Giriş

TheHive'a giriş, proje hakkında, proje gereksinimlerini ve hızlı başlangıç adımlarını içeren bir bölümdür. Bu bölüm, kullanıcıların TheHive platformu hakkında temel bilgiler edinmesini sağlar.

- Proje Hakkında
  - TheHive Nedir?
  - TheHive Tarihçesi
- Gereksinimler
  - TheHive'ın Gereksinimleri
- Hızlı Başlangıç
  - Hızlı Başlangıç

Proje Hakkında

TheHive Nedir?

TheHive, güvenlik olaylarının yönetimine ve analizine yardımcı olmak için tasarlanmış açık kaynaklı ve ücretsiz bir Güvenlik Olayı Müdahale Platformudur (SIRP). SOC'ler, CSIRT'ler, CERT'ler, hızla araştırılması ve harekete geçilmesi gereken güvenlik olaylarıyla ilgilenen tüm bilgi güvenliği uygulayıcılarının hayatını kolaylaştırmak için tasarlanmıştır. Güvenlik analistleri, Bilgisayar Güvenliği Olay Müdahale Ekipleri (CSIRT'ler) ve Güvenlik Operasyon Merkezleri (SOC'ler) için geliştirilen TheHive, tehdit avcıları ve olaylara müdahale edenlerin güvenlik olaylarını verimli ve etkili bir şekilde araştırmaları ve çözmeleri için kapsamlı bir çözüm sunar.

Özelleştirilebilir gösterge tabloları, yerleşik gözlemlenebilir veriler, MISP ve Cortex gibi popüler tehdit istihbaratı araçlarıyla entegrasyon dahil olmak üzere zengin özellikleriyle TheHive, güvenlik uzmanlarının, güvenlik olaylarını etkili ve verimli bir şekilde önceliklendirmesine, analiz etmesine ve bunlara yanıt vermesine olanak tanır. TheHive, Cortex, güvenlik analistleri ve araştırmacılar gözlemlenebilir ögeyi kolaylıkla analiz edebilir.

TheHive Tarihçesi

StrangeBee adındaki şirket, 2019 yılından bu yana TheHive projesini üstlenmiş ve Cortex ekosisteminin geliştirilmesi, sürdürülmesi, desteklenmesi ve dağıtılması gibi önemli görevleri üstlenmiştir. Şirketin kurucularını destekleyen güçlü bir ekip bulunmaktadır. Bu ekipte projenin hayata geçmesine yardımcı olan Nabil Adouani ,Thomas Franco ,Jérôme Leonard gibi önemli isimler liderlik etmiştir.

TheHive, 2013 yılında Fransız Bilgi Güvenliği Ajansı (ANSSI) tarafından başlatılan ve ilk sürümü açık kaynak kodlu bir olay müdahale platformu olarak geliştirilen bir projedir. 2014 yılında ilk resmi sürümünü (v1.0) yayınlayan TheHive, o zamandan beri birçok yeni özellik ve geliştirmeyle güncellenmiştir. Bu süre zarfında, geliştirme ekibi, proje yöneticileri ve topluluk katkılarıyla TheHive'ın sürekli iyileştirilmesine katkıda bulunmuştur.

2022 yılında, TheHive lisansı ticari bir lisansa dönüşmüştür. Bu dönüşüm, TheHive'ın olgunlaşmasını sağlamış ve özellikle şirketlerin karşılaştığı güvenlik zorluklarına daha etkin bir şekilde yanıt verebilme kabiliyetini artırmıştır. Ticari lisansın getirdiği avantajlar, kullanıcılar için daha güçlü ve kapsamlı bir deneyim sunmayı amaçlamaktadır. Proje yönetimi ve geliştirme ekibi, kurucuları destekleyen TheHive'ın başarısını sağlamaktadır.

Gereksinimler

TheHive'ın Gereksinimleri

TheHive platformunu başarılı bir şekilde kurmak ve kullanmak için belirli gereksinimler bulunmaktadır. Bu gereksinimler, platformun sorunsuz bir şekilde çalışması için gerekli olan donanım, yazılım ve yapılandırma gereksinimlerini içermektedir.

TheHive platformu aşağıdaki uygulamalara dayanır:

- Veri depolama Apache Cassandra (Desteklenen sürüm: 4.x)
- İndeksleme motoru olarak Elasticsearch (Desteklenen sürüm: 7.x)
- Dosya depolama çözümü de gereklidir; bağımsız sunucu senaryosunda uygulamayı barındıran sunucunun yerel dosya sistemi yeterlidir; aksi takdirde S3 MINIO

> Lucene Kullanımı 5.1 sürümünden bu yana, TheHive artık dizin motoru olarak Lucene arka ucunu desteklememektedir.

4.1.x ile veri dizinini işlemek için bir seçenekti; dizininizi Elasticsearch'e taşımak gerekir.

TheHive uygulaması, veritabanı & dizin motoru ve dosya depolama bağımsızdır. Tek başına bir düğüm veya küme olarak kurulabilir. Sonuç olarak sanal IP adresleri ve yük dengeleyicileri kullanılarak TheHive karmaşık bir küme mimarisinde kurulabilir.

Bağımsız Sunucu : Tüm uygulamalar aynı sunucuya yüklenir.

- Cassandra
- Elasticsearch
- Dosyalar dosya sisteminde saklanır (veya istenirse MinIO)
- TheHive
- NGINX (isteğe bağlı): HTTPS iletişimlerini yönetmek için

Küme veya Hibrit Mimari : TheHive ve yığının tüm uygulamaları, ihtiyaçlara göre doğru kurulumu seçebilecek kadar esnektir. Bir adanmış işletim sistemi üzerine , başka bir uygulama (örneğin : 1 Cassandra düğümü ile 1 Elasticsearch) ile kurulabilir.

Donanım gereksinimleri, entegrasyonları da içeren eşzamanlı kullanıcı ve sistemi nasıl kullandıklarına bağlıdır. Aşağıdaki tablo, tüm hizmetlerin aynı makinede barındırıldığında güvenli eşikleri göstermektedir:

Number of users	TheHive	Cassandra	ElasticSearch
< 10	2 / 2 GB	2 / 2 GB	2 / 2 GB
< 20	2-4 / 4 GB	2-4 / 4 GB	2-4 / 4 GB
< 50	4-6 / 8 GB	4-6 / 8 GB	4-6 / 8 GB

Öneri : Eğer her şeyi aynı sunucuya kuruyorsanız, en az 4 çekirdek ve 16 GB RAM öneriliyor . Elasticsearch için en azından jvm.options'ı ayarlamayı unutmamalıyız.

İşletim Sistemleri

TheHive a?a??daki i?letim sistemlerini desteklemektedir:

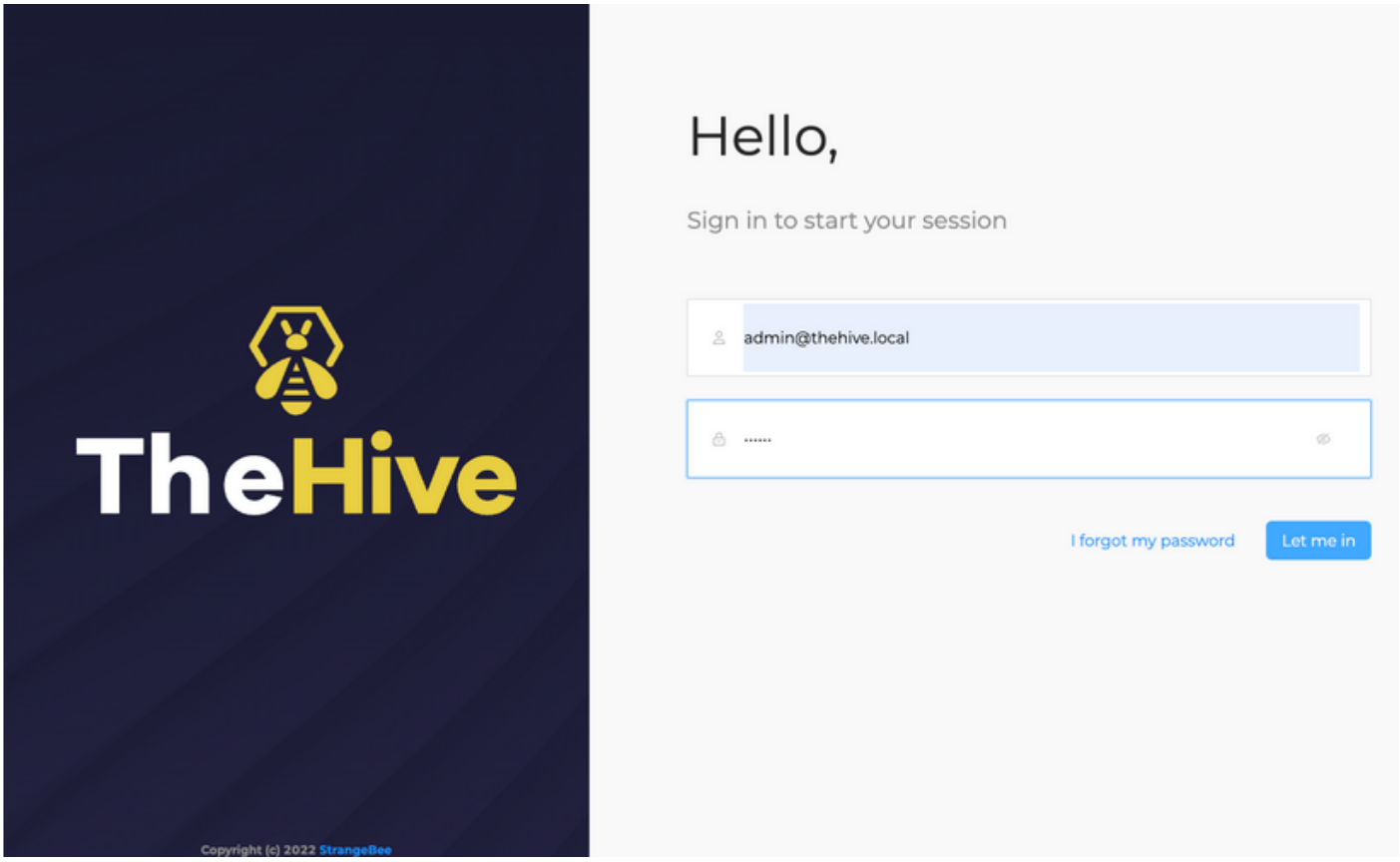
- Ubuntu 20.04 LTS & 22.04 LTS
- Debian 11
- RHEL 8
- Fedora 35 ve 37

Hızlı Başlangıç

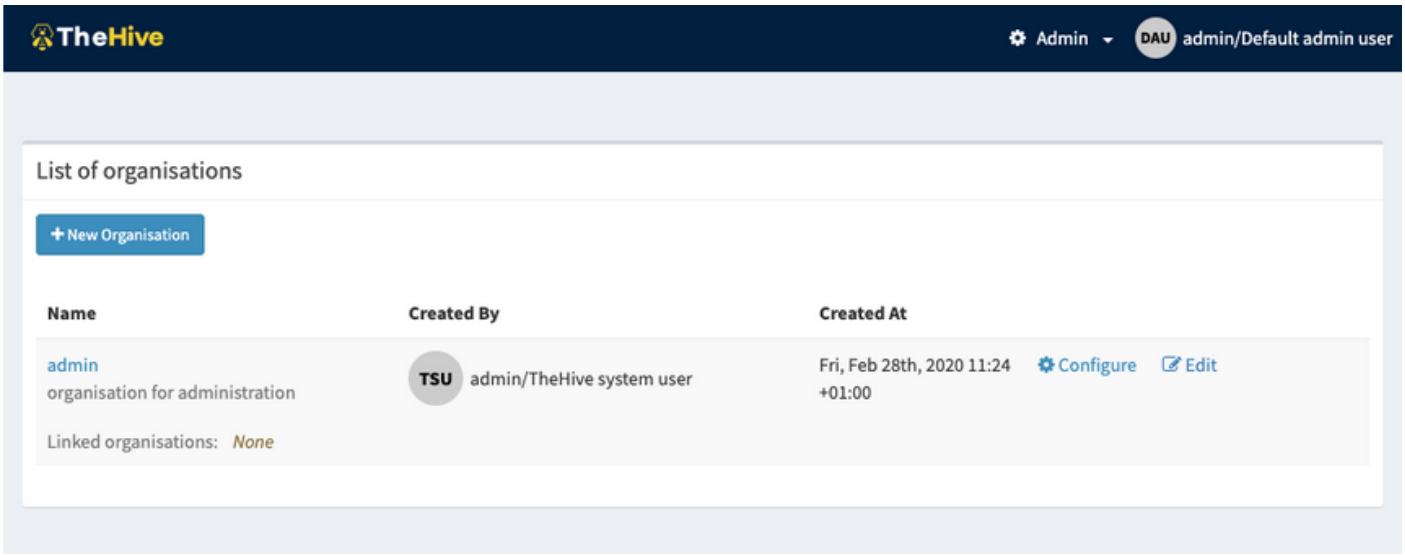
Hızlı Başlangıç

TheHive ilk kez başlatıldığında varsayılan kimlik bilgileri :

Login	`admin@thehive.local`
Password	`secret`



Giriş yaptıktan sonra yönetim sayfasına yönlendirilirsiniz: Burada kuruluşların listesi bulunmaktadır. Bu kuruluş silinemeyeceğini unutmayın.



Admin kullanıcıları için olası işlemlere başlık çubuğunda bulunan "Admin" menüsünden erişilebilir.

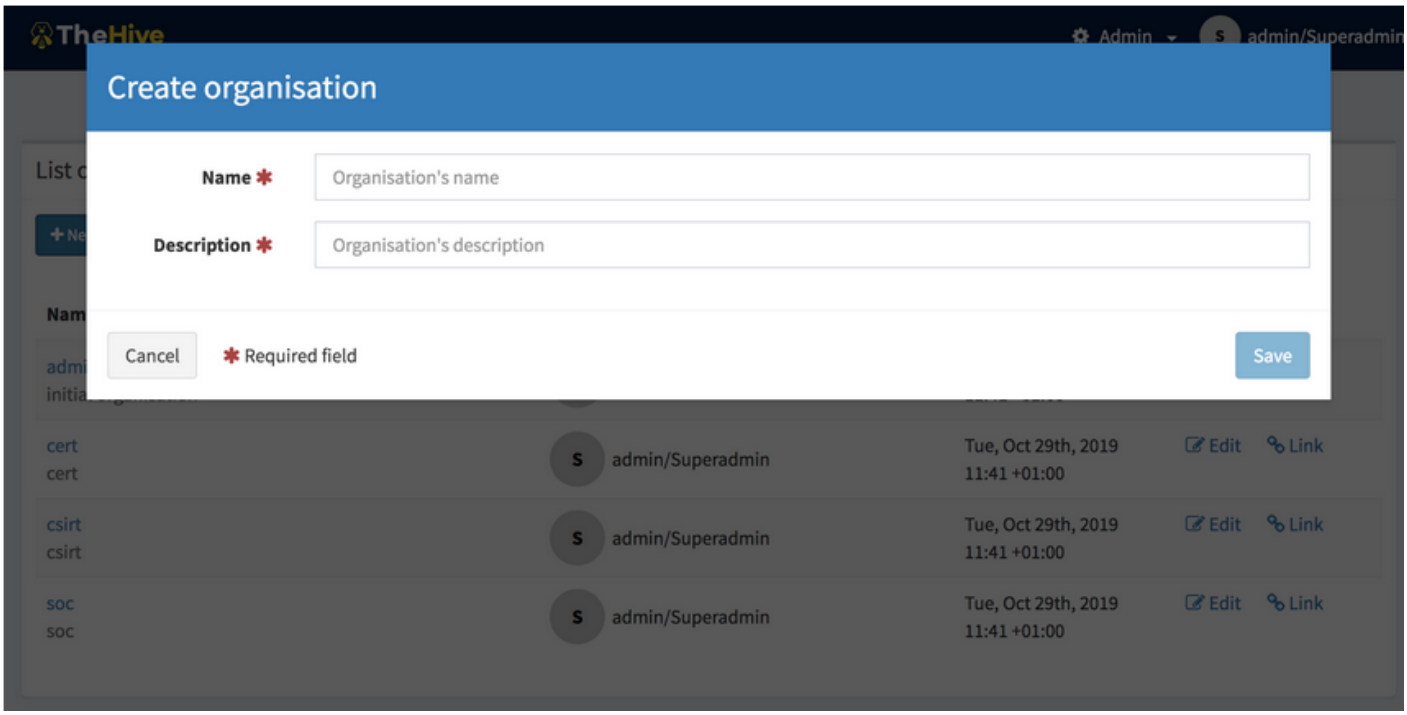
Admin Organizasyon Vakaları yönetemez. Bu yüzden öncelikle bir organizasyon oluşturulmalı ve kullanıcılar eklenmelidir.

Bir Organizasyon Oluşturun

Süper yöneticinin yapması gereken ilk eylem, olay yanıtı ile ilgilenmek için TheHive'ı kullanacak organizasyonları oluşturmaktır.

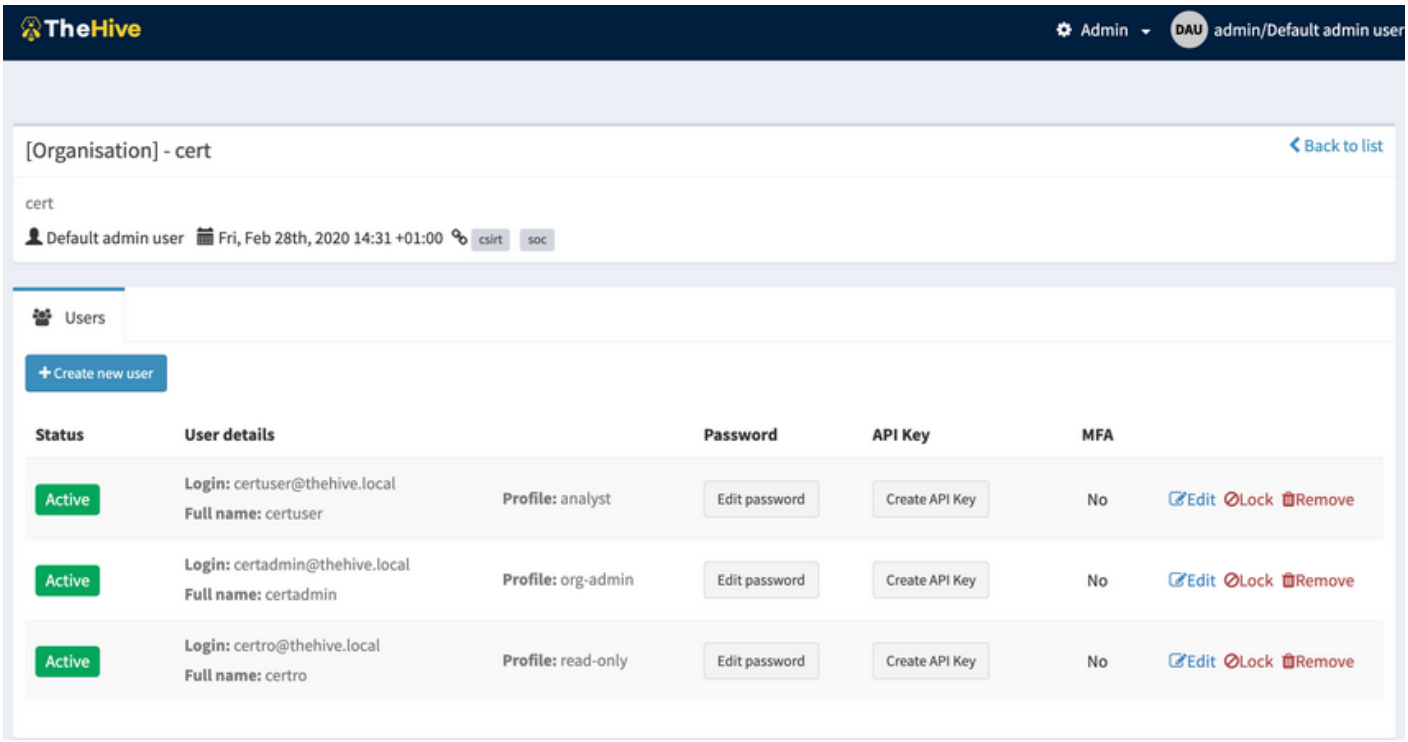
"Organizasyon Listesi" sayfasından, "Yeni Organizasyon" düğmesine basarak organizasyon iletişim kutusunu açın. Organizasyon adı zorunludur ve benzersiz olmalıdır.

Onaylamak için "Kaydet" düğmesine basın.



Bir Kullanıcı Oluşturun

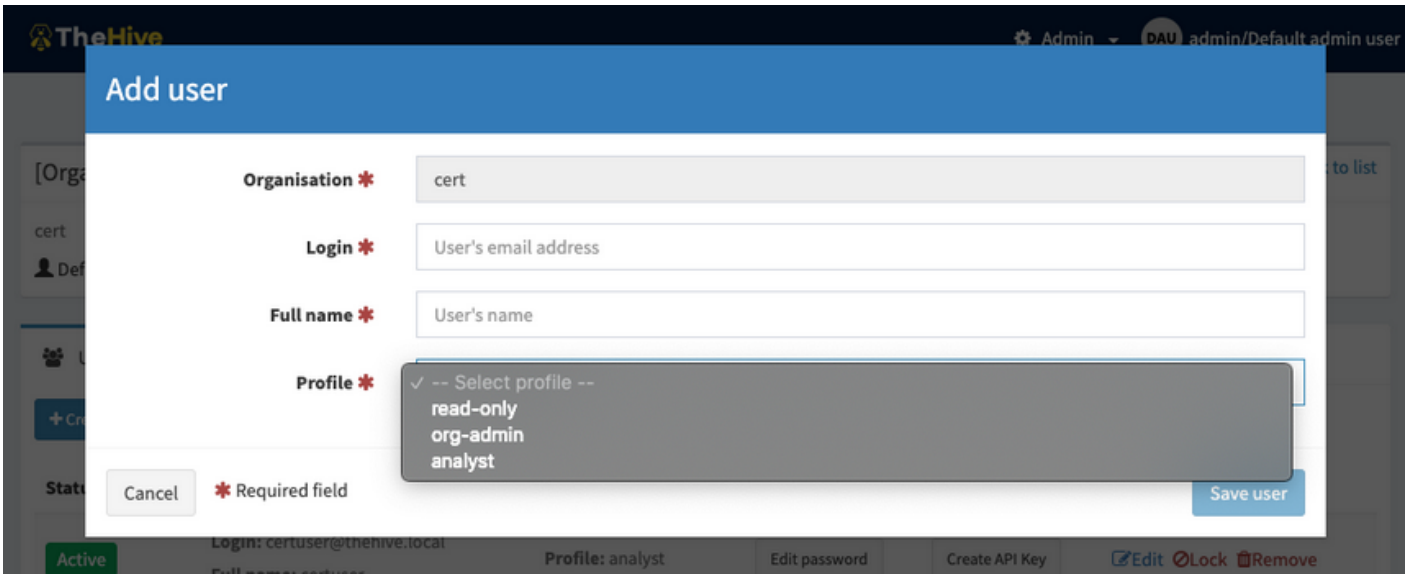
Bir organizasyon oluşturduktan sonra "Yapılandır"a tıklayarak ayrıntılar sayfasını açabilirsiniz. Organizasyon detayları sayfası, "admin" profiline sahip kullanıcılar için sadece organizasyon kullanıcılarını yönetmelerine izin verir.



Bu sayfada şunları görebilirsiniz :

- Organizasyonun detayları: Adı, açıklaması, oluşturan kullanıcı
- Kullanıcıları yönetmek için bir sekme
- Yeni kullanıcılar oluşturmak
- API anahtarlarını düzenlemek
- Profil bilgilerini düzenlemek
- İki faktörlü kimlik doğrulama (2FA) ayarlarını sıfırlamak
- Kullanıcıları kilitleme ve silme

Bir kullanıcı oluşturmak için, kullanıcı oluşturma iletişim kutusunu açan "Yeni kullanıcı oluştur" düğmesine tıklamanız yeterlidir.



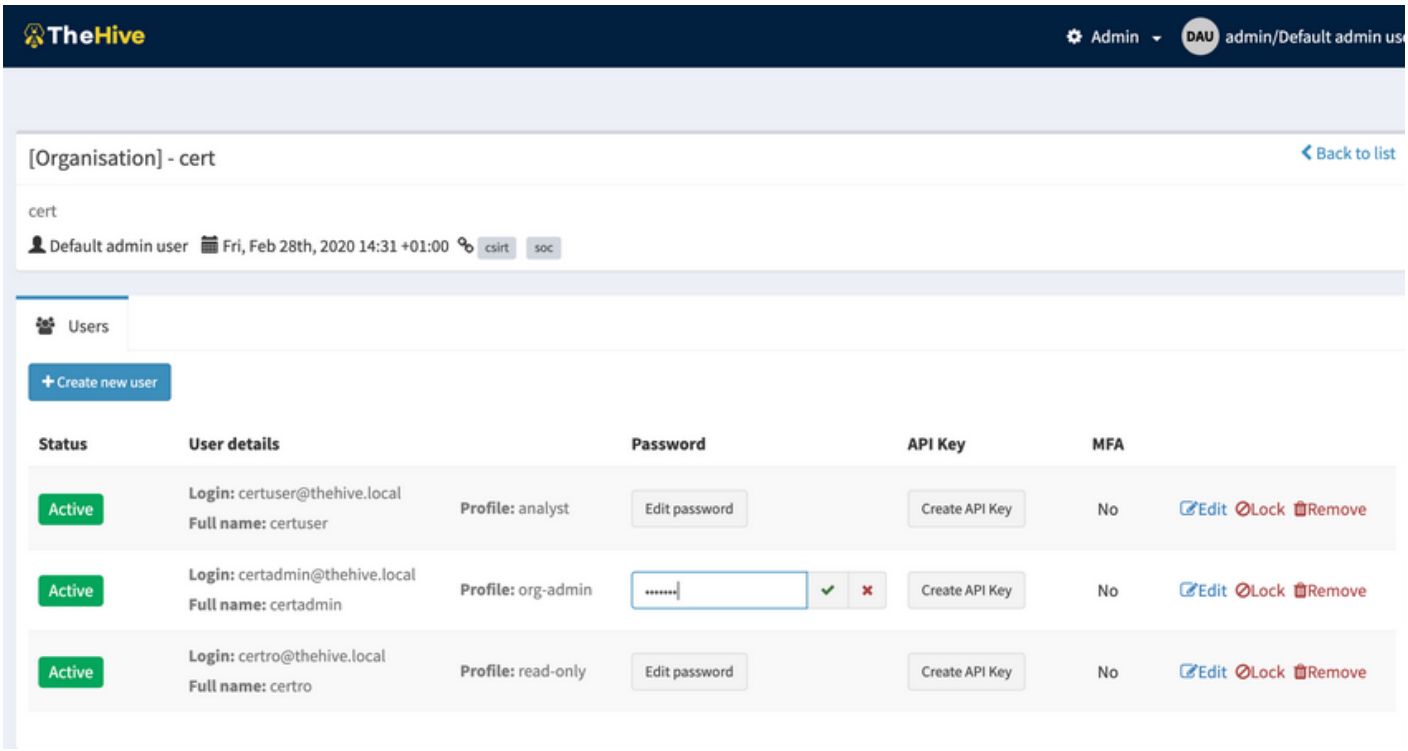
> "Profil" alanı, yalnızca organizasyon kullanıcılarına atanabilecek profillerle doldurulacaktır (Yönetim profilleri listelenmeyecek).

Her organizasyon için oluşturmanız gereken ilk kullanıcı, "org-admin" profiline sahip bir kullanıcı olmalıdır. Bu profil, bir organizasyon içinde tüm işlemlere izin verir.

"org-admin" profiline sahip bir kullanıcı en azından aşağıdaki işlemleri gerçekleştirebilecektir:

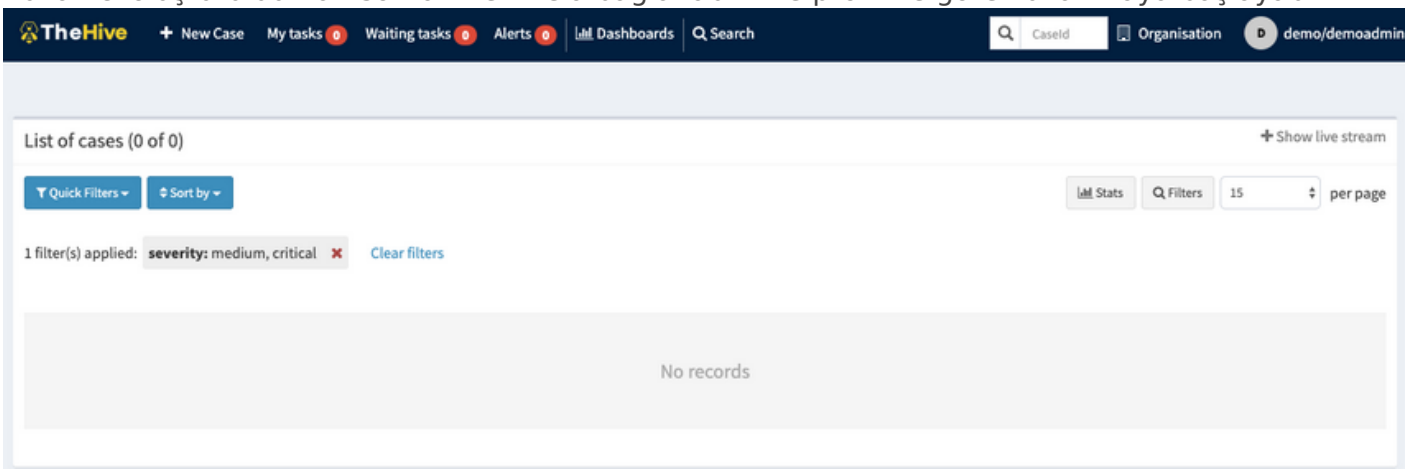
- Diğer kullanıcıları oluşturma
- Vaka şablonları oluşturma

Kullanıcıları oluşturduktan sonra, parolanızı belirleyebilirsiniz. Bunu yapmak için, ilgili kullanıcı satırında "Yeni şifre" düğmesine tıklayın ve ardından ENTER tuşuna basın veya yeşil onay düğmesine tıklayın:

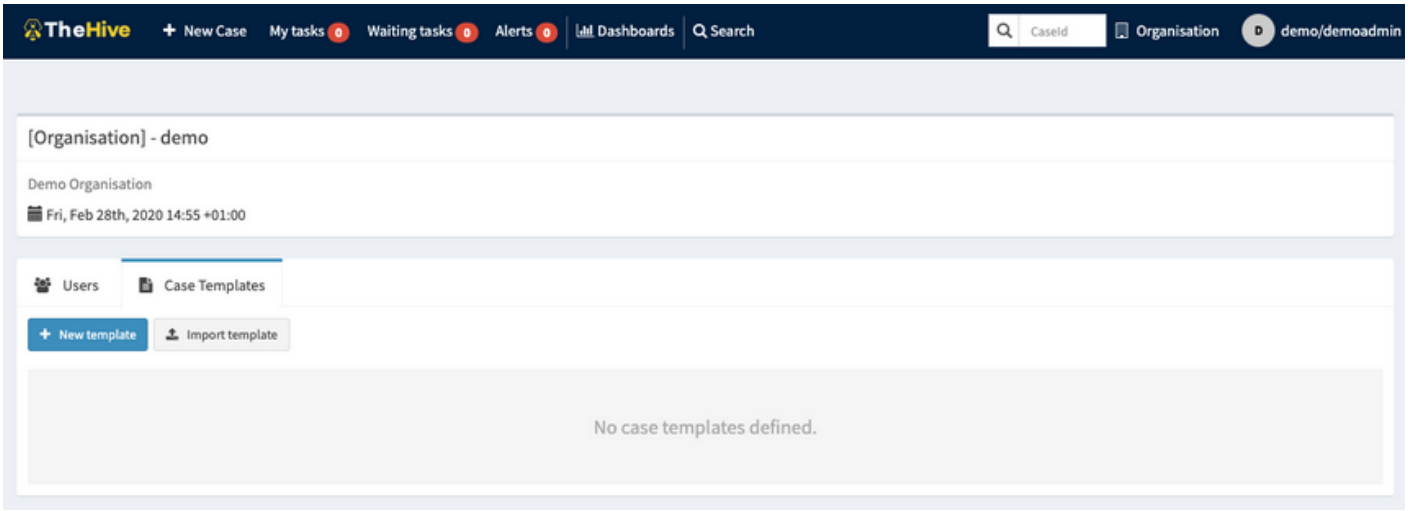


org-admin Kullanıcısı Olarak Girişi

Kullanıcı oluşturulduktan sonra TheHive'a bağlanabilir ve profiline göre kullanmaya başlayabilir.



> "org-admin" profiline sahip kullanıcılar, başlık çubuğunun sağ köşesindeki "Organizasyon" menüsüne erişim sağlarlar. Bu, organizasyon yapılandırma sayfasına ve bir olay şablonu yönetimi için ek bir sekme ile birlikte verilir.



Kuruluş ve kullanıcılar oluşturulduğuna göre, özel alanlar tanımlanmalı ve ardından bunları vaka şablonlarını tanımlamak için kullanılmalıdır.