

TREND MICRO APEX ONE KURULUM

Hazırlayan:

Orhan Tan

Cyber Security Specialist

Tarih:

05.04.2024

İçerik

• Trend Micro Apex One ürünü için On-Prem kurulum anlatımı

Apex One, merkezi yönetime sahip, her türlü tehdide karşı en geniş korumayı sağlamak için nesiller arası tehdit tekniklerinin karışımından yararlanan gelişmiş bir güvenlik yazılımıdır.



www.orphantan.com



iletisim@orphantan.com

Merhaba, bu yazımda Trend Micro Apex One ürününün On-Prem versiyonu için kurulum adımlarını anlatacağım

Kurulum öncesi hazırlık

Apex One On-Prem sürümü için bir makineye ihtiyacımız var, bu makine, Agent'ların ve Apex One ayarlarının yönetimi için zorunlu, bu sayede tek bir ekrandan tüm Agent'ları (Policy, Modules, Update) yönetebileceğiz, sonraki aşamalarda indirme işlemlerini bunun üzerinde yapacağız.

Bu makine için önerdiğimiz donanım aşağıdaki gibi olacak,

- Minimum 4 Core CPU
- 8 GB RAM
- 120 GB SSD Disk
- Windows Server 2019 English veya 2022 English kurulu olmalı
- Klavye ayarları hariç, dil ve saat/tarih biçimi ayarları English-United States olmalı
- Tüm OS güncellemeleri yapılmış ve domain ortamı varsa domain'e alınmış olmalı
- Windows defender ve firewall açık ise kapatılmalı
- SQL Server yok ise kurulumla birlikte SQL Express kuruluyor **Eğer Endpoint Sensor ve diğer gelişmiş özellikler kurulacaksa SQL Standart veya üstü gerekli, mevcutta varsa bunu kullanabilir yada SQL Standart veya üstü sürümleri de kurabilirsiniz*

Sonraki aşamada, eğer lisansımız yoksa veya henüz gelmediyse aşağıdaki linkten bir deneme lisansı talep ediyoruz, bu lisansın geçerlilik süresi 30 gün, lisans talebi için aşağıdaki bağlantıya gidiyoruz;

https://www.trendmicro.com/en_us/business/products.html

Bu sayfada "Endpoint Security with Apex One" başlığı altından "Free trial" bağlantısına tıklıyoruz, Free SaaS trial seçeneği Cloud hizmeti için, bununla şimdilik işimiz yok

Looking for home solutions? Under Attack? Alerts Support Resources Log In

TREND MICRO Business Solutions Platform Research Services Partners Company Free Trials Contact Us

User Protection Solution

Protection for your users on any device, any application, anywhere

Smart Protection Suites

Protection for all user activities with flexible licensing and deployment options

Learn more Free trial

Endpoint Security with Apex One

Automatic, insightful, all-in-one endpoint security

Learn more Free trial Free SaaS trial

Integrated Data Loss Prevention (IDLP)

Guards your private data and intellectual property with integrated modules

Learn more

Endpoint Application Control

Prevent unwanted and unknown applications from executing on your endpoints

Learn more

Daha sonra bu sayfada lisans talebi için istenen bilgileri dolduruyor ve "ÜCRETSİZ DENEME" butonuna tıklayarak işlemi tamamlıyoruz

Business

OfficeScan - Ücretsiz Deneme

Gelişmiş uç nokta ve ransomware korumasını 30 gün boyunca ücretsiz olarak deneyin

Dosyalarınızı, sunucularınızı, bilgisayarlarınızı, diz üstü bilgisayarlarınızı ve sanallaştırılmış masa üstü bilgisayarlarınızı koruyun

Kurumsal ağ içindeki veya dışındaki uç noktaları, kötü amaçlı yazılım, Truva atları, solucanlar, casus yazılım, ransomware'e karşı yeni çıkan bilinmeyen varyantlara karşı koruma sağlamak için uyum gösteren koruma sağlar.

Risk içermeyen ücretsiz deneme sürümünüzü kullanmaya başlayın ve tüm ürün özelliklerini deneyin:

- ✓ **Yüksek duyarlılıklı makine öğrenimi (yürütme öncesi ve çalışma zamanı)**
Herhangi bir kullanıcı aktivitesi ve herhangi bir uç nokta için güvenlik açıklarını ortadan kaldıran tehdit koruma tekniklerinin birleşimi
- ✓ **Davranışsal analiz**
Betik, ekleme, ransomware, bellek ve tarayıcı saldırılarına karşı koruma sağlar
- ✓ **Dosya ve web reputation**
Web alan adlarının güvenilirliğini izler

30 günlük ücretsiz deneme sürümünüzü kullanmaya başlamak için bu formu doldurun

Belirtilmediği sürece, tüm alanların doldurulması zorunludur.

Oturum Açmayı mı Tercih Ediyorsunuz? ⓘ

Ülke (Ülke adı girerek kullanılabilirliği kontrol edin)

Turkey

✓ Teşekkürler.

Adı

Orhan

Soyadı

Tan

E-posta (Bunu paylaşmayacağız)

orhan.tan@newexsecurity.com

Telefon Alan kodu dahil

+905555555555

Şehir

İstanbul

Şirket Adı

Şirket Adı

Şirketinizdeki küresel çalışan sayısı

☒ 0-100 ☐ 101-500 ☐ 501-5000 ☐ 5000+

☒ Trend Micro Lisans Sözleşmesi'ni okudum ve kabul ediyorum

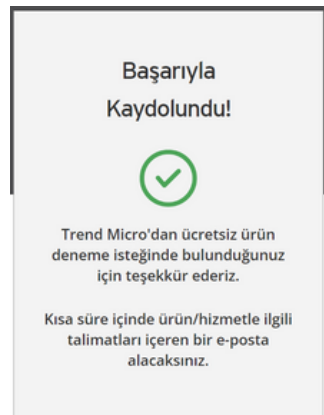
Trend Micro gizliliğinizi korur: [gizlilik ilkemizi okuyun](#)

İsteğe bağlı

☐ EVET, benim için bir Deneme Sürümü indirme hesabı oluşturun.
İleride işletmelere yönelik başka deneme sürümleri indirebileceğinizi düşünüyorsanız bu seçeneği işaretleyiniz.

ÜCRETSİZ DENEME >

Aşağıdaki ekranı gördüysek e-postamızı kontrol edebiliriz



Beklediğimiz e-posta gelen kutumuza iletilmiş.

no-reply

Trend Micro Deneme Sürümü Onayı - Trend Micro Sayın Orhan Tan, Apex One on-premise çözümüne göstermiş olduğunuz ilgi için teşekkürler. Trend Micro, güvenlik çözümlerinde bir dünya...

📧 🗑️ 📧 🕒

Lisans bilgileri aşağıdaki gibi görünecektir, bunu bir yere kaydediyoruz.

Trend Micro Deneme Sürümü Onayı

Gelen Kutusu x

no-reply@trendmicro.com

Alıcı: [Redacted]



Sayın Orhan Tan,

Apex One on-premise çözümüne göstermiş olduğunuz ilgi için teşekkürler. Trend Micro, güvenlik çözümlerinde bir dünya lideridir.

Aşağıda ürünlerinizin Etkinleştirme Kodlarını bulabilirsiniz (kurulum işlemini tamamlamak için bu alfa sayısal kodları girmeniz gerekecektir).

Ürün	Etkinleştirme Kodu
Apex One on-premise	OS-7RB7 [Redacted]
İndir	
Apex One (Windows)	Devam >
Apex One (Mac)	Devam >

Trend Micro'dan başka e-posta almak istemiyorsanız lütfen yazışma listemizden çıkmak için [buraya](#) tıklayın. Trend Micro gizliliğinize saygı gösterir.

Telif Hakkı © 2024 Trend Micro Incorporated. Tüm hakları saklıdır. Trend Micro ve Trend Micro t-ball logosu, Trend Micro Incorporated'ın ticari markaları ya da tescilli ticari markalarıdır. Tüm diğer şirket ve/veya ürün isimleri, sahiplerinin ticari markaları ya da tescilli ticari markaları olabilirler. Bu belgede bulunan bilgiler, bildirimde bulunmaksızın değiştirilebilir.



www.trendmicro.com

Apex One On-Prem Ürün Kurulumu

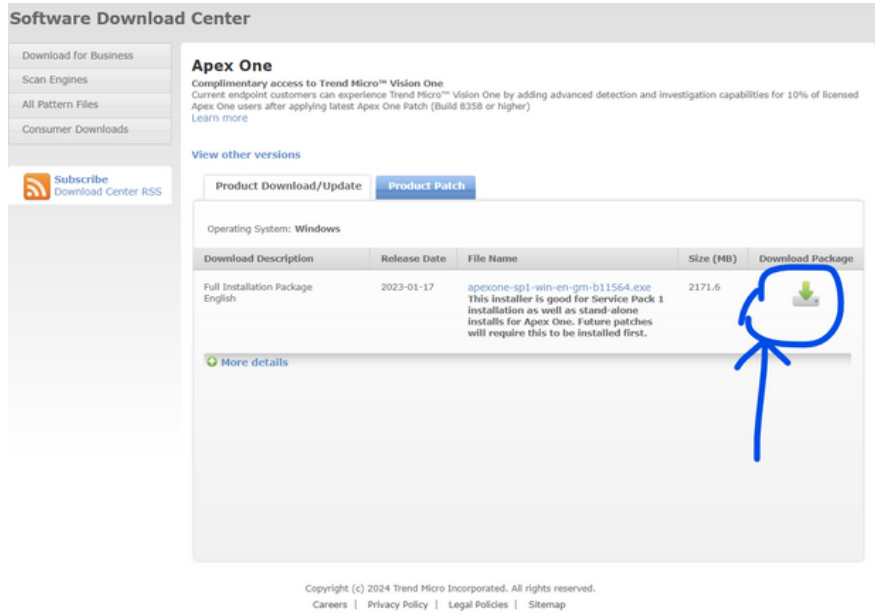
Apex One On-Prem sürümü kurmak için yapmamız gereken indirmeler var, bunun için aşağıdaki bağlantıya tıklıyoruz;

https://www.trendmicro.com/en_us/business/products/downloads.html

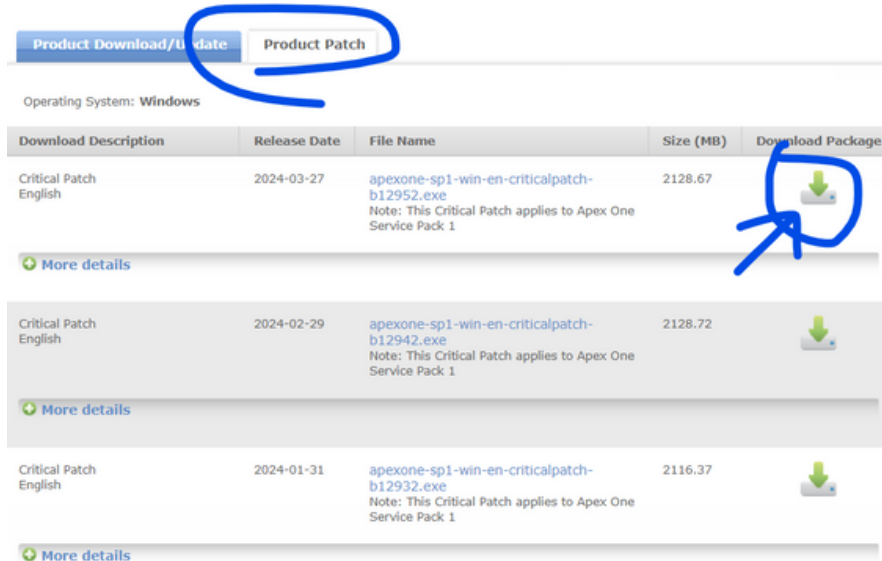
Bu sayfada "User Protection > Endpoint Security" başlığı altından "Apex One" seçeneğine tıklıyoruz.



Açılan sayfada "Product Download/Update" sekmesinden "Full Installation Package"i indiriyoruz



Ardından "Product Patch" sekmesinden yamaları indiriyoruz, eskiden buradan tüm yamaları sırayla indirmemiz gerekiyordu, artık son güncel yamayı indirmeniz yeterli



Kurulum

Kurulumu başlamadan önce sunucunun internete çıktığından emin olmamız lazım,

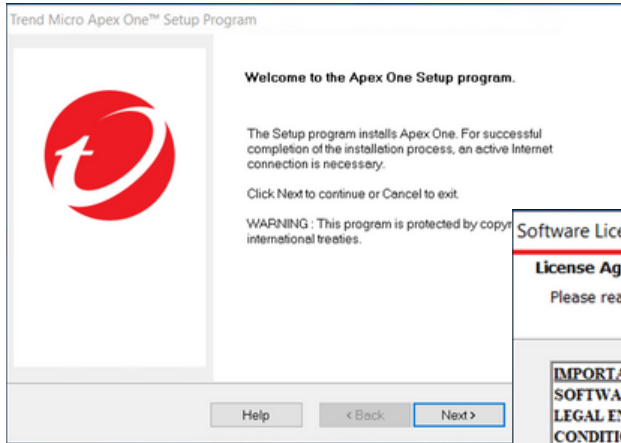
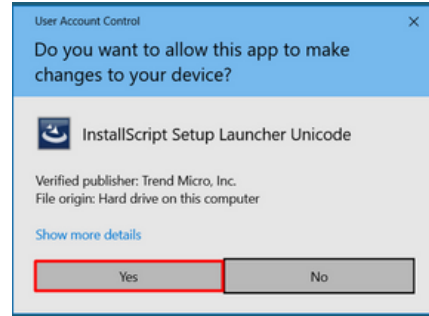
***.trendmicro.com adreslerine 80-443 portlarından erişmesi başlangıç için yeterlidir.**

Hazırladığımız makinede, kurulum/yama dosyaları ve gerekiyor ise SQL Standart ve üstü bir sürüm hazırsa, indirdiğimiz kurulum dosyasına çift tıklayarak kurulumu başlatıyoruz.

apexone-2019-win-en-all-in-one-b2012	2/5/2021 2:45 PM	Application	2,852,589 ...
--------------------------------------	------------------	-------------	---------------

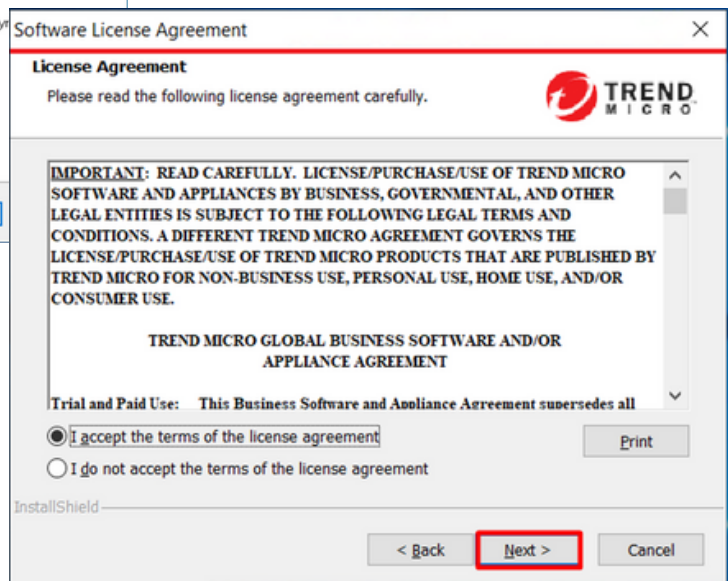


UAC uyarısı çıkarsa "Yes" diyoruz ve yükleme başlıyor.



Açılan ekranda "Next" diyerek devam ediyoruz.

Lisans sözleşmesini kabul ederek devam ediyoruz.



Trend Micro Apex One™ Setup Program

Installation Path

Specify the Apex One installation path. Accept the default path or specify a different location.

C:\Program Files (x86)\Trend Micro\Apex One

Browse...

InstallShield

< Back **Next >** Cancel

Yükleme path'ini seçiyoruz, ben varsayılan olarak bırakıyorum ve "Next" diyorum.

FQDN veya IP adresi ile kurabilirsiniz, tavsiyem DNS sunucularına erişimde sorun yoksa FQDN olarak kurmak olacaktır, ben o şekilde devam ediyorum ve "Next" diyorum.

Trend Micro Apex One™ Setup Program

Server Identification

Specify whether Security Agents identify the server by domain name or IP address.

Trend Micro recommends using the IP address when the server uses multiple network cards and using the fully qualified domain name (FQDN) or host name when the IP address is subject to change.

☒ Fully qualified domain name (FQDN) or host name: [demo] Tip: Before proceeding, verify that the domain name is resolvable.

☐ IP address: [192.168.0.101]
[fe80::9d0a:f07d:70af:2eff
6a80:9d0:1ba7:cd0f:ab5b]

InstallShield

Help < Back **Next >** Cancel

Trend Micro Apex One™ Setup Program

Web Server

Configure the Apex One IIS web server settings. Apex One uses the SSL connection settings for both the connection to the Apex One web console and server-agent communication.

IIS server: IIS virtual website

SSL Settings

Certificate validity period: 3 year(s)

SSL port: 4343

HTTP port: 8080 For legacy agent connection

InstallShield

Help < Back **Next >** Cancel

IIS virtual website olarak web servisini kuruyor, varsayılan olarak HTTPS/SSL portu 4343 olarak geliyor ve 3 yıllık bir sertifika ile kuruluyor, bu ayarları kurumunuzun ihtiyacına göre değiştirebilirsiniz, bu port ile Admin portala ulaşacağız.

"Next" diyerek devam ediyoruz.

Apex One On-Prem Ürün Kurulumu

Trend Micro Apex One™ Setup Program

Endpoint Sensor Installation



Before installing the Endpoint Sensor services, ensure that you have a valid license and have properly set up a supported SQL Server database.

☐ Install Endpoint Sensor

Endpoint Sensor database requirements:

- Version: SQL Server 2016 SP1 (or later)
- Note: SQL Server Express is not supported.
- Prerequisite settings: Enable "Full-Text and Semantic Extractions for Search"

Help

< Back

Next >

Cancel

Endpoint sensor özelliğini EDR gibi düşünebilirsiniz, kullanmak için bu kutucuğu seçebilirsiniz, bunun için kurulum öncesi de belirttiğim gibi SQL standart ve üstü bir sürüme ihtiyacınız olduğu burada yine hatırlatılıyor, ayrıca bu özellik ek lisans gerektirir, biz şu an için deneme lisansı ile kurduğumuz için bunu atlıyoruz ve "Next" diyoruz.

Ben deneme kurulumu yaptığım için kurulum ile gelen ve birlikte kurulan SQL Express'i kullanacağım, buraya bir şifre ve DB name veriyoruz ve "Next" diyoruz.

**Mevcutta SQL server'iniz var ise onu veya SQL'i ayrıca kurduysanız onun üzerinde database oluşturup bu bilgileri ekrana girebilirsiniz*

Trend Micro Apex One™ Setup Program

Apex One Database Setup



☒ Install/Create a new SQL Server Express instance (\\OFFICESCAN)

☐ SQL Server

[Hostname or IP address]InstanceName

Browse...

Database Authentication

Type:

☒ SQL Server Account

☐ Windows Account

User name:

sa

Password:

XXXXXXXXXX

Database Name

Apex One:

ApexOne

InstallShield

Bu ekranda Agent dağıtma paketleri hakkında özet bilgi veriyor, "Next" diyip geçiyoruz.

2 tip tarama metodu var, Agent'ı bu metodlara göre nasıl yükleyebiliriz, script destekler mi, boyutu ne olur? gibi bilgiler mevcut.

Varsayılan olarak Smart Scan metodu aktif gelir, merkezi bir DB'den imzaları kontrol eder, geleneksel antiviruslar gibi tüm agent'lara DB yollanmadığından her bir agent için ayrı DB kullanmaz, yeni bir DB yayınlandığında bunun tüm agent'lara ulaşması zaman alıyor ama Smart Scan method' da merkezi bir DB sunucusu var ve tüm agent'lar sorgularını buraya atıyor.

Trend Micro Apex One™ Setup Program

Apex One Security Agent Deployment



Use the information in this screen to plan the deployment of the Apex One Security Agent.

The size of the Apex One Security Agent package depends on the deployment method used, and the size of the components on the server during deployment.

The package sizes below reflect the size of the components when this product was shipped. The package sizes change each time the Apex One server updates the components.

Conventional scan method

Web installation: 250 MB (x86), 306 MB (x64)
Remote installation: 266 MB (x86), 342 MB (x64)
Login script (AutoPcc.exe): 404 MB (x86), 606 MB (x64)

Smart scan method

Web installation: 238 MB (x86), 294 MB (x64)
Remote installation: 245 MB (x86), 277 MB (x64)
Login script (AutoPcc.exe): 345 MB (x86), 454 MB (x64)

InstallShield

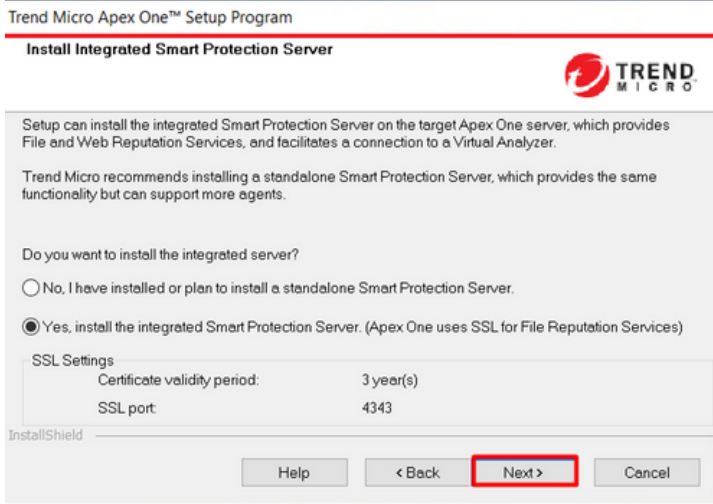
Help

< Back

Next >

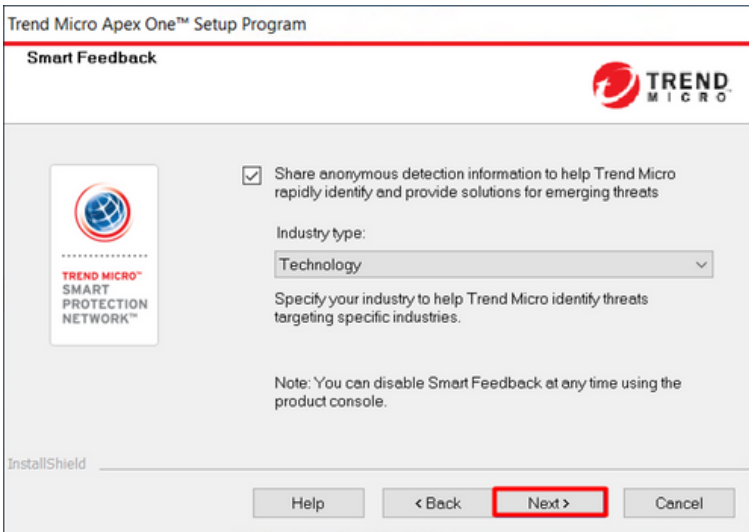
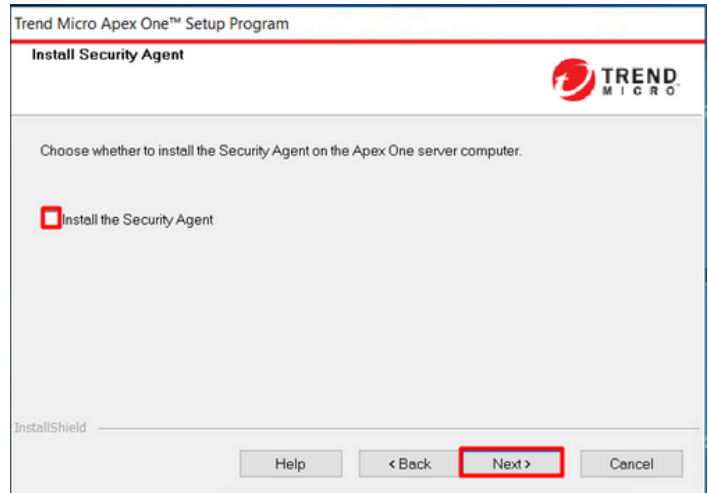
Cancel

Apex One On-Prem Ürün Kurulumu



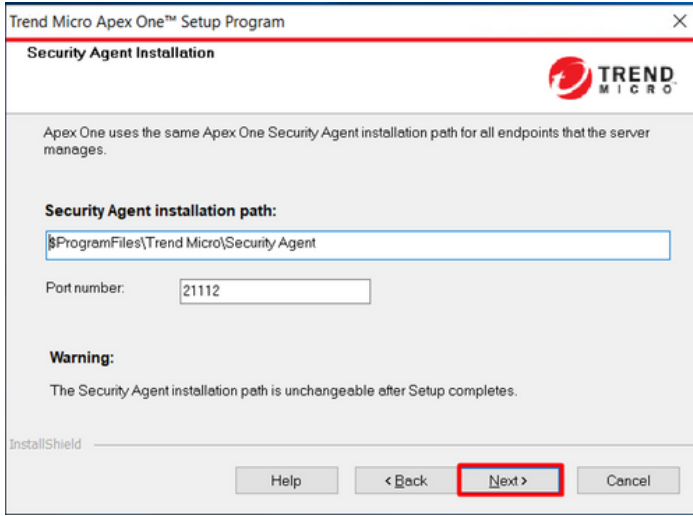
Bir önceki adımda bahsettiğim Smart Scan method kullanan agent'ların sorgularını atacağı Smart Protection Server'ı Apex One sunucusu ile entegre edebiliyoruz, biz hepsinin bu sunucuda olmasını istediğimiz için "Yes" seçeneğini seçerek "Next" diyoruz, bu sunucu üzerine kuracağız.

Kurulum yaptığımız sunucuya da agent yüklemek için bu kutucuğu seçiyoruz ve "Next" diyoruz.



Tespit edilen zararlıların bilgisini Trend Micro'ya geri bildirim olarak göndermek istersek bu kutucuğu seçiyoruz.

Eğer herhangi bir regülasyona tabi isek veya kurum politikalarınıza uygun değilse bunu kapatabiliriz.

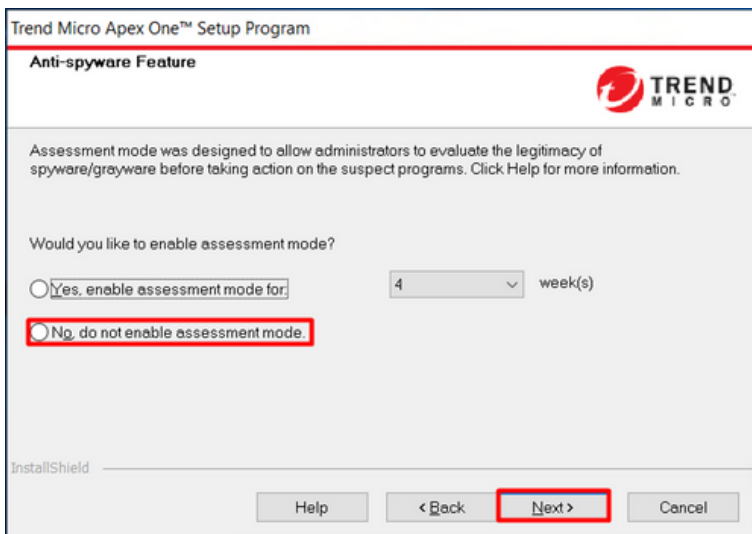
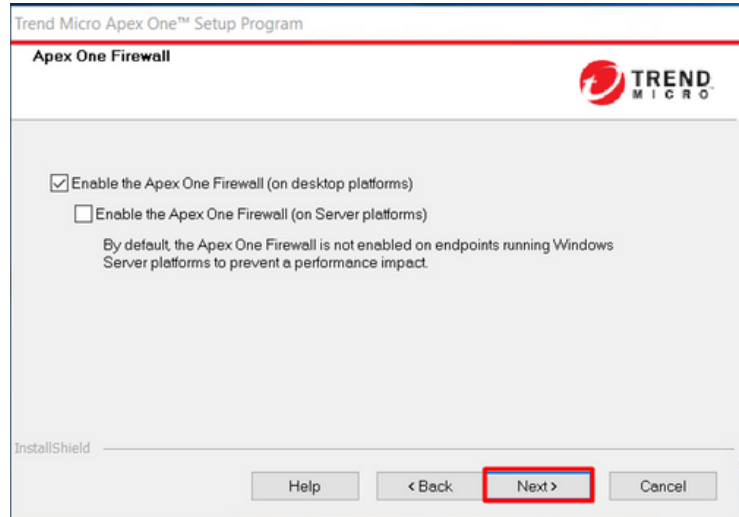


agent kurulum dosyalarının tutulacağı/oluşturulacağı path'i seçiyoruz, kolay erişim için farklı bir path seçebilirsiniz

Ben deneme olduğu için şimdilik varsayılan haliyle bırakıyorum ve "Next" diyerek ilerliyorum.

Agent'ın kurulu olduğu cihazdaki varsayılan firewall'ı Trend Micro ile değiştirmek için bu seçenekleri seçiyoruz, Desktop için kutucuğu seçiyorum, Server'larda bunu kullanmadığımız için ben kapalı tutuyorum ve ilerliyorum.

Kurum ihtiyaçlarınıza bağlı olarak bunu değiştirebilirsiniz.



Bu ekrandaki seçenek "Yes" olarak seçilip süre belirlenirse, Agent'lar yüklendikten sonra, seçtiğiniz süre boyunca cihazları Detect moda alıyor, biz bunu kullanmayacağımız için "No" diyerek devam ediyoruz.

Bu seçenek ile tespit edilen zararlılar loglanıyor ancak aksiyon alınmıyor.

Spesifik ve kritik bir yazılımınız var ise 1 hafta seçerek deneyebilir ve uygulamanızın davranışını nasıl analiz ettiğini gözlemleyebilirsiniz.

Trend Micro Apex One™ Setup Program

Web Reputation Services

Security Agents allow or block access to web pages based on Web Reputation policy settings. Select to enable the internal and external Web Reputation Services policies on Security Agents.

☒ Enable Web Reputation Services (on desktop platforms)
☐ Enable Web Reputation Services (on Server platforms)

InstallShield

Help < Back **Next >** Cancel

Web reputation servisi varsayılan olarak desktoplar için açık geliyor, bu şekilde ilerleyebilirsiniz.

Sonrasında ayarları değiştirebilirsiniz.

Bu ekranda bir tane authentication sertifika üretiliyor, bu sertifika şifresi önemli ve unutmamanız lazım, bir şifre verip ilerliyoruz.

Apex One agent'lar ile console arasındaki bağlantı için kullanıyor bu sertifikayı, bu sayede güvenli bir iletişim kurmuş oluyor.

Kurum ihtiyaçlarınıza bağlı olarak bunu değiştirebilirsiniz.

Trend Micro Apex One™ Setup Program

Server Authentication Certificate

Allow Apex One to generate a new certificate for communication with Apex One Security Agents, or import an existing certificate.
Note: Apex One creates a backup of the new or imported certificate in the <Server_installation_folder>\AuthCertBackup\ folder.

☒ Generate a new authentication certificate

Backup password:
Confirm password:

☐ Import an existing certificate
Note: The certificate is either a ZIP package generated by the Server Authentication Certificate Manager Tool or a properly formatted PFX file.

Browse

Password:

InstallShield

Help < Back **Next >** Cancel

Trend Micro Apex One™ Setup Program

Administrator Account Password

Specify the passwords for opening the web console or unloading/uninstalling the Apex One Security Agent. Passwords prevent unauthorized modification of web console settings or removal of the Apex One Security Agent.

Web console password:

Account:
Password:
Confirm password:

Apex One Security Agent unload and uninstall password:

Password:
Confirm password:

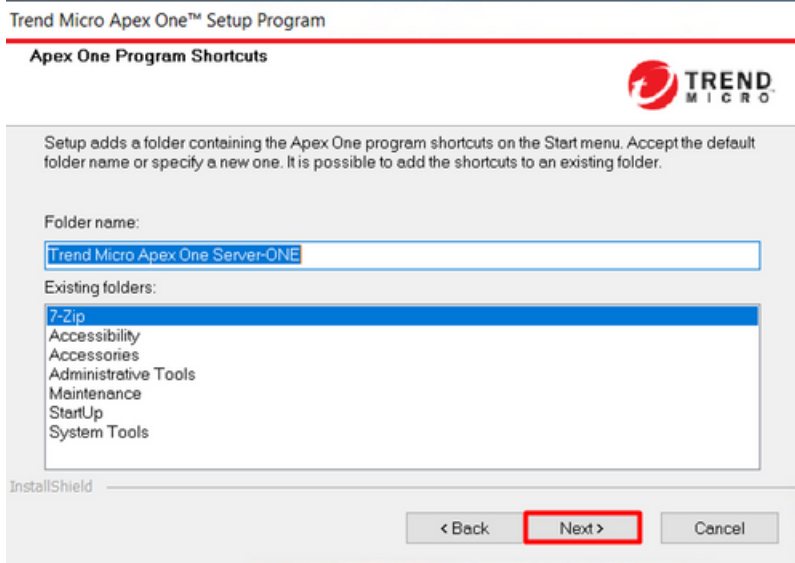
InstallShield

Help < Back **Next >** Cancel

Apex One Web Console için varsayılan admin hesabı **root**, buna bir şifre veriyoruz.

2. kısım ise agent'ları devre dışı bırakmak yada kaldırmak istendiğinde kullanmamız için gereken parola, buraya da bir şifre giriyoruz ve "Next" diyoruz.

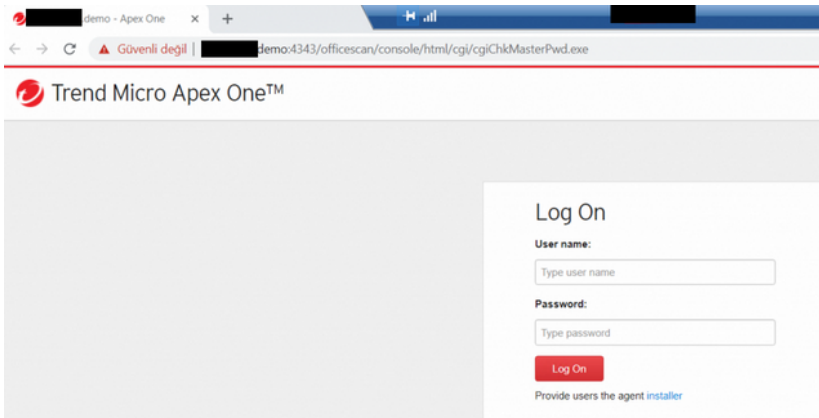
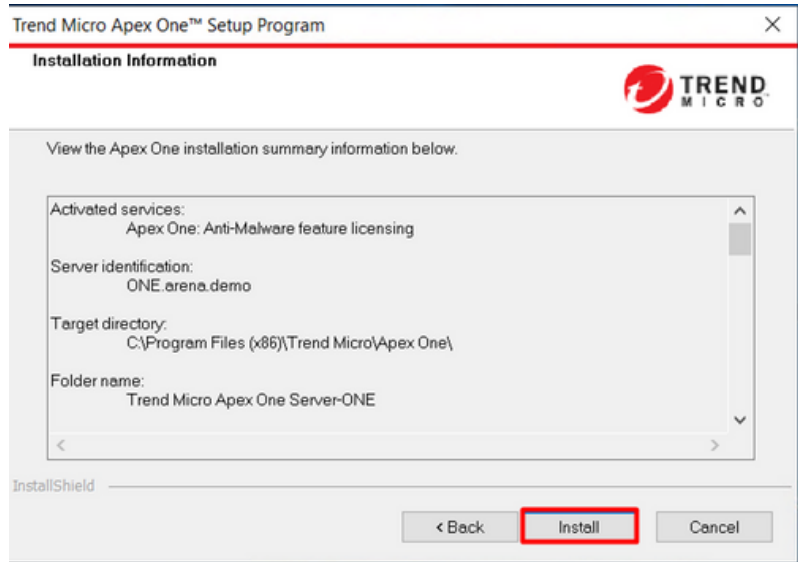
Apex One On-Prem Ürün Kurulumu



Apex One yazılımın başlat menüsündeki ismi belirtiyoruz, ben varsayılanda bıraktım ve "Next" dedim.

Sonrasında ayarları değiştirebiliyorsunuz.

Bir özet sayfası geliyor, tüm ayarları kontrol ettikten sonra "Install" butonu ile kurulumu başlatıyoruz ve bitene kadar hiçbir şeye dokunmuyoruz.



Yükleme bittikten sonra, masaüstünde bulunan "Launch the web console" kısayoluna tıklayarak Apex One web konsola erişebiliriz.

Kullanıcı adı: root
Şifre: kurulumda belirlenen şifre

Şimdilik hepsi bu kadar, panel, agent, policy ayarları ve diğer işlemler için sonraki dökümana geçebilirsiniz.