WISENET

Teknik Belge

Kurulumcu El Kitabı

Ağ Güvenlik Açıklarına Karşı Video Gözetleme Aygıtlarını Koruma

SECURITURK

Hanwha Techwin

Belge No: S20182B0002

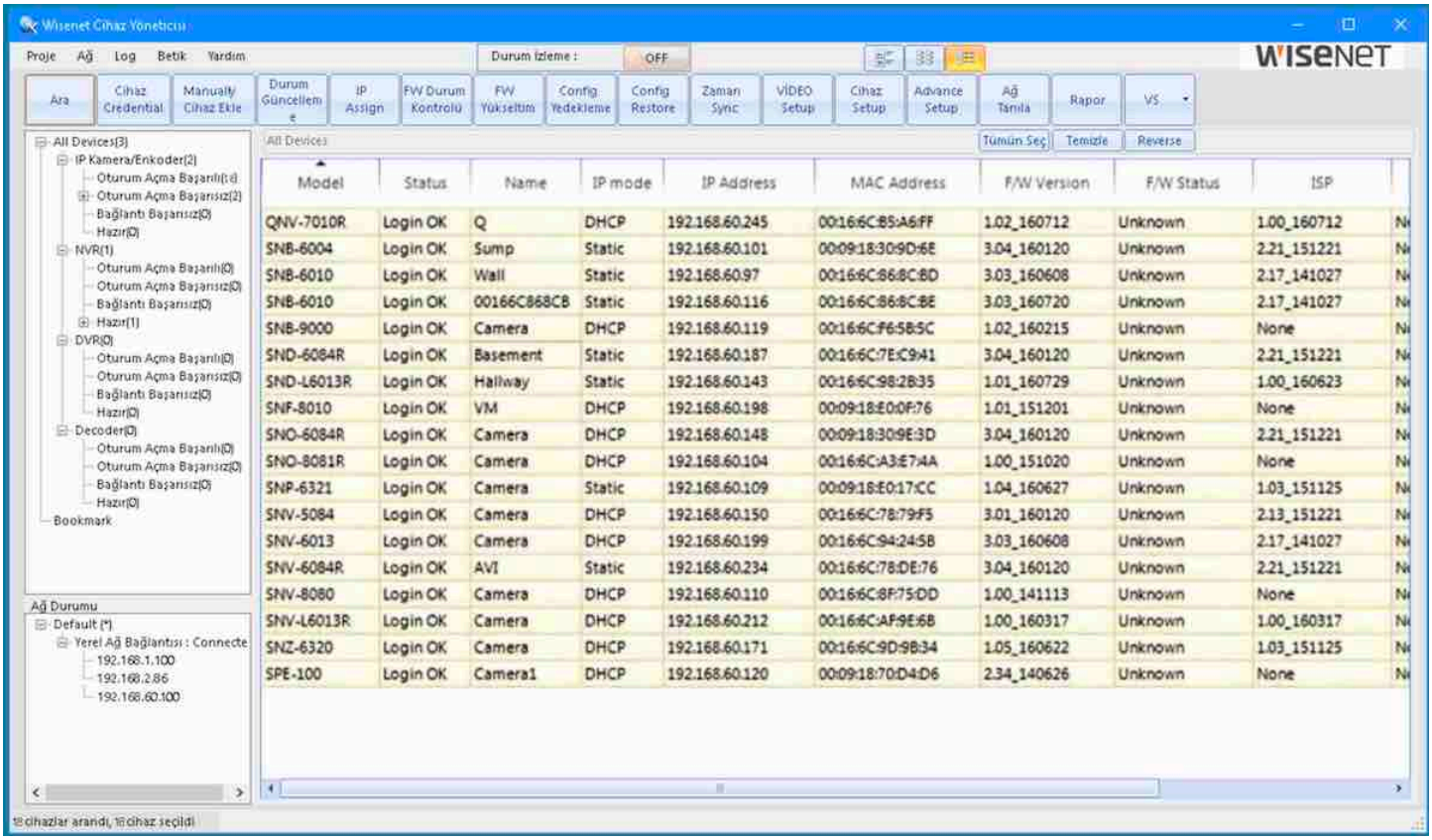
Giriş

Gittikçe birbirine daha bağlı dünyada, daha fazla cihaz ve sistemin diğer sistemlerle bağlandığı ve paylaşıldığı bir dünyada yaşıyoruz. İnsanların istedikleri her yerde cihazlara ve sistemlere bağlanma, bunları kontrol etme beklentisi, bu trendin arkasındaki ana itici güçtür.

Bununla birlikte, gittikçe artan sayıda ağa bağlı cihazın sağladığı eşi benzeri görülmemiş kolaylık seviyesinin bir dezavantajı, artan güvenlik riskidir. Her cihaz, ağlar için bir son nokta olduğu için, bilgisayar korsanlarının ve diğerlerinin kötü niyetli giriş noktaları olma potansiyelini de beraberinde getirirler. Aslında, son zamanlarda meydana gelen en yüksek seviyedeki veri ihlallerinin çoğunda bilgisayar korsanları, POS, HVAC ve diğer ağa bağlı ve bu tür ihlalleri önlemek için yeterli düzeyde güvenlik önlemi olmayan sistemler aracılığıyla şirket ağlarına girişte başarılı oldu.

IP tabanlı olan video gözetimi ve diğer çözümler, popülerlik kazanarak yeni kurulumlar ve güncellemler için kabul gören standart haline gelirken güvenlik sistemleri bir istisna değildir. Bir bilgisayar korsanı, ağa bağlı cihazlar arasında güvenlik gibi kritik bir işlevi yerine getirip getirmediğini bakmaz. Bu nedenle, video gözetim kameraları ve diğer cihazlar, girilebilir zayıf noktalar için araştırılan potansiyel ağ giriş noktalarının uzun listesinin bir parçasıdır. Bu nedenle, kuruluşların ağları ve IP kameraları, kodlayıcıları(enkoder), Ağ Video Kayıt Cihazları(NVR) ve Sayısal Video Kayıt Cihazları (DVR) için en üst düzeyde güvenlik sağlamak için gerekli önlemleri almaları önemlidir. Yetkisiz girişi önlemek ve son kullanıcıların video gözetim sistemleri ve genel ağını korumak için cihaz güvenliğini güçlendirmek üzere üstlenilmesi gereken çok sayıda uygulama bulunmaktadır. Hanwha sadece bu en iyi uygulamalardan haberdar olmakla kalmaz, aynı zamanda kuruluşların ağ güvenliğini geliştirmeye yönelik bu önemli adımları atmalarını kolaylaştırmak için ürünlerine birtakım teknolojiler ve yetenekler kurmuştur. Bu öğeler, güvenlik sisteminin sahibi, BT personeli ve Sistem Kurulumcuları sistemlerini kurarken, kullanım kolaylığı ile kabul edilebilir riskleri dengelerken gerekli güvenlik seviyesini belirlemek için gözden geçirilmelidir.

Bu kılavuz, mümkün olduğunda ağ kameralarından görüntüler gösterecektir. Çoğu ayar, Wisenet Aygıt Yöneticisi Yazılımını kullanarak birden çok kamera için toplu olarak düzenlenebilir (Resim 1).



Resim 1

Şifreler

E-postayı kontrol etmekten akıllı telefonların kilidini açmaya veya bilgisayarlara giriş yapmaya, şifreler günlük hayatımızda ayrılmaz bir parçadır. Dolayısıyla, insanların cihazlarını ve ağlarını korumak için güçlü parolalar oluşturmanın önemini farketmelerine rağmen bu durum gerçekte bu her zaman böyle değildir. Aşağıdaki açıklamalar, en üst düzeyde parola güvenliğini sağlamaya yardımcı olacaktır.

1. Varsayılanları Değiştir

Kurulumcular ve / veya son kullanıcılar çok sık olarak, IP kameralar, kodlayıcılar(enkoder), Ağ Video Kayıt Cihazları(NVR) ve Sayısal Video Kayıt Cihazları (DVR) da dahil olmak üzere IP cihazları için varsayılan şifreleri değiştirme adımını atlamakta ya da unutmaktadırlar. Varsayılan şifreler çevrimiçi veya kullanıcı kılavuzlarında kolaylıkla bulunabilir, bu da cihazları güvensiz kılar ve saldırılara karşı oldukça savunmasız bıraktığından kritik önem taşır. Bu nedenle, varsayılanları değiştirme, belki de aygıtları güvence altına almanın en önemli ilk adımıdır.

Temel> Kullanıcı>

Hanwha şifreleri, uzunluğa bağlı olarak en az 8 karakter ve 2/3 karakter kategorisi (Küçük Harf, Büyük Harf, Rakamlar ve Özel Karakterler gibi) gerektirir. Buna ek olarak, 4 veya daha fazla ardışık veya tekrarlanan karakterlere izin verilmez. Özel karakterlere izin verilir. Parolaların maksimum uzunluğu 15 karakterdir (Resim 2).

Resim 2

2. Sık Yapılan Hatalar

Sadece şifreyi değiştirmek yeterli değildir. Şifre ile yetki gerektiren işlevlerin çokluğu nedeniyle, birçok insanın şifreler oluştururken kolaylık olması için iki hatası yapar. Şifre oluşturulurken çoğunlukla her ikisini de birden yapar.

Birincisi her şey için aynı şifreyi kullanmaya çalışır. Burada tehlike birisi, örneğin e-posta hesabınız için şifreyi deşifre edebilirse, parola korumalı olduğunuz her şeye erişebilir ve böylece hırsızlık, kimlik hırsızlığı ve diğer pek çok olasılığı açabilir. Kullanıcıların şifrelerini daha kolay hatırlamak için yaptıkları ikinci ve en riskli hata, sözlükte bulunan isimleri, doğum tarihlerini ve / veya kelimeleri kullanmalarıdır.

Hacking, parolaları çözmek için muhtemel sözcük kombinasyonları arasında hızlı ve otomatik olarak dönen teknolojiler gibi güçlü araçlar kullanan, oldukça organize ve sofistike bir uygulama haline geldi. Bu araçlar, kullanıcılar için kolayca hatırlanan şifreleri bulmakta oldukça başarılı olmuştur. Ek olarak, çok fazla kişisel bilgi çevrimiçi olduğundan, adları, doğum günlerini veya diğer önemli tarihleri kullanan şifreler aynı zamanda kırılabilir.

Bu nedenle, kırmak için çok daha zor, güçlü parolaları kullanmak zorunludur. Harfler, rakamlar ve diğer sembollerin birleşimini kullanmak en iyisidir.

Örneğin, Hanwha aygıtları, en az sekiz karakter uzunluğunda, büyük harf, küçük harf, sayı ve simgeden en az üç karakter kümesi içeren parolalar gerektirir. 10 karakterden uzun parolalar yalnızca iki karakter kümesi gerektirir. Buna ek olarak, parolalar aynı karakteri 3 kez tekrarlayamaz veya 3 ardışık karakterden fazla olamaz.

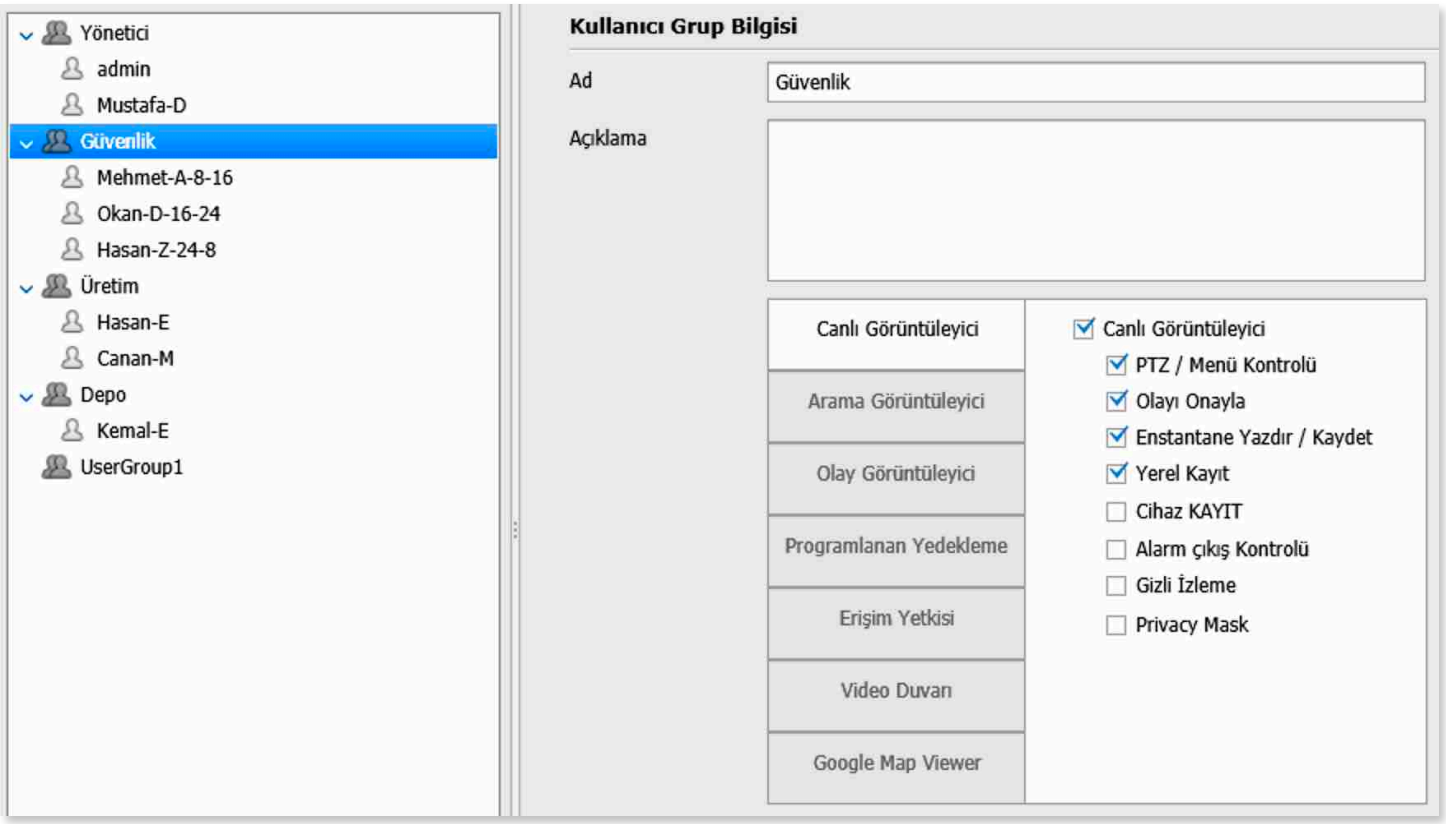
3. Çoklu Kimlik Bilgilerinden Yararlanma

Gerekli olmamakla birlikte, her cihaz için farklı şifreler kullanmak veya aynı şifreyi yalnızca şebekede bulunan cihazların, müşterilerin ve sistemlerin hepsi değil - bazıları için kullanmak iyi bir uygulamadır. Bağlanmak için VMS ve diğer istemciler için yönetici hesabı kullanmak yerine benzersiz bir kullanıcı adı oluşturmak çok önemlidir. Yeni başlayanlar için bunun anlamı, yönetici şifresinin ağ üzerinde sürekli kullanılmasının önüne geçilmiş olur. İkinci olarak, bu benzersiz hesapla ilişkili yetkilendirmeyi sınırlandırmak, bir bilgisayar korsanının erişimini de sınırlar. Bu nedenle, bir hesap tehlikeye atılsa bile , etkisi bütün kameraları kapsamayacaktır. Son olarak, benzersiz kimlik bilgileri, analiz günlüklerini çok daha kolay ve bilgilendirici hale getirir.
Hanwha kameraları ve kayıt cihazları, Resim 3'de gösterildiği gibi birçok kullanıcı / kullanıcı grubunun çeşitli izinler ve kullanıcı seviyeleri ile oluşturulmasına izin verir.

Temel> Kullanıcı>

Resim 3

Misafir Erişimi



Resim 4

Hanwha kameraları kullanıcı adı ve parola korumalı ayrı bir konuk oturum açma özelliği sağlamaktadır. Bu hesabın sınırlı yetkileri vardır ve varsayılan olarak etkin değildir. Bu nedenle kurulum menüsünde özel olarak açılarak kullanılabilir. Bu, sınırlı erişim kullanımları için idealdir, ancak gerekmedikçe devre dışı bırakılmalıdır. Resim 5.

Temel> Kullanıcı

Resim 5

En Az Ayrıcalık İlkesi

Bir diğer en iyi uygulama ise kullanıcının, ses, PTZ, alarm G / Ç gibi hangi özelliklere erişebileceğini sınırlandırmaktır. Kullanıcıya gerekli işlevleri yerine getirmek için gereken asgari özellikleri sunarak en düşük ayrıcalık ilkesini kullanın. Kurulum menüsüne yılda bir kez erişmeleri gerekiyorsa, VMS hesabına tam erişime izin vermek yerine web arayüzünden alternatif bir kullanıcı girişi sağlayın veya daha iyi bir seviyede kullanıcı bu rutin olmayan görevi gerçekleştirsin. Bu, “işletici tarafından" yapılandırma değişikliklerini önlemeye yardımcı olur ve ağdaki üst düzey kimlik bilgilerini mümkün olduğunca saklar. Konfigürasyon seçenekleri Resim 4'deki kamera ve kaydedici ekranlarında gösterilmektedir.

Kimlik Doğrulama ve Şifreleme

Kullanıcı kimlik doğrulaması, kullanıcı adı ve parolalarını ağ üzerinden göndermeyi gerektirdiğinden, en güçlü şifreler bile bu aktarım sırasında kolayca çalınabilir. Bu nedenle, mevcut en güvenli kimlik doğrulama ve şifreleme yöntemlerini seçmek zorunluluktur.

Özetleme ve Temiz Metin Doğrulama

Geleneksel olarak, kullanıcı adları ve şifreler, ağ üzerinden trafik bilgilerini izleyerek bir cihazın bilgilerinin çalınmasına olanak sağlayan ve herkese açık erişim sağlayan düz metin ve base64 kodlamayla gönderilir. İkinci, daha az yaygın olan bir yöntem ise hash fonksiyonunu kullanarak verileri şifrelemek için digest kimlik doğrulamasını kullanıyor ve daha sonra bu cihazda karışık kimlik bilgileriyle karşılaştırılıyor. Sonuç olarak, sindirme kimlik doğrulaması, ağ üzerinden gerçek kullanıcı adlarını ve şifreleri göndererek güvenliği güçlendirir.

Bütün Hanwha Techwin ürünleri digest şifrelerini desteklerken, aynı şey bir aygıta bağlanan her istemci için söylenemez. Bu nedenle, tüm müşterilerin a) çalışmasını sağlamak için yeteneklerini belirlemek ve b) açık metin veya base64 şifrelerine geri dönmemek önemlidir.

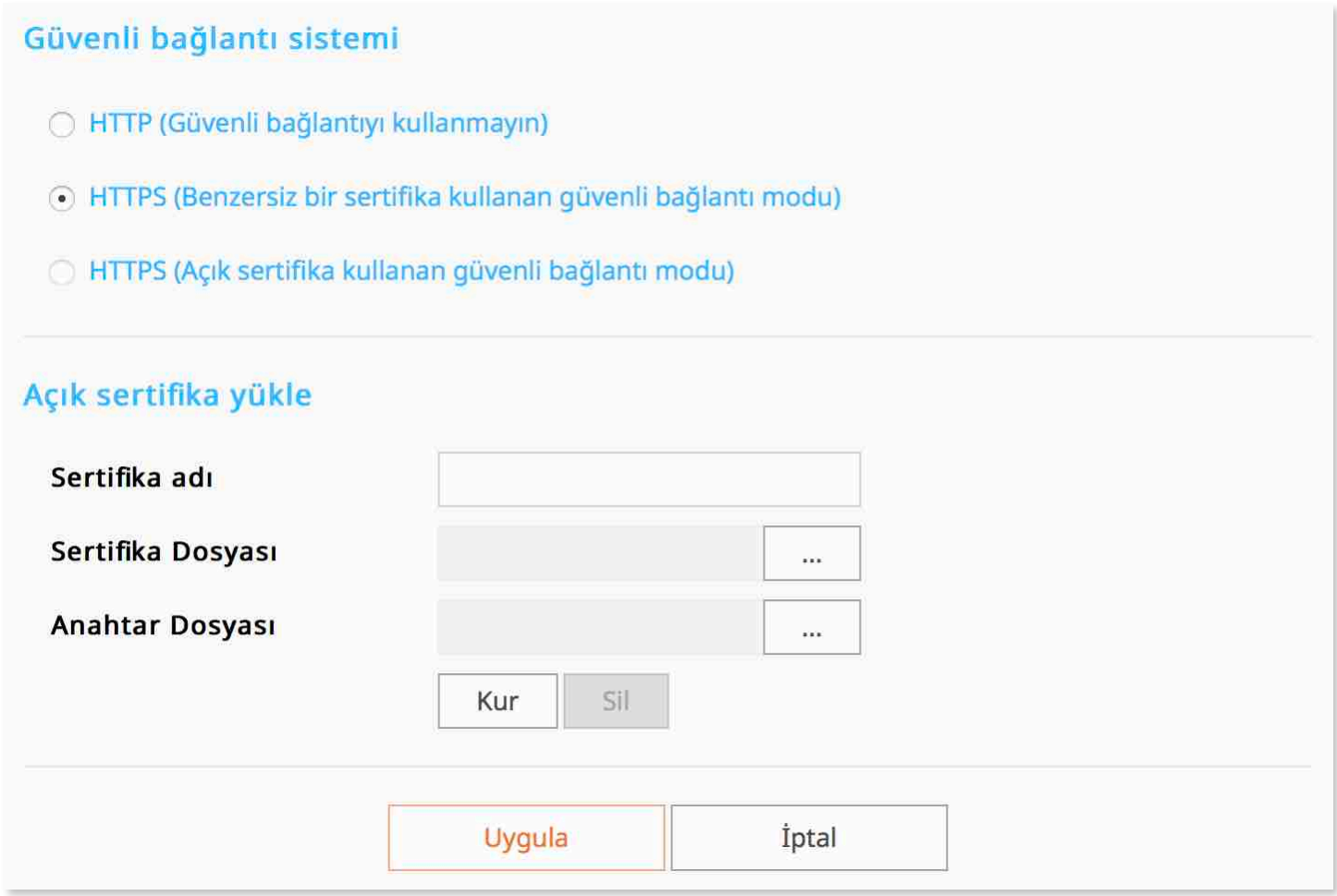
SSL Doğrulama

Kullanıcı kimlik bilgilerinin ve verilerin kendilerini hedeflenen yerlerine gönderilmesi ve güvenli tutulması için mükemmel bir yöntem SSL şifrelemesini kullanmaktır. Bu basit, uygun maliyetli yöntem, bir cihazın güvenliğini daha da geliştirir.

Dahili sertifikalar, SSL şifrelemesinin saniyeler içinde çalışmasına izin verir. SSL sertifikası, bir ticari Sertifika Otoritesinden satın alınabilir veya erişim üzerine bir sertifika güvenlik mesajından kaçınmak için daha da fazla güvenlik için kurumsal kuruluşlar tarafından verilebilir. SSL güvenliği, iletişim kanalınızı potansiyel olarak güvensiz bir ağda veya bulutta güçlendirmenin harika bir yoludur. Ancak hangi kanalların şifrelenmesi gerektiğini ve destekleneceğini belirleyin. Bu, kamera ile NVR / Video Yönetim Sistemine (VYS) ve VYS'den müşteriye. Kimlik bilgilerinin düz metin olarak gönderilmesini önlemek için SMTP protokolünü kullanarak e-posta bildirimleri gönderirken SSL şifrelemesi de kullanılmalıdır. SMTP sunucunuzun SSL / TLS'yi desteklediğinden emin olun ve hangi bağlantı noktasının kullanıldığını öğrenin.

Konfigürasyon seçenekleri, benzersiz bir (yerleşik) veya kamuya açık belgenin seçilmesini ve sertifikanın ve anahtarın kurulumunu ve adlandırılmasını sağlar. HTTPS seçenekleri değiştirildiğinde, kamera yeniden başlatılacak ve ardından sadece HTTPS portu üzerinden şifrelenmiş HTTPS iletişimlerinin gerçekleşmesine izin verilecektir (Resim 6'ya bakınız).

Ağ > HTTPS



Resim 6

Buluttan Kaçının

Sisteminizi kaydetmek veya görüntülemek için bir bulut hizmetini kullanmak yalnızca büyük miktarda bant genişliği gerektirmekle kalmaz aynı zamanda bir güvenlik sorunu da doğurabilir. Bulut bir aygıta bağlandığında, oturum açma bilgileri gönderir. Bu bilgi yakalanırsa veya bir ortadaki adam (man-in-the-middle) (MITM) saldırısına maruz kalırsanız, kimlik bilgileri şifresi çözülmüş olabilir veya yetkisiz erişime izin verilmiş olabilir. Buna ek olarak, tüm bulut hizmetleri SSL şifrelemesini veya hatta digest kimlik doğrulamayı desteklemez.

Ağ Kurulumu ve Konfigürasyonu

Fiziksel Ağ Ayrımı

Bir güvenlik ağının güvenliğini artırmak için kullanılan yaygın ve etkili bir teknik, kameraları ve kaydedicileri şirket ağından fiziksel olarak ayırmaktır. Bu, erişim eksikliği yüzünden saldırganların erişimini engellemektedir. Birçok NVR, birinden kayıt yapmalarına ve diğerinde iş istasyonu erişimi sağlamak için birden fazla ağ arayüzüne sahiptir. Bu teknik, artırılmış güvenlik kontrollerine ihtiyaç duyan cihazların sayısını azaltmaktadır (Resim 7).

Resim 7

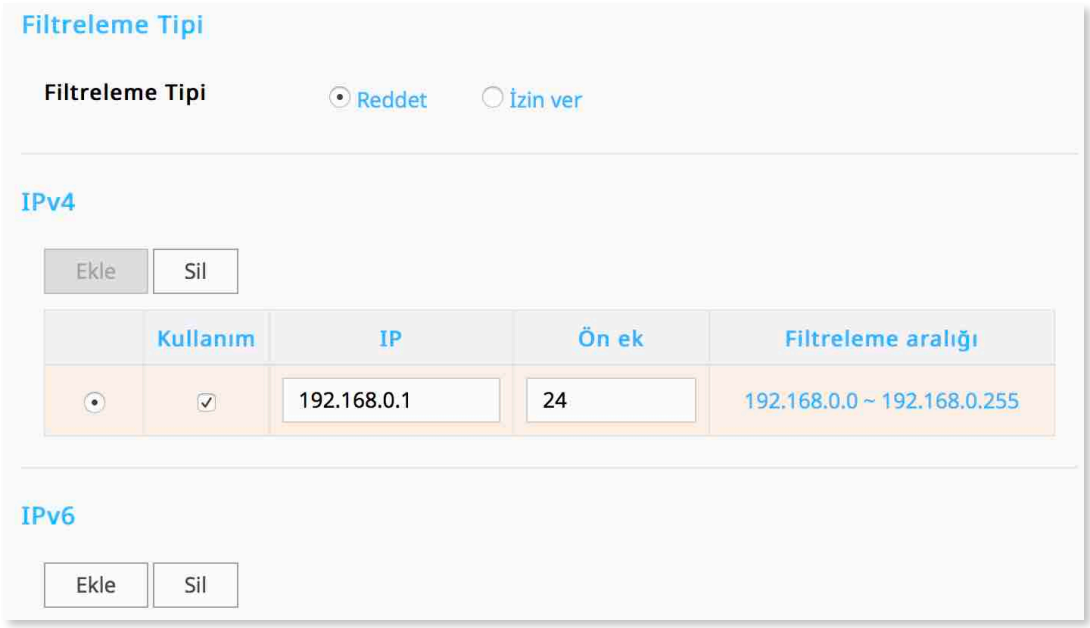
VLAN

Ayrı bir ağ kullanılmadığında, bir güvenlik ağını şirket ağından ayrı tutmak için Sanal Ağ (VLAN) kullanımı önerilir. VLAN'lar şebeke anahtarlarında çalışır ve genelde trafiği geçiş portlarına dayalı olarak ayrıştırır. Bu, duvarların güvenlik aygıtlarını ağdaki diğer aygıtlardan uzak tutmasını sağlar. Belirli cihazlara erişim gerekiyorsa, güvenlik duvarı kuralları oluşturulabilir veya VLAN'a bir cihaz eklenebilir.

IP Filtreleme

IP Filtreleme, bir ağ aygıtına kimlerin erişmesine izin verildiğini açıkça belirtmek için bir yöntemdir ya da tam tersi olarak, aygıta erişimi kimin engellediğini belirtir. Bir IP adresi veya aralık / alt ağ belirlenebilir. Bu, yalnızca bilgisayarlarının IP adreslerine dayalı olarak doğru kişilerin aygıta erişimi olmasını ve yerel ağdan veya İnternet'ten bir drive-by deneme erişiminin engellenmesini sağlayabilir. Hanwha cihazları, erişimi engellemek veya erişimine izin vermek için IPv4 ve IPv6 IP adreslerinin ve ön izinlerinin girilmesini sağlar. Atanacak aralık onaylanmadan önce kendi IP adresiniz ve öncesi x değerlerinin geçerliliğini doğruladığınızdan emin olun, aksi takdirde kendi erişiminizi engelleyebilirsiniz.. IPv4 ve IPv6 için her biri en fazla 10 giriş eklenebilir (Resim 8).

Ağ> IP Filtreleme



Resim 8

VPN

Çoklu ortam veya uzaktaki çalışanlar gibi uzak konumların bağlanması için en iyi uygulama bir VPN çözümü kullanmaktır. VPN, kullanıcı adları ve parolalar gibi bilgi sızıntısı olasılığını ortadan kaldıran güvenli, şifreli bir kanal oluşturur. Bir VPN çözümü, bir VPN yönlendiricisi ve / veya bir istemci bilgisayarda çalışan bir yazılım VPN gibi özel bir donanımı içerebilir.

Kapılar (Portlar) ve Hizmetler(Services)

Günümüzde bağlı olan dünyada birçok cihaz internete bağlı (kasten veya istemeden) ve bilgisayar korsanlarının taramaları gerçekleştirmek için bu cihazları aramak için kullandığı çok sayıda hizmet vardır.

Varsayılan Bağlantı Noktalarını Değiştirin

Bu tarayıcıların yanı sıra komut dosyası parçacıkları, sürücü-bazlı saldırıları ve yanlışlıkla erişime engel olmaya yardımcı olmanın basit bir yolu, çevrimiçi ortamdaki mevcut tanınmış varsayılan değerlerden seçtiğiniz daha yüksek bağlantı noktası numaralarına kadar ağa bağlı aygıtların bağlantı noktalarını değiştirmektir. Özellikle HTTP internet bağlantı noktası, çoğu aygıt için bir web tarayıcısı üzerinden erişime izin vermek için varsayılan 80 bağlantı noktasıdır (portudur). Örneğin, bu bağlantı noktasını 8000 olarak değiştirmek, adresi bir web tarayıcısına girerken fazladan bir adımı gerektirir ve genellikle basit bir tarayıcıdan veya birisinin elle bir internet tarayıcısına bir adres yazarak korunması gerekir (Resim 9).

Temel> IP ve Port> Port

Resim 9

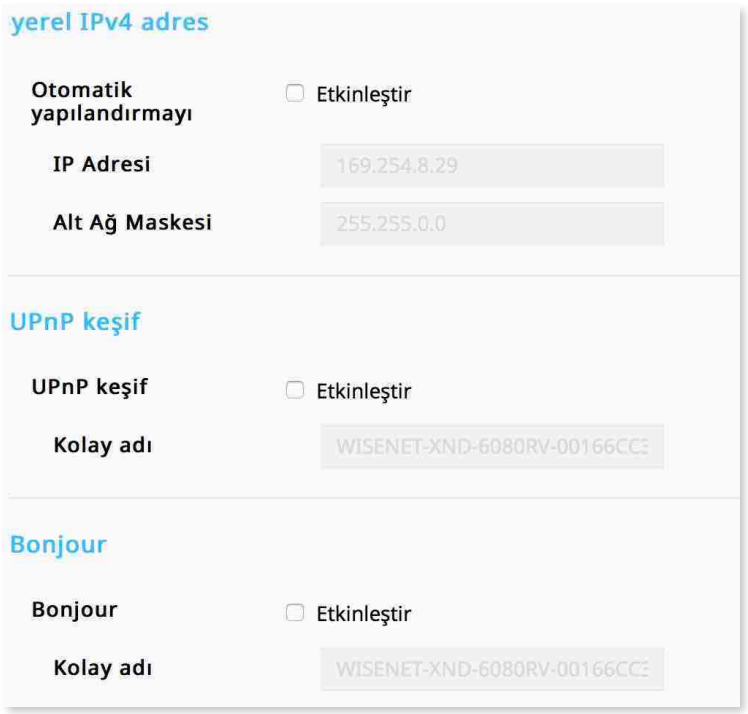
Kullanılmayan Bağlantı Noktalarını, Hizmetleri ve Protokolleri Devre Dışı Bırak

Birçok güvenlik aygıtı modern işletim sistemlerinde çalışan tam donanımlı bilgisayarlar olduğu için Hanwha, özel geliştirilmiş ve basitleştirilmiş Linux işletim sistemlerini kullanan yaklaşımı benimser. Burada kullanılmayan hizmetler kaldırılmış veya devre dışı bırakılmıştır. Diğer birçok üretici, bu hizmetleri hata ayıklama için veya güçlü bir güvenlik bilinci ve / veya işletim eksikliği nedeniyle kaldırmamaktadır. Diğer üreticilerin cihazlarının hack'lendiği bir çok olaydanda anlaşılacağı üzere, saldırganların telnet yoluyla bir çok cihaza girebildiklerini gösteriyor.Ve bu da tüm dosya ve servislere tam komut satırı erişimi sağlandığı anlamına geliyor. Windows tabanlı kayıt platformlarının, zaman, izleme ve Internet erişimi gerektiren sürekli güvenlik güncelleştirmeleri ve düzeltme eklerinin kullanılması gibi bir çok gereksinimi vardır.

Hanwha cihazları, yararlı fonksiyonlar sağlayan çeşitli protokolleri kullanmaktadır. Bununla birlikte, bir uygulama için gerekli olmayan tüm servislerin devre dışı bırakılması önerir. Bunlar, çok noktaya yayın(Multicast),

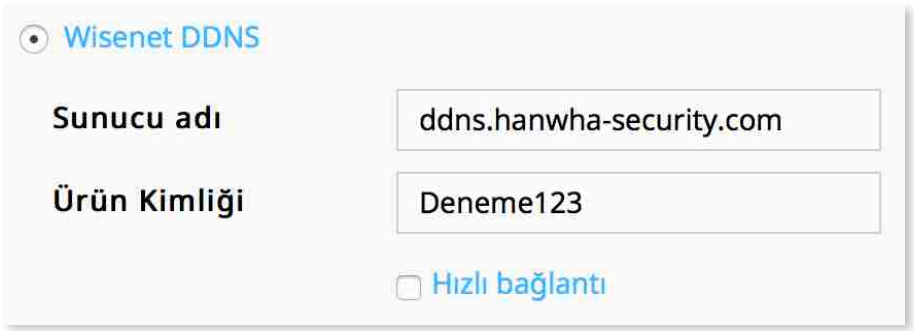
Dinamik yönlendirme, bağlantı yerel adresi, Dosya Aktarım Protokolü (FTP), SNMP, Ağa Bağlı Depolama Alanı (NAS)) ve e-posta uyarıları gibi protokollerdir. Daha önce belirtildiği gibi, benzersiz kimlik bilgilerini uygulamak ve FTP, NAS ve e- posta için ayrıcalıkları kısıtlamak da güvenliği artırmak için uygun yollardır. Otomatik IP Konfigürasyon protokolleri varsayılan olarak etkindir ancak listelenen diğer servislerin tümü devre dışıdır (Resim 10).

Ağ> Otomatik IP Yapılandırma



Resim 10

Ağ> DNS



Resim 11

SNMP

SNMP, bir ağ yöneticisinin ağlarındaki aygıtları yönetmesi için mükemmel bir araçtır. SNMP'nin ağlara sağlayabileceği erişim göz önüne alındığında, varsayılan topluluk dizelerini, tahmin edilmesi zor karışık harf ve sayısal girdileri kullanarak değiştirmek önemlidir. Maalesef, SNMP v1 ve v2c, topluluk dizelerini açıkça yazılmış olarak göndererek yetkisiz erişime izin verebilir. Güvenliği artırmak için IP filtreleme uygulanabilir. SSL şifreleme etkinleştirilmişse, SNMP v3, verileri şifreleyebilir, bu kesinlikle önerilir. Bununla birlikte, SNMP cihaz yönetimi için kullanılmazsa, protokolü devre dışı bırakmanız önerilir. Saldırı riskine katkıda bulunan bir kolaylık, genellikle SNMP v1 veya v2'nin daima etkin olması ve bir kameranın menüsü aracılığıyla devre dışı bırakılamamasıdır.

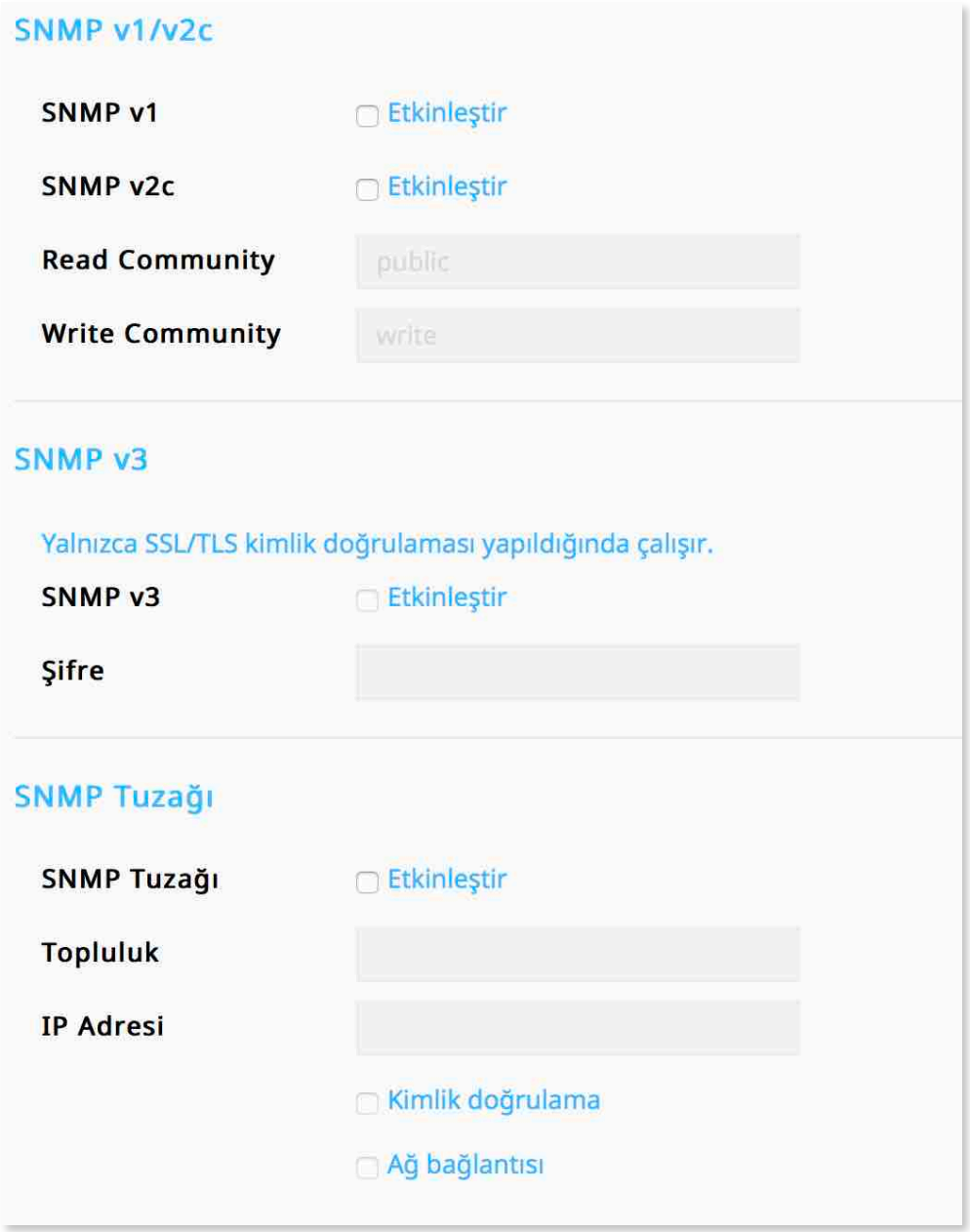
SNMP

Hanwha aygıtları SNMP sürüm 1, 2c ve 3'ü destekler, ancak tüm sürümler kullanıcı arabirimi aracılığıyla devre dışı bırakılamaz. Hanwha kameralar üzerinde SNMP'yi tamamen devre dışı bırakmak için aşağıdaki komutlar kullanılır:

http://<IPADDRESS>/stw-cgi/network.cgi?msubmenu=snmp&action=set&Version1=False
http://<IPADDRESS>/stw-cgi/network.cgi?msubmenu=snmp&action=set&Version2=False

SNMP v2c, "Topluluk" Oku Topluluğu ve "Yaz" Yazma Topluluğu olmak üzere, Hanwha IP kameralarında varsayılan olarak etkindir. SNMP tuzakları, belirli bir Topluluk dizesine ve IP adresine Kimlik Doğrulama Hatası ve Ağ Bağlantısı için etkinleştirilebilir. SNMP v3, bir şifre gerektirir (Resim 12).

Ağ > SNMP



Resim 12

RTSP

Birçok VYS (Video Yönetim Sistemi) görüntü akışında RTSP protokolünü kullanıyor. Hanwha kameralar, RTSP video bağlantılarına kimlik doğrulama gerektirmeden izin vermek için bir seçenek sunar(Resim 13). Kimlik doğrulama kaldırıldığında kullanıcı adı ve şifreler ağa gönderilmez ve eğer üçüncü parti entegrasyonu kimlik bilgileri doğrulamayı desteklemiyorsa bu özellik, akışları internet üzerinden herkese açık olarak gönderirken yararlı olabilir. Hanwha kameralar için bu işlev, gerektiğinde kamera kullanıcı arabiriminden kolaylıkla etkinleştirilebilir. Tüm video akışları için kimlik denetiminin yapılması önerilir. Kamuya açık bir görüntüleme gerekliyse 3. taraf hizmetleri kimliği doğrulanmış akışın içeriğini alabilir ve kamerayı kamusal erişimden izole ederek izlenilmesini sağlayabilir.

Temel> Kullanıcı

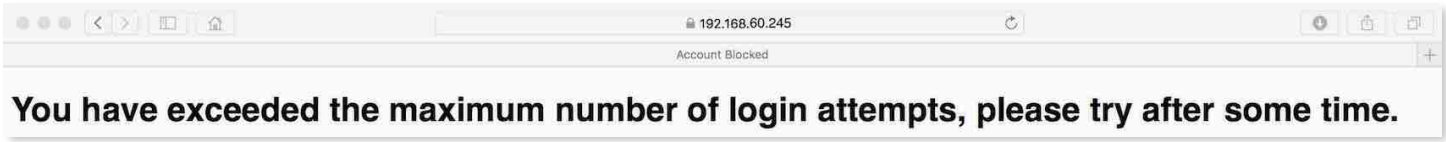
Resim 12

Saldırıları Belirleme ve Engelleme

Bilgisayar korsanlarının en sık kullandıkları saldırı yöntemlerinden ikisi, Denial of Service (DoS) ve arabellek taşmasıdır (Buffer Overflow). Bunların her biri saldırılarda etkin olduğunu kanıtlamıştır. Bu nedenle aygıtları ve ağları yetkisiz erişime karşı korumak için bu yöntemler doğru bir şekilde ele alınmalıdır. Hanwha kameraları, bu amaca ulaşmada oldukça etkili olduğunu kanıtlayan iki yöntem içeriyor.

Kullanıcı Hesabı Engelleme

Hizmet Reddi (DoS) saldırıları, bir cihazın işleyebileceğinden daha hızlı komutlarla değiştirilmesini ve cihazın artık geçerli istekleri sunamayacağı noktaya gelmesine yönelik saldırılardır. DoS saldırılarına karşı koruma sağlamak için, bir Hanwha kamerası çok fazla sayıda kimliği doğrulanmamış istek alırken, kimliği doğrulanmış bağlantıların normal şekilde devam etmesine izin verir. Çok fazla sayıda kimliği doğrulanmamış istek gönderen bu bağlantılar engellenir (Şekil 14).



Resim 12

Arabellek Taşması Koruması

Bilgisayar korsanları için bir başka yaygın saldırı yöntemi, veritabanları veya dosya sistemleri gibi diğer altta yatan hizmetlere doğrudan bilgi veya komutlar göndererek bir aygıta iletmek üzerine kuruludur. Çoğu zaman bu komutlar ayrıştırıcı(parser) veya veritabanındaki bir zayıf noktadan yararlanarak komutların doğrudan veritabanı sunucusuna, işletim sistemine yada sistemin kendisine gönderilmesini sağlamak üzere tasarlanırlar. Hanwha aygıtları, bir web sunucusuna veya veritabanına bilgiyi geçirmeden önce komutları filtreleyerek arabellek taşmalarına ve doğrudan erişime kapalı hale getirilmesini sağlayarak bilgisayar korsanlarının girişimini engeller.

Cihazlara Fiziksel Erişim

Herhangi bir ağ aygıtının güvenliğine fiziksel erişim her şeyden önemlidir. Fiziksel erişimle, çoğu aygıta varsayılan ayar yapılabilir ve böylece yeni ayarların yetkisiz kişilerin potansiyel olarak yapılandırılmasına izin

verilebilir. Derin Savunma (Defense in Depth) güvenlik modeline göre, ağ aygıtlarının kilit ve anahtarın arkasına kurulması, tercihan erişim denetimi ve / veya video güvenlik izlemesi ile birlikte olması önemlidir. Bu önlem, tek bir mekanizmaya güvenmek yerine birden fazla güvenlik katmanı sağlar.

Cihaz Yerleşimi

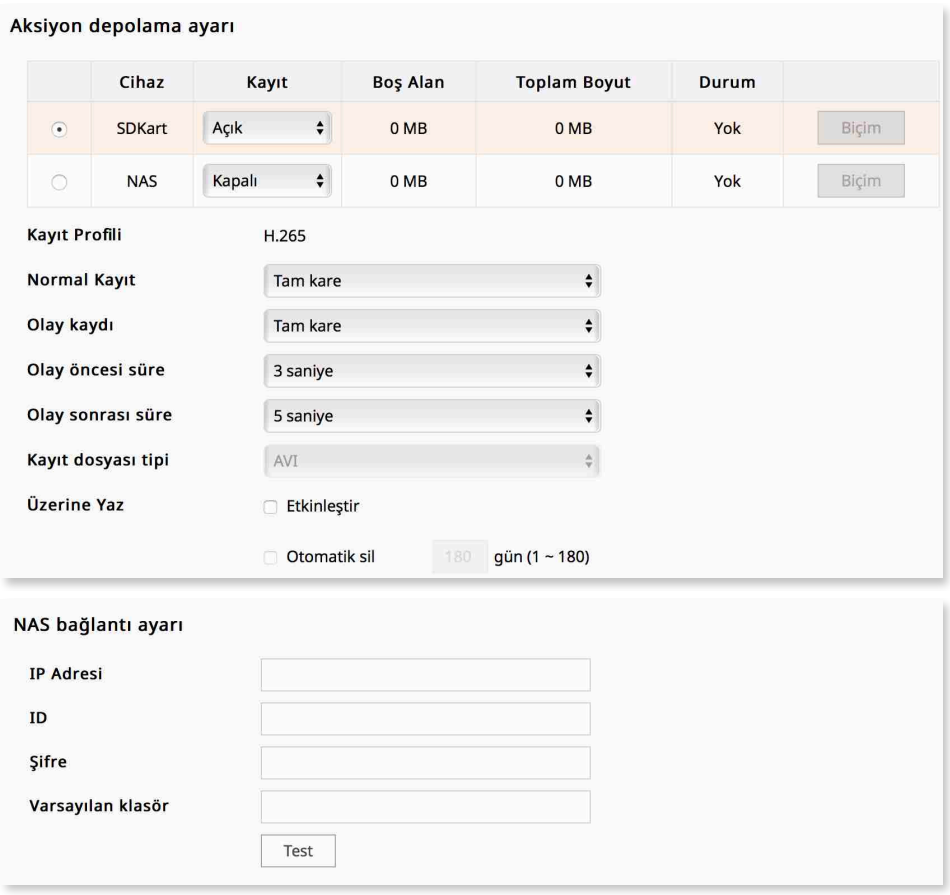
Kameralar, fiziksel erişimin sağlanamaması için tercihen uygun bir gövde ile kolayca erişilemeyecek, yönlendirilemeyen veya fişten çekilemeyen yüklenmelidir. Şebeke ve güç kabloları, kabloların sökülüp engellenememesi için kablo veya duvarlar ve tavanlar arasında / geçmelidir. En iyi fiziksel güvenlik için vandal kubbeli modelleri düşünün.

Kaydın Kesintisiz Olmasını Sağlayın

Olası bir ağ bağlantısı veya ağa fiziksel bir saldırı sırasında, bir hırsız video kanıtını yok etmek amacıyla genellikle bir kaydediciyi veya kayıt sunucusunu çalacaktır. Bunu önlemenin bir yolu, kameralarınızın her birinde SD kart kayıtları kullanmaktır. Sd kartlar uzun kayıt süreleri sunmazlar ancak yedek kayıt olanakları sağlayacaktır. SD kart kaydı, NVR / VYS arızası veya fiziki saldırısı sırasında ve kameranın hala enerjiye sahip olmasına izin verecek şekilde -kasıtlı veya kazara ağ bozulması- durumunda da kullanılabilir.

Konfigürasyon seçenekleri: SD kart işlevlerini etkinleştirme / devre dışı bırakma, tam / I-Çerçeve / yok, olay öncesi ve sonrası kayıt süresi, kayıt tipi (AVI / STW), üzerine yazma, otomatik silme / süre, normal kayıt programı ve SD kart dosya sistemi. Kayıt için herhangi bir profil / kodlama seçilebilir. Gerekirse bir SD kartı yeniden biçimlendirebilir, takılıcak olan boş bir SD kart otomatik olarak yapılandırılacaktır. Bir SD kartı yerine NAS yapılandırılabilir veya bir isteğe bağlı yerine çalışma yedekleme(failover backup) kayıt ortamı olarak SD kartı olan birincil bir kayıt aygıtı olarak da kullanılabilir. NAS kaydı, IP adresi, kullanıcı kimliği, şifre ve varsayılan klasör eklenerek aynı konfigürasyon seçeneklerine sahiptir (Resim 15).

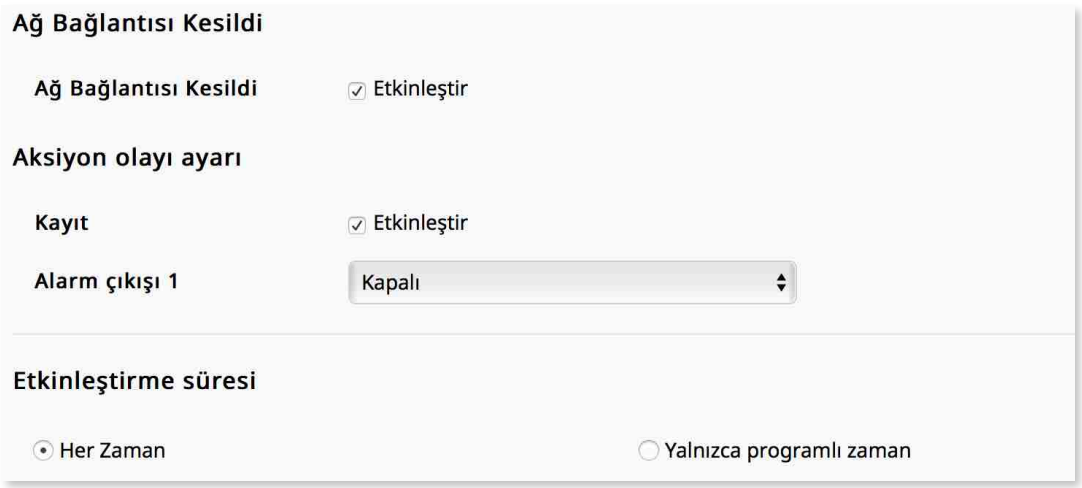
Olay > Depolama



Resim 15

Hanwha kameralar fiziksel bir ağ tabakası bağlantısını algılayabilir ve güç hala mevcutsa, kenarda kayda başlayabilir.

Olay> Ağ bağlantısı kesilmesi algılama



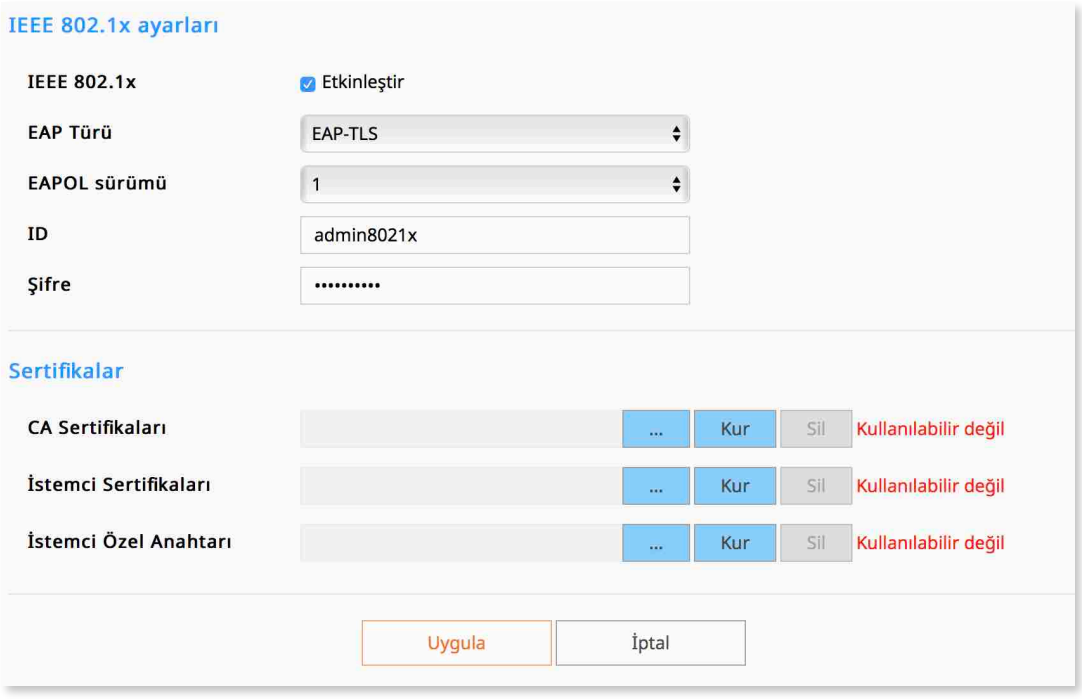
Resim 15

802.1x Sertifika Tabanlı Erişim Kontrolü

Birçok binada, ağ jaklarına ulaşılabilir veya Ethernet ağı altyapısına ulaşmak için bir kamera fişi çekilebilir veya kablolar değiştirilebilir. 802.1x standardı, korunan ağa ulaşmak için bağlı olan her aygıta kurulacak belirleyici bir sertifikaya ihtiyaç duyan bağlantı noktası tabanlı ağ erişim kontrolü sağlar. Böylece, bir saldırgan, yetkisiz bir aygıtı ağa takarsa erişim engellenecektir.

Wisenet Aygıt Yöneticisi, her kameranın arabiriminde yapılandırmalar yapmaya gerek kalmadan merkezi bir konumdan sertifikalar dağıtmanın yanı sıra 802.1x'i kolayca etkinleştirmek için de kullanılabilir. Konfigürasyon seçenekleri arasında, EAP tipi, EAPOL sürümü, kullanıcı kimliği ve şifre seçimi ve sertifikasyon / anahtar kurulumu bulunur (Resim 16).

Ağ>802.1x

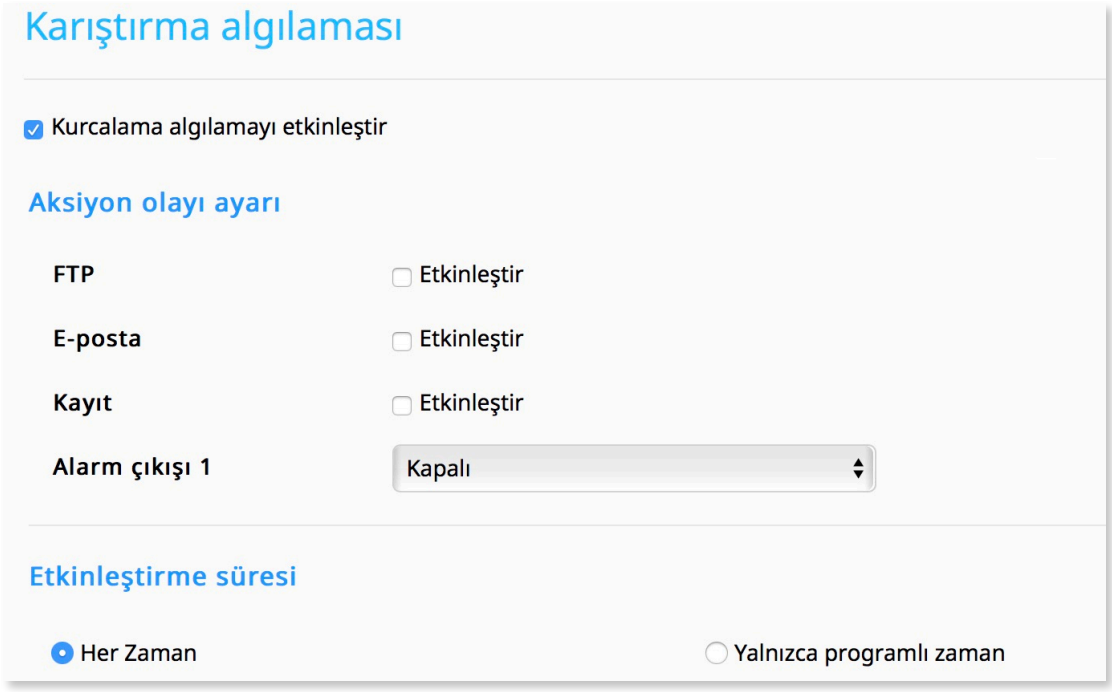


Resim 16

Karıştırma Algılaması (Sabotaj Algılaması)

Torbanın veya sprey boyanın kullanılması gibi bir kameranın objektifini fiziksel olarak engellemek, belirsizleştirmek, kutu tipi veya mermi(bullet tipi) kameranın gözetleme yönünü değiştirme görüntülemeyi bozmak için kullanılan yaygın yöntemlerdir. Karıştırma Algılaması, potansiyel sorunları belirlemek için görüş alanına hızlı bir değişiklik geldiğinde -kamera görevini yapamaza hale gelmeden önce-bir uyarı üretir. Tüm Hanwha IP kameraları, kare hızını düşürmeden karıştırma algılama özelliğini içerir. Ayrıca ad, SNMP gibi ayırt edilebilir özellikler, bir cihazın varsayılana getirilip erişilmediğini veya erişim sağlamak için tehlikeye girip girmediğini tespit etmeye yardımcı olması için kullanılabilir. Ayarların kontrol edilemediği durumlarda, iyi bilinen bir konfigürasyonu geri yükleyin veya varsayılan ayarlara sıfırlayın. Konfigürasyon hassasiyet ayarı içerir (Resim 17).

Olay> Analiz > Karıştırma Algılaması



Resim17 (Resim kırpılmıştır)

Güç

Bir UPS, güç kesintileri, yönetilen kapanmalar, voltaj düşmeleri ve yanlışlıkla veya kötü niyetli bağlantı kesilmesi sırasında ağ aygıtlarınızın güclü kalmasını ve dalgalanmaların hasar görmesini önleyebilir. Bir UPS yönetimi için ağa bağlıysa, düzgün bir şekilde güvenli olduğundan ve güvenlik güncelleştirmelerinin yüklü olduğundan emin olun. Bir LAN'a veya izlemek için İnternet'e bağlı bir UPS gibi yardımcı aygıtlar yoluyla güvenli bir ağa erişim olanağı bulunan saldırganların vakaları olmuştur. Birçok IP kamerada ayrıca, PoE güç bütçesinin aşılması durumunda yedek güç için, modele bağlı olarak PoE ve düşük gerilim 12vDC / 24vAC gibi çift güç kaynakları olabilir. Birçok ağ anahtarı, ne tür bir aygıtın (telefonlar, kameralar, WAP vb.) Veya hangi güç kesintisinde hangi bağlantı noktalarının önemli olduğunu belirtecek şekilde bir önceliğe sahip olabilir.

Ağ yönetimi

Dağıtımın ötesinde, ağ yöneticilerinin kameralarının ve diğer cihazların devam eden güvenliğini sağlamak için sürekli olarak üstlenmeleri gereken bir takım görevler vardır. En kritik olanlar arasında tüm değişiklikleri gözden geçirmek, tutarlı ve onaylanmış yapılandırmalar geliştirmek ve sağlamak, yazılım güncellemeleri yapmak ve yazılımın kuruluşun güvenlik standartlarıyla uyumlu olmasını sağlama. Burada özetlendiği gibi, Hanwha, bu oyunların her birinin, cihazları kilitlemek ve ağları bilgisayar korsanlarına karşı korumak için güçlü bir genel strateji oluşturmada kritik rolü olduğunun farkındadır.

Cihaz Günlüklerini Kontrol Edin

Hanwha kameralar cihaz ayarlarında yapılan tüm değişiklikleri kaydettiğinden, hangi değişikliklerin yapıldığını ve kim tarafından yapıldığını belirlemek için günlükleri kontrol etmek önemlidir. Kolay geri alımı etkinleştirmek için, çoğu kayıt girişi hem önceki hem de yeni ayarları içerir ve günlükler varsayılan fabrika ayarı esnasında saklanır. Wisenet Aygıt Yöneticisi, günlükleri aynı anda birden çok cihazdan kolayca indirmek için kullanılabilir (Resim 18).

Sistem> İşlem kaydı

Günlük

Erişim Günlüğü | Sistem Günlük | Olay Günlük

Günlük türü: All — Yedekle

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

Günlük

Erişim Günlüğü | Sistem Günlük | Olay Günlük

Günlük türü: All — Yedekle

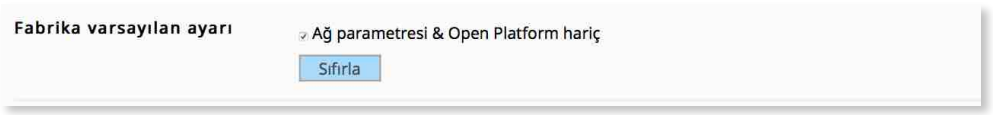
No.	Tarih ve Saat	Açıklama	Bilgi
1	2018-01-29 19:45:40	ConfigChange	Tampering Detection Enable: Off => On
2	2018-01-29 18:16:12	ConfigChange	IPv4 QoS 1: /32/63 => 192.168.2.0/24/63
3	2018-01-29 18:16:12	ConfigChange	IPv4 QoS 1 Use: Off => On
4	2018-01-29 18:11:19	ConfigChange	Secure Connection Mode: HTTP => HTTPS (Unique)
5	2018-01-29 18:11:05	ConfigChange	IPv4 Filter 1: /32 => 192.168.2.0/24
6	2018-01-29 18:11:05	ConfigChange	IPv4 Filter 1 Use: Off => On
7	2018-01-29 18:11:05	ConfigChange	Filtering Type: Deny => Allow
8	2018-01-29 11:08:28	TimeChange	Time Change: 2018-01-29 11:07:35 => 2018-01-29 11:08:28
9	2018-01-27 18:00:13	Network	Physical network connection is connected

Resim 18

Yapılandırmaları Yedekleme

Ayarların doğru olduğu onaylanamıyorsa, varsayılan fabrika ayarlarına dönmek bilinen iyi ayarların yapılmasını sağlamak için bir yoldur. Hanwha kameralar için, kamera açıldığında ve varsayılanı fabrika ayarları düğmesini 5 saniyeliğine basılı tutarak yapabilirsiniz. Kamerayı varsayılan duruma getirdikten sonra, IP adresini ayarlamak ve varsayılan yönetici şifresini değiştirmek önemlidir. Tüm IP, Port ve Ağ menü ayarlarını koruyarak varsayılan ayarlara döndürülebilir.(Resim 19 ve 20).

Sistem> Yükseltme / Yeniden Başlat



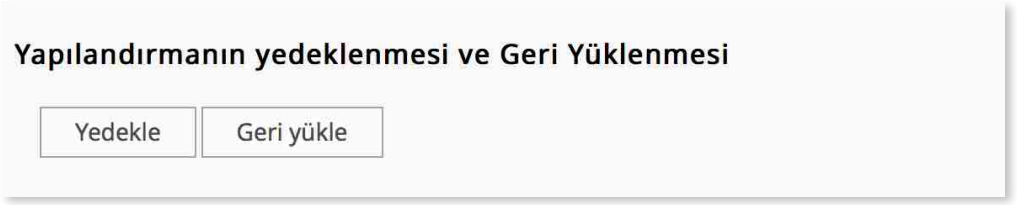
Resim 19

Resim 20

Yapılandırmaları Yedekleme

Bir diğer kritik idari görev, bilinçli olan iyi yapılandırmaların düzenli olarak yedeklenmesidir. Yedeklemenin önemi, hem yanlışlıkla hem de yıkıcı değişiklikler yapılması durumunda ortaya çıkacaktır. Wisenet Aygıt Yöneticisi aracı, aygıt yapılandırmalarının hızlı ve kolay bir şekilde yedeklenmesine, ayıca geri yüklenmesine olanak tanır. İşin tamamlanma kayıtları için ideal olan kamera anlık görüntüleriyle birlikte anahtar ayarları ve bilgileri içeren bir rapor oluşturabilir. Aynı modelin yeni kurulan yedek kameraları için bir şablon olarak da geri yüklenebilir ve tüm ayarların kolay kurulum için sürekli uygulanmasını sağlar (Resim 21).

Sistem> Yükseltme / Yeniden Başlat



Resim 21

Ürün Yazılımını Düzenli Olarak Güncelleme

Bilgisayar korsanları, yazılımdaki güvenlik açıklarını, özellikle de geçerliliği kaybolmuş bellenimleri (Zamanında güncellenmemiş firmware) bulmak, eski sürümü belirlemek ve kullanmak için yorulmadan çalışırlar. Bir güvenlik açığı bulduktan sonra, çoğunlukla hızlı bir şekilde çevrimiçi yayılır; birden fazla kişinin eski bellenim sürümlerini çalıştıran bir aygıta kolaylıkla erişebilmesi için kapıyı açar ve ağın kendisi üzerinde yayılır. Yazılım sağlayıcıları bunu kabul eder ve bu kapıyı kapatarak kullanıcıları yetkisiz erişime karşı koruyacak iyileştirmeler ve / veya yamalar sağlamak için sürekli olarak güncellemeler çıkarır. Her Hanwha aygıtı için gereken yazılım, yöneticilerin en yeni sürümü çalıştırdıklarından emin olmak için başvurabileceği güncellemelerin bir listesini içerir. Yazılımın, bir sistem kurulumundan önce güncel olması, sürekli ve düzenli olarak güncellenmesi önerilir. Çoğu kurulumcu, dağıtımdan önce ürün yazılımını güncelleme, IP adreslerini atama ve tezgahta yönetici parolaları belirlemeyi tercih eder.

Wisenet Aygıt Yöneticisi aracı, tüm cihazlar için ürün yazılımı sürümünü ve güncel durumunu bir kerede kolayca kontrol etmek için kullanılabilir. Yalnızca birkaç tıklama ile ürünün yeni bellenimi (firmware) indirilebilir ve yüklenebilir (Resim 22).

Sistem> Yükseltme / Yeniden Başlat

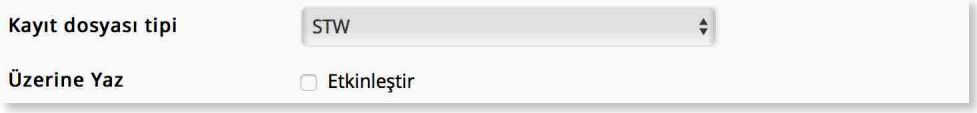
Resim 22

Video Biçimleri (Formatları)

Çoğu güvenlik ekipmanı, endüstri standardı, açık video biçimleri (Avi gibi) ve bazı kendine özel video biçimlerini (SEC gibi) destekler. Kullanıcılar videoyu en sevdikleri medya oynatıcısıyla açabildikleri için açık video biçimleri ilk bakışta ideal görünebilir. Bununla birlikte, güvenlik uygulamaları, düzenlenemez, değiştirilemez veya değiştirilemeyen bir format gerektirir. Video yüklendiğinde, videonun kimliğini doğrulamak ve bu videonun değiştirilmemiş olmasını sağlamak için bir mekanizma olmalıdır. Yalnızca açık biçimlerde mevcut olmayan işlevler bulundurulması gereklidir ve kanıtın geçerliliği açısında bu çok önemlidir.

Hanwha video biçimleri, bu kritik önlemlerin yanı sıra, videonun kanıt olarak kullanılmasını sağlayan, isteğe bağlı, karmaşık bir şifre sağlar. Gerekli oynatıcı herhangi bir kurulum gerektirmeden indirilen veya arşivlenen videoya otomatik olarak dahil edilir. Kullanıcıların video dosyasını görüntülemek için dosyayı çift tıklaması yeterlidir(exe biçimi). Hanwha IP kameralar STW dosya biçiminde de video saklayabilir. Videolar internet tarayıcısı tarafından dışa aktarılabilir veya bağımsız SD Kart oynatıcı kullanılarak oynatılabilir. Bir kaydediciden dışa aktarılan video, oynatıcısı ile birlikte SEC dosyası biçiminde kaydedilebilir (Resim 23).

Olay > Depolama

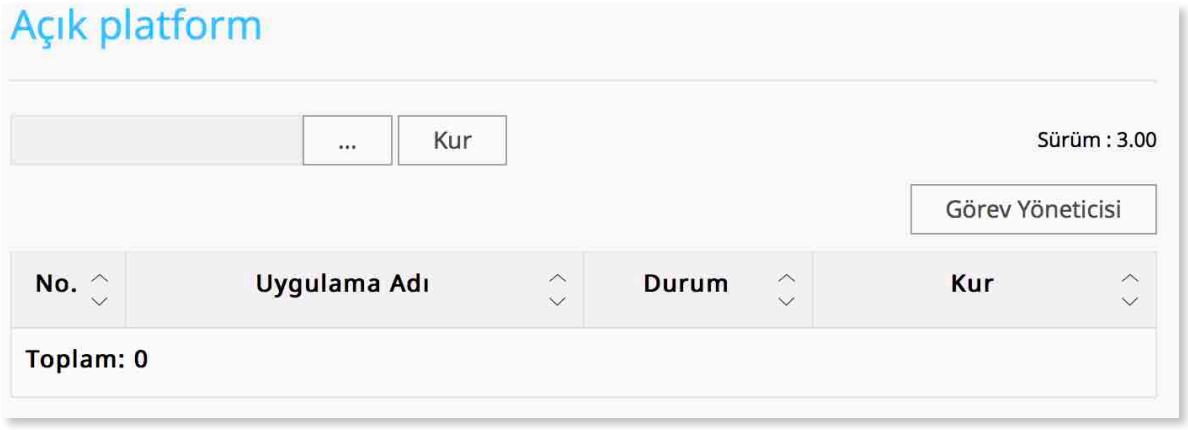


Resim 23

Açık Platform Uygulamaları

Birçok Hanwha kamerası, plaka tanıma, perakende iş zekası, kişi sayma ve daha fazlası gibi işlevlerini geliştirmek için üçüncü parti uygulamaların yüklenmesine izin verir. Kameralarda uygulama çalıştırırken yazılımı kim tarafından yüklendiğini ve yazılım paketinin kaynağını bilmek önemlidir. Kurulum sırasında, Hanwha kameralar bir uygulamanın gerektirdiği izinlerini size bildirir; bu bilgileri dikkatli bir şekilde okuduğunuzdan ve verilerin başka bir yere gönderilip gönderilmeyeceğini anladığınızdan emin olun. Bir uygulama doğrulanamıyorsa veya amacı bilinmiyorsa kurulumu derhal durdurun, uygulamayı kaldırın ve onu sağlayan iş ortağından güvenilir olduğundan emin olun. Yapılandırma seçenekleri, otomatik başlatma, öncelik seviyesi, uygulamaları başlatma / durdurma, uygulamaları yükleme / kaldırma ve bir uygulama internet sayfasını yürütmeyi içerir (Resim 24).

Sistem> Açık Platform



Resim 24

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 America
500 Frank W. Burr Blvd. Suite 43, Teaneck, NJ
07666
Toll Free : 877.213.1222
www.HanwhaSecurity.com
I.H-1607

SECURITURK
Elektronik Güvenlik Sistemleri
D-100 Güney Yan Yol No:25 Lapis Han Ofis:
2069 Kartal, İstanbul / Türkiye
Telefon: +90 850 259 30 00
www.securiturk.com