

# Kimlik Doğrulama

## Genel Ayarlar

### Bilgi:

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

- Menü: Platform Yönetimi
- Sekme: Kimlik Doğrulama

Platform Management / Authentication

Platform Management

License Status Branding Cortex MISP Authentication SMTP Global Endpoints LDAP servers

Session settings

Duration of user inactivity before session expiration \*

8 hours

Warning message display time, before session expiration \*

15 minutes

Advanced settings

Enable API Key authentication

☒

Enable Basic Authentication

☐

Enable HTTP header Authentication

☐

Enable Multifactor authentication

☒

Default User Domain

@ thehive.local

### 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

ORDER	TYPE	ORDER	TYPE
▲ ▼	Local Authentication	▲ ▼	OAuth 2 Authentication
▲ ▼	OAuth 2 Authentication	▲ ▼	Local Authentication
▲ ▼	Directories Authentication	▲ ▼	Directories Authentication

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'in varsayılan davranışıdır. Uygulamalar kullanıcı adlarını ve parolaları yerel bir veritabanında saklar.

### Yapılandırma

Platform Management / Authentication

License
Status
Branding
Cortex
MISP
Authentication
SMTP
Global Endpoints

Advanced settings

Enable API Key authentication

Enable Basic Authentication

Enable HTTP header Authentication

Enable Multifactor authentication

Default User Domain

Authentication providers

ORDER	TYPE
▲ ▼	OAuth 2 Authentication
▲ ▼	Local Authentication
▲ ▼	Directories Authentication

Local Authentication

Enable local authentication

User blocking settings

Number of failed authentications before temporary user blocking

Duration before user automatic unblocking

Configuration

Enabled password policy

Minimum length

Minimum number of lower case characters

Minimum number of upper case characters

Minimum number of digits

Minimum number of special characters

Disallow using usernames as passwords

Cancel
Confirm

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

Authentication providers		
ORDER	TYPE	STATUS
▲ ▼	Local Authentication	Enabled
▲ ▼	Directories Authentication	Disabled
▲ ▼	OAuth 2 Authentication	Disabled

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.

Enable directory



## Configuration

ldap



Servers hostname or IP adress \*

ldap.company.com ✕

auth-Use SSL



DN of the service account \*

cn=thehive,ou=users,dc=company,dc=com

Bind password \*

.....



Users Base DN \*

ou=users,dc=company,dc=com

Filter used to search users \*

(&amp;{uid={0}}(objectClass=inetOrgPerson))

Cancel

Confirm

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.

Platform Management / Authentication

Directories Authentication

Platform Management

License Status Branding Cortex MISP Auth

Session settings

Duration of user inactivity before session expiration \*  
8 hours

Warning message display time, before session expiration \*  
15 minutes

Advanced settings

Enable API Key authentication

Enable Basic Authentication

Enable HTTP header Authentication

Enable Multifactor authentication

Default domain for user login  
@ thehive.local

Authentication providers

ORDER	TYPE
1	OAuth 2 Authentication
2	Local Authentication
3	Directories Authentication
4	SSO/SAML Authentication

5.1.0-1-SNAPSHOT

Enable directory

Configuration

ad

The addresses of the domain controllers

The Windows domain name \*  
DOMAIN

The DNS domain name \*  
domain.local

Use SSL

Cancel

Confirm

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

Create SAML ✕

Type

saml

\* Name

Microsoft

\* Identity Provider metadata type

url

\* Identity Provider metadata value

https://login.microsoftonline.com/

\* Maximum authentication life time

90

days

Configuration gathered using the URL

Create SAML ✕

Type

saml

\* Name

Okta

\* Identity Provider metadata type

xml

\* Identity Provider metadata value

```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <md:EntityDescriptor entityID="http://www.okta.com/exknhwsdZuAGUSK66696"
3   xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">
4   <md:IDPSSODescriptor WantAuthRequestsSigned="false"
5     protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
6     <md:KeyDescriptor use="signing">
7       <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
8
9
10
11
12
13
14
15
```

\* Maximum authentication life time

90

days

## Birden Fazla Hizmet Sağlayıcısı Yapılandırırma

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.



Enable SSO/SAML



Clients



Microsoft



Okta



## OAuth2 / OpenID Bağlantısı

Platform Management / Authentication

Platform Management

License Status Branding Cortex MISP Authentication SMTP Global Endpoints

Session settings

Duration of user inactivity before session expiration \*  
8 hours

Warning message display time, before session expiration \*  
15 minutes

Advanced settings

Enable API Key authentication  
☒

Enable Basic Authentication  
☐

Enable HTTP header Authentication  
☐

Enable Multifactor authentication  
☒

Default User Domain  
thehive.local

Authentication providers

ORDER	TYPE
1	OAuth 2 Authentication
2	Local Authentication
3	Directories Authentication

OAuth 2 Authentication

Enable OAuth 2 provider  
☒

Configuration

Client ID \*  
[Redacted]

Client secret \*  
[Redacted]

Thelive redirect URL \*  
[Redacted]

Response type \*  
code

Grant type \*  
authorization\_code

Authorization URL \*  
[Redacted]

Prefix of the authorization header \*  
Bearer

Token URL \*  
[Redacted]

User information URL \*  
[Redacted]

List of scope \*  
User.Read X

Field that contains the id of the user in user info \*  
mail

User auto creation settings

Enable user auto creation  
☐

### 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

### User auto creation settings

Enable user auto creation



Field that contains the name of the user in user info

profile

Field that contains the name of the organisation in user info

organisation

Default organisation used to create TheHive user

admin

Default profile used to create TheHive user

admin

Cancel

Confirm

Revision #6

Created 8 April 2024 20:05:36 by Güldeniz Akca

Updated 13 April 2024 14:51:12 by Güldeniz Akca