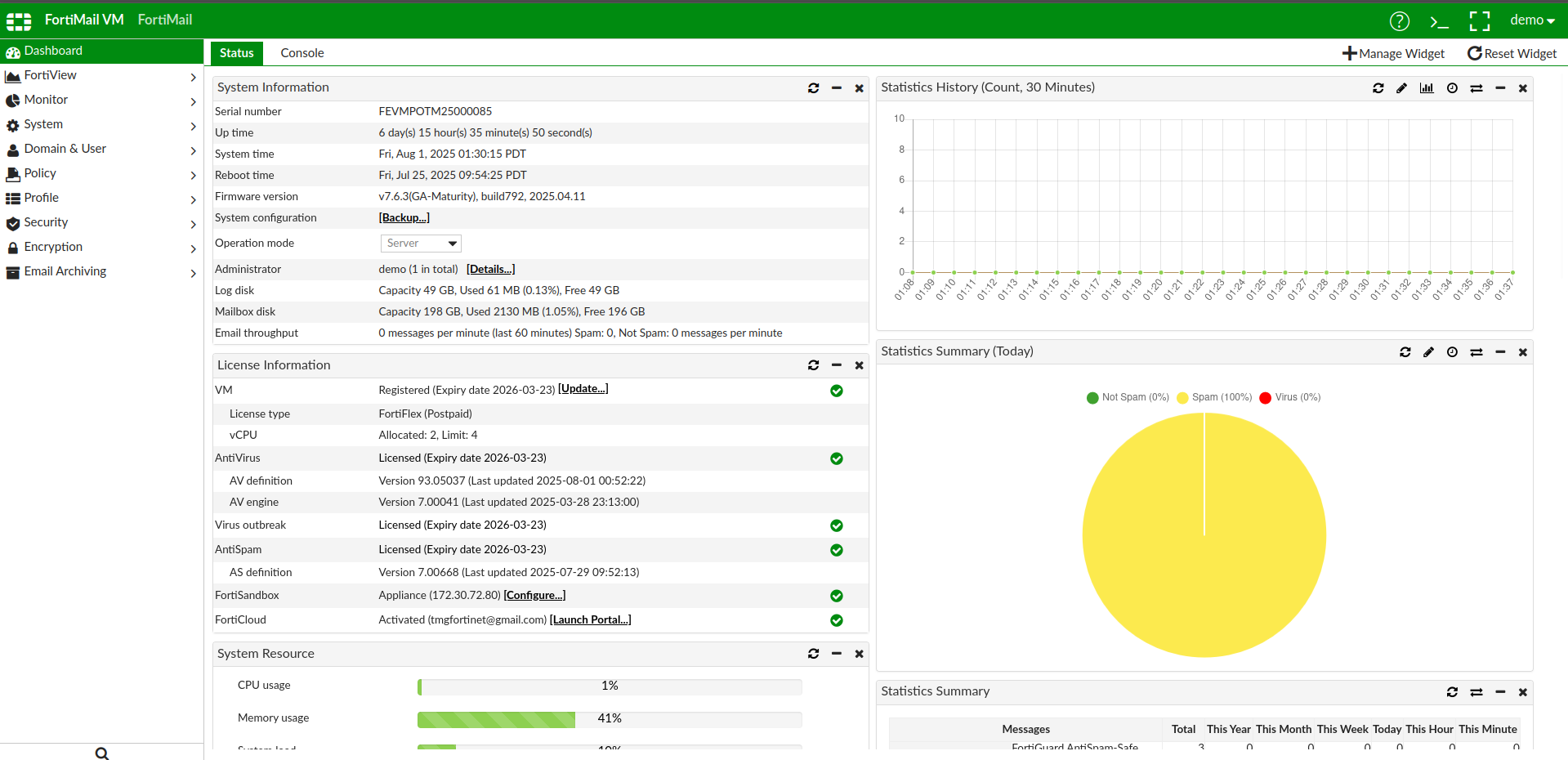
**FortiMail**

FortiMail, Fortinet tarafından geliştirilen, e-posta iletişimini kötü amaçlı yazılımlara, spam'e, kimlik avı saldırılarına ve diğer siber tehditlere karşı korumak için tasarlanmış kapsamlı bir e-posta güvenlik platformudur.

Temel olarak, FortiMail bir e-posta güvenlik ağ geçidi (email security gateway) gibi çalışır. Bir kuruluşun e-posta sunucusu ile internet arasında konumlanır ve tüm gelen/giden e-posta trafiğini inceler. Amacı, zararlı veya istenmeyen e-postaların ağınıza ulaşmasını engellemek ve hassas bilgilerin dışarıya sızmasını önlemektir. Başlıca yetenekler şunlardır:

* **Anti-Spam Koruması:** İstenmeyen toplu e-postaları (spam) algılar ve engeller. Gelişmiş filtreleme teknikleri ve itibar tabanlı kontroller kullanır.
* **Anti-Virüs ve Anti-Malware Koruması:** E-postalardaki ekleri ve bağlantıları virüs, fidye yazılımı (ransomware) ve diğer kötü amaçlı yazılımlara karşı tarar ve temizler.
* **Kimlik Avı (Phishing) Koruması:** Kullanıcıları aldatmaya yönelik sahte e-postaları (kimlik avı saldırıları) tespit eder ve engeller. Sahte web sitelerine yönlendiren bağlantıları bloke eder.
* **İçerik Filtreleme:** Belirli anahtar kelimeler, dosya türleri veya hassas bilgiler içeren e-postaları kural tabanlı olarak engeller veya karantinaya alır. Bu, veri sızıntısı (DLP - Data Loss Prevention) önlemleri için de kullanılabilir.
* **Karantina Yönetimi:** Şüpheli veya engellenen e-postaları kullanıcıların veya yöneticilerin inceleyebileceği güvenli bir alana yönlendirir.
* **E-posta Şifreleme:** Hassas e-postaların güvenli bir şekilde gönderilmesini sağlamak için şifreleme özellikleri sunar.
* **Yüksek Erişilebilirlik ve Performans:** Büyük hacimli e-posta trafiğini işleyebilecek şekilde tasarlanmıştır ve kesintisiz hizmet için yüksek erişilebilirlik seçenekleri sunar.

**Dashboard:**

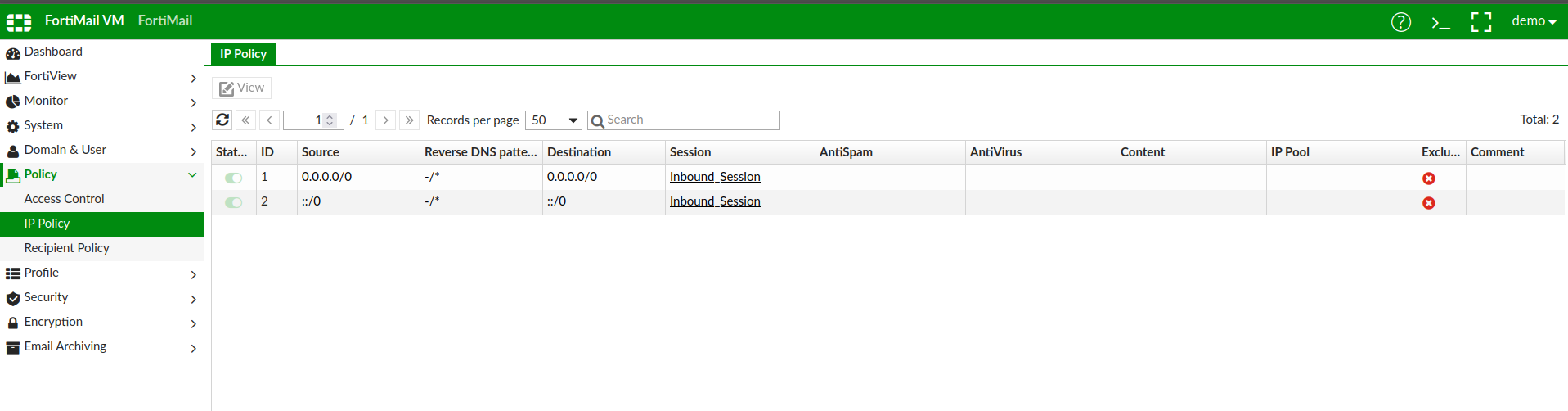


* **Sistem** **Bilgileri**: Cihazın çalışma süresi, yazılım sürümü, disk kullanımı gibi temel operasyonel veriler.
* **Lisans** **Bilgileri**: Antivirüs, anti-spam gibi güvenlik özelliklerinin lisans durumları ve geçerlilik süreleri.
* **Kaynak** **Kullanımı**: İşlemci ve bellek gibi sistem kaynaklarının anlık kullanım oranları.
* **İstatistikler**: Gelen/giden e-posta sayısı, spam ve virüs algılama oranları gibi e-posta trafiği istatistikleri, genellikle grafiklerle görselleştirilmiştir.

**Policy**

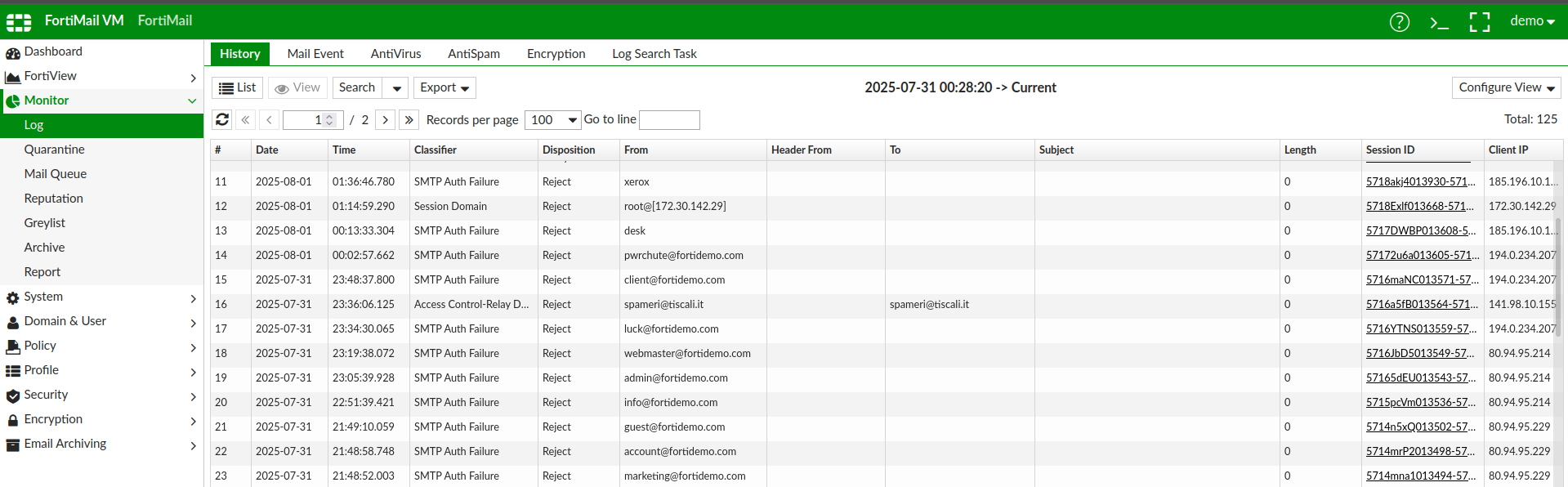
**Access Control:** Bu kısım, kimlerin veya hangi kaynakların FortiMail üzerinden e-posta gönderip alabileceğini kontrol eden kuralları içerir. Genellikle IP adreslerine veya alan adlarına (domain) dayalı olarak e-posta trafiğine izin verme veya engelleme gibi işlemleri yönetir. Örneğin, belirli bir IP adresinden gelen e-postaları reddedebilir veya yalnızca belirli alan adlarına e-posta göndermeye izin verebilirsiniz. Bu, spam gönderenleri veya yetkisiz erişimi engellemek için ilk savunma hattıdır.

* **IP Policy:** Bu politikalar, gelen ve giden e-posta trafiğini kaynak veya hedef IP adreslerine göre filtrelemek için kullanılır. Access Control ile benzer görünse de, IP Policy genellikle daha karmaşık veya öncelikli kurallar belirlemek için kullanılır. Örneğin, belirli bir IP aralığından gelen tüm e-postaları doğrudan reddetmek, veya belirli bir güvenilir IP aralığından gelen e-postalar için daha az katı güvenlik denetimi uygulamak gibi senaryolar için kullanılabilir.
* **Recipient Policy:** Bu politikalar, e-postanın alıcılarına (recipient) göre belirli güvenlik eylemlerinin uygulanmasını sağlar. Örneğin:
  + Belirli bir alıcıya (veya alıcı grubuna) gönderilen e-postalara daha sıkı spam veya virüs taraması uygulamak.
  + Hassas bir departmanın e-postaları için şifreleme zorunluluğu getirmek.
  + Tanımlı olmayan (geçersiz) alıcılara gönderilen e-postaları nasıl işleyeceğini (reddeder, karantinaya alır vb.) belirlemek.
  + Alıcı adresleri yeniden yazma (address rewriting) veya takma ad (alias) yönetimi gibi özellikler de burada yapılandırılabilir.

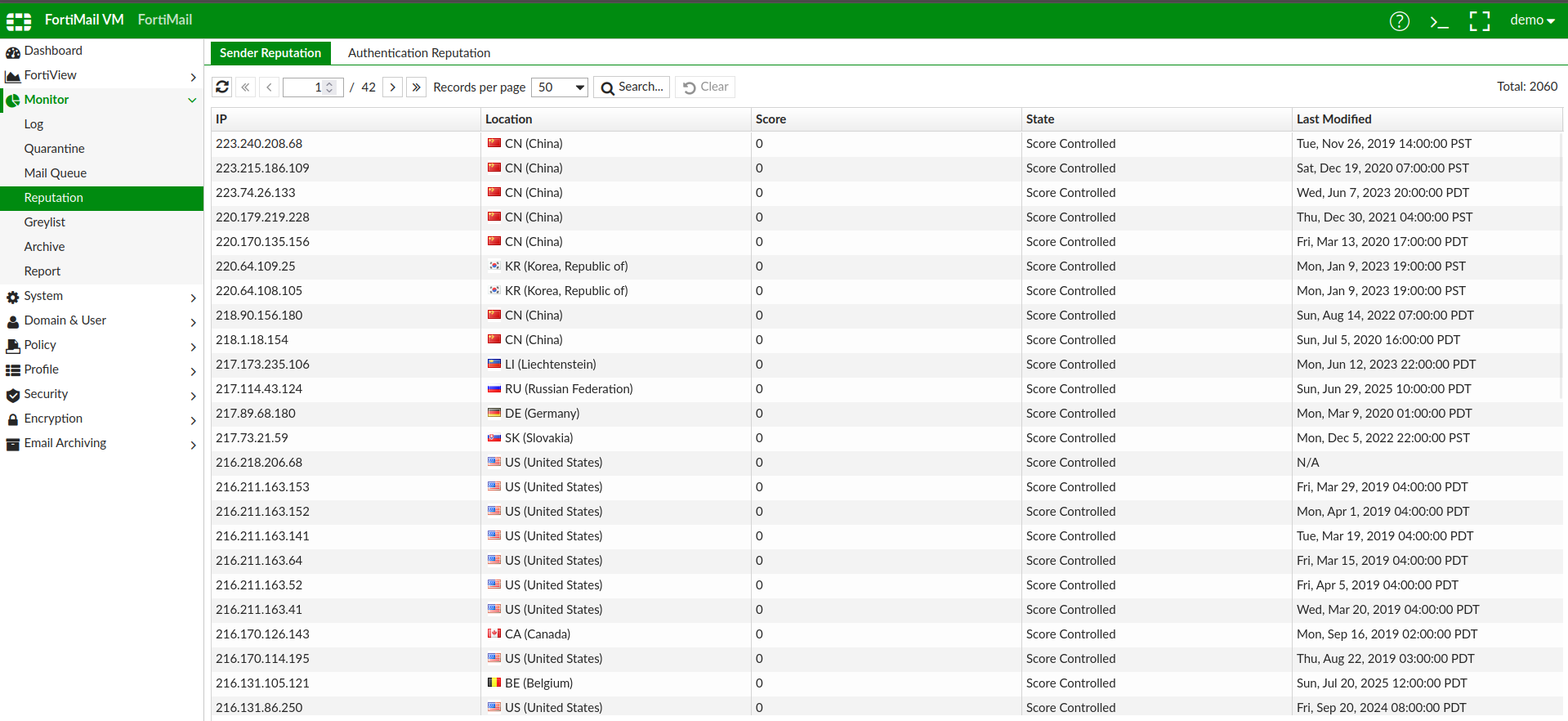


**Monitor**

* **Log:** FortiMail cihazının ürettiği tüm sistem ve güvenlik günlüklerinin (logların) görüntülendiği yerdir. Bu günlükler, e-posta akışı olayları (gelen/giden e-postalar), güvenlik taramalarının sonuçları (spam, virüs tespiti), sistem hataları, yönetici erişimleri gibi çeşitli bilgileri içerir. Sorun giderme, güvenlik olaylarını inceleme ve denetim amaçlı kullanılır.



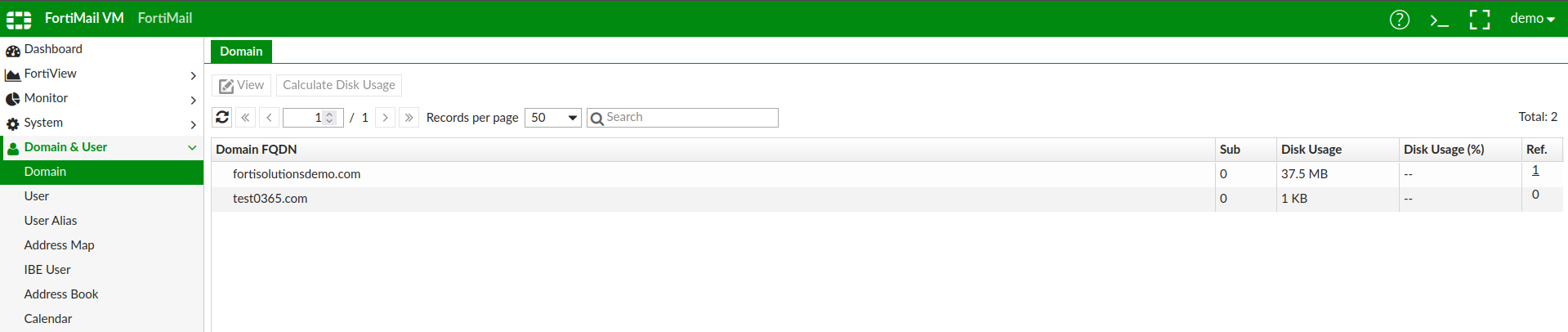
* **Quarantine:** FortiMail tarafından spam, virüs içeren veya politika ihlali yapan e-postaların geçici olarak tutulduğu güvenli alandır. Bu bölümde yöneticiler veya yetkilendirilmiş kullanıcılar, karantinaya alınan e-postaları inceleyebilir, serbest bırakabilir (Inbox'a gönderebilir), silebilir veya kara listeye alabilir.
* **Mail Queue:** FortiMail'in işlenmek üzere bekleyen veya bir hedefe iletilmek üzere sıraya konulmuş e-postaların durumunu gösterir. Eğer e-postalar teslim edilemiyorsa (örneğin, alıcı sunucunun meşgul olması veya DNS sorunları nedeniyle), burada kuyruğa alınırlar. Bu bölüm, e-posta akışındaki olası tıkanıklıkları veya teslimat sorunlarını teşhis etmek için önemlidir.
* **Reputation:** IP adresleri, alan adları veya gönderenler hakkında itibar bilgilerini yönettiğiniz yerdir. FortiMail, FortiGuard Labs'ten gelen itibar verilerini kullanarak bilinen spam gönderenlerini veya kötü niyetli kaynakları engeller. Buradan manuel olarak kara listeler (blacklist) veya beyaz listeler (whitelist) oluşturarak belirli IP'lerin veya alan adlarının itibarını düzenleyebilirsiniz.



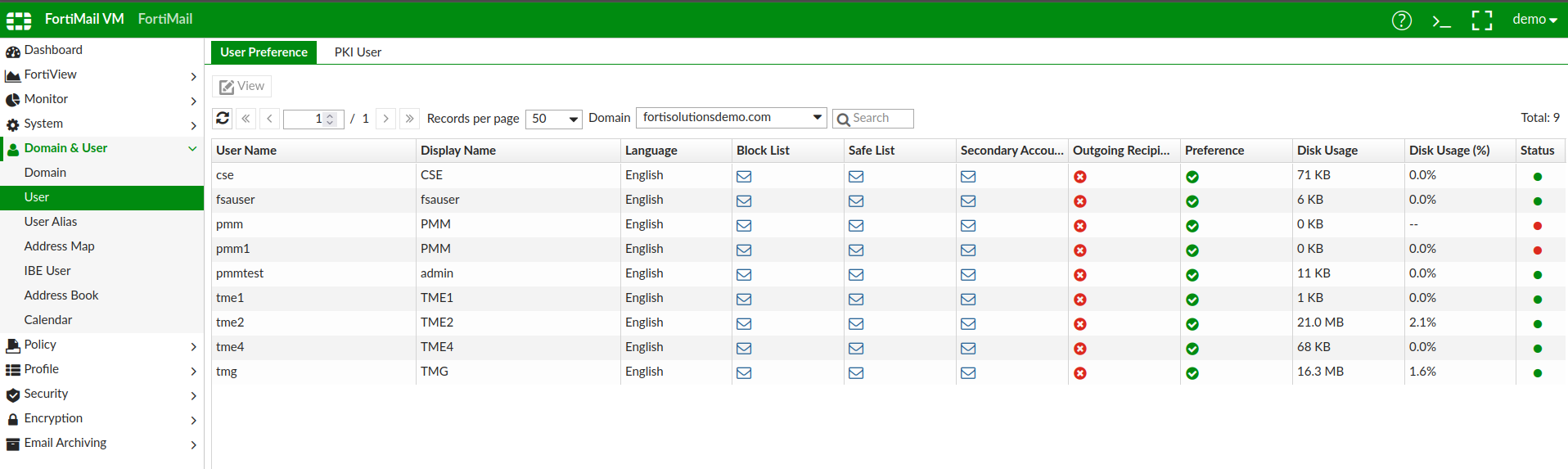
* **Greylist:** Greylisting, spam'i azaltmaya yönelik bir tekniktir. Bilinmeyen bir göndericiden ilk kez gelen e-postayı geçici olarak reddeder ve göndericinin e-postayı yeniden denemesini bekler. Meşru posta sunucuları yeniden denerken, çoğu spam göndericisi denemez. Bu bölümde, greylist'e alınan IP adreslerini ve bunların durumunu görebilir, manuel olarak izin verebilir veya engelleyebilirsiniz.
* **Archive:** FortiMail'in arşivleme özelliği etkinleştirilmişse, bu bölümde arşivlenmiş e-postaları görüntüleyebilir, arayabilir ve yönetebilirsiniz. E-posta arşivleme, yasal uyumluluk, e-posta kurtarma veya denetim amaçları için önemli olabilir.
* **Report:** FortiMail'in topladığı verilerden yola çıkarak çeşitli raporlar oluşturmanızı sağlar. Bu raporlar, spam ve virüs istatistikleri, e-posta akışı özetleri, en çok e-posta gönderen/alanlar, politika ihlalleri gibi bilgileri içerebilir. Güvenlik performansı hakkında düzenli bilgi edinmek ve trendleri izlemek için kullanılır.

**Domain & User**

* **Domain:** FortiMail'in e-posta trafiğini yönettiği alan adlarının (örneğin, "https://www.google.com/search?q=ornekfirma.com", "sirketim.net") eklendiği, düzenlendiği ve yapılandırıldığı yerdir. Her bir alan adı için farklı ayarlar (örneğin, MX kayıtları, e-posta rotalama, varsayılan politika atamaları) tanımlanabilir. FortiMail, bu tanımlı alan adlarına gelen veya bu alan adlarından giden e-postaları işler.



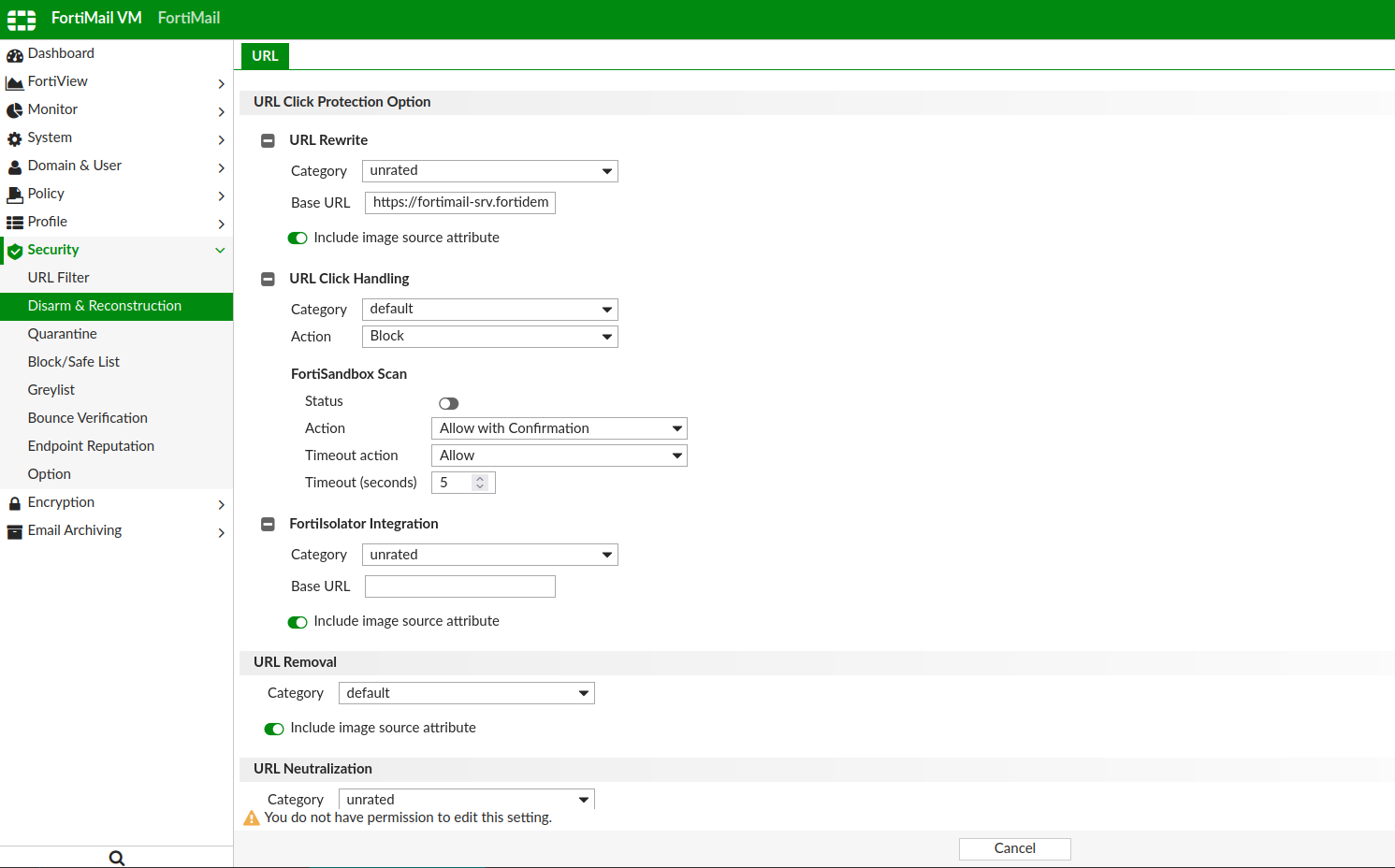
* **User:** FortiMail üzerinde e-posta hesabı olan veya e-posta hizmetlerinden faydalanan bireysel kullanıcı hesaplarının yönetildiği bölümdür. Kullanıcı adları, şifreler, e-posta adresleri ve her kullanıcı için geçerli olabilecek belirli ayarlar (örneğin, karantina erişimi, dil ayarları) burada tanımlanır. Kullanıcılar FortiMail'in kendi yerel veritabanında saklanabilir veya FortiMail, LDAP, Active Directory gibi harici dizin servisleriyle entegre olabilir.



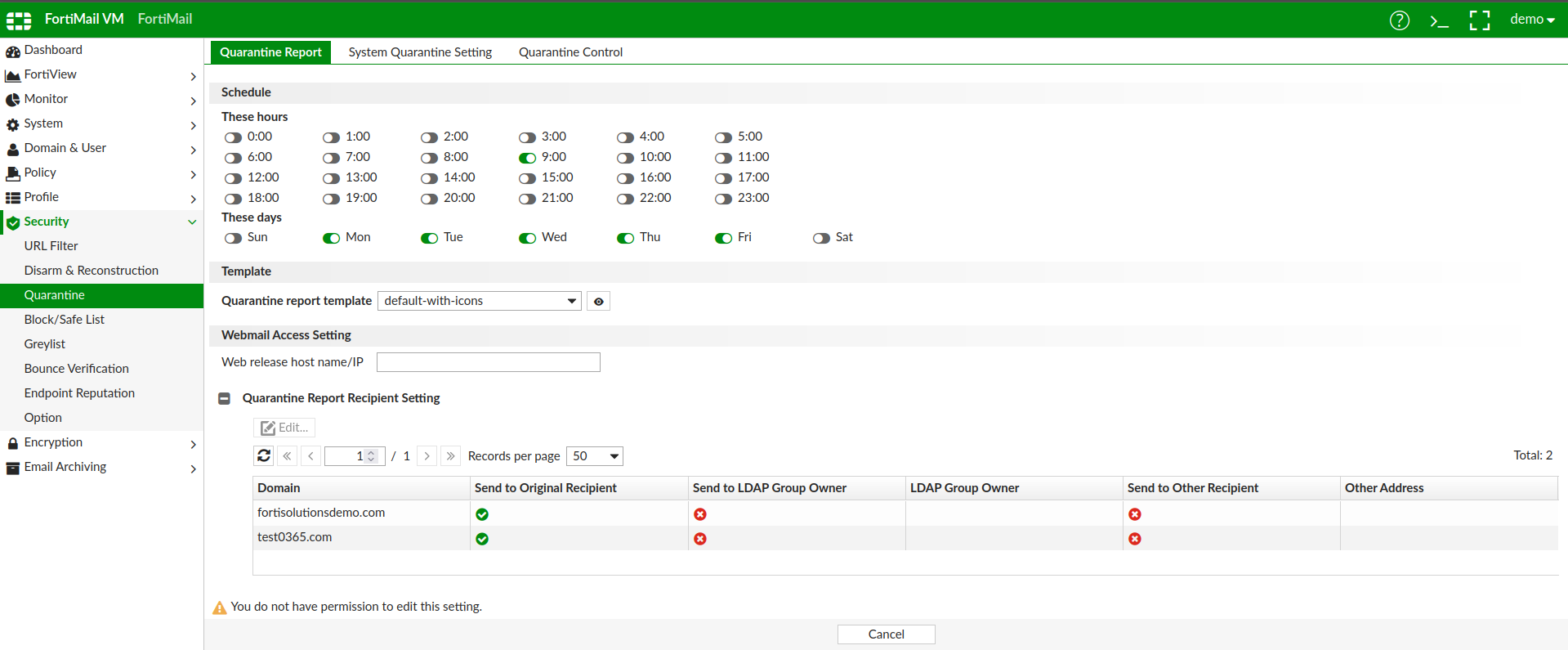
* **User Alias:** Bir kullanıcı hesabına atanmış ek e-posta adreslerinin (takma adların) yönetildiği yerdir. Örneğin, "bilgi@https://www.google.com/search?q=ornekfirma.com" ve "destek@https://www.google.com/search?q=ornekfirma.com" adreslerinin aslında "ahmet.yilmaz@https://www.google.com/search?q=ornekfirma.com" kullanıcısının posta kutusuna yönlendirilmesini sağlamak için kullanılır. Bu, aynı posta kutusuna birden fazla adresten e-posta almayı mümkün kılar.
* **Address Map:** E-posta adreslerinin eşleştirilmesi veya yeniden yazılması (address rewriting) kurallarının tanımlandığı bölümdür. Özellikle karmaşık e-posta yönlendirme senaryolarında veya dahili ve harici adresleme farklılıklarını yönetmek için kullanılır. Örneğin, dahili bir e-posta adresini dışarıya farklı bir adla göstermek veya belirli gelen adresleri başka bir adrese yönlendirmek için kullanılabilir.
* **IBE User:** IBE (Identity-Based Encryption - Kimlik Tabanlı Şifreleme) özelliği kullanılan kullanıcıların yönetildiği bölümdür. FortiMail'in şifreli e-posta gönderme/alma yeteneklerinden yararlanan kullanıcılar için özel ayarlar ve kayıtlar burada tutulur. Bu kullanıcılar genellikle özel bir parola veya kimlik doğrulama yöntemiyle şifreli e-postalarına erişirler.
* **Address** **Book**: FortiMail'de tanımlanmış e-posta adreslerinin veya gruplarının bir listesidir. Bu adres defteri, e-posta politikalarında kaynak veya hedef olarak kullanılabilir, böylece belirli gruplara yönelik kuralların tanımlanması kolaylaşır. Örneğin, "Tüm Satış Ekibi" gibi bir grup oluşturup bu gruba giden e-postalar için belirli bir kural uygulayabilirsiniz.
* **Calendar**: FortiMail'in bazı entegrasyonlarında veya yönetim arayüzünde takvimle ilgili özellikleri veya zamanlanmış raporları/işlemleri gösteren bir bölüm olabilir. Bu, doğrudan e-posta gönderme/alma işlevselliğiyle ilgili olmaktan ziyade, yönetimsel veya operasyonel planlamaya yardımcı olabilir. (Genellikle e-posta gateway cihazlarında pek sık rastlanmayan bir özellik olmakla birlikte, burada listelenmesi FortiMail'in geniş yeteneklerine işaret eder.)

**Securtiy**

* **URL Filter**: Gelen e-postalardaki web bağlantılarını (URL'leri) analiz ederek kötü amaçlı, kimlik avı (phishing) veya istenmeyen sitelere yönlendiren URL'leri engellemek için kullanılır. Kullanıcıları zararlı web sitelerinden korur.
* **Disarm & Reconstruction:** Bu, e-posta eklerindeki veya HTML içeriğindeki potansiyel olarak zararlı aktif içeriği (makrolar, gömülü komut dosyaları vb.) kaldırma işlemidir. Orijinal dosyayı "silahsızlandırılmış" bir versiyona dönüştürürken, dosyanın işlevselliğini mümkün olduğunca korur. Gelişmiş tehdit koruması sağlar.



* **Quarantine**: FortiMail tarafından zararlı veya istenmeyen olarak algılanan e-postaların geçici olarak tutulduğu yerdir. Kullanıcılar veya yöneticiler karantinadaki e-postaları inceleyebilir, serbest bırakabilir veya kalıcı olarak silebilir. Bu, yanlış pozitifleri yönetmek ve şüpheli e-postaları izlemek için önemlidir.



* **Block/Safe List:**
  + **Block List:** Belirli göndericilerden (e-posta adresleri, etki alanları veya IP adresleri) gelen e-postaları doğrudan reddetmek veya karantinaya almak için kullanılır.
  + **Safe List:** Belirli göndericilerden gelen e-postaların her zaman teslim edilmesini sağlamak için kullanılır, böylece bu e-postalar güvenlik taramalarından etkilenmez. Güvenilir kaynaklardan gelen e-postaların engellenmemesini garanti eder.
* **Greylist:** İstenmeyen e-posta (spam) ile mücadele etmek için kullanılan bir tekniktir. İlk kez gelen bilinmeyen göndericilerden gelen e-postaları geçici olarak reddeder ve göndericinin e-postayı standartlara uygun olarak yeniden göndermesini bekler. Çoğu yasal e-posta sunucusu yeniden deneyeceği için e-posta sonunda ulaşır, ancak spam göndericiler genellikle yeniden denemezler.
* **Bounce Verification:** Geri dönen (teslim edilemeyen) e-postaların (bounce mesajları) gerçek mi yoksa sahte mi olduğunu doğrulamak için kullanılır. Spam göndericileri, e-posta adreslerini doğrulamak veya sahte geri dönüş mesajları oluşturmak için sıkça kullanırlar, bu özellik bu tür sahtekarlıkları engellemeye yardımcı olur.
* **Endpoint Reputation:** Bu özellik, bir uç noktanın (genellikle FortiClient ile izlenen bir bilgisayar veya cihaz) güvenlik durumunu ve itibarını dikkate alır. E-posta güvenlik kararları alınırken (örneğin, bir kullanıcının güvenilir bir uç noktadan e-posta gönderip göndermediği gibi) bu itibar bilgisi kullanılabilir. Bu, Fortinet Security Fabric'in bir parçası olarak daha geniş bir güvenlik perspektifi sunar.
* **Option:** Bu genellikle "Security" bölümündeki diğer alt menü öğelerinin genel ayarlarını veya özel seçeneklerini içeren bir bölümdür. Diğer menülerdeki belirli güvenlik özellikleriyle ilgili ek yapılandırmalar veya global ayarlar burada bulunabilir.