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.orhantan.com

iletisim@orhantan.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 aşamalardaki indirme işlemlerini bunun üzerinde yapacağız.

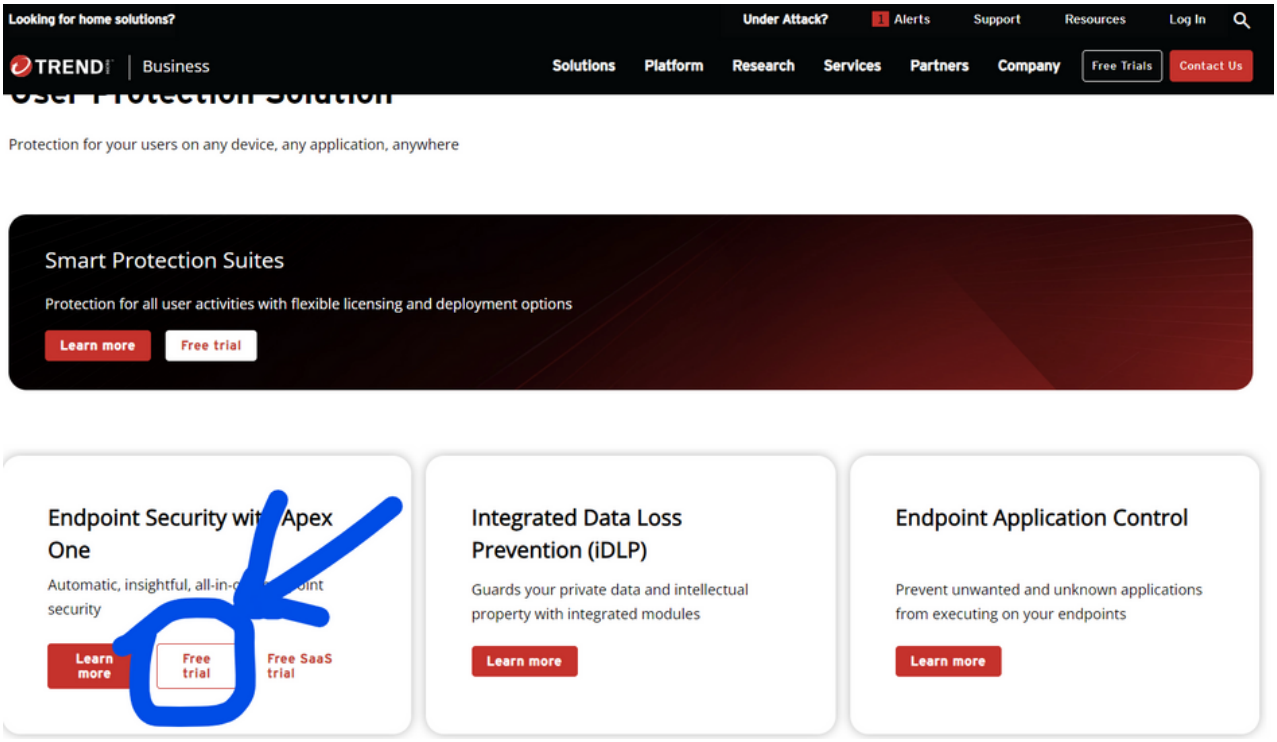
Bu makine için önerdiğimiz donanım aşağıdaki gibi olacak,

- 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;

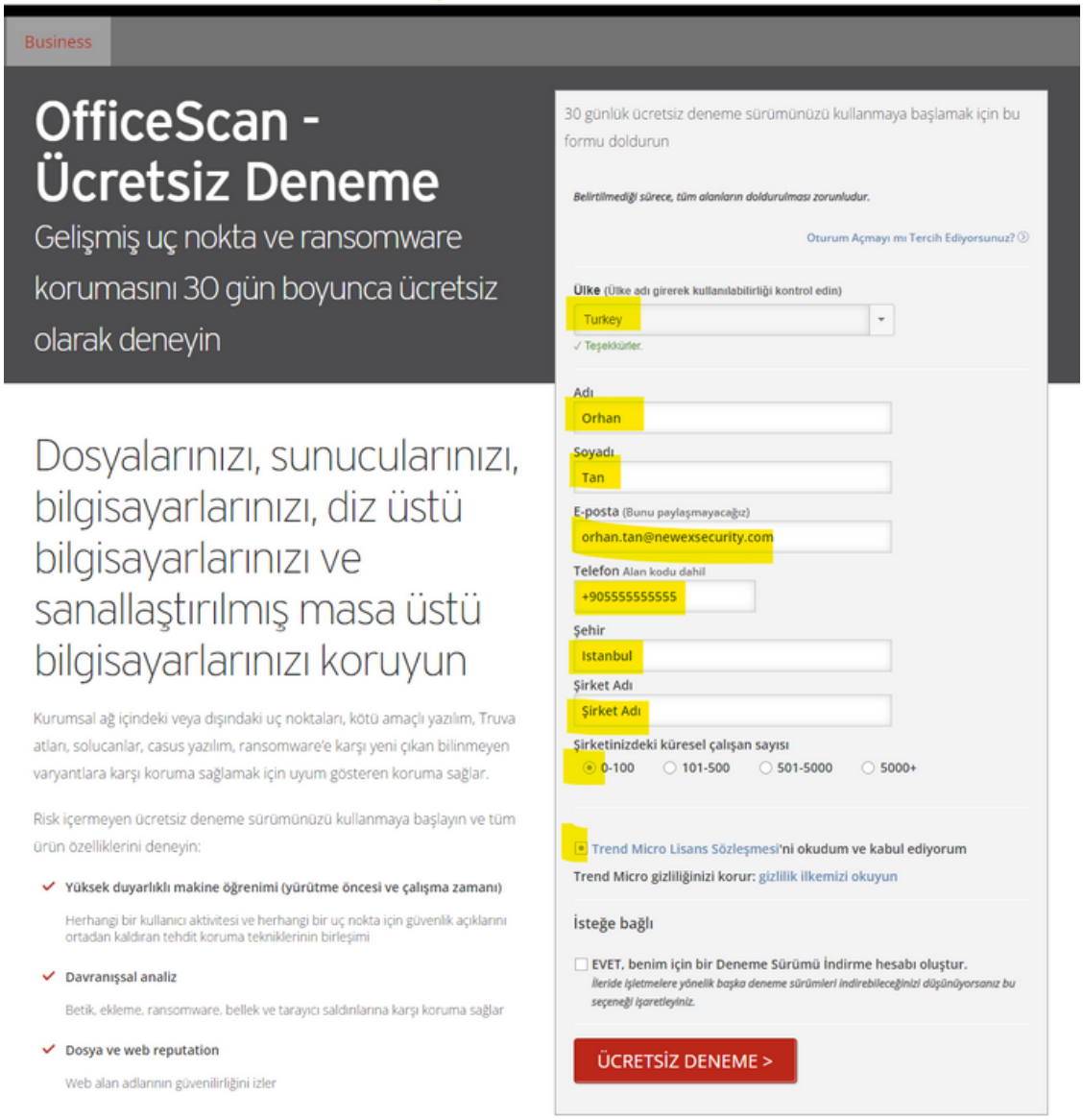
https://www.trendmicro.com/en_us/business/products.html

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

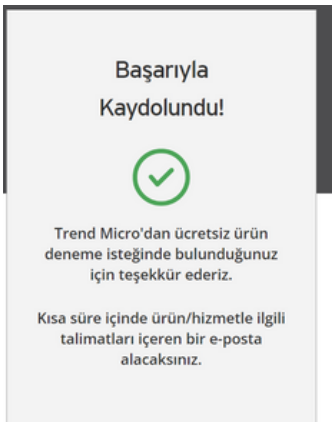


HAZIRLAYAN
Orhan Tan
Cyber Security Specialist
orhan.tan@newexsecurity.com
iletisim@orhantan.com
www.orhantan.com

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



Aşağıdaki ekranı gördüysek e-postamızı kontrol edebiliriz



Beklediğimiz e-posta gelen kutumuza iletilmiş.

Lisans bilgileri aşağıdaki gibi görünecektir, bunu bir yere kaydediyoruz.

Trend Micro Deneme Sürümü Onayı Gelen Kutusu ×

no-reply@trendmicro.com
Alıcı: [redacted]

TREND MICRO

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:

www.trendmicro.com

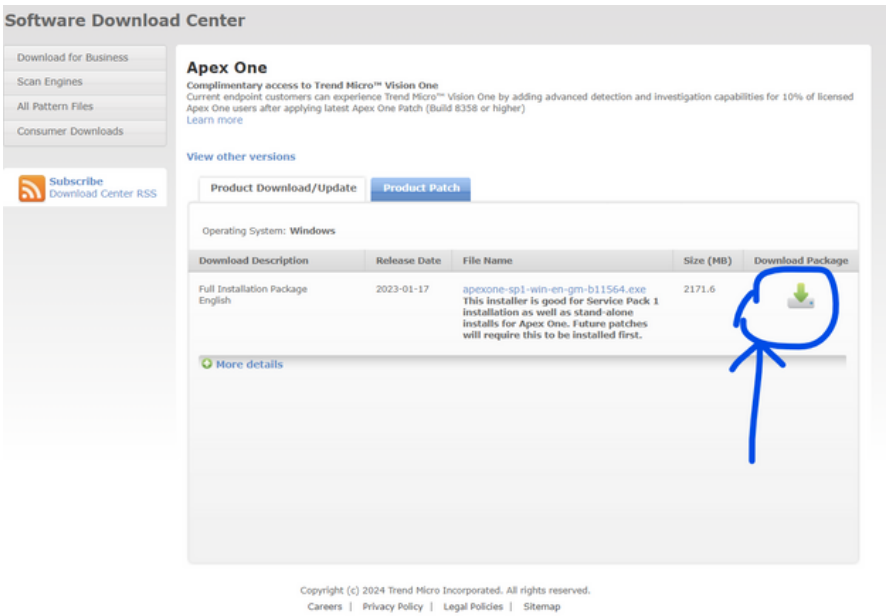
Apex One On-Prem Ürün Kurulumu

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

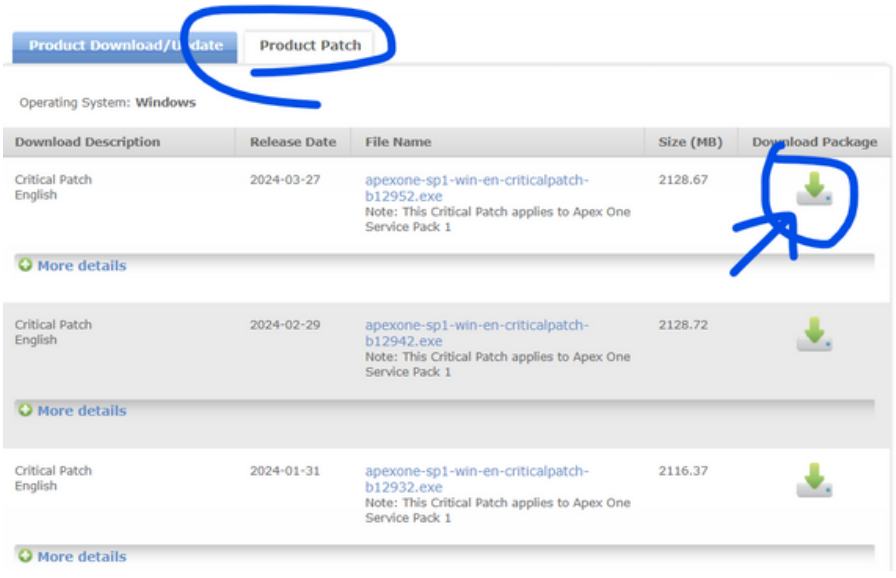
https://www.trendmicro.com/en_us/business/products/downloads.html

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



HAZIRLAYAN
Orhan Tan
Cyber Security Specialist
orhan.tan@newexsecurity.com
iletisim@orhantan.com
www.orhantan.com

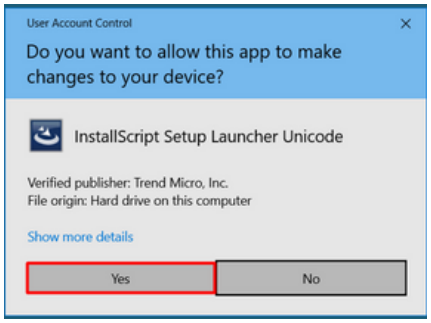
❑ Kurulum

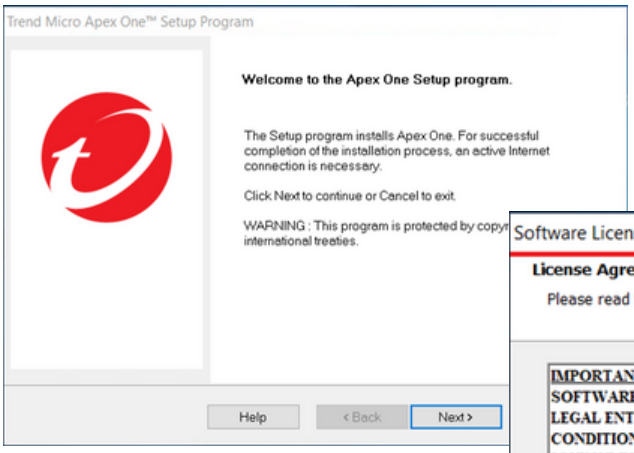
Kuruluma başlamadan önce sunucunun internete çıktığından emin olmamız lazım,

*.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.

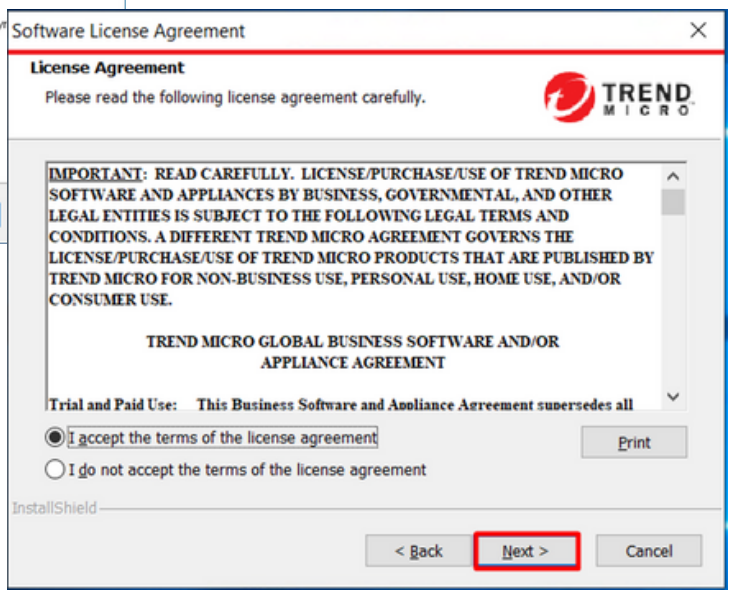
UAC uyarısı çıkarsa “Yes” diyoruz ve yükleme başlıyor.





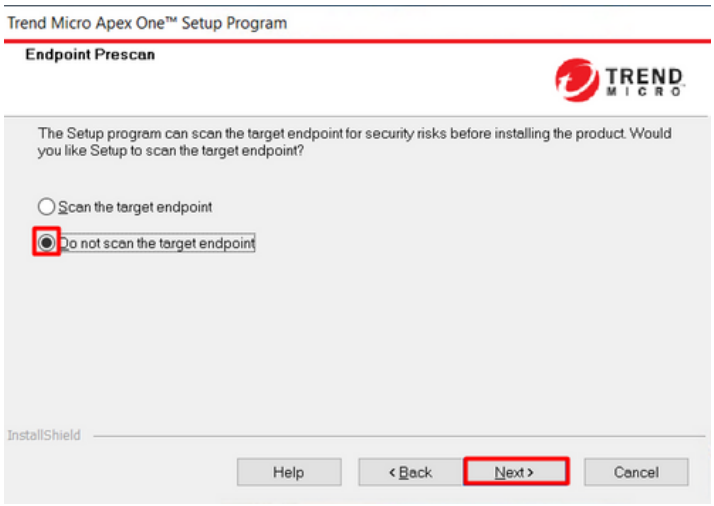
Açılan ekranda “Next” diyerek devam ediyoruz.

Lisans sözleşmesini kabul ederek devam ediyoruz.



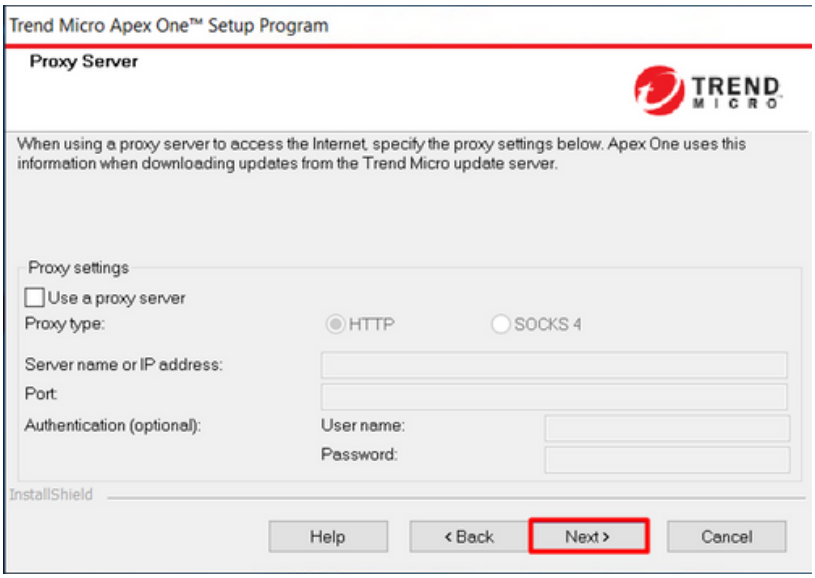
HAZIRLAYAN
Orhan Tan
Cyber Security Specialist
orhan.tan@newexsecurity.com
iletisim@orhantan.com
www.orhantan.com

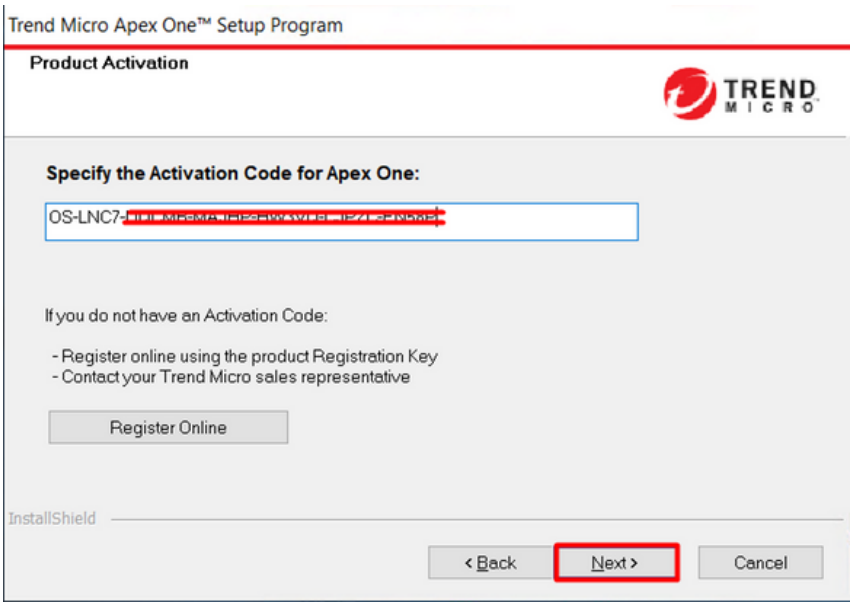
Apex One On-Prem Ürün Kurulumu



Yükleme yapmadan önce kurulumun yapılacağı sunucuyu taramasını istiyorsak "Scan the target endpoint" seçeneğini seçiyoruz, sunucumuz temiz kurulum olduğu için biz şu an buna ihtiyaç duymayacağımızdan bir alttaki seçeneği seçerek "Next" diyorum ben.

Proxy kullanılıyor veya kullanılacaksa gerekli ayarları yapıyoruz, biz direkt bağlantı sağladığımız için bu ekranı "Next" diyerek geçiyorum.

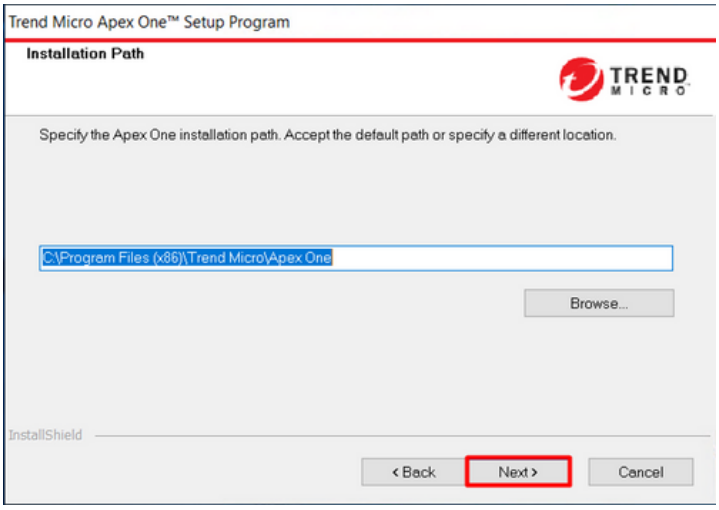




E-posta adresimize gelen lisans anahtarını bu ekrana giriyoruz ve "Next" diyoruz.

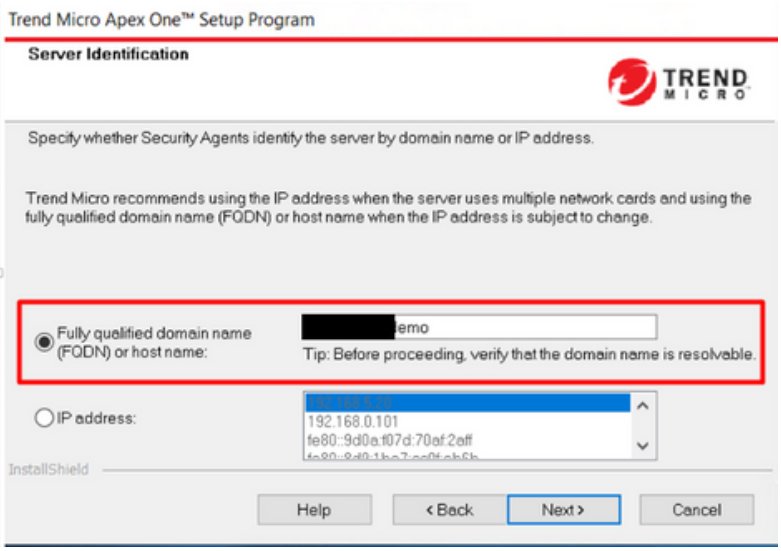
HAZIRLAYAN
Orhan Tan
Cyber Security Specialist
orhan.tan@newexsecurity.com
iletisim@orhantan.com
www.orhantan.com

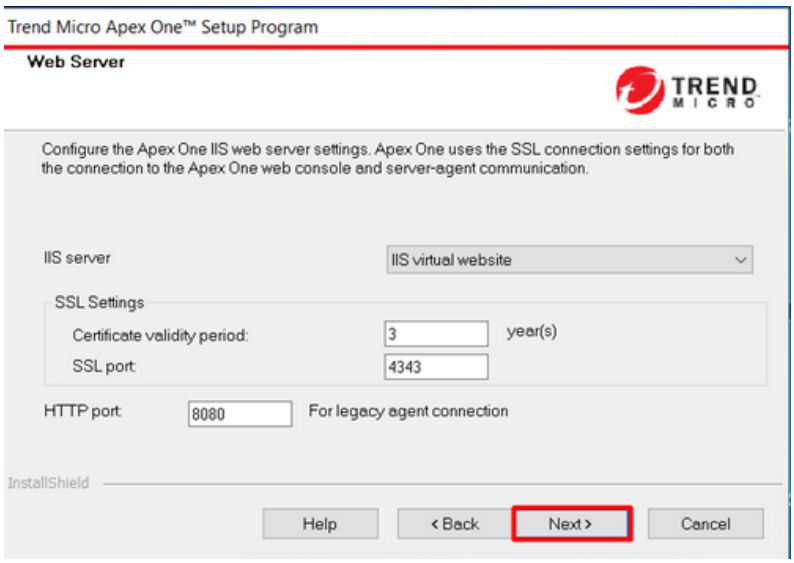
Apex One On-Prem Ürün Kurulumu



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.

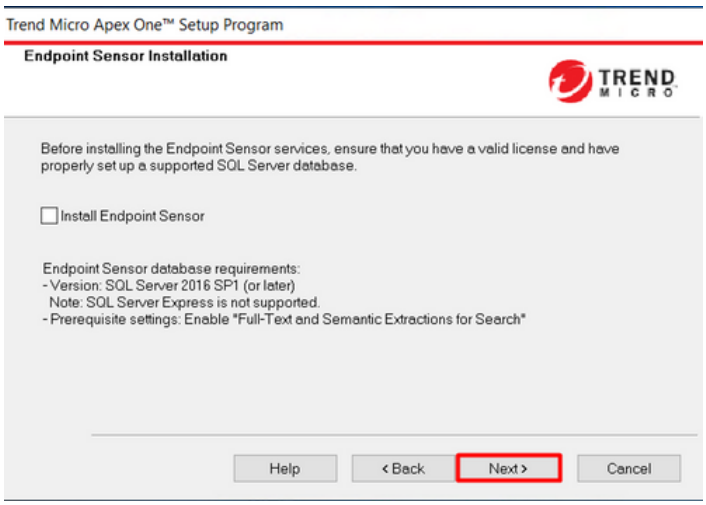




IIS virtual website olarak web servisini kuruyor, varsayılan olarak HTTPS/SSL portu 4343 olarak geliyor ve 3 yıllık bir sertifika ile kuruluyor, bu ayarları kurumunuzun ihtiyacına göre değiştirebilirsiniz, bu port ile Admin portala ulaşacağız.

"Next" diyerek devam ediyoruz.

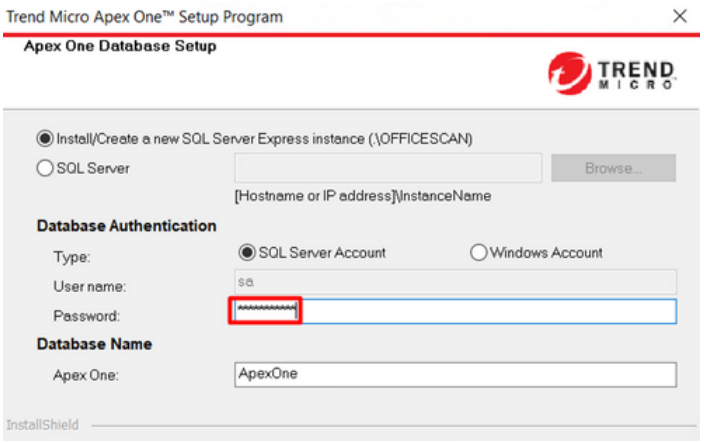
Apex One On-Prem Ürün Kurulumu

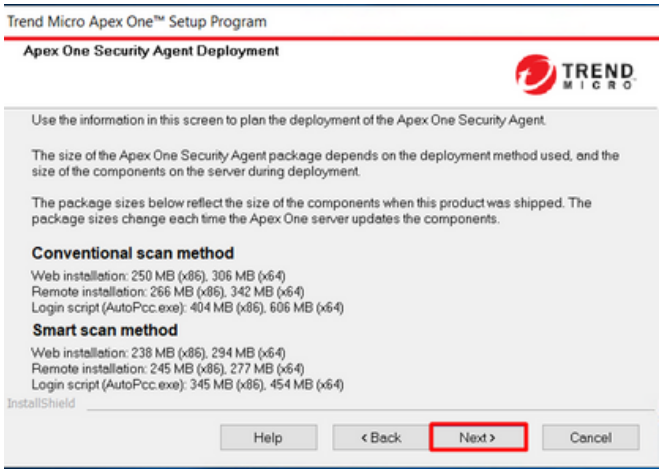


Endpoint sensor özelliğini EDR gibi düşünebilirsiniz, kullanmak için bu kutucuğu seçebilirsiniz, bunun için kurulum öncesi de belirttiğim gibi SQL standart ve üstü bir sürüme ihtiyacınız olduğu burada yine hatırlatılıyor, ayrıca bu özellik ek lisans gerektirir, biz şu an için deneme lisansıyla kurduğumuz 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'ınız var ise onu veya SQL'i ayrıca kurduysanız onun üzerinde database oluşturup bu bilgileri ekrana girebilirsiniz*





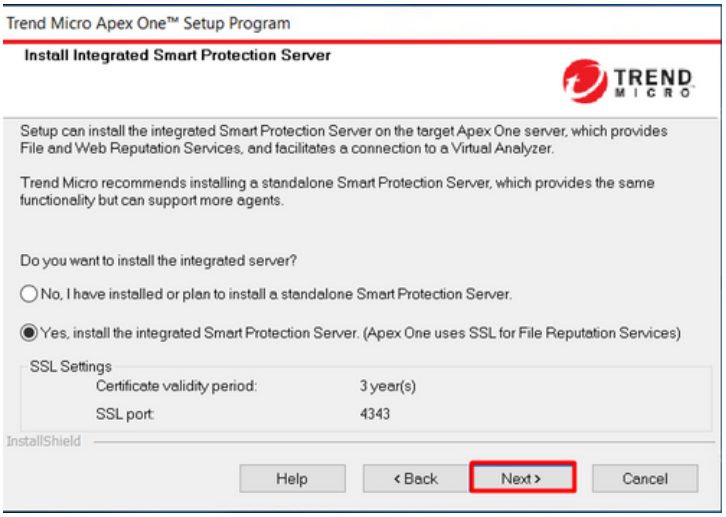
Bu ekranda Agent dağıtma paketleri hakkında özet bilgi veriyor, "Next" diyip geçiyoruz.

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

Varsayılan olaran Smart Scan metodu aktif gelir, merkezi bir DB'den imzaları kontrol eder, geleneksel antivirusler 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.

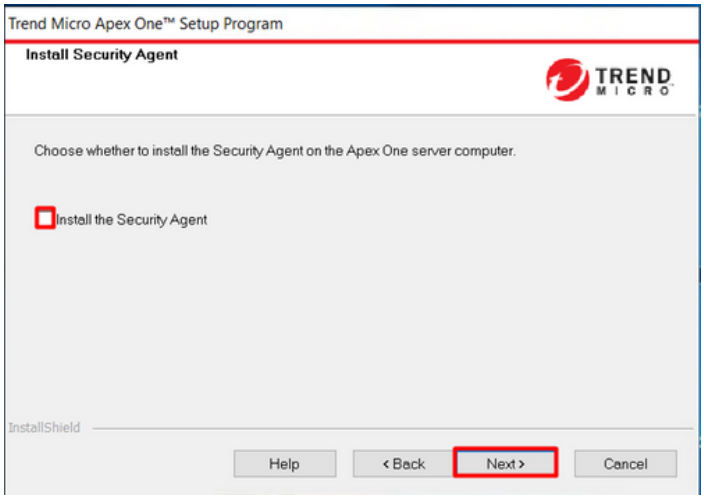
HAZIRLAYAN
Orhan Tan
Cyber Security Specialist
orhan.tan@newexsecurity.com
iletisim@orhantan.com
www.orhantan.com

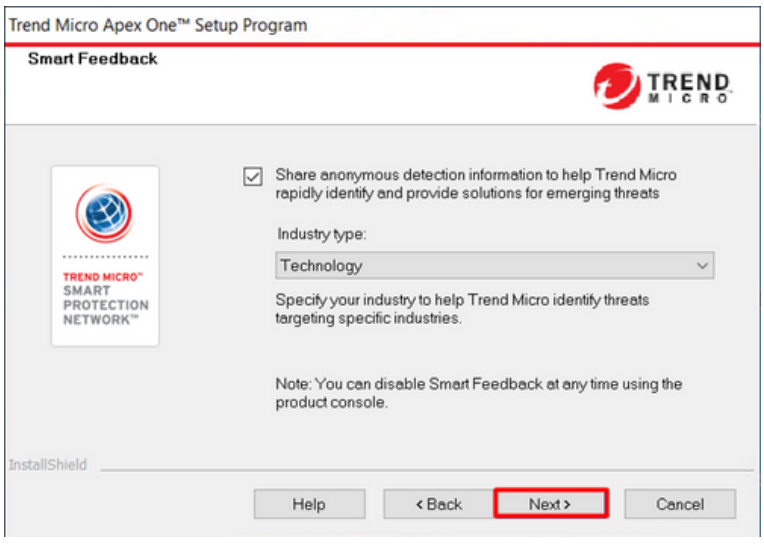
Apex One On-Prem Ürün Kurulumu



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.



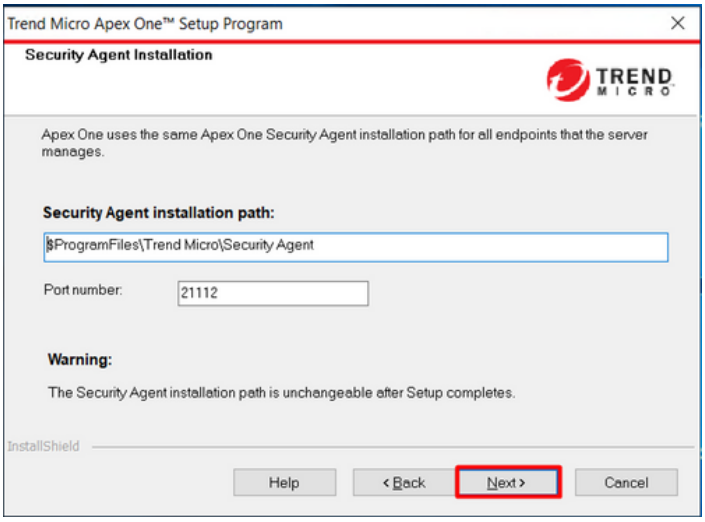


Tespit edilen zararlıların bilgisini Trend Micro' ya geri bildirim olarak göndermek istersek bu kutucuğu seçiyoruz.

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

HAZIRLAYAN
Orhan Tan
Cyber Security Specialist
orhan.tan@newexsecurity.com
iletisim@orhantan.com
www.orhantan.com

Apex One On-Prem Ürün Kurulumu

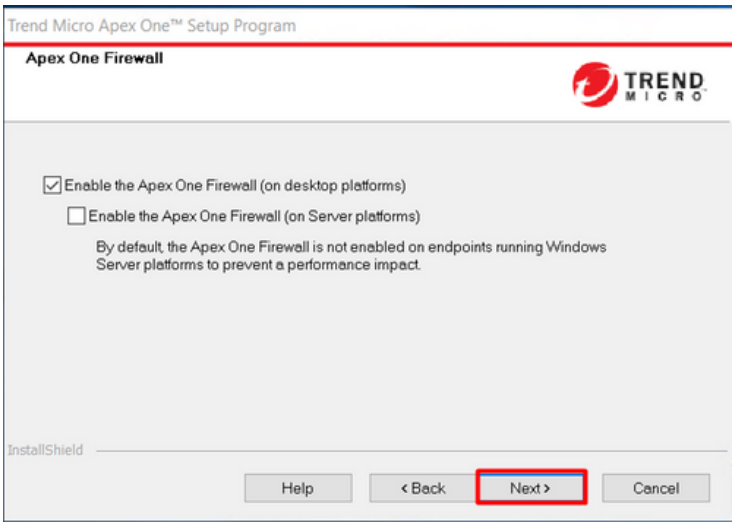


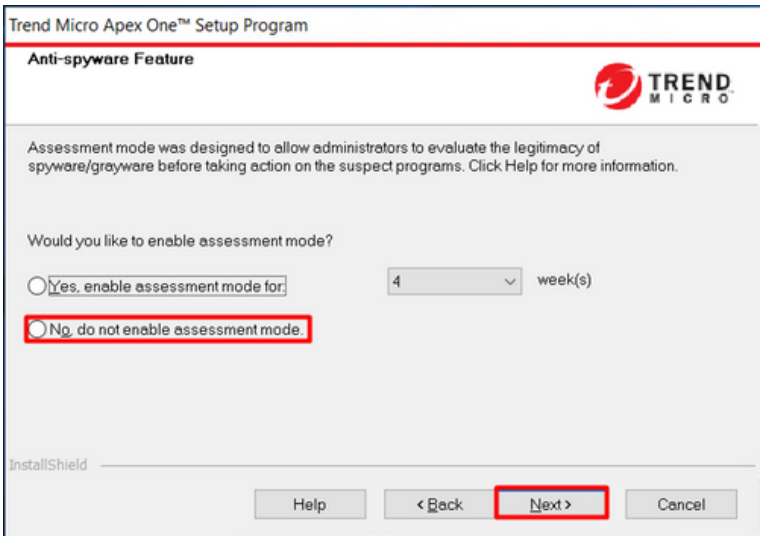
agent kurulum dosyalarının tutulacağı/oluşturulacağı path'i seçiyoruz, kolay erişim için farklı bir path seçebilirsiniz

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

Agent'ın kurulu olduğu cihazdaki varsayılan firewall'u 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.





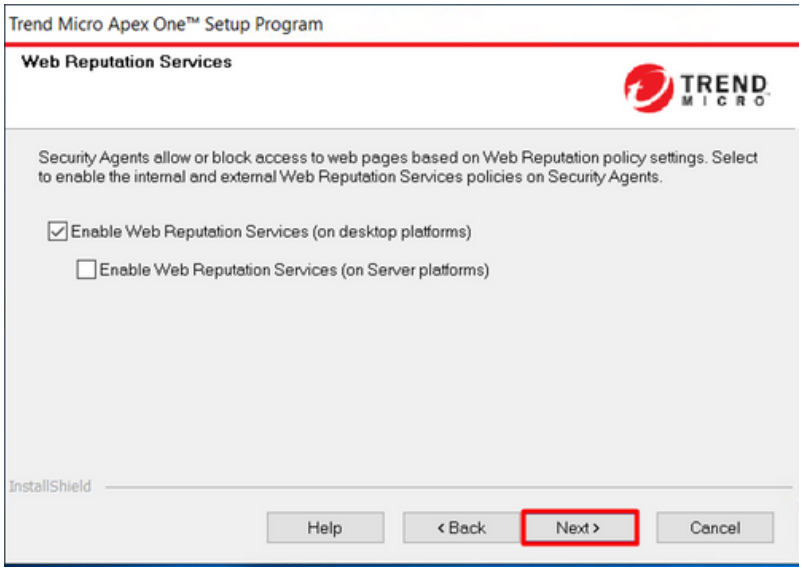
Bu ekrandaki seçenek "Yes" olarak seçilip süre belirlenirse, Agent'lar yüklendikten sonra, seçtiğiniz süre boyunca cihazları Detect moda alıyor, biz bunu kullanmayacağımız için "No" diyerek devam ediyoruz.

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.

HAZIRLAYAN
Orhan Tan
Cyber Security Specialist
orhan.tan@newexsecurity.com
iletisim@orhantan.com
www.orhantan.com

Apex One On-Prem Ürün Kurulumu



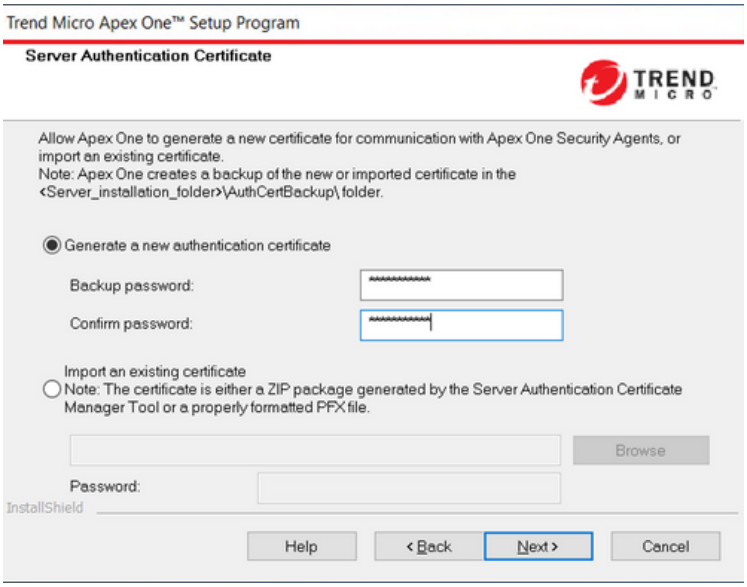
Web reputation servisi varsayılan olarak desktoplar için açık geliyor, bu şekilde ilerleyebilirsiniz.

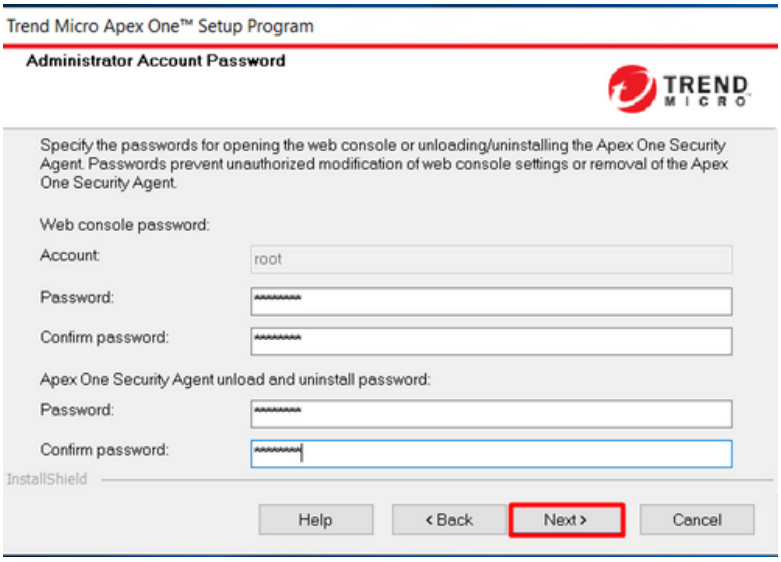
Sonrasında ayarları değiştirebiliyorsunuz.

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.



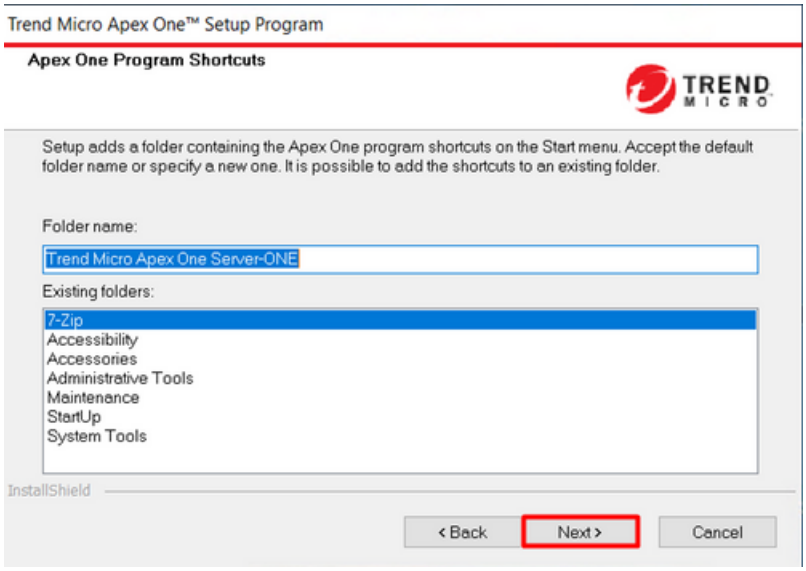


Apex One Web Console için varsayılan admin hesabı **root**, buna bir şifre veriyoruz.

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

HAZIRLAYAN
Orhan Tan
Cyber Security Specialist
orhan.tan@newexsecurity.com
iletisim@orhantan.com
www.orhantan.com

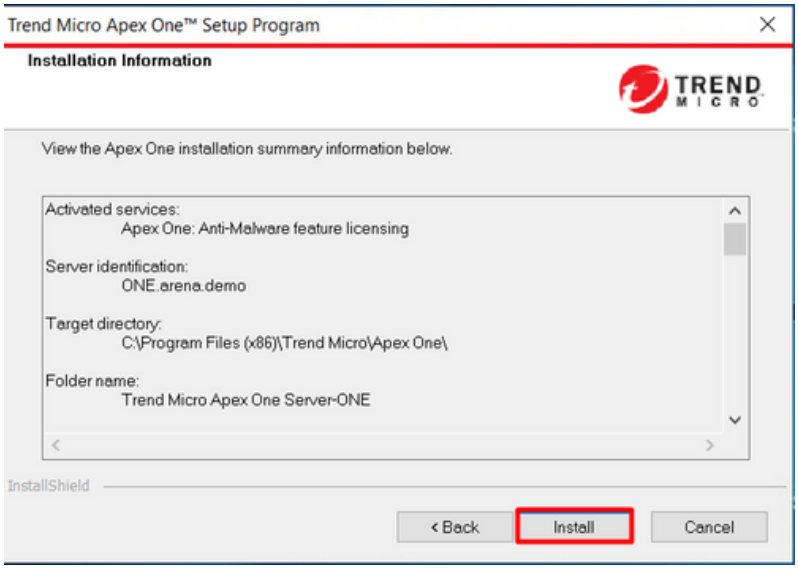
Apex One On-Prem Ürün Kurulumu

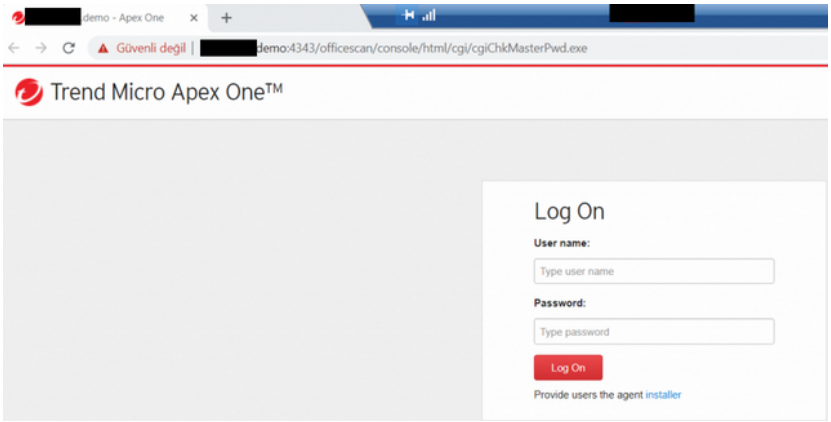


Apex One yazılımın başlat menüsümdeki ismi belirtiyoruz, ben varsayılanda bıraktım ve “Next” dedim.

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.

HAZIRLAYAN
Orhan Tan
Cyber Security Specialist
orhan.tan@newexsecurity.com
iletisim@orhantan.com
www.orhantan.com