WISENET

Teknik Belge

Ağ Güvenliğini Pekiştirme Kılavuzu

SECURITURK

Hanwha Techwin

Belge No: S20182B0001

İçindekiler

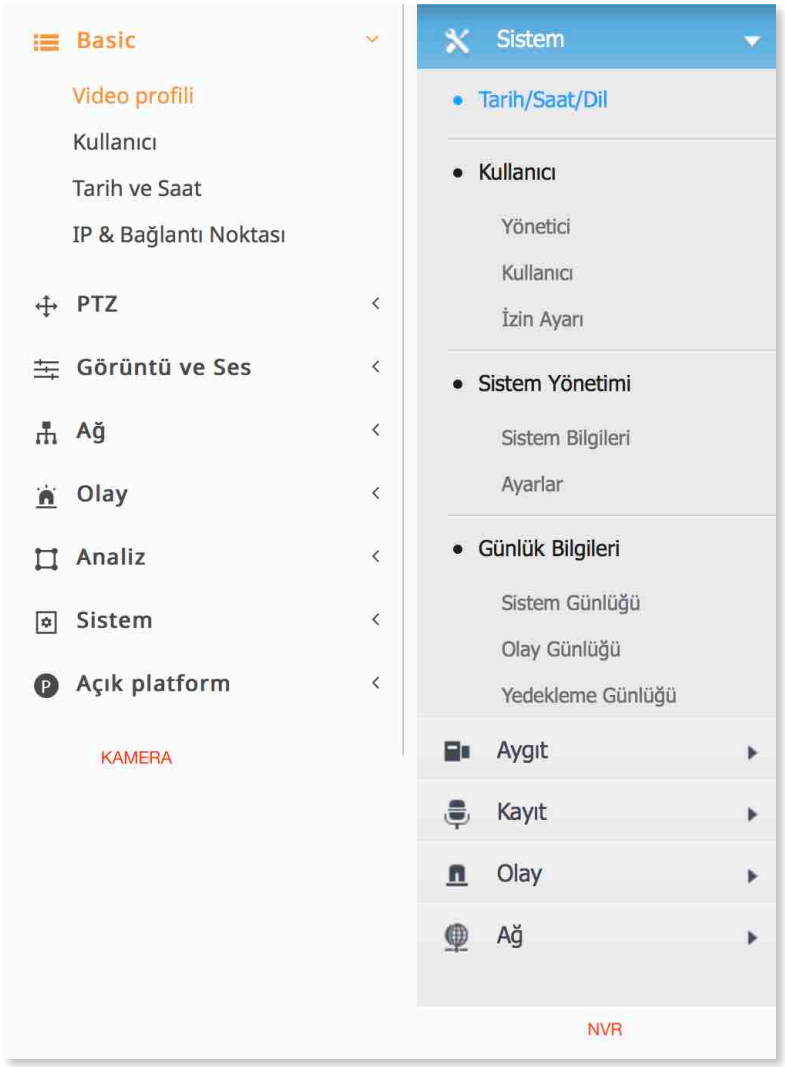
Giriş

Son yıllarda kamera sistemi pazarında, müşterilerin mülkiyetini ve kişisel bilgilerini korumak için geliştirilen kameralar ve kayıt cihazlarının, hassas kişisel ve kurumsal bilgileri ele geçirmek için bir araç olarak kullanıldığı bir paradoks ortaya çıkmıştır. Ağ kamera sistemi cihazları hassas kişisel bilgiler olarak kullanılabilecek video verilerini işler ve yönetir. Sistemlere bilgisayar ağlarına bağlandığından beri dünyanın her yerinden uzaktan erişim mümkündür. Bu nedenle, ağ kamera sistemi cihazları, yerel ağa nüfuz etmeye çalışan siber saldırılara maruz kalmaktadır.

Hanwha Techwin, müşterilerin mülkiyet ve kişisel bilgilerini dikkatle göz önüne alarak, siber güvenliği güçlendirme yönünde sürekli çalışmalar yapıyor. Bu kılavuzun Hanwha Techwin ürünlerinde uygulanan güvenlik özelliklerini anlamanıza ve kullanmanıza yardımcı olacağını umuyoruz.

Bu belgede açıklanan ve gösterilen yapılandırma değişikliklerinin İnternet Tarayıcısı kullanıcı arabirimine atıfta bulunduğu unutulmamalıdır. Wisenet Aygıt Yöneticisi, önemli güvenlik ayarlarının hızlı ve tutarlı bir şekilde yapılandırılmasına olanak tanıyan, IP kameraların tüm yapılandırma değişikliklerini toplu halde yapmak için kullanılan bir araçtır.

Aşağıdaki kılavuzda, Hanwha Techwin IP kameraları için talimatlar ve ekran görüntüleri verilecektir. Yapılandırma öğelerinin birçoğu NVR ürünleri için de geçerlidir ve menü konumunda ufak değişiklikler olur.



Güvenlik Düzeylerinin Tanımı

Bu kılavuz, aşağıdaki kriterlere göre siber güvenlik seviyelerini belirtir; her seviye ve önceki seviyenin uygulandığı varsayılarak belirlenmiştir.

- Ürün tasarım seviyesi, kullanıcıların ayarlama yapmadan sağladığı siber güvenlik ürünleriyle ile elde edebileceği güvenlik seviyesidir.
- Koruyucu seviye, satın alınan ürünlerin fabrika ayarları veya fabrika ayarlarına döndürdükten hemen sonra elde edilebilecek varsayılan güvenlik ayarlarıdır.
- Güvenli düzey, gereksiz özellikleri veya hizmetleri devre dışı bırakmak, güncel tutmak ve sistem günlüklerini incelemek suretiyle elde edebileceği bir güvenlik düzeyidir.
- Çok güvenli düzey, sağlanan güvenlik özelliklerini, ek harici güvenlik çözümleri ile birleştirerek elde edilebilecek güvenlik seviyesi anlamına gelir.

<Tablo 1>

Güvenlik seviyesi	Siber Güvenlik için Sıkılaştırma Özellikleri & Etkinlikleri	Fabrika Değeri	Önerilen Ayar
Ürün Tasarım Düzeyi	Karmaşık şifreye zorlama ayarı	Standart	
	İlk şifre yok	Varsayılan	
	Ard arda yanlış şifreyle giriş için sınır	Varsayılan	
	HTTP kimlik doğrulaması (Yalnızca Derleme)	Varsayılan	
	Arka kapı girişi yok (Telnet, SSH *Kapalı)	Varsayılan	
	Yapılandırma dosyasını şifreleme	Varsayılan	
	Bellenim (Firmware) şifrelemesi	Varsayılan	
	Yedeklenen Video için filigran ve şifrelenmesi	Varsayılan	
	Fabrika ayarlarına döndürüldüğünde korunan günlükler	Varsayılan	
Koruyucu Düzey	Fabrika ayarlarına döndür	-	
	Konuk olarak oturum açma	Devre Dışı	Devre Dışı
	Kimlik doğrulamadan RTSP bağlantısı	Devre Dışı	Devre Dışı
	Çok noktaya yayın (Multicast)	Devre Dışı	Devre Dışı
	DDNS (Kullanılmayacaksa Kapalı Tutun*)	Kapalı	Kapalı
	QoS (Kullanılmayacaksa Kapalı Tutun*)	Devre Dışı	Devre Dışı
	FTP (Kullanılmayacaksa Kapalı Tutun*)	Devre Dışı	Devre Dışı
	Ses girişi (Kullanılmayacaksa Kapalı Tutun*)	Devre Dışı	Devre Dışı
Güvenli Düzey	Yazılım sürümünü kontrol etme ve güncelleme	-	
	Doğru tarih ve saati ayarlama	Başlangıç Değeri	Değiştirin
	HTTPS (Hanwha Techwin sertifikası)	HTTP	HTTPS (Kendi Sertifikası)
	HTTPS (kimliği doğrulanmış belge)	HTTP	HTTPS (Yetkili Sertifikası)
	Varsayılan bağlantı noktası	Başlangıç Değeri	Değiştirin
	IP Filtreleme	Devre Dışı	Açık
	TLS kullanarak e-posta gönderme	Kullanılmıyor	Kullanın
	Yerel IPv4 bağlantı adresi (Kullanmayacaksanız Kapatın*)	Kullanıma açık	*Kapalı
	UPnP (Kullanmayacaksanız Kapatın*)	Kullanıma açık	*Kapalı
	Bonjour (Kullanmayacaksanız Kapatın*)	Kullanıma açık	*Kapalı
	SNMP'yi güvenli bir şekilde kullanma	SNMP v2c	SNMP v3
	Kullanılmayan SNMP'yi devre dışı bırakma	SNMP v2c	*Kapalı
	Ek kullanıcı hesapları oluşturma	-	-
	Günlüğü kontrol etme	-	-
Çok Güvenli Düzey	802.1 X Sertifika tabanlı erişim kontrolü	Kapalı	Kullanın

Ürün Tasarım Düzeyi

Hanwha Techwin'in, birçok varsayılan ayarı güvenli olsa bile, siber güvenlik tehditlerine karşı güvenlik sağlamak için tasarımını geliştirdi.

<Tablo 2>

Güvenlik Politikası	Siber Güvenlik için Özellikler	Kısa Açıklama
Şifre Politikası	Karmaşık şifreye zorlama	**1)** Büyük harf, **2)** küçük harf, **3)** sayı, **4)** özel karakterler. Bunlardan 3/4'ü kullanılan şifreler için 8 karakter, 2/4'ü kullanılan şifreler için 10 karakter uzunluğunda şifreyi zorunlu tutar.
	İlk şifre yok	İnternet tarayıcısıyla ilk bağlantıda şifre ayarlama zorunluluğu vardır
	Ard arda yanlış şifreyle giriş için sınır	Ard arda yanlış şifre girildiğinde engeller.
Kullanıcı Doğrulama	HTTP Kimlik Doğrulaması (Yalnızca Derleme)	HTTP iletişimi sırasında kullanıcı parolasını korunur.
Uzaktan Erişim Kontrolü	Arka kapı girişi yok (Telnet, SSH Kapalı)	Sisteme uzaktan erişebilen tüm hizmetleri kaldırın
Tercih bilgileri	Yapılandırma dosyası şifreleme	Yapılandırma yedeklemesini koruyun
Bellenim	Bellenim (Firmware) şifrelemesi	Bellenim'leri koruyun. Zararlı yazılımların bellenimlerim içine girmesini engelleyin.
Yedeklenen Video	Yedeklenen Video için filigran ve şifrelenmesi	Yedeklenen videonun doğruluğundan ve bütünlüğünden emin olun ve orijinalinin kimliğini doğrulayın
Günlükler	Fabrika ayarlarına döndürüldüğünde korunan günlükler	Davetsiz misafirlerin kötü amaçlı günlük silinmesini önleyin.

Karmaşık şifreye zorlama

Hanwha Techwin ürünleri en az 8 karakterli şifre gerektirir. 1) Büyük harf, 2) küçük harf, 3) sayı, 4) özel karakterler. Bunlardan 3/4'ü kullanılan şifreler için 8 karakter, 2/4'ü kullanılan şifreler için 10 karakter uzunluğunda şifreyi zorunlu tutar. Politika, 4 veya daha fazla tekrarlanan veya sıralı karakterin kullanımını sınırlar (aaaaa, abcde, qwerty, 12345). Tüm standart klavye özel karakterleriyle karmaşık bir şifre oluşturmasına izin verilir. NVR / DVR / IP kamera için 15 karakterlik bir şifreye izin verilirken ve VMS için 31 karaktere kadar desteklenir. Bu uygulama, bir kullanıcının dikkatsizliği nedeniyle zayıf bir şifrenin kullanılmasını engelleyerek, yetkisiz kişilerin şifre çalma, tahmin etme veya kırma olasılığını azaltmaya yardımcı olur.

Ürün Tasarım Düzeyi

İlk şifre yok

Bir kullanıcı ilk parolayı kullanıyorsa veya üreticinin varsayılan parolasını değiştiremezse, yetkisiz erişime izin verebilecek ciddi bir güvenlik açıklığına neden olabilir. Kullanıcı hatasından kaynaklanabilecek herhangi bir güvenlik açığını ortadan kaldırmak için, tüm Hanwha Techwin ürünlerinin ilk parolaları yoktur. Ürünün arayüzüne internet tarayıcısı(ie, safari, edge, firefox, chrome gibi) ile ilk kez girildiğinde, kullanıcıyı kendi parolasını oluşturmaya zorlamak üzere tasarlanmıştır.

Ard arda yanlış şifreyle giriş için sınır

Hackerlar, doğru şifre bulunana kadar ortak şifreleri ve / veya olası tüm şifreleri sistematik olarak deneyen yazılımlar üretir. Bu tür saldırılara izin verilirse, yeterince uzun bir süre sonunda şifre bulunabilir. Hanwha Techwin aygıtları, güvenliğini artırmak için 30 saniye içinde gerçekleşen 5 veya daha fazla kimlik doğrulama isteğini engelleyerek kaba kuvvet(Brute-Force) saldırılarını önler. Kimlik doğrulama istekleri engellenirken, bir hizmet reddi oluşmasını önlemek için yetkili kullanıcıların mevcut bağlantıları korunmaktadır. Bu geçici blok, şifre tahmininde bulunulması gereken süreyi çok büyük ölçüde artırır. Genellikle bilgisayar korsanının kendisine daha kolay bir hedef seçmesini sağlar.

HTTP Kimlik Doğrulaması (Yalnızca Karşılıklı Derleme)

Hanwha Techwin NVR / IP kameralar varsayılan olarak HTTP modunu güvenli hale getirmek için kullanıcı adı ve parolalar HTTP üzerinden sunucu ve istemci arasındaki bilgi iletimi / alımı sırasında korunmaktadır. Düz metin, base64 kodlaması veya temel kimlik doğrulama HTTP moduna izin verilecek olursa, şifre ağın paket izlenmesiyle kolaylıkla keşfedilebilir. Bu nedenle istemci ve sunucu arasında iletişim iki tarafın bildiği bir algoritmaya bağlı çalışır.
Aktarılan videonun şifreye ek olarak şifrelenmesi gerekiyorsa, güvenlik seviyesi HTTPS modunu iyileştirerek geliştirilebilir (Bkz. Tablo 3).

<Tablo 3>

Seçenek	Karşılık Düzey	İlk Ayar
HTTP (Güvenli bağlantı yok)	Varsayılan Düzey	✓
HTTPS (Benzersiz bir sertifika kullanarak güvenli bağlantı modu)	Güvenli Düzey	X
HTTPS (Genel bir sertifika kullanarak güvenli bağlantı modu)	Güvenli Düzey	X

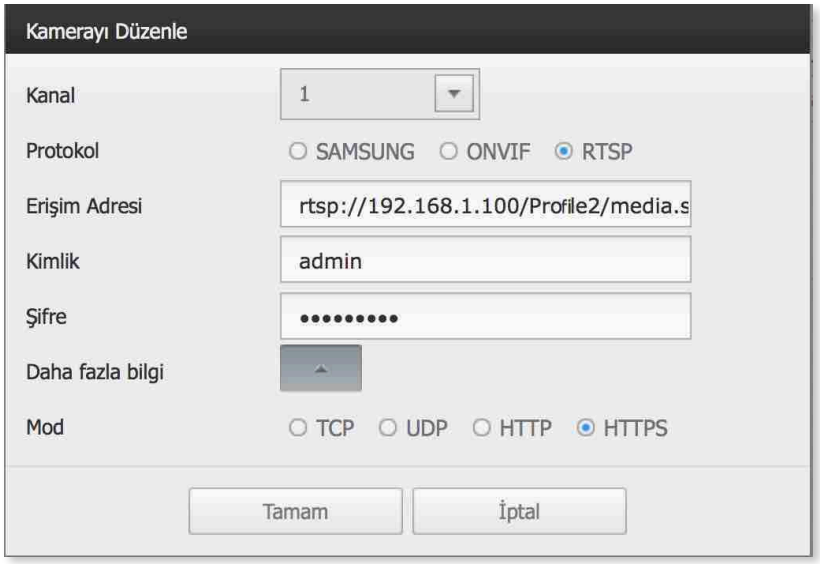
<Tablo 4>

Mod	Şifre Koruması	Video/ Veri Koruması	Kullanıcı Kimliği Koruması	Kullan/Kullanma
HTTP (Temel)	X	X	X	Kullanma
HTTPS (Digest)	✓	X	✓	Kullan(Varsayılan)
HTTPS	✓	✓*	✓	Kullan

* HTTPS modu, yalnızca kullanıcı kimlik doğrulaması ve API komutları gibi HTTP protokolünde iletilen verileri korur. RTSP protokolü tarafından aktarılan video akışını korumak için, HTTPS üzerinden RTSP tünelinin açılması için ek kurulum yapılması gerekir.
Örneğin, IP kameradan NVR'ye gönderilen videoyu HTTPS ile korumak isterseniz, IP kameranın modunu HTTPS'ye ayarlayın. RTSP'yi HTTPS modunda ayarlamak için IP kameranın arayüzünde bir yapılandırma yoktur. Bu nedenle kamerayı NVR'ye bağlamak ve karşılık gelen modu NVR aracılığıyla aşağıdaki gibi ayarlamak gerekir:

Ürün Tasarım Düzeyi

NVR Arayüzünde, Aygıt > Kamera > Kamera Kayıt > Kanalı seçimi > Kamera Düzenle



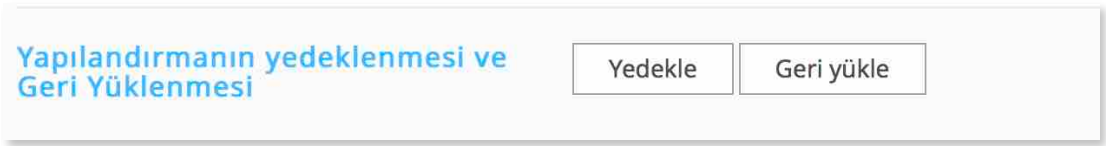
Arka kapı girişi yok (Telnet, SSH Kapalı)

Bir ağ aygıtı, telnet gibi uzaktaki hizmetleri destekliyorsa, üreticinin kolayca müşteri hizmetleri sunması için avantajlıdır. Bu hizmetler, sorun giderme ve teşhis için yararlı olan doğrudan root(kök) erişimi sağlar. Bununla birlikte, bir bilgisayar korsanı -veya kötü niyetli bir üretici- için telnet gibi hizmetlerin açık olması, en tehlikeli güvenlik olaylarına neden olan bir faktör olabilir. Hanwha Techwin, bu riskleri, servis kolaylığı değil, müşteri bilgilerinin güvenliği açısından elimine etti. Bütün aygıtlarda Telnet ve SSH erişimi kapalıdır.

Yapılandırma dosyası şifreleme

Yedekleme işlevi, geçerli cihazın yapılandırma bilgisini içeren ikilik kodlama sistemindeki bir dosya (IP ve Port, DDNS, IP filtreleme, HTTPS, 802.1x, QoS, SNMP hariç) kaydetmenize izin verir. Böylece, yönetici, geri yükleme işlevi ile yedeklenen bu yapılandırma bilgisini geri yükleyebilir.
Bu işlevleri kullanarak, yönetici, aynı model adıyla tüm cihazlar için aynı konfigürasyonu yalnızca bir cihaz ayarı ile ayarlayabilir. Yedeklenen yapılandırmayı içeren ikilik kodlama sistemindeki dosya kullanıcı aygıt ortamının önemli bilgilerini içerdiğinden Hanwha Techwin, yedekleme sırasında konfigürasyon bilgilerini kaydetmek için güvenli bir şifreleme algoritması kullanmaktadır.

Kamera Arayüzünde;
Sistem > Yükseltme / Yeniden Başlatma > Yapılandırma yedekleme ve geri yükleme



Bellenim (Firmware) Şifreleme

Üreticiler, resmi internet sitesinde özellik eklemeleri, hata düzeltmeleri ve güvenlik geliştirmeleri için donanım yazılımı sağlar. Bu yazılım, ürünün çalışma şeklini denetler. Dosya değiştirilirse, kötü amaçlı yazılımlar tanıtılabilir. Hanwha Techwin'in yazılımları, önemli dahili bilgileri korumak ve bir arka kapı gibi kötü amaçlı yazılım tanıtımını önlemek için şifrelenir. Böylece kullanıcılar en son ürün yazılımı ile güvenle yeni sürüme geçebilirler. Bir bellenim şifrelenmezse, dosya sistemi, veritabanı yapısı ve temel programlama kodu incelenebilir ve kullanılabilir.

Yedeklenen Video için Filigran ve Şifrelenmesi

Hanwha Techwin NVR ve VYS'si kullanılarak SEC formatında yedeklenen video dosyaları bilgisayarlarla birlikte gelen veya bilindik normal oynatma / düzenleme yazılımları ile açılamaz, bu korumayla dosya sahteciliği önlenebilir.

• SEC dosyası çalar, yedekleme işlemi sırasında otomatik olarak yedeklemeye dahil edilir.

Gerekli yasal veya gizlilik koruması için bir video dosyası yedeklemek istiyorsanız, şifre korumasıyla SEC biçiminde ayıklayabilirsiniz. Filigran ve şifreleme, videonun kurcalamaya karşı korumalı ve düzgün olmasını sağlamak için yedek SEC dosyasına uygulanır. SSM VYS yedekleme için kullanılıyorsa, dijital imza işlevi de desteklenir. Dosyanın özgünlüğünü ve bütünlüğünü hızlı bir şekilde sağlamak için ek şifreleme işlevleri sağlar.

<Tablo 5>

Aygıt	Yöntem	Yedekleme Biçimi	Filigran / Şifreleme	Sayısal İmza	Oynatıcı
Kamera	İnternet Arayüzü	STW	X	X	SD Kart Oynatıcı
		AVI*	X	X	Genel Video Oynatıcı
NVR	Set	NVR	X	X	Sadece sette oynatılabilir
		SEC*	✓	X	Backup Viewer Yazılımı
	İnternet Arayüzü	NVR	✓	X	Backup Viewer Yazılımı
		AVI	X	X	Genel Video Oynatıcı
Kamera/ SSM ile NVR	-	SEC*	✓	✓	Backup Viewer Yazılımı
		AVI	X	X	Genel Video Oynatıcı
Kamera/ Smart Viewer ile NVR	-	SEC*	✓	X	Backup Viewer Yazılımı
		AVI	X	X	Genel Video Oynatıcı

* Varsayılan yedekleme biçimini gösterir.

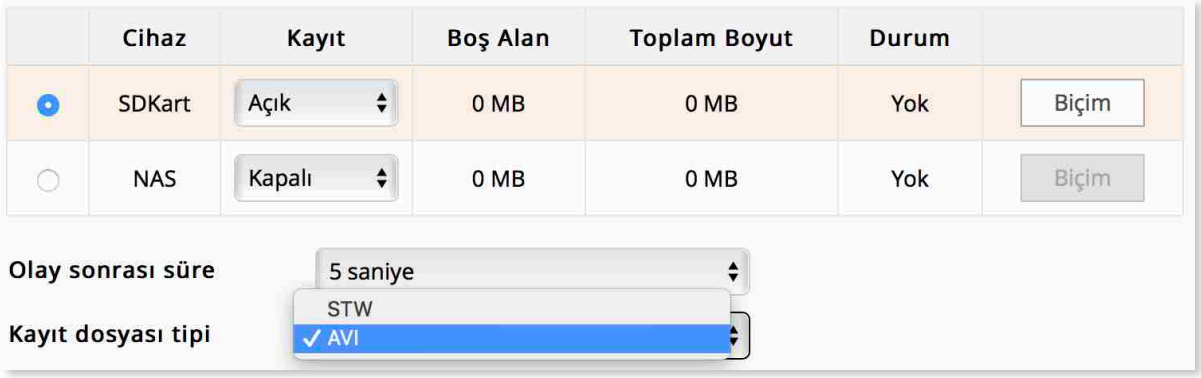
Dijital İmza ve Filigranın Karşılaştırması

<Tablo 6>

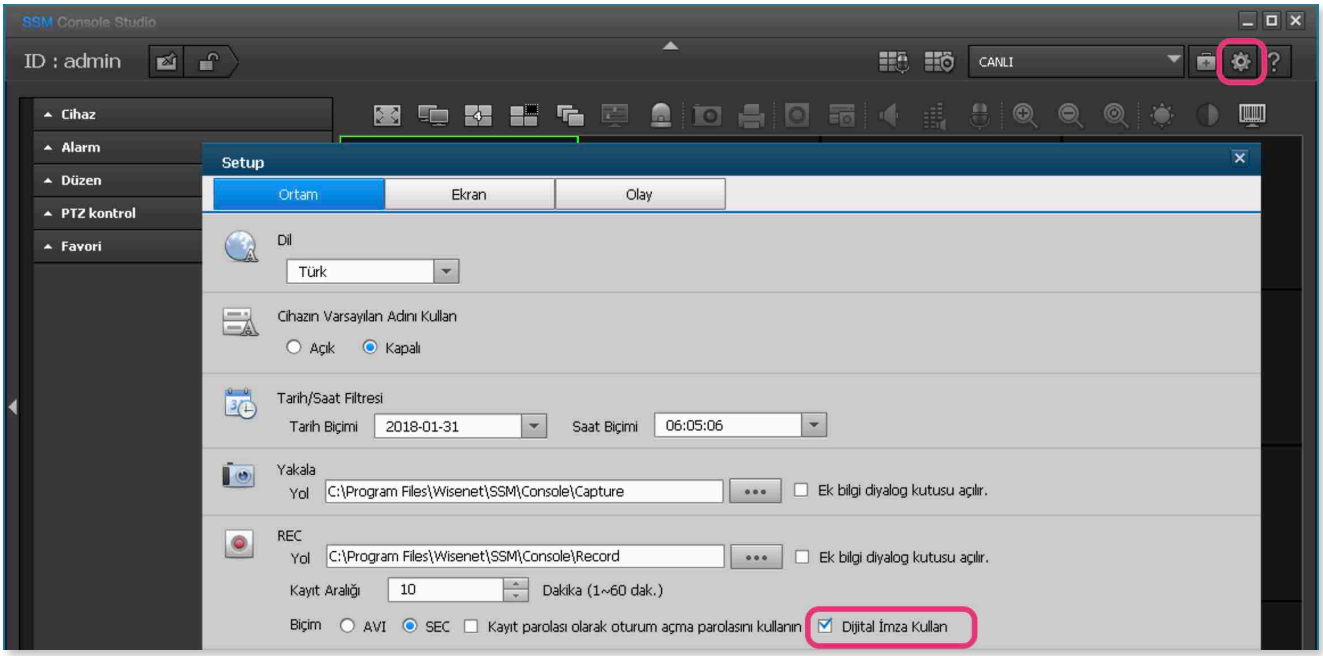
Elektronik İmza	Filigran
Tüm yedekleme dosyası verilerini doğrulayabilir	Yedekleme dosyasının her karesini doğrulayabilir
Video ve ses verisinin yanı sıra başlık bilgilerini de doğrulayabilir	Sahte video veya ses verilerini doğrulayabilir, başlık bilgisini değiştiremez
Tüm çerçevenin kaldırılması durumunda doğrulayabilir	Tüm bir çerçevenin kaldırılıp kaldırılmadığını doğrulayabilir
Sahte çerçevenin tarih / saatini kontrol edemez	Bir çerçevenin tarih / saatinin sahte olup olmadığını kontrol edebilir
Tüm dosyayı bir kerede doğrulayabilir	Sahte çerçeveyi belirlemek için tüm dosya oynatılmalı
SSM tarafından desteklenmektedir	SmartViewer, SSM, NVR, DVR tarafından desteklenir

Ürün Tasarım Düzeyi

IP kamera Kurulumu > Olay Depolama > Depolama aksiyonu ayarı > Kayıt tipi



SSM Konsol > Ayarlar > Ortam > Kayıt > Biçim



FABRİKA AYARLARINA DÖNDÜRÜLDÜĞÜNDE KORUNAN GÜNLÜKLER

Ağ veya güvenlik yöneticileri, saldırı yolunu analiz etmek veya birisi bir ağ aygıtına girmeye çalıştığında olayı anlamak için günlüğü kontrol etmede çok önemlidir.

Bununla birlikte, davetsiz misafirler bu ağ aygıtlarının günlüklerinden haberdar oldukları için, günlükleri silerek iz bırakmazlar. Hanwha Techwin ürünleri, bu gibi kötü niyetleri önlemek için aygıtın güç döngüsü veya sıfırdan başlatma (fabrika ayarlarına sıfırlama) ile kayıt dosyalarını silinmesini engellecek şekilde geliştirilmiştir. Bu günlükler, adli soruşturma için kolayca tek tek veya toplu olarak indirilebilir. Çoğu ürünün, Sistem günlüğü, Olay günlüğü ve Erişim günlüğü vardır.

Koruyucu Düzey

Fabrika ayarlarına döndür

Kurmak istediğiniz cihaz fabrika ayarlarında değilse, cihaza uygulanmış ayarlarını silmek için cihaza fabrika ayarlarına sıfırlama yapılması önerilir. Bir cihazın yetkisiz kişilerce düzenlendiği veya erişildiği düşünülüyorsa, cihazın varsayılan fabrika ayarlarına döndürülmesi önerilir. Hanwha Techwin ürünleri, yalnızca ilk duruma getirilmesiyle birlikte güvenlik seviyesini koruyabilir. Fabrika varsayılan ayarlarına döndürme, internet sayfası arayüzünden üzerinden, Wisenet Aygıt Yöneticisi veya donanımsal sıfırlama düğmesi* aracılığıyla yapılabilir.

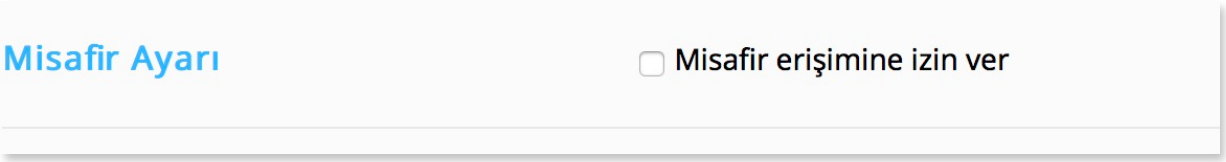
İnternet sayfası arayüzünden fabrika varsayılanlarını uygulamak için:
1) Sistem > Yükseltme / Yeniden Başlatma > Fabrika varsayılan Ayarı
2) 'Ağ parametresini & Open Platform hariç' onay kutusunun işaretini kaldırın.
3) 'Sıfırla'yı tıklayın.

* Donanım düğmesini kullanarak varsayılan fabrika ayarlarına dönmek için cihaz açıkken ve tamamen açıldığında düğmeyi 5 saniye basılı tutun.

Konuk Girişini Devre Dışı Bırakma

Hanwha Techwin kameralar konuk giriş fonksiyonu sağlar. Bu konuk hesabı, yalnızca en düşük ayrıcalıklara izin verecek şekilde sınırlıdır. Ancak konuk girişi etkinleştirilirse, yetkisiz kullanıcılarında video akışlarını izlemesine izin verilmiş olur. Konuk erişimine ihtiyaç duymadığınız zamanlarda, konuk girişi devre dışı bırakılmalıdır. Konuk girişi, bir kullanıcının kullanıcı adı ve parolasını kullanır.

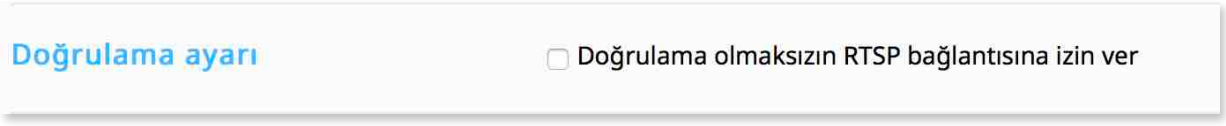
IP kamera Arayüzü> Ayarlar > Temel > Kullanıcı > Misafir Ayarı



Kimlik doğrulamadan RTSP bağlantısı

Hanwha Techwin kameralar, kimlik doğrulaması olmaksızın RTSP bağlantılarına izin veren bir işlev sunar. Bu özellik, kamuya açık bir şekilde bir RTSP video akışı sağlamak için kullanışlıdır. Ancak RTSP video akışını yetkisiz kullanıcılardan korumak isterseniz, kimlik doğrulama özelliği olmadan RTSP bağlantısını devre dışı bırakmalısınız.

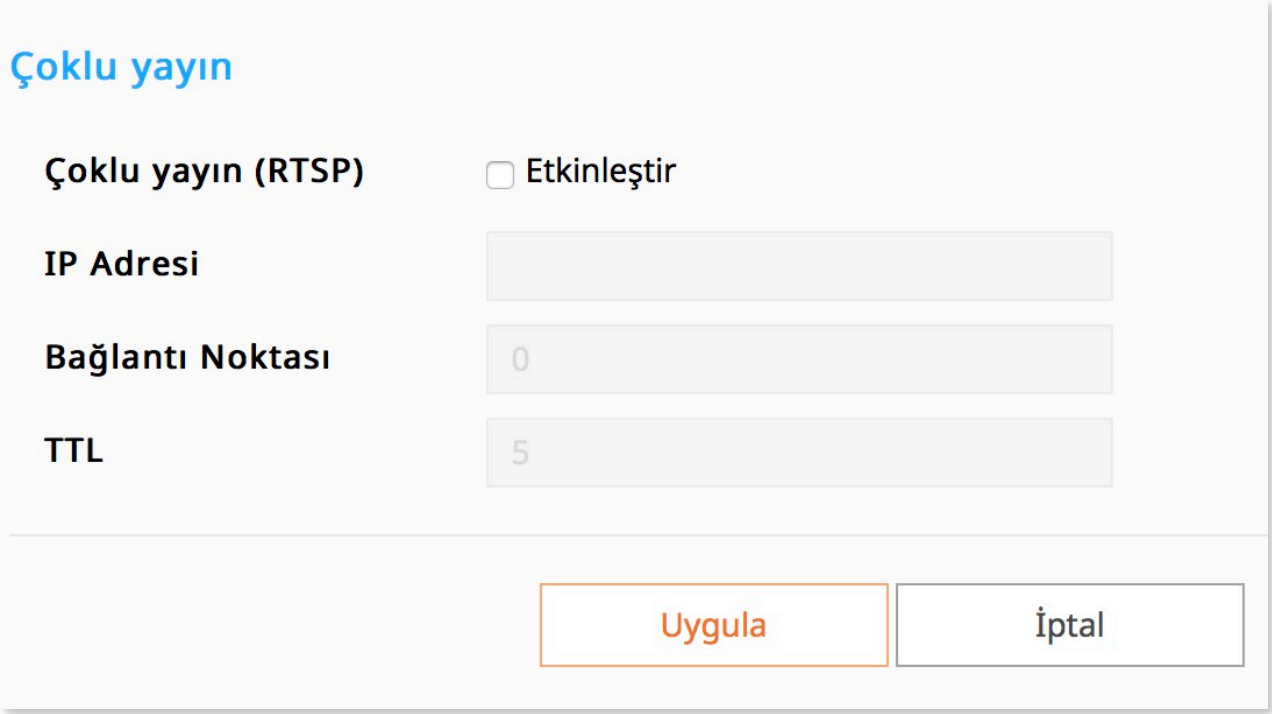
1) IP kamera kurulumu > Temel > Kullanıcı > Doğrulama ayarı
2) 'Doğrulama olmaksızın RTSP bağlantısına izin ver' onay kutusunundan onayı kaldırın.



Kullanılmayan (Multicast) Çoklu Yayın'ı Devre Dışı Bırakma

Hanwha Techwin kameraları SVNP ve RTSP protokollerini kullanarak video akışını çok noktaya yayın yapabilirler. Bu hizmetlere gerek duyulmazsa, ek güvenlik için servis özelliklerinin seçimini kaldırdığınızdan emin olun.

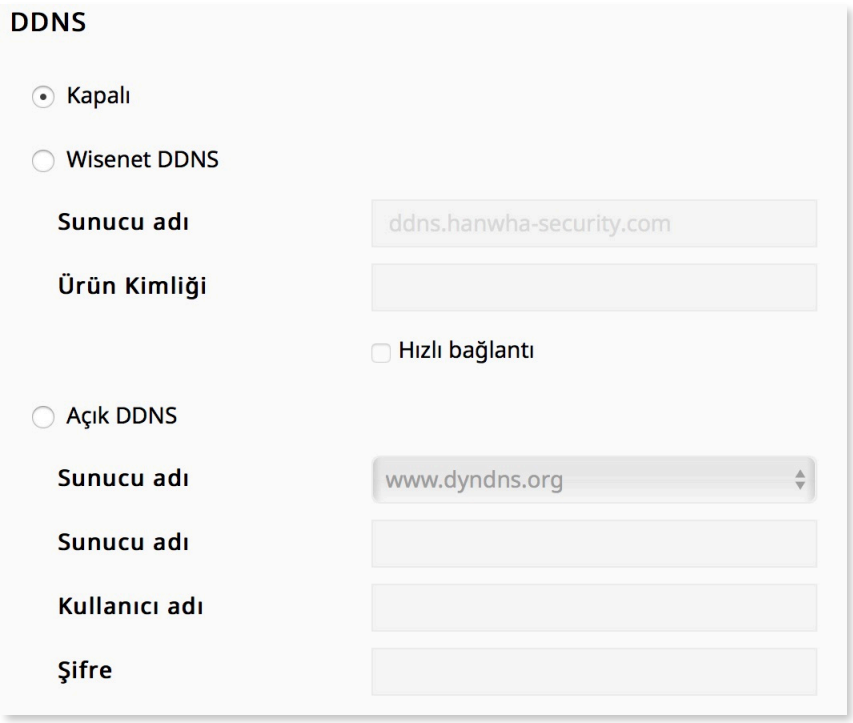
1) Ayarlar > Video >Profil2
2) Çoklu Yayın (RTSP) nin 'Etkinleştir' kutusunun işaretini kaldırın.
3) 'Uygula'yı tıklayın.
4) Diğer tüm video profilleri için tekrarlayın.



Kullanılmayan DDNS'i Kapatma

İnternet üzerindeki IP adresi zaman zaman değişebilir. Kamera veya kayıt cihazının internete açık olarak kullanılması durumunda, kullanıcı IP adresinin ne zaman değişeceğini bilmeyecek ve görüntüleri izleyemeyecektir. DDNS işlevi, geçerli IP adresini ve bağlantı noktasını izlerken cihaza erişmek için kullanıcı tarafından seçilen sabit bir ad sağlar. Servis kullanılmıyorsa, ek güvenlik için servisin devre dışı bırakıldığından emin olun.

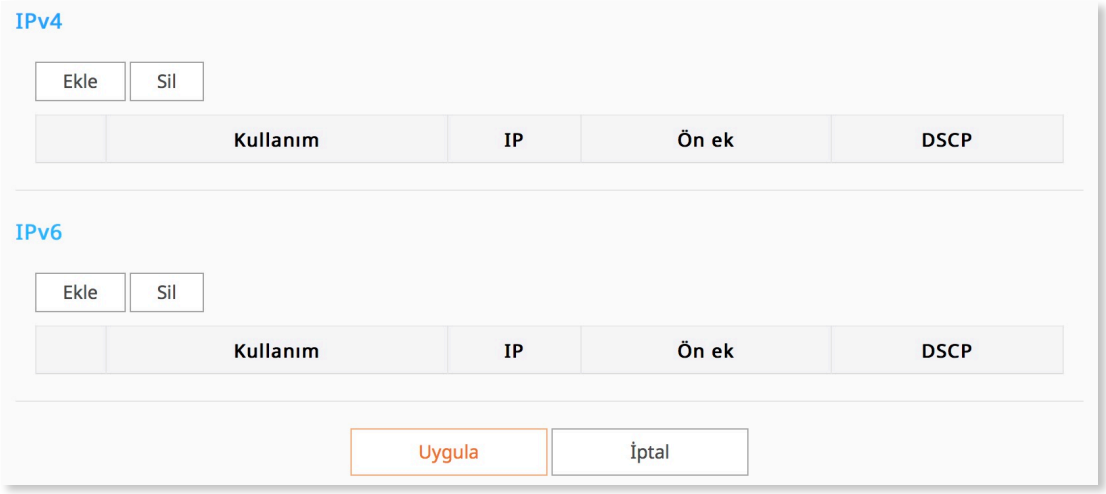
1) Ayarlar > Ağ > DDNS
2) DDNS için 'Kapalı'yı işaretleyin.
3) 'Uygula'yı tıklayın.



Kullanılmayan QoS'i Devre Dışı Bırakma

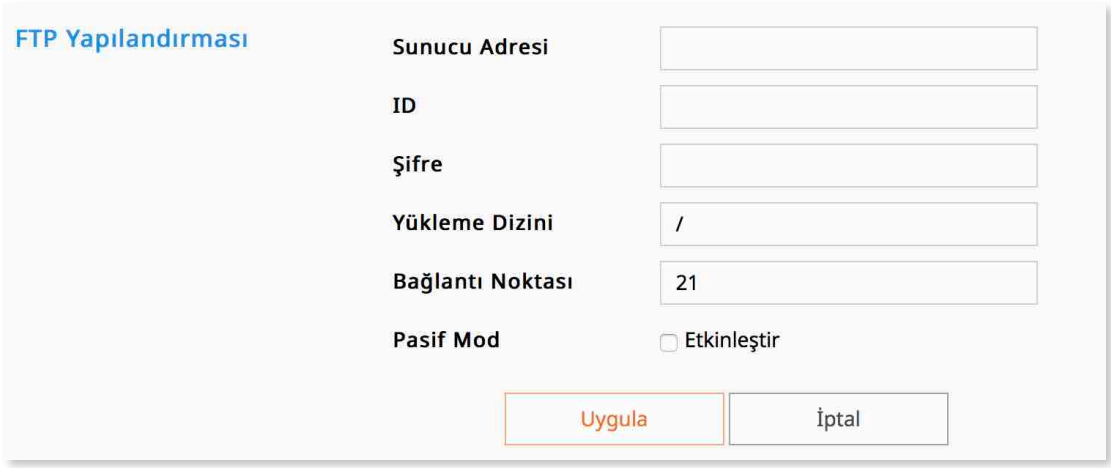
QoS (Hizmet Kalitesi), video aktarımının belirli IP adreslerine kalitesini garantilemek için bir öncelik seviyesi belirlemek üzere kullanılan bir işlevdir. Hizmetin gereksiz olduğunu düşünüyorsanız, ek güvenlik için hizmeti devre dışı bıraktığınızdan emin olun.

1) Ayarlar > Ağ > QoS
2) QoS için listelenen IP'yi seçin ve ardından silin.
3) 'Uygula'yı tıklayın.



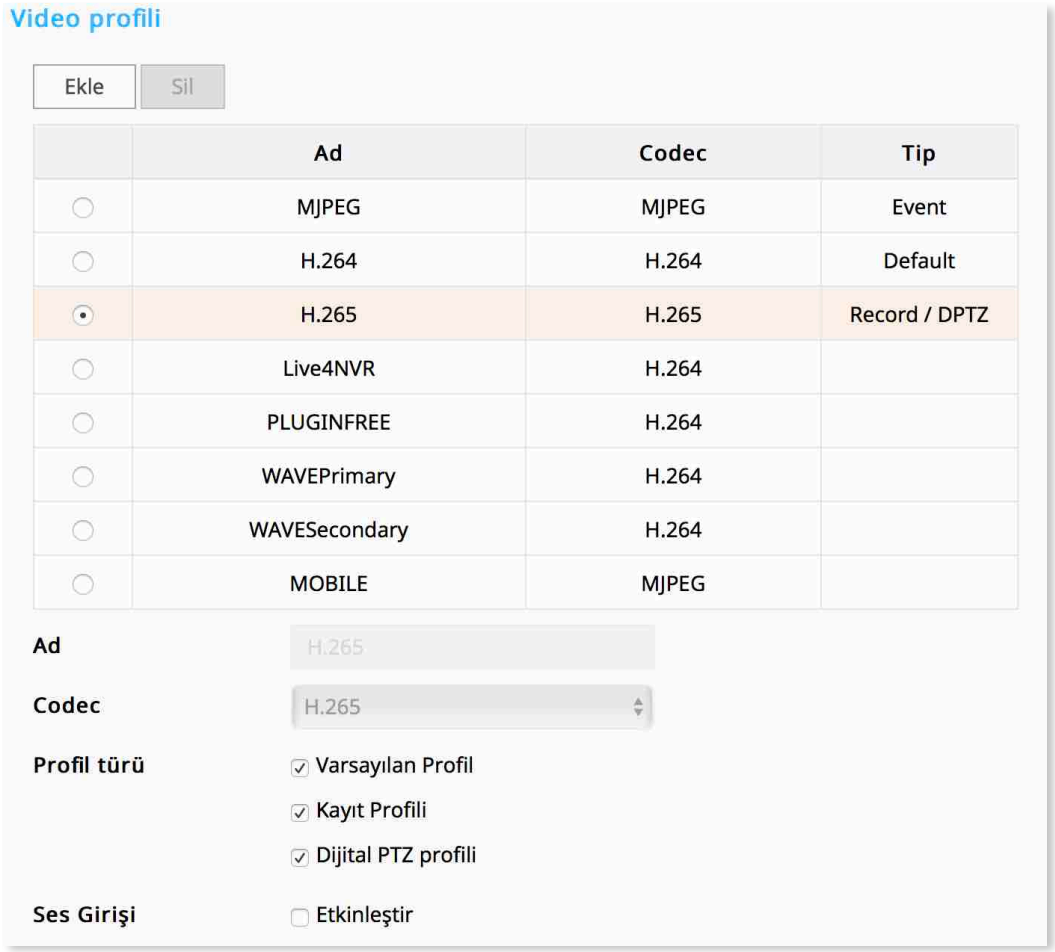
Kullanılmayan FTP'yi Devre Dışı Bırakma

FTP işlevi, periyodik bir zamanlayıcı çizelgesinde, bir alarm veya olay meydana geldiğinde bir dosya sunucusuna görüntü aktarmak için kullanılır. Hizmetin gereksiz olduğunu düşünüyorsanız, ek güvenlik için hizmeti devre dışı bıraktığınızdan emin olun.
1) Ayarlar > Etkinlik > FTP / E-posta > FTP Yapılandırma
2) Sunucu adresini, kimliğini ve şifresini kaldırın.
3) 'Uygula'yı tıklayın.



Kullanılmayan Ses Girişini Devre Dışı Bırakma

Ses Girişi, kamera modeline bağlı olarak, bir hat girişi, mikrofon girişi veya dahili mikrofondan video akışına ses girmenizi sağlayan bir işlevdir*. Ses Girişi işlevi, bu işleve erişimi kısıtlamak için bir yol sağlayabilecek her kullanıcı hesabı için etkinleştirilebilir veya devre dışı bırakılabilir. Özelliğin gereksiz olduğunu düşünüyorsanız, ek güvenlik için devre dışı bıraktığınızdan emin olun. Ses girişi işlevi, her video profili için ayrı olarak ayarlanır; bu nedenle her bir profili seçmeniz ve ardından işlevi devre dışı bırakmanız gerekir.



* Ses girişi işlevini kullanma, gizlilik beklenen bazı ülkelerde veya kurulum yerlerinde yasadışı olabilir.

1) Ayarlar > Video Profili
2) Video profillerini seçin ve ‘Ses' seçeneğinin işaretini kaldırın.
3) 'Uygula'yı tıklayın.

Güvenli Düzey

Bellenimin Sürümünü Denetleme ve Güncelleme

En son özelliklerle ve güvenlik düzeltmeleriyle çalıştığınızdan emin olmak için ağa bağlı herhangi bir cihazın bellenimini güncelleme önemlidir. Bellenim, ürünün piyasaya sürülmesinden sonra ortaya çıkmış olabilecek sorunları giderir. Ürün yazılımı, web sunucusu, veritabanı gibi temel bileşenleri iyileştirebilir ve güncelleyebilir. Ürünün yükseltilmesi işlemi birkaç dakika alırken, bunun düşük riskli bir zamanda gerçekleştirmesi önerilir. Yeni sürüme geçerken cihazın sabit güce sahip olduğundan emin olun. Yapılandırmanın tamamı, yükseltme sırasında saklanır ve çoğu durumda doğrudan en yeni sürüme geçebilirsiniz. Herhangi bir uyarı için lütfen bellenim indirmesiyle birlikte gelen sürüm notlarına bakın. Hanwha Techwin internet sitesinden kullandığınız ürünlerin en son bellenimini kolayca kontrol edebilir ve indirebilirsiniz.

• www.hanwha-security.eu veya www.hanwha-security.com > Ürün Sayfası > Ürün Yazılımı

Kamera arayüzünde aracılığıyla, mevcut bellenim sürümünü ve dağıtım tarihini kontrol edebilirsiniz. Lütfen mevcut ürününüzün ürün yazılımı sürümünü kontrol edin ve daima en yeni sürüme güncelleyin.

1) Sistem Yükseltme / Yeniden Başlatma Yükseltme
2) Mevcut Yazılım ve ISS sürümün numarasını Hanwha sitesindeki sürüm numarası ile karşılaştırın. Daha üst bir sürüm yayınlanmışsa bilgisayarınıza indirin.
3) 'Gözat'ı tıklayın ve en son firmware .IMG dosyasını seçin
4) 'Yükseltme'yi tıklayın

Wisenet Aygıt Yöneticisi, yeni bellenimi kontrol etme, bellenimi indirme, dosyaları açma ve aygıtları yükseltme işlemlerini otomatikleştirebilir. Dağıtımı hızlandırmak için Aygıt Yöneticisi, bir defada 16 aygıtı yükseltme ve arzu edilirse kalan aygıtları kuyruklama yeteneğine sahiptir.

Doğru Tarih ve Saati Ayarlama

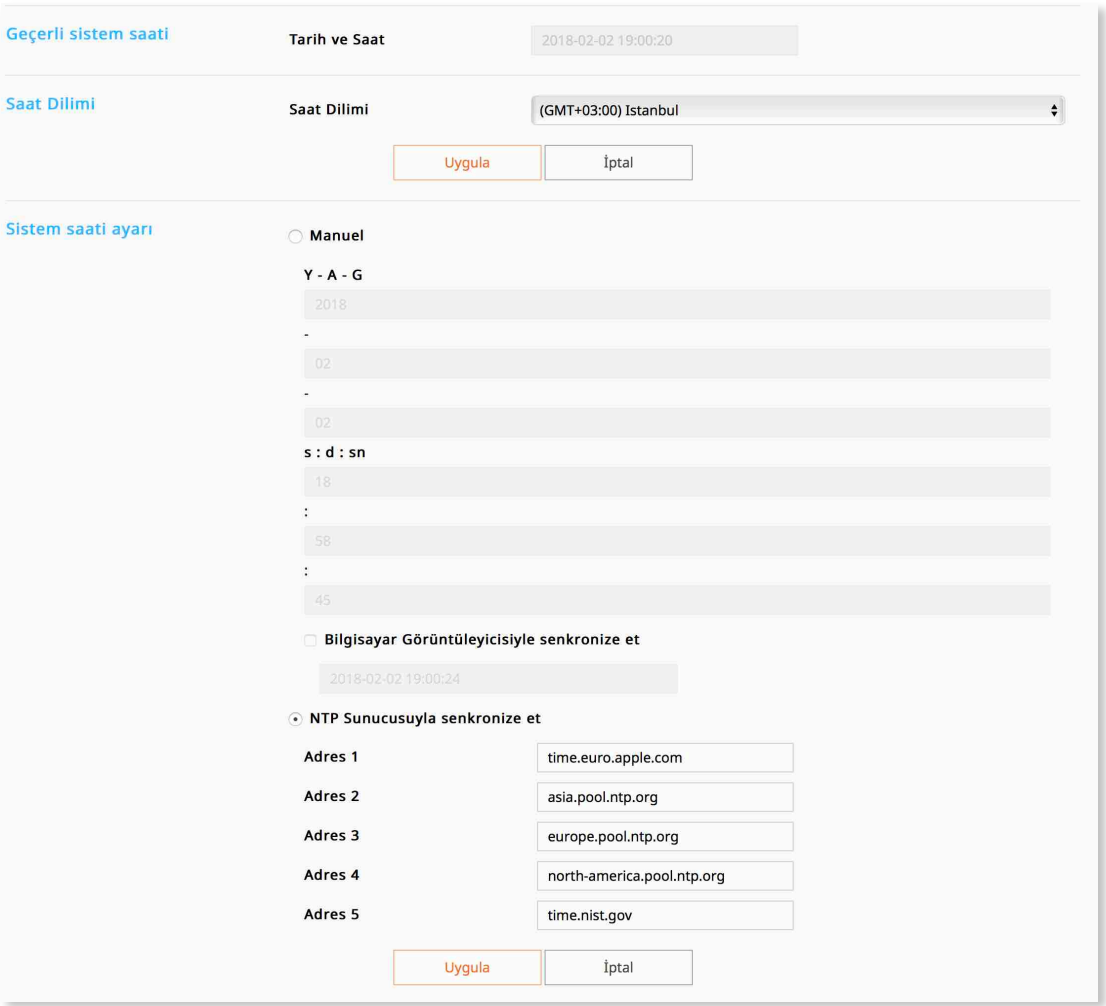
Dahili saat işlevi, tarih ve saati güncel tutar. Bir cihazı dağıtırken saatin doğru olup olmadığını kontrol etmek önemlidir. Saat, kayıtları kaydetmek ve video kaydetmek için kullanılır. Saat yanlışsa, bir ağ ihlalinde adli soruşturma çok zor olacaktır. Ayrıca, saat doğru değilse, video kanıtları mahkemede kabul edilmeyebilir. Son olarak, diğer pek çok hizmet doğru bir saat kullanır ve saat doğru ayarlanmadıysa, HTTPS, ONVIF, SNMP v3 ve 802.1x de dahil olmak üzere düzgün çalışmayabilir.

NTP protokolü, zaman içerisinde, saatin kaymasının önüne geçmek ve doğru kalmasını sağlamak için kullanılabilir. Tüm Hanwha Techwin NVR'ler, -etkinleştirildiğinde- kameraların senkronize edilmesi için bir NTP sunucusu içerir.

Güvenli Düzey

Geçerli sistem saatinin doğru ayarlanıp ayarlanmadığını kontrol etmek için kullanıcının üç yöntemi vardır:

1) IP kamera kurulumu Temel Tarih ve Saat
2) Saat dilimini seçin ve uygulanıyorsa 'Gün ışığından yararlanma saatini kullan'ı işaretleyin.
3) Saat dilimi kurulumu için 'Uygula'yı tıklayın.
4) Sistem zamanını şu şekillerde ayarlayabilirsiniz:
    - Manuel: Geçerli saati el ile ayarlamanıza izin verir
    - PC izleyici ile senkronize etme: Saati bilgisayarınızın saatine göre ayarlar
    - NTP sunucusuyla senkronize et: NTP sunucusunun saatiyle senkronize edilir (önerilen yöntem)
5) Sistem saati ayarının 'Uygula'yı tıklayın.

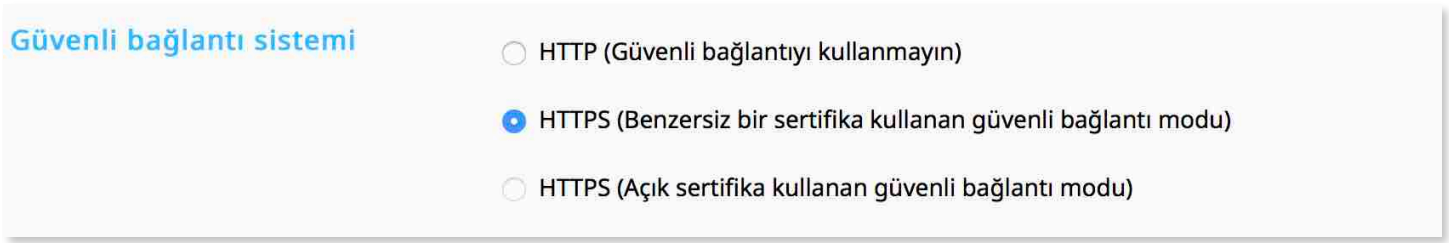


HTTPS (Hanwha Techwin sertifikası)

HTTPS (Hanwha Techwin sertifikası), cihaz ve istemci arasında güvenli bir bağlantı sağlayan bir işlevdir.

Hanwha Techwin tarafından sağlanan bir sertifika. 'HTTPS (benzersiz bir sertifika kullanarak güvenli bağlantı modu)' seçeneğini belirlerseniz, cihazın dahili sertifikası güvenli bağlantı modunda kullanılır ve ayrı bir sertifika satın alıp yüklemeniz gerekmez. Etkinleştirildiğinde, iletişim HTTPS bağlantı noktası üzerinden gerçekleşir.

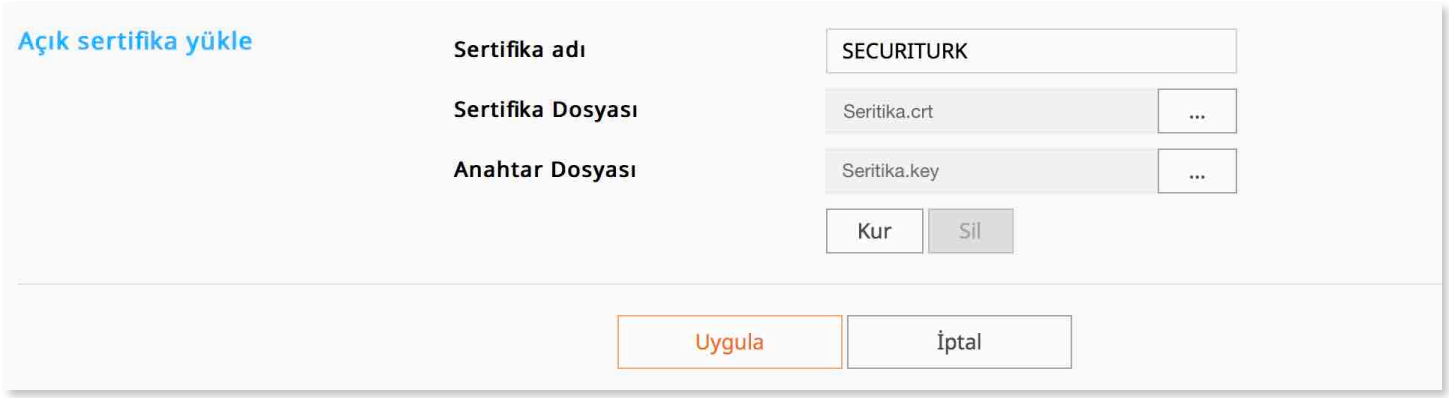
1) Ayarlar > Ağ > HTTPS Güvenli bağlantı sistemi
2) 'HTTPS (benzersiz bir sertifika kullanarak güvenli bağlantı modu)' seçin.
3) 'Uygula'yı tıklayın.



HTTPS (kimliği doğrulanmış sertifika)

HTTPS (kimliği doğrulanmış sertifika), kullanıcının cihaz ile istemci arasındaki bağlantıyı güvence altına almak için kendi yetkili sertifikalarını kaydetmesine olanak tanıyan bir işlevdir. Genel sertifika ve özel anahtarı kaydettirerek 'HTTPS (Herkese açık güvenli bağlantı modu)' seçmek mümkündür ve cihaz güvenli bağlantı modunda kullanılır.

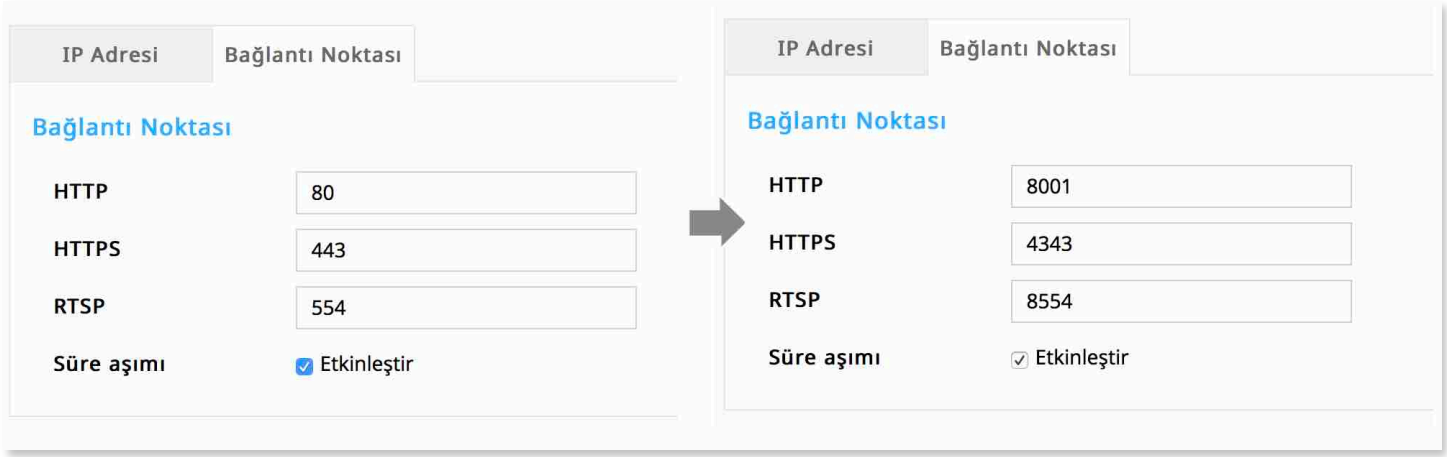
1) Ayarlar > Ağ > HTTPS Kamu sertifikası yükleyin
2) Sertifika için bir ad girin ve sertifika dosyasını ve anahtar dosyasını açın.
3) 'Yükle'yi tıklayın ve ardından HTTPS'yi seçin (genel sertifika kullanarak Güvenli bağlantı modu)
4) 'Uygula'yı tıklayın.



Varsayılan Bağlantı Noktasını Değiştirme

Bir ağ aygıtının varsayılan bağlantı noktasını iyi bilen giriş denemelerini veya saldırıları önlemek için bağlantı noktasını değiştirmeniz önerilir. 8000+ veya 10000+ gibi yaygın olanlardan daha yüksek port numaraları kullanılmalıdır. Örneğin, HTTP web servisi bağlantı noktasını 80 yerine 8000 olarak değiştirirseniz, web sunucunuzu basit tarama programlarından gelen saldırılara karşı koruyabilir veya internet tarayıcısına doğrudan adres girilerek yapılan denemelerin önüne geçmiş olursunuz.

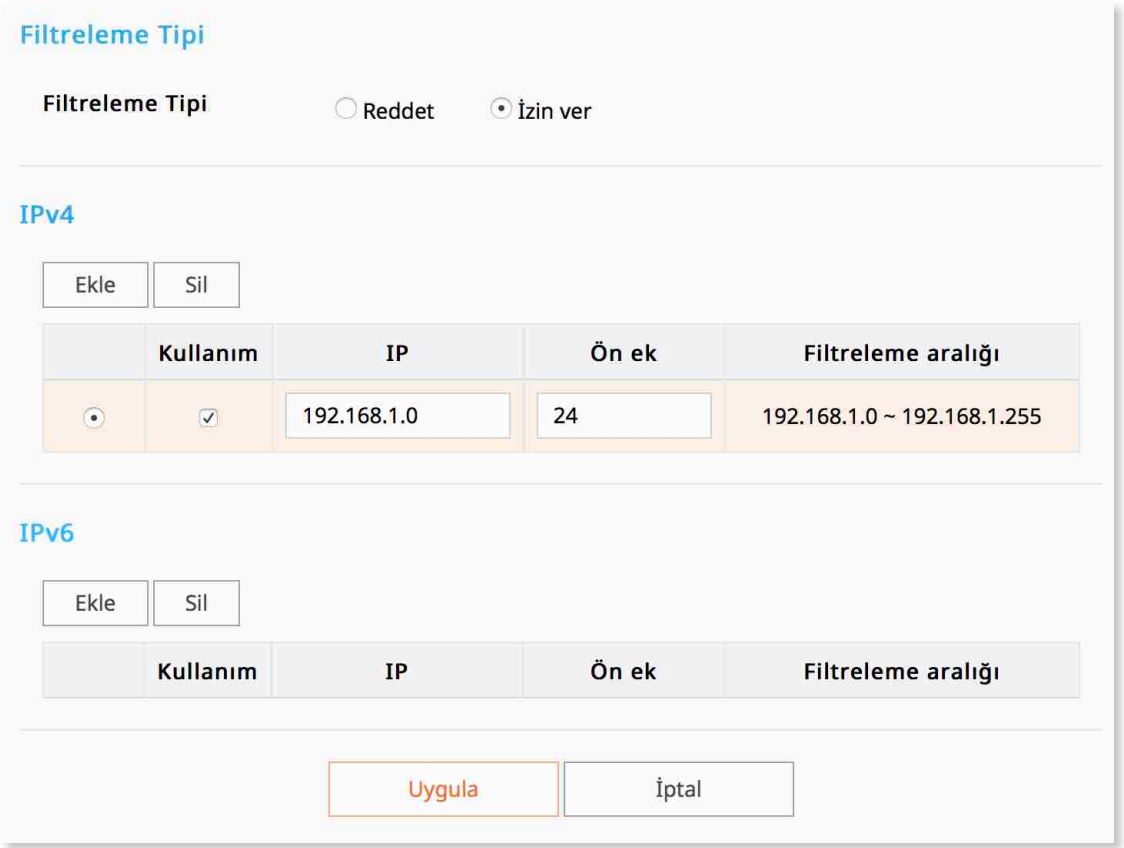
1) Ayarlar > Temel > IP ve Port > Bağlantı Noktası
2) HTTP ve HTTPS bağlantı noktası numaralarını 80'den ve 443'den yüksek bir sayıya çevirin.
3) RTSP bağlantı noktası numarasını 554'ten yüksek bir sayıya çevirin.
4) Cihaz port numarasını 4520'den farklı bir sayıyla değiştirin.
5) 'Uygula'yı tıklayın.



IP Filtreleme

Hanwha Techwin ürünleri belirli IP adreslerine erişimi sağlamak ya da reddetmek için IP listelerinin oluşturulmasını desteklemektedir. Bu, yalnızca güvenlik birimine erişimi vermek, İnternet yönlendiricisinden (Router) yalıtmak veya IP adreslerinin kablosuz havuzundan erişimi önlemek için kullanılabilir.

1) Ayarlar > Ağ > IP filtreleme >Filtreleme tipi
2) Erişim izin vermek veya erişimi reddetmek için 'Ekle'yi, ardından bir IP adresini tıklayın.
IP adresi ve ön ek girildiğinde, filtreleme IP adresi aralığı görüntülenir*.
3) 'Uygula'yı tıklayın.

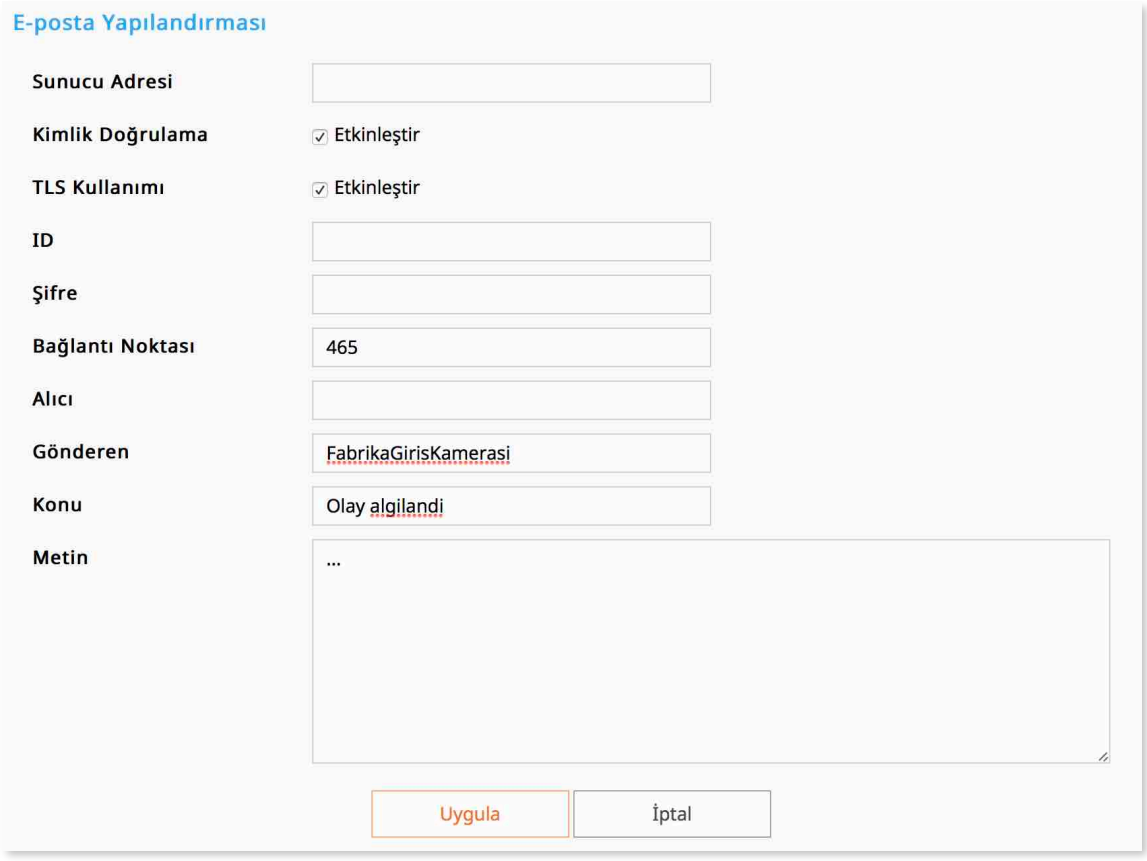


* Kurulum için halen kullanılmakta olan bilgisayarın IP adresi engellenme filtresi için eklenemez. Filtrelemeye izin vermek için PC IP adresi eklenmelidir.

TLS kullanarak e-posta gönderme

Hanwha Techwin kameraları, bir alarm veya olay meydana geldiğinde çekilen görüntülerin e-posta yoluyla iletilmesini destekler. Bu işlevi kullanırken, TLS modu, kullanıcı kimlik bilgilerinin tekrarlanan resim aktarımlarından geçmesini önlemek için kameradan posta sunucusuna güvenli e-posta iletimi yapılmasını sağlar.

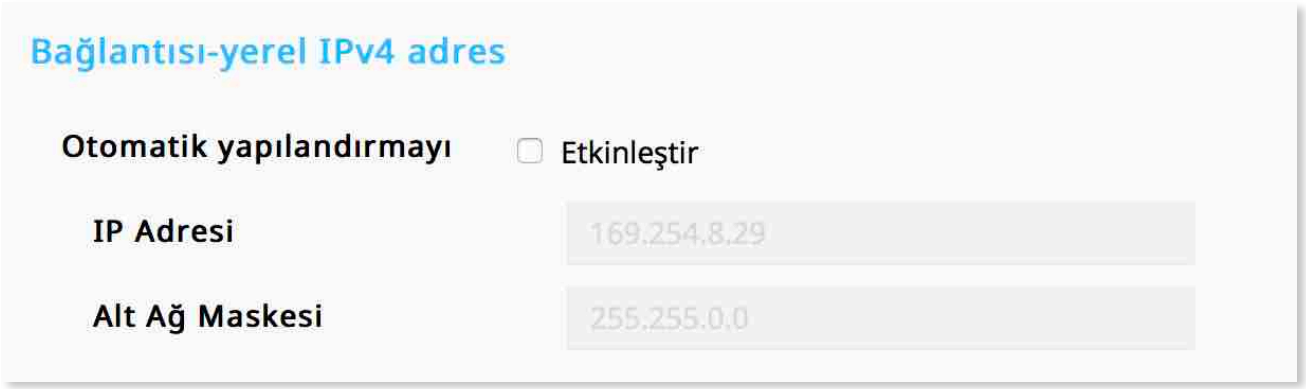
1) Ayarlar > Etkinlik > FTP / E-posta > E-posta yapılandırması
2) E-posta sunucusu adresini girin.
3) 'Kimlik doğrulama kullan' ve 'TLS kullan' için 'açık' seçeneğini belirleyin.
4) E-posta sunucusuna bağlanmak için kullanıcı hesabı kimliği ve parolasını girin.
5) E-posta sunucusu bağlantı noktası için varsayılan değer TLS ile 25 veya 465'tir. Bazı e-posta sunucuları diğer bağlantı noktalarını kullanabilir. Türkiye için bu değer 587'dir.
6) Alıcı alanına E-posta alıcısı adresini ve Gönderen alanına E-posta gönderen adresini girin.
7) E-posta konusunu ve içeriğini (Gövde) girin ve 'Uygula' düğmesine tıklayın. E-posta gönderirken alarm ve etkinlik görüntüleri ek olarak teslim edilir.



Kullanılmayan Bağlantı-Yerel IPv4 Adresini Devre Dışı Bırakma

Link-Yerel IPv4 adres otomatik yapılandırma işlevi, 169.254.xxx.xxx aralığında bir IP adresini bir DHCP sunucusuna benzer şekilde bir bağlantı yerel ağında (bir bağlantı, kamera ve kamera ile bağlanan bir ağa) atar. Ana bilgisayar aynı anahtara bağlı) IP adresi yoksa. Hizmetin gereksiz olduğunu düşünüyorsanız, ek güvenlik için hizmeti devre dışı bıraktığınızdan emin olun.

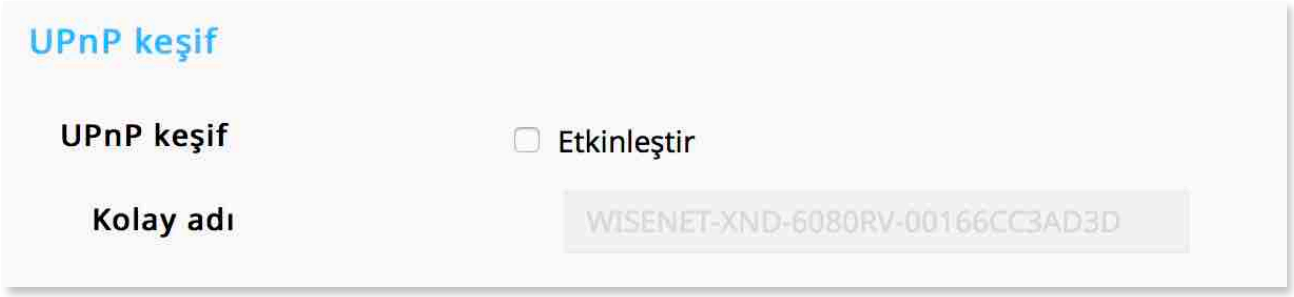
1) Ayarlar > Ağ > Otomatik IP yapılandırması > Bağlantı-Yerel IPv4 adresi
2) 'Otomatik yapılandır' onay kutusunun işaretini kaldırın.
3) 'Uygula'yı tıklayın.



Kullanılmayan UPnP'yi Devre Dışı Bırakma

UPnP bulma işlevi, istemciler ve işletim sistemleri için otomatik UPnP protokol aramasını destekler. İşletim Sistemi'ndeki grafik arayüzlerden kolay görüntüleme ve cihazlara erişime izin verirken, izinsiz kişilerin cihazla ilgili bilgi almasına izin verebilir. UPnP bulma işleminin UPnP Otomatik Yöneltme Yönünden ayrı olduğunu unutmayın. Hizmetin gereksiz olduğunu düşünüyorsanız, hizmeti ayarlamayı devre dışı bırakmak isteyebilirsiniz.

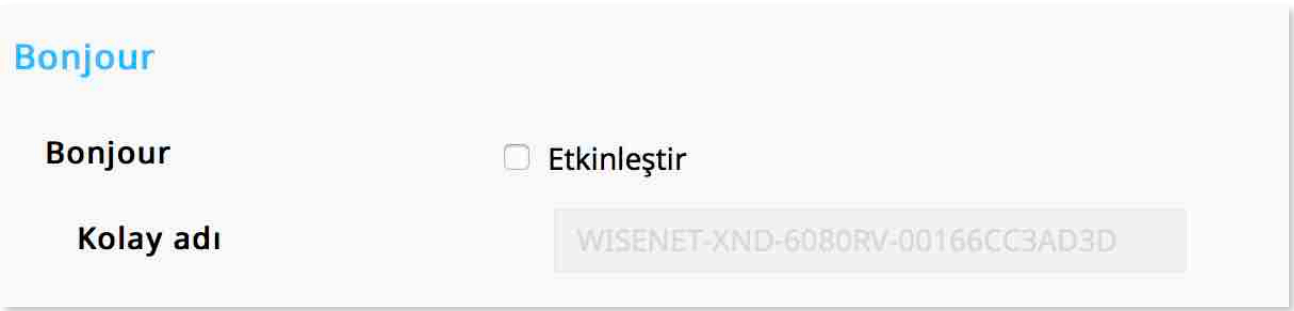
1) Ayarlar > Otomatik IP yapılandırması > UPnP keşfi
2) 'UPnP bulma' seçeneğinin işaretini kaldırın.
3) 'Uygula'yı tıklayın.



Kullanılmayan Bonjour'u Devre Dışı Bırakma

Bonjour işlevi, Bonjour protokolünü destekleyen istemci ve işletim sisteminin kameraları otomatik olarak aramasına izin verir. İşletim Sistemi'ndeki grafik arayüzlerden kolay görüntüleme ve cihazlara erişime izin verirken, izinsiz kişilerin cihazla ilgili bilgi almasına izin verebilir. Hizmetin gereksiz olduğunu düşünüyorsanız, ek güvenlik için hizmeti devre dışı bıraktığınızdan emin olun.

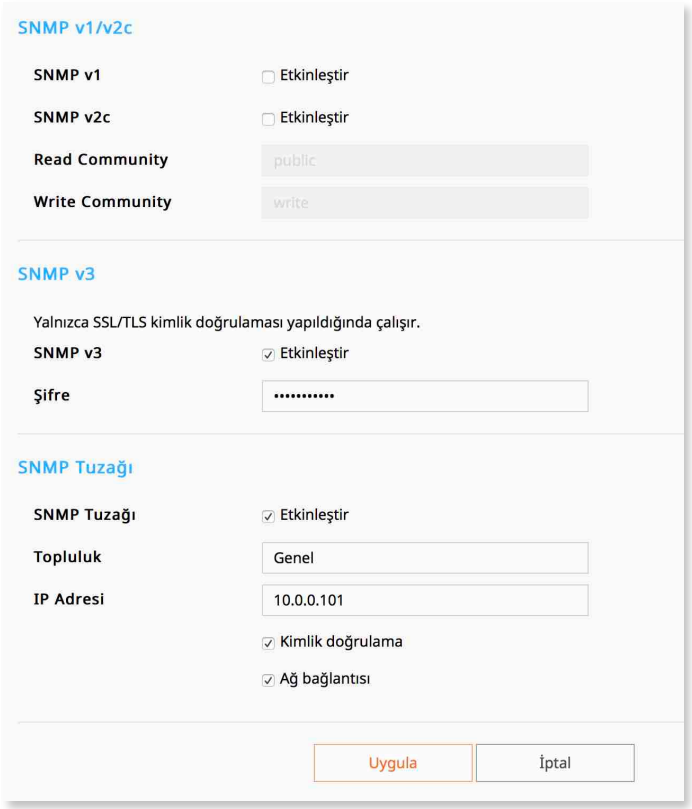
1) Ayarlar > Otomatik IP yapılandırması > Bonjour
2) 'Bonjour'un işaretini kaldırın.
3) Uygula'yı tıklayın.



SNMP'yi Güvenli Kullanma

SNMP, ağ aygıtlarını rahatça yönetme olanağı sağlar. Bununla birlikte, SNMP v1 ve v2c açık metin dizeleri kullandıkları için savunmasızdır. Bu işlevi kullanmak istiyorsanız, yalnızca güvenli SNMP v3'ü kullanmanız önerilir. SNMP v3, kamera HTTPS modunda çalışırken kullanılabilir.

1) Ayarlar > Ağ > HTTPS Güvenli bağlantı sistemi
2) 'HTTPS (benzersiz bir sertifika kullanarak güvenli bağlantı modu) seçin.'
3) 'Uygula'yı tıklayın.
4) Ağ > SNMP
5) SNMP v1 ve SNMP v2'yi devre dışı bırakın.
6) SNMP v3'ü etkinleştirin ve şifreyi ayarlayın.

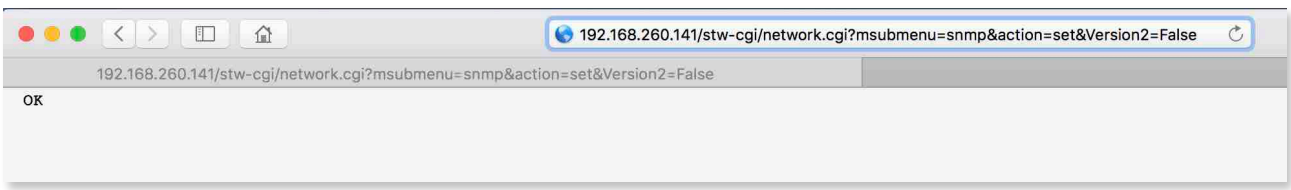


Kullanılmayan SNMP'yi Devre Dışı Bırakma

SNMP v1, v2c ve v3 sürümleri aynı anda desteklenebilir. Birçok model, SNMP'nin web görüntüleyici arayüzü aracılığıyla tamamen devre dışı bırakılmasına izin vermez. Tüm SNMP protokollerini devre dışı bırakmak için Wisenet Aygıt Yöneticisi'ni kullanın veya aşağıdaki komutları gönderin:

• SNMP v2c Devre Dışı Bırakma
http: // (IP adresi) /stw-cgi/network.cgi?msubmenu=snmp&action=set&Version2=False

• SNMP v1 Devre Dışı Bırakma
http: // (IP adresi) /stw-cgi/network.cgi?msubmenu=snmp&action=set&Version1=False

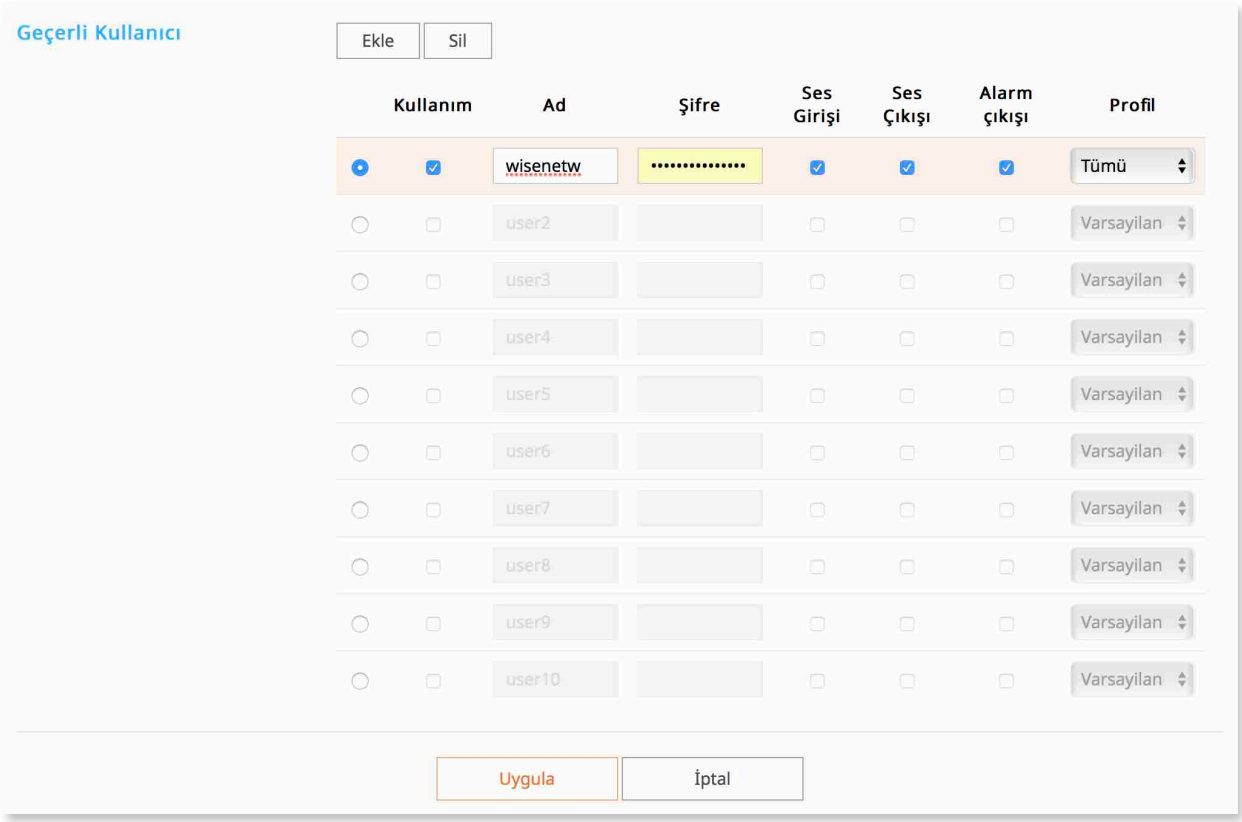


Ek Kullanıcı Hesapları Oluşturma

Cihaza, yalnızca bir yönetici hesabı ile erişmek, yönetici şifresinin ağ üzerinden sürekli iletilmesine neden olur. Bu, kötü niyetli kişilere hassas bilgileri gösteren bir güvenlik açığına neden olabilir. Dahası, yönetici düzeyinde erişime olan bağımlılık, tüm kullanıcıların ayrıcalıklarını artırır. Her kullanıcının yalnızca yanlışlıkla veya kötü amaçlı ayar değişikliklerini önlemek için iş işlevlerini yerine getirmek için gereken az miktarda ayrıcalığa sahip olması gerekir. Bu nedenle, yalnızca yapılandırma için yönetici hesabını kullanarak ve sık kullanılan video izleme özellikleri gibi sınırlı ayrıcalıklara sahip kullanıcı hesaplarını ekleyerek güvenliğinizi geliştirebilirsiniz.*

1) Ayarlar > Temel > Kullanıcı > Geçerli kullanıcılar
2) Eklenecek hesabı seçtiğinizde, ayar maddeleri etkinleştirilir.
3) 'Kullan'ı işaretleyin, ardından adı ve parolayı girin.
4) Ses girişi / çıkışı ve alarm çıkışı kullanıp kullanmamayı seçin.
5) Bir profil seçin ve 'Uygula'yı tıklayın.

* PTZ / balıkgözü kameraların PTZ izni ayrıca ayarlanmalıdır.



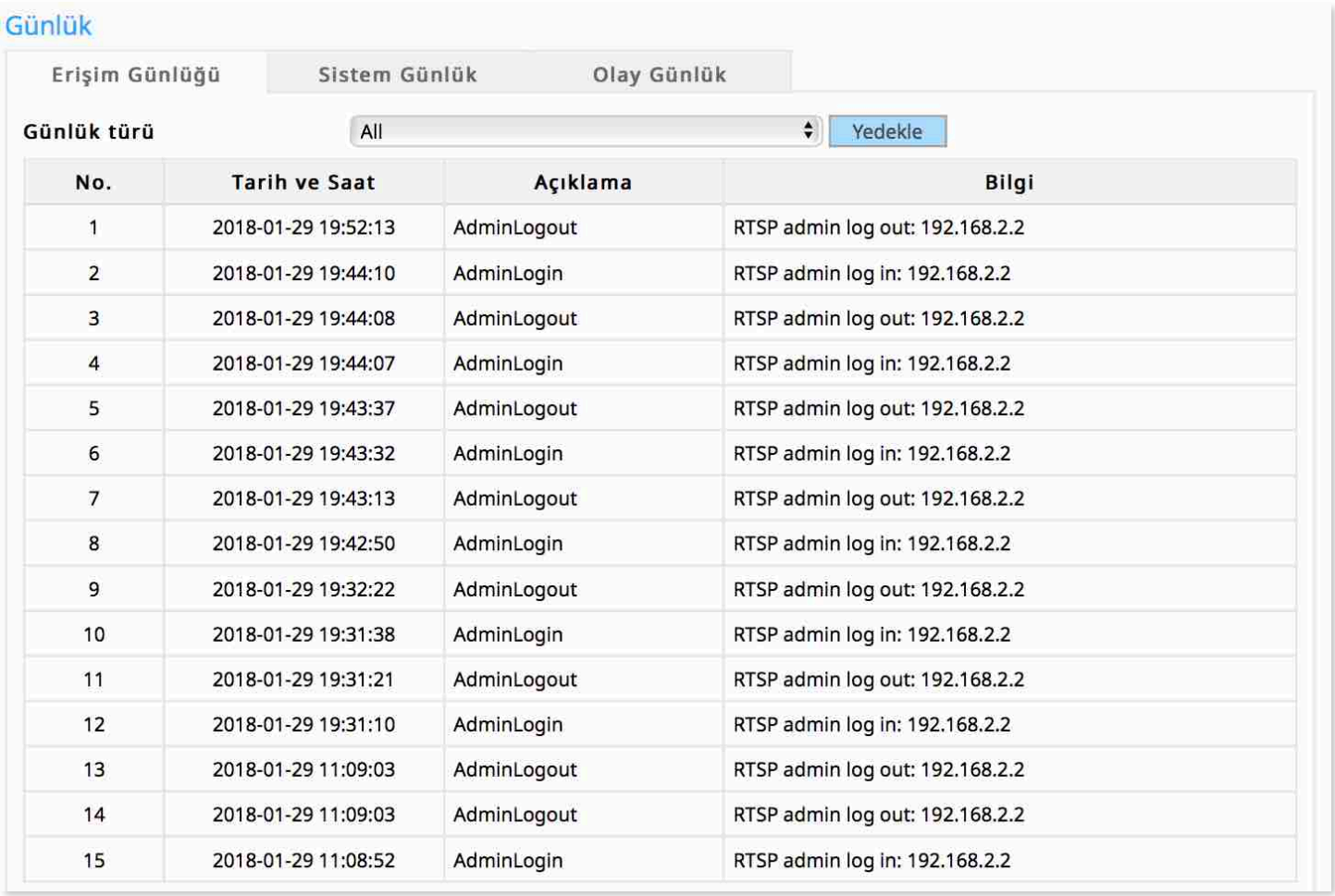
Günlüğü Kontrol Etme

Yöneticiler, kötü niyetli amaçlarla yetkisiz erişime ve cihazdaki değişiklikleri kanıtlamak için sistemde depolanan günlükleri analiz edebilirler. Aygıt erişimi, sistem ayarı değiştirme ve olay geçmişi gibi çeşitli bilgileri kontrol edebilirsiniz. Günlükler, bir ağ sisteminin güvenliğini artırmak için önemli veriler olarak hizmet eder. Günlük verilerinin kontrol edilmesi ve analiz edilmesi gerekçesi şu şekildedir:

- Sistemde oluşan hatalar (hatalar ve güvenlik konuları dahil) kaydedilir ve faydalı bir ipucu haline gelir.
- Sistemdeki hataları aramaktadır.
- Olası sistem problemlerini tahmin etmek için kullanılabilir.
- Sorun çıkması durumunda kurtarma için bilgi olarak kullanılabilir.
- İhlalin kanıtı olarak kullanılabilir.
- Günlük yönetimi, çeşitli yasalar ve yönergeler tarafından zorunlu kılınmıştır.

Örneğin, şifre girişiniz art arda başarısız olursa, hesabınız kilitlenebilir. Erişim günlüğü aramaları, çok sayıda oturum açma hatası veya hesap kilitlemesi gibi bu tür saldırıları tanımlayabilir.

• Ayarlar > Sistem > Kullanıcı Günlüğü



No.	Tarih ve Saat	Açıklama	Bilgi
1	2018-01-29 19:52:13	AdminLogout	RTSP admin log out: 192.168.2.2
2	2018-01-29 19:44:10	AdminLogin	RTSP admin log in: 192.168.2.2
3	2018-01-29 19:44:08	AdminLogout	RTSP admin log out: 192.168.2.2
4	2018-01-29 19:44:07	AdminLogin	RTSP admin log in: 192.168.2.2
5	2018-01-29 19:43:37	AdminLogout	RTSP admin log out: 192.168.2.2
6	2018-01-29 19:43:32	AdminLogin	RTSP admin log in: 192.168.2.2
7	2018-01-29 19:43:13	AdminLogout	RTSP admin log out: 192.168.2.2
8	2018-01-29 19:42:50	AdminLogin	RTSP admin log in: 192.168.2.2
9	2018-01-29 19:32:22	AdminLogout	RTSP admin log out: 192.168.2.2
10	2018-01-29 19:31:38	AdminLogin	RTSP admin log in: 192.168.2.2
11	2018-01-29 19:31:21	AdminLogout	RTSP admin log out: 192.168.2.2
12	2018-01-29 19:31:10	AdminLogin	RTSP admin log in: 192.168.2.2
13	2018-01-29 11:09:03	AdminLogout	RTSP admin log out: 192.168.2.2
14	2018-01-29 11:09:03	AdminLogout	RTSP admin log out: 192.168.2.2
15	2018-01-29 11:08:52	AdminLogin	RTSP admin log in: 192.168.2.2

Çok Güvenli Düzey

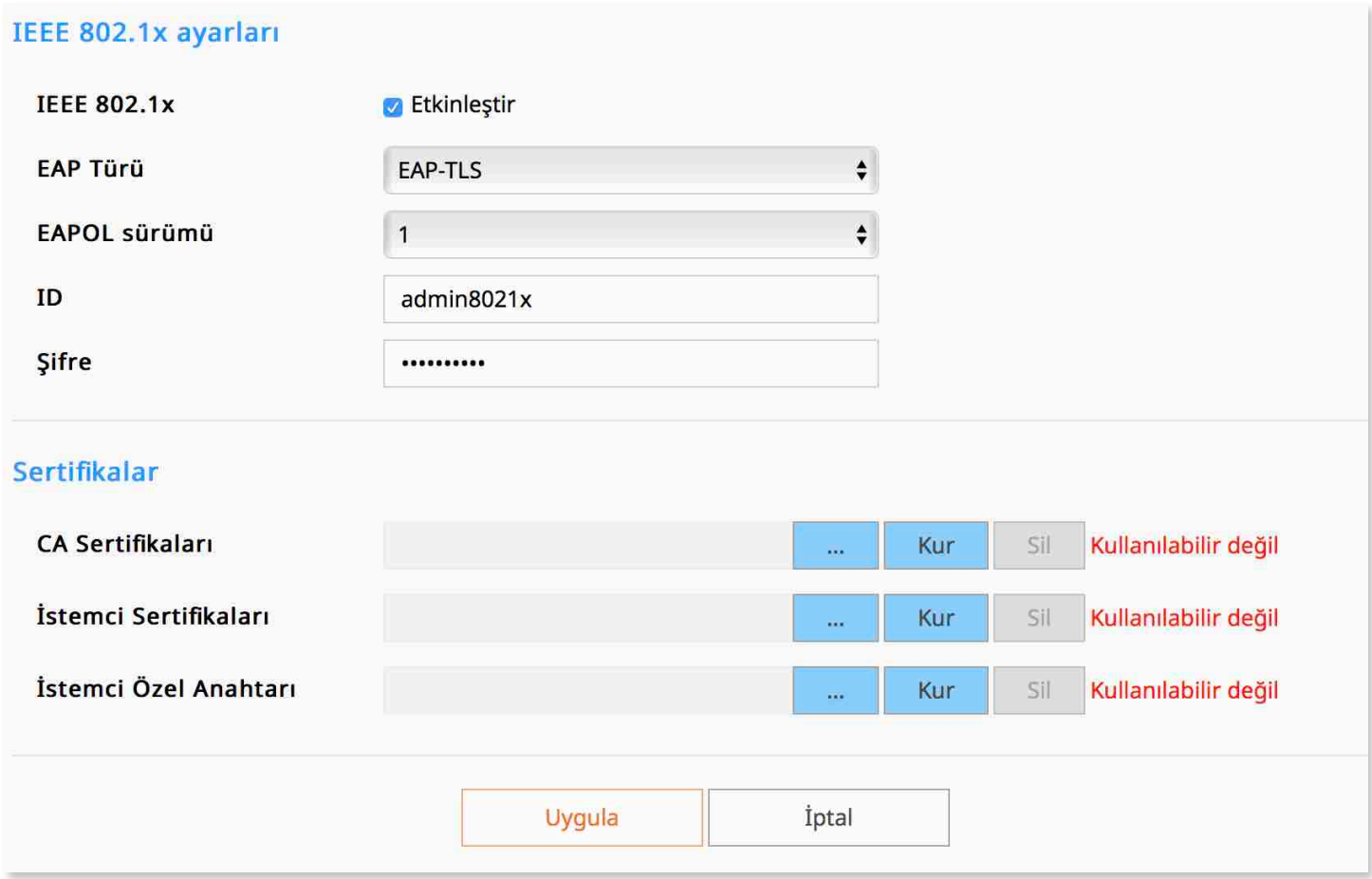
802.1 X Sertifika Tabanlı Erişim Kontrolü

Birçok binada, ağ jaklarına ulaşılabilir, ethernet ağı altyapısına erişmek için bir kamera fişi çekilebilir veya kablolar sabote edilebilir. 802.1x standardı, korunan ağa erişmek için bağlı olan her aygıta kurulacak belirleyici bir sertifikaya ihtiyaç duyan bağlantı noktası tabanlı ağ erişim kontrolü sağlar. Böylece bir saldırgan izinsiz bir aygıtı ağa takarsa erişim engellenecektir. Bağlantı noktası tabanlı erişim denetimini ayarlama ağ aygıtlarının tamamı için, ağ anahtarları, ortam dönüştürücüleri, yazıcılar ve kablosuz erişim noktaları (AP'ler) de dahil olmak üzere ağ üzerindeki tüm aygıtları bir araya getirerek daha sağlam bir ağ güvenlik ortamı sağlar.

Hanwha Techwin ürünleri, sertifikalar gerektiren standart bir yöntem olan 802.1x EAP-LEAP ve EAP-TLS'yi desteklemektedir.
Bu özelliği kullanmak için 802.1x ve 802.1s kimlik doğrulama sunucusunu, aygıt sertifikalarını ve özel anahtarı destekleyen bir ağ anahtarına (veya köprü, kablosuz AP vb.) ihtiyacınız vardır. 802.1x yapılandırması, genellikle, güvenli bir ağa taşınmadan önce izole edilmiş bir ağda veya VLAN'da gerçekleştirilir.

1) Ayarlar > Ağ > 802.1x > IEEE 802.1x ayarı
2) 'Kullan' seçeneğini işaretleyin ve EAP türünü seçin.
3) EAPOL sürümünü seçin.
4) Müşteri sertifikasının kimliğini ve şifresini giriniz.
5) Bir CA sertifikası yükleyin
6) Bağlantı noktası tabanlı erişim kontrolü için bir istemci sertifikası ve özel anahtar yükleyin*
7) 'Uygula'yı tıklayın.

* İstemci sertifikası ve özel anahtar, RADIUS sunucusu ve istemci aygıtı arasındaki TLS iletişimi için kullanılır.



Özet

Cihazların birbirine bağlı olduğu günümüz dünyasının acımasız gerçekliği, bireylerin ve grupların güvenlik açıklarını belirlemek ve bunlardan yararlanmak için ağ güvenliğini aşma girişimlerine devam ettikleridir. Birbirine bağlı bilgisayar ağları vasıtasıyla giderek artan sayıda cihazdan yararlanıyor olmamız, yetkisiz kişilerin bu ağlara erişim olasılığını artırıyor. Bilgisayar korsanlarından korunmak için birbirine bağlı bu cihazlarda, açık bir kapı olması önlenmeli ve emniyet altına alınmalıdır. Bilinen ve yukarıda ayrıntılarıyla anlatılmış bu en iyi yöntemlerin kullanılması, yalnızca ağa bağlı video gözetim aygıtlarının sistemlere giriş noktaları olarak kullanılmasını engellemekle kalmaz, aynı zamanda bu kritik işlevin bütünlüğünü ve sürekliliğini sağlar; böylece insanların ve varlıkların güvenliğini de sağlar. Bu adımların birçoğu dünya standardıdır, diğer ağa bağlı aygıtlar ve sistemler için de geçerlidir.

Bu nedenle, ağ güvenliği için bilinen en iyi yöntemleri kullanmak, ağlarının güvenliğini sağlamanın önemini fark eden ciddi kuruluşlar için zorunluluktur. Ağa bağlı iş yapan bütün tarafların bunları konuşması gerektiğini gösterir. Son kullanıcı, BT bölümü, ağ kurulumcu ve güvenlik sistemi kurulumcusu arasında açık ve bilgilendirmeye dayalı yapıcı diyalog, bir kurumun güvenlik ihtiyaçlarına en iyi çözüm bulmanın anahtarıdır.

Hanwha Techwin ürün güvenliğini denetler, kendi güvenlik ekibi ve uzmanlaşmış kurum tarafından geliştirme safhasındaki güvenlik açığını tanılar. Kişilerin güvenebileceği bir güvenlik için tüm ürünlere kullanıcı kimlik doğrulaması, veritabanı şifreleme, bellenim şifreleme, arka kapı kaldırma ve sıkı şifre kimliği kuralı gibi sıkı politikalar uygulanır.

Hanwha Techwin America
500 Frank W. Burr Blvd. Suite 43, Teaneck, NJ
07666
Toll Free : 877.213.1222
www.HanwhaSecurity.com

SECURITURK
Elektronik Güvenlik Sistemleri
D-100 Güney Yan Yol No:25 Lapis Han Ofis:
2069 Kartal, İstanbul / Türkiye
Telefon: 0850 259 30 00
www.securiturk.com