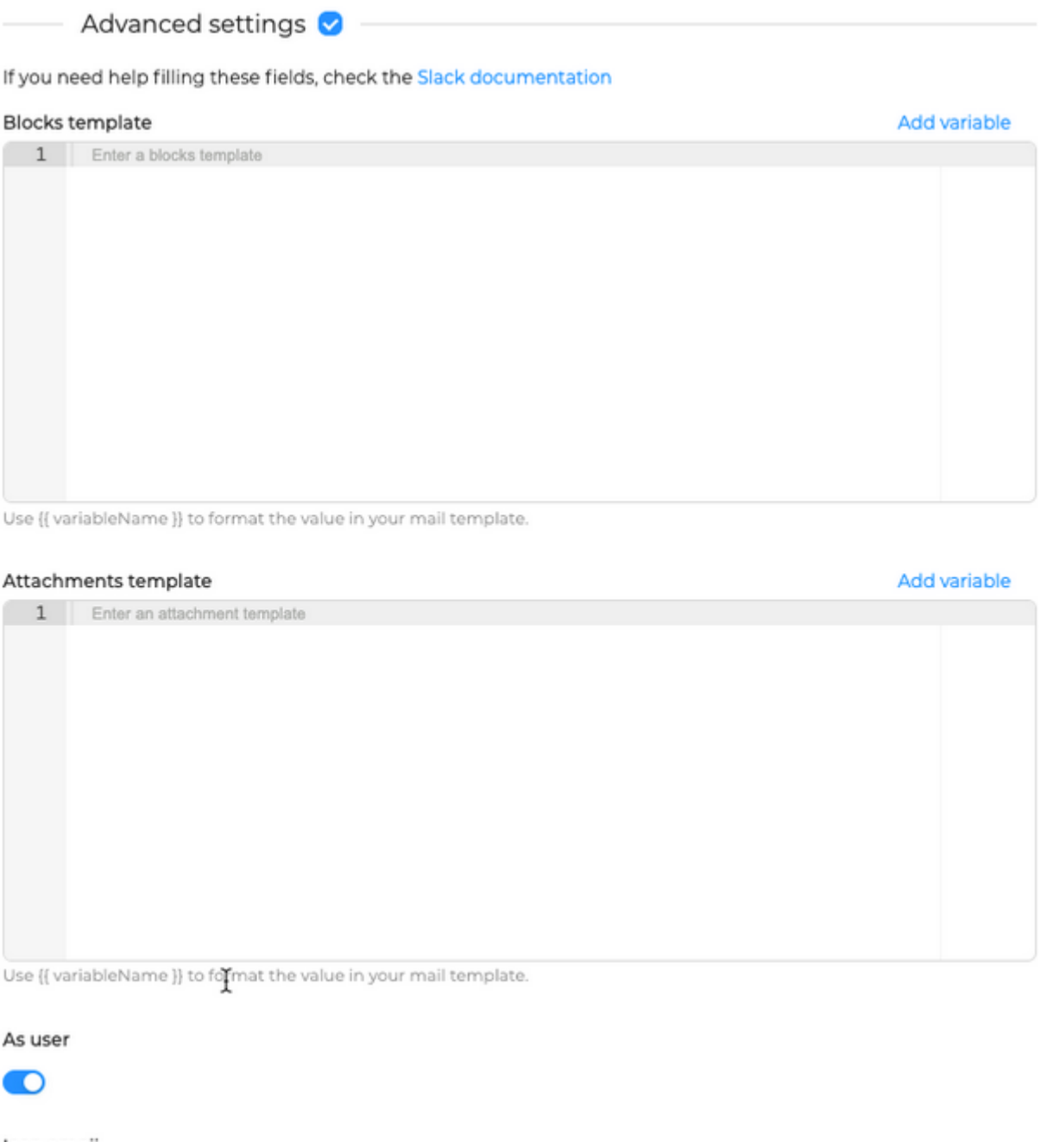
- Bitiş noktası: kullanılacak bitiş noktasını seçin

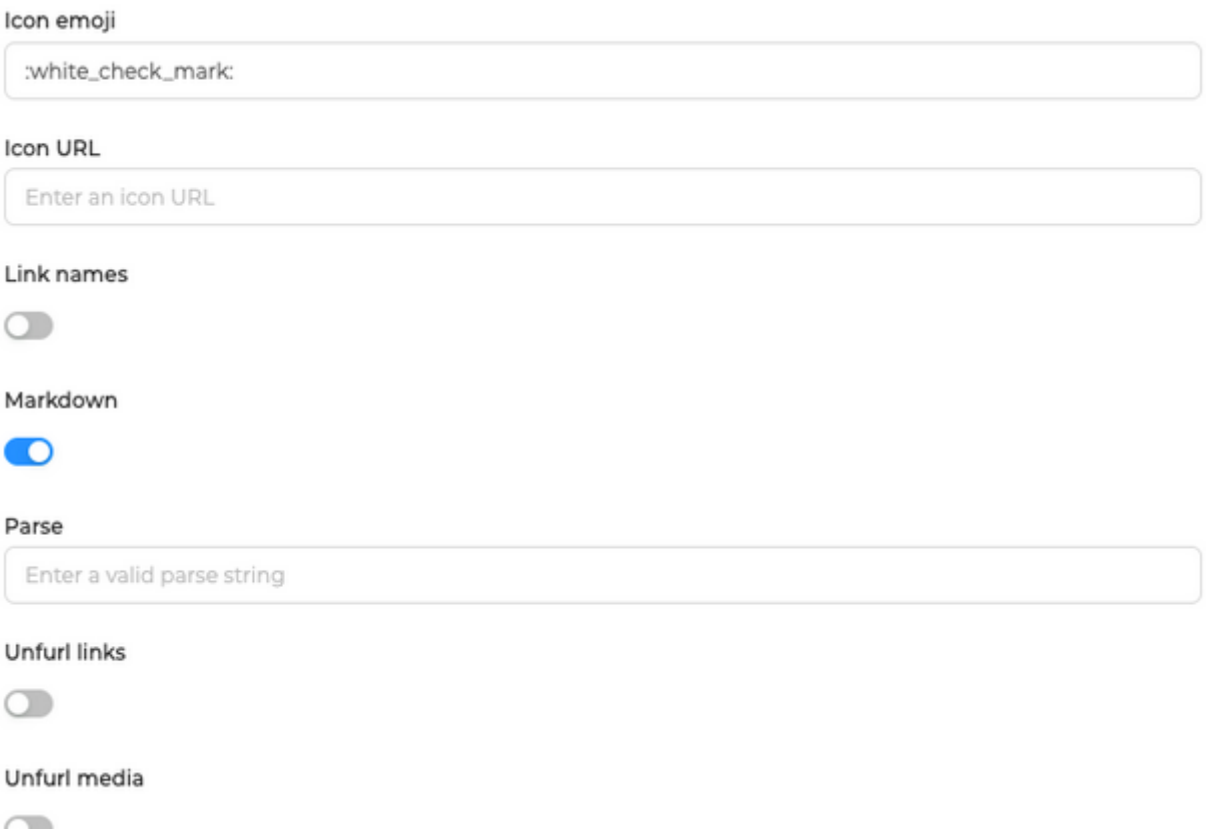
- Kullanıcı adı: bir kullanıcı adı seçin. Giriş verilerinden bir bilgi kullanmak istiyorsanız değişken ekle seçeneğine tıklayın. Bu, uç noktada yapılandırılan varsayılan kullanıcı adını geçersiz kılacaktır
- Kanal: Slack'te veri gönderilecek hedef kanalı seçin. Giriş verilerinden bir bilgi kullanmak istiyorsanız değişken ekle seçeneğine tıklayın. Bu, uç noktada yapılandırılan varsayılan kanalı geçersiz kılacaktır
- Şablon: * Mevcut formatlar şunlardır: JSON, Markdown ve Düz metin
  Şablona eklenecek bir değişken seçmek için Değişken ekle'ye tıklayın

Ardından bu Bildiriciyi kaydetmek için onayla'ya tıklayın.

Gelişmiş ayarlar

Slack entegrasyonu ile birlikte çeşitli yapılandırma seçenekleri gelir.





Örnekler

Blok şablonu örneği: vaka oluşturma hakkında bildirim gönderme

- Tetikleyici: CaseCreated
- Bildirici: Slack

```
[
  {
    "type": "section",
    "text": {
      "type": "mrkdwn",
      "text": "*New Case created: Case #{{object.number}}*"
    }
  },
  {
    "type": "divider"
  },
  {
    "type": "section",
    "text": {
      "type": "mrkdwn",
      "text": "<{{url}}|{{object.title}}> \n :bee: \n {{object.description}}"
```

```
    }
  },
  {
    "type": "section",
    "fields": [
      {
        "type": "mrkdwn",
        "text": "*Created by*\n{{object._createdBy}}\n*Assigned to*\n{{object.assignee}}"
      }
    ]
  }
]
```

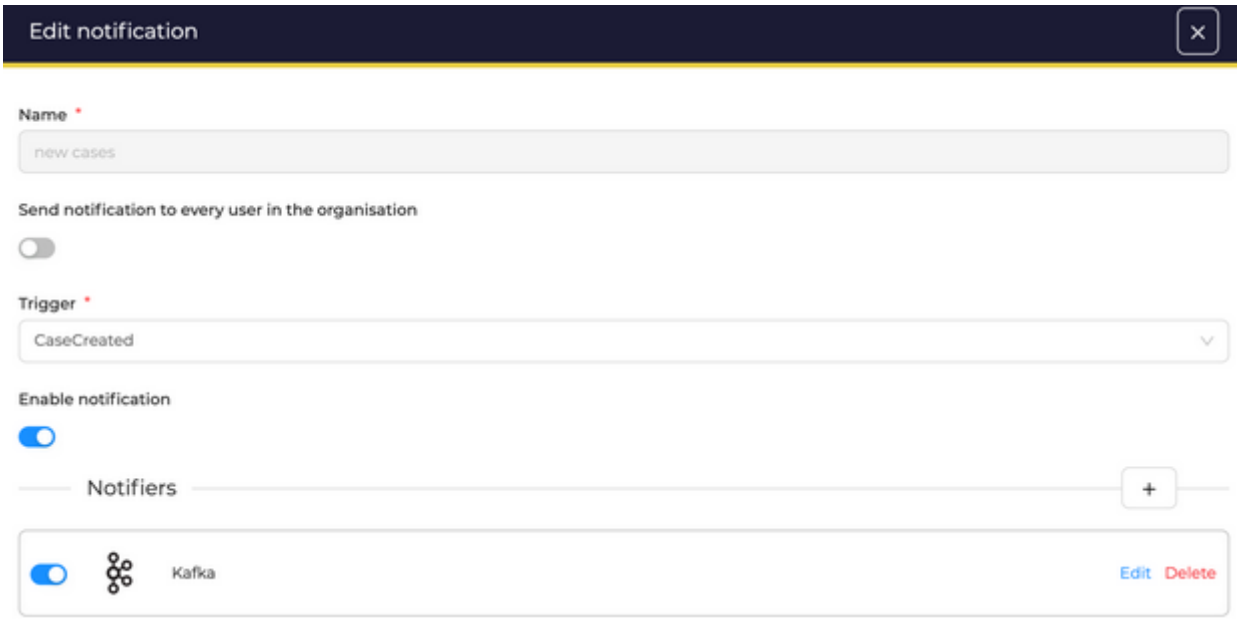
Kafka'ya bildirim gönderme

Yapılandırma

- Bir Bildirim oluştururken Bildirimci olarak Kafka'yı seçin ve formu doldurun:
- Kafka'da kullanılan Konu
- Bağlanılacak IP adresi/homstname ve port



Daha sonra, diğer bildirimcileri eklemek için+ düğmesine tıklayın veya Bildirimi oluşturmak için onaylamak için Onayla'ya tıklayın.



Revision #10
Created 9 April 2024 18:34:39 by Güldeniz Akca
Updated 14 April 2024 23:33:29 by Güldeniz Akca