MISP

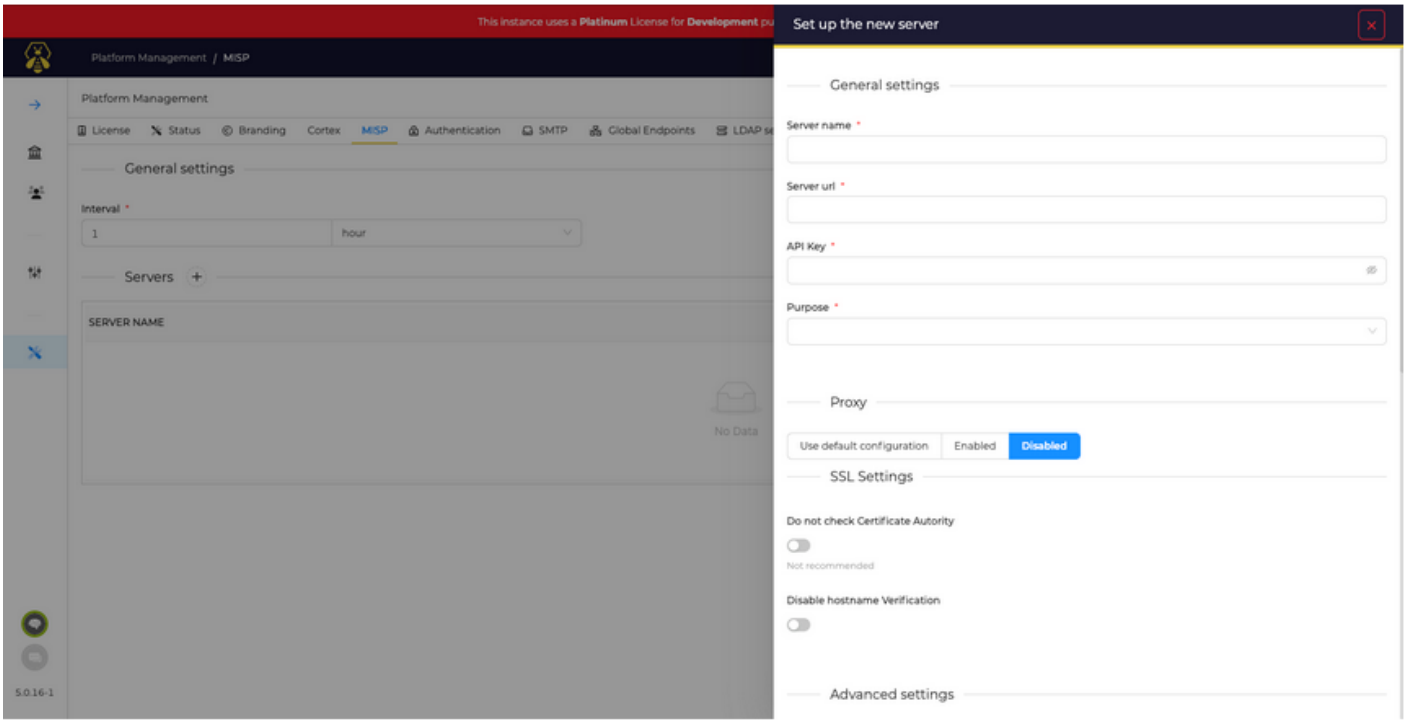
Giriş

> Bir bağlantı tanımlamak için MISP sunucusunda bir hesap ve bir API anahtarı gereklidir.

- Bir veya daha fazla MISP örneği TheHive'a bağlanabilir.
- Her biri için:
- MISP etkinlikleri, TheHive'da Uyarılar olarak içe aktarılabilir. İçe aktarılan etkinlikleri hassaslaştırmak için bir filtre seti kullanılabilir.
- Bir Vaka'da IOC olarak işaretlenmiş Gözlemlenebilirler, MISP'te yeni bir etkinlik olarak dışa aktarılabilir.

MISP bağlantılarını yönetme

Yeni bir MISP sunucusu ekleyin

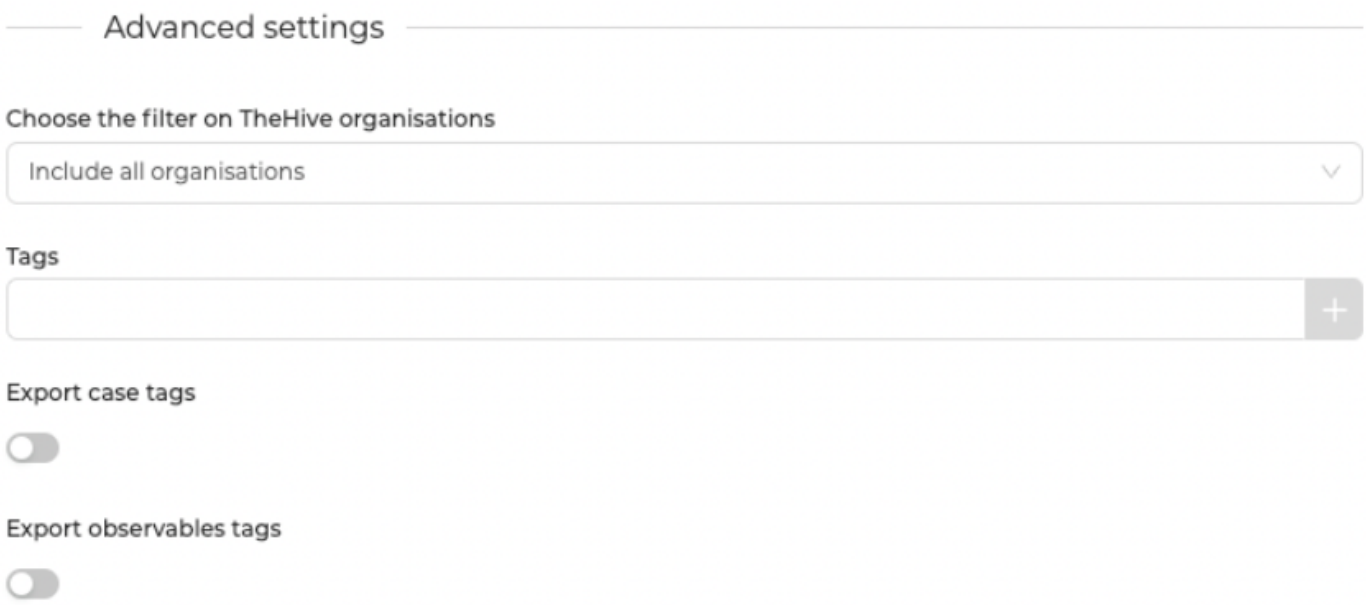


Bağlantı için şunları belirtin:

- Bu bağlantı için bir isim, örneğin: misp1
- Bağlanılacak MISP sunucusunun URL'si, örneğin: https://misp.mycompany.com
- Ayrılmış MISP hesabının API anahtarı

- Bu bağlantının amacı: Yalnızca İçe Aktar, Yalnızca Dışa Aktar veya İçe Aktar ve Dışa Aktar
- TheHive'in MISP ile bağlantı kurması için gerekiyorsa Proxy ayarları

Gelişmiş Ayarlar



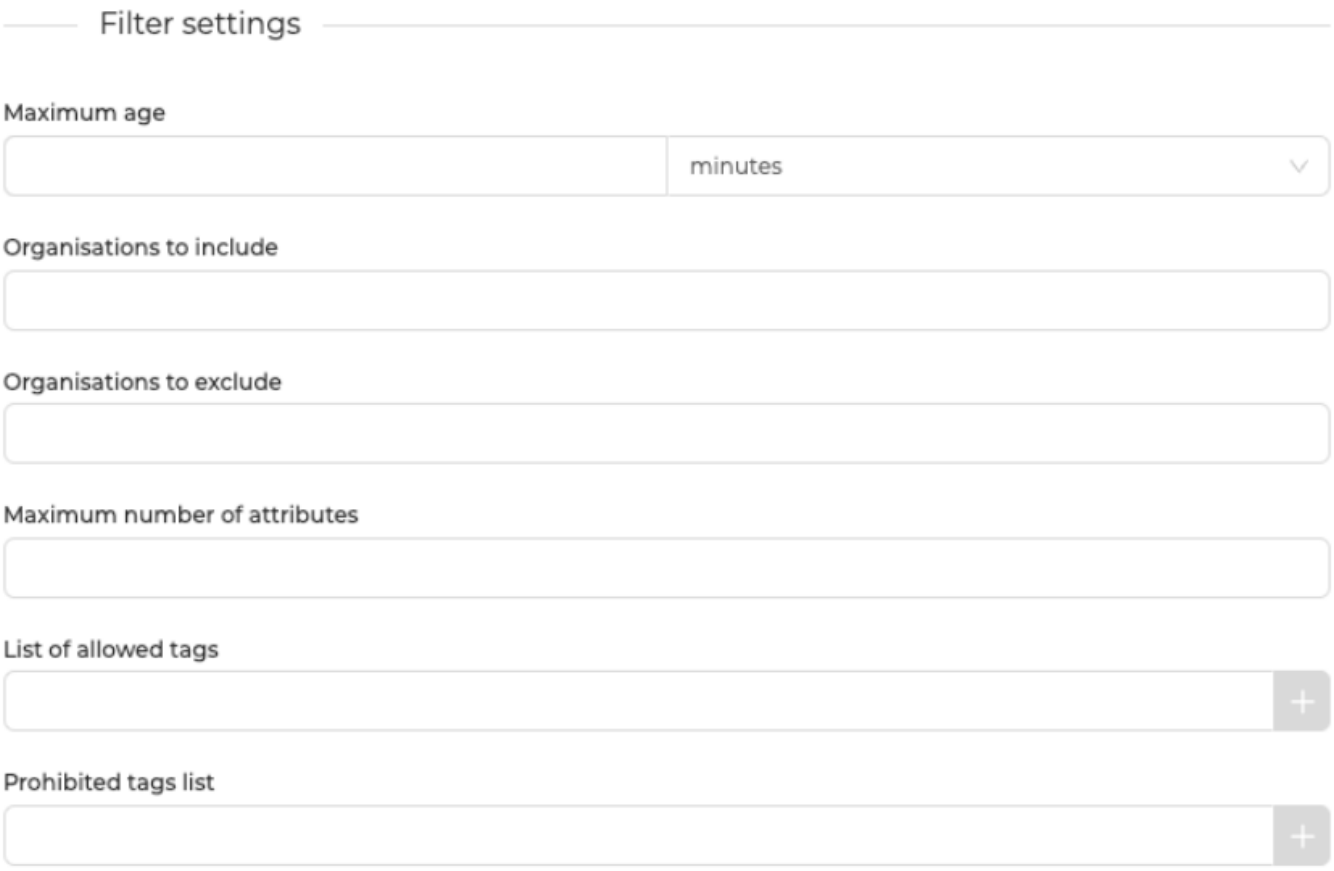
Varsayılan olarak, TheHive'daki tüm organizasyonlar bu bağlantıdan faydalanır. Ek olarak, 2 seçenek daha bulunmaktadır:

- Bu bağlantıyı yalnızca TheHive'daki mevcut organizasyonların bir alt kümesine kullanılabilir hale getirin.
- Bu bağlantıyı TheHive'daki mevcut organizasyonların bir alt kümesine kullanılamaz hale getirin.

Ek seçenekler size şunları sağlar:

- MISP etkinliklerini içe aktardığınızda Uyarılara eklenen etiketleri tanımlayın
- IOC'leri MISP'te dışa aktardığınızda, yeni MISP etkinliğinde Vakadaki gözlemlenebilirlerden gelen etiketleri de dışa aktarın
- IOC'leri MISP'te dışa aktardığınızda, gözlemlenebilirlerden gelen etiketleri de dışa aktarın

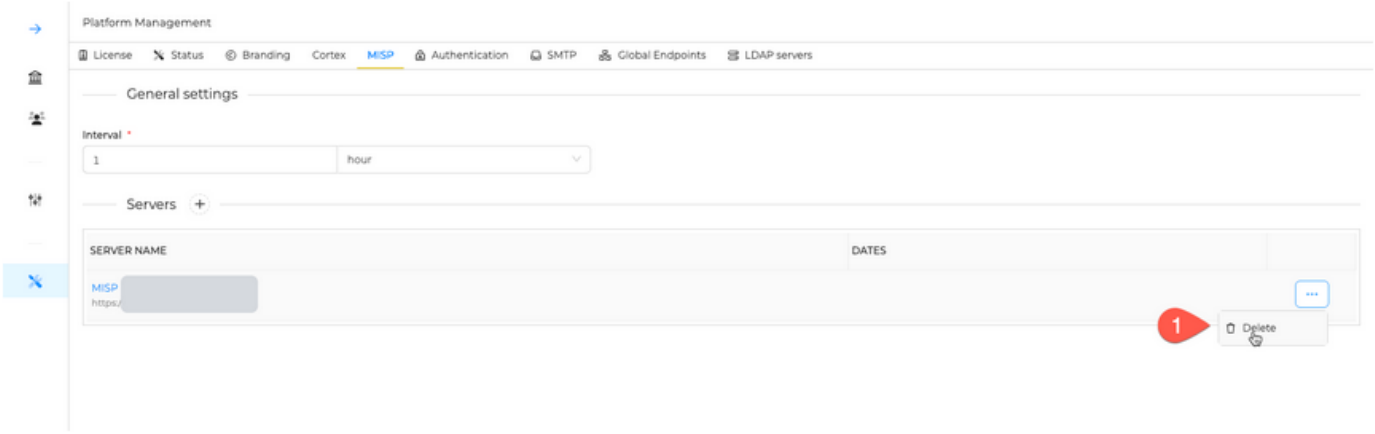
Filtreler



MISP etkinliklerini TheHive Uyarıları olarak içe aktardığınızda, birkaç seçenek mevcuttur:

- İçe aktarılmasına izin verilen bir MISP etkinliğinin maksimum yaşını belirleyin
- İçe aktarılmasına izin verilen MISP etkinliklerinin sahibi olan organizasyonların bir listesini belirtin
- İçe aktarılmasına izin verilmeyen MISP etkinliklerinin sahibi olan organizasyonların bir listesini belirtin
- İçe aktarılması için MISP etkinliğine dahil edilecek gözlemlenebilirlerin (~ özniteliklerin) bir limitini belirleyin
- İçe aktarılması için MISP etkinliğinde bulunması gereken etiketlerin bir listesini belirtin
- İçe aktarılması için MISP etkinliğinde bulunması gereken etiketlerin bir listesini belirtin ve bunu görmezden gelin

Bir Bağlantıyı Sil



Revision #4
Created 8 April 2024 19:47:36 by Güldeniz Akca
Updated 13 April 2024 15:09:59 by Güldeniz Akca