

Remote Access

Forti EMS üzerinde her bir gruba farklı güvenlik prosedürleri uygulamak gerekebiliyor. Bu isteği karşılayabilmek için “Endpoint Profiles” sekmesi altında bulunan güvenlik özelliklerinin ne için kullanıldığı ve nasıl ayarlandığının bilinmesi gerekiyor. Bu yazıda Endpoint Profiles sekmesi altındaki Remote Access güvenlik özelliğinin kullanım amacını ve nasıl konfigüre edildiği açıklanmaya çalışılacaktır.

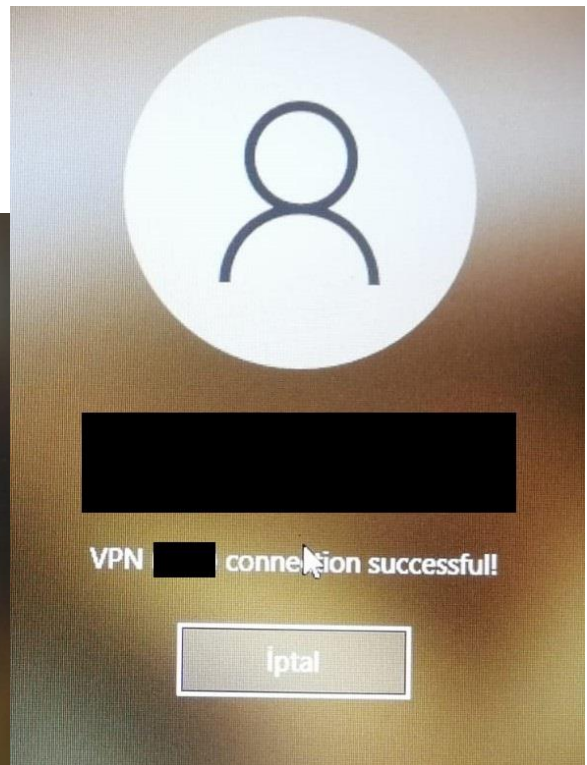
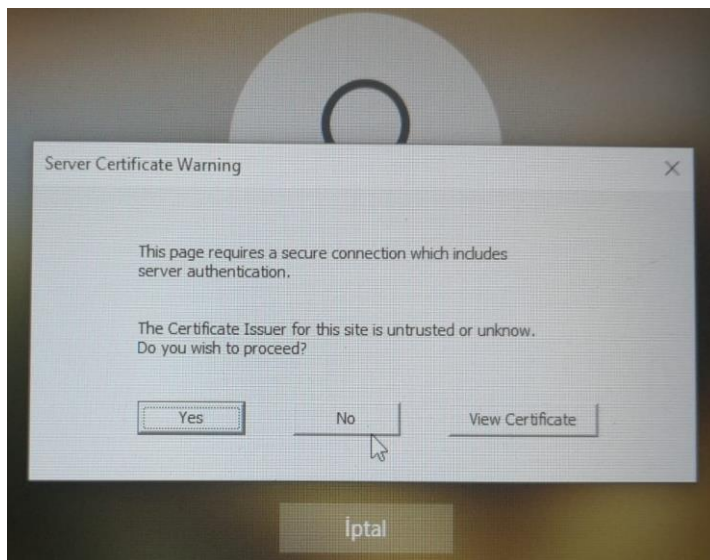
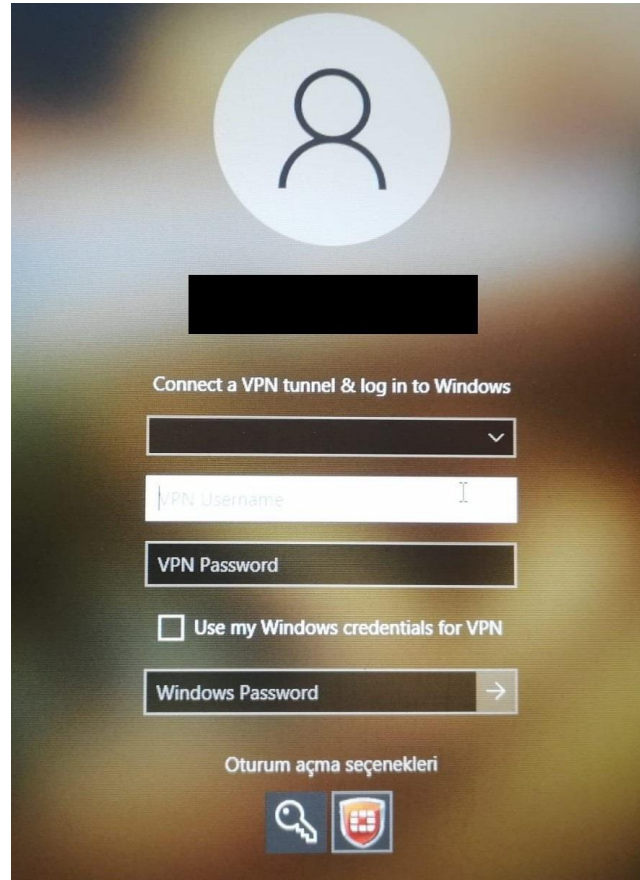
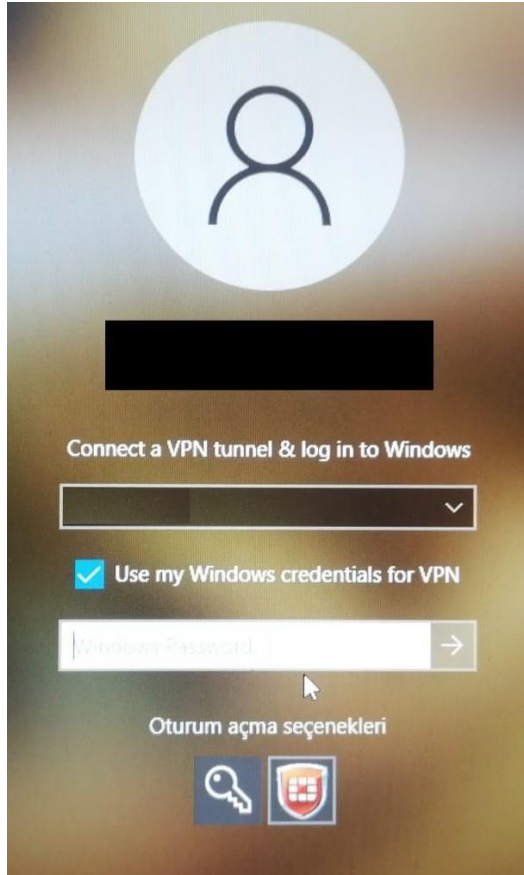
Remote Access

Remote Access sekmesi, istemcilere yüklenecek Agent üzerinden kullanılacak uzak bağlantı türüne yönelik parametrelerin ayarlanması için kullanılmaktadır. Burada tanım yapabilmek için “**Endpoint Profiles -> Remote Access -> Add**” yolu izlenmelidir. Burada;

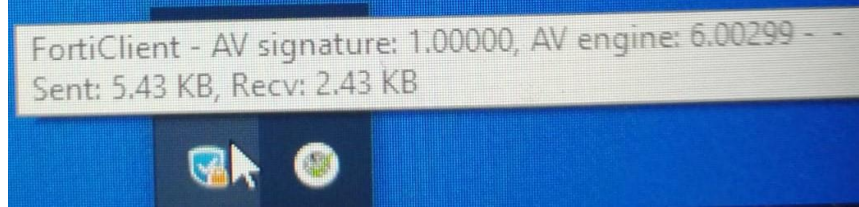
- İlk olarak oluşturulacak Remote Access Profile tanımına bir isim verilmeli ve Profile tanımı devreye alınmalıdır.

GENERAL

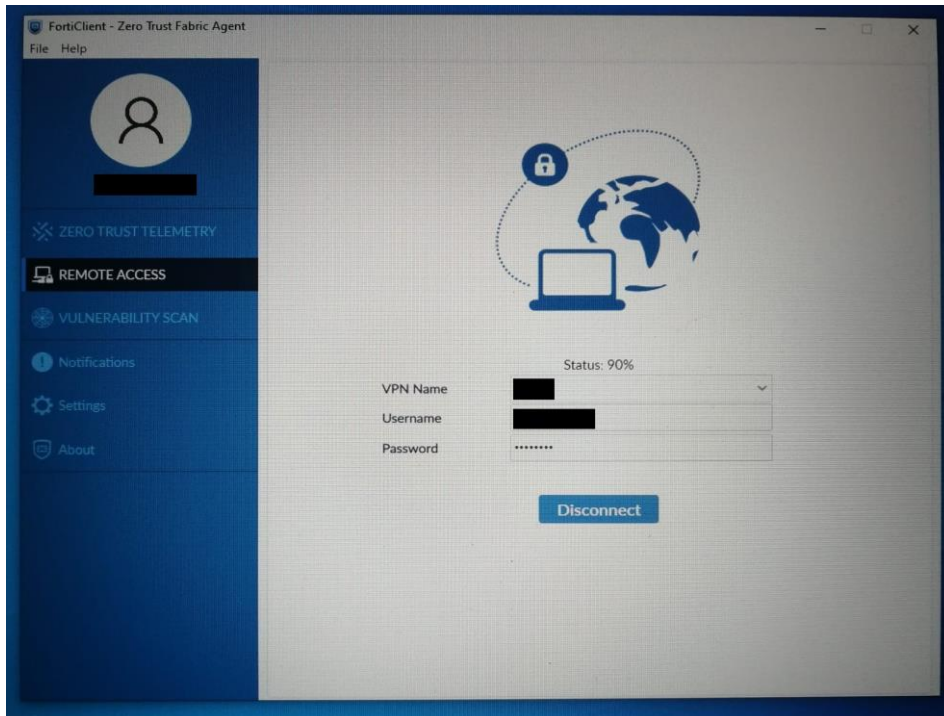
- **Allow Personnel VPN** -> Kullanıcıların FortiClient üzerindeki VPN ayarlarında değişiklik yapabilmesine izin verilip verilmeyeceğini belirleyen seçenektir. Kullanıcının cihazıyla farklı bir FW’a VPN olması gerekebilir veya farklı kullanıcı bilgileriyle oturum açması gerekebilir. Bu durumda VPN ayarlarında değişiklik yapmasına izin verilmesi gerekecektir.
- **Show VPN Before Logon** -> Kullanıcıların cihazlarında oturum açmadan önce (Windows oturum açma ekranı geldiğinde) FortiClient istemcisinin otomatik olarak başlatılmasını ve VPN bağlantısının kurulmasını sağlayan özelliktir.
 - o **Use Windows Credentials** -> **Show VPN Before Logon** seçeneği devreye alındığında VPN olmak için kullanıcının işletim sisteminde oturum açarken kullandığı oturum açma bilgilerinin mi yoksa farklı kullanıcı bilgileriyle mi VPN olunacağı belirlenmelidir.
 - o Şirketlerde hassas verilerin korunması gereken durumlarda, kullanıcıların sisteme yalnızca güvenli bir VPN bağlantısı üzerinden erişmesini sağlamak için bu özellik kullanılabiliyor.



- **Minimize FortiClient Console on Connect** -> Kullanıcıların VPN olduğunda FortiClient uygulamasının otomatize şekilde küçülerek bilgisayarın köşesindeki görev tepsisinde ikon olarak konumlanmasını sağlar (VPN olunduktan sonra pencereyi kapatmaya gerek kalmıyor).
 - o VPN bağlantısının durumu hakkında bilgiyi sistem tepsisindeki simgeler aracılığıyla kolayca görebilir. Bu sayede istemciyi sürekli açık tutmaya gerek kalmadan, bağlantı durumunu denetlemelerini sağlar.



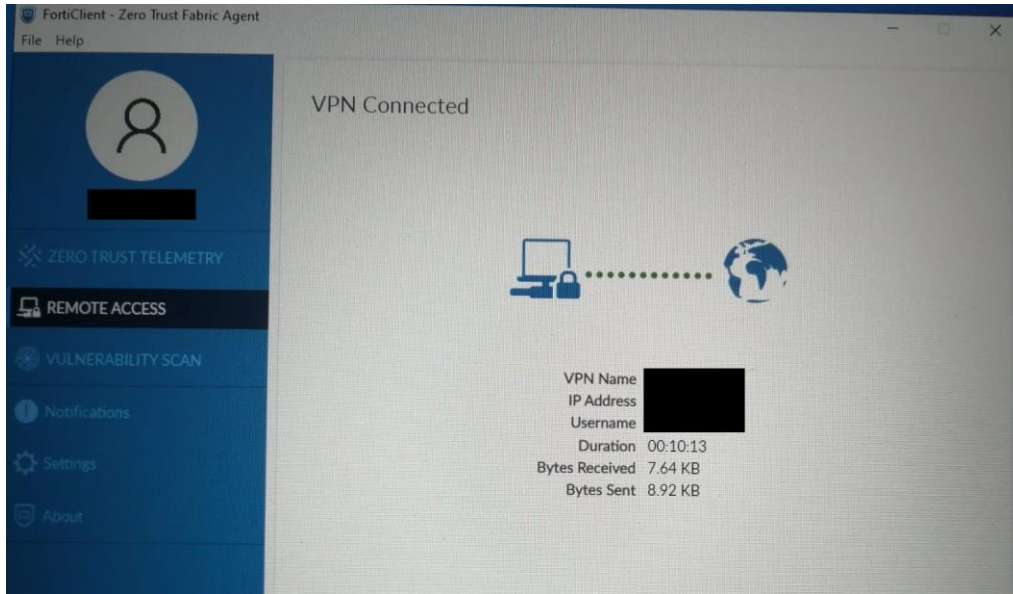
- **Show Connection Progress** -> Kullanıcılar VPN olurken bağlantı sürecinin hangi aşamada olduğunu kullanıcıya görsel olarak gösterilmesini sağlayan özelliktir.
 - o Eğer VPN bağlantısı uzun sürüyorsa veya bir sorun meydana gelirse sorunun hangi aşamada oluştuğunu daha kolay anlayabilmeleri adına kullanılabilir. Bu sayede sorun çözme aşamasında sorunun daha hızlı anlaşılması ve giderilmesi sürecinde Teknik destek ekiplerine de faydası olacaktır. Örnek olarak bağlantı süreci %48'de kalıyorsa bu kullanıcı bilgilerinin doğru olmadığını gösterecektir.



- **Suppress VPN Notifications** -> FortiClient istemcisi ile VPN olunması veya VPN bağlantısının kesilmesi gibi durum değişimlerinde kullanıcıya bildirim gönderilmesini önlemek için kullanılan özelliktir.
 - o Kullanıcıların sürekli VPN bağlantısı kurduğu, fakat bağlantı bildirimlerinin rahatsız edici olduğu durumlarda (örneğin, sürekli mobil veya uzak ofis bağlantıları) veya VPN bağlantısının arka planda sürekli aktif kalması gereken durumlarda (örneğin, bir yazılımın sürekli olarak ağ kaynaklarına erişmesi gereken durumlarda), bu özellik aktif hale getirilebilir.
- **Use Vendor ID** -> FortiClient istemcisinin VPN bağlantısı sırasında kullanılan kimlik doğrulama süreci ile ilgili olarak VPN sunucusuna ek bir kimlik doğrulama bilgisi sağlamak için kullanılır. Bu özellik, özellikle VPN bağlantılarının güvenliğini artırmak amacıyla, istemciden sunucuya bir **Vendor ID** değerini iletilmesi için yapılandırılır.
 - o Eğer ağda birden fazla VPN sunucusu ve istemcisi varsa ve bu cihazlar farklı satıcılardan geliyorsa, Vendor ID kullanımı, doğru istemcinin doğru sunucuya bağlanmasını garanti edecektir.
- **Enable Secure Remote Access** -> Uzaktan erişim sürecini daha güvenli hale getirmek için kullanılan bir güvenlik özelliğidir. Özellikle VPN olup uzaktan çalışan kullanıcıların, ağ kaynaklarına ve uygulamalara daha güvenli bir VPN bağlantısı üzerinden erişmesini sağlamaya yönelik ek güvenlik önlemleri sunar. Özellik burada devreye alındıktan sonra uygulanması istenen özelliklerin ayarlanması **Zero Trust Tags** sekmesinde yapılmaktadır. Bu özellik ile uygulanabilecek ek güvenlik özelliklerinden birkaçına bakıldığında (Detayları “**Zero Trust Tags**” notlarında bulabilirsiniz);
 - En son AV imzalarına sahip olmayan uç noktaların, kritik güvenlik açıklarına sahip istemcilerin VPN tüneline bağlanması engellenebiliyor.
 - Mobil cihazlar (telefon, tablet vb.) ile VPN üzerinden şirket kaynaklarına erişim sağlayan kullanıcılar için bu özelliğin devreye alınması gerekebilir. Nedeni, bu tür çok sık güncelleme almayan cihazlar güvenlik zafiyetlerine sahip oluyor ve dolayısıyla VPN üzerinden kurum kaynaklarına erişim sağlayarak zarar verebilme ihtimali bulunuyor.
- **Current Connection** -> aktif VPN bağlantılarının anlık durumunu izlemek ve yönetmek için kullanılan bir özelliktir. Bu özellik, özellikle ağ yöneticileri ve güvenlik ekiplerinin o anda VPN olan kullanıcı bağlantılarının durumu hakkında bilgi sahibi olmasını ve bu bağlantılara müdahale edebilmesini (bağlantıyı koparması gibi) sağlar



(Burada özelliği devreye almak ve seçim yapabilmek için sayfanın en alt kısmında bulunan “**VPN Tunnels**” alanında VPN tanımı yapılması gerekiyor).

- **Auto Connect** -> Kullanıcı FortiClient istemcisi açıldığında otomatik olarak bağlanacağı bir VPN tüneli belirlemek için kullanılıyor. Bu sayede kullanıcı FortiClient istemcisini açtığında VPN olması için gerekli ip ve port bilgileri otomatik olarak tanımlı olacaktır. Bu özelliğin sağlıklı çalışabilmesi için kullanıcının az bir kez FortiClient GUI'sinden manuel olarak VPN bağlantısı kurulmuş olması gerekiyor.
 - **Disable Connect/Disconnect** -> FortiClient üzerinde kullanıcının VPN olma veya VPN'den ayrılma seçeneklerinin gizlenmesini sağlar. Bu sayede kullanıcı VPN bağlantısını koparamıyor.
 - **Auto Connect Only When Off-Fabric** -> Sadece Off-Fabric (Manage Policies kısmında tanımlı Policy'de belirtilen ip aralığından ip almamışsa/kurum dışındaysa) durumdayken Auto Connect özelliğiyle VPN bilgilerine otomatik olarak bağlanması sağlanabiliyor.
 - **Auto Connect on Install** -> FortiClient istemcisi bir cihaza kurulduğunda otomatik bağlanma sürecinin yüklemenin hemen sonrasında çalışmasını sağlamak için devreye alınan özelliktir.



- **Always Up Max Tries** -> kullanıcının ağ sorunları nedeniyle kesilen VPN bağlantısını sonrasında bağlantının yeniden denenmesi için belirlenen maksimum deneme miktarıdır. Bu değer 0 olarak ayarlanırsa, VPN bağlantısı sürekli denenmeye devam edecektir.












Remote Access sekmesindeki “General” alanı için uygulanabilecek özelliklerin genel görüntüsü aşağıdaki gibidir.

Remote Access Profile  

▼ Expand All ▲ Collapse All

Name EMS-REMOTE-ACCESS-1 Basic **Advanced** XML

General

Allow Personal VPN ⓘ	
Show VPN before Logon ⓘ	
Use Windows Credentials ⓘ	
Minimize FortiClient Console on Connect	
Show Connection Progress ⓘ	
Suppress VPN Notifications	
Use Vendor ID	
Enable Secure Remote Access	
Current Connection	SSL_VPN ▼
Auto Connect	SSL_VPN ▼
Disable Connect/Disconnect	
Auto Connect Only When Off-Fabric	
Auto Connect on Install ⓘ	
Always Up Max Tries ⓘ	0

Network Lockdown

Kullanıcıların **Off-Fabric** durumdayken VPN olmadığı zamanlarda internet erişimini kısıtlamak için kullanılan özelliktir. Bu özellik sadece Windows işletim sistemlerinde desteklenmektedir. Bu özellik devreye alınmışsa kullanıcı tekrar VPN olana kadar internete erişimi kesilecektir.

- **Grace Period** -> Kullanıcının Off-Fabric durumdayken VPN bağlantısı kesildiğinde yeniden VPN oluncaya kadarki süreçte interneti ne kadar süre daha kullanabileceğinin belirlendiği alandır.
- **Maximum Connection Attempts** -> Kullanıcının yeniden VPN bağlantısı kurma sürecinde geçerli kullanıcı kimlik bilgilerini doğrulayarak yeniden bağlanması sürecinde yapabileceği maksimum deneme miktarıdır. Bu miktar dışında çıkılırsa internet bağlantısı kilitlenecektir.
- **Paths to Excluded Applications** -> Kullanıcının VPN bağlantısı kesildikten sonra internet erişimi kesilecektir. Bu süreçte internete çıkması gereken uygulamaların internete çıkarılmasını sağlamak için kullanılan özelliktir.

- **Excluded IPs** -> VPN bağlantısı kesilse dahi internet erişiminin kesilmesi istenmeyen ip adresleri olacaktır. Bu kısımda Network Lockdown özelliği dışında tutulmak istenen ip adresleri tanımlanıyor.

Network Lockdown

Grace Period: 120 seconds

Maximum Connection Attempts: 3

Paths to Excluded Applications

Example
C:\Windows\explorer.exe
%WINDIR%\explorer.exe

Enter one fully qualified path per line. Environmental variables are allowed. Wildcards aren't allowed.

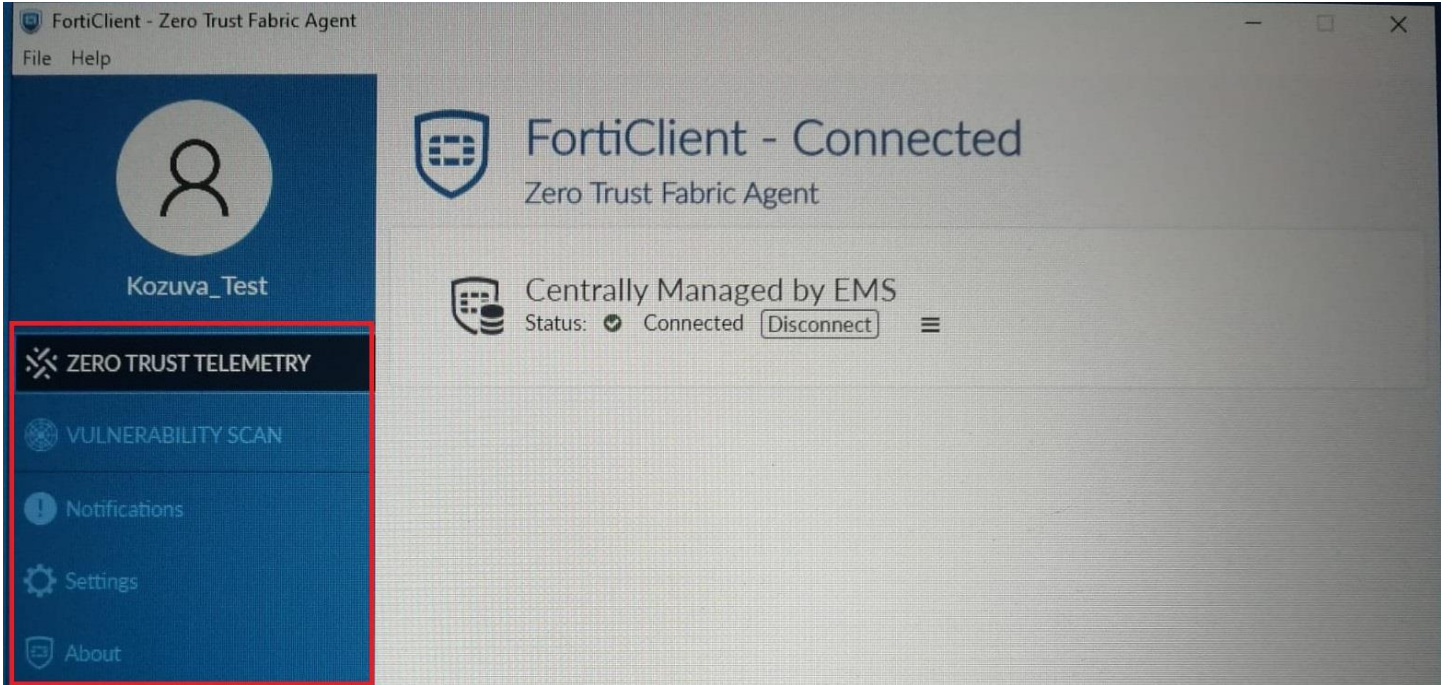
Excluded IPs

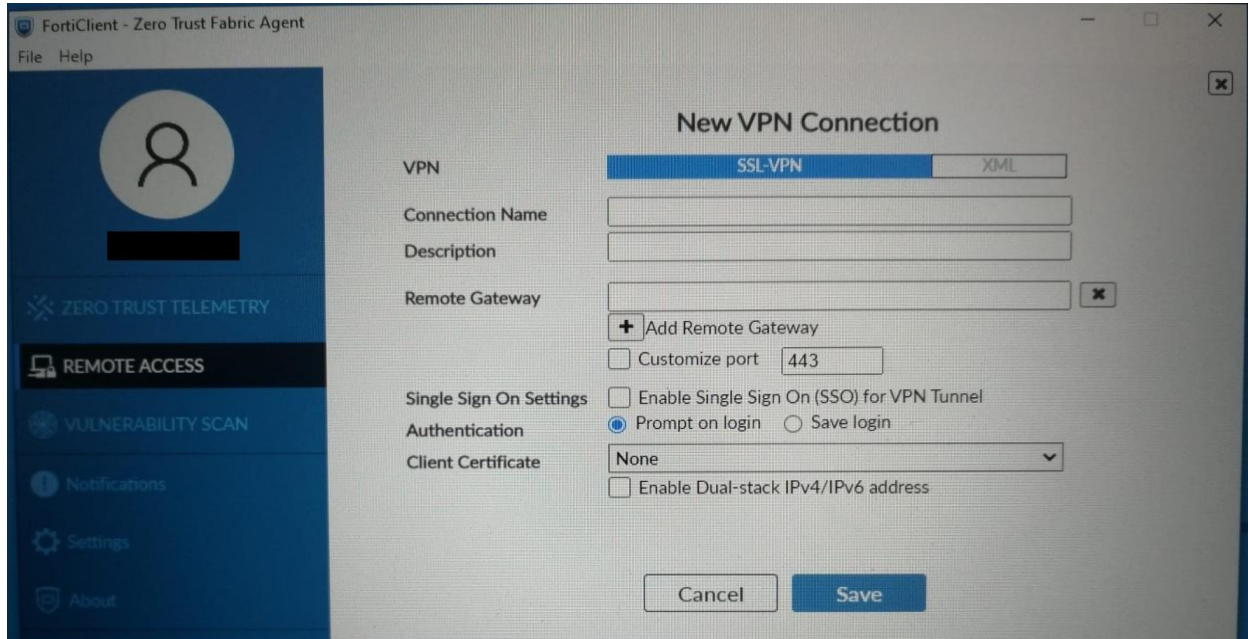
Optional

One IP address/IP subnet per line.

SSL VPN

SSL VPN özelliği FortiClient üzerinden SSL VPN bağlantısının kurulabilmesini sağlayan özelliktir. Devre dışı bırakıldığında aşağıdaki gibi FortiClient istemcisi üzerinde Remote Access sekmesi kaybolmaktadır. Bu özellik devreye alındığında aşağıdaki özelleştirmeler yapılabilmektedir;





- **DNS Cache Service Control** -> Normalde FortiClient istemcisi üzerinden SSL VPN olduğunda Windows DNS önbelleğini devre dışı bırakır. Windows DNS önbelleği, FortiClient SSL VPN tüneline bağlantısını kestikten sonra geri yüklenir. SSL VPN olduğunda DNS önbellek hizmetinin ne olacağını belirlemek için kullanılır.

DNS Cache Service Control ⓘ

- **Prefer SSL VPN DNS** -> Bu özellik devre dışı bırakıldığında, EMS SSL VPN bağlantısından gelen özel DNS sunucusunu fiziksel arayüze eklemeyiz. Etkinleştirildiğinde, EMS SSL VPN bağlantısından gelen özel DNS sunucusunu fiziksel arayüze ekler.
- **Do Not Accept Invalid Server Certificate** -> Geçersiz bir SSL VPN sunucu sertifikası kullanıldığında FortiClient istenen VPN bağlantısının kurulamamasını sağlayan özelliktir.
- **Enable Invalid Server Certificate Warning** -> Geçersiz bir SSL VPN sertifikası kullanıldığında FortiClient istemcisinin kullanıcıya bir uyarı görüntülemesi sağlanır.

- **Register the Address in DNS** -> FortiClient istemcilerinin VPN bağlantısı kurduğunda istemcinin IP adresinin ve cihaz ismini otomatik olarak bir DNS sunucusuna kaydedilmesini sağlayan özelliktir. Bu sayede uzak bağlantı yapan cihazın ip adresini öğrenmeye gerek kalmadan isimden çözerek erişilebilmesi sağlanır.
- **Preferred DTLS Tunnel** -> FortiClient VPN istemcilerinin VPN bağlantılarını kurarken hangi protokolün kullanılacağını belirlemek için kullanılmaktadır. DTLS (Datagram Transport Layer Security), özellikle UDP tabanlı iletişim için kullanılan ve TLS (Transport Layer Security) protokolünün bir uzantısıdır. Bu özellik devreye alındığında FortiClient istemcisinin VPN bağlantısı kurarken DTLS protokolünü tercih etmesini sağlar.
- **Split Tunnel Route Metric** -> Gerektiğinde belirli network adresleri için Route Metric değerleri üzerinde oynamalar yapılarak öncelik verilmesi gereken ağ bağdaştırıcıları üzerinde manipülasyonlar yapılmasına sağlayan özelliktir.

☒ SSL VPN

DNS Cache Service Control ⓘ	Disable dnscache service ▼
Prefer SSL VPN DNS ⓘ	<input checked="" type="checkbox"/>
Do Not Accept Invalid Server Certificate ⓘ	<input type="checkbox"/>
Enable Invalid Server Certificate Warning ⓘ	<input checked="" type="checkbox"/>
Register the Address in DNS	Register both physical adapter and tunnel IP's to DNS server ▼
Preferred DTLS Tunnel	<input type="checkbox"/>
Split Tunnel Route Metric	Optional

|→ EMS üzerinde varsayılanda SSL VPN özelliği devrede gelmiyor. SSL VPN özelliğini devreye alabilmek için “**System Settings -> Feature Select -> Remote Access -> SSL VPN**” yolu takip edilerek “**SSL VPN**” seçeneği işaretlenmelidir.

☒ Remote Access ⓘ

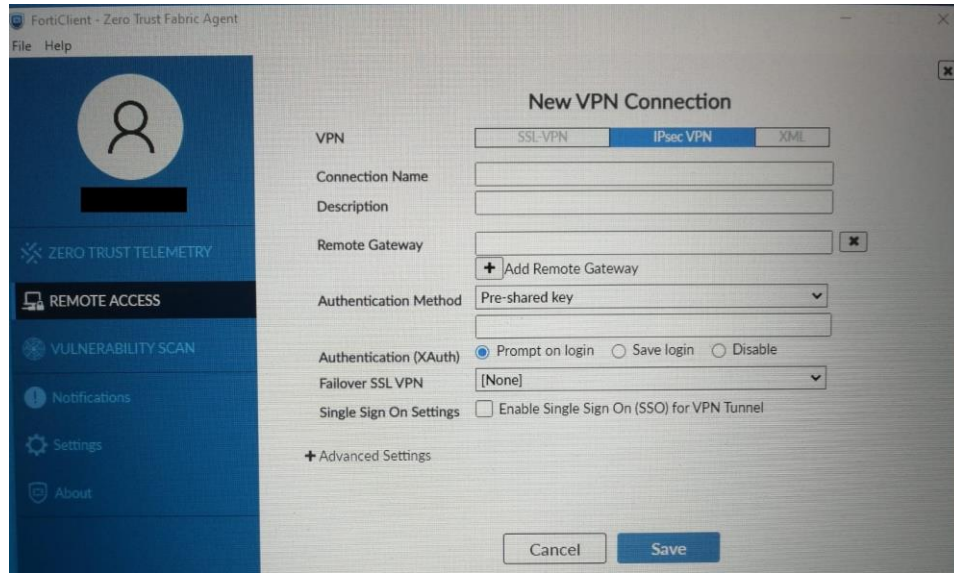
☒ SSL VPN ⓘ ▼

Enable SSL VPN visibility

IPsec VPN

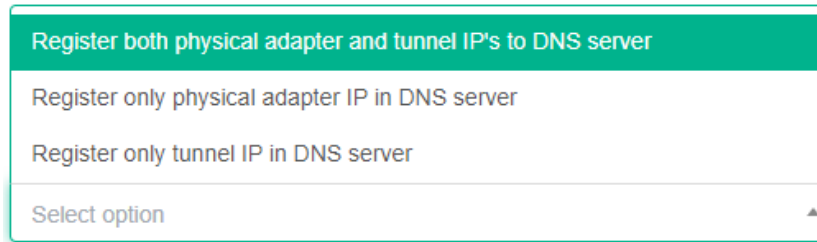
IPsec VPN özelliği FortiClient istemcisi üzerinden IPsec VPN kurulması için kullanılan özelliktir. İlk aşamada IPsec VPN özelliğinin devreye alınması gerekiyor. Bu özellik devreye alındıktan sonra EMS üzerinde yapılması gereken tanımlara ve özelleştirmelere bakıldığında (Uygulamasını izlemek için <https://www.youtube.com/watch?v=bl2G2CTW144>);

- **Beep If Connection Fails** -> IPsec VPN bağlantısı kurulmaya çalışılırken herhangi bir hata ile karşılaşılmaması sonucu bağlantı kurulamadığı durumlarda kullanıcıya sesli bir uyarı verilmesi için kullanılan özelliktir.



- **Use Windows Store Certificates** -> IPsec tüneli kurulurken kimlik doğrulama sürecinde Windows işletim sisteminde kayıtlı sertifika deposunun kullanılması için kullanılan seçenektir.
 - o **Current User Windows Store Certificates** -> IPsec VPN kurulurken, oturum açılan kullanıcının sahip olduğu sertifikaların kullanılması istendiği durumlarda devreye alınan özelliktir.
 - o **Local Computer Windows Store Certificates** -> IPsec VPN kurulurken, bilgisayar Local'inde bulunan/depolanan sertifikaların kullanılması istendiği durumlarda devreye alınan özelliktir.
- **Use Smart Card Certificates** -> akıllı kartlar aracılığıyla sertifika tabanlı kimlik doğrulaması sağlamak için kullanılan özelliktir. Bu özellik, kullanıcıların kimliklerini güvenli bir şekilde doğrulamak için akıllı kartlar üzerinde depolanan dijital sertifikaları kullanmalarına olanak tanır.

- **Show Auth Certificates Only** -> Yalnızca kimlik doğrulama sertifikalarını göstermek için kullanılır. Bu özellik, sertifika listesinin daha sade ve odaklı bir şekilde görüntülenmesini sağlar, böylece yöneticiler yalnızca kimlik doğrulama işlemlerinde kullanılan sertifikalara odaklanabilir.
- **Block IPv6** -> IPv6 adreslerinin ağda kullanılmasını engellemek için kullanılır. Bu özellik etkinleştirildiğinde, sistem IPv6 trafiğini bloklar ve yalnızca IPv4 adresleri üzerinden iletişime izin verir.
- **Enable UDP Checksum** -> UDP trafiği için checksum kontrolünü devreye almak için kullanılan özelliktir. UDP, bağlantısız bir protokol olduğu için veri iletiminde hata kontrolü yapma mekanizması kısıtlıdır. Bu özellik iletilen verinin doğruluğunu kontrol etmek için kullanılır.
- **Disable Default Route** -> IPsec VPN bağlantısı kurulduktan sonra bütün trafiği varsayılanda VPN üzerinden göndermeyip sadece IPsec konfigürasyonundaki tünel tanımının Phase2 aşamasında kullanılan ip adreslerine trafik oluşturulduğunda trafiğin VPN tüneline yönlendirilmesini sağlamak için kullanılan özelliktir.
- **Check for Certificate Private Key** -> bu özellik devreye alındığında istemcilerin bağlanmadan önce sertifikalarının özel anahtarlarının olup olmadığını kontrol edilip edilmeyeceğini belirlemek için kullanılıyor.
- **Enhanced Key Usage Mandatory** -> VPN bağlantılarında sertifikalarının kullanımını daha sıkı bir şekilde kontrol etmek için kullanılır. Bu özellik, sertifikaların belirli kullanım senaryoları için geçerli olmasını sağlayarak, güvenlik önlemlerini artırır.
- **Register the Address in DNS** -> VPN bağlantısı kurulan istemcilerin IP adreslerinin otomatik olarak DNS sunucusunda kaydedilmesini sağlayan özelliktir.



Register both physical adapter and tunnel IP's to DNS server

Register only physical adapter IP in DNS server

Register only tunnel IP in DNS server

Select option ▲

- **Do Not Accept Invalid Server Certificate** -> VPN bağlantısında istemcilerin yalnızca geçerli ve güvenilir sunucu sertifikalarını kabul etmesini sağlamak için kullanılan özelliktir.

☒ IPsec VPN

Beep If Connection Fails

☐

Use Windows Store Certificates

☒

Current User Windows Store Certificates

☒

Local Computer Windows Store Certificates

☒

Use Smart Card Certificates

☒

Show Auth Certificates Only

☒

Block IPv6

☒

Enable UDP Checksum

☒

Disable Default Route

☐

Check for Certificate Private Key

☒

Enhanced Key Usage Mandatory

☒

Register the Address in DNS

Register both physical adapter and tunnel IP's to DNS server

Do Not Accept Invalid Server Certificate ⓘ

☒

VPN Tunnels

Remote Access sekmesinin son kısmında bulunan ama ilk tanımlanması gereken tanım alanıdır. FortiClient istemcisini yükleyen kullanıcıların VPN bağlantısı için kullanacakları erişim bilgileri ve bu erişimler üzerinde özelleştirmelerin yapılması için kullanılan alandır (Burada tanıma başlanmadan önce Remote Access → SSL VPN kısmının devreye alınması gerekmektedir). Burada ilgili VPN tipinde tanım yapabilmek için VPN Tunnel kısmının köşesinde bulunan “Add Tunnel” butonuyla yeni bir VPN tanımı oluşturulmalıdır.

VPN Tunnels

Name

Type

Remote Gateway

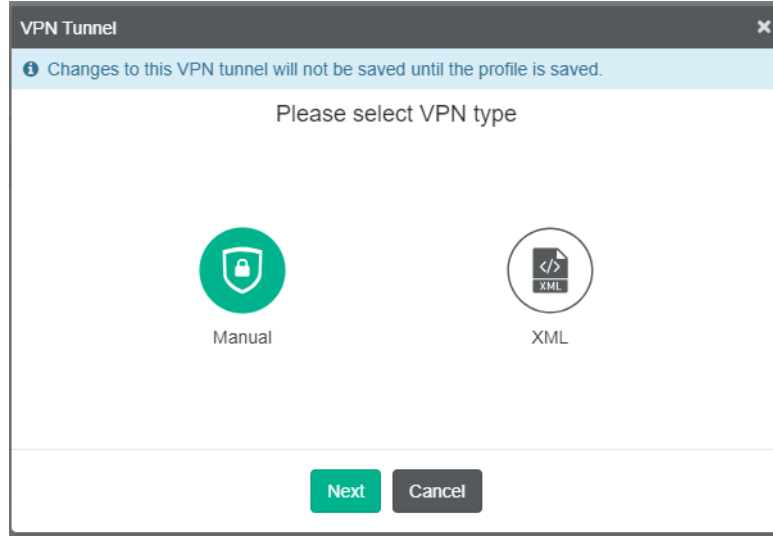
+ Add Tunnel

Add

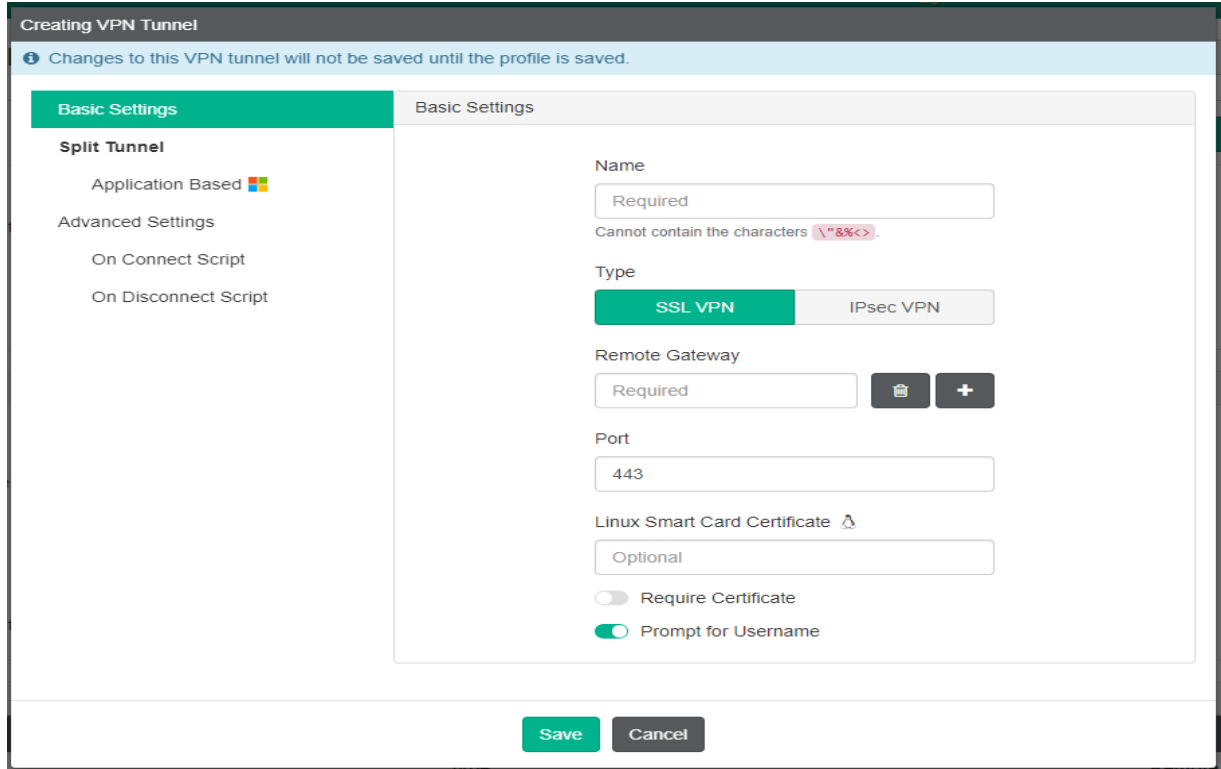
No Items Found

Showing: 0 Total: 0

Tunnel tanımı Manuel olarak tanımlanabildiği gibi hazır XML formatında tanım girişi yapılarak da gerçekleştirilebiliyor. Burada Manuel tanımıyla devam edilerek oluşturulacak VPN bağlantı tipi belirlenmelidir.



Basic Settings, istemcilere yüklenecek FortiClient istemcisinde Remote Access sekmesine girildiğinde kullanıcıya varsayılanda gelecek VPN bağlantı bilgilerine yönelik tanımların yapıldığı alandır. Burada yapılacak VPN bağlantısının **SSL VPN** kullanılarak mı yoksa **IPsec VPN** kullanılarak mı yapılacağı belirlenmelidir.



SSL VPN tanımı için SSL VPN ismi, VPN sunucusunun DIŞ BACAK ip ve port bilgilerinin girilmesi yeterlidir. Bu tanımlar sonrasında “**Advance Settings**” kısmı burada tanımlanan SSL VPN tanımı üzerinde özelleştirmeler yapılabilmesini sağlamaktadır.

Advance Settings, Tanımlı SSL VPN bağlantısı sürecinde özelleştirmeler yapmak için kullanılan alandır. Özelleştirilebilecek alanlara bakıldığında;

- **Enable Single User Mode**, Tanımlanan VPN bağlantısında sadece tek bir cihazın veya kullanıcının oturum açmasına izin vermek için kullanılan özelliktir.
- **Save Username**, Bağlantı kurma sürecinde kullanılan kullanıcı adının sonraki bağlantı sürecine kadar kaydedilip kaydedilmeyeceğini belirlemek için kullanılıyor.
- **Allow Non-Administrators to Use Machine Certificates**, sistem üzerinde yönetici olmayan kullanıcıların makine sertifikalarını kullanmalarına izin vermek için kullanılan özelliktir.
- **Enforce Acceptance of Disclaimer Message**, VPN bağlantısı sırasında kullanıcıların belirli bir feragat veya sorumluluk reddi mesajını kabul etmelerini zorunlu kılmak için kullanılmaktadır. Kullanıcının bağlantı sürecinde kullanıcıya bildiri çıkarmak için kullanılır.
- **Enable SAML Login**, VPN bağlantı sürecinde SAML tabanlı kimlik doğrulama yöntemini etkinleştirmek için kullanılan özelliktir (SAML, Microsoft Entra ID gibi kimlik sağlayıcılarının kimlik doğrulaması verilerini bir hizmet uygulaması olarak yazılım gibi bir hizmet sağlayıcıya geçirmesine olanak tanıyan açık standart bir XML teknolojisidir. Detaylar için [https://www.fortinet.com/resources/cyberglossary/saml#:~:text=Security%20Assertion%20Markup%20Language%20\(SAML\)%20is%20a%20protocol%20that%20enables,user%20to%20access%20a%20service.](https://www.fortinet.com/resources/cyberglossary/saml#:~:text=Security%20Assertion%20Markup%20Language%20(SAML)%20is%20a%20protocol%20that%20enables,user%20to%20access%20a%20service.)
- **FQDN Resolution Persistence**, alan adı çözümlemelerinin sonuçlarının kalıcılığını belirler. Bu özellik, bir FQDN tanımlı IP adresiyle eşleştirildiğinde, bu eşleştirmenin belirli bir süre boyunca geçerli olmasını sağlamak için kullanılan özelliktir.
- **Use External Browser as User-agent for SAML Login**, FortiClient üzerinde SAML tabanlı kimlik doğrulama işlemleri sırasında kullanıcıların dış bir tarayıcı kullanarak oturum açmasını sağlayan özelliktir.
- **Enable Azure Auto Login**, Azure Active Directory ile entegre olduğu durumlarda, kullanıcıların Azure hesaplarıyla otomatik olarak oturumun açılmasını sağlayan özelliktir. Bu özellik etkinleştirildiğinde, kullanıcılar FortiEMS üzerinden erişim sağlarken, Azure kimlik bilgilerini manuel olarak girmek zorunda kalmadan hızlıca oturum açabilirler.

- **Do not set DNS for tunnel adapter**, VPN bağlantısı kurulurken Fortinet adaptörü için DNS ayarlarını otomatik olarak yapılandırmamasını sağlar. Bu özellik etkinleştirildiğinde, VPN bağlantısı kurulduğunda Fortinet adaptörüne özel bir DNS sunucusu atanmaması için kullanılmaktadır.
- **Redundant Sort Method**, FortiClient üzerinde birden fazla SSL VPN sunucusu tanımlanması/kullanılması durumunda FortiClient istemcisinin hangi SSL VPN sunucusuna bağlanacağını kararını vermek için göz önünde bulunduracağı kriterin seçimidir. FortiClient, her SSL VPN bağlantı denemesinden önce sırayı hesaplar.
 - o **Server**, FortiClient istemcisi, tanımlanma sırasına göre belirler.
 - o **Ping Speed**, FortiClient istemcisi, sırayı ping yanıt hızına göre belirler.
 - o **TCP Round Trip Time**, FortiClient istemcisi, sırayı TCP gidiş dönüş süresine göre belirler.

Basic Settings

Split Tunnel

Application Based

Advanced Settings

On Connect Script

On Disconnect Script

Advanced Settings

☒ Enable Single User Mode

☒ Save Username

☒ Allow Non-Administrators to Use Machine Certificates

☒ Enforce Acceptance of Disclaimer Message

☒ Enable SAML Login

☒ FQDN Resolution Persistence ⓘ

☒ Use External Browser as User-agent for SAML Login

☒ Enable Azure Auto Login

☒ Do not set DNS for tunnel adapter

Tenant Name

Required

Client ID

Required

Redundant Sort Method

Server

Ping Speed

TCP Round Trip Tim

Tags ⓘ

✓

Select a Tag

☒ Customize Host Check Fail Warning

The following features need to also be configured on FortiGate to be enabled.

☐ Show "Remember Password" Option

☐ Show "Always Up" Option

☐ Show "Auto Connect" Option

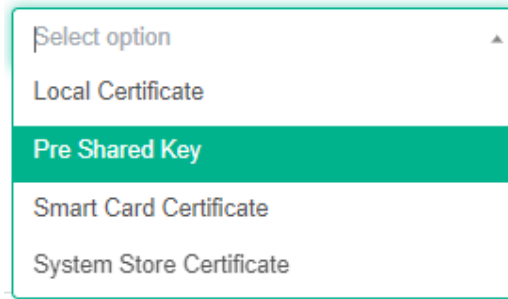
Save

Cancel

- **Tags**, Forti EMS üzerinde Zero Trust sekmesi altında tanımlanan Etiketler uygulanarak SSL VPN sürecinde Zero Trust olarak belirlenen özelliklerin (Güncel AV imzalarına sahip olup olmadığı, OS'un en son güncellemelere sahip olup olmadığı gibi) kontrol edilmesi sağlanabiliyor (Linux ve MacOS işletim sistemlerinde bu özellik desteklenmiyor).
- **Costumize Host Check Fail Warning**, uygulanan Zero Trust etiketi nedeniyle istemcilerin VPN tüneline bağlanması engellendiğinde kullanıcıya görüntülenecek özel bir mesajı/metni devreye almak için kullanılan özelliktir. Kullanıcının neden bağlanamadığına ilişkin bilgilendirme mesajları koyularak kullanıcının eksikliğini giderdikten sonra bağlanmayı denemesi sağlanabilir.
- **Show "Remember Password" Option**, FortiClient istemcisi üzerinde "Remember Password" seçeneğinin olup olmayacağını belirlemek için kullanılan özelliktir. Bu seçeneği FortiGate üzerinde de etkinleştirmeniz gerekmektedir.
- **Show "Always Up" Option**, FortiClient istemcisi üzerinde "Always Up" seçeneğinin olup olmayacağını belirlemek için kullanılan özelliktir.
- **Show "Auto Connect" Option**, FortiClient istemcisi üzerinde "Auto Connect" seçeneğinin olup olmayacağını belirlemek için kullanılan özelliktir.

IPsec VPN tanımı için isim, VPN sunucusunun dış bacak ip adresi tanımlandıktan sonra IPsec bağlantısında kullanılacak kimlik doğrulama metodu belirlenmelidir.

Authentication Method



Select option

Local Certificate

Pre Shared Key

Smart Card Certificate

System Store Certificate

Kimlik doğrulama sürecinde Pre-Shared Key kullanılması durumunda burada PSK değeri de girilmelidir. Temel tanımlamalar yapıldıktan sonra sırasıyla **VPN Settings**, **Phase1** ve **Phase2** tanımları yapılmalıdır.

Creating VPN Tunnel

Changes to this VPN tunnel will not be saved until the profile is saved.

Basic Settings

VPN Settings

Phase 1

Phase 2

Split Tunnel

Application Based

Advanced Settings

On Connect Script

On Disconnect Script

Basic Settings

Name

Required

Cannot contain the characters %<>.

Type

SSL VPN

IPsec VPN

Remote Gateway

Required

Authentication Method

Pre Shared Key

Pre-Shared Key

Required

Prompt for Username

Save

Cancel

VPN Settings, IPsec VPN oluřturma srecinde kullanılacak **IKE** versiyonu, **Mode** seęimi ve FortiClient tarafında kullanılacak **network** adres bilgileri tanımlanmalıdır.

- Normalde iki Network cihazı arasında IPsec Tunnel tanımı yapılırken Phase2 ařamasında kurulan tnel zerinden hangi Local networklerin haberleřeęi karřılıklı olarak tanımlanır. Burada tanımlanan ip adres bilgileri, VPN tanım srecinde istemcinin/FortiClient istemcisinin Local network bilgisi nitelięi tařıyacaktıř.

Creating VPN Tunnel

Changes to this VPN tunnel will not be saved until the profile is saved.

Basic Settings

VPN Settings

Phase 1

Phase 2

Split Tunnel

Application Based

Advanced Settings

On Connect Script

On Disconnect Script

VPN Settings

IKE

Version 1

Version 2

Mode

Aggressive

Main

Options

Mode Config

Manual Set

DHCP over IP...

Specify DNS Server (IPv4)

0.0.0.0

Assign IP Address (IPv4)

0.0.0.0

0.0.0.0

Split Table

IP Address

Subnet Mask

Save

Cancel

- **Phase1**, normal şartlarda IPsec Tunnel bağlantısının Phase1 aşamasında yapılması gereken tanımların bulunduğu sekmedir. Burada bağlantı sürecinde kullanılacak şifreleme algoritmaları, kimlik denetimi metotları, DH grubu gibi özelliklerin IPsec kurulacak hedef cihaz (VPN Server) ile aynı tanımlanması gerekmektedir. Bu nedenle IPsec VON tanımında Phase1 ve Phase2 aşamalarında karşılıklı tanımlanacak özelliklerin (IKE Proposal, DH Group, Key Lifetime, DPD ...) bilindiği düşünülerek ayrıca açıklama gereği duyulmamıştır. Burada tanımlanan parametrelerin ve özelliklerin detayları için Fortigate -> IPsec VPN notlarını inceleyebilirsiniz.

Basic Settings

VPN Settings

Phase 1

Phase 2

Split Tunnel

Application Based

Advanced Settings

On Connect Script

On Disconnect Script

Phase 1

IKE Proposal

Encryption Authentication

AES128 SHA1

Encryption Authentication

AES256 SHA256

DH Groups

☐ 1 ☐ 2 ☒ 5 ☐ 14

☐ 15 ☐ 16 ☐ 17 ☐ 18

☐ 19 ☐ 20 ☐ 21

Key Life

86400 seconds

Local ID

☒ Enable Implied SPDO

Implied SPDO Timeout

0 seconds

☒ Dead Peer Detection

☒ NAT Traversal

☒ Enable Local LAN

☒ Enable IKE Fragmentation

☒ Allow non-administrators to use machine certificates

Save Cancel

- **Phase2**, Phase1 aşamasında olduğu gibi bu tanımların IPsec bağlantısı kurulacak hedef cihaz ile karşılıklı olarak aynı ayarlanması gerekmektedir

Basic Settings

VPN Settings

Phase 1

Phase 2

Split Tunnel

Application Based

Advanced Settings

On Connect Script

On Disconnect Script

Phase 2

IKE Proposal

Encryption

AES128

Authentication

SHA1

Encryption

AES256

Authentication

SHA256

DH Groups

5

Key Life

Seconds

43200

seconds

Enable Replay Detection

Enable Perfect Forward Secrecy (PFS)

Save

Cancel

Fortigate üzerinde de “VPN -> IPsec Wizard -> Remote Access” veya “VPN -> IPsec Wizard -> Custom (Dailyup User)” kısmında ilgili tanımlamalar yapılarak FortiClient istemcisi ile Fortigate FW arasında IPsec Tunnel kurulması sağlanabilmektedir.

Dashboard

Network

Policy & Objects

Security Profiles

VPN

Fabric Overlay Orchestrator

Overlay Controller VPN

IPsec Tunnels

IPsec Wizard

IPsec Tunnel Template

VPN Creation Wizard

1 VPN Setup

2 Authentication

3 Policy & Routing

4 Client Options

5 Review Settings

Name

Template type

Site to Site

Hub-and-Spoke

Remote Access

Custom

Remote device type

Client-based

Native

FortiClient

Cisco

Dialup - FortiClient (Windows, Mac OS, Android)

This FortiGate

Internet

FortiClient

< Back

Next >

Cancel

Split Tunnel

Split Tunnel özelliği ile tünele girmesi istenen trafiklerin uygulama bazında ayırt edilebilmesi sağlanabiliyor. Bu özellik ile kurulan VPN tünel bağlantısına hangi uygulama trafiklerinin dahil edileceğini veya hangi uygulama trafiklerinin tünele dahil edilmemesi gerektiği burada belirtilebiliyor. Bu özelliği devreye almak için sol üst köşede bulunan “Application Based” seçeneğinin seçilmesi gerekiyor.

Creating VPN Tunnel

Changes to this VPN tunnel will not be saved until the profile is saved.

Basic Settings

Split Tunnel

Application Based

Advanced Settings

On Connect Script

On Disconnect Script

Application Based

Type

Include

Exclude

Cloud Applications

+ Add

Applications

No Domain Found

Domain

+ Add

Domains

No Domain Found

Save

Cancel

Örnek olarak yüksek bant genişliği harcayan uygulama trafikleri Exclude edilebiliyor (Bunun için ilgili uygulamanın bilgisayardaki uzantısının girilmesi gerekiyor).

Creating VPN Tunnel

Changes to this VPN tunnel will not be saved until the profile is saved.

Basic Settings

Split Tunnel

Application Based

Advanced Settings

On Connect Script

On Disconnect Script

Application Based

Type

Include

Exclude

Local Applications

+ Add

Applications

No Application Found

Cloud Applications

+ Add

Applications

No Domain Found

Domain

+ Add

Domains

No Domain Found

Save

Cancel

Add Local Application

Add Application(s)

Required

Application can be specified by its name, full path or the directory where it is installed. Environment variables (e.g. `%programfiles%`, `%appdata%`) can be used in file and directory path. Multiple entries can be separated by `;` (e.g. `chrome.exe;iexplore.exe`)

For example:
Application Name: `chrome.exe`
Full Path: `C:\Program Files\Internet Explorer\iexplore.exe`
Directory: `C:\windows\` (must end with `"\"`)

Add

Close

Son olarak **“VPN Tunnels -> Add Tunnel -> Manual -> On Connect Script”** veya **“VPN Tunnels -> Add Tunnel -> Manual -> O Disconnect Script”** kısımları kullanılarak VPN bağlantısı kurulan istemciler üzerinde Script tanımları çalıştırılabilir (https://help.fortinet.com/fclient/olh/5-4-1/Content/FortiClient-5.4-Admin/1100_Remote%20Access/840_VPN%20tunnel%20and%20script+.htm).

Basic Settings

VPN Settings

Phase 1

Phase 2

Split Tunnel

Application Based

Advanced Settings

On Connect Script

On Disconnect Script

On Connect Script

Linux On Connect Script

1

Windows On Connect Script

Mac On Connect Script

Save

Cancel

Günün sonunda burada yapılan Remote Access tanımının bir grup üzerinde uygulanabilmesi için **“Endpoint Policy & Components -> Manage Policies -> Endpoint Policies”** yolu izlenerek eşleştirilmesi istenen ilgili Policy tanımında uygulanmalıdır.

Kaynaklar

- <https://docs.fortinet.com/document/fortigate/7.6.0/administration-guide/190553/remote-access>
- <https://docs.fortinet.com/document/forticlient/6.4.0/new-features/386752/secure-remote-access-compliance-enforcement-6-4-4>
- <https://docs.fortinet.com/document/forticlient/7.4.0/ems-administration-guide/682498/remote-access>
- https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/1048fc2-f6f3-11ec-bb32-fa163e15d75b/FortiClient_EMS_7.0.6_Administration_Guide.pdf
- https://help.fortinet.com/fclient/olh/5-4-1/Content/FortiClient-5.4-Admin/1100_Remote%20Access/840_VPN%20tunnel%20and%20script+.htm
- <https://docs.fortinet.com/document/fortigate/5.6.0/cookbook/530530/site-to-site-ipsec-vpn-with-certificate-authentication>
- [https://www.fortinet.com/resources/cyberglossary/saml#:~:text=Security%20Assertion%20Markup%20Language%20\(SAML\)%20is%20a%20protocol%20that%20enables,user%20to%20access%20a%20service.](https://www.fortinet.com/resources/cyberglossary/saml#:~:text=Security%20Assertion%20Markup%20Language%20(SAML)%20is%20a%20protocol%20that%20enables,user%20to%20access%20a%20service.)