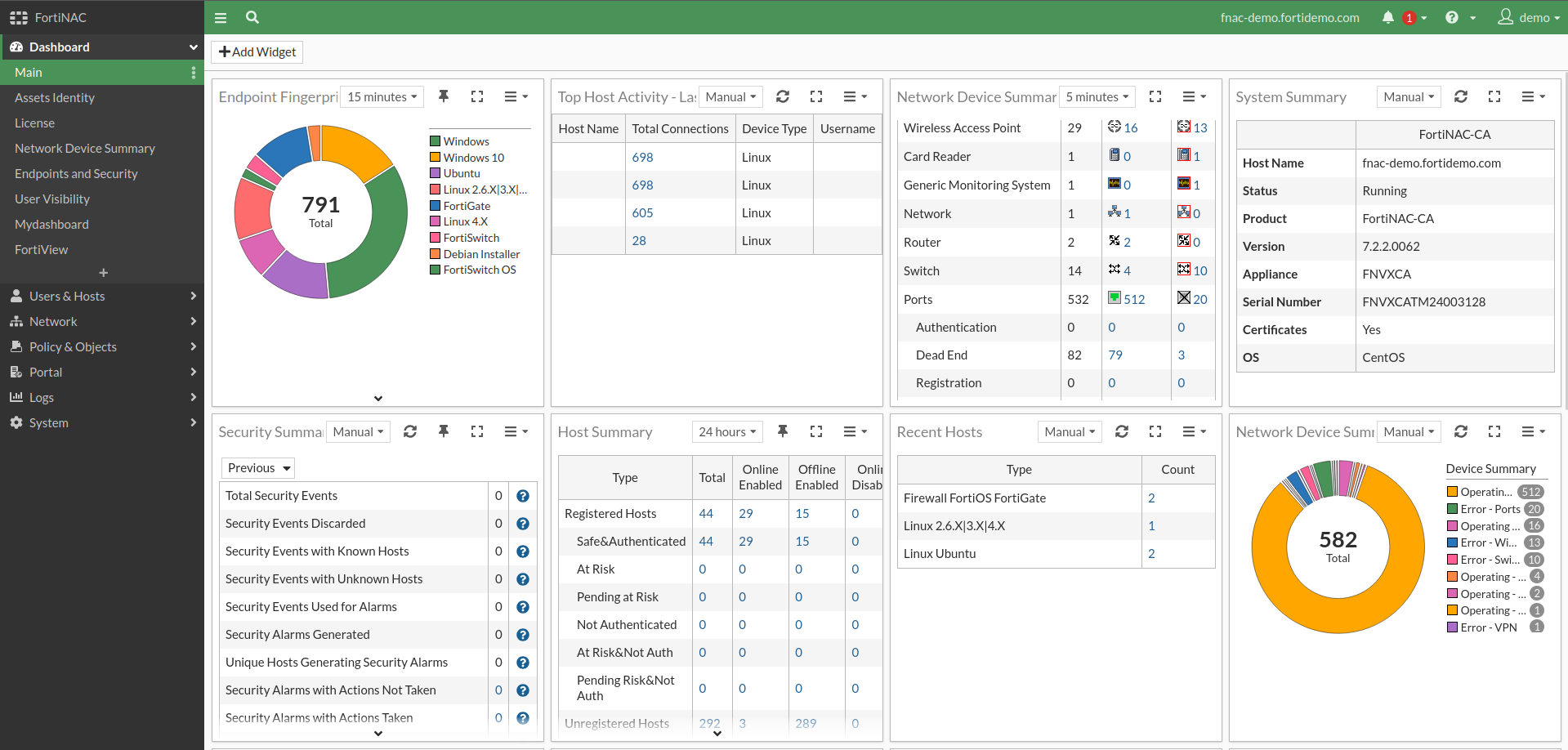
**FortiNAC**

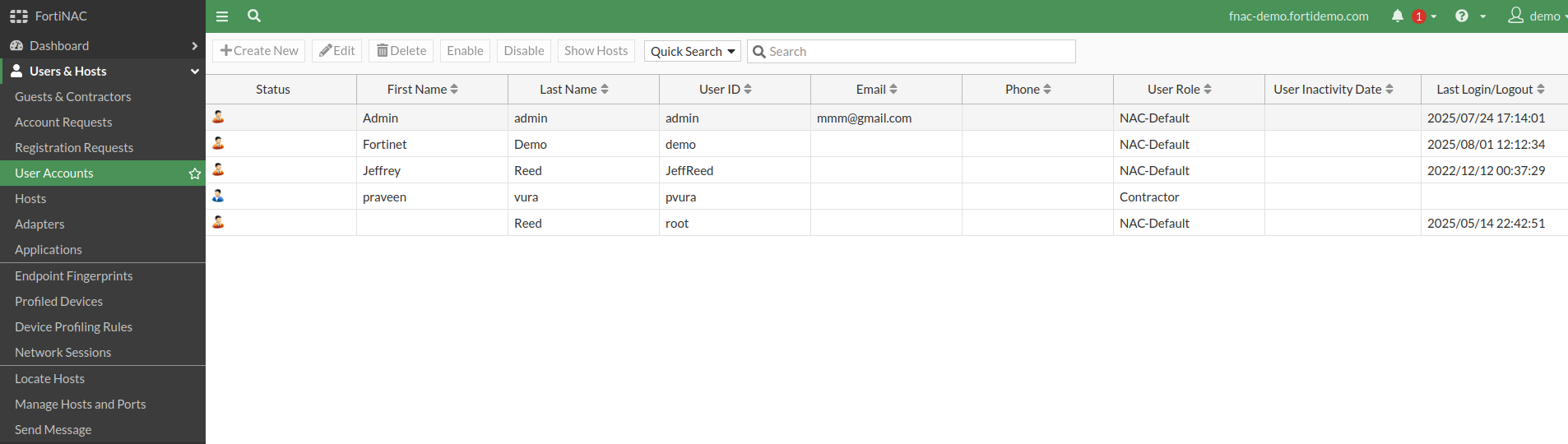
FortiNAC, Fortinet tarafından geliştirilen bir Ağ Erişim Kontrolü (Network Access Control - NAC) çözümüdür. Temel olarak, bir ağa bağlanmaya çalışan her cihazın ve kullanıcının kimliğini doğrulamak, güvenlik duruşunu değerlendirmek ve önceden belirlenmiş politikalara göre ağ kaynaklarına erişimini düzenlemek için kullanılır.



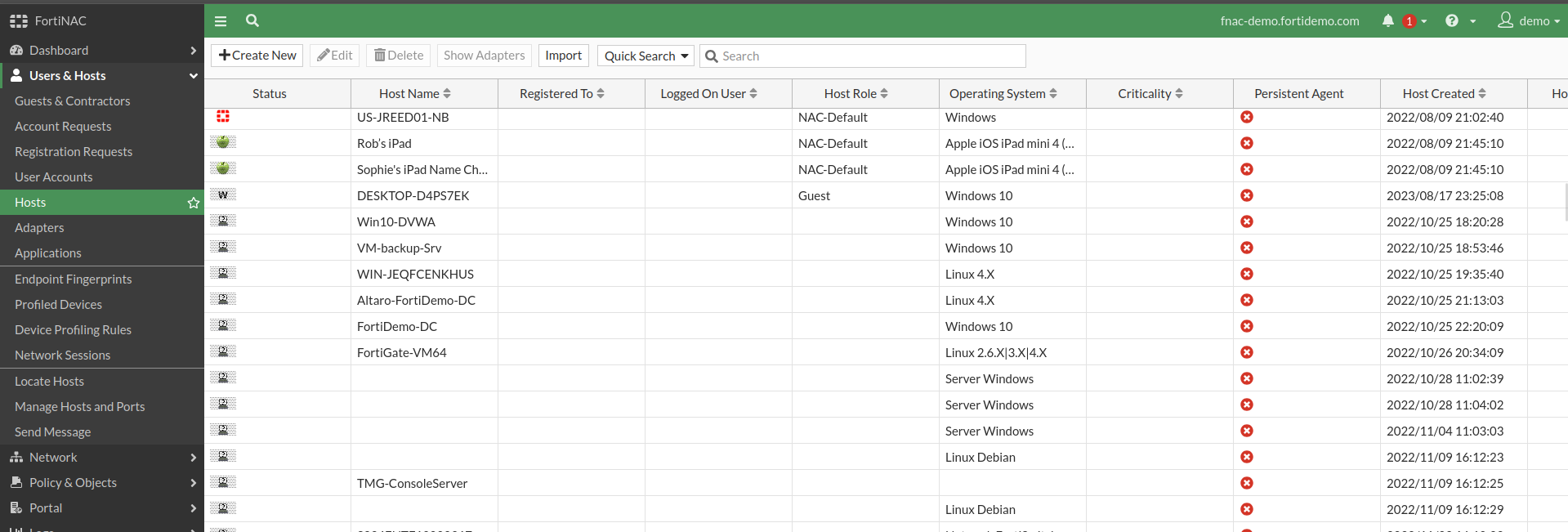
* **Main:** FortiNAC kontrol panelinin ana görünümüdür. Genellikle sistemin genel durumunu, ana bilgisayar (host) ve ağ cihazı özetlerini, güvenlik durumunu gösteren varsayılan widget'ları içerir. Bu, sisteme genel bir bakış atmak için kullanılan ilk sayfadır.
* **Assets Identity:** Ağdaki cihazların (varlıkların) kimliklendirilmesi ve parmak izi bilgileriyle ilgili özel bir kontrol paneli görünümüdür. Hangi cihazların tanımlandığı, işletim sistemleri ve cihaz türleri gibi detayları burada özetlenir.
* **License:** FortiNAC lisans bilgilerini ve geçerlilik durumunu gösteren bir kontrol paneli görünümüdür.
* **Network Device Summary:** FortiNAC tarafından yönetilen ağ cihazlarının (anahtarlar, yönlendiriciler, AP'ler) durumunu, sayılarını ve ilgili özet istatistiklerini gösteren özel bir kontrol paneli görünümüdür.
* **Endpoints and Security:** Ağdaki uç noktaların (son kullanıcı cihazları) güvenlik duruşu ve uyumluluk durumu hakkında detaylı özetler sunan bir kontrol paneli görünümüdür. Karantinaya alınan veya uyumsuz cihazlar gibi bilgiler burada vurgulanır.
* **User Visibility:** Ağdaki kullanıcıların bağlantılarını, oturumlarını ve davranışlarını izlemeye odaklanan bir kontrol paneli görünümüdür. Kimlerin, ne zaman ve hangi cihazla ağa bağlandığına dair özet bilgiler sunar.
* **Mydashboard:** Kullanıcıların kendi tercihlerine göre özelleştirebilecekleri veya oluşturabilecekleri kişisel kontrol panellerini içerir. Bu, belirli bir rol veya görev için önemli olan widget'ları bir araya getirme esnekliği sağlar.
* **FortiView:** FortiNAC'in güçlü bir görselleştirme ve raporlama aracıdır. Ağdaki erişim olaylarını, kullanıcı ve cihaz bağlantılarını, güvenlik ihlallerini gerçek zamanlı veya geçmişe dönük olarak detaylı grafikler ve tablolarla gösterir. Bu, derinlemesine analiz ve sorun giderme için kullanılır.

**Users & Hosts**

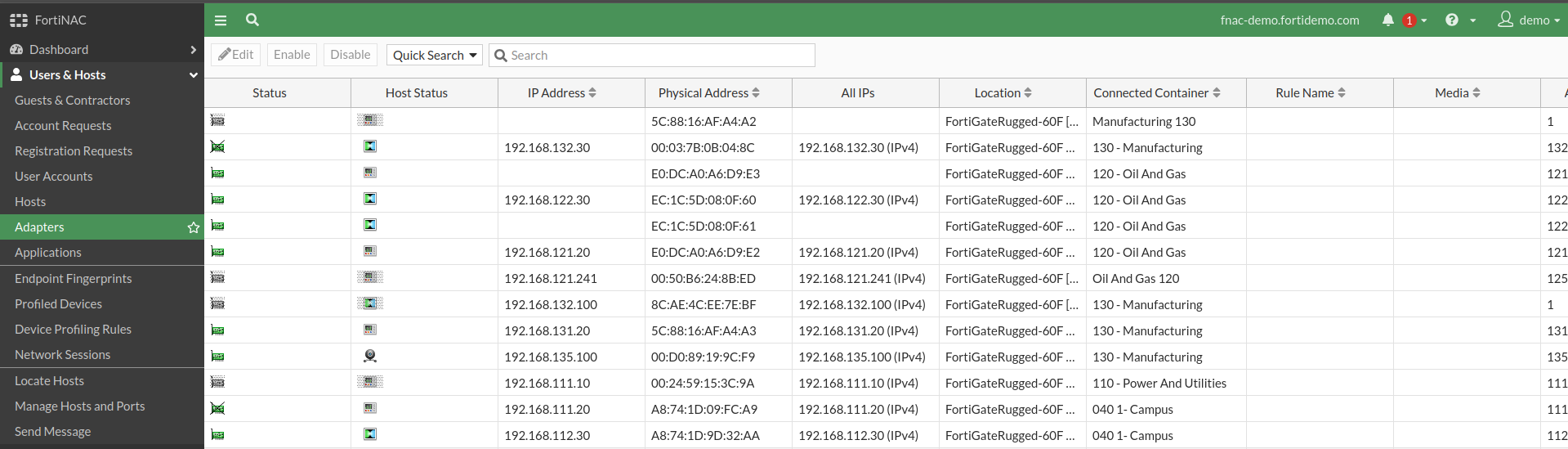
* **Guests & Contractors:** Misafir kullanıcılar ve yükleniciler gibi geçici ağ erişimi gerektiren kişilerin hesaplarının yönetildiği yerdir. Bu bölüm, misafir kaydı, hesap oluşturma ve misafir erişim politikalarını yapılandırma gibi işlevleri içerir.
* **Account Requests:** Misafirlerin veya diğer kullanıcıların ağ erişimi için gönderdiği hesap taleplerinin incelendiği ve onaylandığı veya reddedildiği yerdir.
* **Registration Requests:** Belirli cihazların veya kullanıcıların ağa bağlanmadan önce kendilerini kaydettirmelerini gerektiren durumlarda gelen kayıt taleplerinin yönetildiği bölümdür.
* **User Accounts:** FortiNAC üzerinde tanımlı tüm kullanıcı hesaplarının (misafir, çalışan vb.) yönetildiği yerdir. Bu hesaplar FortiNAC'in kendi veritabanında olabilir veya LDAP/Active Directory gibi harici sistemlerden senkronize edilebilir. Kullanıcı detayları, rolleri ve erişim izinleri burada ayarlanır.



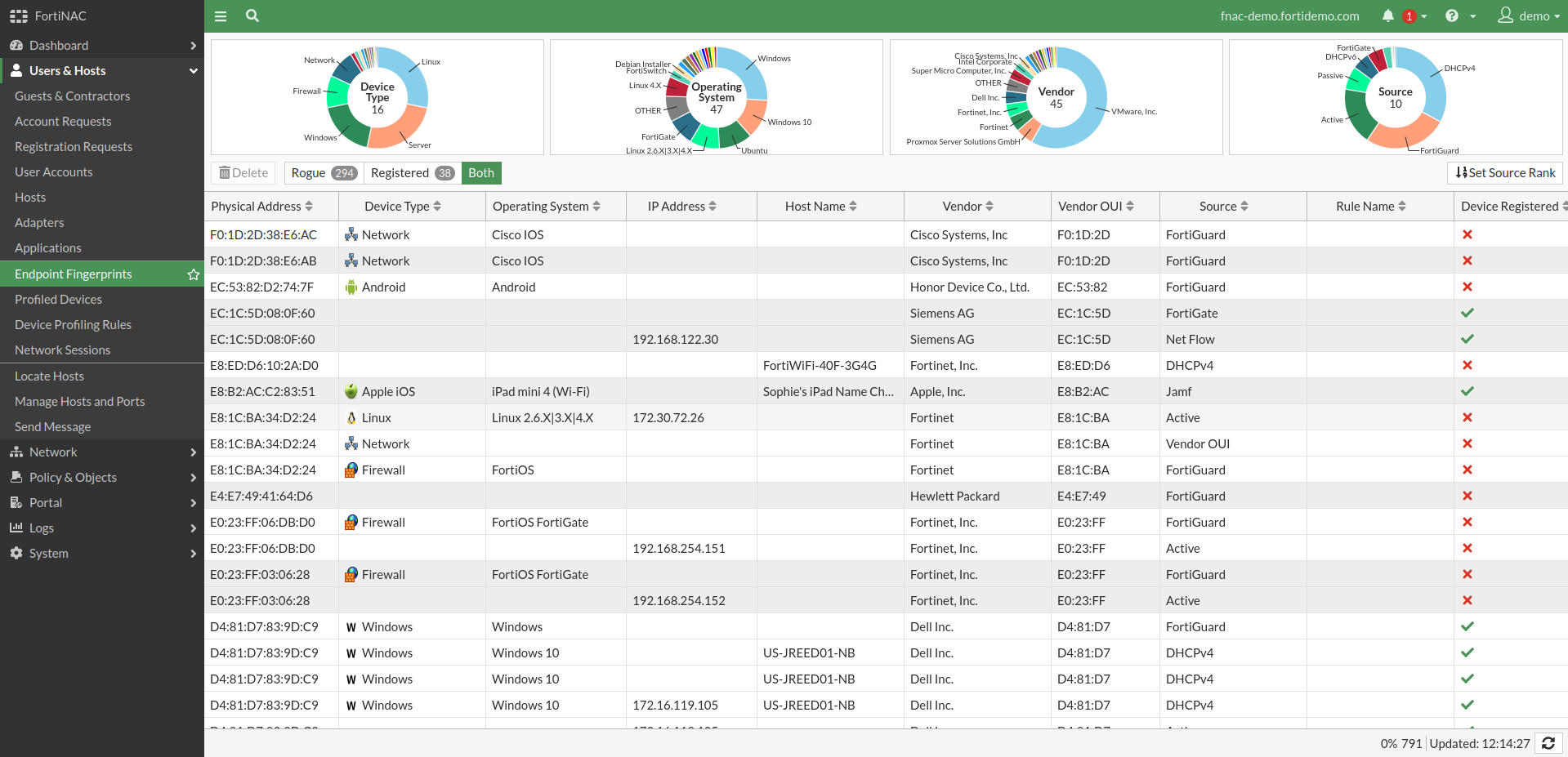
* **Hosts:** Ağınıza bağlı olan veya daha önce bağlanmış tüm cihazların (bilgisayarlar, sunucular, telefonlar vb.) listesidir. Her bir ana bilgisayarın MAC adresi, IP adresi, işletim sistemi, bağlantı durumu ve atanan profili gibi detayları buradan izlenebilir.



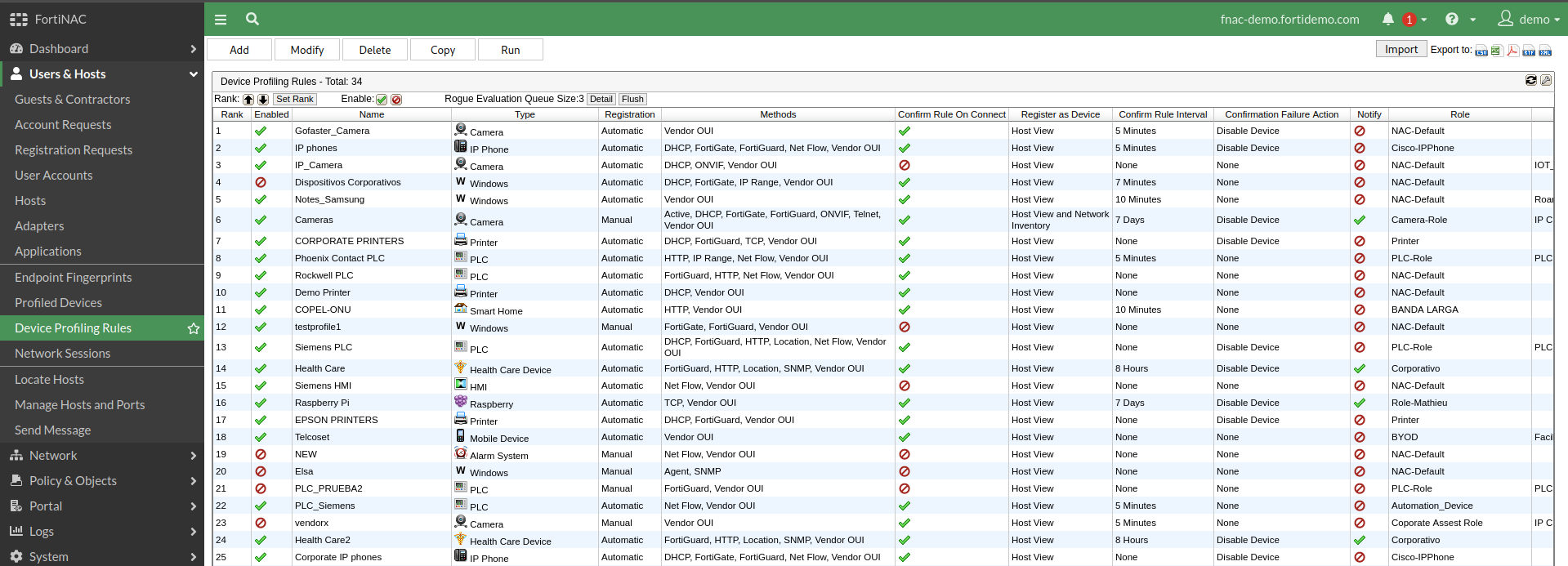
* **Adapters:** Cihazların ağa bağlanmak için kullandığı ağ bağdaştırıcıları (örneğin, Ethernet kartları, Wi-Fi bağdaştırıcıları) ile ilgili bilgileri gösterir.



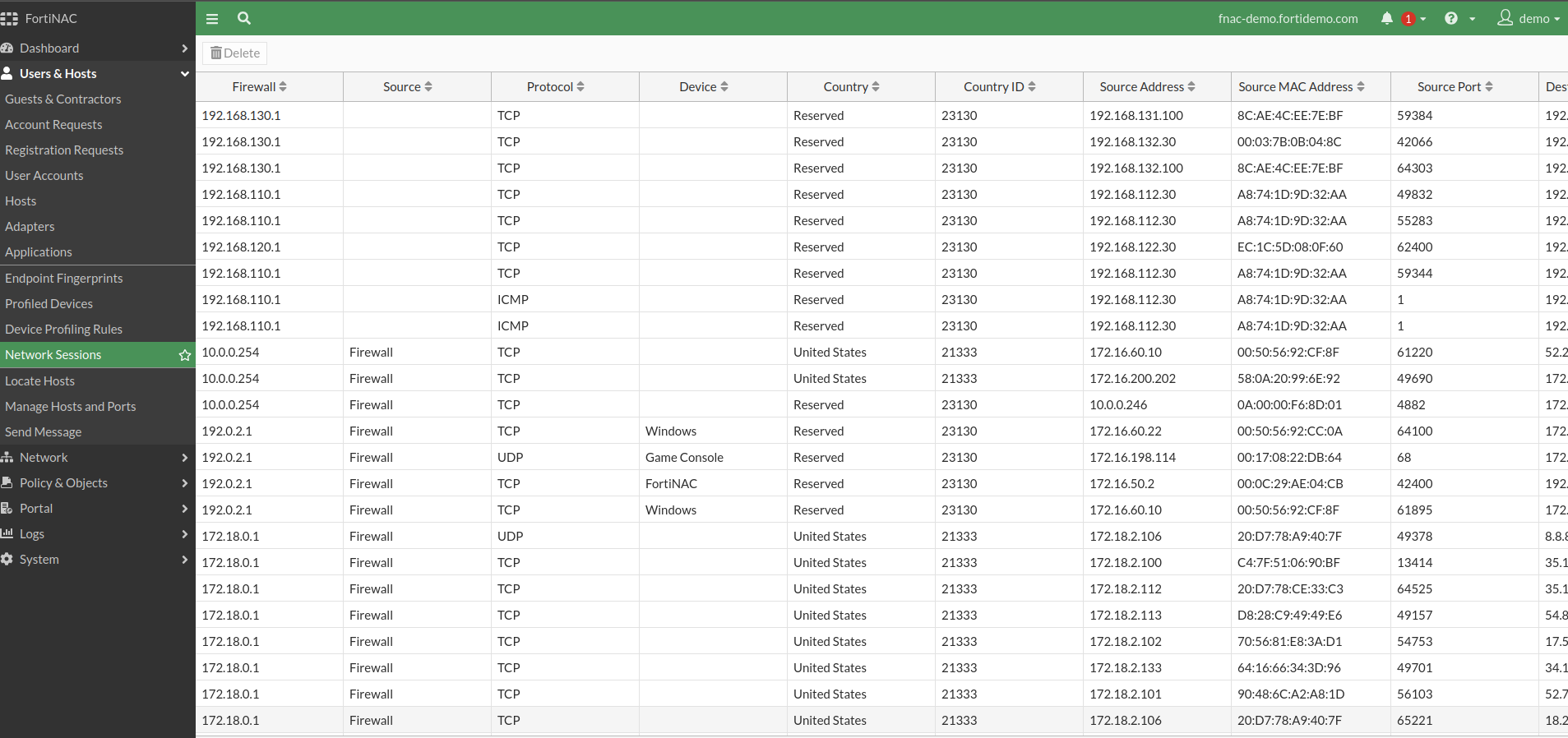
* **Applications:** Ağdaki cihazlar üzerinde çalışan uygulamalarla ilgili algılanan bilgileri veya FortiNAC'in kontrol edebileceği uygulama tabanlı politikaları içerebilir.
* **Endpoint Fingerprints:** Ağdaki uç noktaların (cihazların) otomatik olarak tespit edilen ve sınıflandırılan parmak izi bilgilerinin gösterildiği yerdir. FortiNAC, cihaz türünü (mobil, masaüstü, yazıcı), işletim sistemini, üreticisini vb. bu parmak izi bilgileriyle belirler.



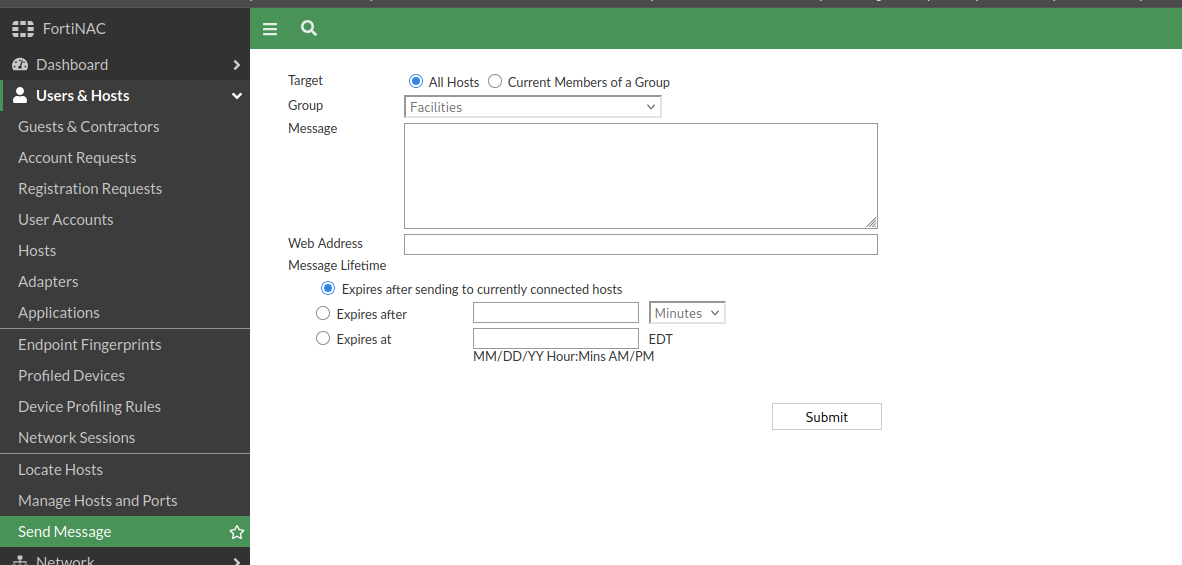
* **Profiled Devices:** Parmak izi çıkarma işlemiyle profil oluşturulmuş cihazların listesidir. Bu cihazlar genellikle belirli bir kategoriye (örneğin, "Windows Bilgisayar", "iPhone", "Güvenlik Kamerası") atanır ve bu profillere göre erişim politikaları uygulanır.
* **Device Profiling Rules:** FortiNAC'in cihazları nasıl profilleyeceğini (sınıflandıracağını) belirleyen kuralların yapılandırıldığı yerdir. Belirli MAC adresleri, DHCP seçenekleri veya diğer ağ özelliklerine göre özel profil kuralları oluşturulabilir.



* **Network Sessions:** Ağdaki aktif kullanıcı ve cihaz oturumlarının gerçek zamanlı olarak izlendiği bölümdür. Kimin, nerede, ne zaman ve ne kadar süreyle ağa bağlı olduğunu gösterir.

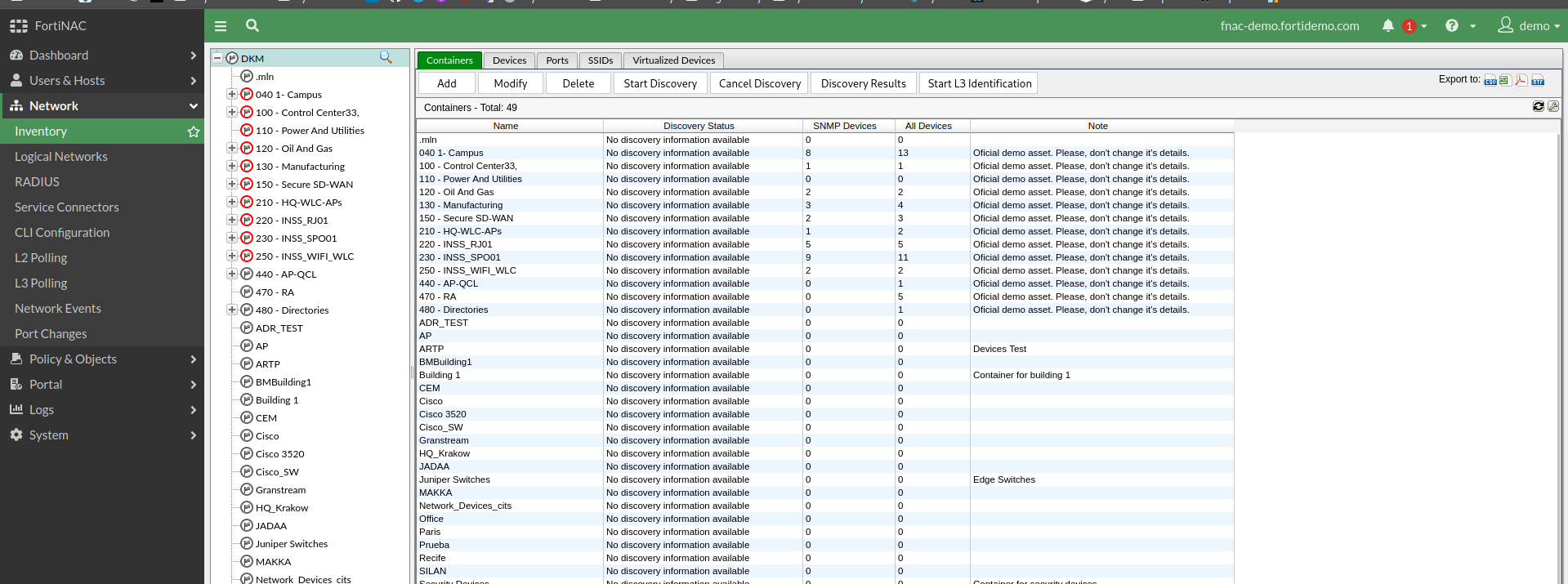


* **Locate Hosts:** Ağdaki belirli bir cihazı (ana bilgisayarı) bulmaya yardımcı olan bir araçtır. Genellikle MAC veya IP adresini kullanarak cihazın hangi anahtara veya AP'ye bağlı olduğunu belirler.
* **Manage Hosts and Ports:** Ağdaki cihazları ve bunların bağlı olduğu ağ cihazı portlarını yönetmek için kullanılır. Örneğin, bir portu devre dışı bırakma, VLAN ataması yapma veya bir cihazı karantinaya alma gibi işlemler buradan yapılabilir.
* **Send Message:** FortiNAC ajanının yüklü olduğu cihazlara veya belirli kullanıcılara mesaj gönderme özelliğidir. Genellikle bir güvenlik uyarısı veya talimat iletmek için kullanılır.

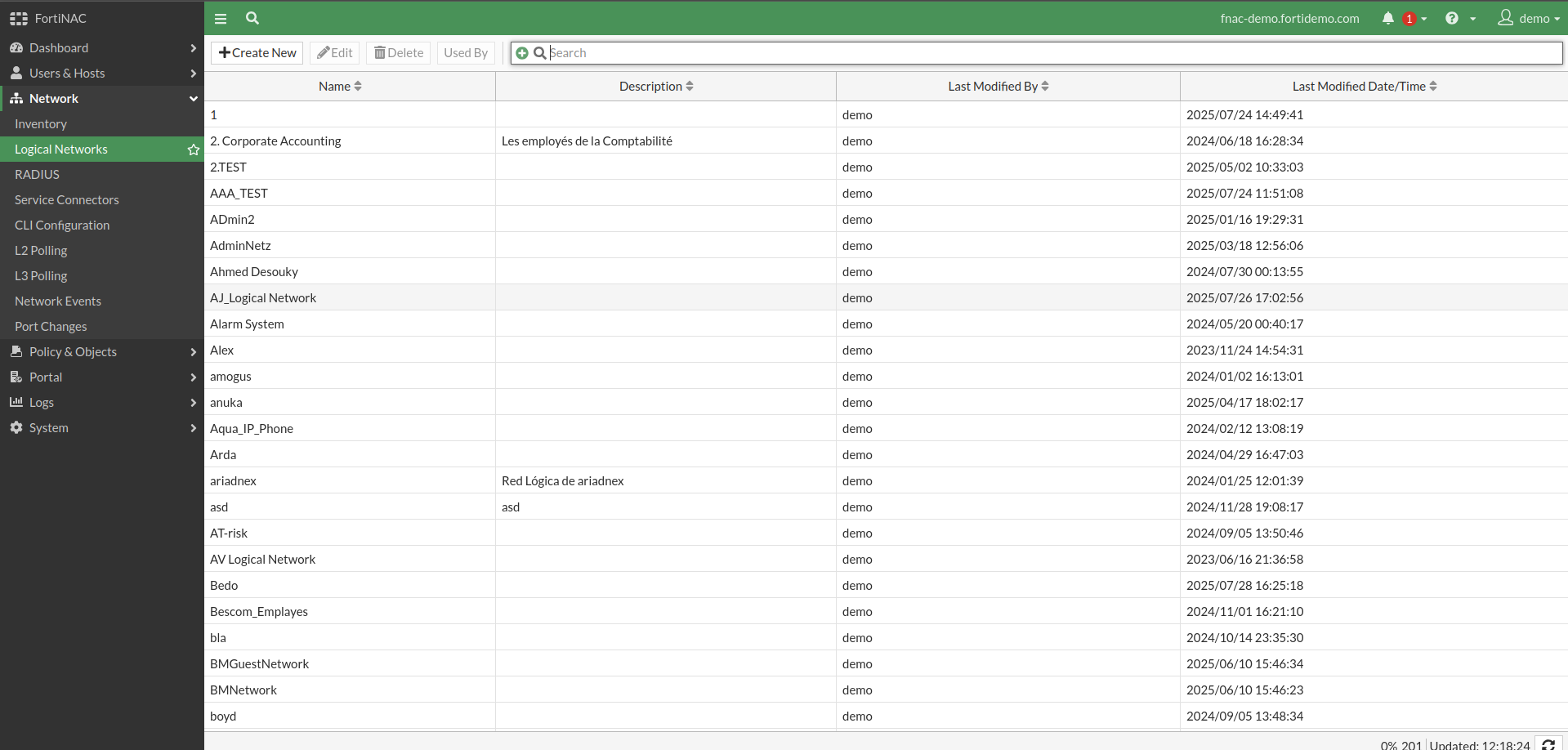


**Network**

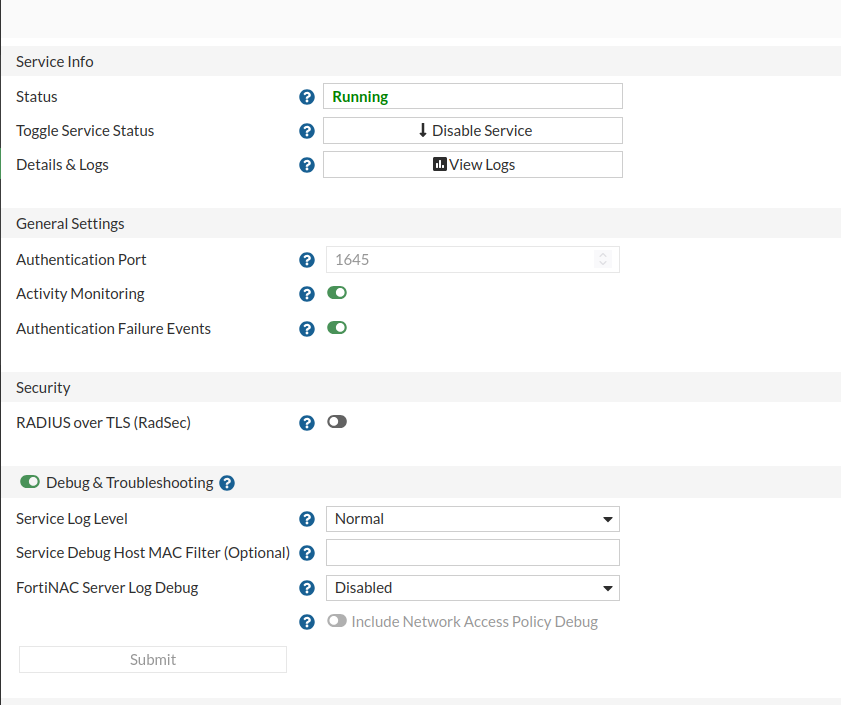
* **Inventory**: FortiNAC'in ağınızda keşfettiği ve yönettiği tüm ağ cihazlarının (anahtarlar, yönlendiriciler, kablosuz erişim noktaları vb.) bir listesidir. Bu envanter, cihazların modelini, üreticisini, IP adresini ve FortiNAC ile entegrasyon durumunu içerir.



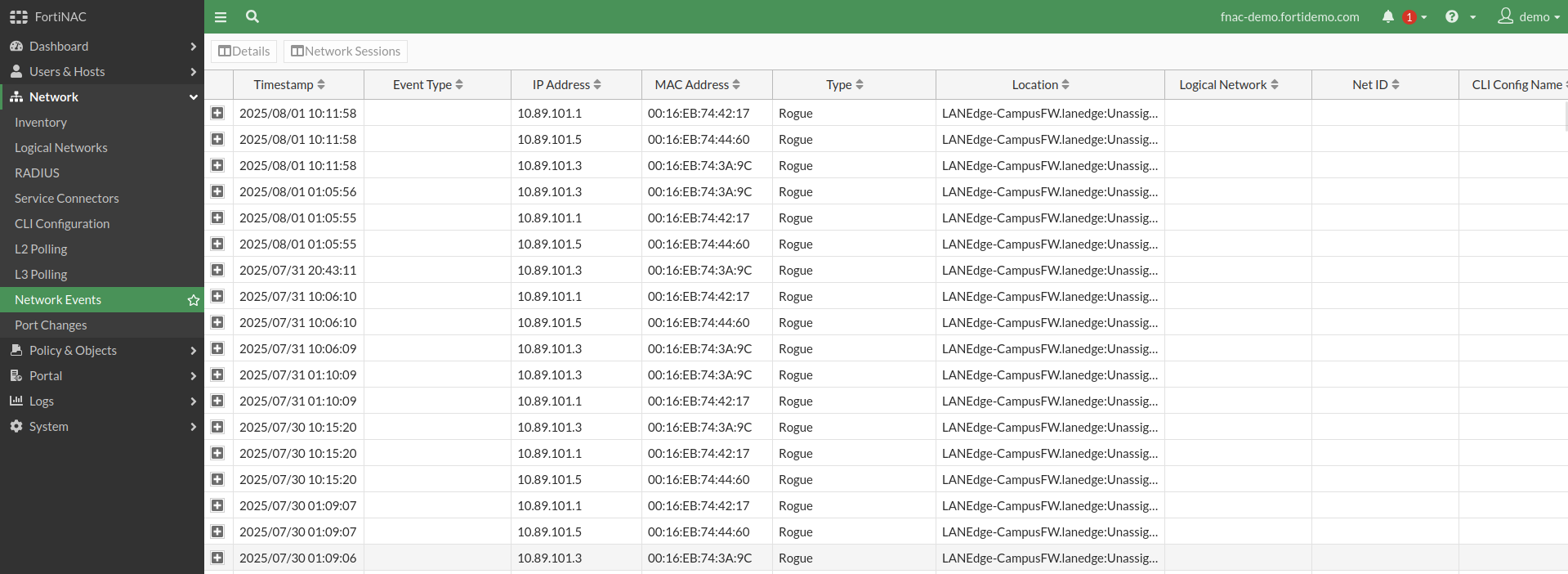
* **Logical** **Networks**: Ağınızdaki farklı mantıksal ağ segmentlerinin (örneğin, VLAN'lar, alt ağlar) tanımlandığı yerdir. FortiNAC, bu mantıksal ağları kullanarak cihazlara ve kullanıcılara farklı erişim politikaları uygulayabilir.



* **RADIUS:** RADIUS (Remote Authentication Dial-In User Service), ağ erişimi için merkezi kimlik doğrulama, yetkilendirme ve muhasebe (AAA) hizmeti sağlayan bir protokoldür. Bu bölümde FortiNAC'in RADIUS sunucusu olarak nasıl davranacağı veya harici RADIUS sunucularıyla nasıl entegre olacağı yapılandırılır. Ağ cihazları (anahtarlar, AP'ler) kimlik doğrulama isteklerini FortiNAC'e RADIUS üzerinden gönderir.



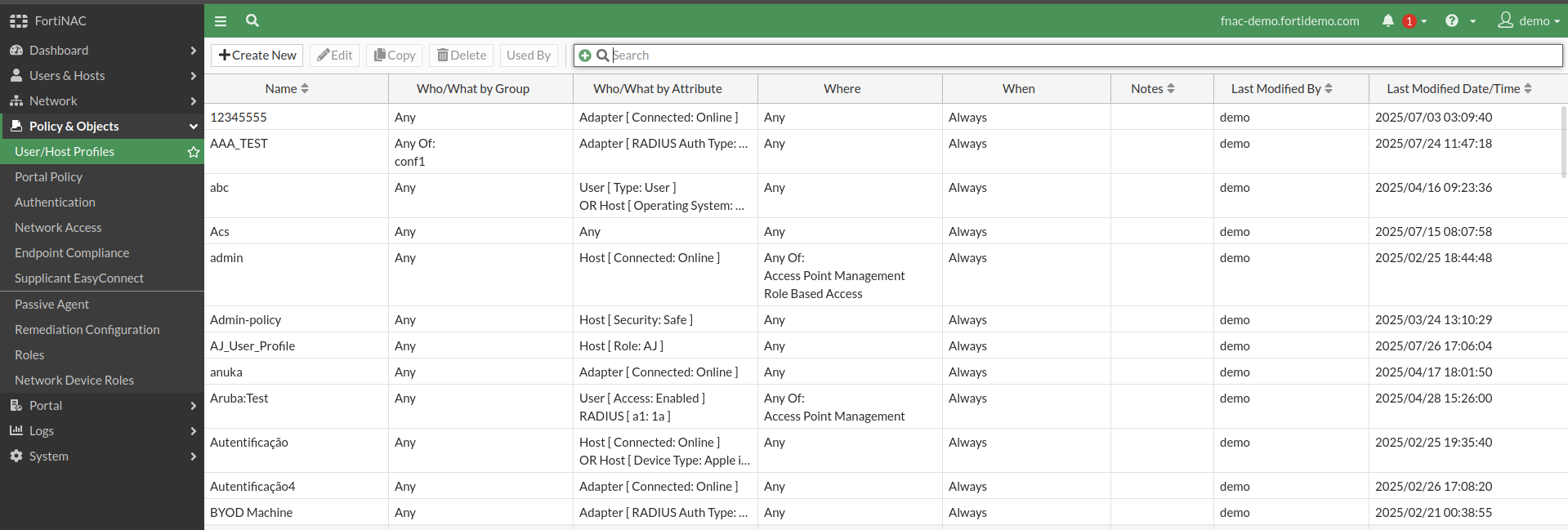
* **Service Connectors:** FortiNAC'in diğer güvenlik veya ağ servisleriyle (örneğin, güvenlik duvarları, SIEM sistemleri, MDM çözümleri) entegrasyonunu sağlayan bağlantı noktalarının yapılandırıldığı yerdir. Bu entegrasyonlar, FortiNAC'in ağ genelinde daha geniş bir görünürlük ve otomasyon sağlamasına olanak tanır.
* **CLI Configuration:** FortiNAC'in kontrol ettiği ağ cihazlarının (anahtarlar gibi) komut satırı arayüzü (CLI) aracılığıyla yapılandırılmasını sağlayan ayarları içerir. FortiNAC, otomatik olarak portları etkinleştirmek/devre dışı bırakmak veya VLAN atamaları yapmak gibi işlemleri CLI komutları göndererek gerçekleştirebilir.
* **L2 Polling:** Katman 2 (Layer 2) seviyesinde ağ cihazlarının (anahtarların) sorgulanması ve izlenmesiyle ilgilidir. FortiNAC, bağlı cihazların MAC adreslerini, port durumlarını ve diğer Layer 2 bilgilerini toplamak için düzenli olarak anahtarları sorgular. Bu, cihazların ağdaki fiziksel konumunu belirlemeye yardımcı olur.
* **L3 Polling:** Katman 3 (Layer 3) seviyesinde ağ cihazlarının (yönlendiricilerin) sorgulanması ve izlenmesiyle ilgilidir. FortiNAC, IP adresi bilgilerini, rotalama tablolarını ve diğer Layer 3 detaylarını toplamak için yönlendiricileri sorgular. Bu, ağdaki mantıksal yapıyı ve cihazların IP adresleme durumunu anlamaya yardımcı olur.
* **Network Events:** Ağda meydana gelen önemli olayların (örneğin, cihaz bağlantıları/bağlantı kesilmeleri, port durumu değişiklikleri, kimlik doğrulama hataları) listesidir. Bu olay günlükleri, ağdaki aktiviteleri izlemek ve sorun gidermek için kritiktir.



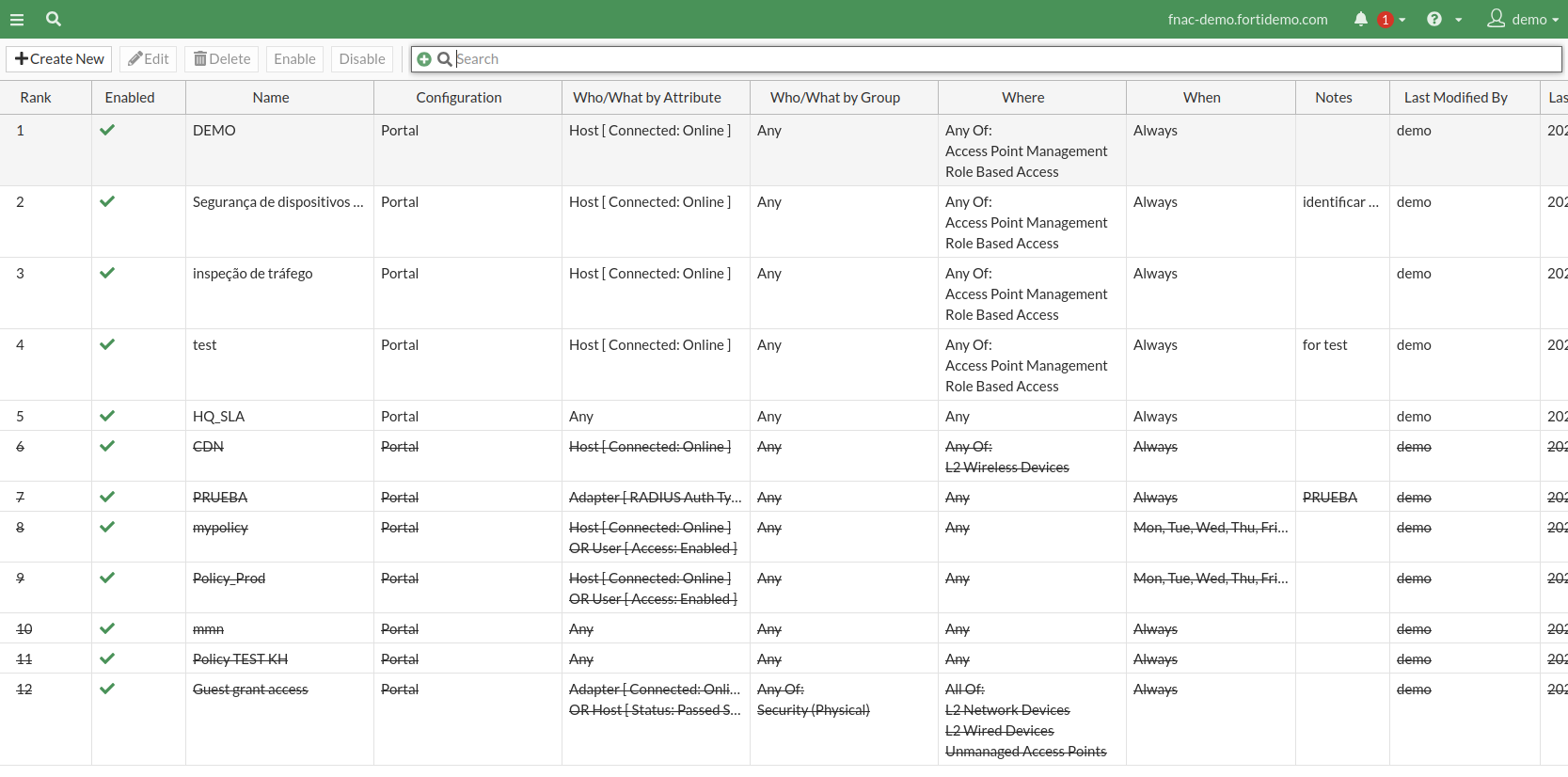
* **Port Changes**: Ağ cihazlarının portlarında meydana gelen değişikliklerin (örneğin, bir cihazın bir porta bağlanması veya bağlantısının kesilmesi, portun durumunun değişmesi) takip edildiği yerdir. Bu, yetkisiz bağlantıları veya fiziksel güvenlik ihlallerini tespit etmeye yardımcı olabilir.

**Policy & Objects**

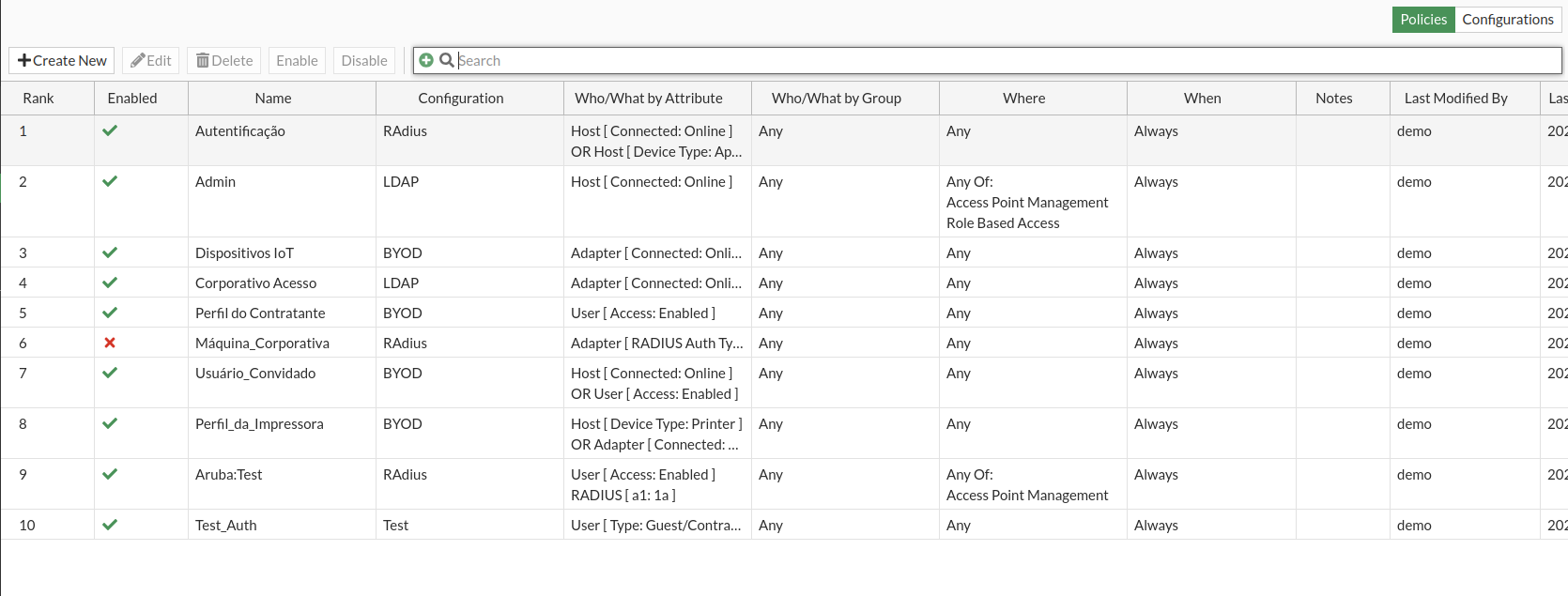
* **User/Host Profiles:** Ağdaki kullanıcıların ve cihazların (ana bilgisayarların) profillerinin tanımlandığı yerdir. Bu profiller, bir kullanıcının veya cihazın ağdaki kimlik doğrulaması ve güvenlik duruşuna göre sahip olacağı özellikleri ve erişim haklarını belirler. Örneğin, "Uygun Şirket Dizüstü Bilgisayarı" veya "Misafir Akıllı Telefonu" gibi profiller oluşturulabilir.



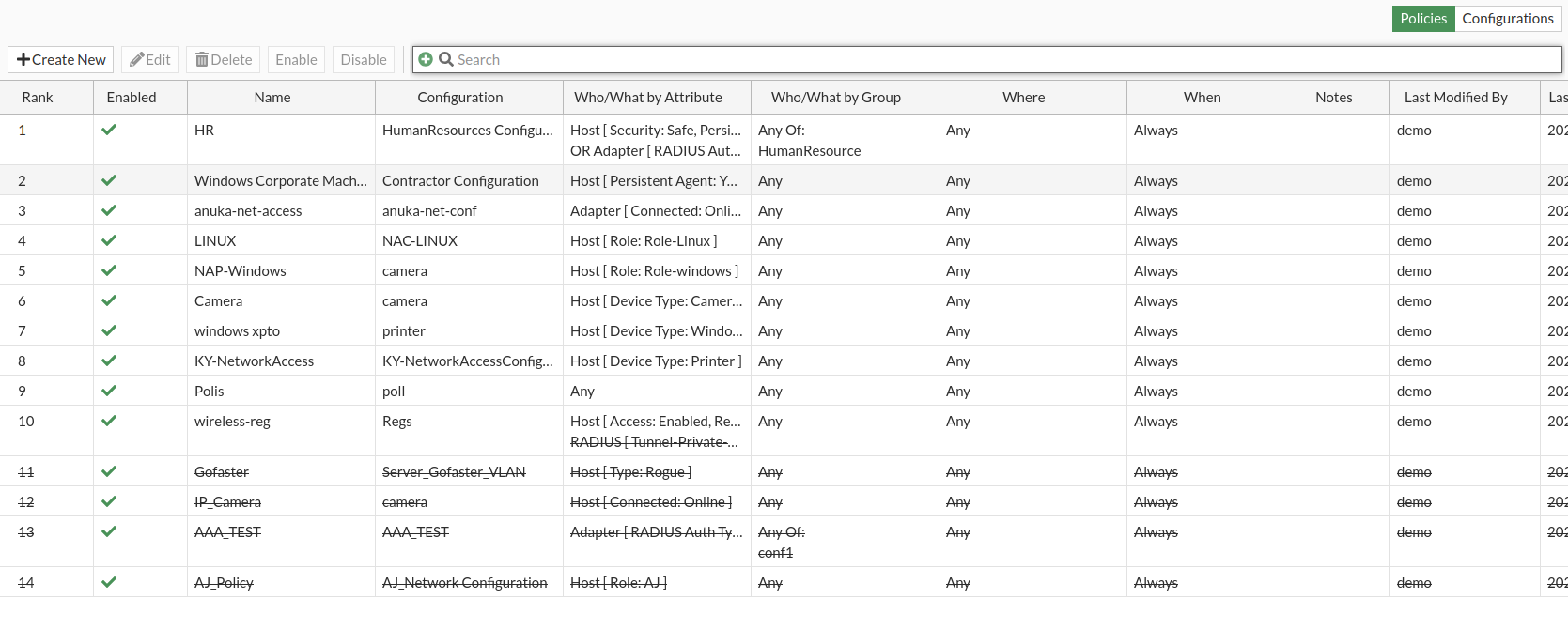
* **Portal Policy:** Ağ erişimi için kullanılan web tabanlı portalların (Captive Portal) ve bu portallar aracılığıyla uygulanan politikaların yapılandırıldığı bölümdür. Misafir kaydı, kendiliğinden kayıt veya belirli bir ağa erişmeden önce kabul edilmesi gereken kullanım koşulları gibi senaryolar için kullanılır.



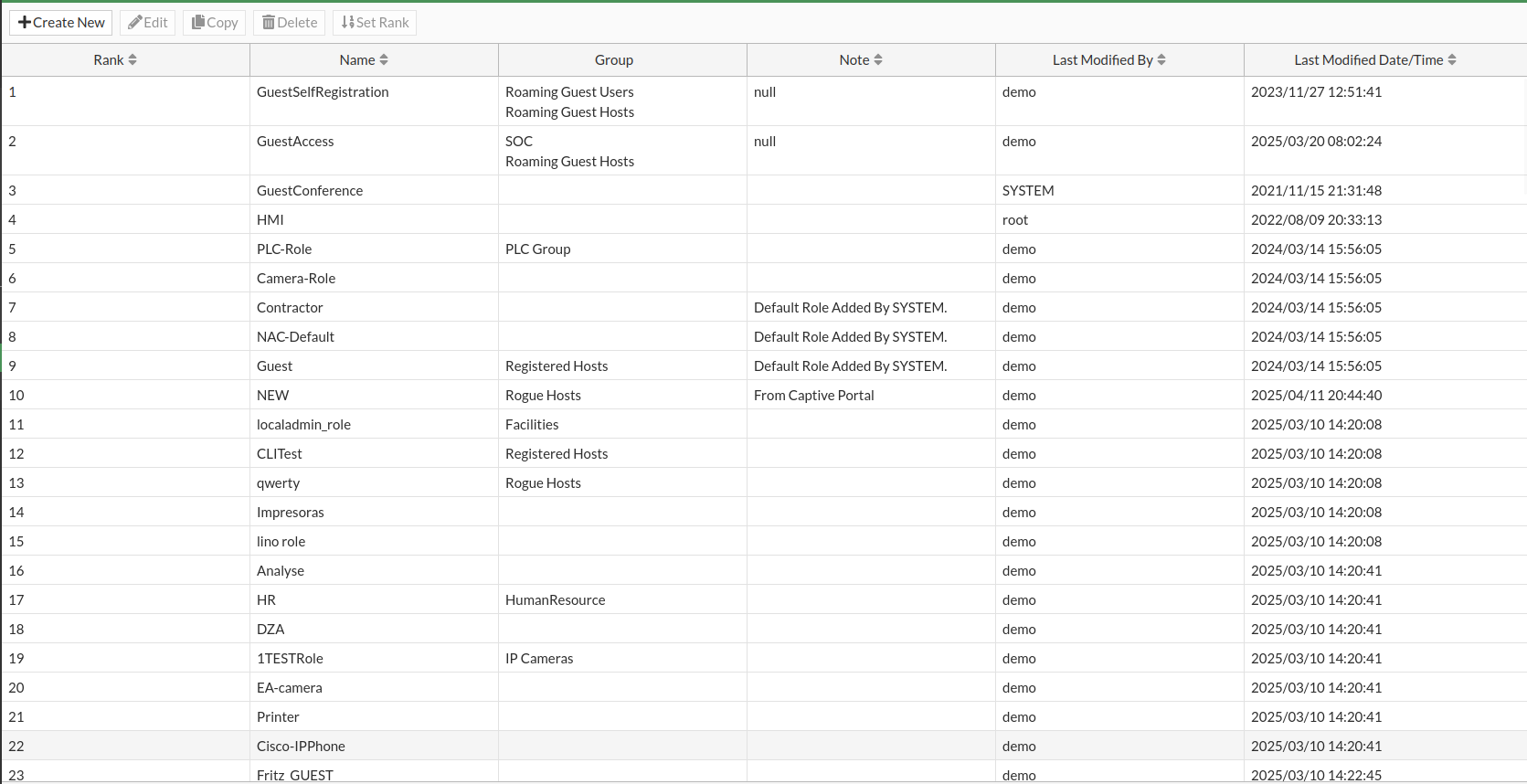
* **Authentication:** Kullanıcıların ve cihazların ağa bağlanırken kimliklerinin nasıl doğrulanacağını belirleyen ayarları içerir. RADIUS, LDAP, Active Directory entegrasyonları, yerel veritabanı gibi kimlik doğrulama yöntemleri ve bu yöntemlerin sırası burada yapılandırılır.



* **Network Access:** Cihazların ve kullanıcıların ağa nasıl erişeceğini kontrol eden politikaların tanımlandığı yerdir. Bu politikalar, kimlik doğrulama başarılı olduktan sonra hangi VLAN'a atanacaklarını, hangi güvenlik katmanlarından geçeceklerini ve hangi ağ kaynaklarına erişebileceklerini belirler.



* **Endpoint Compliance:** Uç noktaların (cihazların) ağa bağlanmadan önce belirli güvenlik gereksinimlerini (uyumluluk) karşılayıp karşılamadığını denetleyen politikaların oluşturulduğu yerdir. Örneğin, işletim sistemi yamalarının güncel olması, antivirüs yazılımının etkin olması veya belirli yazılımların yüklü olmaması gibi kurallar tanımlanabilir. Uyumsuz cihazlara ne yapılacağı (karantinaya alma, erişimi kısıtlama vb.) burada belirlenir.
* **Supplicant EasyConnect**: 802.1X gibi gelişmiş kimlik doğrulama yöntemlerini kullanırken istemci cihazların (supplicant) kolayca ağa bağlanmasını sağlamak için özel ayarları veya araçları içerir. Bu, karmaşık istemci konfigürasyonlarını basitleştirmeye yardımcı olabilir.
* **Passive Agent:** Ağdaki cihazlardan pasif olarak (herhangi bir yazılım yüklemeden) bilgi toplamak için kullanılan ajanların veya yöntemlerin yapılandırıldığı bölümdür. Bu, cihaz profilleme ve envanter oluşturma için kullanılır.
* **Remediation Configuration:** Bir cihazın uyumsuz veya güvenli olmadığı tespit edildiğinde, bu durumu düzeltmek için ne tür eylemlerin gerçekleştirileceğini (remediation) belirleyen ayarların yapıldığı yerdir. Örneğin, bir yama sunucusuna yönlendirme, uyarı mesajı gösterme veya belirli bir karantina ağına atama gibi eylemler tanımlanır.
* **Roles:** Ağdaki kullanıcılara ve cihazlara atanabilecek rolleri tanımladığınız yerdir. Her rol (örneğin, "Çalışan", "Misafir", "Yönetici", "IoT Cihazı") belirli erişim hakları, güvenlik profilleri ve ağ davranışları ile ilişkilendirilir. Politikalar bu rollere göre uygulanır.



* **Network Device Roles:** Ağ altyapı cihazlarının (anahtarlar, yönlendiriciler) FortiNAC içinde sahip olacakları rolleri ve bu rollere özgü konfigürasyonları belirler. Bu, FortiNAC'in farklı ağ cihazı türleriyle entegrasyonunu ve yönetimini sağlar.