E POSTA GÜVENLİK CİHAZI KULLANMA KILAVUZU
MARKA: CİSCO
MODELLER: C380, C680 E POSTA GÜVENLİK CİHAZI

Her gün 100 milyardan fazla şirket e-posta mesajı değiş tokuş edilir. E-posta kullanımı arttıkça, güvenlik her zamankinden daha büyük bir öncelik haline geliyor. Cisco ® çözümleri, kurumunuzu etkileyen dinamik ve hızla değişen tehditlere karşı yüksek kullanılabilirlikli e-posta koruması sunar.

Özellikler ve faydalar

İster fiziksel, ister sanal, bulut isterse hibrit olsun, e-posta güvenliği çözümlerimiz aşağıdakileri sunan endüstri liderleri olarak tanınır:

- **Hızlı, kapsamlı koruma,** çoğu zaman yarışmadan saatler veya günler önce
- Cisco Talos'un kapsamlı toplu güvenlik analizleri üzerine inşa edilmiş **en büyük tehdit istihbarat ağlarından biri**
- Aygıttaki Veri Kaybını Önleme (DLP) ve e-posta şifreleme yoluyla **giden ileti koruması**
- **Az yer** kaplayan, kolay uygulama yapan ve uzun vadede tasarruf sağlayan otomatik yönetim ile **düşük toplam sahip olma maliyeti**

Ürüne Genel Bakış

Bugün, spam ve kötü amaçlı yazılım, gelen tehditleri ve giden risklerini içeren karmaşık bir e-posta güvenlik resminin bir parçasıdır. Hepsi bir arada Cisco Email Security Appliance, az bakım gereksinimi, düşük gecikme süresi ve düşük işletme maliyetleri ile basit, hızlı dağıtım sunar. Ayarla ve unut teknolojisi, otomatik politika ayarları yayına girdikten sonra personelinizi serbest bırakır. Çözüm daha sonra otomatik olarak güvenlik güncellemelerini Cisco'nun bulut tabanlı tehdit istihbarat çözümüne yönlendirir . Tehdit istihbarat verileri, e-posta cihazında her 3 ila 5 dakikada bir yenilenerek size diğer satıcılardan saatler veya günler önce güncel bir tehdit savunması yanıtı sunar. Esnek dağıtım seçenekleri ve mevcut altyapınızla sorunsuz entegrasyon, bu cihazı işletme ihtiyaçlarınız için mükemmel bir seçim haline getirir.

Sanal Uygulama

Cisco E-posta Güvenliği Sanal Uygulaması, özellikle yüksek oranda dağıtılmış ağlarda, e-posta güvenliğinin kullanılmasının maliyetini önemli ölçüde azaltır. Bu cihaz, ağ yöneticinize, mevcut ağ altyapınızı kullanarak, nerede ve ne zaman ihtiyaç duyuldukları konusunda örnekler oluşturmasını sağlar. Fiziksel cihazın bir yazılım versiyonu olan VMware ESXi hipervizörü ve Cisco Unified Computing System ™ (Cisco UCS ®) sunucularının üzerinde çalışır. Herhangi bir Cisco Email Security yazılım paketini satın alarak sanal cihaz için sınırsız bir lisans alırsınız.

Sanal cihazla, artan kapasite artışına anında basitleştirilmiş kapasite planlaması ile yanıt verebilirsiniz. Cihaz satın almanız ve göndermeniz gerekmez, böylece bir veri merkezine karmaşıklık eklemeden veya ek personel kiralamak zorunda kalmadan yeni iş fırsatlarını destekleyebilirsiniz.

Ana Yetenekler

Kritik görevli e-posta sistemlerinizi fiziksel, sanal, bulut ve karma çözümlerle savunabilirsiniz. Tablo 1, e-posta güvenliği çözümlerimizin temel yeteneklerini özetlemektedir.

Sahte E-posta Tespiti, yüksek değerli hedefler olarak da bilinen üst düzey yöneticilere odaklanan sahtekârlık saldırılarına karşı korur. Sahte E-posta Algılama, bu özelleştirilmiş saldırıları özel bir içerik filtresiyle engellemenize yardımcı olur. Bu özellik yapılan tüm girişimler ve yapılan işlemlerle ilgili ayrıntılı günlükler sağlar.

Tablo 1. Ana Yetenekler

Kabiliyet	Açıklama
Küresel tehdit istihbarat	Dünyanın en büyük tehdit algılama ağlarından biri tarafından desteklenen hızlı ve kapsamlı e-posta koruması edinin. Cisco, aşağıdakileri içeren geniş bir görünürlük ve geniş bir alan kaplar ● Günlük 100 Terabayt (TB) güvenlik zekâsı ● Güvenlik duvarları, Cisco IPS sensörleri ve web ve e-posta cihazları dâhil olmak üzere 1,6 milyon konuşlu güvenlik cihazı ● 150 milyon son nokta ● Günde 13 milyar web talebi ● dünyadaki e-posta trafiğinin yüzde 35'i Cisco Talos, küresel trafik etkinliğine 24 saat boyunca bakış sağlar. Anomalileri analiz eder, yeni tehditleri açığa çıkarır ve trafik eğilimlerini izler. Talos, sürekli olarak güvenlik cihazlarına güncellemeleri besleyen kurallar oluşturarak sıfır saatlik saldırıların önlenmesine yardımcı olur. Bu güncellemeler her 3 ila 5 dakikada bir meydana gelir ve sektör lideri tehdit savunması sağlar.
Spam engelleme	Spam, karmaşık bir çözüm gerektiren karmaşık bir sorundur. Cisco kolaylaştırır. İstenmeyen postaların gelen kutunuza ulaşmasını engellemek için çok katmanlı bir savunma, gönderenin itibarına dayalı bir dış filtreleme katmanını ve iletinin derinlemesine analizini yapan bir iç filtreleme katmanını birleştirir. İtibar filtrelemesi ile spam'ın yüzde 80'inden fazlası ağınıza çarpmadan engellenir. Son gelişmeler, kar ayakkabısı kampanyalarına karşı güçlü bir savunma sağlamak için bağlamsal analiz ve geliştirilmiş otomasyonun yanı sıra otomatik sınıflandırma içerir. Kısa sürelerde büyük miktarda e-posta alan müşteriler, gönderen veya konuya göre filtreler uygulayabilir ve ilişkili iletileri engeller veya karantinaya alırlar.
Graymail tespiti ve güvenli abonelik iptali	Graymail, pazarlama, sosyal ağ ve toplu mesajlardan oluşur. Graymail algılama özelliği, bir kuruluşa giren graymail'i tam olarak sınıflandırmaya ve izlemeye yardımcı olur. Bir yönetici daha sonra her kategoride uygun işlemi yapabilir. Genellikle graymail, son kullanıcıların gönderene bu tür e-postaları almaktan vazgeçmek istediklerini belirtmelerini sağlayan bir abonelik iptali bağlantısına sahiptir. Abonelikten çıkma mekanizmasını taklit etmek popüler bir kimlik avı tekniği olduğundan, kullanıcılar bu abonelikten çıkma bağlantılarını tıklatma konusunda dikkatli olmalıdırlar. Güvenli abonelik iptali çözümü şunları sağlar: ● Abonelikten çıkma bağlantıları olarak gizleyen kötü amaçlı tehditlere karşı koruma ● Tüm abonelikleri yönetmek için tek tip bir arayüz ● E-posta yöneticileri ve son kullanıcılar için bu e-postaları daha iyi görebilme

Kabiliyet	Açıklama
Gelişmiş Kötü Amaçlı Yazılım Koruması	Cisco Email Security Appliance artık Cisco Advanced Malware Protection'ı içeriyor. E-posta ağ geçidinden geçtikten sonra bile, sürekli tehdit analizi için dosya itibari puanlama ve engelleme, statik ve dinamik dosya analizi (sanal alan) ve tehditlerin sürekli incelenmesi için dosya retrospektifini sunar. Kullanıcılar daha fazla saldırıyı engelleyebilir, şüpheli dosyaları izleyebilir, bir salgının kapsamını azaltabilir ve hızlı bir şekilde düzeltebilir. Gelişmiş Zararlı Yazılımlara Karşı Koruma, tüm Email Security Appliance müşterileri için ek bir lisanslı özellik olarak kullanılabilir. Cisco AMP Threat Grid , kötü amaçlı yazılım örneklerini buluta göndermeye ilişkin uyumluluk veya politika kısıtlamaları olan kuruluşlar için şirket içi bir araçla kötü amaçlı yazılım koruması sağlar. AMP sistemi artık AMP özel bulut lisansı ile tamamen yerinde dağıtılabilir. Bu, AMP genel bulutunun kullanımına izin vermeyen katı politika gereksinimlerine sahip müşteriler için önemlidir, ancak AMP genel bulut güncellemelerinden yararlanmaya devam ederler. AMP'li Office 365 müşterileri için kötü amaçlı yazılımların otomatik olarak düzeltilmesi, geriye dönük güvenlik, ihlallerin daha hızlı ve daha az çabayla düzeltilmesine yardımcı olur. Müşteriler, virüs bulaşmış e-postalar üzerinde otomatik işlem yapacak şekilde e-posta güvenlik çözümlerini ayarladılar.
Salgın filtreleri	Salgın filtreleri ortaya çıkan tehditlere ve karma saldırılara karşı koruma sağlar. Bir mesajdaki dosya türü, dosya adı, dosya boyutu ve URL'ler dâhil altı parametrenin herhangi bir kombinasyonu hakkında kurallar yayınlayabilirler. Talos bir salgın hakkında daha fazla şey öğrendiğinde, kuralları değiştirebilir ve mesajları karantinadan buna göre serbest bırakabilir. Salgın filtreleri, şüpheli mesajlara bağlı URL'leri de yeniden yazabilir. Tıklandığında, yeni URL'ler alıcıyı Cisco Web Securit y proxy üzerinden yönlendirir. Web sitesi içeriği daha sonra etkin bir şekilde taranır ve site kötü amaçlı yazılım içeriyorsa, salgın filtreleri kullanıcıya blok ekran görüntüler.
Web etkileşimi takibi	Tamamen tümleşik bir çözüm, BT yöneticilerinin E-posta Güvenliği Uygulaması tarafından yeniden yazılmış URL'leri tıklayan son kullanıcıları izlemelerine olanak tanır. Raporlar göster: ● Kötü amaçlı URL'leri tıklayan en iyi kullanıcılar ● Son kullanıcılar tarafından tıklanan en kötü niyetli URL'ler ● Tarih ve saat, yeniden yazma nedeni ve URL'lerde yapılanlar Yönetici ayrıca, belirli bir URL'yi içeren tüm mesajları geri izleyebilir.
Giden mesaj kontrolü	E-posta Güvenliği Araçları, giden iletileri DLP, e-posta şifreleme yoluyla kontrol eder. Bu kontrol, en önemli mesajlarınızın endüstri standartlarına uymasını ve nakliye sırasında korunmasını sağlamaya yardımcı olur. Ek olarak, giden antispam ve antivirüs taraması, giden ücret sınırlamasıyla birlikte, zarar görmüş makinelerin veya hesapların şirketinizi e-posta kara listelerine sokmasını engellemek için kullanılabilir. Yeni: E-posta Güvenliği Uygulaması artık Aktarım Katmanı Güvenliği'ne (TLS) ek olarak Güvenli / Çok Amaçlı Internet Posta Uzantıları (S / MIME) şifrelemesini ve imzalamayı da destekliyor.

Kabiliyet	Açıklama
Sahte e-posta algılama	Sahte E-posta Tespiti, yüksek değerli hedefler olarak da bilinen yöneticilere odaklanan sahtekârlık saldırılarına karşı korur. Sahte E-posta Algılama, bu özelleştirilmiş saldırıları özel bir içerik filtresiyle engellemenize yardımcı olur. Bu özellik yapılan tüm girişimler ve yapılan işlemlerle ilgili ayrıntılı günlükler sağlar.
Mükemmel performans	Güvenlik cihazları, yeni gelen e-posta virüslerini hızla engeller. Etki alanı teslim kuyrukları teslim edilemeyen e-postaların diğer etki alanlarına kritik teslimatların yedeklenmesine neden olmasını engeller. Bu çözüm, sektör lideri spam yakalama oranını yüzde 99,9'dan ve yanlış pozitif oranı 1 milyonda 1'den az sunuyor.
DLP	Gizli verilerin ağdan ayrılmasını önlemeye yardımcı olmak için hükümeti, özel sektörü ve şirkete özgü düzenlemeleri kapsayan 100'den fazla uzman politikası içeren kapsamlı bir politika kütüphanesinden seçim yapın. İsterseniz, kendi özel politikalarınızı oluşturmak için bu önceden tanımlanmış politikaların parçalarını kullanabilirsiniz. Cisco Email Security DLP motorumuz, birkaç yanlış pozitif ile hızlı bir şekilde doğru politikalar oluşturmak için kelimeler, ifadeler, sözlükler ve normal ifadeler gibi kendi isteğe bağlı veri noktalarınızla birlikte önceden ayarlanmış veri yapılarını kullanır. DLP motoru ihlalleri ciddiyetle puanlar, böylece gereksinimlerinize uyacak farklı iyileştirme düzeyleri uygulayabilirsiniz. Düzeltme seçenekleri arasında şifreleme, altbilgi ve feragatname ekleme, Kör Karbon Kopyaları (BCC'ler) ekleme, bildirme ve karantinaya alma bulunur.
Düşük maliyetli	Küçük bir alan, kolay kurulum ve otomatik güncelleme yönetimi, e-posta güvenliği çözümünüzün ömrü boyunca tasarruf anlamına gelir. Cisco'nun çözümü mevcut en düşük TCO'lardan birine sahip.
Esnek dağıtım	Tüm Cisco e-posta güvenlik çözümleri, uygulamaya basit bir yaklaşım sunar. Sistem kurulum sihirbazı karmaşık ortamları bile idare edebilir ve birkaç dakika içinde çalışmaya başlamanızı ve korunmanızı sağlar, böylece daha güvenli ve hızlı olursunuz. Lisanslama, cihaza dayalı değil, kullanıcı bazındadır, bu nedenle gelen ve yanı sıra giden e-posta ağ geçidi korumasını ek ücret ödemeden sağlamak için cihaz başına kullanıcı başına uygulayabilirsiniz. Bu özellik, iş gereksinimlerinizi tam olarak desteklemek için giden iletileri antispam ve antivirüs motorları ile taramanıza olanak tanır. Sanal cihaz, sanal uygulama modelinde ek kolaylık ve maliyet tasarrufu ile birlikte fiziksel cihazla aynı özellikleri sunar. Anında self-servis provizyonu sunar. Bir Cisco Email Security Sanal Uygulama lisansıyla, ağınızdaki e-posta güvenlik ağ geçitlerini İnternet bağlantısı olmadan dağıtabilirsiniz. Bu lisans, içine gömülü yazılım lisansları satın aldı. Yerel olarak depolanan yeni bir sanal görüntü dosyasına istediğiniz zaman lisans uygulayabilirsiniz. Gerekirse bozulmamış sanal görüntü dosyaları klonlanabilir ve bu sayede anında birkaç e-posta güvenlik ağ geçidini dağıtabilirsiniz. Donanım ve sanal e-posta güvenlik çözümlerini aynı dağıtımda çalıştırabilirsiniz. Böylece, küçük şubeleriniz veya uzak yerleriniz, bu yerlerde donanım kurmanıza ve desteklemenize gerek kalmadan merkezde aldığınız

Kabiliyet	Açıklama
	korumanın aynısını alabilir. Özel dağıtımları Cisco Content Security Management Appliance veya Cisco Content Security Management Virtual Appliance ile kolayca yönetebilirsiniz.
İşinize uygun çözümler	Cisco Cloud Email Security , yazılım, bilgi işlem gücü ve desteği ile kapsamlı ve güvenilir bir hizmettir. Ortak yönetilen kullanıcı arayüzü, Cisco fiziksel ve sanal e-posta güvenlik cihazlarınınkiyle aynıdır. Bu nedenle, çok az yönetim ek yükü ve izlenecek ve yönetilebilecek donanım bulunmadığında olağanüstü koruma elde edersiniz. Microsoft Office 365 müşterileri, Office 365 için Cloud Email Security ile aynı endüstri lideri korumayı da sağlayabilir. Bu çözümün kullanımı kolaydır ve en yüksek düzeyde hizmet kullanılabilirliği ve veri koruması için birden fazla esnek veri merkezi aracılığıyla garantili güvenilirliğe güvenebilirsiniz. Hibrit çözüm, buluttaki düşük maliyetli kolaylıktan yararlanmanıza yardımcı olurken, sitede hassas mesajların gelişmiş kontrolünü sağlar. Ayrıca, toplam kullanıcı sayısının değişmediği varsayılarak, kurum içi kullanıcılara karşı bulut kullanıcılarının sayısını sözleşmeniz boyunca istediğiniz zaman değiştirebilirsiniz. Bu, kuruluşunuzun ihtiyaçları değiştikçe dağıtım esnekliği sağlar. Yerinde donanım ve sanal cihazlar takılmaya hazır hale gelir. Ağ geçidinizde gelen ve giden mesajları korumak için ortamınız için en uygun modeli seçebilirsiniz.

Ürün Özellikleri

Tablo 2, Email Security Appliance'ın performans özelliklerini, Tablo 3, cihazın donanım özelliklerini, Tablo 4, sanal cihazın özelliklerini ve Tablo 5, Security Management Appliance'ın özelliklerini göstermektedir.

Tablo 2. E-posta Güvenlik Cihazı Performans Özellikleri

Yayılma	Model	Disk alanı	RAID Yansıtma	Bellek	CPU'lar
Büyük işletme	ESA C680	1,8 TB (300 x 6)	Evet (RAID 10)	32 GB DDR3	2 x 2.0 GHz, 6 çekirdekli
Orta ölçekli işletme	ESA C380	1,2 TB (600 x 2)	Evet (RAID 1)	16 GB DDR3	1 x 2.0 GHz, 6 çekirdekli

Not: Doğru boyutlandırma için, Cisco içerik güvenliği uzmanıyla en yüksek posta akış hızını ve ortalama mesaj boyutunu kontrol ederek seçiminizi doğrulayın.

Tablo 3. E-posta Güvenliği Araçları Donanım Özellikleri

Model	**ESA C680**	**ESA C380**
Raf Üniteleri (RU)	2RU	2RU
Boyutlar (Y x G x D)	3,5 x 19 x 29 inç (8,9 x 48,3 x 73,7 cm)	3,5 x 19 x 29 inç (8,9 x 48,3 x 73,7 cm)
DC güç seçeneği	Evet (930W)	Evet (930W)
Uzaktan güç bisiklet	Evet	Evet
Yedekli güç kaynağı	Evet	Evet
Çalışırken değiştirilebilir sabit disk	Evet	Evet
Güç tüketimi	2216.5 BTU / saat	2216.5 BTU / saat
Güç kaynağı	650W	650W
Ethernet arayüzleri	4 bağlantı noktalı 1GBASE-T bakır ağ arabirimi (NIC), RJ-45	4 bağlantı noktalı 1GBASE-T bakır ağ arabirimi (NIC), RJ-45
Hız (Mbps)	10/100/1000, özdevinir	10/100/1000, özdevinir
Fiber seçeneği	Evet, ayrı SKU'lar 2 bağlantı noktalı 1GBASE-SX Fiber: ESA-C680-1G 2 bağlantı noktalı 10GBASE - SR Fiber: ESA-C680-10G	Yok hayır
Hd boyutu	Cisco C680 Email Security cihazı altı (6) 300 G HDD içerir	Cisco C380 Email Security cihazı iki (2) 600 G HDD içerir
İşlemci	İki Intel Xeon E5-2620 Serisi işlemci (2,0 G, 6C)	Bir Intel Xeon ES-2620 Serisi işlemci (2,0 G, 6C)
Veri deposu	Sekiz (8) 4 GB DDR3-1600-MHz RDIMM DRAM	Dört (4) 4 GB DDR3-1600-MHz RDIMM DRAM

Tablo 4. E-posta Güvenliği Sanal Uygulama Spesifikasyonları

Email kullanıcıları				
	Model	Disk	Bellek	Çekirdekler
Sadece değerlendirmeler	ESAV C000v	200 GB (10K RPM SAS)	4 CİGABAYT	1 (2,7 GHz)
Küçük işletme (en fazla 1000 çalışan)	ESAV C100v	200 GB (10K RPM SAS)	6 GB	2 (2,7 GHz)
Orta ölçekli işletme (5000 çalışana kadar)	ESAV C300v	500 GB (10K RPM SAS)	8 GB	4 (2,7 GHz)
Büyük işletme veya servis sağlayıcı	ESAV C600v	500 GB (10K RPM SAS)	8 GB	8 (2,7 GHz)
Sunucular				
Cisco UCS	VMware ESXi 5,0, 5,1 ve 5,5 Hiper Yönetici			

Tablo 5. Güvenli Yönetim Cihazı M-Serisi Platformu Teknik Özellikleri

Model	**SMA M690 / 690X / 680**	**SMA M390 / 380**	**SMA M190 / M170**
Kullanıcı sayısı	10.000 ya da daha fazla	10.000'e kadar	1.000'e kadar

KURULUM

Cihazı Takma

Kuruluma Genel Bakış

Cisco 380 ve Cisco 680 series cihazının kurulumuna hazırlanmak için aşağıdaki adımları izleyin:

Adım	Bunu yap	Daha fazla bilgi
Adım 1	Güvenlik ve Uygunluk Kılavuzunda belirtilen güvenlik önlemlerini gözden geçirin.	http://www.cisco.com/en/US/docs/unified_computing/ucs/c/regulatory/compliance/cseries_regulatory_compliance_information.html
Adım 2	Cisco 380 ve Cisco 680 serisi cihazlar için uygun Cisco AsyncOS sürüm notlarını okuyun.	http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-release-notes-list.html
Adım 3	Cihazı ambalajından çıkarın.	Unpacking and Inspecting the Appliance, page 2-2.
Adım 4	Cihazı sabit bir çalışma yüzeyine yerleştirin	
Adım 5	Kurulum yönergelerini, raf gereksinimlerini ve ekipman gereksinimlerini görüntüleyin.	Preparing for Appliance Installation, page 2-3.
Adım 6	Cihazı verilen kayar raylarla monte edin.	Installing the Appliance in a Rack, page 2-5.
Adım 7	Ağ bağlantısı kurun	Connecting the Interface Cables and Verifying Connectivity, page 2-7.
Adım 8	Kurulum öncesi ve kurulum sonrası görevler hakkında ek bilgi için, donanım Hızlı Başlangıç Kılavuzlarını inceleyin.	http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-installation-guides-list.html

Cihazı Açma ve İnceleme

Dikkat Cihazı açmayın. Bunu yapmak, destek sözleşmenizi ihlal eder. Cihazda servis yapılabilecek hiçbir bileşen yoktur.

İpucu Cihazın gelecekte nakliyesi gerekebileceği durumlarda nakliye konteynırını saklayın.

Not Şasi sevkıyattan önce iyice kontrol edilir. Nakliye sırasında herhangi bir hasar veya herhangi bir parça eksikse, derhal müşteri hizmetleri temsilcinize başvurun.

Adım 1 Cihazı, karton kutusundan çıkarın ve tüm ambalaj malzemelerini saklayın.

Adım 2 Gönderiyi, müşteri hizmetleri temsilciniz tarafından sağlanan ekipman listesine göre karşılaştırın. Tüm öğelerin bulunduğunu doğrulayın.

Adım 3 Hasar olup olmadığını kontrol edin ve herhangi bir tutarsızlığı veya hasarı müşteri hizmetleri temsilcinize bildirin. Aşağıdaki bilgileri hazırlayın:

• Göndericinin fatura numarası (paketleme fişine bakınız)

• Hasar görmüş birimin model ve seri numarası

• Hasar açıklaması

• Tesisat üzerindeki hasarın etkisi

Kargo kutusu içeriği şunları içerir:

• Aletler

• Kızaklı ray takımı

• Güç kabloları (2)

• Cihazı ağınıza bağlamak için Ethernet kablosu

• Bir bilgisayarı konsol bağlantı noktasına bağlamak için RJ-45 - DB-9 kablosu

• Hızlı başlangıç Kılavuzu

• Düzenleyici Güvenlik ve Uygunluk Bilgisi

Not Cisco 680 series cihazının kilitleme ön yüzü sürümünde iki adet kilitleme anahtarı bulunur.

Cihaz Kurulumuna Hazırlanma

Bu bölüm cihaz kurulumuna hazırlanma hakkında bilgi sağlar ve aşağıdaki konuları içerir:

Kurulum kuralları

Uyarı Sistemin aşırı ısınmasını önlemek için çalıştırmayın.

Uyarı Priz kombinasyonuna her zaman erişilebilir olmalıdır, çünkü ana bağlantı kesme cihazı olarak kullanılır.

Uyarı Aşağıdaki prosedürlerden herhangi birini gerçekleştirmeden önce, gücün DC devresinden kesildiğinden emin olun.

Uyarı Bu ürün, bina kurulumunun bir parçası olarak sağlanacak kısa devre (aşırı akım) koruması gerektirir. Sadece ulusal ve yerel kablolama yönetmeliklerine uygun olarak kurun.

Uyarı Bu ürün, binanın kısa devre (aşırı akım) koruması için kurulumuna dayanır. Koruyucu cihazın şu değerden büyük olmamasına dikkat edin: 250 V, 15 A

Uyarı Cihazın kurulumu yerel ve ulusal elektrik kurallarına uygun olmalıdır.

Dikkat Cihazın kapağının üstündeki hava deliklerini tıkamayın. Başka bir cihazı doğrudan cihazın üzerine istiflemeyin. Bunu yapmak, aşırı ısınmaya, daha yüksek fan hızlarına ve daha yüksek güç tüketimine neden olabilecek doğru hava akışını engeller.

Dikkat ferroresonant teknolojisi kullanan UPS türlerinden kaçının. Bu UPS tipleri, değişken veri trafiği desenlerinden önemli miktarda akım dalgalanmasına neden olabilen Cisco 380 ve Cisco 680 serisi cihaz gibi sistemlerde dengesiz olabilir.

Bir cihaz takarken, aşağıdaki yönergeleri kullanın:

• Sitenizi yapılandırın ve cihazı kurmadan önce siteyi hazırlayın.

• Cihazın bakımını yapmak ve yeterli hava akımı sağlamak için cihazın çevresinde yeterli alan olduğundan emin olun. Bu cihazın içindeki hava akımı önden arkaya doğru.

• Klimanın Cihaz Teknik Özellikleri bölümünde listelenen termal gereksinimleri karşıladığından emin olun.

• Kabin veya rafın 2-4. Sayfadaki “Raf Gereksinimleri” bölümünde listelenen gereksinimleri karşıladığından emin olun.

• Site gücünün, Cihaz Teknik Özellikleri'nde listelenen güç gereksinimlerini karşıladığından emin olun. Mümkünse, elektrik kesintilerine karşı koruma sağlamak için kesintisiz bir güç kaynağı (UPS) kullanabilirsiniz.

Raf Gereksinimleri

Bu bölüm standart açık raflar için gereksinimleri sağlar.

Raf aşağıdaki tipte olmalıdır:

• Standart bir 19 inç. (48,3 cm) genişliğinde, dört direkli EIA rafı, ANSI / EIA-310-D-1992'nin 1. bölümüne göre İngilizce evrensel delik açıklığına uygun montaj direkleri ile.

• Ürünle birlikte verilen kızak rayları kullanılırken, raf direk delikleri 0.38 inç (9.6 mm) kare, 0.28 inç (7.1 mm) yuvarlak, # 12-24 UNC veya # 10-32 UNC olabilir.

• Cihaz başına minimum dikey raf alanı, 3,5 inç (88,9 mm) 'ye eşit olan iki RU olmalıdır.

Ekipman Gereksinimleri

Cisco Systems tarafından sağlanan kayar raylar, 0.38 inç (9.6 mm), yuvarlak 0.28 inç (7.1 mm) veya # 12-24 UNC dişli yuvarlak bir rafa takarsanız, kurulum için alet gerektirmez delikleri. İç raylar cihazın yanlarına önceden takılmıştır.

Bununla birlikte, sürgü raylarını # 10-32 yuvarlak delikli bir rafa yerleştirirseniz, daha büyük kare / yuvarlak montaj mandallarını sürgü raylarının önünden çıkarmak için bir tornavida gerekir.

Slayt Ray Ayar Aralığı

Bu cihazın kaydırma rayları 26 ila 36 inç (660 ila 914 mm) arasında bir ayar aralığına sahiptir.

Cihazı Rafa Takma

Bu bölümde cihazın rafa nasıl monte edileceği açıklanmaktadır.

Uyarı Bu üniteyi rafa monte ederken veya bakım yaparken bedensel yaralanmayı önlemek için, sistemin sabit kalmasını sağlamak için özel önlemler almalısınız. Güvenliğinizi sağlamak için aşağıdaki yönergeler sağlanmıştır:

Bu ünite, raftaki tek ünite ise rafın altına monte edilmelidir.

Bu üniteyi kısmen doldurulmuş bir rafa monte ederken, rafı en alt kısımdan rafın en ağır kısmına gelecek şekilde yükleyin.

Rafa dengeleme cihazları sağlanmışsa, birimi rafa monte etmeden veya bakımını yapmadan önce dengeleyicileri takın.

Sürgü raylarını ve cihazı bir rafa monte etmek için aşağıdaki adımları izleyin:

Adım 1 Sürgü raylarını rafa takın (bkz. Şekil 2-1):

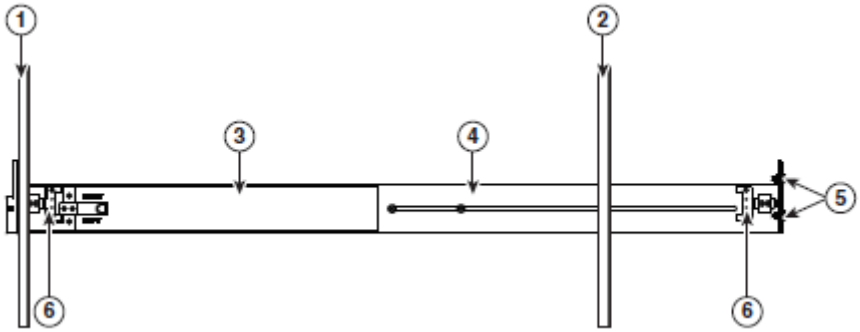
a. Raf direklerinin içindeki kayan ray düzeneğini uzunluk ayarlama braketi (Şekil 2-1, öğe 4) ile rafın arkasına doğru hizalayın.

b. Uzunluk ayar dirseğini montaj mandalları (öğe 5) ve kilitleme klipsleri (öğe 6) ön ve arka raf direklerine istenen raf deliklerine oturana kadar sıkıştırın.

- Montaj dübelleri 0,38 inç (9,6 mm), yuvarlak 0,18 inç (7,1 mm) veya # 12-24 UNC dişli deliklere sahiptir. Kazıklar sıkıştırıldığında, delik şekline uyarlar.

- Küçük # 10-32 yuvarlak montaj mandalları, sıkıştırılabilir arka mandalların ortasına yerleştirilmiştir. Ancak, # 10-32 mandalları kullanmak için kare / yuvarlak ön mandalları çıkarmak için bıçaklı bir tornavida kullanmanız gerekir.

Şekil 2-1 Sürgü Kızağı Tertibatının Takılması



1	Sağ ön raf direkleri	4	Uzunluk ayar braketi
2	Sağ arka raf direkleri	5	Montaj mandalları (montajın her iki ucunda iki adet)
3	Kızak rayı montajı	6	Kilitleme klipsleri (montajın her iki ucunda bir tane)

c. İkinci kayan ray tertibatını rafın diğer tarafına takın. İki kayan ray düzeneğinin düz ve birbiriyle aynı yükseklikte olduğundan emin olun.

d. Her tertibattaki iç kızaklı rayları, iç durduruculara çarpıp yerine kilitleninceye kadar rafın önüne doğru çekin.

Adım 2 Cihazı kayar raylara yerleştirin.

Dikkat Bu cihaz, bileşenlerle birlikte tam olarak yüklendiğinde yaklaşık 60 kilogram (28 kilogram) ağırlığındadır. Cihazı kaldırırken en az iki kişi kullanmanızı öneririz. Bu prosedürü tek başına denemek kişisel yaralanmalara veya ekipman hasarına neden olabilir.

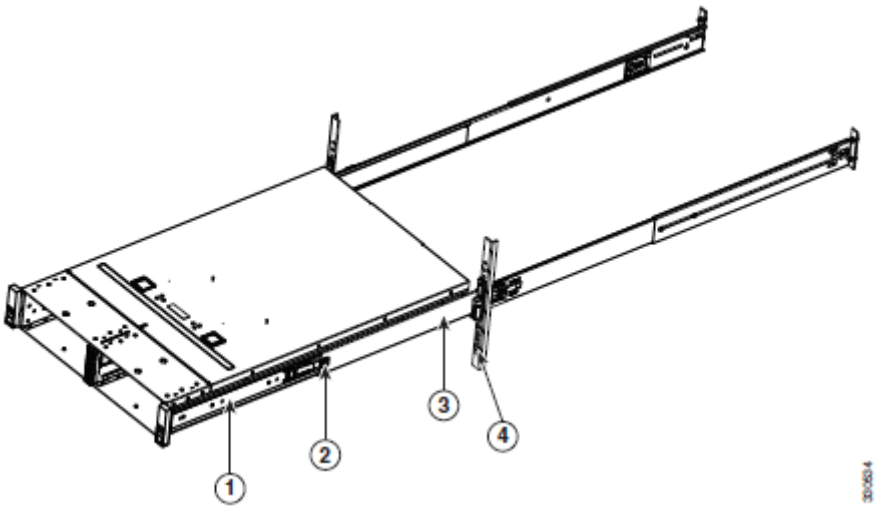
Not İç raylar fabrikada cihazın yanlarına önceden takılmıştır. Bunlar hasarlı veya kayıpsa yedek iç raylar sipariş edebilirsiniz (Cisco PID CCS-RAIL =).

a. Cihazın yanlarına tutturulmuş olan iç rayları boş kızakların ön uçlarıyla hizalayın.

b. Cihazı dahili duraklarda durana kadar kızak raylarının içine doğru itin.

c. Her bir iç rayda kayar ray kilitleme klipsini (madde 2) içeri itin ve ardından ön flanşları raf direklerine kilitlenene kadar cihazı rafa doğru itmeye devam edin.

Şekil 2-2 Cihazın Kızaklı Raylara Takılması



1	Cihaz üzerinde iç ray	3	Kızaklı ray üzerinde ray montajı
2	Kızak rayı kilitleme klipsi	4	Sağ ön raf direkleri

Arabirim Kablolarını Bağlama ve Bağlantı Doğrulama

Bu bölümde kabloların konsola ve bağlantı noktalarına nasıl bağlanacağı açıklanmaktadır.

Uyarı Bu ekipmanı yalnızca eğitimli ve kalifiye personel kurmalı, değiştirmeli veya bakımını yapmalıdır.

Dikkat Cisco Content Security Appliances'ın Yasal Uygunluk ve Güvenlik Bilgilerindeki ve Cisco IronPort Appliances'ın Güvenlik ve Uygunluk Kılavuzundaki güvenlik uyarılarını okuyun ve bu belgedeki herhangi bir görevi gerçekleştirirken uygun güvenlik prosedürlerini izleyin.

Kabloları bağlantı noktalarına bağlamak için aşağıdaki adımları izleyin:

Adım 1 Cihazı düz, sağlam bir yüzeye veya rafa yerleştirin (rafa monte ediyorsanız).

Adım 2 Bir bilgisayarı veya terminali portlara bağlamadan önce, bilgisayar konsolu portunun baud hızını belirleyin.

Baud hızı, Cisco 380 ve Cisco 680 Series cihazının konsol portunun varsayılan baud hızı (9600 baud) ile eşleşmelidir. Terminali şu şekilde ayarlayın: 9600 baud (varsayılan), 8 veri biti, eşlik yok, 1 durdurma biti ve Donanım olarak ayarlanmış Akış Kontrolü (FC).

Adım 3 Kabloları bağlantı noktalarına bağlayın.

a. Yönetim portu - Daha fazla bilgi için, Cisco 380 ve Cisco 680 cihazındaki yönetim portu çizimleri için PCI NIC Slot Konfigürasyonları, sayfa 1-4'teki rakamlara bakın.

- Bir RJ-45 konektörünü yönetim arayüzü bağlantı noktasına bağlayın.

- Ethernet kablosunun diğer ucunu bilgisayarınızdaki yönetim bağlantı noktasına bağlayın ve bilgisayarınızın DHCP kullanarak bir IP adresi alacak şekilde yapılandırıldığından emin olun.

b. Konsol portu - CLI ile kullanım için.

- Konsol kablosunu bağlayın. Konsol kablosunun, bir ucunda bilgisayarınızdaki konsol bağlantı noktası için bir DB-9 konektörü bulunur ve diğer ucu bir RJ-45 konektörüdür.

- RJ-45 konektörünü Cisco 380 ve Cisco 680 cihazındaki konsol portuna bağlayın.

- Kablonun diğer ucunu, DB-9 konektörünü, bilgisayarınızın konsol portuna bağlayın.

c. Ethernet bağlantı noktaları - doğrudan bağlantı.

- RJ-45 konnektörünü Ethernet portuna bağlayın.

- Ethernet kablosunun diğer ucunu yönlendirici, anahtar veya hub gibi ağ cihazınıza bağlayın.

Adım 4 Güç kablosunu Cisco 380 ve Cisco 680 cihazına bağlayın ve diğer ucunu güç kaynağınıza bağlayın.

Adım 5 Cihazı açın.

Not Cihaza güç verildikten sonra hızlı bir şekilde açılırsa, cihaz açılır, fanlar döner ve LED'ler yanar. 30-60 saniye içinde fanlar durur ve tüm LED'ler söner. Cihaz 31 saniye sonra açılır.

Bu davranış, sistem üretici yazılımının ve denetleyicisinin senkronize edilmesine izin vermek için tasarım gereğidir.

Adım 6 Cisco 380 ve Cisco 680 cihazının önündeki Güç LED'ini kontrol edin. Sürekli yeşil olduğunda, cihaz açıktır.

Cihazın Bakımı

Bu bölüm, önceden kurulmuş sabit disk sürücülerinin nasıl değiştirileceğini de içeren Cisco 380 ve Cisco 680 serisi cihazla ilgili bakım bilgileri sağlar.

Güç kaynakları

Cisco 380 ve Cisco 680 series cihazı, iki AC güç kaynağı ya da iki DC güç kaynağı takılı olarak gönderilir.

Her bir AC güç kaynağı 650 watt çıkış gücü sağlar. Her DC güç kaynağı, 930 watt çıkış gücü sağlar. Ek bilgi için, sayfa A-3'teki “Güç Özellikleri” bölümüne bakın.

AC güç kaynakları, sayfa C-1'deki “Desteklenen Güç Kabloları ve Fişleri” bölümünde listelenen güç kablolarından herhangi birini kullanabilir. DC güç kaynakları, güç ünitesinde bulunan yalnızca bir güç kablosu modelini kullanır.

Not Ek güç kaynakları ekleyemezsiniz, ancak hatalı bir güç kaynağını değiştirebilirsiniz. AC ve DC güç kaynaklarının bir kombinasyonunu kullanamazsınız. Bir güç kaynağını değiştirdiğinizde, aynı tip ünite ile değiştirmeniz gerekir.

Uzaktan Güç Yönetimi

Uzaktan güç yönetimi, cihazın uzaktan yeniden başlatılmasını sağlar. Uzak güç döngüsünü gerçekleştirmek için yapmanız gerekenler:

• Cihaz arayüzünü uzaktan erişilebilir bir ağa bağlayın.

• "remotepower" komutunu kullanarak arayüzü AsyncOS üzerinden yapılandırın

• Gerektiğinde, IPMI (Intelligent Platform Management Interface) konuşan yazılımı kullanarak Power Rest'i doğrudan kasaya uygulayın.

Uzaktan Güç Yönetimini Etkinleştir

Uzaktan güç yönetimini etkinleştirmek için:

Adım 1 Cihazın "uzaktan güç yönetimi" RPC arayüz portunu uzaktan erişilebilir bir ağa bağlayın.

Adım 2 Cihaza AsyncOS CLI erişmek için SSH, Telenet veya seri portu kullanarak "remotepower" komutunu giriniz. Bu komut yalnızca CLI üzerinden kullanılabilir.

IPMI uzaktan güç komutlarına erişim şu anda devre dışı olarak gösteriliyor.

Adım 3 Kurulum isteminde, şasi uzaktan güç erişimi için IPMI'yi yapılandırmak üzere kurulumu girin.

Adım 4 Uzaktan erişimi etkinleştirmek için y yazın ve girin.

Adım 5 Kasa için IP adresini (sadece IPv4) girin. Örneğin: 1.1.1.2

Adım 6 Ağ maskesini girin. Örneğin: 255.255.255.0

Adım 7 Ağ geçidi adresini girin. Örneğin: 1.1.1.1

Adım 8 kasaya oturum açmak için kullanılacak kullanıcı adı ve şifreyi girin. Örneğin, kullanıcı adı "admin" ve şifre.

Not Buraya girilen kullanıcı adı ve şifre AsyncOS'tan bağımsızdır.

Bu kullanıcı adı ve şifre açık metin olarak gönderilir ve ağınızı izleyebilen herkes tarafından görülebilir. Uzaktan yönetim bağlantı noktasının doğrudan güvenli bir ağa bağlandığından emin olmak için önlem almalısınız.

Adım 9 Onaylamak için şifreyi tekrar girin.

Geçerli uzaktan güç ayarları görüntülenir.

Adım 10 Kurulum isteminde girin (veya dönüş tuşuna basın) ve kasa isteminde değişikliklerinizi kaydetmeyi taahhüt edin.

Not Değişiklik yapıldığında, yalnızca IPMI "kasa gücü" seçeneklerini denetleyebilirsiniz. Örneğin,

Diğer IPMI Seçenekleri

Şebekeyi uzaktan kapatmak ve yeniden başlatmak için kullanılabilecek diğer IPMI istemci yazılımı da mevcuttur.

• Unix tipi ana bilgisayarlar için Ipmitool kullanılabilir ve aşağıdaki komutu kullanır:

remotemachine $ ipmitool -I lanplus -H 1.1.1.2 -U admin-P şifre şasi güç sıfırlama

• Supermicro’nun Windows için IPMI Görünümü gibi Windows için mevcut olan yazılım.

Sabit Sürücüleri Değiştirme

Uyarı Boş ön paneller ve kapak panelleri üç önemli işleve sahiptir: kasa içindeki tehlikeli gerilimlere ve akımlara maruz kalmayı önler; diğer ekipmanları bozabilecek elektromanyetik girişim (EMI) içerirler ve soğutma havasının akışını kasadan yönlendirirler. Tüm kartlar, ön yüz panelleri, ön kapaklar ve arka kapaklar yerinde olmadıkça sistemi çalıştırmayın.

Uyarı Sınıf 1 lazer ürünü.

Dikkat Cihaz bileşenlerini tutarken, hasarı önlemek için bir ESD kayışı kullanın.

İpucu Cihazın ön ve arka panellerinde yanıp sönen bir Tanımlama LED'ini açmak için ön paneldeki veya arka paneldeki Tanımlama düğmesine basabilirsiniz. Bu, rafın diğer tarafına giderken servis verdiğiniz belirli cihazı bulmanıza olanak sağlar. Bu LED'lerin yerleri için sayfa 1-7'deki “Durum Işıkları ve Düğmeleri” bölümüne bakın. Belirli bir Cisco 380 veya Cisco 680 uygulamasının yerini bulmak için seri numarası kullanmak için, ünitenin arkasındaki etikete bakın.

Sabit Sürücüleri Değiştirme

Bu bölüm aşağıdaki bilgileri içerir:

• Nüfus Yönergeleri,

• Tahrik Değiştirme Prosedürü,

Not Yalnızca arızalı bir sürücüyü değiştirebilirsiniz. Ek bir sürücü ekleyemezsiniz. Kullanıcının yüklediği ek sürücüler sistem tarafından tanınmaz.

Popülasyon Yönergelerini Artırın

Cisco 380 ve Cisco 680 series cihazı 24 sürücülü arka panel ve genişleticiye sahip sekiz adede kadar küçük form faktörü (SFF) sürücüsü içerir. Bununla birlikte, Cisco 380 ve Cisco 680 serisi cihazların çeşitli modelleri, sabit sürücüler için yalnızca iki ila sekiz yuva kullanımını destekler.

Not Modellerin hiçbiri sekizden fazla sabit sürücüyü desteklemez. Her model farklı bir maksimum sayıda sabit sürücüyü desteklediğinden, her belirli model tarafından desteklenen sabit sürücü sayısı için sayfa A-2'deki “Donanım ve Teknik Özellikler” bölümüne bakın.

Sürücü yuvası numaralandırması Şekil 3-1'de gösterilmektedir. Herhangi bir Cisco 380 ve Cisco 680 serisi cihaz modelinin desteklediği sayıdan çok daha fazla olan yirmi iki sabit sürücüyü gösterir.

Şekil 3-1 Sürücü Numaralandırması, Küçük Form Faktörlü Sürücüler

Optimum performans için bu sürücü popülasyon kurallarına uyun:

• Modellerin hiçbiri, sürücülerin 10 ila 23 arasındaki yuvalarda kullanılmasını desteklemez. Ön çerçeve mandalları, sürücü yuvalarının ikisini kaplar (yuva 1 ve yuva 24).

• Modeliniz için desteklenen numaradan daha fazla sürücü kuramazsınız. Artık çalışmayan sürücüleri değiştirebilirsiniz.

• Bir sürücüyü değiştirirken, değiştirdiğiniz sürücü ile aynı yuvayı kullanmanız gerekir.

• Boş sürücü yuvalarını kaplayan panelleri çıkarmayın.

Sürücü Değiştirme Prosedürü

Çalışırken takılabilir bir sabit sürücüyü değiştirmek veya takmak için aşağıdaki adımları izleyin:

İpucu Sabit disk sürücülerini değiştirmek için, çalışırken takılabilir olduklarından cihazı kapatmanız veya kapatmanız gerekmez.

Adım 1 Değiştirdiğiniz sürücüyü çıkarın veya boş bir sürücü tepsisini boş bir bölmeden çıkarın:

a. Sürücü tepsisinin önündeki serbest bırakma düğmesine basın. Şekil 3-2'ye bakınız.

b. Ejektör kolunu kavrayın ve açın ve ardından sürücü tepsisini yuvasından çıkarın.

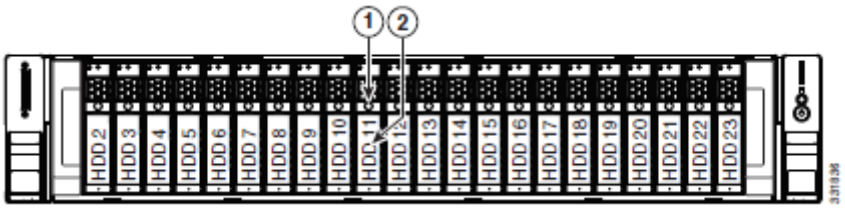
Adım 2 Yeni bir sürücü takın:

c. Sürücü tepsisindeki ejektör kolu açıkken, sürücü tepsisini boş sürücü bölmesine yerleştirin.

d. Tepsiyi arka panele temas edene kadar yuvanın içine doğru itin, ardından sürücüyü yerine kilitlemek için ejektör kolunu kapatın.

Not Yuvaların çoğunu sabit sürücüler için kullanamazsınız. Her belirli model için desteklenen maksimum sabit sürücü sayısını görmek için, sayfa A-2'deki “Donanım ve Teknik Özellikler” bölümüne bakın. Bir sürücüyü değiştirirken, değiştirdiğiniz sürücüyle aynı yuvayı kullanmanız gerekir.

Şekil 3-2 Sabit Sürücüleri Değiştirme



1	Serbest bırakma düğmesi	2	İtici kol

BAKIM, ONARIM VE KULLANIMDA UYULMASI GEREKEN KURALLAR:

Ürünün kullanıcı tarafından yapılabilecek her hangi bir bakım ya da onarım işlemi bulunmamaktadır. Potansiyel zararlardan korunmak için cihazı, sıcaktan, sıvı temasından, nemden ve tozdan koruyunuz. Cihaz ısı kaynağından en az 30 cm uzak olmalıdır.

KULLANIM SIRASINDA İNSAN VEYA ÇEVRE SAĞLIĞINA TEHLİKELİ VEYA ZARARLI OLABİLECEK DURUMLARA İLİŞKİN UYARILAR:

Lütfen kullanım ömrü tamamlandığında elektronik çöp dönüşümü yapabilen yerlere ürünü teslim ediniz.

KULLANIM HATALARINA İLİŞKİN BİLGİLER:

Burada belirtilenler ile sınırlı olmamak kaydı ile bu bölümde bazı kullanıcı hatalarına ilişkin örnekler sunulmuştur. Bu ve benzeri konulara özen göstermeniz yeterlidir.
Örnekler:
Aleti çalışır durumda taşımak, temizlemek vb. eylemler Alet üzerine katı ya da sıvı gıda maddesi dökülmesi Aletin taşıma sırasında korunmaması ve darbe alması

TÜKETİCİNİN KENDİ YAPABİLECEĞİ BAKIM, ONARIM VEYA ÜRÜNÜN TEMİZLİĞİNE İLİŞKİN BİLGİLER:

Ürünün tüketici tarafından yapılabilecek bir bakım prosedürü bulunmamaktadır. Cihaz çalışır durum da iken temizlik yapmayınız. Islak bezle, köpürtülmüş deterjanlarla, sulu süngerlerle temizlik yapmayınız.

ÜRÜN HERHANGİ BİR PERİYODİK BAKIM ONARIM GEREKTİRMEMEKTEDİR.

MALIN ENERJİ TÜKETİMİ AÇISINDAN VERİMLİ KULLANIMINA İLİŞKİN BİLGİLER

Satın almış olduğunuz ürünün ömrü boyunca enerji tüketimi açısından verimli kullanımı için bakım hizmetlerinin yetkilendirilmiş sertifikalı elemanlarca yapılması gerekmektedir.

TAŞINMA ve NAKLİYE SIRASINDA DİKKAT EDİLECEK HUSUSLAR

- Paketlerken, orijinal kutusunu ve paketleme malzemelerini kullanın.
- Cihazı kullanırken ve daha sonra bir yer değişikliği esnasında sarsmamaya, darbe, ısı, rutubet ve tozdan zarar görmemesine özen gösteriniz.

TÜKETİCİNİN SEÇİMLİLİK HAKLARI

Malın ayıplı olduğunun anlaşılması durumunda tüketici, 6502 sayılı Tüketicinin Korunması Hakkında Kanunun 11 inci maddesinde yer alan;

a- Sözleşmeden dönme,

b- Satış bedelinden indirim isteme,

c- Ücretsiz onarılmasını isteme,

ç- Satılanın ayıpsız bir misli ile değiştirilmesini isteme, haklarından birini kullanabilir.

Tüketicinin bu haklardan ücretsiz onarım hakkını seçmesi durumunda satıcı; işçilik masrafı, değiştirilen parça bedeli ya da başka herhangi bir ad altında hiçbir ücret talep etmeksizin malın onarımını yapmak veya yaptırmakla yükümlüdür. Tüketici ücretsiz onarım hakkını üretici veya ithalatçıya karşı da kullanabilir. Satıcı, üretici ve ithalatçı tüketicinin bu hakkını kullanmasından müteselsilen sorumludur.

Tüketicinin, ücretsiz onarım hakkını kullanması halinde malın;

- Garanti süresi içinde tekrar arızalanması,

- Tamiri için gereken azami sürenin aşılması,

- Tamirinin mümkün olmadığının, yetkili servis istasyonu, satıcı, üretici veya ithalatçı tarafından bir raporla belirlenmesi durumlarında; tüketici malın bedel iadesini, ayıp oranında bedel indirimini veya imkân varsa malın ayıpsız misli ile değiştirilmesini satıcıdan talep edebilir. Satıcı, tüketicinin talebini reddedemez. Bu talebin yerine getirilmemesi durumunda satıcı, üretici ve ithalatçı müteselsilen sorumludur.

Tüketici, garantiden doğan haklarının kullanılması ile ilgili olarak çıkabilecek uyuşmazlıklarda yerleşim yerinin bulunduğu veya tüketici işleminin yapıldığı yerdeki Tüketici Hakem Heyetine veya Tüketici Mahkemesine başvurabilir.

AEEE YÖNETMELİĞİNE UYGUNDUR. 

İthalatçı Firma

TECH DATA BİLGİSAYAR SİSTEMLERİ A.Ş.

Saray Mahallesi, Site Yolu Sokak

Anel İş Merkezi No:5 Kat:8

Ümraniye, İstanbul,34768

Tel : +90 216 999 53 50

Üretici Firma

Cisco Systems, Inc.

170 West Tasman Drive San Jose, CA 95134-1706 USA http://www.cisco.com

Tel: 408 526-4000 800 553-NETS (6387) Fax: 408 527-0883