Cortex

Varsayılan olarak, TheHive hiçbir Cortex sunucusuna bağlı değildir.

TheHive'i Cortex'e bağlayın ve Gözlemlenebilirler hakkında bilgi ve istihbarat toplamak için Analizörlerden yararlanın, ayrıca Aksiyonları etkinleştirerek ağınızda veya üçüncü taraf hizmetlerinde(TheHive ve Cortex'in dışında gelen ve bu platformlarla entegre olarak çalışabilen diğer yazılım veya servisler) işlemler çalıştırın.

Giriş

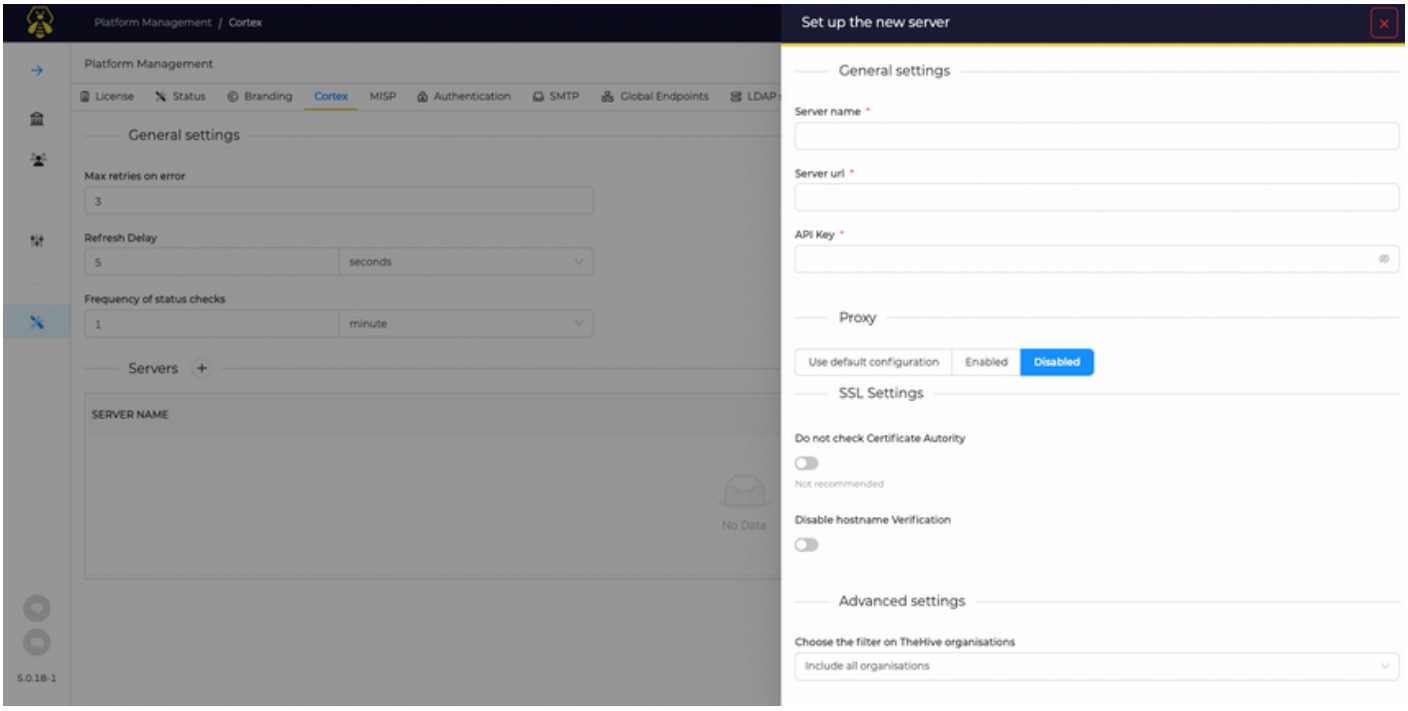
> Bir bağlantı tanımlamak için bir Cortex sunucusunda bir hesap ve bir API anahtarı gereklidir.

- Gözlemlenebilirler üzerinde ayrıntılar, bağlamsal bilgi, istihbarat elde etmek için Analizörler başlatılabilir.
- Yanıtlayıcılar, Araştırma ve Olay Yanıtı sırasında etkin işlemleri çalıştırmak için Vaka, Görevler, Gözlemlenebilirler, görev Günlükleri ve Uyarılar üzerinde başlatılabilir.

Bir veya daha fazla Cortex örneği TheHive'e bağlanabilir.

Cortex Bağlantılarını Yönetme

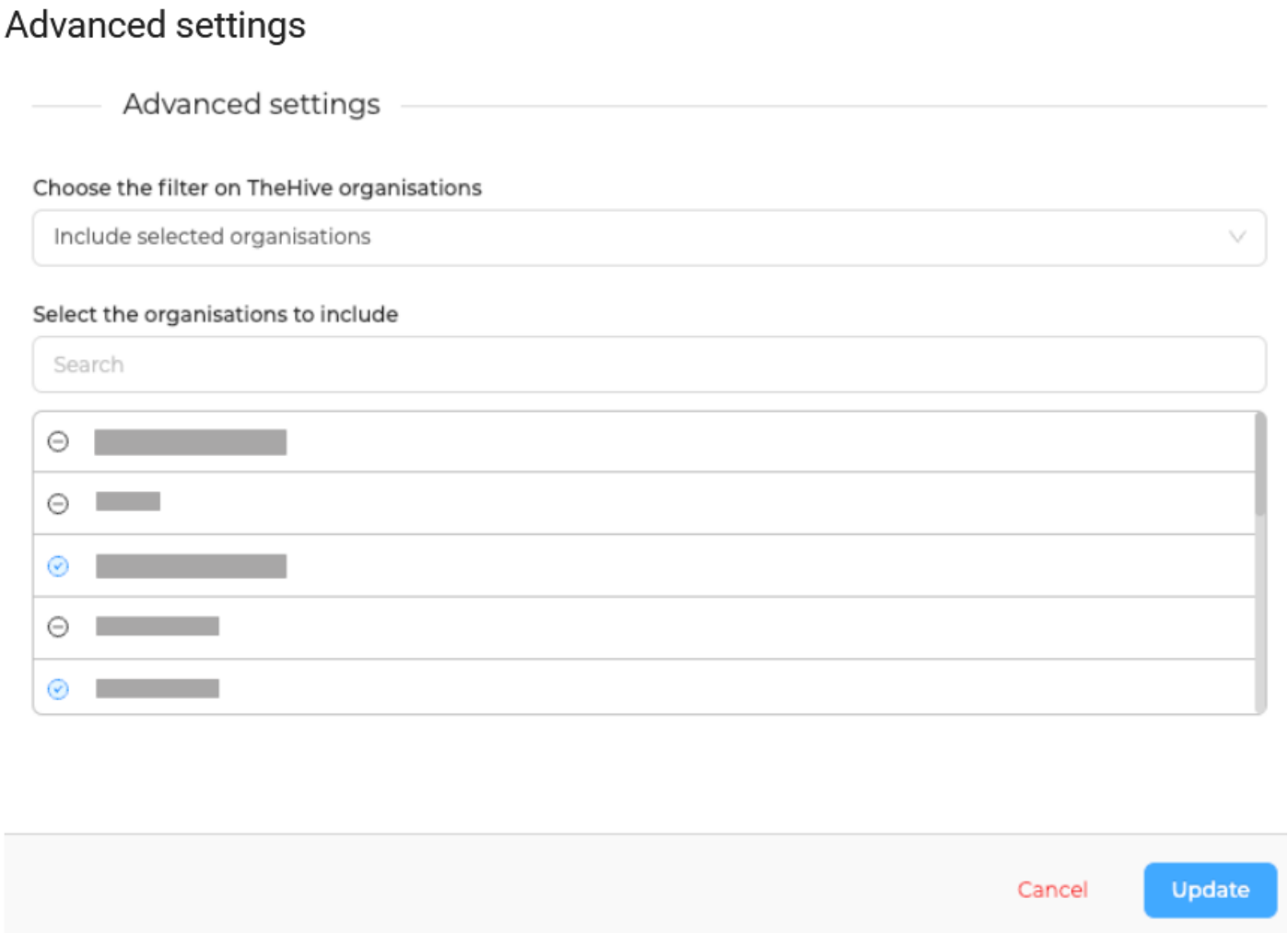
Yeni Bir Cortex Sunucusu Ekleyin



Cortex bağlantısını belirtin:

- Bu bağlantı için bir isim, örneğin: Cortex1
- Bağlanılacak Cortex sunucusunun URL'si, örneğin: https://cortex.mycompany.com
- Ayrılmış Cortex hesabının API anahtarı
- Cortex ile bağlantı kurmak için gerekiyorsa Proxy ayarları

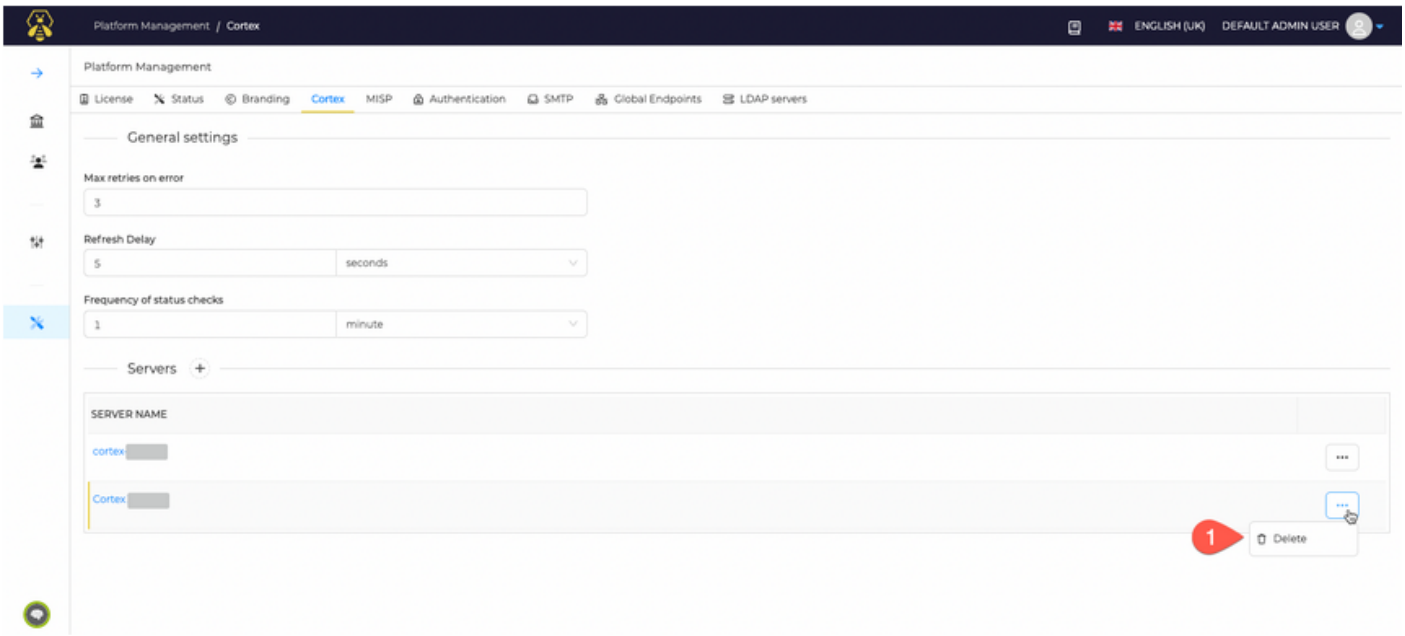
Gelişmiş Ayarlar



Cortex tarafından sunulan tüm Analizörler ve Yanıtlayıcılar TheHive'deki tüm organizasyonlar için kullanılabilir durumdadır. Ayrıca, 2 seçenek daha bulunmaktadır:

- Onları sadece TheHive'daki mevcut Organizasyonların bir alt kümesine kullanılabilir hale getirin.
- Onları TheHive'daki mevcut Organizasyonların bir alt kümesine kullanılamaz hale getirin.

Bir Bağlantıyı Sil



Revision #4
Created 8 April 2024 18:03:17 by Güldeniz Akca
Updated 13 April 2024 15:09:33 by Güldeniz Akca