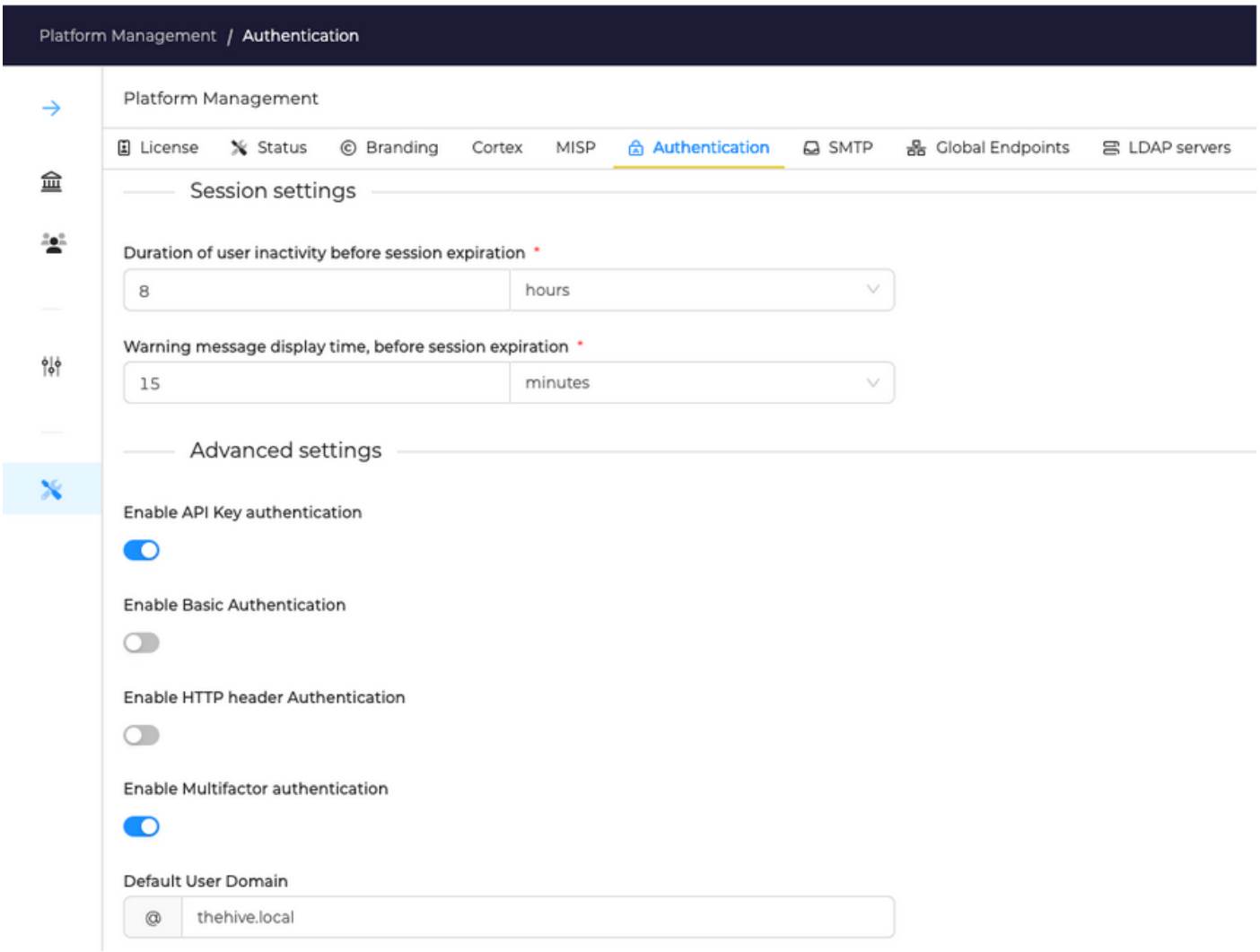
Kimlik Doğrulama

Genel Ayarlar

Bilgi:

- Gerekli izinler: yönetici
- Organizasyon: admin
- Konum:

1. Menü: Platform Yönetimi
2. Sekme: Kimlik Doğrulama



Oturum Ayarları

- Kullanıcının oturumu hareketsiz kalma süresi öncesi sona erme süresi: Hareketsiz kalırsa kullanıcıyı oturumdan çıkarma süresi
- Oturum sona ermeden önce uyarı mesajının görüntülenme süresi: Oturumdan çıkmadan önce uyarı mesajının görüntülenme süresi

Birkaç seçenek mevcuttur:

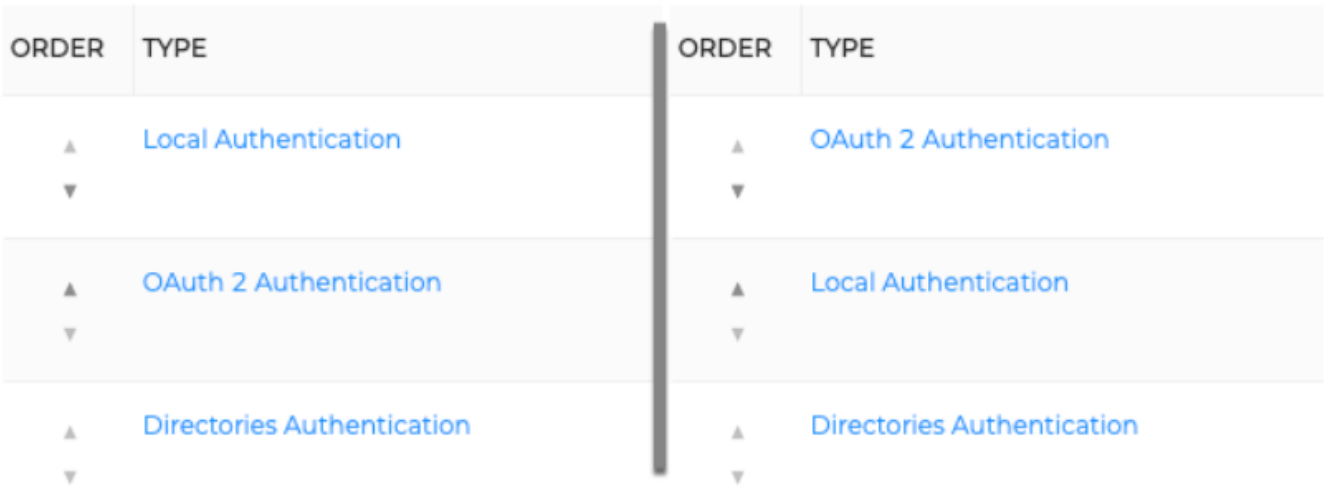
- Temel Kimlik Doğrulamayı Etkinleştir: Sağlanan giriş ve parola ile HTTP isteklerini kimlik doğrular
- API Anahtar Kimlik Doğrulamasını Etkinleştir: Sağlanan bir API anahtarı ile HTTP isteklerini kimlik doğrular
- HTTP Başlık Kimlik Doğrulamasını Etkinleştir: Kullanıcı girişini içeren bir HTTP başlığı kullanarak HTTP isteklerini kimlik doğrular
- Çok Faktörlü Kimlik Doğrulamasını Etkinleştir: Çok Faktörlü Kimlik Doğrulama varsayılan olarak etkindir. Bu, kullanıcıların Çok Faktörlü Kimlik Doğrulamalarını Kullanıcı Ayarları sayfası üzerinden yapılandırabilecekleri anlamına gelir.
- Varsayılan kullanıcı alanı: Varsayılan olarak, kullanıcılar bir e-posta adresiyle giriş yaparlar, örneğin: user@domain.com. Kurulduğunda, kullanıcıların alan olmadan da giriş yapma izni verilir (örneğin, kullanıcı).

Kimlik Doğrulama Sağlayıcılarını Yönetmek

Kullanıcıları doğrulamak için birkaç seçenek bulunmaktadır:

- Yerel hesaplar: Parola politikasını yapılandırabileceğiniz yerel bir kullanıcı veritabanını yönetin.
- LDAP dizini kullanma: TheHive'ı bir LDAP sunucusunu kullanacak şekilde yapılandırın.
- Active directory kullanma: TheHive'ı bir LDAP sunucusunu kullanacak şekilde yapılandırın.
- SAML: Kullanıcıları doğrulamak için bir veya daha fazla SAML sağlayıcısı aracılığıyla tek oturum açmayı kullanın.
- OAuth2: Kullanıcıları doğrulamak için harici bir OAuth2 sunucusu aracılığıyla tek oturum açmayı kullanın.

Birden fazla sağlayıcı kullanımı

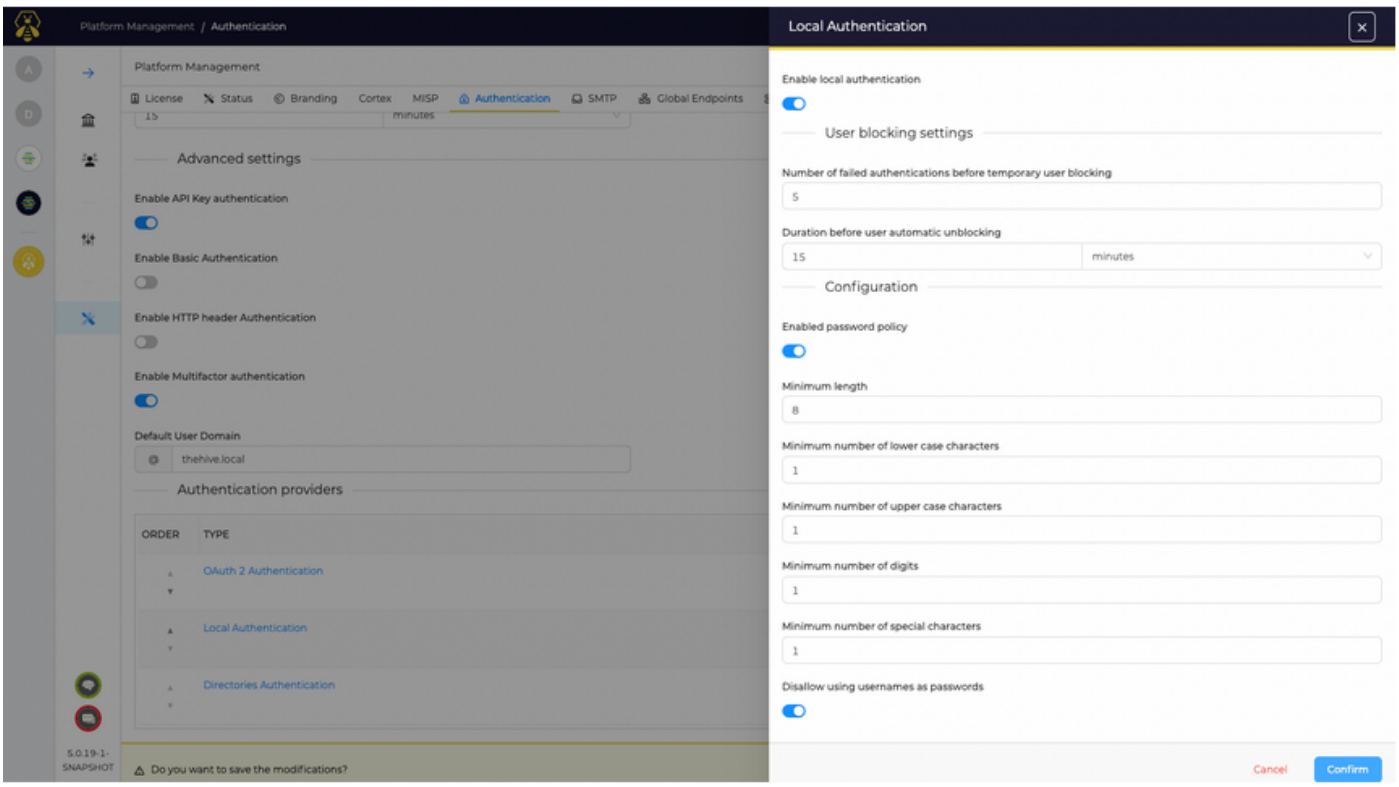


TheHive, kullanıcıları doğrulamak için birden fazla sağlayıcı kullanabilir, öncelik sırasını değiştirmek için okları kullanın (örneğin: önce Oauth2 doğrulamasını deneyin, sonra yerel veritabanını).

Yerel Hesap

Bu, TheHive'ın varsayılan davranışıdır. Uygulamalar kullanıcı adlarını ve parolaları yerel bir veritabanında saklar.

Yapılandırma



Varsayılan olarak, yerel hesaplar için herhangi bir politika etkin değildir. Bununla birlikte, bir parola politikası ve engelleme ayarları ayarlanabilir:

- Bir kullanıcının geçici olarak engellenmeden önce kimlik doğrulama için başarısız deneme sayısı
- Kullanıcının engelini kaldırmak için ilgili süre

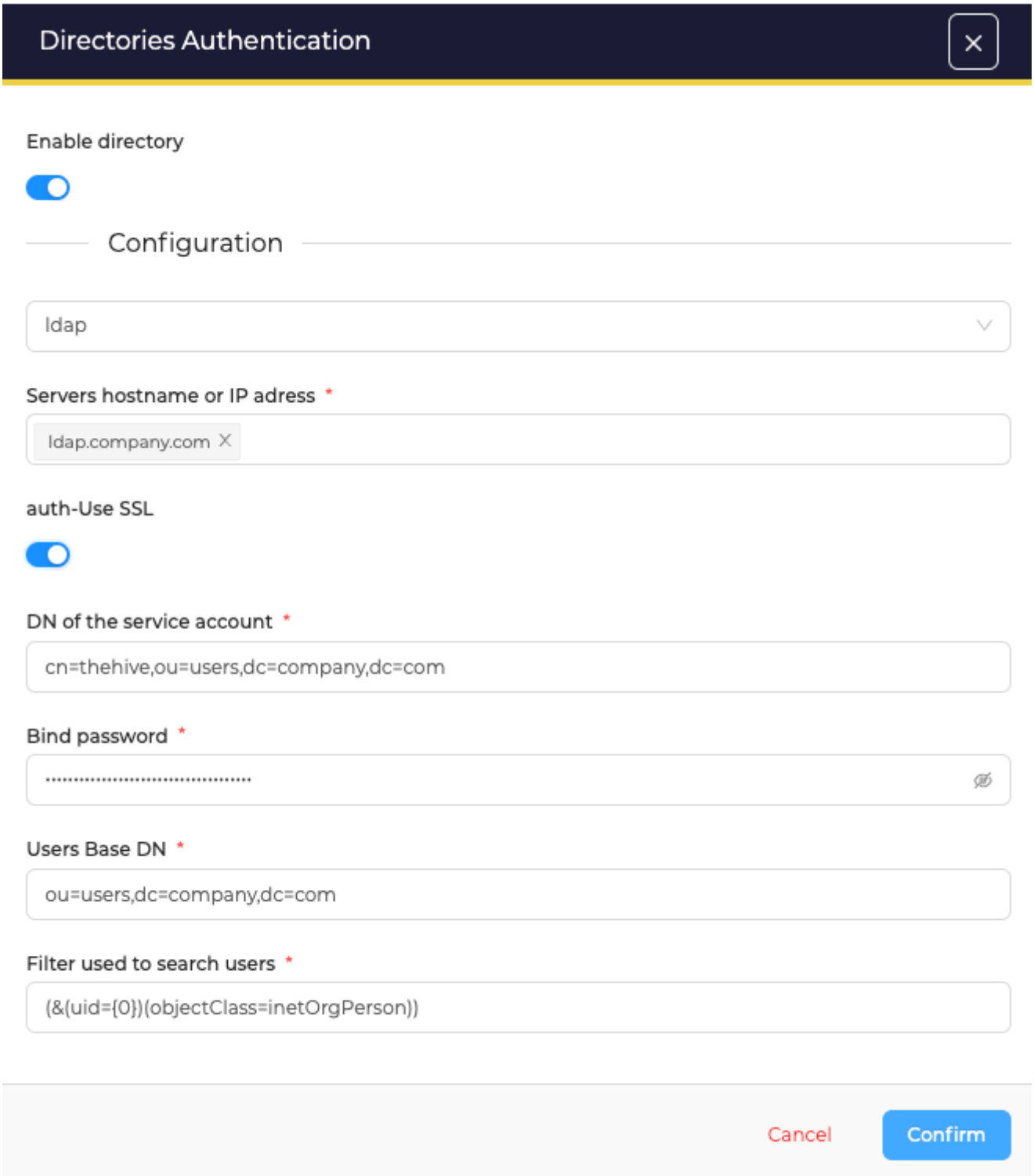
Parola Politikası

- Bu seçenek varsayılan olarak devre dışı bırakılmıştır. Etkinleştirildiğinde, aşağıdaki öğeler yapılandırılabilir:
- Parolada minimum uzunluğu
- Parolada bulunması gereken minimum küçük harf sayısı
- Parolada bulunması gereken minimum büyük harf sayısı
- Parolada bulunması gereken minimum rakam sayısı
- Parolada bulunması gereken minimum özel karakter sayısı
- Kullanıcı adlarının parola olarak kullanımını izin verme veya izin vermemeyi ayarlama

LDAP Kimlik Doğrulamasını Ayarlama

LDAP kimlik doğrulamasını kurmak için şu adımları izleyin:

1. Dizin Kimlik Doğrulaması'na tıklayın.
2. Dizini etkinleştirmek için anahtarı kullanın.
3. Ardından menüden LDAP'ı seçin; gerekli parametrelerin listesi görüntülenir.



4. Değişikliklerinizi onaylayın ve kaydedin.

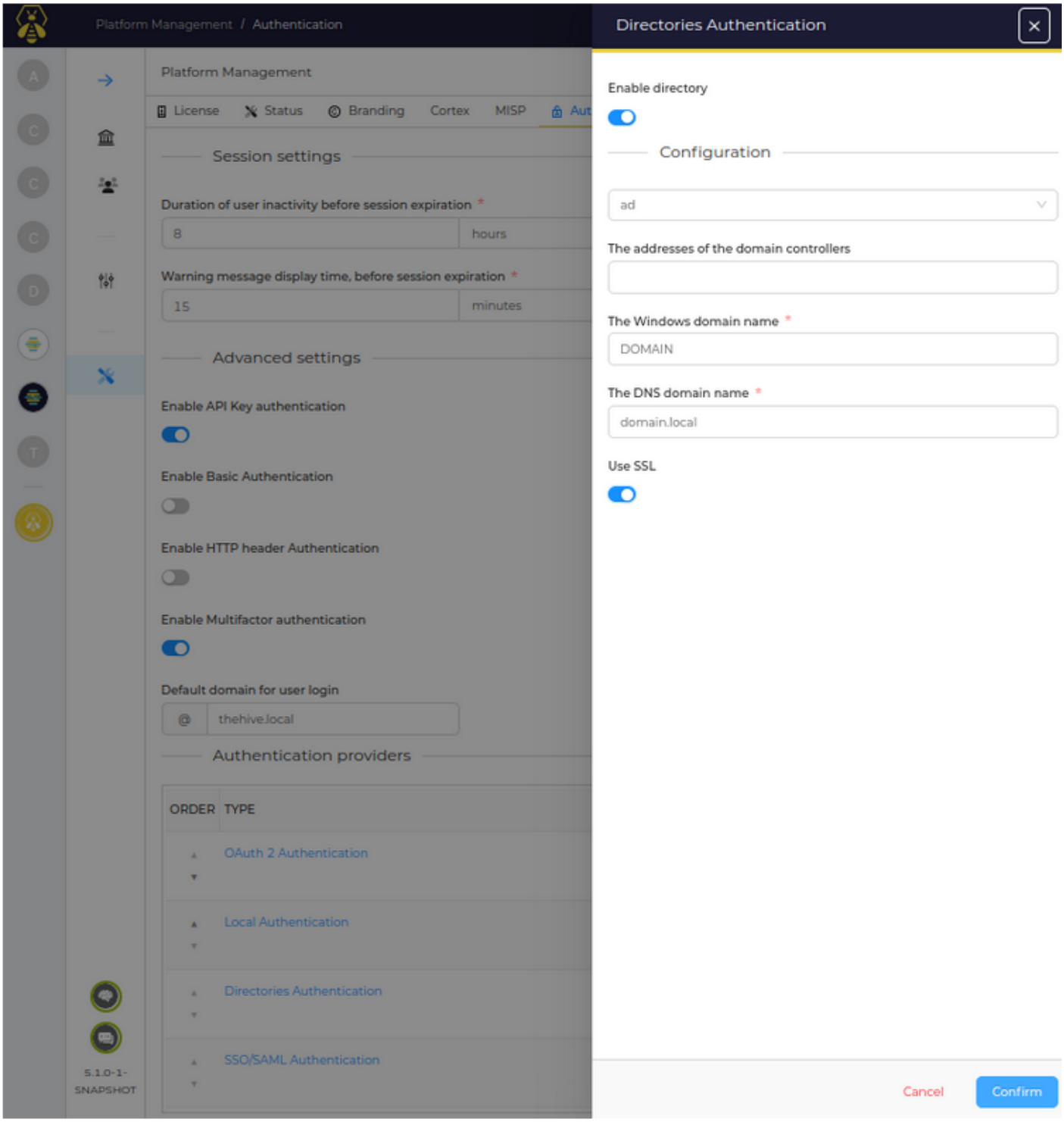
5. Dizin Kimlik Doğrulaması satırını, kimlik doğrulama sağlayıcıları listesinde kullanılacak ilk sağlayıcı olarak taşıyın.

LDAP ile Kimlik Doğrulama

Kimlik doğrulama yapabilen kullanıcıların zaten TheHive yerel veritabanında bir hesap oluşturmuş olmaları gerekir.

Active Directory

Active Directory kimlik doğrulamasını yapılandırmak için bir lisans gereklidir.



AD kimlik doğrulamasını yapılandırmak için aşağıdaki bilgilere ihtiyacınız olacak:

- Alan denetleyicilerinin adresleri
- Windows Alan Adı
- DNS alan adı
- SSL kullanılıp kullanılmadığı

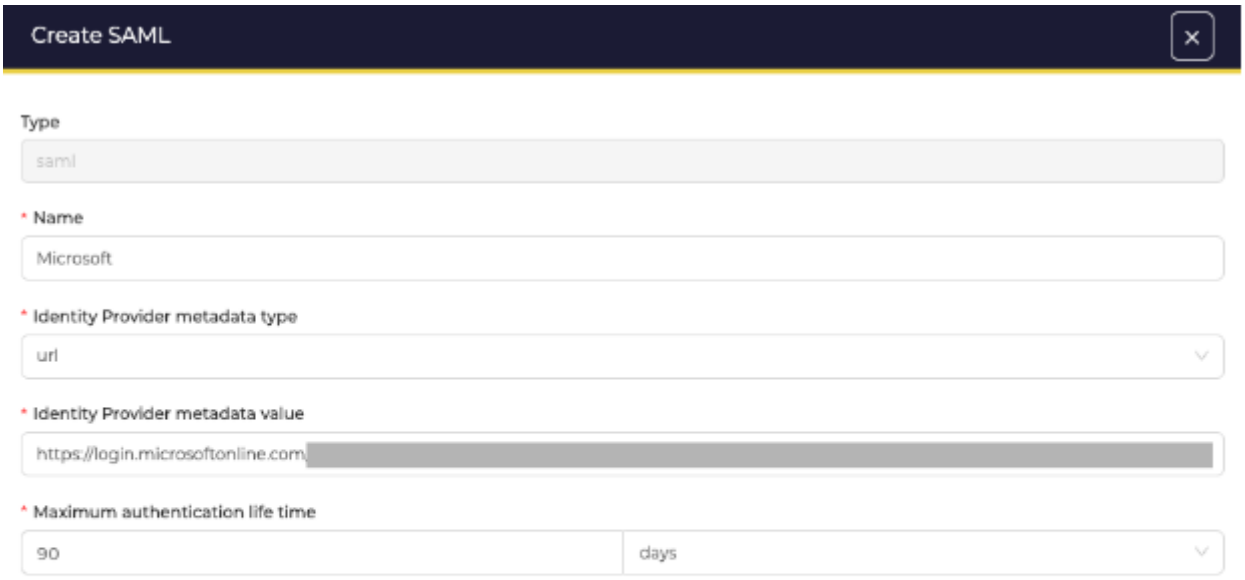
SAML

TheHive SAMLv2.0 kimlik doğrulama sağlayıcılarını destekler.

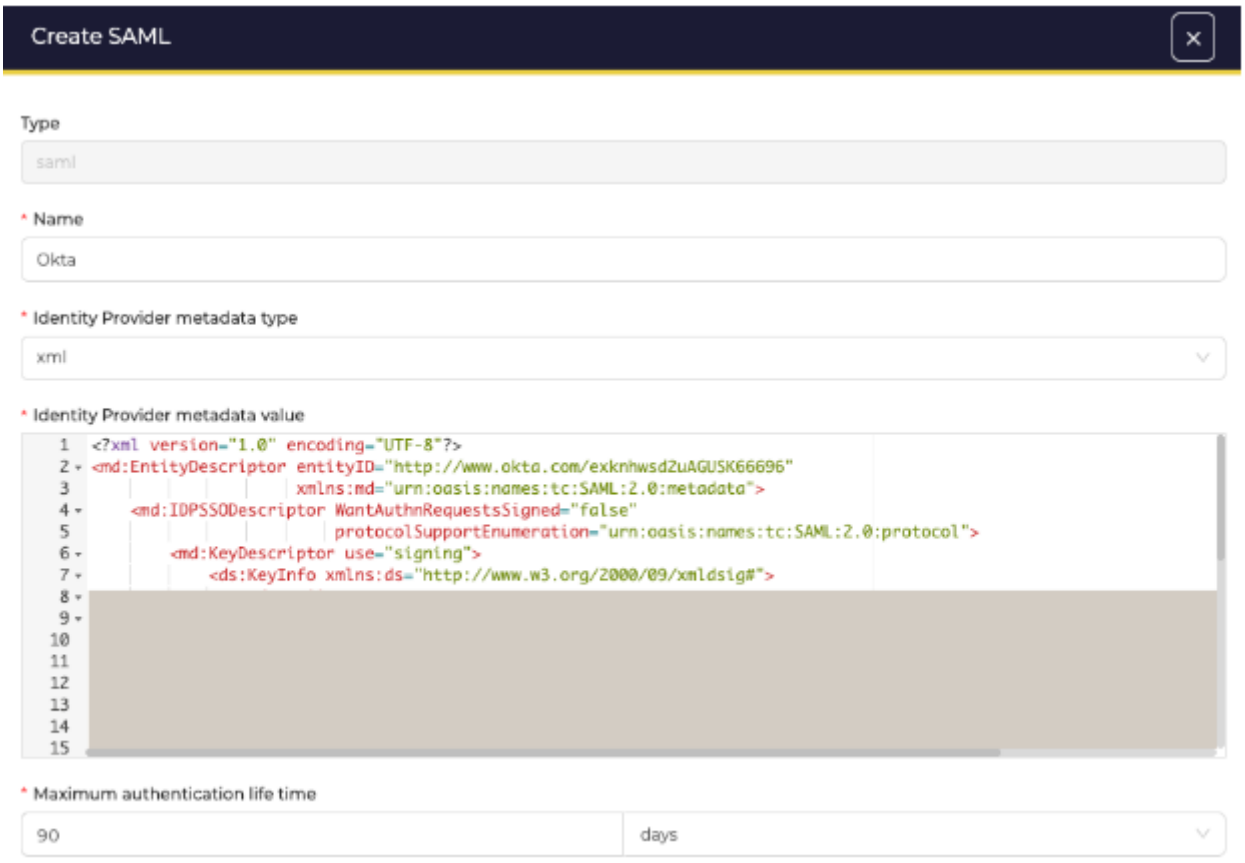
Yapılandırma

Bir SAML kimlik doğrulama sağlayıcısı aşağıdaki yapılandırma parametrelerini kabul eder:

- Ad: TheHive'daki sağlayıcıya bir ad verin.
- Kimlik Sağlayıcı meta veri türü: Bilgi toplama yöntemini seçin: xml veya url
- Kimlik Sağlayıcı meta veri değeri: Hizmet bilgisiyle birlikte URL veya XML içeriği verin
- Maksimum kimlik doğrulama süresi: Bu değer, kimlik sağlayıcıdan alınan değerle eşleşmelidir



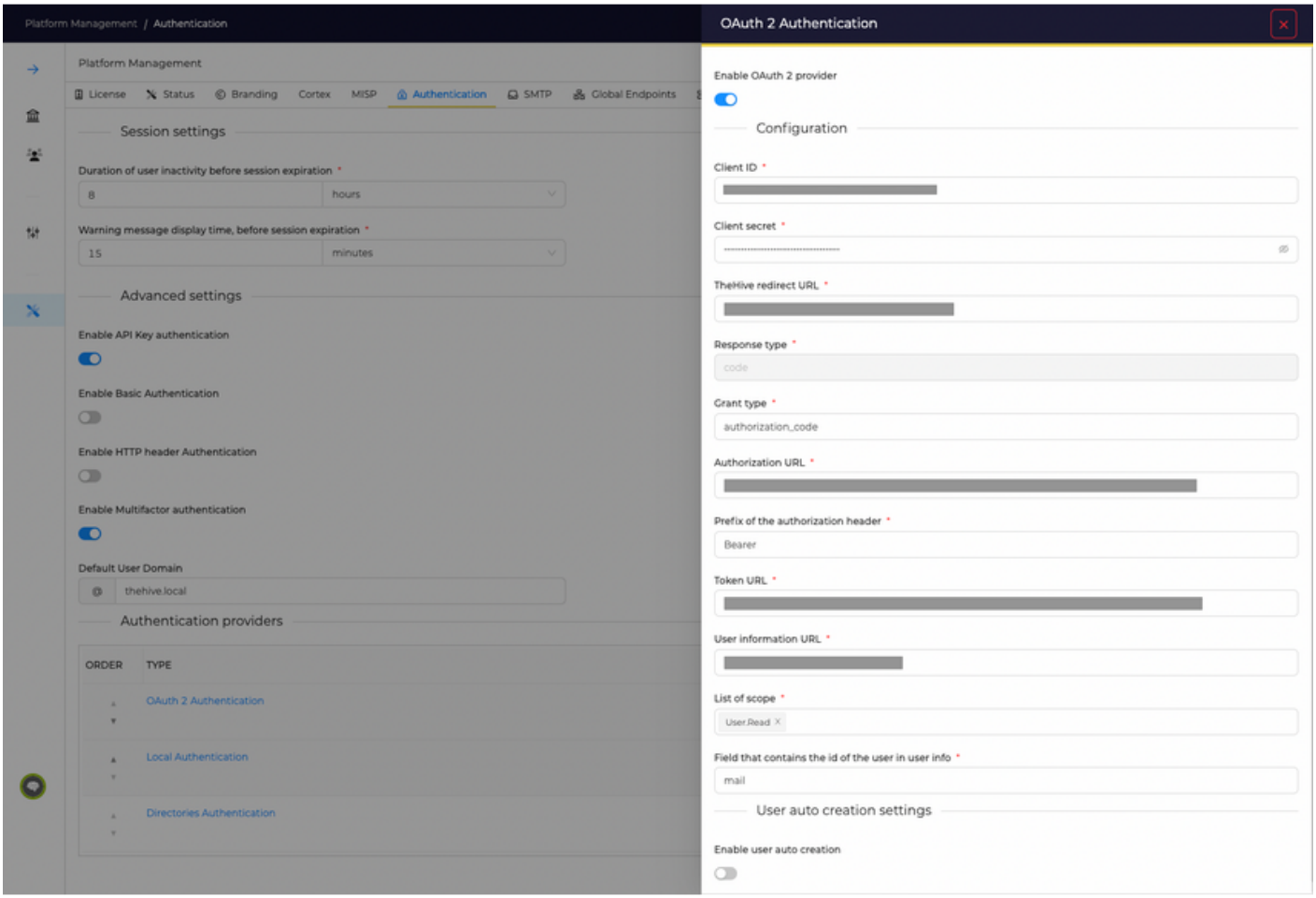
Configuration gathered using the URL



Birden Fazla Hizmet Sağlayıcısı Yapılandırıma

Birden fazla hizmet sağlayıcısı yapılandırılabilir. Bu durumda, bir kullanıcı giriş yapmaya çalıştığında, TheHive her bir hizmet sağlayıcısına sırayla sorgu gönderir. Bir hizmet sağlayıcı giriş yapma yetkisiyle yanıt verdiğinde sorgular durur.

OAuth2 / OpenID Bağlantısı



Yapılandırma

Kullanıcıyı harici bir OAuth2 kimlik doğrulayıcı sunucusu kullanarak kimlik doğrulayın. Aşağıdaki yapılandırma parametrelerini kabul eder:

Parametre ve Açıklamaları :

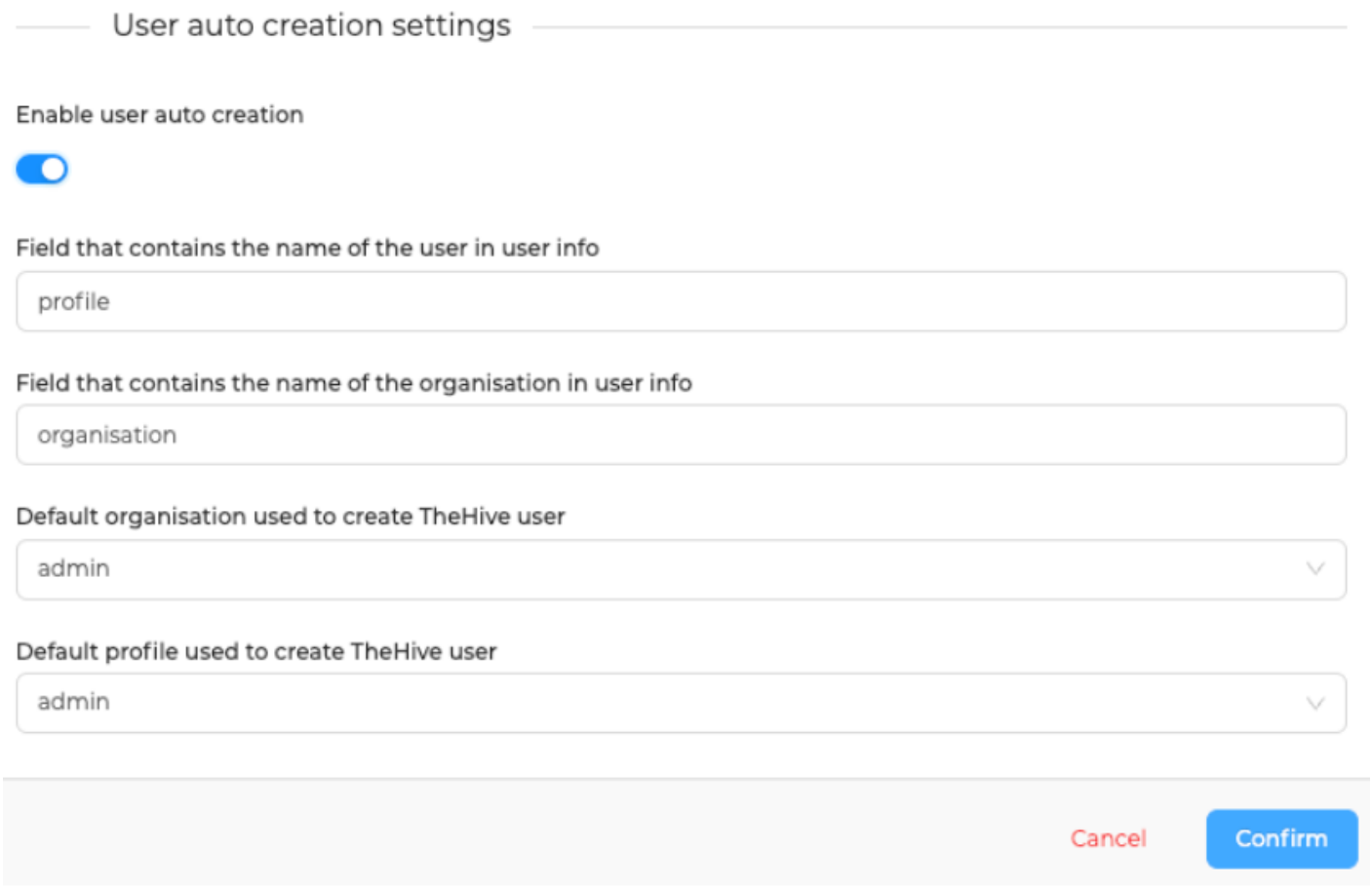
- İstemci ID: OAuth2 sunucusundaki istemci Kimlik Bilgisi
- Gizli İstemci: OAuth2 sunucusundaki istemci Gizli Bilgisi

- TheHive yönlendirme URL'si: TheHive OAuth2 sayfasının URL'si (https://xxx/api/ssoLogin)
- Yetkilendirme URL'si: OAuth2 sunucusunun yetkilendirme URL'si Token URL'si: OAuth2 sunucusunun token URL'si
- Kullanıcı bilgisi URL'si: OAuth2 sunucusundan kullanıcı bilgisini almak için URL
- Kapsam listesi: Kapsam listesi Kullanıcı bilgisinde kullanıcı
- Kimlik Bilgisini içeren alan: Kullanıcı bilgisinde kullanıcı Kimlik Bilgisini içeren alan

Kullanıcı Otomatik Oluşturma

Kullanıcıların önceden oluşturulmadan giriş yapmalarına izin vermek için otomatik oluşturmayı etkinleştirebilir ve birkaç seçenek belirleyebilirsiniz:

- Kullanıcı bilgisinde kullanıcının adını içeren alan
- Kullanıcı bilgisinde kuruluşun adını içeren alan
- Yeni kullanıcılara uygulanan varsayılan kuruluş
- Yeni kullanıcılara uygulanan varsayılan profil



Revision #6
Created 8 April 2024 20:05:36 by Güldeniz Akca
Updated 13 April 2024 14:51:12 by Güldeniz Akca