

# System Management

Systems Management  Search

User: uatugay@hotmail.com (Upgrade) Security Level: administrator Log Out

ACCOUNT SITES COMPONENTS COMSTORE SCHEDULED JOBS SCHEDULED REPORTS HELP SETUP

Menü	Açıklama
Account	Hesap seviyesine erişim.
Sites	Site düzeyine erişim.
Components	Yönetici tarafından indirilen ve erişilebilir bileşenlere erişim.
Comstore	Panda Systems Management'ın yeteneklerini genişleten Panda Security tarafından oluşturulan bileşenlerin depolanması.
Scheduled Jobs	Aktif ve bitmiş işler listesi.
Scheduled Reports	Yapılandırılmış ve varsayılan raporların listesi.
Help	Panda Güvenlik kaynaklarına bağlantı sağlayan yardım merkezi.
Setup	Ana yönetim hesabının ayrıntılarına ve yeni güvenlik düzeyleri ve kullanıcıları oluşturmaya yönelik kaynaklara erişim.

## Tab bar / List bar (Sekme Çubuğu / Liste Çubuğu)

Site: Home

SUMMARY DEVICES AUDIT MANAGE MONITOR SUPPORT REPORT POLICIES SETTINGS

**Devices**

Total: 2  
Online: 2  
Offline: 0  
Offline > 1 Week: 0

**Security**

Anti-Virus: 100%  
Firewall: 100%  
MS Updates: 100%  
Patch Mgt: 3

**Energy Usage**

Previous Month: 60hrs  
Previous Cost: 2,56 €  
Current Month: 205hrs  
Current Cost: 8,61 €

**Security Status**

Security Status is displayed for Windows devices in your Environment. It does not include Servers as they do not report Security Center information, or Anti-Spyware Status for Windows XP Devices.

**Anti-Spyware Summary**

At least one active and updated product: 2 Devices  
At least one active but not up-to-date product: 0 Devices  
No active product: 0 Devices

**Anti-Virus Summary**

At least one active and updated product: 2 Devices  
At least one active but not up-to-date product: 0 Devices  
No active product: 0 Devices

**Firewall Summary**

At least one active product: 2 Devices  
Not applicable: 0 Devices  
No active product: 0 Devices

Product Name	Status
Windows Defender	1 0 1
Panda Endpoint Protection	1 0 0

Product Name	Status
Windows Defender	1 0 1
Panda Endpoint Protection	1 0 0

Product Name	Status
Windows Firewall	2 0

Sekme çubuğu konsolda bulunan listelerin üretilmesi ve sunulması için konsoldaki mevcut araçlara erişim sağlar ve erişilen seviyeye ait cihazların durumu ile ilgili ayrıntılar sağlar. Ayrıca yapılandırmaların tanımlanmasını ve görüntülenmesini sağlar.

## Bileşenler

Menü	Açıklama
Summary	Durum Bilgisi
Devices	İlgili bilgilerle erişilebilen cihazların listesi
Audit	Donanım, yazılım ve lisans denetim listesi
Manage	Uygulanan ve bekleyen yamalar, cihazlarda yüklü yazılımların yanı sıra ağda bulunan ve Hesap Yönetimi tarafından yönetilen cihazların listesi
Monitor	Monitörler veya bitmiş işler tarafından oluşturulan uyarılar listesi
Support	Biletlerin listesi oluşturuldu
Report	Talep üzerine raporların listesi ve üretimi
Policies	Daha sonra açıklanacak politikaların listesi ve oluşturulması.
Settings	Siteyle ilişkili yapılandırma

## Simge çubuğu / Eylem çubuğu (Icon bar / Action bar)

Simge çubuğu veya Eylem çubuğu, cihazların durumunu değiştirmek için eylemlere erişir. Bu çubuk, genel menü Hesabında mevcut değildir ve yönetim kapsamı farklı olduğundan, Genel menülerden veya belirli bir cihazdan erişildiğinde biraz değişiklik gösterir. Simge çubuğunun kapsamı, bir sitede seçilen cihazları manuel olarak seçerek oluşturulacaktır.

Site: Home

SUMMARY DEVICES AUDIT MANAGE MONITOR SUPPORT REPORT POLICIES SETTINGS

Showing 1 - 2 of 2 results. Show me 25 per page

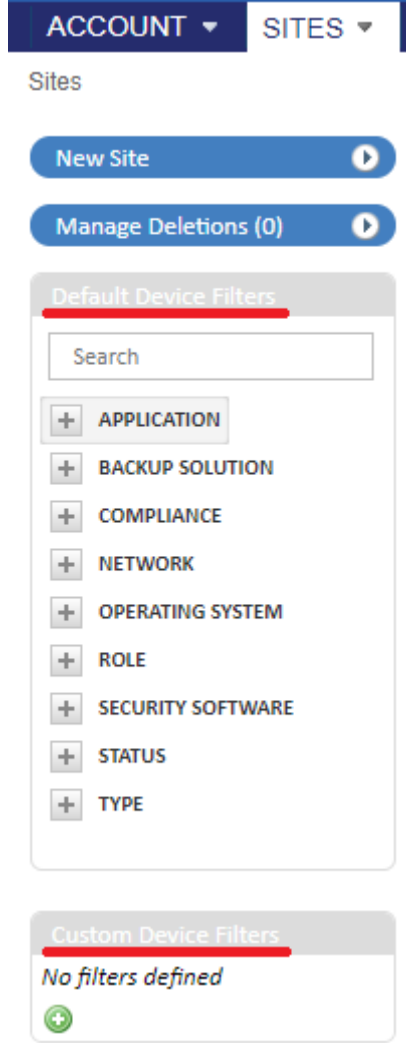
Actions:

All  Desktops  Laptops  Servers  Network  ESXi Host  Unknown

	Hostname	Description	IP Address	Ext IP Addr	Last User	Operating System
<input type="checkbox"/>	DESKTOP-QLJ7RMK	DESKTOP-QLJ7RMK				Microsoft Windows 10 Pro 10.0.17134
<input type="checkbox"/>	ISMAIL	ISMAIL				Microsoft Windows 10 Home Single Language 10.0.17134

<b>Menü</b>	<b>Açıklama</b>
<b>Move Device to</b>	Seçilen cihazları başka bir siteye taşıyın.
<b>Add Device to</b>	Seçilen cihazları bir gruba taşıyın.
<b>Edit</b>	Filtreler tarafından kullanılabilir seçili cihazlara notlar ve özel alanlar ekleyin.
<b>Toggle</b>	Özet / Gösterge Tablosundan hızlı erişim için cihazları favori olarak işaretleyin.
<b>Delete</b>	Bir siteden bir cihazı siler. Cihaz artık yönetilmeyecek, Aracı kaldırılacak ve cihaz, genel menü Hesabı altındaki Askıya Alınmış cihazlar sekmesine eklenecektir.
<b>Request audit</b>	Bir denetimin başlatılmasını zorlayın.
<b>Schedule Job</b>	Daha sonraki bir tarih için planlanmış bir iş oluşturun.
<b>Run a Quick Job</b>	Önceden oluşturulmuş bir işi oluşturun ve çalıştırın.
<b>Add/Remove Cache</b>	Ağ cihazlarına yazılım dağıtımının yanı sıra bileşen indirme ve kurulumunu hızlandırmak için cihazı ağ önbelleği olarak işaretleyin.
<b>Network node settings</b>	Bir cihazı bir Ağ Düğümü olarak atayın ve bunu Panda Systems Management'ı dağıtmak ve sunucuyla daha kolay iletişim kurmak için kullanın.
<b>Turn Privacy On</b>	Kullanıcı tarafından onaylanmadığı sürece, yönetici tarafından cihazlara uzaktan erişimi engelle
<b>Send a message</b>	Seçilen cihazlara mesaj gönder
<b>Schedule Reports</b>	Daha sonraki bir tarih için program raporları
<b>Refresh</b>	Ekrandaki verileri yenileyin

## Filtreler ve gruplar paneli (Filters and groups panel)



- **Cihaz filtreleri:** Cihazların yerini tespit etmek için önceden yapılandırılmış filtreler.
- **Site Cihazı Filtreleri / Özel Cihaz Filtreleri:** tarafından oluşturulan cihaz filtreleri Sırasıyla Site Düzeyinde veya Hesap Düzeyinde yönetici.
- **Site cihazı grupları / Özel cihaz grupları:** tarafından oluşturulan cihaz grupları Sırasıyla Site Düzeyinde veya Hesap Düzeyinde yönetici.
- **Site grupları:** Yalnızca Hesap Düzeyinde kullanılabilir, bunlar çeşitli sitelerin gruplarıdır.

## Gösterge Tabloları(Dashboard)

- Güvenlik Durumu
- Hesap Gösterge Tablosu
- Özet (Site)
- Özet (Cihaz)

## Güvenlik Durumu

Genel menüden erişilebilen Hesap, tüm yönetilen cihazların güvenlik durumunu yansıtır.

Anti-Spyware Summary	Anti-Virus Summary	Firewall Summary	
<p>✓ At least one active and updated product 2 Devices</p> <p>⚠ At least one active but not up-to-date product 0 Devices</p> <p>✗ No active product 0 Devices</p>	<p>✓ At least one active and updated product 2 Devices</p> <p>⚠ At least one active but not up-to-date product 0 Devices</p> <p>✗ No active product 0 Devices</p>	<p>✓ At least one active product 2 Devices</p> <p>⚠ Not applicable 0 Devices</p> <p>✗ No active product 0 Devices</p>	
Product Name	Status	Product Name	Status
Windows Defender	✓ 1 ⚠ 0 ✗ 1	Windows Defender	✓ 1 ⚠ 0 ✗ 1
Panda Endpoint Protection	✓ 1 ⚠ 0 ✗ 0	Panda Endpoint Protection	✓ 1 ⚠ 0 ✗ 0

Product Name	Status
Windows Firewall	✓ 2 ✗ 0

## Hesap Gösterge Tablosu

Hesap, Gösterge Panosu'nu tıklayarak genel menü Hesabından erişilebilir.

Tüm cihazların durumu hakkında genel bilgiler toplar: bildirimler, işler, uyarılar vb.

DASHBOARD	AUDIT	MANAGE	MONITOR	SUPPORT	REPORT	POLICIES	SUSPENDED DEVICES	
<b>Devices</b>	<b>Notifications</b>						<b>Active Jobs</b>	
Total 2	There are currently no unresolved alerts.						Devices scheduled 0	
Online 1							Devices running 0	
Offline for 7+ days 0							Devices with warnings 0	
							Devices with failures 0	
<b>Components</b>							<b>Open Alerts</b>	
Total 3							Priority 1 0	
ComStore 166							Priority 2 0	
Updates 1							Priority 3 0	
							Priority 4 0	
							Priority 5 0	

## Özet (Site)

Genel menü Siteleri'nden erişilebilir ve belirli bir site seçilebilir. Seçilen siteye ait tüm cihazların durumunu yansıtır. Oluşturulan her site için bir özet gösterge panosu olacak.

Site: Home

SUMMARY DEVICES AUDIT MANAGE MONITOR SUPPORT REPORT POLICIES SETTINGS

**Devices**

Total: 2  
Online: 1  
Offline: 1  
Offline > 1 Week: 0

**Security**

Anti-Virus: 100%  
Firewall: 100%  
MS Updates: 100%  
Patch Mgt: 3

**Energy Usage**

Previous Month: 60hrs  
Previous Cost: 2,56 €  
Current Month: 226hrs  
Current Cost: 9,49 €

**Security Status**

Security Status is displayed for Windows devices in your Environment. It does not include Servers as they do not report Security Center information, or Anti-Spyware Status for Windows XP Devices.

**Anti-Spyware Summary**

At least one active and updated product: 2 Devices  
At least one active but not up-to-date product: 0 Devices  
No active product: 0 Devices

**Anti-Virus Summary**

At least one active and updated product: 2 Devices  
At least one active but not up-to-date product: 0 Devices  
No active product: 0 Devices

**Firewall Summary**

At least one active product: 2 Devices  
Not applicable: 0 Devices  
No active product: 0 Devices

Product Name	Status
Windows Defender	✓ 1 ⚠ 0 ✗ 1
Panda Endpoint Protection	✓ 1 ⚠ 0 ✗ 0

Product Name	Status
Windows Defender	✓ 1 ⚠ 0 ✗ 1
Panda Endpoint Protection	✓ 1 ⚠ 0 ✗ 0

Product Name	Status
Windows Firewall	✓ 2 ✗ 0

## Özet (Cihaz)

Bir cihazdan erişilebilir. Belirli bir cihazın durumunu yansıtır. Her yönetilen cihaz için bir tane var.

Device: DESKTOP-QLJ7RMK

SUMMARY AUDIT MANAGE MONITOR SUPPORT REPORT POLICIES

Description: DESKTOP-QLJ7RMK  
Power Rating: 350 Watts

Groups: Version: 4.4.2017.2017

Actions: [Icons]

**System**

Hostname: DESKTOP-QLJ7RMK  
Network Node: Localhost  
ID: d6befed2-39cb-c318-81b3-4dc05e158c02  
Device Type: Laptop  
Domain: WORKGROUP  
Last User: DESKTOP-QLJ7RMK  
Status: Offline  
Last Seen: 2018-07-17 18:23:00 UTC  
Last Reboot: 2018-07-17 18:13:04 UTC  
Last Audit Date: 2018-07-17 08:46:25 UTC  
Create Date: 2018-06-26 12:31:07 UTC  
Int IP Address: 192.168.0.16  
Ext IP Address: 46.2.241.171  
Additional IP(s): 10.0.0.100  
SNMP Credentials: [Edit]  
Manufacturer: TOSHIBA  
Model: SATELLITE L50-A-1D1  
Operating System: Microsoft Windows 10 Pro 10.0.17134  
Service Pack: 0  
Architecture: 64-Bit  
Serial Number: XD0818275

Type	Product	Status
Anti-Virus	Panda Endpoint Protection	✓
Anti-Virus	Windows Defender	✗
Anti-Spyware	Panda Endpoint Protection	✓
Anti-Spyware	Windows Defender	✗
Updates	Windows Updates	✓

NOTE: You need an agent installed on your local device to use RDP or VNC.

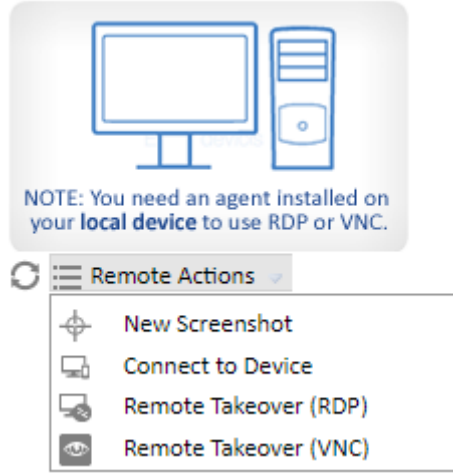
## Cihazları Yönetme (Managing Devices)

Panda Systems Management, PCSM Agent ile uyumlu olup olmadıklarına bağlı olarak, ürün tarafından yönetilen cihazlara erişmek için farklı araçlar sunar.

PCSM Agent ile uyumlu cihazlar

- Genel menüyü tıklayın. Siteler, cihazın ait olduğu siteyi seçin ve yönetmek için cihazı tıklayın.

- Özet sekmesi, cihaza erişebileceğiniz farklı simgeleri gösterir.



<b>Refresh</b>	Cihazın masaüstünün yeni bir ekran görüntüsünü alır ve ekranda gösterir
<b>New Screenshot</b>	Cihazın masaüstünün ekran görüntüsünü indirmenizi sağlar
<b>Connect to device</b>	Yerel aracı seçilen cihaza bağlar
<b>Remote takeover (RDP)</b>	Cihazın uzak masaüstüne RDP üzerinden bağlanır
<b>Remote takeover (VNC)</b>	VNC aracılığıyla cihazın uzak masaüstüne bağlanır

## Cihaz Bilgilerini Görüntüleme

Her cihazdan toplanan bilgiler, ilgili cihazla ilişkili Cihaz Düzeyinde mevcuttur. Erişmek için Genel menüler menüsüne gidin, cihazın ait olduğu siteyi seçin, Cihazlar sekmesini ve ardından görüntüleyeceğiniz cihazı tıklayın. Aşağıdaki genel bilgiler görüntülenir.

Görüntülenen bilgiler beş kategoriye ayrılmıştır:

- Genel cihaz bilgisi
- Sistem bilgisi
- Yönetici notları
- Etkinlik bilgisi
- Performans bilgileri

## Yönetici Notları

Burada yöneticiler, diğer yöneticilerle işbirliğini sağlamak için cihazla ilgili tekrarlanan sorunların çözümüne yönelik prosedürlerin yanı sıra hatırlatıcılar ve yorumlar da ekleyebilir.

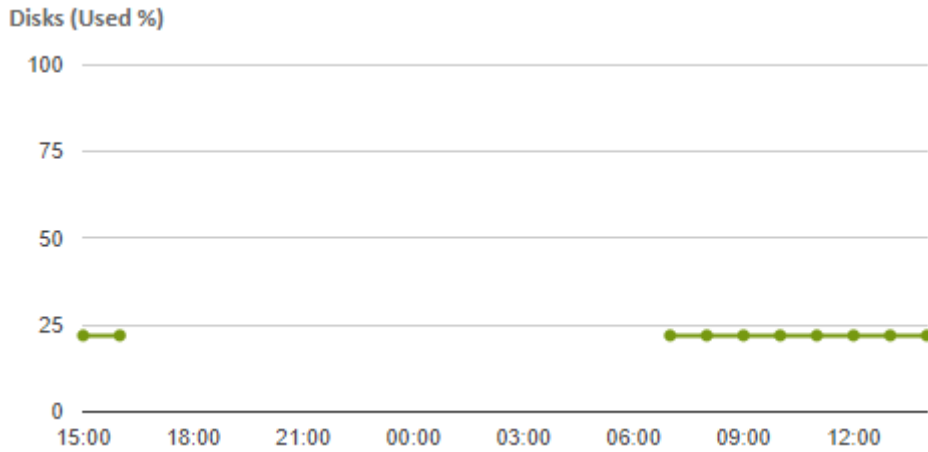
## Etkinlik günlüğü

Cihazda gerçekleştirilen eylemleri görüntüler. Bu, Etkinlik sekmesini seçerek Raporlar sekmesinde görüntülenen bilgilerin bir özetidir. Bu ekrana, listenin en altındaki **more...** bağlantısını tıklayarak doğrudan ulaşabilirsiniz.

## Performans

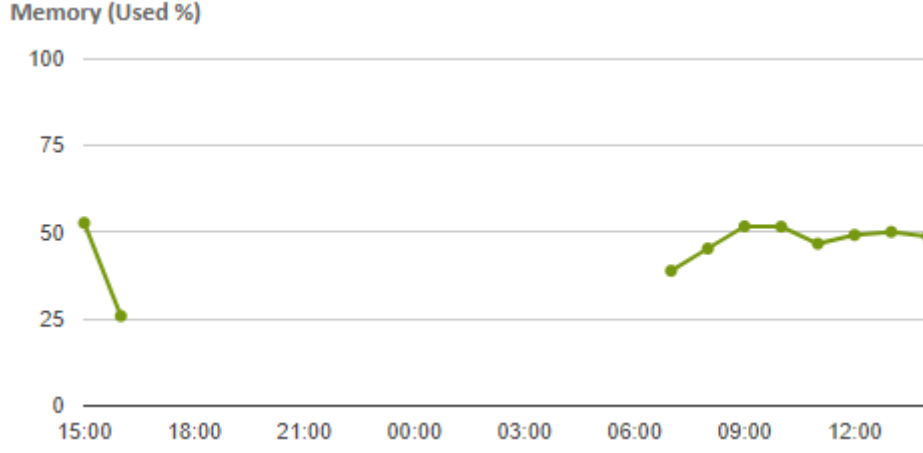
Konsol, CPU, bellek ve sabit diskin kullanımını gösteren üç çizgi grafik görüntüler. Ayrıca cihazın çalıştığı zamanı gösterir.

## Disk kullanımı (cihazdaki her disk için bir satır)





## Hafıza kullanımı



## CPU kullanımı



## Cihazın açıldığı toplam süre (mevcut günde)

Uptime

Today

**8h15m**

## Ölçek

Grafiklerde görüntülenen zaman dilimini tanımlamanızı sağlar:

- 24 saat
- 1 hafta
- 1 ay

## Cihazın türünü belirtme

Panda Systems Management, tüketim açısından dört ana cihaz grubunu birbirinden ayırır.

- Desktop
- Laptop
- Server
- Network
- ESXi Host
- Unknown

Sistem, yönetilen her bir cihazı en iyi tanımlayan aygıt türünü otomatik olarak atar, ancak bu doğru değilse de, Özet sekmesindeki ilgili Aygıt Düzeyinde değer değiştirilebilir.

## Her cihaz türü için güç derecelendirmesini belirtme

Varsayılan olarak, sistem dizüstü bilgisayarlar, akıllı telefonlar ve sunucular için belirli güç derecelendirmeleri atar. Bunlar tipik donanım konfigürasyonlarına göre hesaplanan ortalama değerlerdir.

- Yönetilen tüm siteler için bu değerler nasıl değiştirilir: Genel menü Kurulum, Hesap Ayarları sekmesi, Güç Derecelendirmesi bölümüne gidin. Her bir cihaz türü için tüketilen watt değerini girin.

- Belirli bir site için bu değerleri nasıl değiştirilir: Seçilen sitenin Ayarlar sekmesini tıklayın.

Elektrik fiyatları ülkeden ülkeye ve hatta bölgelere göre büyük ölçüde değiştiğinden, Kwh başına maliyeti belirtmek de mümkündür.

## Gruplar ve filtreler nelerdir?

Gruplar ve filtreler, aygıt kümelerine benzer şekilde, ancak daha kolay ve dinamik olarak aygıt kümeleri oluşturmak için kaynaklardır. Dolayısıyla, siteler belirli bir müşteri hesabına veya ofise üyelik gibi cihazların statik yönlerini dikkate alırken, gruplar ve filtreler, cihazların geçici özelliklerine veya kriterlerine göre kolayca değiştirilebilecek şekilde tasarlanmıştır.

## Grup ve filtre türleri

Çeşitli gruplar / filtreler vardır:

**Site Cihaz Grupları / Site Cihaz Filtreleri:** Bunlar belirli bir site içinde oluşturulan gruplardır. Sadece seçilen siteye ait cihazları içerebilirler.

**Cihaz Grupları / Özel Cihaz Filtreleri:** Bunlar Hesap Düzeyinde oluşturulan gruplardır. Bir, çeşitli veya tüm sitelere ait cihazlar içerebilirler.

**Site Grupları:** Hesap Düzeyinde düzenlendi, tam site grupları.

## Gruplar

Gruplar statik aygıtların gruplarıdır. Bir aygıt, bir yönetici tarafından doğrudan ayırma yoluyla bir gruba manuel olarak atanır. Tek bir cihaz birden fazla gruba ait olabilir.

## Filtreler

Filtreler dinamik cihaz gruplarıdır. Bir cihaz belirli bir filtreye ait olsun veya olmasın, söz konusu cihaz, söz konusu cihaz için yönetici tarafından belirlenen kriterleri karşıladığında otomatik olarak belirlenir. Bir cihaz birden fazla filtreye ait olabilir.

## Öntanımlı Filtreler

Panda Systems Management, hizmette kayıtlı cihazların organizasyonunu ve yerini basitleştiren bir dizi önceden tanımlanmış filtre içerir.

Öntanımlı filtreler yedi gruba ayrılmıştır:

- **Uygulama:** Bu grup Adobe Flash, Java, Microsoft Office, vb. Uygulamalar için filtreler içerir.
- **Yedekleme Çözümü:** Bu grup Backup Exec, StorageCraft, Veeam gibi yedekleme çözümleri için filtreler içerir.
- **Uyumluluk:** Bunlar, bellek alanı yetersizliği, devre dışı bırakılmış antivirüs, bekleyen yeniden başlatma vb. Nedeniyle yönetici tarafından kontrol edilmesi gereken cihazları gösteren filtrelerdir.
- **İşletim sistemi:** Bu filtreler, cihazları kurdukları işletim sistemine göre görüntüler.
- **Rol:** Bu filtreler sunucuları rollerine göre gösterir.

- **Güvenlik yazılımı:** Bu filtreler, kurulu olan güvenlik çözümüne uygun olarak cihazları görüntüler.
- **Durum:** Bu grup, cihazları durumlarına göre belirler (açık / kapalı, ağ düğümü, vb.).
- **Tip:** Bu filtreler cihazları türlerine göre tanımlar (ESXi sunucuları, akıllı telefonlar, tabletler vb.)

## Cihazları verimli bir şekilde yönetme

### Siteler, gruplar ve filtreler arasındaki farklar

#### Siteler(Sites)

##### Yararları

- Aynı Ajan İnternet bağlantı ayarlarını tüm cihazlarla ilişkilendirirler: Aracıyı her cihaz için yerel olarak manuel olarak yapılandırmaktan kaçınmak.
- Raporlar, uyarılar, biletler vb. Göndermek için e-posta iletişim bilgilerini bağlarlar.
- Sekme çubuğuna ve Simge çubuğuna erişebilir, eylemlerin ve görüntü listelerinin yürütülmesini ve sitede bulunan tüm aygıtları kapsayan uygun raporların hızlı ve kolay bir şekilde yapılmasını sağlar.

##### Sınırlamalar

- Bir cihaz sadece bir siteye ait olabilir.
- Site içerisinde bir sitenin yerleştirilmesi mümkün değildir.

### Filtreler ve gruplar

##### Yararları


- Gruplar / filtreler, bir veya daha fazla sitede bulunan cihazlar alt kümelerini oluşturmanıza olanak tanır.
- Bir cihaz çeşitli gruplara / filtrelere ait olabilir.

##### Sınırlamalar

- Gruplar / filtreler Sekme çubuğu erişilebilir olmadığından sınırlı işlevselliğe sahiptir, bu nedenle grup veya filtre üyeleriyle ilgili konsolide bilgiler içeren listeler oluşturmak mümkün değildir.
- Raporlara erişim sınırlıdır; oluşturulan raporlar sadece bir cihaz hakkında bilgi içerecektir.

## Cihaz bilgilerinin hızlı görünümü

Cihaz bilgilerinin hızlı bir şekilde görülebilmesi Cihazların doğru bir şekilde düzenlendiğinden, bir bakışta bilgiye hızlı bir şekilde erişebilmek önemlidir. Yönetim Konsolu, yönetici tarafından yapılandırılabilen bilgi alanlarına sahip cihazların listelerini görüntüler.

Herhangi bir cihaz listesinde görüntülenen bilgileri yapılandırmak için simgeyi tıklamanız gerekir: 

Bu simgeye herhangi bir cihaz listesinden erişilebilir (siteler, gruplar veya filtreler). Mevcut seçenekler şöyledir:

Alan	Description
UID	Cihazın dahili kimliği
Site	Cihazın ait olduğu sitenin adı
Host name	Cihazın adı
Description	
IP Address	Cihazın yerel IP adresi
Addit. IP's	Takma IP
Ext IP Addr	Cihazı internete bağlayan yönlendiricinin veya cihazın IP adresi
Last User	Son kullanıcı cihaza giriş yapmak için
Group	
Date Created	Cihazın sistemde oluşturulduğu tarih
Last Updated	Sunucunun cihaza son eriştiği tarih.
Last Audited	Son yazılım tarihi ve donanım denetimi.
Session Name	Kullanımda değil
Favorite	Sistem gösterge panellerinden hızlı erişim için cihazı yer imlerine kaydeder.
Privacy Mode	Cihazdaki gizlilik modu.
Agent Version	Küçük ajan versiyonu
Display Version	Tam ajan sürümü
Web Port OK	Cihaz markalama öğelerini, bileşenleri, güncellemeleri, vb. İndirmek için Web servisine bağlanabilir.
SNMP monitör	Aracının Bağlantı Aracısı rolünün etkin olması
Status	Durum (Çevrimiçi, Çevrimdışı). Çevrimiçi, Aracının "canlı kalsın" göndermek için Kontrol Kanalına bağlanabileceğini gösterir.
Model	
Operating System	
Service Pack	

<b>Serial Number</b>	
<b>Motherboard</b>	
<b>CPU</b>	Marka, model ve CPU hızı.
<b>Memory</b>	Yüklenen bellek miktarı.
<b>MAC Address(es)</b>	
<b>Custom field 1-10</b>	Tanımlanan Özel Alanların İçeriği.
<b>Device Type</b>	Cihaz tipi (iş istasyonu, dizüstü bilgisayar, tablet, akıllı telefon, yazıcı, ağ cihazı, ESXi ana bilgisayar).
<b>Domain</b>	Cihazın ait olduğu Windows alanı
<b>Disk Drive (total/Free)</b>	Cihazda yüklü olan tüm disklerin toplam alanı ve boş alanı.
<b>Online Duration (hrs)</b>	
<b>Cost</b>	Tüketimine göre cihaza karşılık gelen maliyet.
<b>Architecture</b>	32 bit veya 64 bit
<b>Display Adapters</b>	Cihaza takılı grafik kartının modelini yapın ve modeli.
<b>BIOS Name</b>	BIOS yap ve modeli.
<b>BIOS Release Date</b>	
<b>BIOS Version</b>	
<b>Last Reboot</b>	Cihaz son kez yeniden başlatıldı.
<b>Reboot required</b>	Yükleme işlemini tamamlamak için bir aygıtın yeniden başlatılmasını gerektirip gerektirmediğini belirtir.

## **Panda Systems Management'ı kullanmaya başlamak için ilk 8 adım**

### **Panda Systems Management'in mevcut başlangıç durumu**

Hizmet başlatma işleminin, müşterinin ağındaki hizmetin dağıtım durumunu grafik olarak gösteren bir yönetim konsolu bölümünden tamamlanıp tamamlanmadığını görebilirsiniz.

Bunu görmek için genel menüler Siteler'i tıklayın. Ekranın altında, her adımın ilerleyişini gösteren üç adımlı bir sihirbaz var:

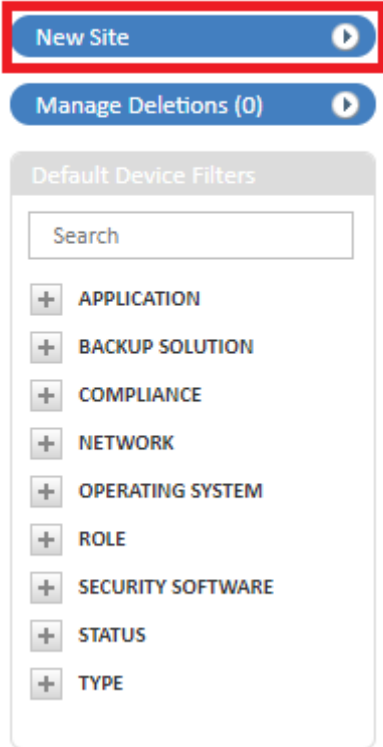
- Adım 1: Aracının cihazlarda dağıtımı
- Adım 2: Monitör oluşturma
- Adım 3: Denetim yürütme, yama yönetimi, politika yapılandırması

## İlk siteyi oluşturma ve yapılandırma

İlk olarak, kullanmakta olduğunuz yönetim kriterlerine bağlı olarak yeni bir site oluşturup oluşturmayacağınızı veya kullanımda olanı yeniden kullanıp kullanmayacağınızı belirlemelisiniz. Yeni bir müşteri hesabı genellikle yeni bir siteye karşılık gelecektir.

Genel olarak Siteler menüsünde Yeni site'yi tıklayın ve gerekli bilgileri girin. Açıklama alanının, eklediğiniz ve bu alanın içeriğine başvuran filtreler tarafından kullanılabilceğini unutmayın.

Sites



Sitedeki cihazlar Internet'e erişmek için kullanılan HTTP proxy hakkında ek bilgi gerektiriyorsa, bu bilgi burada sağlanabilir veya daha sonra eklenebilir.

Siteyi oluşturduktan sonra, Ayarlar sekmesi aracılığıyla yapılandırmanız önerilir. Bu yapılandırma, yönetilen her cihazda yüklü Aracıya dahil edilecektir.

## Systems Management Agent'ı Dağıtma

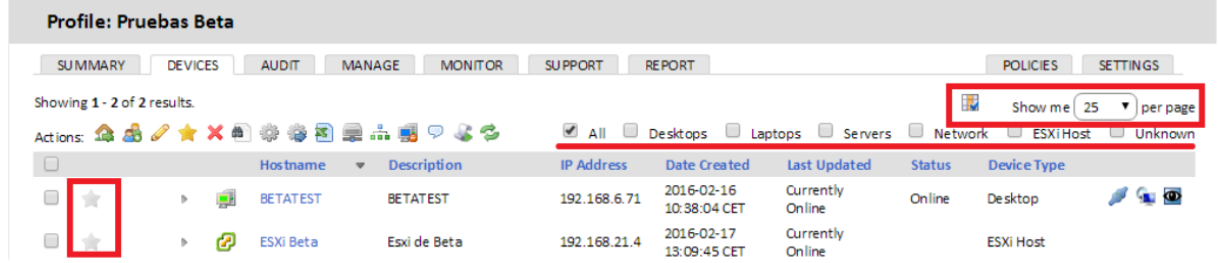
Müşterinin cihazlarında yüklü olan Aracı, işletmek için belirli bazı temel bilgileri gerektirir:

- Ait olacağı site.
- İnternete bağlanmak ve Sunucuya bağlanmak için gereken minimum bilgi.

İndirme bağlantısının indirilmesi veya gönderilmesi site üzerinden yapılırsa, Arayanın ait olduğu site otomatik olarak ayarlanır.

## Sitenin cihaz listesini ve temel filtrelemeyi kontrol etme

Cihazlara daha hızlı erişmek, listeleri düzenlemek, cihazı rolüne göre hızlı bir şekilde filtrelemek ve daha fazla veya daha az öge görüntülemek için listenin boyutunu değiştirmek için favori olarak işaretleyebilirsiniz.



Profile: Pruebas Beta

SUMMARY DEVICES AUDIT MANAGE MONITOR SUPPORT REPORT POLICIES SETTINGS

Showing 1 - 2 of 2 results.

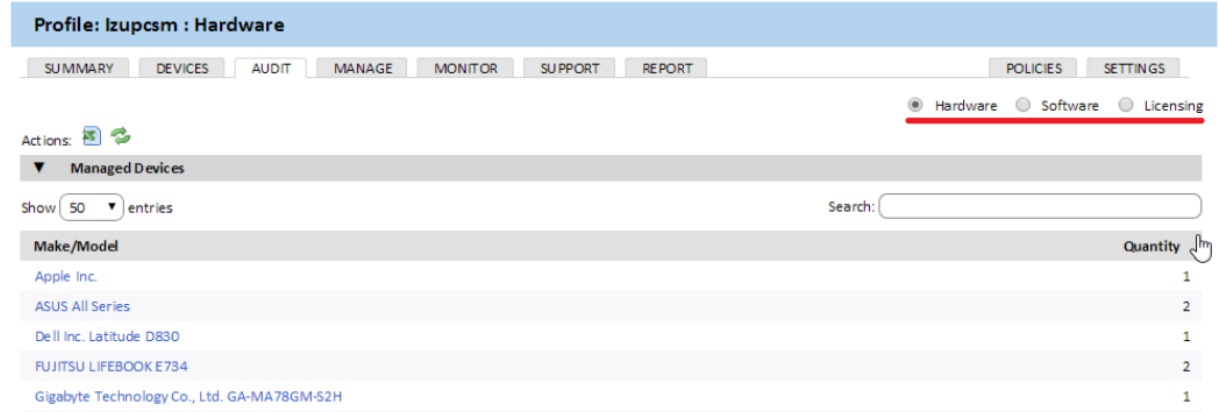
Actions:

All  Desktops  Laptops  Servers  Network  ESXi Host  Unknown

	Hostname	Description	IP Address	Date Created	Last Updated	Status	Device Type
<input type="checkbox"/>	BETATEST	BETATEST	192.168.6.71	2016-02-16 10:38:04 CET	Currently Online	Online	Desktop
<input type="checkbox"/>	ESXI Beta	Esxi de Beta	192.168.21.4	2016-02-17 13:09:45 CET	Currently Online	Online	ESXi Host

## Donanım, yazılım ve lisans denetimi(Hardware, software and license audit)

Sekme çubuğu, Denetim, siteye ait cihazların tüm denetim ayrıntılarını içerir veya Cihaz Düzeyinde erişilirse, cihaz hakkında ayrıntılı bilgi görüntüler.



Profile: Izupcsm : Hardware

SUMMARY DEVICES AUDIT MANAGE MONITOR SUPPORT REPORT POLICIES SETTINGS

Hardware  Software  Licensing

Actions:

Managed Devices

Show 50 entries Search:

Make/Model	Quantity
Apple Inc.	1
ASUS All Series	2
Dell Inc. Latitude D830	1
FUJITSU LIFEBOOK E734	2
Gigabyte Technology Co., Ltd. GA-MA78GM-S2H	1

## Yama yönetimi(Patch Management)

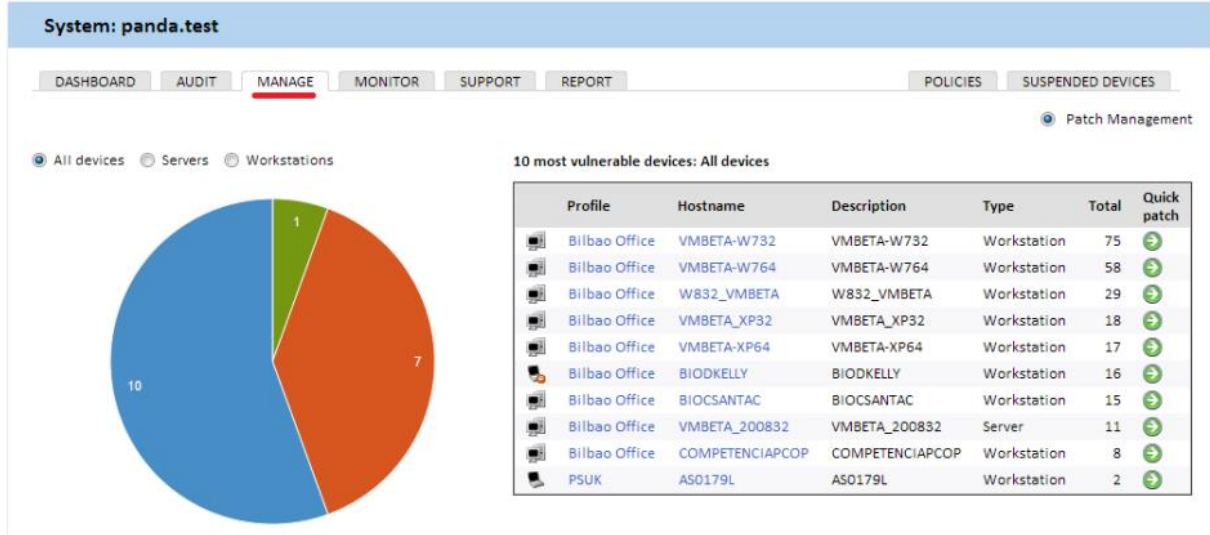
Yönetilen cihazlarınıza yüklenmemiş yamaları kaldırmak veya sekme çubuğundan kaldırmak istediğinizi geri almak için Yönet, Yönet'i tıklayın.

Sitedeki ilkelerin siteye ne zaman uygulanacağını, bir kerede uygulanacak adımları ve sekme çubuğundan bir Windows Update veya Yama Yönetimi ilkesi oluşturarak diğer parametrelerini, Sitedeki ilkeleri uygulayarak yapılandırın.



## Monitörler oluşturma(Creating monitors)

Ağ cihazlarının izlenmesini uygulamak için monitörlerin kurulması ve kurulması gerekir. Bu monitörler, herhangi bir cihaz belirli bir süre içinde belirlenen kriterleri karşılamadığı zaman Sunucuya bildirir.



Panda Systems Management, yönetim konsoluna eklenen cihazın türüne bağlı olarak belirli monitörleri otomatik olarak yapılandırır. Bu şekilde, yöneticilerin cihazlarının durumunu görüntülemek için temel bir dizi monitör ayarlayarak zaman harcamasına gerek yoktur.

En başından itibaren hizmetten en iyi şekilde yararlanabilmek için ithal edilebilen monitörler de var.

Yeni Site İlkesi'ni tıklayarak Genel menüden veya belirli bir siteden sekme çubuğundaki Politikalar bölümünden ek monitörler ekleyebilirsiniz.

Türü'nde İzleme(Monitoring) seçeneğini seçin.

The screenshot shows the 'Create a policy' form. The 'Name' field is filled with 'MyMonitor'. The 'Type' dropdown menu is set to 'Monitoring'. The 'Based on' dropdown menu is set to '- New Policy -'. There are 'Cancel' and 'Next' buttons at the bottom right.

Bir hedef (bir veya çeşitli gruplar veya filtreler) ve bir monitör ekleyin. Monitör eklendiğinde, gerekli ayarları yapılandırabileceğiniz 4 adımlı bir sihirbaz görünür.

## Create a monitoring policy

Name:

Policy type: Monitoring

Last updated: 2013-05-22 09:55:39 UTC

Last deployed:

Targets:

Type	Name
<i>There are currently no targets specified.</i>	
<input type="button" value="Add a target..."/>	

Monitors:

Category	Type	Alert if	Respond	Ticket	Severity
<i>There are currently no monitors specified.</i>					
<input type="button" value="Add a monitor..."/>					

## ComStore

ComStore, Panda Systems Management hizmetini geliřtiren ve üçüncü taraf yazılımların merkezi olarak yüklenmesini sađlayan önceden tanımlanmış bileşenlerin bir deposu.

Dođrudan iş ortađı / IT Yöneticisi tarafından kullanılan bileşenler ComStore'dan indirilmelidir.

Bir bileşeni indirmek için onu seçin ve Satın Al'ı tıklayın. Bileşenlerime hemen eklenecektir.

Bileşen tipine bađlı olarak, bir iş olarak veya bir monitör tarafından oluşturulan bir uyarıya yanıt olarak çalıştırılabilir.

Sekme çubuğunda, Sitelerdeki cihazlar, bileşenin uygulanacađı cihazları seçer ve Bir İş Planla (Schedule a Job) ile Hızlı İş Çalıřtır(Run a quick Job) arasında seçim yap.

## Uzaktan yönetilen cihazlarda kaynaklara erişme

Dođrudan bir çok günlük işlem Konsoldan gerçekleştirilebilmesine rağmen, doğrudan Ajan aracılıđıyla cihaza doğrudan erişim gerekebilir. Bu, aracıyı teknisyenlerin cihazlarına kurmayı gerektirir; böylece uzaktan destek sağlayabilir ve kullanıcı adı ve şifresiyle giriş yapabilirler.

PCSM Agent aracılıđıyla bir cihaza erişmek için aşağıdaki adımları izleyin.

Aracıyı uzaktan destek sağlayacak teknisyenin cihazına kurun.

- Cihazın ait olduđu siteyi seçin.
  - Cihazın içerik menüsünü genişletmek için simgeye tıklayın. Alternatif olarak, cihazın adını ve ardından Özet sekmesinin simgesini tıklayın.
  - Cihaza Bađlan'ı seçin. PCSM Agent otomatik olarak açılacak ve bađlanacaktır.
- cihaz.

- Cihazı bulduktan sonra, tüm uzaktan erişim ve uzaktan kumanda seçenekleri hem simgeler hem de menüler aracılığıyla erişilebilir.

Kullanıcının sistem üzerinde çalışmaya devam etmesini engellemeyen seçenekler şunlardır:

- **Uzak ekran yakalama:** Hata mesajlarının hızlı görüntülenmesi.

- **Windows Hizmetleri Sekmesi:** Uzak masaüstüne erişmeye gerek kalmadan hizmetleri durdurmak, başlatmak ve yeniden başlatmak için uzaktan erişim,

- **Ekran Paylaşımı Oturumu:** Paylaşılan uzak masaüstü. Kullanıcı teknisyenin cihazda ne yaptığını görüyor

- **Komut kabuğu:** Uzak DOS komut satırı

- **Aracı dağıtımı:** Aracıyı LAN üzerinden dağıtın.

- **Görev yöneticisi:** Uzak masaüstüne erişmeye gerek kalmadan görev yöneticisine uzaktan erişim.

- **Dosya aktarma:** Hedef aygıtın dosya sistemine tam erişim sağlar ve yöneticinin dosyaları bilgisayarları ile kullanıcının bilgisayarı arasında aktarmasına ve dosyaları taşımaya, klasörler oluşturup silip yeniden adlandırmasına izin verir.

- **Sürücü bilgisi:** Cihaza bağlı mevcut yerel ve ağ sürücülerini listeler ve yöneticinin ağ yollarını eklemesine veya silmesine izin verir.

- **Kayıt defteri düzenleyicisi:** Uzaktaki masaüstüne erişmeye gerek kalmadan regedit aracına uzaktan erişim

- **Hızlı İşler:** İşleri Başlatın.

- **Olay görüntüleyici:** Uzak masaüstüne erişmeye gerek kalmadan etkinlik görüntüleyicisine uzaktan erişim.

- **Uyandırma:** Aynı LAN segmentindeki cihazların geri kalanını uzaktan açmak için "sihirli paket" e göndermek üzere açık olan bir cihaza izin verir.

Kullanıcının cihazı kullanmasını engelleyen seçenekler şunlardır:

- **Windows RDP:** RDP aracılığıyla kullanıcının oturumu kapatacak uzak masaüstü erişimi.

- **Kapat / Yeniden Başlat:** Hedef cihazı kapatın veya yeniden başlatın.

## Politikalar(Policies)

Politikalar belirli bir süre boyunca düzenli aralıklarla tekrarlanması planlanan belirli yönetim veya iyileştirme eylemlerini uygulamak için kullanılır veya bir veya çeşitli yönetilen cihazlarda belirli koşullar sağlandığında tetiklenir.

Politikalar şunlardan oluşan yapılandırma kapsayıcılarıdır:

- **Hedefler:** Politikanın uygulanacağı cihaz grupları.
- **Hizmetler:** Politika türüne bağlı olarak, Ajan her cihazda belirli bir dizi işlem gerçekleştirecektir.

Politikalar, cihaz sayısına ve aynı müşteriye mi yoksa çeşitli şirketlere mi ait olduğuna bağlı olarak mevcut üç seviyede oluşturulabilir:

- **Hesap politikası:** Cihaz grupları, Site grupları veya Özel Cihaz Filtreleri için uygulanacak bir eylem tanımlar.
- **Site politikası:** Site Cihazı Grupları için Site Cihazı Filtrelerine uygulanacak bir eylem tanımlar.
- **Cihaz politikası:** Belirli bir cihaza uygulanacak eylemi tanımlar.

## Politika oluşturma

Politika oluşturmak için aşağıdaki adımları izleyin:

- Hedef cihazlara göre politikanın kapsamını veya seviyesini tanımlayın.
- Bir hesap politikası oluşturmak için, Hesap, Politikalar sekmesi genel menüsüne gidin ve pencerenin altındaki Yeni hesap politikası düğmesini tıklayın.
- Site ilkesi oluşturmak için Genel menülere gidin, önceden oluşturulan sitelerden birini seçin, İlkeler sekmesini ve ardından pencerenin altındaki Yeni site ilkesi düğmesini tıklatın.
- Bir cihaz politikası oluşturmak için genel menüler Sites menüsüne gidin, önceden oluşturulmuş sitelerden birini seçin ve politikanın atandığı cihazı tıklayın. Ardından, Monitör sekmesini ve pencerenin altındaki Monitör ekle düğmesini tıklayın.
- Politikanın adını, türünü ve oluşturma sürecini kolaylaştırmak için daha önce oluşturulmuş başka bir ilkeye dayanıp dayanmayacağını belirtin.
- Politikayı seçilen politika türüne göre yapılandırmak için gereken verileri girin. Bu bölümde daha sonra Panda Systems Management tarafından desteklenen politika türleri hakkında daha fazla bilgi verilmektedir.
- İlkesine (Hesap, Site veya Aygıt) bağlı olarak ilke hedefini (gruplar veya filtreler) ekleyin.

## Politikaları yönetme

Politikalar üç düzeyde oluşturulabileceğinden, belirli bir grup tarafından hangi aygıt gruplarının hedeflendiğini veya farklı düzeylerde oluşturulan politikalar arasında örtüşen sorunlar varsa belirlemek zor olabilir.


## Hesap Düzeyinde politikaları yönetme

Genel menü Hesap, Politikalar sekmesine gidin. Hesap Düzeyinde oluşturulan tüm politikaları ve bunlarla ilişkili bilgileri gösteren bir pencere görüntülenecektir:

- İsim: Politikanın adı.
- Hedefler: Politikanın uygulanacağı cihaz grupları.
- Tür: Politika türü. Bu bölümde daha sonra Panda Systems Management tarafından desteklenen politika türleri hakkında daha fazla bilgi verilmektedir.
- Etkin (AÇIK / KAPALI): Politikayı etkinleştirir / devre dışı bırakır.

Ayrıca, aşağıdaki beş ek kontrol mevcuttur:


- **Geçersiz kılmayı düzenle:** Hesap Düzeyinden devralınan politikayı düzenlemenizi sağlar. Bu seçenek yalnızca Hesap Düzeyinde tanımlanan ve Site Düzeyinde yönetilen Yama Yönetimi politikaları için görüntülenir.
- **İtme değişiklikleri:** Politikayı hedef olarak seçilen tüm cihazlara dağıtır.

-  : Politikayı alacak cihazları görmeyi sağlar.

- **Bu site için etkinleştirildi:** Sitenin veya hesabın tümünün politikasını etkinleştirir / devre dışı bırakır.

- **Sil**  : Politikayı siler.

## Politikadan etkilenen cihazları görüntüleme

Politika ilişkilendirmeleri ekranına gitmek için simgeyi tıklayın  . Orada politikadan etkilenen tüm cihazların listesini görebilirsiniz:

- **Site hariç tutmaları:** Politika dışında bırakılan siteler.
- **Site manuel olarak etkinleştirildi:** Politika için manuel olarak etkinleştirilen siteler.
- **Tüm Cihazlar:** Politika ile ilişkili cihazlar.
- **Dahil Olan Cihazlar:** Şu anda politikaya sahip olan cihazlar.
- **Hariç Tutulan Cihazlar:** Şu anda politikadan hariç tutulan cihazlar

## Politika nasıl dağıtılır?

Bir politika oluşturulduktan sonra, sitenin ekranına bir satır eklenir.

Politikayı dağıtmak için Değişiklikleri başlat'ı tıklayın. Bu, politikayı, etkilenen tüm aygıtlara uygulayarak yürütmesini tetikler.

## Policy types

Aşağıda özetlenen sekiz politika türü vardır:

### Ajan(Agent)

Bu tür bir ilke, Ajan görünümünü ve kullanıcının kullanabileceği işlev özelliklerini belirlemenizi sağlar.

### Gizlilik Modu Seçenekleri

- **Gizlilik Modunu Etkinleştir:** Gizlilik modunun etkinleştirilmesi, bir kullanıcının, yöneticinin uzaktan erişme girişimlerini kabul etmesini veya reddetmesini sağlar. Bir cihazda gizlilik modu etkinleştirildiğinde, uzaktan yönetim araçlarını (uzak masaüstü, ekran görüntüleri, uzak kabuk, servis yönetimi vb.) Kullanmadan önce kullanıcının iznini almak gerekir.
- **Kullanıcı girişi yapılmadığında bağlantılara izin ver:** Gizlilik modu etkinleştirildiğinde, bu seçenek yöneticilerin giriş yapma girişimine izin vermek veya reddetmek için giriş yapmadığı zaman bir cihaza bağlanmasına izin verir.
- **Yalnızca Sınırlı Araçlar için izin almanız gerekir:** Gizlilik modunu yapılandırır, böylece müşteri yalnızca etkileşimli olarak veya ekran görüntüsü almak için uzak masaüstüne erişmeye çalıştığında müşterinin onay isteklerini alır. Başka herhangi bir uzaktan yönetim aracı, yönetici tarafından kullanılmak üzere kullanıcıdan izin almayı gerektirmez.

### Servis Seçenekleri(Service Options)

- **Yalnızca servis yükle:** Windows saatinin yanındaki bildirim alanında görüntülenen simgeyi gizler. Bu, kullanıcının ayar ekranlarına erişmesini engeller.
- **Gelen işleri devre dışı bırak:** Cihazdaki işlerin yürütülmesini önler.
- **Gelen desteği devre dışı bırak:** Cihaza uzaktan erişimi devre dışı bırakır.
- **Denetimleri devre dışı bırak:** Seçilen cihazların donanım / yazılım denetim verileri göndermesini engeller.
- **Gizlilik Seçeneklerini Devre Dışı Bırak:** Kullanıcıların, Acenta'nın seçenekler menüsünden erişilebilen gizlilik seçeneklerine erişmelerini önler.
- **Ayarları Devre Dışı Bırak menüsü:** Kullanıcıların, Aracı simgesinin sağ tıklatıldığında görüntülenen Ayarlar menüsüne erişmesini engeller.

- Çıkış Seçeneklerini Devre Dışı Bırak.

- Biletleri Devre Dışı Bırak sekmesi: Aracı'nın Biletleri sekmesini devre dışı bırakır.

- Ajan Tarayıcı Modu: Ajan'ın çalışma şeklini ayarlamanıza izin verir.

## ESXi

Bu politika, yöneticilerin performansı, veri depolama kapasitesini ve sıcaklığını izlemek için ESXi sunucularına monitör oluşturup atamasını sağlar.

## Bakım Penceresini İzleme(Monitoring Maintenance Window)

Bakım politikaları, cihazlarda oluşturulan uyarıların e-posta bildirimleri veya bilet oluşturmayacağı bir süre tanımlamanızı sağlar.

BT politikaları BT ağında uzun bir süre boyunca bakım yapmak zorunda olduğunda bu politikalar kullanılır; Bu dönemde, uyarılar gereksiz gürültü yaratabilir.

## İzleme (Monitoring)

Bu politika, cihaz kaynağı izleme süreçlerini eklemenizi sağlar.

## Yama Yönetimi(Patch management)

Yama yönetimi, yazılım yamalarını indirmek ve yüklemek için Panda Systems Management'teki araçlardan biridir.

## Güç(Power)

Bu politika, güç tasarrufu ayarlarının bunları destekleyen cihazlarda yapılandırılmasına izin verir.

### Power Policy Options

Turn off disk after:  minutes

Turn off display after:  minutes

Standby after:  minutes

Schedule:  :  :  daily

## **Windows güncelleme(Windows update)**

Windows Update, bir WSUS sunucusunda bulunan seçeneklerin bir aktarımıdır ve Microsoft sistemlerinde en yaygın Yama Yönetimi seçeneklerinin yapılandırılmasına izin verir.

## **Mobil Cihaz Yönetimi(8 Mobile Device Management)**

Mobil Cihaz Yönetimi (MDM), iOS cihazları (tabletler ve akıllı telefonlar) için politika oluşturmanıza olanak tanır. Bu politikalar, bu tür cihazların kullanımını kısıtlamanıza izin verir.

## **Bileşenler ve ComStore(Components and ComStore)**

### **Bileşen nedir?**

Bileşen, Panda Systems Management platformunun, yöneticilerin PCSM Agent'a izleme ve sorun giderme özellikleri eklemesine izin veren bir uzantısıdır.

Bileşenler, bunları geliştirenlere göre iki gruba ayrılabilir:

- Yönetim ve uzaktan sorun giderme aracı olarak Panda Systems Management kullanan şirketin yöneticileri veya BT ekibi tarafından geliştirilen bileşenler.
- Panda Security tarafından geliştirilen ve ComStore aracılığıyla tüm müşterilere ücretsiz sunulan ürünler.

### **Yönetici tarafından geliştirilen bileşenler**

Bunlar amaçlarına, davranışlarına ve koşu yöntemlerine göre üç gruba ayrılır:

## **Uygulamalar(Applications)**

Bunlar normalde sadece bir kez veya çok özel koşullar altında çalıştırılan betiklerdir ve bunlarla ilişkili harici dosyalara sahip olabilirler (kurulum bileşenleri söz konusu olduğunda, bunlar kullanıcının aygıtına yükleme yazılımıdır).

## **Monitor**

İzleme politikaları her zaman kullanıcının cihazlarını izlemek için bir bileşen içerir. Panda Systems Management, CPU veya sabit disk kullanımı gibi cihazların birçok yönünü izleyen bir dizi varsayılan monitörle birlikte gelir. Ancak, yöneticinin izlemesi gerekebilir. Öncelikle platform tarafından tasarlanmayan yönler. Bu durumda, politikaya bir monitör bileşeni eklemek gerekli olacaktır.



## Scripts

Bunlar, müşterinin cihazlarında çalışan bir betik dilinde geliştirilmiş küçük programlardır. Tek seferlik bir iş olarak veya periyodik olarak görev zamanlayıcısında yapılandırılan zamanlamaya göre çalıştırılabilirler.

Aşağıda, yönetici tarafından geliştirilen bileşen türlerini özetleyen bir tablo görebilirsiniz.

<b>Bileşen tipi</b>	<b>Kaçmak</b>	<b>Çalışma</b>	<b>Amaç</b>
<b>Uygulamalar (Applications)</b>	Hızlı iş veya planlı iş	0 sırada veya bileşeni oluştururken veya planlandığında.	Merkezi olarak dağıtın ve yükleyin.
<b>Monitörler(Monitors)</b>	Site veya hesap politikası	60 saniye (sabit aralık).	Monitor devices
<b>Scripts</b>	Hızlı iş veya planlı iş	0 sırada veya bileşeni oluştururken veya planlandığında.	Run applications developed by the administrator
<b>Ağ Monitörleri (Network Monitors)</b>	Cihaz politikası	60 saniye (sabit aralık).	Bir Systems Management Agent ile uyumlu olmayan cihazları izleyin.

## Panda Security tarafından geliştirilen bileşenler

ComStore, Panda Systems Management kullanıcıları için Panda Security tarafından geliştirilmiş ve onaylanmış bileşenlerin çevrimiçi bir kütüphanesidir.

ComStore'un amacı, IT ekibi için bileşenlerin daha kolay erişilebilir olmasını sağlamaktır.

## Platformdaki bileşenleri kullanma

### Bileşenleri platforma entegre etme

Yönetici tarafından kullanılacak bir bileşen için öncelikle Panda Systems Management platformuna dahil edilmelidir.

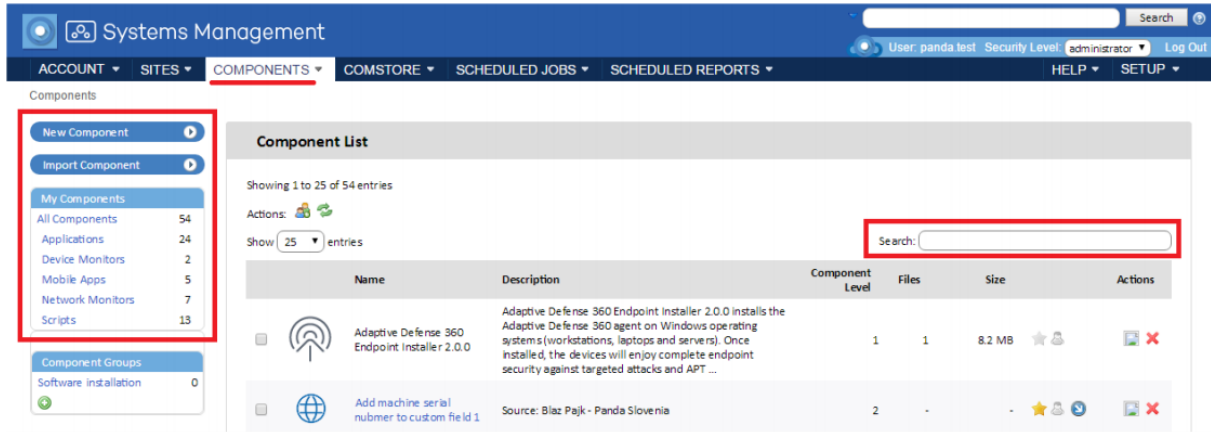
### ComStore'dan bir bileşen eklemek

Panda Security tarafından geliştirilen ve onaylanan bileşenlerin kütüphanesine erişmek ve Panda Systems Management müşterilerinin kullanımına sunulan ComStore'un genel menüsüne gidin.

ComStore'dan Bileşen Listesine bir bileşen eklemek için, onu tıklamanız yeterlidir. Bileşen açıklaması, yayınlanma tarihi, derecelendirme ve onu kullanan diğer yöneticilerin yorumlarıyla birlikte bir pencere görüntülenecektir. Bileşeni Bileşen Listesine eklemek için Satın Al'a tıklayın.

## ComStore'daki bileşenlerin aranması

Bileşenleri aramak için ComStore'a gidin ve soldaki paneli kullanın. Bu panel, Panda Security'nin Bileşenler bölümünün Bileşenlerim paneli ile aynı şekilde ComStore'a eklediği bileşenleri sınıflandırır. Bileşenleri adlarına göre aramak için arama aracını ekranın sağ üst köşesinde de kullanabilirsiniz.



The screenshot shows the 'Systems Management' interface. The 'COMPONENTS' menu is selected. On the left, there is a sidebar with 'New Component', 'Import Component', and 'My Components' sections. The 'My Components' section lists various categories and their counts. The main area displays a 'Component List' table with columns for Name, Description, Component Level, Files, Size, and Actions. A search bar is located in the top right corner of the table area.

Name	Description	Component Level	Files	Size	Actions
Adaptive Defense 360 Endpoint Installer 2.0.0	Adaptive Defense 360 Endpoint Installer 2.0.0 installs the Adaptive Defense 360 agent on Windows operating systems (workstations, laptops and servers). Once installed, the devices will enjoy complete endpoint security against targeted attacks and APT ...	1	1	8.2 MB	⋮
Add machine serial number to custom field 1	Source: Blaz Pajk - Panda Slovenia	2	-	-	⋮

## Bileşenleri içe aktarma(Importing components)

Bir bileşeni doğrudan PCSM Konsolu'ndan içe aktarmak için genel menüde Bileşenler'e gidin ve Bileşeni İçe Aktar'ı tıklayın.

Yalnızca PCSM Konsolu'ndan daha önce dışa aktarılan bileşenleri alabilirsiniz. Bir bileşeni diske vermek için bileşen listesindeki ok simgesini tıklayın.

Name	Description	Component Level	Files	Size	Actions
Spotify		5	1	718.5 KB	⋮

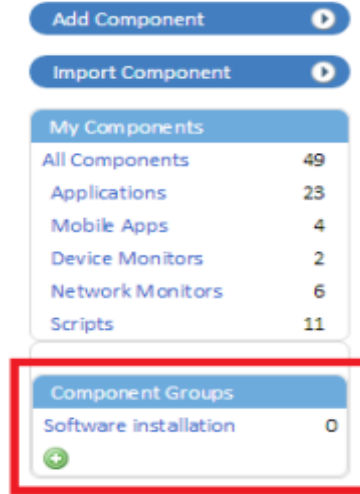
## Entegre bileşenlerin sınıflandırılması ve sınıflandırılması

Halihazırda platforma entegre edilmiş bileşenleri görmek için Genel menüye gidin.



Ekranın sol tarafındaki Bileşenlerim bölümü, tümleşik bileşenleri işlevlerine göre otomatik olarak sınıflandırır. Altı kategori mevcuttur:

- Tüm Bileşenler (All Components)
- Uygulamalar (Applications)
- Mobil uygulamalar (Mobile Apps)
- Uzantılar (Extensions)
- Cihaz Monitörleri (Device Monitors)
- Scripts

Ayrıca, yöneticiler Bileşen Listesi altında bulunan bileşen gruplama aracını kullanarak yeni bileşen grupları oluşturabilir.



Bir bileşen grubu oluşturmak için aşağıdaki adımları izleyin:

- Go to general menu Components
- Simgesini tıklayın  . Yeni bileşen grubunun adını girmeniz için bir pencere açılacaktır.
- Bir isim girin ve Kaydet'i tıklayın.
- Gruplanacak bileşenleri seçin ve simgeye tıklayın  .
- Tüm mevcut bileşen gruplarını listeleyen bir pencere görüntülenecektir. Seçilen bileşenleri eklemek için grubu seçin.

Systems Management

ACCOUNT SITES COMPONENTS COMSTORE SCHEDULED JOBS

Components

New Component

Import Component

My Components

All Components	66
Applications	28
Device Monitors	8
Extensions	2
Integrations	1
Mobile Apps	6
Scripts	21

Component Groups

Software installation	0
-----------------------	---

Component List

Showing 1 to 50 of 66 entries

Actions: [Update Icon]

Show 50 entries

Name
<input type="checkbox"/> Adaptive Defense 360 Endpoint Installer 2.0.0
<input type="checkbox"/> Add machine serial number to custom field 1
<input type="checkbox"/> Adobe Flash Player [WIN]

## Bileşenleri Güncelleme(Updating Components)

Panda Security, düzenli aralıklarla ComStore'da yayınlanan bileşenlerin güncellemelerini yayınlar. Bu güncellemeler ComStore'un güncellemesini kontrol et bölümünde bir araya getirilmiştir.

Bu bölüm, Yöneticilerime yönetici tarafından eklendiğinden beri güncellenmiş olan tüm ComStore bileşenlerini gösterir. Bileşenlerimdeki tüm bileşenleri güncellemek için Tümünü Güncelle'yi tıklatın.

Updates

Update All

Google Chrome [WIN] Applications Free <input type="button" value="Get Update"/>	Malwarebytes Anti-Malware 2.2.0.1024 [WIN] Applications Free <input type="button" value="Get Update"/>	Adobe Reader [WIN] Applications Free <input type="button" value="Get Update"/>
---	--	--

Ayrıca, yöneticiler, son hafta içinde ComStore'a eklenen tüm bileşenlerin bir listesiyle haftalık olarak e-posta bildirimleri ve Bileşenlerim bölümünde bulunan bileşenlerin güncellemeleri alabilir.


Bu haftalık bildirimini etkinleştirmek için, Genel menü Kur, Hesap Ayarları'na gidin ve E-posta alıcılarındaki ComStore Bileşenleri'ni seçin.

## Bir Hızlı İşten Bileşenleri Kullanma

### Scheduled Jobs tab

Bir Hızlı İş başlatıldıktan sonra, sonuçları hem Aktif İşleri hem de Tamamlanmış İşleri gösteren Zamanlanmış İşler sekmesinde görebilirsiniz.



Hızlı bir iş ile Panda Systems Management'a entegre edilmiş bir bileşeni çalıştırmak için aşağıdaki adımları izleyin:

- Genel menüye git Bileşenler(Components).
- Bileşen listesinden, çalıştırmak istediğiniz bileşenin simgesini tıklayın .

Name	Description	Component Level	Files	Size	Actions
<input type="checkbox"/>  Spotify		5	1	718.5 KB	    

Çalışma alanınıza istediğiniz kadar bileşen ekleyebilir ve istediğiniz kişileri seçebilirsiniz.

Hızlı bir iş yapılandırmak için şu adımları izleyin:

- İşin uygulanacağı bilgisayarları seçin ve simge çubuğunda bulacağınız simgeyi tıklayın .
- Hızlı iş simgesi, Hesap Seviyesi, Site Düzeyi ve Cihaz Seviyesi altındaki simge çubuğunda bulunabilir. Yani, bir veya birden fazla sitede bulunan tüm aygıtlarda, aynı sitedeki birkaç bilgisayarda ve tek bir aygıtta hızlı bir iş başlatabilirsiniz.
- Görüntülenen aşağı açılır menüden çalışacak bileşeni seçin. Sadece simgeyi kullanarak hızlı iş listesine eklenmiş olan bileşenler  görüntülenecektir.

## Aktif İşler(Active Jobs)

Bu sekme, yürütmeyi bekleyen sıraya alınmış işleri gösterir. Sonuçları filtrelemek için mevcut araç çubuğunu kullanabilirsiniz.

## Completed Jobs(Tamamlanmış İşler)

Bu sekme, tamamlanan her işi ve iş sonucunu belirten bir hata kodunu gösterir.

## Zamanlanmış Bir İşten Bileşenleri Kullanma

Zamanlanmış İşler, Hızlı İşler gibidir, tek fark, daha sonra çalıştırılmak üzere programlanmasıdır. Zamanlanmış İşler, oluşturmak için daha fazla bilgi girmeyi gerektirir, örneğin, işin ne zaman yapılacağı, sıklığı, işin bitmiş sayılmadan önce kaç kez çalıştırılması gerektiği gibi.

Bir Hızlı İşi(Quick Job) yapılandırmak için Hesap, Site veya Aygıt Düzeyindeki Simge çubuğuna gidin ve Zamanlanmış İş(Scheduled Job) simgesine tıklayın. İlgili ayarları girmeniz için bir pencere açılacaktır.

## **Execution cycle(Execution cycle)**

Yürütme döngüsünü ayarlamak için, Programlama bölümünde değiştirmek için tıklayın. Seçtiğiniz sıklığa (günlük, haftalık, vb.) Bağlı olarak, sağdaki panel, yürütme tarihlerini belirtmeniz için farklı seçenekler gösterecektir.

## **Bileşen seçimi(Component selection)**

Çalıştırılacak bileşeni seçmek için bir pencere açmak için Bileşen Ekle(Add Component) bağlantısına tıklayın.

## **İş bitiş tarihi(Job end date)**

Bu bölüm, işin tekrar etmeyi durdurduğu ve bitmiş sayıldığı tarihi girmenizi sağlar.

Ayrıca, etkileşimli bir oturum açmak için Zamanlanmış İşin çalıştırılacağı bilgisayarları zorlamanıza izin verir.

## **Uyarılar(Alerts)**

Bu bölüm, yapılandırılmış koşullardan herhangi biri karşılandığında uyarı oluşturmanızı sağlar. Uyarıları birden çok alıcıya göndermek için e-posta adreslerini girmek için İş Alıcıları bölümünü kullanın.

## **Zamanlanmış İş çıkışını postalama(Mailing the Scheduled Job output)**

Bu seçenek, Zamanlanmış Bir İşin getirdiği hata kodunu bir e-postaya kopyalamanızı sağlar.

## **Gelişen bileşenler(Developing components)**

Geliştirme bileşenleri, yöneticinin, kullanıcıların cihazlarında çalışacak ve Panda Systems Management platformuna fazladan işlevsellik katacak yeni süreçler oluşturmasına olanak tanır.

Panda Systems Management, temel işlevlerini genişleten bir varsayılan bileşen deposu (ComStore) sağlasa da, kullanıcıların aygıtları üzerinde çok özel görevleri gerçekleştirmek için belirli bileşenlerin geliştirilmesi veya çözümün izleme yeteneklerinin kurulumunu desteklemeyen aygıtlara genişletmesi gerekebilir.

Panda Systems Management bu nedenle her müşterinin özel ihtiyaçlarına çok kolay uyum sağlayan genişletilebilir bir uzaktan yönetim ve izleme platformudur.

## Bileşenleri geliştirme gereksinimleri nelerdir?

Genel bileşenler geliştirmek için, yöneticinin desteklenen komut dosyası dillerinden birinde programlama ile ilgili temel bilgiye ihtiyacı vardır:

Dil(Language)	Standart olarak dahil	Sağlayıcı(Provider)
Batch	Tüm Windows sürümleri	Microsoft
Visual Basic Script	Windows 98 ve üstü Windows NT 4.0 Option Pack ve sonrası	Microsoft
JavaScript (Jscript)	Windows 98 ve üstü Windows NT 4.0 Option Pack ve sonrası	Microsoft
Powershell	Windows 7	Microsoft
Python	Mac OS X 10.3 (Panter)	Python Yazılım Vakfı
Ruby	Yok	Yukihiro Matsumoto
Groovy	Yok	Önemli ve Groovy Topluluğu
Unix (Linux, Mac OSX)	Linux, Mac OS X	Değişken

Ayrıca, seçilen komut dosyası diliyle ilişkili ayrıştırıcı, kullanıcının aygıtına yüklenmeli ve çalıştırılmalıdır.

## Bir monitör bileşeni oluşturma

Aşağıda bir monitör oluşturma ve belirli bir sitedeki cihazlara dağıtma adımlarının ayrıntıları yer almaktadır.

Bileşenin amacı, güvenlik ürünü Panda Endpoint Protection'ın karantinasını kolayca ve basit bir şekilde yönetmektir. Karantina, kötü amaçlı yazılım içerebilen şüpheli dosyaları ve ayrıca virüs olarak algılanan dosyaları depolar. Bu nedenle, yöneticinin her zaman kaç öğenin karantinada olduğunu bilmesi gerekir.

Örnek ayrıca, yeni monitörleri diğer yazılım çözümlerine uyarlamanın ve entegre etmenin ne kadar basit olduğunu da göstermektedir.

Aşağıda bileşen özelliklerinin bir özeti verilmiştir.

Etkilenen cihazlar	Ana Sayfadaki tüm Windows 7 cihazları
Komut dili(Script language)	Visual Basic Script
Bilgi gönderme sıklığı	Her 10 dakikada bir, karantinadaki madde sayısının artırılıp artırılmadığına dair bir bildirim gönderilir.
Sistem Yönetimi eylemleri	İzleme sonuçlarıyla yöneticiye bir e-posta gönderilir. Bir uyarı olacak otomatik olarak üretilecek

Ele alınması gereken sorunlardan biri, Ajanın her 60 saniyede bir otomatik olarak betiği yürütmesidir, ancak her 10 dakikada bir bilgi verir.

Ele alınması gereken sorunlardan biri, Ajanın her 60 saniyede bir otomatik olarak betiği yürütmesidir, ancak her 10 dakikada bir bilgi verir.

## **Gerekli elemanlar (Necessary elements)**

Bu örneği takip etmek için, bir Panda Endpoint Protection lisansı gereklidir ve Agent'ın cihaza yüklenmesi gerekir. Bununla birlikte, Panda Endpoint Protection tarafından karantinaya eklenen öğeler cihazdaki belirli bir klasördeki dosyalar olduğundan, bu örnek sistemdeki başka herhangi bir klasörle kullanılabilir.

Panda Endpoint Protection, masaüstleri, sunucular, dizüstü bilgisayarlar ve Exchange Server için gerçek zamanlı olarak spam ve bilinen tehditlere karşı maksimum koruma sağlamak için Kolektif Zekanın gücünü kullanması ve kullanması kolay olan eksiksiz bir bulut tabanlı güvenlik çözümüdür.

Bileşen, Visual Basic Script geliştirildi ve bu nedenle, Wscript.exe veya Cscript.exe ayrıştırıcısının kullanıcının aygıtına yüklenmesi gerekir. Bu ayrıştırıcı, tüm Windows işletim sistemlerinde standart olarak gelir.

## **Bileşen ve Sunucu arasındaki iletişim protokolü**

Hemen hemen tüm bileşenlerin Sunucudan bilgi alması ve yürütme işleminin sonucunu Sunucu'ya geri getirmesi gerekecektir. Sunucu ile bileşen arasındaki tüm bilgi alışverişi, cihaz üzerinde oluşturulan ortam değişkenleri aracılığıyla gerçekleştirilecektir.

Bir bileşen başlatıldığında bu ortam değişkenleri, Aracı tarafından otomatik olarak oluşturulur. Ancak, komut dosyasının toplanacak ve Console'a ekleyeceği Sunucuya yanıt göndermek için el ile ortam değişkenleri oluşturması normaldir.

Bu durumda, üç ortam değişkenleri gereklidir.



<b>Değişken Adı</b>	<b>Yön</b>	<b>Amaç</b>
PCOP_PATH	Oku(Read)	Read Komut, Sunucudan, Panda Endpoint Protection'ın her kullanıcının cihazında karantınayı depoladığı yolu kurtarır.
Result	Yaz(Write)	Verileri standart çıktıya her 10 dakikada bir Sunucuya gönderin.
Errorlevel	Yaz(Write)	Komut dosyası hata kodu. 0 ise, Sunucu izlemenin doğru olduğu sonucuna varır ve standart çıktı verilerini toplamaz. Eğer 1 ise, Panda Systems Management, izlemenin yanlış olduğunu, standart çıktı verilerini (Sonuç değişkenini) toplar ve işler.

Bileşeni müşterinin cihazında yürütmek için gerekli ayarlar, izlenecek klasörün yolu olacaktır. Bu yol, komut dosyası kaynak kodunda kodlanmış olabilir, ancak bu örnekte, bileşene daha fazla esneklik eklemek için yöneticinin Konsola girmiş olduğu değerler kullanılacaktır.

Errorlevel, Komut dosyası cevabını (Sonuç değişkeni) işlemesi gerekip gerekmediğini Sunucuya bildirir: Karantinadaki dosyaların sayısı aynı veya daha düşükse (karantina boşaltımı) bir Hata seviyesi 0 gönderilir. Ancak, dosya sayısı arttıkça 1 gönderilir ve standart çıktıda (Sonuç değişkeninde) belirli bilgiler yazılır. Sunucunun standart çıktıyı doğru şekilde yorumlaması ve bileşenin Sonuç değişkeninin içeriğini ayıklaması için aşağıdaki format kullanılmalıdır:

- Linea 1: <-Start Result->
- Linea 2: Result=(datos a enviar)
- Linea 3: <-End Result->

Sonuç, sunucunun, bileşenin yürütülmesini sonlandırmak için verileri çıkaracağı değişken olacaktır. "=" Seçeneğinin sağındaki dizge, Sunucunun depolayacağı ve işleyeceği içeriktir.

# Bir monitör bileşeniyle nasıl çalışılır?

## Monitör bileşenini Panda Systems Management platformuna yükleme.

Monitör bileşenini Panda Systems Management platformuna yükleme.

- Komut dosyası türlerini seçin.
- Kullanılacak betik dilini seçin, bu örnekte VBScript.

Script

Script: - Select script type -

- Select script type -
- Batch
- Unix (Linux, Mac OSX)
- VBScript
- JavaScript
- PowerShell
- Python
- Ruby
- Groovy

Timeout this script if not completed (seconds)

Variables

- Bileşenin maksimum yürütme süresini ayarlayın. Bu süre geçtikten sonra, Aracı yürütmeyi durdurur.

- Girdi ve çıktı değişkenlerini ayarlayın, bu örnekte PCOP\_PATH, Panda Son Nokta Koruması karantina klasörüne giden yolu içerecektir. Sonuç, komut dosyasının çıktısını içerecektir.

Variables

Input Variables

Name	Type	Default Value	Description
PCOP_PATH	Value	c:\users\olopez\desktop\gd\	

Output Data

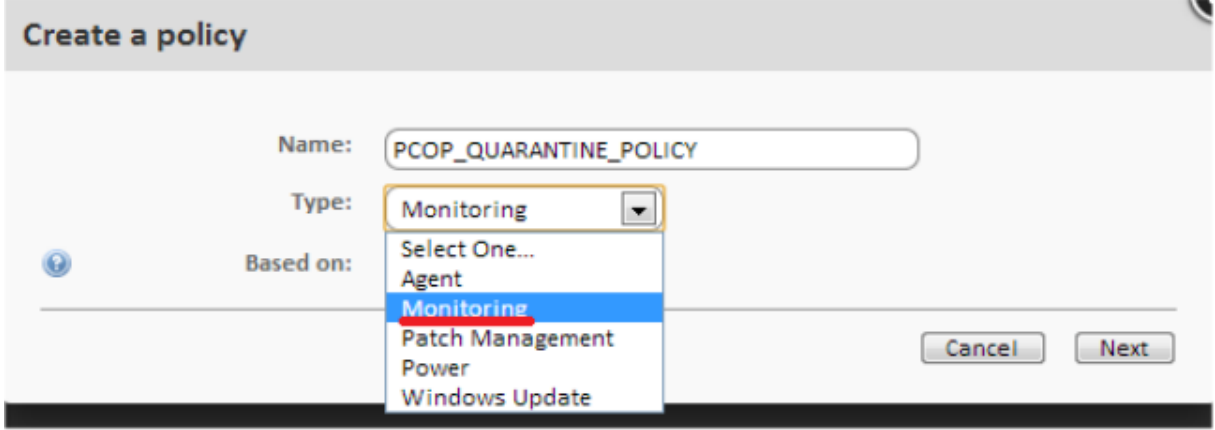
Name	Type	Description
Result	String	

Save Cancel

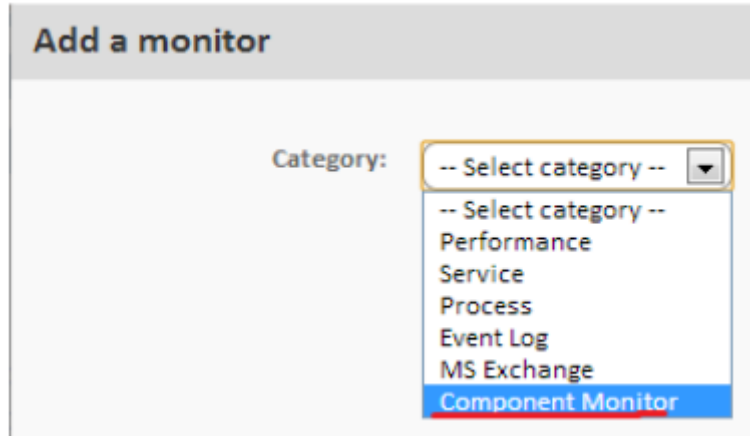
- Kaydet'i tıkladığınızda, bileşen depoya eklenir.

## Monitörü Hesap Politikaları veya Site Politikaları aracılığıyla dağıtma

- Bir monitör geliştiriyorsanız izleme sitesi politikası veya hesap politikası oluşturulmalıdır.



- Hedef ve bir Bileşen Monitörü ekleyin.



- Son oluşturulan bileşeni seçin ve kaydedin.



- Monitör bir hata durumu döndürdüğünde ve belirli bir süre sonra uyarının otomatik olarak çözülüp çözülmeyeceği veya yöneticinin manuel olarak çözülüp çözülmeyeceği konusunda Panda Systems Management'ın oluşturulması gereken uyarının şiddetini belirtebilirsiniz.

- Karantinede yeni öğeler tespit edildiğinde Sunucunun bir e-posta üretmesi için, alıcının adresi ile bir e-posta yanıtı (Yanıtla) tanımlayın. Yanıt değişkeninin içeriği, yöneticiye gönderilecek e-postaya kopyalanacaktır.

Respond:

Response options

Run the following component:  
- Select component -

Email the following recipients:

Default recipients (As per profile and account settings)

Additional recipients:

Name	Address	Type
Administrador	administrador@domain.com	HTML

Save

Create Support Ticket:

Ticket owner

Assignee: CCF22PLC2K Ticket Email Notification

- Bir monitör oluşturulduktan sonra, Politikalar ekranına bir çizgi eklenecektir. Bu ekrana genel menü Hesap, Sekme Politikaları'ndan veya sitenin genel menüsünden, ilkenin oluşturulduğu siteyi seçerek ve İlkeler sekmesini tıklatarak erişilebilir. Bu, politikanın oluşturulduğu Düzeye bağlı olacaktır.

Profile : Home

SUMMARY DEVICES AUDIT MANAGE MONITOR SUPPORT REPORT POLICIES SETTINGS

► 0 Account Policies

▼ 1 Profile Policies

Name	Targets	Type	Enabled for this profile
PCOP_QUARANTINE_POLICY	Default filter: MS Win 7	Monitoring	Push changes...  ON

Add profile policy...

- Monitörü dağıtmak için Değişiklikleri Push Changes tıklayın. Bu, politikayı uygular ve monitör, tüm etkilenen cihazlara dağıtılarak yürütmesini tetikler.

## Komut dosyası bileşeni oluşturma


Bir komut bileşeni, bir monitör bileşeni ile aynı şekilde oluşturulur.

- Genel menü Bileşenleri'ne gidin ve Yeni Bileşen'e tıklayın.
- Komut tipini seçin.
- Bir komut dosyası bileşeni için ayarlar ekranı, bilgi toplama bölümündeki bir monitör bileşeninin ayarlar ekranından farklıdır: Çıkış değişkenlerini tanımlayamazsınız, ancak konsoldaki uyarıları tetiklemek için standart çıktıda (stdout) veya hata çıktısında (stderr) aranacak dizeleri ayarlayabilirsiniz.
- Bir komut dosyası bileşeni kullanmak için, önce yıldız simgesini tıklatarak bileşen listesinde favori olarak işaretleyin. Daha sonra hızlı iş ve zamanlanmış iş listelerinde görünecektir.

## Bileşenleri düzenleme

İthal edilen veya ComStore'dan eklenen bileşenler doğrudan değiştirilemez; Panda Sistemleri Yönetimi, yalnızca yönetici tarafından geliştirilen bileşenlerin doğrudan değiştirilmesine izin verir.

İçe aktarılan veya ComStore'dan eklenmiş bir bileşeni değiştirmek ve yönetmek için ağır gereksinimlerine uyarlamak için:

- Genel menü Bileşenleri'nde, bileşeni kopyalamak için belgeler(documents icon)  simgesini tıklatın.

- İlgili düzenleme komutunu, adını ve diğer özelliklerini düzenleyebileceğiniz bileşen düzenleme penceresi açılacaktır.

- Önceden kopyalanmış bir bileşeni düzenlemek için adını tıklayın. Bir bileşenin adını tıklayamazsanız, daha önce kopyalanmadığı için.

## Varlık Denetimi(Assets Audit)

Panda Systems Management, tüm donanım ve yazılım varlıklarınızı kataloglamanıza yardımcı olur ve yeni cihazların görünümünü ve şirketin edindiği ücretli lisansları izleyerek üzerlerinde kurulu olan yazılımı izler.

Tüm bu özellikler sekme çubuğundaki Denetim sekmesinden erişilebilir.

- Hesap Düzeyindeki denetim özelliklerine erişmek için genel menü Hesap, Denetim sekmesine gidin.

- Site Düzeyindeki denetim özelliklerine erişmek için, Genel menüler Sites menüsüne gidin, bir site seçin ve Denetim sekmesine tıklayın.

- Cihaz Düzeyindeki denetim özelliklerine erişmek için Genel menülere gidin, bir site seçin, bir cihaz seçin ve Denetim sekmesine tıklayın.

Denetim sekmesi seçilen seviyeye bağlı olarak daha ayrıntılı veya genel bilgiler gösteren üç seviyede (Hesap, Site ve Cihaz) kullanılabilir.

- **Donanım:** Müşterinin ağındaki cihazlar, yüklü donanım vb.

- **Yazılım:** Ajan yüklü olan cihazlardaki yazılım.

- **Lisanslar:** Kullanılan yazılım lisanslarının ayrıntıları.

- **Hizmetler:** Windows bilgisayarlarda yüklü olan hizmetleri ve durumlarını gösterir.

- **Değişiklikler:** Kayıt sistemi, yazılım ve donanım değişiklikleri.

### Seçilen seviyeye bağlı olarak bilgiye erişim

Seçilen bölümlere (Hesap, Site veya Cihaz) bağlı olarak belirli bölümler kullanılabilir. Aşağıda, seçilen seviyeye göre mevcut bilgi türüne sahip bir tablo bulunmaktadır.

Bölüm / Seviye	Hesap	Site	Cihaz
Donanım	EVET	EVET	EVET
Yazılım	EVET	EVET	EVET
Lisanslar	EVET	EVET	HAYIR
Hizmetler	HAYIR	HAYIR	EVET
Değişiklikler	HAYIR	HAYIR	EVET

## Donanım denetimi

### Hesap Seviyesi

u, tüm hesaplar için yönetilen cihazlarda kullanılan donanım platformlarını (modelleri) gösterir. Bir cihazın platformu, özel veya klonlanmış cihazlarda ana kartın marka ve modeline ve PC'lerin ve cihazların montajcılarının ticari adı ve modeline rastlar.

Her platform için cihaz sayısını da göreceksiniz.

Panda Systems Management tarafından yönetilen cihazları seçilen kriterlere göre görüntülemek için platforma tıklayın.

### Site Düzeyi

Bu, müşterinin ağında bulunan yönetilen donanım hakkındaki bilgileri iki farklı bölüme ayrılarak gösterir:

#### Yönetilen cihazlar

Modelde gruplandırılmış olan ağdaki Panda Systems Management tarafından yönetilen cihazların bir listesini içerir.

Modellerine göre gruplandırılmış cihazların listesini görmek için Model'i tıklayın.

#### Yönetilmeyen cihazlar

Panda Systems Management tarafından yönetilmeyen, ancak yöneticinin denetim amacıyla Konsolda görmek istediği ağ aygıtlarının el ile yönetilen bir listesini içerir.

Yönetilmeyen cihazla ilgili bilgileri girmesi için yöneticiye bir form görüntülemek için + simgesini tıklayın.

Please enter unmanaged device information below:

Model\*:

Manufacturer\*:

Quantity\*:

Serial No. :  Description :

## Cihaz seviyesi

Cihaz Seviyesi denetimleri, seçilen cihazla ilgili tüm bilgileri görüntüleyen en detaylı olanlardır.

Denetim sekmesinin içeriği, cihazın türüne bağlı olarak değişir. Görüntülenen bilgiler aşağıdaki gibi olacaktır:

### Windows, Linux ve OS X için

Alan	Açıklama
Ana bilgisayar adı	Cihaz adı
UID	Cihazın dahili kimliği
İşletim sistemi	Aygıtta yüklü işletim sistemi ve iç sürüm
Anakart	Anakart marka ve model
BIOS adı	BIOS üreticisi
BIOS Sürümü	
BIOS Release Date	
İşlemci	İşlemci yapmak ve model
Bellek	Boş ve kullanılan bellek yuvalarının yanı sıra parça numarası, seri numarası, kapasite ve hız sayısı
Görüntü Bağdaştırıcısı	Ekran kartı modeli ve modeli
Depolama	Sabit diskler ve kurulu yerel depolama kaynakları hakkında bilgi: Disk Sürücüsü, Boyut, Ücretsiz ve Açıklama
Monitörler	Bağlı monitörün modelini yapmak ve modeli
Ağ Bağdaştırıcıları	Network card information: make and model, Mac address and interface speed

### Android ve iOS sistemleri için

Alan	Açıklama
Ana bilgisayar adı	Cihaz adı
UID	Cihazın dahili kimliği
İşletim sistemi	
IMEI	Mobil cihaz kimliği
Model	Akıllı telefon veya tablet modeli
ICCID	SIM kart kimliği
Şebeke	Telefon hizmeti veren şirket
Numara	Telefon numarası
Ağ adaptörü	Ağ kartı bilgileri: mantıksal tanımlayıcı, Mac adresi ve arayüz hızı



## ESXi sistemleri için

Alan	Açıklama
Ana bilgisayar adı	Cihaz adı
UID	Cihazın dahili kimliği
İşletim Sistemi	
İşlemci	İşlemci yapmak ve model
Ziyaretçi bilgisi	ESXi sunucusunda oluşturulan sanal makineler hakkında bilgi: Ana Bilgisayar Adı, Misafir Adı, İşletim Sistemi, Veri Deposu, CPU, RAM, Anlık Görüntüler
Memory	Takılı bellek bankaları hakkında detaylı bilgi: Modül, Tip, Parça Numarası, Seri Numarası, Kapasite, Hız
Depolama	Sunucuda yapılandırılan yerel ve uzak veri depoları hakkında ayrıntılı bilgiler: Veri Deposu Adı, Üretici, Dosya Sistemi, Kapasite, Ücretsiz, Abonelik, Durum
Network Adapters	Ağ kartı bilgileri: mantıksal tanımlayıcı, Mac adresi ve arayüz hızı

## Yazılım denetimi

### Hesap seviyesi

Bu, programın adı ve sürümü tarafından düzenlenen müşterinin ağında bulunan cihazlara yüklenen yazılım hakkındaki tüm bilgileri görüntüler.

Yüklemiş olduğunuz aygıtların listesini görmek için bir programın adını tıklatın ve yazılım paketlerini kaldırmak için sürüm yükseltmeleri veya komut dosyalarını çalıştıran grup olarak eylemler gerçekleştirin.

### Site seviyesi

Listelenen programlar, seçilen sitedeki aygıtlara yüklenmiş olanlardır. Bilgi türü, önceki noktadaki Hesap seviyesi için açıklananla aynıdır.

### Cihaz seviyesi

Listelenen programlar seçilen cihaza yüklenmiş olanlardır. Bilgi türü, yukarıdaki Hesap seviyesi için açıklananla aynıdır.

# Lisans denetimleri

## Hesap seviyesi

Lisans denetimlerinin amacı, her bir programın kurulum sayısını belirlemek ve bu sayede şirketin kullandığı lisans sayısını ve satın alınması gerekenleri hesaplamaktır.


Bu amaçla, birkaç programı bir arada gruplamak mümkündür ve Panda Systems Management bu grupları cihazlarda kurulu yazılımlarla karşılaştırır.

## Paketler

Bir grup veya yazılım paketi oluşturmak, gruptaki programlar tek bir varlık olarak lisanslandığında veya satın alındığında anlamlıdır. Örneğin, Microsoft Office paketi, şirketlerin normal olarak ayrı olarak satın almayacağı çeşitli programlar içermektedir (Word, Excel, PowerPoint vb.). Bu durumda, bu programlardan birinin yüklü olması, paketin tamamı için lisans satın alma ihtiyacını gösterir.

Çeşitli yönetilen sitelerde ortak yazılım kullanılıyorsa, Hesap Düzeyinde paketlerin oluşturulması önerilir. Bu şekilde, her bir sitede paket tanımlarının çoğaltılmasını önlemenin en etkili yolu, tüm olası yazılım paketlerini Hesap düzeyinde tanımlamak ve bunları gerekli Saha seviyelerinde etkinleştirmektir.

## Bir yazılım paketi oluşturma

İlgili tüm bilgileri içeren bir pencereyi görüntülemek için simge çubuğunu tıklayın  :

- **İsim:** Yazılım paketinin adı.
- **Arama:** Panda Systems Management hesabı aracılığıyla yönetilen cihazlarda yüklü olan tüm programların bir listesinde belirli bir program bulun.
- **Tümü:** Arama alanında seçilen kriterlere uyan tüm programları seçin.
- **Spesifik:** Listedeki belirli bir programı (ve sürümü) seçmenizi ve pakete dahil etmenizi sağlar.

Paket oluşturulduktan sonra, paket, paketin içerdiği programlar ve paketteki programlardan herhangi birine sahip olan hesaptaki cihaz sayısı dahil olmak üzere, yazılım paketleri listesinde görüntülenir.

## Site seviyesi

Site düzeyinde, yalnızca sitede bulunan aygıtlarda yüklü olan yazılımlar için de Hesap düzeyinde olduğu gibi paketler oluşturabilirsiniz.

Ayrıca, Site düzeyinde sadece yazılım paketlerini tanımlamakla kalmaz, aynı zamanda Hesap düzeyinde tanımlanmış olanları da kullanamazsınız, ayrıca siteye izin verilen maksimum kurulum sayısını tanımlayabilirsiniz.

Bu şekilde, belirli bir paketi kullanan aygıtların sayısı, konsoldaki yönetici tarafından yapılandırılan kullanılabilir lisans sayısını aştığında, daha fazla lisans alma gereksinimi konusunda yöneticiyi uyaracak bir uyarı tetiklenir.

### Bir yazılım paketi oluşturma

Bir yazılım paketi oluşturma süreci, Hesap seviyesi için açıklananla aynıdır.

### Hesap düzeyinde oluşturulan bir yazılım paketini içe aktarma

Hesap düzeyinde ve Site düzeyinde oluşturulan tüm yazılım paketlerini görüntülemek için simge çubuğunu tıklayın. Siteye içe aktarılabilecekleri seçmek için onay kutularını kullanın.

## Maksimum lisans sayısını yapılandırma

Yazılım paketlerini ekledikten sonra, aşağıdaki bilgilerle birlikte bir tablo görüntülenir:

- **Yazılım paketi:** Yapılandırılmış yazılım paketi. Paket ayarlarını düzenleyebileceğiniz bir pencere açmak için adı tıklayın.
- **Miktar:** Paketin içindeki yazılımın yönetilen sitede bulunan cihazlarda görülme sayısı.
- **Uyarı:** İzin verilen maksimum kurulum sayısı. Yükleme sayısı bu miktarı aşarsa, yöneticiye bir uyarı gönderilir.

## Services audit

### Cihaz seviyesi

Bu, bir cihaza yüklenen hizmetleri geçerli durum ve başlangıç tipi ile birlikte görüntüler.

- **Görünen ad:** Kullanıcının gördüğü servisin adı.
- **Servis adı:** Servisin dahili adı.
- **Son denetimdeki durum:** Cihazın en son denetlendiği zaman servis durumu (çalışma, durdurulan).
- **Başlangıç türü:** Servis başlangıç yapılandırması (Otomatik, manuel, devre dışı).

# Değişiklikler denetimi

## Cihaz seviyesi

Bu, cihazda yapıldığı tarihle birlikte yapılan donanım ve yazılımdaki değişiklikleri gösterir.

Bu, yöneticilerin, bilgisayarda yapılan değişikliklerle ilgili olabileceğinden, doğru şekilde çalışmayan aygıtlardaki sorunları tanılamasını sağlar.

Değişiklikler üç blok halinde gruplandırılmıştır:

- **Sistem Değişiklikleri:** Bu, cihazdaki işletim sistemi modüllerinde yapılan değişiklikleri gösterir.
- **Yazılım Değişiklikleri:** Bu, yüklenen, güncellenen veya cihazdan silinen yazılımları gösterir.
- **Donanım Değişiklikleri:** Bu, cihazdan yüklenen veya cihazdan kaldırılan donanımı gösterir.

## Biletleme(Ticketing)

Yönetilecek cihaz sayısındaki artış ve problemleri çözmek için atanan teknisyen sayısının artması, BT Departmanı tarafından ele alınan her bir davanın belgelenmesini ve koordine edilmesini sağlayan bir sistemin uygulanmasını gerektirir.

Biletleme sistemleri, her olayı, kapatılıncaya kadar oluşturulduğu andan itibaren takip ettiği tüm ara durum durumlarını kaydetmek için kullanılır.

Bu nedenle, orijinal teknisyen mevcut değilse ya da görev çok özel bir bilgi gerektiriyorsa, tüm dokümantasyonu saklamak ve belirli bir teknisyene bir vaka atamak ve bir diğerine yeniden atamak mümkündür ve o zamana kadar kaydedilen ilerleme ve aynı sorun hakkında bilgi için tekrar gereksinimleri ile son kullanıcıya kesintileri en aza indirir.

İkincisi, olayların belgelenmesini zorlamak, prosedürün gelecekte yeniden kullanılmasına ve açık vakalar için yanıt süresini en aza indirerek ince ayar yapılmasına izin verir.

Son olarak, bir bilet sistemi, BT Departmanının iş yükünü tanımlamanıza, belirli bir zamanda açık olan biletleri filtrelemenize ve gerektiğinde daha fazla kaynak atamanıza olanak tanır.

## Biletin tanımı

Her bilet, onu tanımlayan bir dizi alan içerir:

**Ticket 3b570001-9**

---

**Creator:** BIODKELLY  
**Profile:** Bilbao Office  
**Date Created:** 2013-05-21 21:23:22 SST  
**Status:** Closed (change)  
**Severity:** 5(change)  
**Assigned To:** panda.test (change)

---

**Summary:** I cannot print a document  
**Content:** Can you help me as soon as possible

---

**Comments:** [Add a new comment to this ticket](#)

panda.test added a comment at 2013-05-21 21:24:57 SST  
**We are on it, I am going to connecto to you machine now**

panda.test added a comment at 2013-05-21 23:07:57 SST  
**Another comment**

panda.test added a comment at 2013-05-21 23:08:17 SST  
**another comment**

added a comment at 2013-05-21 23:08:45 SST  
**sdcsd**

1 2 Next

- **Oluşturan(Creator):** Ticket yaratıcısı. Bir aygıt (bir kullanıcı tarafından Agent'dan oluşturulmuşsa) veya sistem hesabı (bir monitör tarafından oluşturulmuş ve bir teknisyene atanmışsa) olabilir.

- **Site:** Biletin ait olduğu cihaz grubu

- **Oluşturulma Tarihi(Date Created):** Biletin yaratılış tarihi.

- **Durum(Status):** Dört durum vardır:

- **Yeni:** Sorunun açıklanmasıyla birlikte yeni oluşturulmuş ve atıcıya atanmış bilet. Henüz bir görev yapılmadı.
- **Devam ediyor:** BT Departmanından atanan teknisyen olayı yönetiyor.
- **Bekliyor:** Olayın çözümü harici nedenlerle durduruldu (bilgi eksikliği, kullanıcılar veya başkaları tarafından yapılan değişiklikleri onayla).
- **Tamamlandı:** Olay çözüldü ve kapatıldı.

- **Önem derecesi(Severity):** Biletin şiddeti. Bir monitör tarafından oluşturulmuşsa, kendisine verilen önem kopyalanır.

- **Atanan(Assigned to):** Olayı çözmek için atanan teknisyen.

- **Özet(Summary):** Olayın özeti.

- **İçerik(Content):** Olayın tanımı.

- **Yorumlar(Comments):** Bu alanda, hem teknisyen hem de kullanıcı olayı tamamlayan ve güncelleyen girişler ekleyebilir.

## Bilet oluşturma(Creating a ticket)

Biletler üç şekilde oluşturulmuştur:

- Kullanıcı tarafından manuel olarak bilgisayarında yüklü olan aracıyı oluşturur.

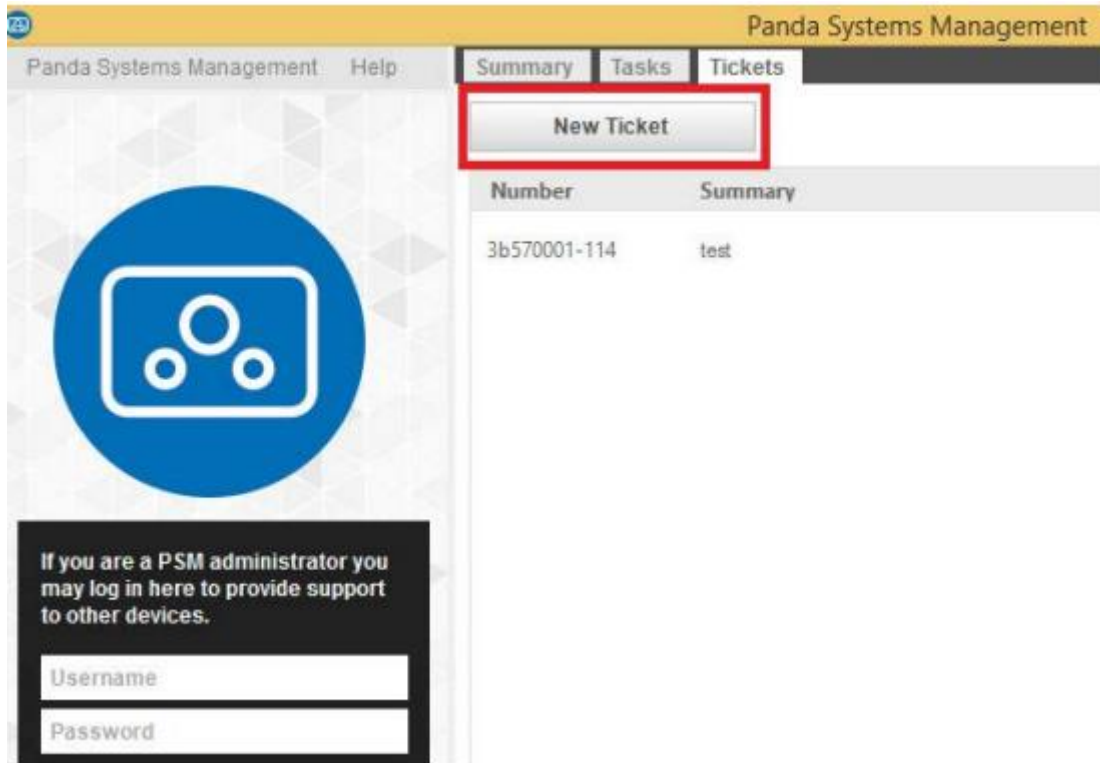
- Bir kullanıcının cihazında bir anormallik olarak tanımlanan bir durumu algılayan bir monitörden otomatik olarak.

- Konsoldan IT departmanı tarafından manuel olarak.

## Ajandan kullanıcı tarafından manuel olarak

Kullanıcı cihazın düzgün çalışmadığını fark ederse ve belirtilerin yazılı bir kaydını bırakmak isterse.

Bir biletin manuel olarak kaydedilmesi için, kullanıcının simgesini sağ tıklatması, Aç'ı seçin ve Biletler(Tickets), Yeni Bilet Aç'ı(Open a New Ticket) seçin.

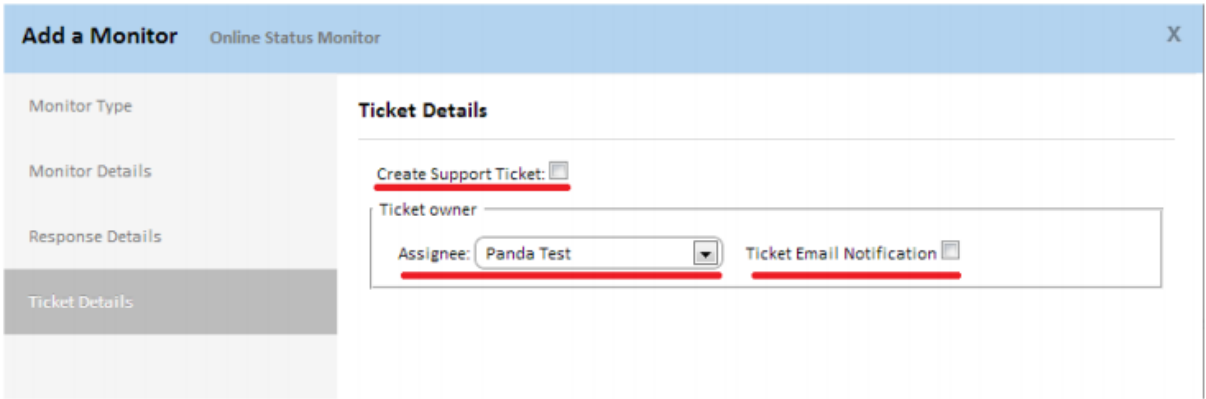


Bilet oluşturulduktan sonra yeni yorumlar eklenebilir ve kapatılabilir.



## Bir kullanıcının cihazında anormallik olarak tanımlanan bir durumu algılayan bir monitörden otomatik olarak

Bu, bir izleme politikası tanımlanırken, Bilet Detayları sekmesinde yapılandırılabilir.



Bu durumda, atanmış teknisyeni seçebilir ve biletin oluşturulduğunu bildiren bir e-posta oluşturulacaktır.

## Konsoldan IT Departmanı tarafından manuel olarak yapma

Bu özellik, BT personelinin hatırlatıcıları ayarlamasına ve Departmanın kuyruğuna görev eklemesine izin verir.

Konsoldan bir bilet oluşturmak için şu adımları izleyin:

- Biletin şu anda yaratılması gereken Seviyeyi belirleyin:

- Hesap Düzeyinde bir bilet oluşturmak için genel menü Hesap, Destek sekmesine gidin.
- Site Düzeyinde bir bilet oluşturmak için, genel menüler Sites menüsüne gidin, bir site seçin ve Destek sekmesine tıklayın.

- Yeni bilet'e(New Ticket) tıklayın

The screenshot shows the 'Systems Management' web interface. The top navigation bar includes 'ACCOUNT', 'SITES', 'COMPONENTS', 'COMSTORE', 'SCHEDULED JOBS', 'SCHEDULED REPORTS', 'HELP', and 'SETUP'. The 'SITES' menu is expanded, showing 'Pruebas Beta > Support'. A 'New Ticket' button is highlighted with a red box. Below it, the 'Site: Pruebas Beta' section is visible, with tabs for 'SUMMARY', 'DEVICES', 'AUDIT', 'MANAGE', 'MONITOR', 'SUPPORT', 'REPORT', 'POLICIES', and 'SETTINGS'. The 'SUPPORT' tab is active, showing a list of tickets. The list has columns for 'Number', 'Site', 'Created by', 'Summary', 'Description', 'Priority', 'Status', 'Create Date', 'Assigned To', and 'Synced'. Two tickets are visible, both for 'Pruebas Beta' and 'VMBETA-W8132', with a priority of 3 and status of 'New'. The first ticket (3b570001-122) was created on 2016-09-06 at 14:13:12 CEST, and the second (3b570001-121) was created on 2016-09-05 at 14:23:12 CEST. Both tickets are assigned to 'panda.test'.

Bu durumda, biletin ve içeriğinin önem derecesini belirtebilir ve çözülecek veya yeniden atanacak bir teknisyene atayabilirsiniz.

## Bilet Yönetimi (Ticket Management)

Önceden oluşturulmuş olan biletler, sekme çubuğundan, Site, Hesap veya Cihaz düzeyinde Destek'ten yönetilir.

Eylem çubuğundaki simgeler, bilet listesini (Açık Biletler, Biletlerim, Tüm Biletler) filtrelemenize veya durumlarını kalem simgesiyle düzenlemenize izin verir. Atanan ciddiyeti, durumu ve teknisyeni değiştirmek için Bilet numarasını tıklayın.

## Yama Yönetimi (Patch Management)

### Yama yönetimi(Patch Management) nedir?

Yama yönetimi, yamaların ve yazılım güncellemelerinin merkezi olarak dağıtımı ve yüklenmesi için bir dizi kaynaktır.

Yama yönetimi yalnızca yazılımların cihazlarındaki günlük güncellenmesini kolaylaştırmakla kalmaz, aynı zamanda güncellemeleri olmayan veya bilinen güvenlik açıkları olan cihazların hızlı ve kolay bir şekilde görüntülenmesi için denetimler gerçekleştirmenizi de sağlar.

Yama yönetimi ile yönetici, ağ güvenliğini güçlendirebilir ve yazılım hatalarını en aza indirerek tüm cihazların yayınlanan en yeni yamalarla güncellendiğinden emin olabilir.

### Hangi yamaları dağıtabilirim / uygulayabilirim?

Microsoft tarafından Windows Update aracılığıyla yayınlanan tüm yamalar ve güncellemeler, Panda Systems Management aracılığıyla merkezi olarak yönetilebilir.

Microsoft, şu anda desteklenen tüm Windows işletim sistemleri ve geliştirdiği yazılımlar için güncellemeler yayınlamaktadır:

- Microsoft Office
- Microsoft Exchange



- SQL Server
- Windows Live
- Windows Defender
- Visual Studio
- Zune Software
- Virtual PC
- Virtual Server
- CAPICOM
- Microsoft Lync
- Silverlight
- Windows Media Player
- Diğer...

## **Yama dağıtımı ve yükleme**

Panda Sistemleri Yönetimi, birbirinden bağımsız iki tamamlayıcı Yama Yönetimi yöntemini içerir. Her birinin, tüm olası ihtiyaçlara ve / veya senaryolara uyum sağlamak için farklı işlevleri vardır:

- Windows Güncellemeleri politikası.
- Yama Yönetimi politikası.

## **Yöntem I: Windows Update ilkesi**

Windows Update politikaları, ağdaki her Windows aygıtının Denetim Masası'ndan erişilebilen Windows Update hizmetinin merkezi yapılandırmasına izin verir.

Yöneticinin, ağdaki tüm Windows cihazlarının işletim sistemi ve Microsoft yazılım güncellemeleri konusunda nasıl davranacağını kontrol etmesine izin verirler.

Bir politika olduğu için, bu yöntemle desteklenen gruplama düzeyleri Hesap Düzeyi ve Site Düzeyi'dir.

## **Windows Update Policy yöntemine erişim**

Bu yöntemle erişmek için Site Düzeyinde veya Hesap Düzeyinde bir Windows Güncelleme politikası oluşturun.

Oluşturulan ilkeden etkilenen tüm aygıtlarda Windows Update davranışını merkezi olarak yapılandırabileceğiniz bir ekran görünür.

Windows Update ilkeleri, her Windows uygulamasında Windows Update kaynakları ile aynı şekilde yapılandırılmıştır.

Windows Update, aldığı yamaları üç kategoriye ayırır:

- **Önemli (Important)**
- **Tavsiye edilen (Recommended)**
- **İsteğe bağlı (Optional)**

Sadece önemli ve önerilen yamalar otomatik olarak yüklenebilir. Yamaların geri kalanı, kullanıcının cihazından veya diğer yama yönetim yöntemlerini kullanarak Panda Systems Management'dan manuel olarak kurulacaktır.

Aşağıda bu tür politikalar için uygun ayarlar bulunmaktadır:

- **Hedef Ekle(Add Target):** Politikanın uygulama kapsamını sınırlandıran filtreler veya gruplar eklemenizi sağlar.

- **Yama İlkesi(Patch Policy):** Microsoft tarafından “Önemli” olarak sınıflandırılan yamalar ile ilgili olarak, her bir aygıtta Windows Update'in genel davranışını belirtir:

- Otomatik olarak indir ve yükle.
- Kullanıcı tarafından elle indirme ve seçim.
- İndirmeden bildir.
- Windows Güncellemesini Devre Dışı Bırak.

- **Yeni güncellemeleri yükle(Install new updates):** Yamaların ne zaman yükleneceğini belirtir.

- **Önerilen güncelleştirmeleri, önemli güncelleştirmeler aldığım şekilde ver(Give me recommended updates the same way I receive important updates):** Önemli ve Önerilen yamalar için Düzeltme ilkesinde seçilen ilkeyi uygular.

- **Tüm kullanıcıların bilgisayarda güncellemeleri yüklemesine izin ver(Allow all users to install updates on the computer):** Kullanıcının yamaları elle yüklemesine izin verir.

- **Microsoft ürünleri için güncellemeler verin ve Windows'u güncellerken yeni isteğe bağlı Microsoft yazılımlarını kontrol edin(Give me updates for Microsoft products and check for new optional Microsoft software when updating Windows):** İsteğe bağlı yamalar için kontroller, genellikle diğer Microsoft ürünleri için yamalar.

- **Yeni Microsoft yazılımı mevcut olduğunda bana ayrıntılı bildirimleri göster(Show me detailed notifications when new Microsoft software is available):** Yeni Microsoft yazılımı mevcut olduğunda kullanıcıya detaylı bildirimler gösterilir.

- **Zamanlanmış otomatik güncellemeler yüklemeleri için oturum açmış kullanıcılarla otomatik yeniden başlatma(No auto-restart with logged on users for scheduled automatic updates installations):** Bu seçenek seçilirse, yamalar uygulanır ve kullanıcıya yeniden başlatma

ihtiyacı bildirilir. Etkin değilse, yama yüklenecek ve kullanıcıya cihazın 5 dakika içinde yeniden başlatılacağı bildirilecektir.

- **Yeniden zamanlanmış kurulumlarla yeniden başlatmayı isteme(Re-prompt for restart with scheduled installations):** Windows Update'den önce kullanıcıya, uygulamayı gerektiren yamalar yüklenmişse, cihazı yeniden başlatmasını isteyen süreyi tanımlar.

- **Zamanlanmış kurulumlar için gecikmeli yeniden başlatma(Delay restart for scheduled installations):** Sistemin yamaları yükledikten sonra yeniden başlatmak için bekleyeceği süreyi tanımlar. Hiçbir şey belirtilmemişse, varsayılan değer kullanılır: 15 dakika.

- **WSUS:** Her ağ aygıtının tek tek yamaları indirmeyi en aza indirmek için alternatif bir yerel veya uzak Windows Server Update Services sunucusuna izin verir.

- WSUS Sunucusu kullanırken Microsoft'un Yamalama veya Arama için herhangi bir bağlantısına izin vermeyin: Yöneticinin ağda bir WSUS sunucusu kurulu olması durumunda, bu seçenek, WSUS sunucusu olmadığı Microsoft ağında yamaları aramayı engeller.
- İstemci Tarafı Hedeflemeyi Etkinleştir: İstemci Tarafı Hedefleme etkinleştirilmiş bir WSUS sunucusu kullanılıyorsa, içerdikleri gruplar ve aygıtlar WSUS sunucusunda manuel olarak tanımlanır. Bu parametre, ilkenin uygulandığı aygıtın ait olduğu grupları belirtmenize izin verir (bir noktalı virgülle ayrılmış).

### **Windows Update yöntemi: Kullanım senaryoları**

- Yöneticinin tüm önemli yamaların tüm ağ aygıtlarına otomatik olarak yüklenmesini sağlaması gerektiğinde, son kullanıcı işlemi engellemeden.

- Yönetici daha fazla bakım gerektirmeyen merkezi bir yama yönetimi politikasını hızlı bir şekilde dağıtmak istediğinde.

- Ağdaki tüm bilgisayarlar birbirine çok benzediğinde ve yama hariç tutmayı gerektiren hiçbir koşul olmadığında

- İsteğe bağlı olarak sınıflandırılan yamaların otomatik olarak kurulmasına gerek yoktur.

### **Yöntem 2: Yama Yönetimi ilkesi**

Yama Yönetimi ilkeleri, Windows Update ilkelerine benzer bir şekilde yamaların otomatik olarak yüklenmesine izin verir.

Temel fark, yüklenecek yamaların nasıl yönetileceğidir. Windows Update yöntemi, yamaları seviyeye göre uygulamanıza izin verirken (Önemli, Önerilen veya İsteğe Bağlı), Yama Yönetimi, çok özel koşullara dayalı olarak uygulanacak yamaları seçmenize ve ayrıca, yama aygıtının yüklenmesinden sonra hedef aygıtın yeniden başlatılıp başlatılmayacağını belirlemenizi sağlar.

Bir politika olduğu için, bu yöntemle desteklenen gruplama düzeyleri Hesap Düzeyi ve Site Düzeyi'dir.

## Genel iş akışı ve Yama Yönetimi ilkesi geçersiz kıl

Orta ve büyük ağlarda, Hesap Düzeyinde tanımlanan genel Yama Yönetimi ilkesiyle uyumsuz olabilecek belirli koşulların ve senaryoların sayısı oldukça anlamlı olabilir. Bu, yöneticilerin ağda özel durumlar olduğu kadar Yama Yönetimi ilkelerini tanımlamasını zorlayabilir. Bu, özellikle farklı profillere ve sorumluluklara sahip kullanıcılar tarafından kullanılan çoklu cihazlara sahip heterojen ağlarda, bakım görevlerini büyük ölçüde artırır.

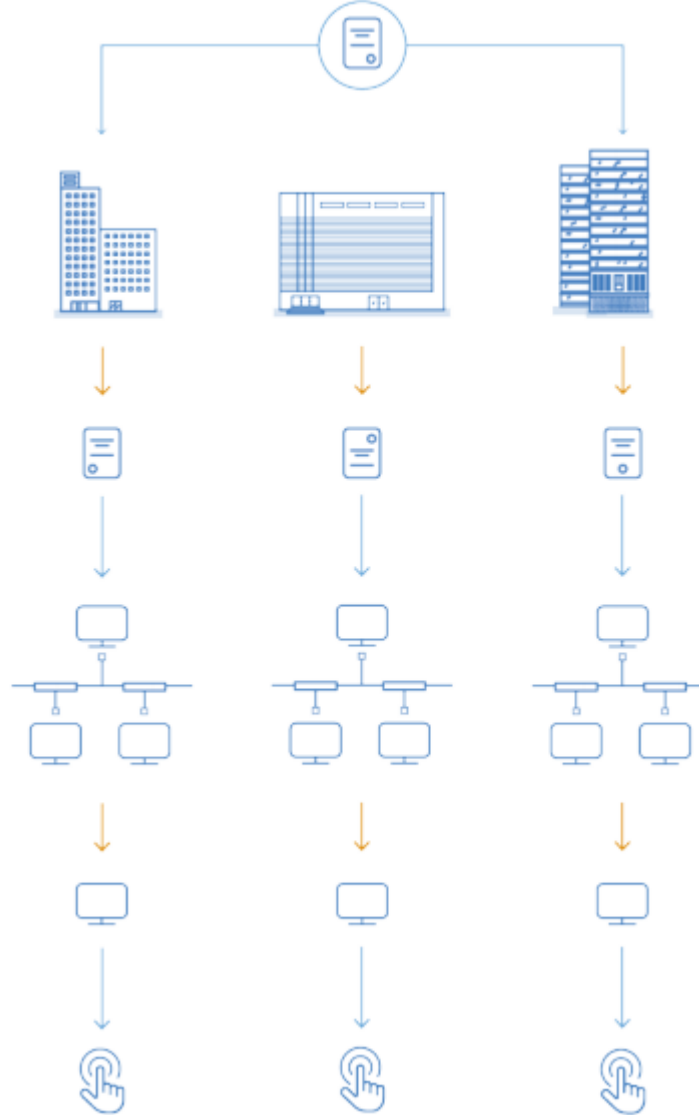
Bu nedenle, Panda Systems Management, sistemdeki diğer politikalardan tamamen farklı Yama Yönetimi politikaları için bir iş akışı oluşturulmasına izin verir. Bu iş akışının amacı, ağdaki her bir ağıta yüklenecek yamaları tanımlamak için esneklikten ödün vermeden Yama Yönetimi ilkelerini oluşturmayı hızlandırmaktır.

Aşağıdaki şekil iş akışı aşamalarını göstermektedir:

### Account Level

#### Policy definition

Create a policy for all devices in all of your company's offices/sites.



### Site Level

#### Policy override

Override the Account-Level policy per site.

### Device Level

#### Manual override

Manually override the policy per device if necessary.

İş akışı üç aşamaya ayrılabilir:

### **Hesap Düzeyinde Yama Yönetimi ilkesi oluşturma**

En genel düzeyde tüm aygıtlarınızı kapsayan ve varsayılan en yaygın ayarları uygulayan bir Yama Yönetimi ilkesi belirtin.

Hesap yalnızca bir Site varsa, bu adım gerekli olmayacaktır.

Bir Yama Yönetimi ilkesini yapılandırma hakkında bilgi için kılavuzda daha sonra Yama Yönetimi ilkesi oluşturma bölümüne bakın.

### **Politikanın Site Düzeyinde geçersiz kılınması**

İhtiyaçlarınıza göre Site Düzeyindeki politikayı geçersiz kılın. Konsoldaki diğer politikalardan farklı olarak, Hesap Düzeyinde tanımlanan Yama Yönetimi politikaları kısmen değiştirilebilir. Bu, her bir Site için, daha yüksek düzeyde yaratılmış olanı geçersiz kılan tamamen yeni konfigürasyonlar yaratma ihtiyacını ortadan kaldırır. Hesap Düzeyinden devralınan ayarlar, hedeflenen cihazları her zaman koruyarak kısmen değiştirilebilir.

### **Cihaz başına yama politikası geçersiz kılma**

Son olarak, belirli bazı aygıtlar için küçük ayarlamalar yapmanın gerekli olabileceği durumlar için, tanımlanan Yama Yönetimi ilkesini Aygıt Düzeyinde değiştirebilirsiniz.

Ayrıca, belirli bir cihaza atanan politikayı, sitenin ait olduğu Politikalar sekmesinden de devre dışı bırakabilirsiniz. Bu, Hesaptaki tüm diğer cihazlar için tanımlanmış olandan tamamen farklı bir Yama Yönetimi ilkesi gerektiren cihazlar için çok kullanışlıdır.

## **Yama Yönetimi ilkesi oluşturma**

Site Düzeyinde veya Hesap Düzeyinde bir Yama Yönetimi ilkesi oluşturmak için İlkeler sekmesini tıklayın ve ilke türünde Yama Yönetimi'ni seçin.

Oluşturulan ilkeden etkilenen tüm aygıtlar için yama yönetiminin davranışını merkezi olarak yapılandırabileceğiniz bir ekran görünür.

### **Yama onayı ve öncelik sırası**

Yama Yönetimi ilkeleri, yama yüklemelerini otomatik olarak izin vermek veya reddetmek için filtre ve koşulları ayarlamanızı sağlar. Bu filtreler, Microsoft tarafından yayınlanan eklere eşlik eden meta verileri alır ve bunları yükleyip yüklememeye karar vermek için değerlendirir.

Bir ya da birden fazla aygıt üzerinde bir yamanın ya da bir grup yamanın yüklenmesine izin vermek ya da reddetmek için bunları onaylamanız gerekir. Bu, Yama Yönetimi ilkesi yapılandırma işleminin bir parçasıdır:

- **Yamaları onaylayın:** Bir yamayı onaylamak, tüm hedeflenen cihazlarda, politikada tanımlanan bir sonraki yama penceresinde yüklenmesini işaretler.

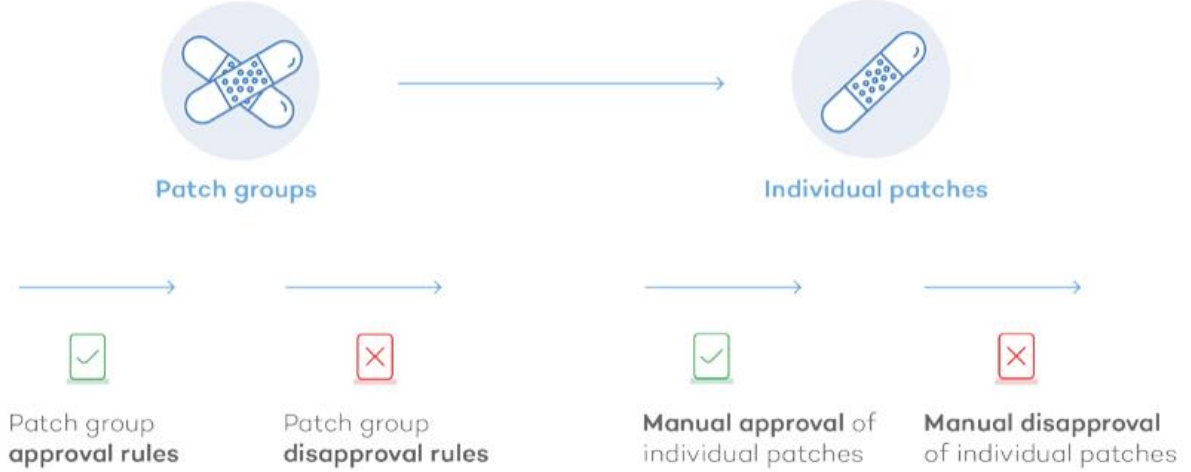
- **Yamaları onaylamayın:** Onaylanmamış yamalar, cihaz yama işlemlerinden süresiz olarak hariç tutulur.

Onaylamak veya onaylamamak için seçim yapabilirsiniz:

- **Yama grupları:** Bu gruplar, yönetici tarafından bir veya daha fazla yamayı gruplandırmak için oluşturulan kurallarla tanımlanır. Örneğin: "Tüm Kritik yamalar yayınlandı". Konsol, yamalar için çok sayıda filtreleme özneliği ve doğru, karmaşık ölçütler oluşturmak için bunları birleştirmek için mantıksal işlemler sağlar.

- **Bireysel yamalar:** Onaylamak veya onaylamamak için belirli bir yamayı elle seçebilirsiniz.

Bu, aşağıdaki öncelik sırasına göre aşağıdaki dört kombinasyon ile sonuçlanır:



Her aşama bir öncekine göre önceliklidir. Örneğin: Bir grup kuralı daha sonra bireysel düzeyde reddedilen bir yamayı onaylarsa, ikincisi geçerli olacaktır.

## Yama Yönetimi ilkesini yapılandırma

Bunlar bir Yama Yönetimi ilkesi için mevcut ayarlardır.

- **Hedefler:** Politikanın uygulama kapsamını sınırlandıran filtreler veya gruplar eklemenizi sağlar. Politikanın oluşturulduğu Seviyeye bağlı olarak (Site Düzeyi veya Hesap Seviyesi), farklı filtreler ve cihaz grupları gösterilecektir.

- **Zamanlama seçenekleri:** Yamalar uygulanacak ve yama penceresi süresini belirleyeceğiniz zaman seçmenizi sağlar.

- **Schedule:** Yama penceresini tanımlamanızı sağlar. Yama yükleme aralığını ve sıklığını seçebileceğiniz bir form görüntülemek için Zaman Çizelgesi Seç'in yanındaki Değiştir düğmesini tıklatın.

Choose when you want the policy to run.

At selected date and time

Daily

Weekly

Monthly

Monthly Day of Week

Yearly

Start: 24 February 2016 10 : 23

*This policy will run once at the date/time indicated above.*

OK Cancel

Bir frekans seçin. Sağdaki panel, ağ yöneticisinin yamaların yüklenmesi gerektiğinde kesin zamanları ve tarihleri belirtmesine izin verecek şekilde değişecektir.

- **Süre:** Yama işleminin ne kadar süreceğini ayarlar. Yama işlemi belirlenen süreyi aşarsa, politika bir hatayla kesintiye uğrayacaktır.

- **Yama konumu:** PCSM araçlarının kurulacak yamaları toplamasını istediğiniz deposu seçmenizi sağlar.

- Windows Güncellemesi'nden yama indirin: Hedeflenen cihazlar yamaları indirmek için Windows Update sunucusuna bağlanır.
- Yerel bir önbellek kullanın: Yamaları indirmek için hedeflenen cihazların yerel önbellek olarak belirlenen cihazı kullanmasına izin verir.
- Aygıtlara Windows Update ile iletişim kurmaya izin verme: Yerel önbellek olarak belirlenen aygıtlar kullanılmıyorsa, hedeflenen aygıtlar gerekli düzeltme eklerini indirmek için Windows Update sunucusuna bağlanır.

- **Yama Onayı:** Yüklenecek yamaları seçmek için filtreler ayarlamınızı sağlar. Mevcut yamalar iki kategoriye ayrılır: Onayla ve Onaylama.

- Bu yamaları onayla: Hedeflenen aygıtlara yüklemek için Microsoft tarafından yayımlanan yamanın özelliklerini temel olarak filtreler tanımlamanıza izin verir.
- Bu yamaları onaylamayın: Yüklemelerini önlemek için Microsoft tarafından yayımlanan yamanın özelliklerini temel olarak filtreler tanımlamanıza izin verir. 'Onaylama' seçimleri, 'Onaylandı' seçimlerine göre önceliklidir.
- Bir filtrenin nasıl tanımlanacağı hakkında bilgi için bu bölümün ilerleyen bölümlerine bakın.

- **Tek tek yamaları yapılandırın:** Yamaları el ile onaylamınızı veya reddetmenizi sağlar.

- **Kullanılabilir:** Microsoft'un dizininde yayınlanan tüm yamaları görüntüler.
- **Onaylayın:** Kurulum için seçilen yamalar.
- **Onaylamayın:** Yüklenmeyen yamalar.

Üç seçenek, aşağıdaki ölçütleri temel olarak yamaları filtrelemenizi sağlayan arama filtrelerini içerir:

- **Önem Derecesi:** Filtrelerin önem derecesine göre yaması: Kritik, Önemli, Orta, Düşük, Belirlenmemiş

- **Yeniden başlatma gerektirebilir:** Yükleme işlemini tamamlamak için yeniden başlatma gerektirebilecek tüm yamaları görüntüler.
- **Kullanıcı girişi gerektirebilir:** Yükleme işlemini tamamlamak için kullanıcı etkileşimi gerektirebilecek tüm yamaları görüntüler.
- **Arama:** Yamaları tanımlayan alanlarda sınırsız arama yapmanızı sağlar.

- **Güç:** Cihazlarınızın yama işleminden önce ve sonra nasıl davranması gerektiğini tanımlamanızı sağlar:

• **Boot (Önyükleme):** Seçildiğinde, yama işlemi ile başlamadan on dakika önce Wake-On-LAN özelliği ile uyumlu tüm hedeflenen cihazları uyandırır.

• **Yeniden başlatma:** Hedeflenen cihazların yama işleminden sonra nasıl davranması gerektiğini tanımlamanıza olanak sağlar:

- **Güç kapat:** Yama program penceresinden sonra hedeflenen cihazları kapatır
- **Aygıtları yeniden başlat:** Gerekirse, ilke çalıştırıldıktan sonra hedeflenen aygıtlar yeniden başlatılır. Bir USB çubuğu programlanmış yeniden başlatma zamanında bağlanırsa, yeniden başlatmaya izin vermez. Bu, sistemlerin bir USB cihazında saklanan işletim sisteminden yeniden başlatılmasını engellemektir. Yeniden başlatma izni seçeneğini seçerek bu davranışı değiştirebilirsiniz.
- **Yeniden başlatma:** Hedeflenen cihazların yama program penceresinden sonra yeniden başlatılmasını durdurur. Son kullanıcıdan 1-12 saat / 1 gün / 2 günde bir yeniden başlatmayı hatırlatmanıza ve son kullanıcının yeniden başlatma hatırlatıcısını reddetmesine ne kadar izin verileceğini ayarlamanıza olanak tanır.

## Bir yama filtresi oluşturma

Düzeltilme Eki bölümü, yöneticilerin gelişmiş ölçütleri seçilen ölçütlere göre grup yamaları olarak tanımlamasına olanak tanıyan bir dizi kaynak içerir.

Yamalar için filtre oluşturmak için mevcut alanlar aşağıda açıklanmıştır:

- **Tümü:** Tüm yayınlanan yamaları seçer

- **Kategori:** Kritik Güncelleştirmeler veya Sürücüler gibi kategorilere göre yamaları filtreler.

- **Açıklama:** Yamaun açıklamasına göre filtrelemenizi sağlar

- **İndirme boyutu**

- **KB Numarası:** Bir düzeltme ekinin ilişkili olduğu belirli Microsoft Bilgi Bankası makale numarasını aramanızı sağlar.

- **Öncelik:** Microsoft Güvenlik Bültenlerinde (Kritik, Önemli, Orta, Düşük, Belirtilmemiş) belirtilen "önem derecesi" öncelikli olarak filtrelenmenizi sağlar. Systems Management Yama Yönetimi ilkeleri, Windows Update'te değil, Güvenlik Bülteni sınıfının önem derecesini gösterir.



- **Yeniden başlatma davranışı:** Yüklemeden sonra nasıl davranışlarına bağlı olarak yamaları filtreler: Yeniden başlatma (0), Her zaman yeniden başlatma gerektirir (1), Yeniden başlatma isteğinde bulunabilir (2)

- **Yayın tarihi**

- **Kullanıcı girişi isteyin:** Kullanıcı girişi gerektirebilecek yamaları filtrelemenize izin verir (Mayıs gerektirebilir) ya da değil (Gerekmiyor)

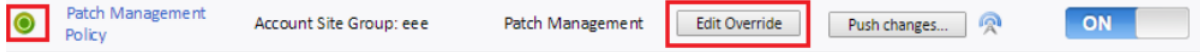
- **Başlık:** Yamaun adına göre filtrelemenizi sağlar

- **Type:** Yama tipine göre filtrelemenizi sağlar. Yazılım veya Sürücü seçin

## Hesap Düzeyinde tanımlanan politikaların geçersiz kılınması

Hesap Düzeyinde oluşturulan yapılandırmanın dışında kalan sitelere özel politikaların oluşturulmasını hızlandırmak için, Panda Systems Management, yöneticilerin tamamen yeni bir ilke oluşturmaya gerek kalmadan bir Hesap Seviyesi politikasının kısımlarını değiştirmesine veya geçersiz kılmasına izin verir. Bu özellik, yöneticilerin sistemi daha hızlı bir şekilde yapılandırmasını ve yönetilecek daha az ilke olacak şekilde bakım görevlerini azaltmalarını sağlar.

Bir Hesap Seviyesi politikasını geçersiz kılmak için, Site'de politikasını değiştirmek istediğiniz Politikalar menüsüne gidin. Ekranın alt kısmında, Hesap Düzeyinde oluşturulan Yama Yönetimi politikalarının bir listesini göreceksiniz. Bu politikalar, sol taraflarında düzenli politikardan ayıran yeşil bir simgeye sahiptir ve Düzenle Geçersiz Kılma(Edit Override) düğmesini görüntüler.



Geçersiz Kılmayı Düzenle düğmesine tıklamak, Hesap Düzeyindeki politikanın ayarlarını seçici olarak değiştirmek için kontrollerin bulunduğu bir ekranı gösterir. Ancak, politikanın adını tıklamak politikanın orijinal ayarlarına götürür.

İlke ayarlarını düzenlemek, orijinal değerleri değiştirmek ve geçersiz kılmak için Geçersiz Kıl düğmesini tıklatın.

## Her cihaz için Yama Yönetimi politikalarını değiştirme

Aygıt Düzeyindeki (Ağdaki her aygıtı temsil eden) Yönet menüsü, bir Yama Yönetimi ilke oluşturma işleminin önceki aşamalarında onaylanmış ve reddedilen düzeltme eklerini değiştirmenize izin verir. Ayrıca, bu ekran Yama Yönetimi ilkesinin çalıştırıldığı tarihi görüntülemenizi ve gerekirse yeniden çalışmaya zorlamanızı sağlar.

## Update Patch Management Policy

Save Cancel

Name: Patch Management Policy  
Policy type: Patch Management  
Created: 2017-01-16 10:18:20 UTC  
Modified: 2017-01-16 10:18:20 UTC (panda.test)

Type	Name
Site Group	eee

### Timing Options

Override  ON

Please ensure that all of your devices are on the latest Agent version.

Schedule:

Duration: Patching runs for 1 hours

### Patch Location

Override  OFF

Bu ekran iki bölüme ayrılmıştır: cihaza uygulanan politikaları görüntülemenizi sağlayan, diğeri ise cihaza atanmış Yama Yönetimi politikası uyarınca onaylanmış ve reddedilen yamaları görmeyi sağlayan bir diğeri bölümdür.

### Device: BIOOLOPEZ - Patch Management

SUMMARY AUDIT **MANAGE** MONITOR SUPPORT REPORT POLICIES

● Patch Management

Operating System: Microsoft Windows 10 Pro 10.0.14393  
Service Pack: 0

Policies:

Name	Last Run	Next Run	Run Now
PMP		Run once at 2017-01-20 10:26	<input checked="" type="button" value="Run Now"/>

*It is not recommended to have more than one Policy targeting a single device.  
Patch approvals or removals are applied during the Update window as specified on the device. This schedule and other settings can be changed using Patch Management Policies at either the Site or Account level.*

#### Operating System Patches

*This list is only updated following a device re-audit.*

- ▶ Approve (0)
- ▶ Installed (20)
- ▶ Do Not Approve (4)

## Atanan Yama Yönetimi politikasının durumu

Bu bölümde, cihaza yüklenen işletim sistemi ve Servis Paketi numarası görüntülenir. Ayrıca cihaza uygulanan politikaları da görüntüler:

- **İsim:** Politikanın adı

- **Son Çalıştır:** Politikanın en son çalıştırıldığı tarih.
- **Sonraki Çalıştırma:** Politikanın çalıştırılmak üzere zamanlandığı tarih.
- **Hemen çalıştır:** Yama politikasını şu anda planlananın dışında çalıştırır

## İşletim sistemi yamaları

Bu bölüm, yöneticilerin belirli bir aygıtta yüklenecek yamaları daha da hassaslaştırmasına izin verir.

Aşağıdaki seçenekler kullanılabilir:

- **Onayla:** Bu cihazda onaylanmak üzere işaretlenmiş olan yamaları işaret eder. Onaylanan yamalar, politika programı penceresinde cihaza aktarılır ve kurulumlarının ardından, Yüklenen adlı bir sonraki listeye taşınır.
- **Yüklendi:** Cihazda onaylanmış ve yüklenmiş yamaları tanımlar.
- **Onaylamayın:** Bu cihazda kurulmaktan çıkarılmış olan yamaları belirtir. Bunu hedefleyen bir yama ilkesi olmayan bir aygıtınız varsa, bu bölüm Microsoft tarafından yayınlanan tüm yamaları içerecektir.

Yukarıda belirtilen bölümlerin her biri, aşağıdaki parametrelere dayanan yamaları aramanıza izin veren arama filtreleri sağlar:

- **Önem Derecesi:** Filtreler önem derecelerine göre değişir: Kritik, Önemli, Orta, Düşük, Tanımlanmamış
- **Yeniden başlatma gerektirebilir:** Yükleme işlemini tamamlamak için yeniden başlatma gerektirebilecek tüm yamaları görüntüler.
- **Kullanıcı girişi gerektirebilir:** Yükleme işlemini tamamlamak için kullanıcı etkileşimi gerektirebilecek tüm yamaları görüntüler.
- **Arama:** Yamaları açıklayan alanlarda sınırsız bir arama gerçekleştirmenizi sağlar.

## Yama Yönetimi yöntemi: Kullanım senaryoları

- Yönetici, her bir cihaza uygulanan yamaları doğru bir şekilde denetlemeyi gerektirdiğinde.
- Yönetici istisnasız tüm yamaları merkezi olarak kurması gerektiğinde, otomatik olarak.
- Yöneticinin bilgisayarları otomatik olarak başlatması ve yama yüklemeyi önce ve sonra kapanması gerektiğinde.

## Cihaz yama durumu

Site veya Hesap Düzeyindeki Yönet sekmesine gidin ve tüm BT ağınızın yama durumunu bir bakışta görmek için Yama Yönetimi'ni tıklayın.

### Site: Pruebas Beta: Patch Management

SUMMARY DEVICES AUDIT **MANAGE** MONITOR SUPPORT REPORT POLICIES SETTINGS

Patch Management  Network Management  Software Management

The chart below shows device compliance with the approved patch list. Patches not approved are not reported as missing.

All Policies

#### 10 Most vulnerable devices in terms of Approved Pending Patches

Hostname (Description)	Policy	Last Run	Next Run	Last Audit Date	Approved Pending Patches
VMBETA-W764 (VMBETA-W764)	patch pruebas beta		Run once at 2017-01-17 18:00	2017-01-18 15:58:57 CET	98

All devices Workstations Servers

#### 1 Account Policies

Name	Targets	Last Run	Next Run	Actions	Enabled for this site
PMP	Account Site Group: North		Run once at 2017-01-20 10:26	Push changes...	ON

#### 1 Site Policies

Name	Targets	Last Run	Next Run	Actions	Enabled for this site
patch pruebas beta	Site Pruebas Beta (Group: beta)		Run once at 2017-01-17 18:00	Push changes...	ON


Yönet ekranı aşağıdaki üç alana ayrılmıştır:

- Pasta grafiği: Tamamen yamayan cihazların ve bekleyen yamaları olan cihazların yüzdesini gösterir
- 10 Onaylanmış Beklemedeki Yamalar bakımından en savunmasız aygıtlar: Onaylanmış bekleyen yamalarla ilgili olarak yöneticiden en fazla dikkat isteyen on bilgisayarı görüntüler.
- Atanan politikaların listesi: Siteye atanan Yama Yönetimi politikalarını bulmanıza yardımcı olur

## Yuvarlak Diyagram(Pie Chart)

Tamamen yamalı cihazların ve bekleyen yamaları olan cihazların yüzdesini gösterir.

Tüm onaylanmış parşömenler başarıyla kurulduğunda bir bilgisayarın tamamen yamalı olduğu kabul edilir. Grafik, henüz yüklenmemiş onaylanmış yamaları olan bilgisayarları kırmızı renkte gösterecek ya da yüklemeyi engelleyen hatalar döndürecektir.

Varsayılan olarak, grafik Site / Hesaptaki tüm cihazları görüntüler. Ancak, yalnızca belirli bir politikaya atanan cihazları görüntülemek için politika listesindeki simgeyi tıklayabilirsiniz .

Ayrıca, grafiğin altında cihaz türüne göre görüntülenen verileri filtrelemek için bir seçici bulabilirsiniz (Tüm cihazlar, İş İstasyonu, Sunucular).

### 10 En hassas cihazlar


Bu bölüm, onaylanmış bekleyen yamalarla ilgili en hassas on cihazınızın listesini gösterir. Yamaların ciddiyetine bakılmaksızın, en çok onaylanmış bekleyen yama sayısına sahip cihaz ilk olarak listelenecektir. Her bilgisayar için aşağıdaki ayrıntıları göreceksiniz:

- Ana bilgisayar adı: Cihazınızın adı. Ana Makine Adı bağlantısına tıklamak sizi Cihaz Düzeyindeki Yönet sekmesine yönlendirecektir.
- Site: Cihazın eklendiği site. Bu alan sadece Hesap Düzeyinde görünür.
- Politika: Cihazı hedefleyen politikanın adı.
- Son Run: Politikanın son çalışma zamanı.
- Sonraki Çalıştır: Politikanın bir sonraki çalışma zamanı. Geçersiz bir programa sahip olan politikalar, orijinal verileri değil, geçersiz verileri gösterir.
- Son Denetim Tarihi: Cihazın son denetimi yapıldı.
- Onaylanmış Bekleyen Yamalar: Her bir cihaz için onaylanmış bekleyen yamaların toplam sayısı.


### Atanan politikaların listesi

Bu bölüm Hesap Düzeyinde ve Site Düzeyinde oluşturulan Yama Yönetimi ilkelerinin listesini görüntüler.

Her politika için aşağıdaki ayrıntıları göreceksiniz:


- **Etkin simgeyi geçersiz kıl**  . Bu simge yalnızca söz konusu Hesap Seviyesi politikası Site Düzeyinde geçersiz kılınırsa görünür. Geçersiz kılmayı görüntülemek / düzenlemek için Site Düzeyindeki Politikalar'ı tıklayın. Politikanın orijinal ayarlarını görmek için adını tıklayın.


- **Hedefler(Targets):** Politikanın hedefleri
- **Son Çalıştır(Last Run):** Politikanın son çalışma zamanı
- **Sonraki çalışma(Next run):** Politikanın bir sonraki çalışma zamanı


-  Bu simgeye tıklamak, politika listesinin üzerindeki (büyük) pasta grafiğinde gösterilenleri değiştirecektir. Simge, Tüm Politikalara genel bakış ile söz konusu politikanın verileri arasında geçiş yapar ve politika ismini pasta grafik üzerinde gösterir.


- **İtme değişiklikleri:** Politika tarafından hedeflenen tüm cihazlara politika değişikliklerini hemen uygulamak için bu düğmeye tıklayın.

- **Eylemler:** Politikanın belirli yönlerini kontrol etmenizi sağlar:

-  : Politikaların yayınlandığı son zamandaki sonuçları görüntülemenizi sağlar. Simgeye tıklamak, son çalışma süresini ve aşağıdaki yama bilgilerini gösteren bir açılır pencere açar: Yama Açıklaması, Boyut, Hedeflenen Aygıtlar, Başarılar ve Hatalar.

-  : Politika şimdi çalıştırıldıysa hangi yamaların yükleneceğini görmenizi sağlar. Oluşturulan ilkeyi doğrulamanıza izin verir, onaylanmış tüm yamaların listeye dahil edildiğinden emin olun ve onaylanmamış tüm düzeltme eklerinin dışında bırakılır.

-  : Politika tarafından hedeflenen tüm siteleri gösterir. Ayrıca, geçersiz kılınan politikaları görüntüler ve siteleriniz için politikaları etkinleştirmenizi veya devre dışı bırakmanızı sağlar.

-  : Bu simgeye tıklamak, politikayı şimdi de programın dışında çalıştırmak isteyip istemediğinizi onaylayabileceğiniz bir iletişim kutusu görüntüler.

- **Bu site için etkinleştirildi(Enabled for this site):** Politikayı AÇIK veya KAPALI duruma getirmek için bir geçiş:

## Yama Yönetimi ilke yöntemi: Kullanım senaryoları

Yöntem(Method)	Yama seçimi ayrıntı düzeyi(Patch selection granularity)	Otomasyon(Automation)	Yapılandırma süresi(Configuration time)
Windows Güncelleme Politikası	Düşük "Önemli" ve "Önerilen" gruplara göre yama seçimi	Yüksek Yüklenecek yamalar grupları bir kez yapılandırılır	Düşük "Önemli" ve "isteğe bağlı" yamalar yüklenip yüklenmediğini seçin
Patch Management	İlimli Birden çok yapılandırılabilir kriterle yama seçimi	Yüksek Filtreleri oluşturduktan sonra, Microsoft bunları yayınladıkça yamalar otomatik olarak yüklenir	İlimli Yüklenecek yamaları seçmek için filtreleri tanımlayın

# Kullanıcı Hesapları ve Güvenlik Seviyeleri(User Accounts and Security Levels)

## Kullanıcı hesapları

Bir kullanıcı hesabı, PCSM Konsolu'na erişimi düzenleyen bilgi ve teknisyenlerin kullanıcıların cihazlarına alabileceği eylemlerden oluşan bir kaynaktır.

Kullanıcı hesapları sadece PCSM konsoluna veya Panda Systems Management tarafından sağlanan diğer hizmetlere erişen BT yöneticileri tarafından kullanılır.

Genel olarak, her BT yöneticisinin tek bir kullanıcı hesabı vardır.

## Ana kullanıcı

Ana kullanıcı, Panda Systems Management servisinin sağlanması sırasında müşteriye Panda Security tarafından sağlanan kullanıcı hesabıdır. Bu hesaba yönetici güvenlik seviyesi atanır (bu bölümde daha sonra açıklanacaktır).

Güvenlik nedenleriyle, ana kullanıcının şifresini veya konfigürasyonunu değiştirmek veya bir PCSM Temsilcisinden giriş yaparak servise erişmek mümkün değildir; Bununla birlikte, ana kullanıcı hesabı, yöneticinin bilgisayarında yüklü olan Aracıya PCSM Konsolu'ndan erişmek için kullanılabilir.

## Güvenlik seviyeleri

Güvenlik düzeyi, bir veya daha fazla kullanıcı hesabına uygulanan Konsol'a erişmek için özel bir izin yapılandırmasıdır. Bu, kullanıcı hesabının Panda Systems Management'a erişim için kullandığı güvenlik düzeyine bağlı olarak, belirli Konsol kaynaklarını görüntülemek veya değiştirmek için belirli bir yöneticiye yetki verir.

Bir veya daha fazla kullanıcı hesabı bir veya daha fazla güvenlik düzeyine ait olabilir.

## Güvenlik seviyeleri: Amaç

Küçük bir BT Departmanında, tüm teknisyenler Console'a herhangi bir kısıtlama olmaksızın yönetici olarak erişir. Bununla birlikte, orta veya büyük bir BT Departmanında veya birçok müşterinin ortaklarında, cihazlara erişimin üç kritere göre bölümlere ayrılması gerekebilir:

- **Yönetilecek cihaz sayısı.**

Aynı şirketin ofislerine veya aynı partnerin farklı müşterilere ait orta / büyük ağlarda veya ağlarda, teknisyenlere cihazların dağıtılması ve atanması gerekli olabilir. Bunu yaparak, belirli bir teknisyen tarafından yönetilen bir ofisin cihazları, diğer ofislerin cihazlarını yöneten teknisyenler tarafından görülmeyecektir.

Belirli müşterilere ait hassas verilere kısıtlı erişim de olabilir; bu da, onu içeren cihazları işleyebilecek teknisyenlerin hassas kontrolünü gerektirir.



- Yönetilecek cihazın amacı.

Bir cihazın işlevine bağlı olarak, bu alanda uzman bir teknisyen atanabilir. Örneğin, bir grup uzman teknisyen, iş ortağı tarafından yönetilen bir veya tüm müşterinin veritabanı sunucusuna atanabilir ve aynı şekilde, posta sunucuları gibi diğer hizmetler bu gruba görünmeyebilir.

- Teknik bilgi.

Teknisyenlerin bilgisine veya BT departmanındaki güvenlik düzeyine bağlı olarak, Konsola yalnızca izleme / doğrulama (salt okunur) erişimi veya cihaz ayarlarının değiştirilmesi gibi daha gelişmiş erişim ihtiyaçları olabilir.

Üç kriter örtüşebilir, esnek ve tanımlanması ve bakımı kolay olan çok güçlü bir konfigürasyon matrisi oluşturabilir, bu da her teknisyen için erişilebilir olan Konsol özelliklerini profillerine ve sorumluluklarına göre mükemmel bir şekilde kısıtlamanıza izin verir.

## Yönetici güvenlik seviyesi

Bir Panda Systems Management kullanıcı lisansı, yönetici adı verilen varsayılan bir toplam kontrol güvenlik seviyesi ile birlikte gelir. Varsayılan yönetim hesabı bu güvenlik düzeyine aittir ve Konsolda gerçekleştirilebilecek tüm eylemlerin gerçekleştirilmesine kesinlikle izin verir. Yönetici aynı zamanda yeni güvenlik seviyeleri ve kullanıcılar oluşturabilecek ve mevcut güvenlik seviyelerini değiştirebilecek tek güvenlik seviyesidir.

Yönetici güvenlik düzeyi Sunucudan silinemez ve herhangi bir kullanıcı hesabı, Konsol aracılığıyla atandıktan sonra bu güvenlik düzeyine ait olabilir.

- **Kullanıcılar:** Yeni kullanıcı hesapları oluşturmanızı ve bunların bir veya daha fazla güvenlik düzeyine ait olup olmadığını tanımlamanızı sağlar.

- **Güvenlik seviyeleri:** Panda Systems Management kaynaklarına erişmek için yeni ayarları oluşturmanıza ve değiştirmenize izin verir.

## Kullanıcı hesaplarını oluşturma ve yapılandırma

Genel menüsünde Hesap, Kullanıcılar, kullanıcı hesaplarını oluşturma ve değiştirme ile ilgili tüm gerekli işlemleri gerçekleştirebilirsiniz.

- Yeni kullanıcı hesabı ekle: Yeni bir kullanıcı eklemek, bir şifre belirlemek, ait olduğu seviye veya güvenlik seviyelerini belirlemek ve ilişkili Bileşen seviyesini (1'den 5'e kadar) tanımlamak için Kullanıcı Ekle'ye tıklayın.

Kullanıcı hesaplarını oluşturma ve yapılandırma

Genel menüsünde Hesap, Kullanıcılar, kullanıcı hesaplarını oluşturma ve değiştirme ile ilgili tüm gerekli işlemleri gerçekleştirebilirsiniz.

- **Yeni kullanıcı hesabı ekle(Add new user account):** Yeni bir kullanıcı eklemek, bir şifre belirlemek, ait olduğu seviye veya güvenlik seviyelerini belirlemek ve ilişkili Bileşen seviyesini (1'den 5'e kadar) tanımlamak için Kullanıcı Ekle'ye tıklayın.

**Add User**

Enter the details of the user you wish to add. You will assign rights for this user later.

Username:

Password:

Password Again:

Email:

First name:

Last name:

Roles:

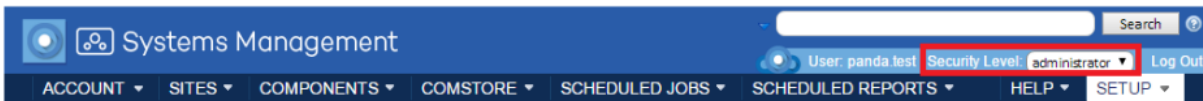
<input type="radio"/>	<input type="checkbox"/>	Default	
<input type="radio"/>	<input type="checkbox"/>	accountadmin	
<input type="radio"/>	<input type="checkbox"/>	Custom_panda.test@panda345.com	Migrated custom role for panda.test@pand...
<input type="radio"/>	<input type="checkbox"/>	Custom_panda1234@panda.com	Migrated custom role for panda1234@panda...
<input type="radio"/>	<input type="checkbox"/>	Custom_panda@example.com	Migrated custom role for panda@example.c...

- **Bir kullanıcı hesabı düzenleyin:** Bir kullanıcı isminin tıklanması, tüm hesap detaylarını içeren bir form görüntüler.

- **Kullanıcı hesaplarını silin veya devre dışı bırakın:** İlgili onay kutusunu işaretleyerek bir kullanıcı seçin ve Eylem çubuğundaki yasaklanmış ve çapraz simgeleri tıklayın.

- **Toplam kontrol izinleri atayın:** Hesap Yöneticisi'nde Açık / Kapalı'yı tıklayın.

Bir kullanıcı hesabı bir güvenlik seviyesine veya daha fazlasına ait olabilir. İkinci durumda, Konsol, kullanıcı hesabının çalışacağı güvenlik seviyesini seçebileceğiniz bir açılır liste görüntüler.



## Güvenlik seviyeleri oluşturma ve yapılandırma

Genel menüde, Hesap, güvenlik seviyeleri, güvenlik seviyelerini oluşturmak ve değiştirmek için gerekli tüm işlemleri gerçekleştirebilirsiniz.

- **Yeni Güvenlik seviyesi ekle:** Yeni bir güvenlik düzeyi eklemek için Güvenlik düzeyi ekle'yi tıklayın. Adı girmeniz istenir ve boş bir yapılandırma / şablon temel olarak mı yoksa yeni güvenlik düzeyi bir önceki güvenlik düzeyine mi dayalı olacaksınız.

- **Güvenlik Düzeyi Düzenle:** Bir güvenlik seviyesi adına veya kurşun kalem simgesine tıklayarak tüm ayarları içeren bir form görüntülenir.

- **Güvenlik seviyesini sil:** X simgesi seçilen güvenlik seviyesini siler.

## Güvenlik düzeylerini yapılandırma

Bir güvenlik düzeyinin yapılandırması dört bölüme ayrılmıştır:

- **Cihaz görünürlüğü:** Cihaz gruplarına erişimi etkinleştirir veya kısıtlar.
- **İzinler:** Konsol özelliklerine erişimi etkinleştirir veya kısıtlar.
- **Aracı Tarayıcı Araçları:** Aracı özelliklerine erişimi etkinleştirir veya kısıtlar.
- **Üyelik:** Yapılandırılmış güvenlik düzeyine ait kullanıcı hesaplarını belirtir.

## Cihaz görünürlüğü

Bu kurulum grubu, belirli bir güvenlik düzeyine ait olan Konsol kullanıcıları tarafından görülebilen ağ aygıtlarını belirlemenizi sağlar.

Panda Systems Management'ın güvenlik düzeyleri, kullanıcıların erişimin Konsolda kullanılabilen dört tür statik gruplamaya sahip olmasını ve sınırlanmasını sağlar:

- **Siteler**
- **Site cihazı grubu**
- **Cihaz grubu**
- **Site grubu**

Daha spesifik olarak, güvenlik seviyeleri, her cihaz gruplaması türünde bulunan tek tek öğelere erişimi tanımlamanıza olanak tanır. Bir grupta yer alan tüm öğelere erişime izin vermek için, yanındaki AÇIK seçeneğini seçin. Bir ayarlar penceresi görüntülenecektir.

The screenshot shows the 'Device Visibility' configuration window. At the top, there is a 'Device Visibility' header. Below it, there are two toggle switches: 'Profiles' (set to OFF) and 'Profile Device Groups' (set to ON). The 'Profile Device Groups' toggle is highlighted with a red underline. Below the toggles, there are two lists: 'Include' (empty) and 'Exclude' (containing 'Bilbao Office : Laptops', 'Bilbao Office : PCs', and 'Bilbao Office : Servers'). Between the lists are four buttons: '< Include', '<< Include all', 'Remove >', and 'Remove all >>'.

Dahil et metin kutusunda listelenen bir grup, bu güvenlik düzeyine ait tüm kullanıcı hesaplarına görünür olacaktır. Benzer şekilde, grup Hariç tutulan metin kutusunda listeleniyorsa, bu aygıt grubu Konsol'da görünmez.

## İzinler

İzinler bölümü, konsoldaki her kaynağa erişim düzeyini ayarlamanızı sağlar. Bunun için ilk önce genel menüdeki girdilerle çıkan konsoldaki alanların listesini gösterir:

		None	View	Manage
Account	<input type="checkbox"/>	OFF		
Sites	<input type="checkbox"/>	OFF		
Components	<input type="checkbox"/>	OFF		
ComStore	<input type="checkbox"/>	OFF		
Jobs	<input type="checkbox"/>	OFF		
Reports	<input type="checkbox"/>	OFF		
Setup	<input type="checkbox"/>	OFF		

Her bir rolün erişim düzeyini konsoldaki her alana (genel menüdeki sekmeler) ayarlamak için, anahtarı ON konumuna getirin. Bu, her alanla ilişkili kaynakları gösterecektir. Örneğin, alan kaynaklarını görüntülemek ve her birinin erişim seviyesini belirlemek için anahtarı Hesaptaki ON (Açık) konumuna getirin.

Erişim seviyeleri:

- **Yok(None):** Kaynak konsolda görüntülenmiyor.
- **Görünüm(View):** Kaynak konsolda görüntülenir, ancak herhangi bir parametresini yapılandırmak veya değiştirmek mümkün değildir.
- **Yönet(Manage):** Kaynak konsolda görüntülenir ve tam izinlerle erişilebilir.

## Ajan Tarayıcı Araçları

Bu kurulum grubu, Aracı'da bulunan uzaktan yönetim araçlarına erişim belirlemenizi sağlar.

Toggle all options:	<input type="checkbox"/> OFF		
ScreenShot	<input type="checkbox"/> OFF	LAN Deploy	<input type="checkbox"/> OFF
Services	<input type="checkbox"/> OFF	Task Manager	<input type="checkbox"/> OFF
VNC	<input type="checkbox"/> OFF	File Transfer	<input type="checkbox"/> OFF
RDP	<input type="checkbox"/> OFF	Registry Editor	<input type="checkbox"/> OFF
Command Shell	<input type="checkbox"/> OFF	Quick Jobs	<input type="checkbox"/> OFF
Restart/Shutdown	<input type="checkbox"/> OFF	Event Viewer	<input type="checkbox"/> OFF
Thumbnail Screen	<input type="checkbox"/> OFF	Notes	<input type="checkbox"/> OFF
Chat	<input type="checkbox"/> OFF	Wake-On-Lan	<input type="checkbox"/> OFF

## Üyelik

Yapılandırılmış güvenlik düzeyine ait kullanıcı hesaplarını yapılandırmanıza izin verir.

## Güvenlik seviyeleri oluşturma stratejileri

Güvenlik seviyesinin amacının, daha yüksek güvenlik ve insan hatalarına karşı koruma sağlamak amacıyla cihazlara veya Konsol kaynaklarına yönetici erişimini kısıtlamak olduğunu akılda tutarak, gerektiği kadar güvenlik seviyesi oluşturabilirsiniz. Bununla birlikte, bu yüksek güvenlik, teknik personelin çeşitli müşteriler veya görevler arasında yeniden kullanılmasında daha düşük esneklik ile birlikte gelir, böylece bir sistemdeki güvenlik düzeylerinin tam sayısı iki değişkenin ağırlıklandırılmasının sonucudur: esneklik vs. güvenlik

## Yatay güvenlik seviyeleri

Genel olarak, her birinde birden fazla ofisi bulunan ve bağımsız bir IT ekibine sahip olan bir şirket, her bir ofiste bulunan cihazlarla sınırlı bir toplam kontrol güvenlik seviyesi isteyecektir.

Bu şekilde, A ofisi tarafından yönetilen cihazlar ofis B'ye görünmeyecek ve tersi de geçerli olmayacaktır.

Birkaç ofisi bulunan bir şirkette, her ofiste aşağıdaki konfigürasyon gerekli olacaktır:

- Ofisin cihazlarını gruplandırın 1 site veya cihaz grubu.
- Sitedeki cihazlara erişime izin veren ve diğerlerine erişimi engelleyen 1 güvenlik seviyesi.
- Belirlenen ofisi kapsayan güvenlik seviyesine atanan her teknisyen için bir hesap.

Aynı şema, müşterileri ayırmak ve onlara belirli teknisyenleri atamak isteyen bir ortak tarafından kullanılabilir.

## **Dikey güvenlik seviyeleri**

Büyük ölçüde, yazdırma, veritabanı, posta sunucuları, vb. Gibi belirli görevleri hedef alan aygıtlar için, bu tür aygıtlara erişimi kısıtlayan güvenlik düzeyleri oluşturabilirsiniz.

Bu, bir çok ofis veya müşterinin posta sunucularına sahip bir şirket veya partnerin onları gruplandırmasını ve bunları yönetmek için bir grup teknisyenin görevlendirmesini sağlayarak, teknisyenlerin geri kalanının daha genel bir profile sahip kullanıcı cihazlarını yönetmesini sağlayacaktır.

Aşağıdaki genel yapılandırma gerekli olacaktır:

- Tüm posta sunucularını, ait oldukları site / müşteri / ofisinden bağımsız olarak gruplandırılan bir Aygıt grubu.
- Cihaz grubundaki cihazlara erişime izin veren ve diğer cihazlara erişimi engelleyen A güvenlik seviyesi.
- Cihaz grubundaki cihazlara erişimi reddeden ve diğer cihazlara erişim sağlayan bir B güvenlik seviyesi.
- Bir güvenlik seviyesi Şirket veya iş ortağının posta sunucularında bakım yapan her teknisyen için bir kullanıcı hesabı.
- Şirket veya iş ortağının kullanıcı cihazlarında bakım yapan her teknisyen için bir B güvenlik seviyesi kullanıcı hesabı.

## **Kaynak erişim güvenlik seviyeleri**

Her teknisyenin profiline veya deneyim düzeyine uygun olarak, BT Departmanı yöneticisi çalışmayı bölüm üyeleri arasında paylaşabilir. Bu, tamamlayıcı sorumluluklara sahip teknisyen grupları oluşturmanıza olanak tanır:

- İzleme teknisyenlerini izleme ve rapor etme: Sekme çubuğuna tam erişim, Raporlar ve Konsolun geri kalanına okuma erişimi.
- Komut geliştirme ve yazılım dağıtım teknisyenleri: Genel menüye erişim ile, Bileşenler ve ComStore
- Destek teknisyenleri: Sekme çubuğu, Destek ve kullanıcının cihazındaki Ajan'a erişim ile.

Ayrıca, ComStore'daki belirli bileşenlere erişimi kısıtlayabilir veya kullanıcı cihazlarında hassas işlemleri gerçekleştiren BT Departmanı tarafından geliştirilebilir ve kullanıcı hesabında ayarlanandan daha yüksek Bileşen seviyeleri atayabilirsiniz.

# Etkinlik günlüğü(Activity log)

## Giriş

Panda Systems Management, servis yöneticileri tarafından gerçekleştirilen eylemlerin kaydını tutar. Bu günlük, kullanıcıların cihazlarında yapılan değişiklikleri, değişiklikleri gerçekleştiren değişiklikleri kaydeder.

Etkinlik kaydı, gereken ayrıntı seviyesine bağlı olarak konsolda üç bölüme ayrılmıştır.

## Hesap düzeyinde etkinlik günlüğü

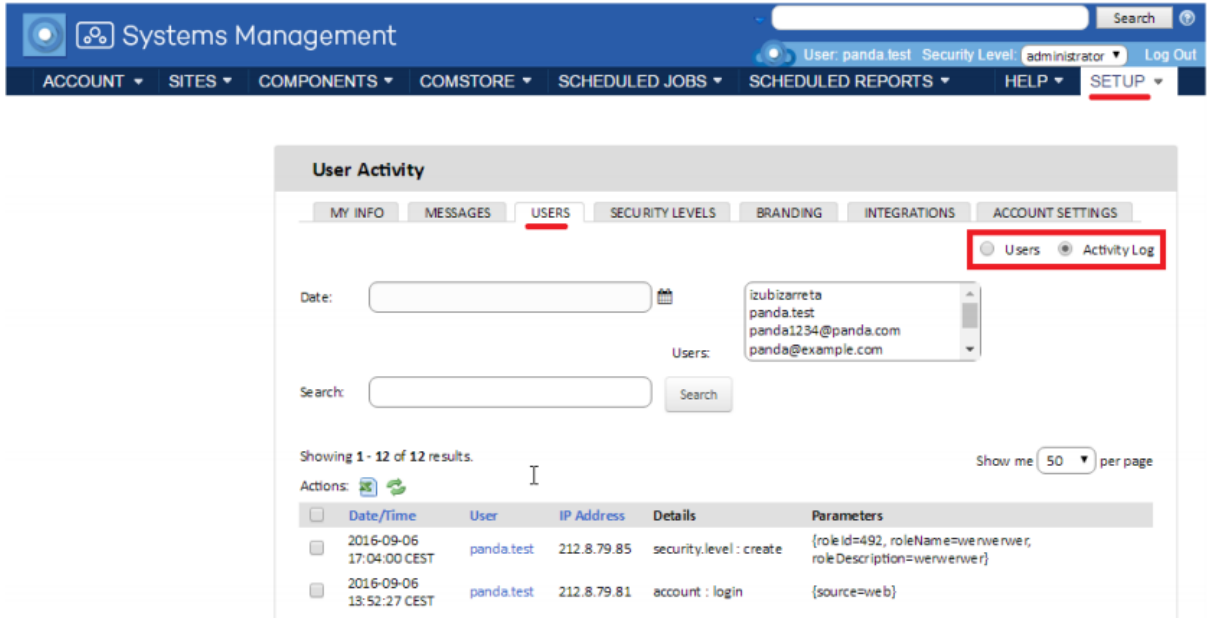
Bu raporlar sekmesini ve ardından Etkinlik günlüğünü tıklayarak genel Hesap menüsünden erişilebilir.

Hesap düzeyinde etkinlik günlüğü, yalnızca, hareketlerin tarihini ve saatini belirterek, siteler arasındaki aygıtların hareketlerini gösterir.

## Genel etkinlik günlüğü

Genel etkinlik günlüğü, ağ yöneticilerinin yönetim konsolu üzerindeki en önemli eylemlerini görmenizi sağlar.

Kullanıcıların genel etkinlik günlüğüne, Kullanıcılar'ı tıklayıp Etkinlik günlüğü'nü seçerek genel Kurulum menüsünden erişebilirsiniz.



The screenshot displays the Panda Systems Management interface. The top navigation bar includes 'ACCOUNT', 'SITES', 'COMPONENTS', 'COMSTORE', 'SCHEDULED JOBS', 'SCHEDULED REPORTS', 'HELP', and 'SETUP'. The main content area is titled 'User Activity' and features a tabbed interface with 'USERS' selected. A red box highlights the 'Activity Log' radio button. Below the tabs, there are search and filter options, including a 'Date' field, a 'Users' dropdown menu, and a 'Search' button. The main table shows a list of activities with columns for 'Date/Time', 'User', 'IP Address', 'Details', and 'Parameters'. The table contains two entries for the user 'panda.test'.

Date/Time	User	IP Address	Details	Parameters
2016-09-06 17:04:00 CEST	panda.test	212.8.79.85	security.level : create	{roleId=492, roleName=wenwenwe, roleDescription=wenwenwe}
2016-09-06 13:52:27 CEST	panda.test	212.8.79.81	account : login	{source=web}

## Faaliyetlerin listesi

Bu, her eylem için aşağıdaki bilgileri içeren bir faaliyet listesi tablosundan oluşur:

- **Checkbox:** Bu, Excel'e dışa aktarma gibi işlemler yapmak için listeden aktiviteler seçmenizi sağlar.
- **Tarih / saat:** Eylemin tarihi, saati ve saat dilimi.
- **Kullanıcı:** Panda Systems Management kullanıcısı eylemi yürütmek için yönetici tarafından kullanıldı.
- **IP Adresi:** Yöneticinin konsola bağlı olduğu IP adresi.
- **Ayrıntılar:** Eylemin gerçekleştirildiği Panda Systems Management ögesinin ve gerçekleştirilen işlemin türünü gösterir.
- **Parametreler:** Birime uygulanan eylemin alanlarını ve değerlerini gösterir.

## Etkinlik filtresi ve aramalar

Aşağıdaki araçlar, etkinlikleri aramanıza yardımcı olacak şekilde tasarlanmıştır:

### Tarih

- Bu, bir zaman aralığı seçmek için çeşitli seçenekler sunar:
- **Hızlı:** Varsayılan dönemlerden birini seçin: Son 24 saat, Son 2 gün, Son 2 hafta, Geçen ay, Son iki ay, Son 6 ay.
- **Özel Aralık:** Zaman aralığının başlangıcını ve sonunu belirlemenizi sağlar.

### Kullanıcılar

Bu, kullanıcıyı seçebileceğiniz bir açılır menü sunar. Bir kullanıcıyı seçtiğinizde, yalnızca bu kullanıcının etkinliğini göreceksiniz.

### Arama

Bazı belirli alanların içeriğine göre filtrelemenizi sağlayan bir metin kutusu

## Cihaz düzeyinde etkinlik kaydı

Cihaz düzeyinde aktivite kaydı, kullanıcı veya eylemden sorumlu yöneticiden bağımsız olarak, belirli bir cihazda gerçekleştirilen işlemleri görüntülemenizi sağlar.

Bu günlüğe erişmenin iki yolu vardır: Cihaz düzeyindeki Özet sekmesinden (Genel menü Siteler, cihazı içeren siteyi seçin ve belirli bir aygıtı tıklatın) ve Etkinlik günlüğü seçiciyi kullanarak Raporlar sekmesinden.

Her iki durumda da, eylemlerin bir listesi görüntülenir, her etkinlik için bir giriş, aşağıdaki bilgilerle birlikte:



- **Tip(Type):** Bu, cihazdaki etkinlik türünü göstermek için bir simge kullanır.

- Uzak masaüstü RDP ile.
- Uzak ekran görüntüsü.
- İşi başlat.
- Komut Kabuğu.
- VNC üzerinden uzak masaüstü.
- Dosya transferi.

- **İsim(Name):** Etkinliğin adı.

- **Başladı(Started):** Etkinlik başladığında.

- **Sona erdi(Ended):** Etkinlik bittiğinde.

- **Durum(Status):** Etkinlik durumu.

- **Sonuçlar(Results):** simgesine tıklayarak yöneticinin eyleminin sonucunu görüntüler.
- **İlerleme(Progress):** Etkinlik bir görev ise, durumu göstermek için bir ilerleme çubuğu eklenir.
- **Stdout:** Yapılandırılmış görev, yürütmenin sonucu olarak standart çıktıda veri görüntülense, bu simgeye tıklanarak görüntülenir.
- **Stderr:** Yapılandırılmış görev, yürütmenin sonucu olarak standart çıktıda veri görüntülense, bu simgeye tıklanarak görüntülenir.

# Raporlar(Reports)

## Giriş

Panda Systems Management, şirketin BT kaynaklarından toplanan bilgileri görüntülemenin birçok yolunu sunar ve bunlardan biri de rapor sistemidir.

Rapor sistemi, cihazlarınızın durumu hakkındaki verileri .PDF formatına aktarmanızı ve verileri raporların hedeflendiği kişilerin ihtiyaçlarına göre yapılandırmanızı sağlar. Bilgileri harici araçlarla yönetmek istiyorsanız, veriler ayrıca .XLS'ye aktarılabilir.

Panda Systems Management tarafından yönetilen tüm yönleri kapsayan 50'den fazla rapor türü vardır. Bu bölüm, kime yönelik olduğuna bağlı olarak raporun nasıl seçileceğini açıklar ve her raporun genel bir tanımını sunar.

## Rapor sistemine erişim

Rapor sistemine, üç Sistem Yönetimi seviyesi üzerinden erişilebilir. Bilgilerin detay seviyesi, seçilen seviyeye ve ayrıca rapora dahil edilecek olan veriye bağlı olarak değişir.

Bütün raporlar her seviyede mevcut değildir; Bunların çoğu sadece belirli cihazlar içindir (Cihaz seviyesi) veya belirli bir site veya yönetilen hesabın tamamı için daha uygundur.

Üç rapor düzeyi, sekme menüsündeki Raporlar sekmesinden erişilebilir. Sekme menüsüne genel Hesap menüsünden erişildiğinde, bu seviyeye uygun raporları içeren bir pencere göreceksiniz. Benzer şekilde, belirli bir site veya cihaz seçerken, Raporlar sekmesi Site veya Cihaz düzeyinde kullanılabilen raporları görüntüler.

## Rapor oluşturma(Generating reports)

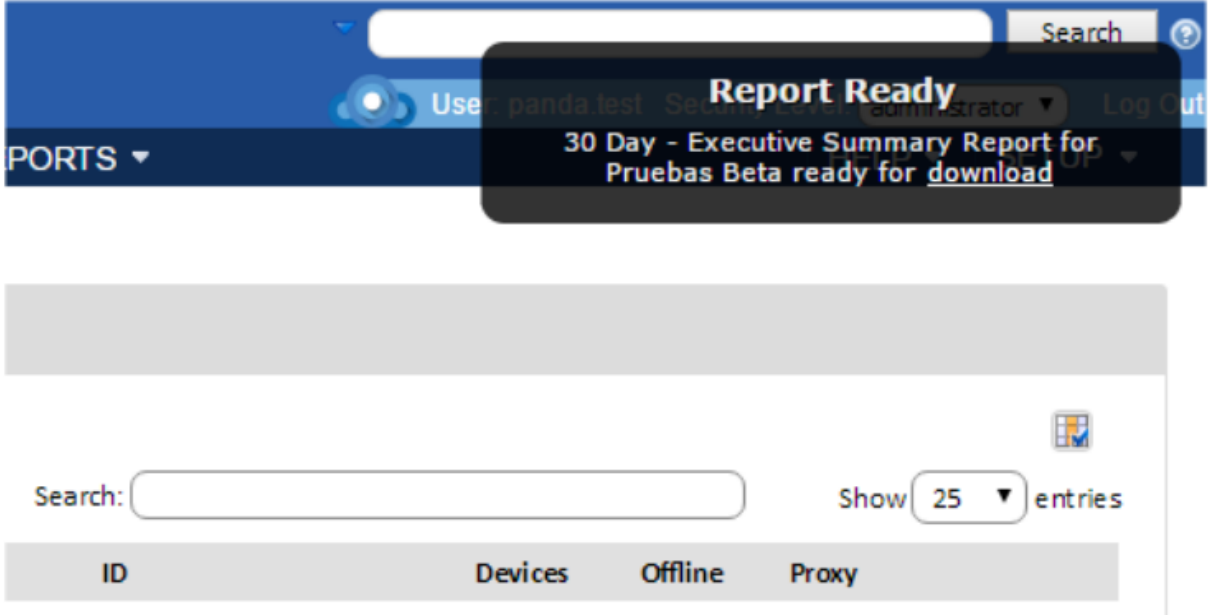
Raporlar talep üzerine veya planlı olarak oluşturulabilir.

## Talep raporları oluşturmak

Ekranın sağ üst köşesinde bir indirme açılır pencere ile sonuçlanacak arka planda veri toplamak için bir işlem başlatmak için Raporlar sekmesindeki raporlar listesindeki simgeleri

tıklayın





İhtiyacınız olan kadar çok rapor oluşturabilirsiniz.

## Zamanlanmış rapor raporları

Raporların oluşturulmasını, Raporlar sekmesinin işlemler çubuğunda ilgili simgeye tıklayarak planlayabilirsiniz.

Bir veya daha fazla raporun oluşturulmasını planlamak için gereken bilgilerle yeni bir pencere görüntülenecektir.

### - Genel

- **İsim(Name):** Rapor oluşturma işinin adı.
- **Açıklama(Description):**
- **Zamanlama(Schedule):** Rapor oluşturma işinin ne zaman çalışacağını belirleyebilirsiniz.
- **Etkinleştir(Enable):** Bu, rapor oluşturma ayarlarının kullanılmaya hazır olmasını ve gereksiz gürültü oluşturmadan etkinleştirebilmenizi veya devre dışı bırakabilmenizi sağlar.

- **Raporlar:** PDF ve / veya Excel'de oluşturulacak raporları seçin.

- **E-posta alıcıları(Email recipients)**
- **Konu(Subject)**
- **Metin(Text)**
- **Varsayılan hesap raporu alıcıları(Default account report recipients):** Raporları, site için ayarlanan e-posta hesaplarına gönderir; bu raporlar seçilen sekmedeki Ayarlar sekmesindeki E-posta Alıcıları'nda yapılandırılabilir.
- **Varsayılan site raporu alıcıları(Default site report recipients):** Raporları, Genel Kurulum menüsündeki E-posta Alıcıları'nda yapılandırılabilen tüm Sistem Yönetimi hesabı için ayarlanan e-posta hesaplarına gönderir.

- **Ek alıcılar(Additional recipients):** Bu, Hesap veya Site düzeyinde yapılandırılmış olanlara ek e-posta adresleri eklemenizi sağlar.

## Rapor özelliklerini ve bilgi türünü

Raporlar, doğru raporu oluşturmak için anlaşılması gereken önceden yapılandırılmış parametreler ve özellikler ile tanımlanır. Parametreler raporun adı ve oluşturuldukları seviye (Hesap, Site veya Aygıt) olarak yansır.

Bir raporu tanımlayan parametreler aşağıdaki gibidir:

- **Seviye(Level)**
- **Zaman Dilimi(Time Period)**
- **Rapor Türü(Type of report)**

### Seviye(Level)

Raporun kapsamını tanımlamak için seviye (Hesap, Site veya Cihaz) kullanılır.

- **Hesap(Account):** Hesaptaki tüm cihazları içerir.
- **Site(Site):** Seçilen sitede bulunan tüm cihazları içerir.
- **Cihaz(Device):** Seçilen cihaz için bilgi.

### Zaman dilimi

Raporun kapsayacağı süreyi belirler. Bu dönem "x gün" öneki raporun adıyla tanımlanacaktır.

- **30 Gün(30 Day):** Son 30 günün bilgilerini içerir. Rapor, oluşturulmadan önceki güne kadar olan verileri içerir.
- **7 Gün(7 Day):** Son yedi güne ait bilgileri içerir. Rapor, oluşturulmadan önceki güne kadar olan verileri içerir.
- **Önek yok(No Prefix):** Raporun oluşturulduğu anda yalnızca cihazın durumuyla ilgili verileri içeren raporlar.

### Rapor türü

Rapor türü isimde belirtilir ve raporda yer alan şirketin BT kaynaklarının yönlerini yansıtır. Aşağıda farklı rapor türlerini görebilir ve daha sonra bu bölümde çeşitli raporlar her biri için bir açıklama ile türlere göre gruplandırılmıştır.

#### Yönetici(Executive)

Yönetici raporları, yönetilen ağın çeşitli yönlerini tek bir belgede özetlemektedir. Ağ durumuna ilişkin hızlı bir fikir edinebilmek için çok fazla ayrıntıya girmeden ve genel eğilimleri ve gelişmeleri göstermek için faydalıdır.

## **Aktivite(Activity)**

Bunlar, şirketin cihazlarını yönetmekten sorumlu olan ağ yöneticilerinin etkinliğini gösterir. Raporla bağlı olarak, etkinlik aşağıdaki gruplara ayrılabilir:

- **Meslekler(Jobs)**
- **Komut Kabuğu(Command Shell)**
- **Uzaktan Destek(Remote Support)**
- **Notlar(Notes)**

## **Alarm(Alert)**

Bunlar, monitörler ve diğer bileşenler tarafından üretilen ve BT kaynaklarının normal şekilde çalışmasını sağlayan uyarıları gösterir. Ayrıca, BT başarısızlıklarına bağlı aksama sürelerinin azaldığı ve IT personelinin olay anında ortalama çözüm süresiyle ölçülen çalışanların verimliliğini de göstermektedir.

## **Envanter(Inventory)**

Bunlar, BT departmanı tarafından yönetilen varlıkların hem donanım hem de yazılımla ilgili derleme detaylarını derlemekte ve değiştirilmesi gereken ağ üzerinde eski veya yetersiz teknolojinin olup olmadığını belirleyebilir.

## **Sağlık(Health)**

Bunlar, bir antivirüs, kritik yamaların yokluğu, vb. Gibi parametrelere bağlı olarak problemlerin üretilmesi için cihazların eğilimini yansıtır.

## **Performans(Performance)**

Bunlar CPU ve sabit disk kullanımı ile bir cihazın performansını gösteren diğer parametreler hakkında ayrıntıları içerir.

## **Yama yönetimi(Patch Management)**

Bu raporlar, ağdaki sistemlerin yamalar ile ne ölçüde uyum içerdiğini yansıtmaktadır: ağ aygıtlarının güvenlik düzeyi ve kritik olan yamalar gereklidir.

## **Diğer raporlar(Other Reports)**

Bu kategori, diğer kategorilere sığmayan raporları içerir.

## **Yönetici Raporları(Executive Reports)**

### **30/7 Günlük Hesap Yürütme Özeti (Hesap)**

**Zaman periyodu:** Son 7 veya 30 gün.

**Kapsam:** Hesap.

**Bilgi:**

- Faaliyetlere göre en iyi 5 site
- Uyarılar ile en iyi 5 site
- Her site için:
  - Faaliyetler için toplamlar
  - Kategoriye göre uyarılar
  - Bireysel kullanıcı etkinliği

**30 Gün - Yönetici Özet Raporu (Site Düzeyi)**

**Zaman periyodu:** Son 7 veya 30 gün.

**Kapsam:** Site.

**Bilgi:**

- Mevcut sunucu durumlarına genel bakış:
  - Envanter
  - Disk kullanımı
  - Yama durumu
  - Eksik kritik yamalar
  - Çalışma zamanı
- İş istasyonlarının mevcut durumuna genel bakış:
  - Değişirme önerileri
  - Kullanılan işletim sistemleri
  - Stok kontrolleri
- Ayrıntılar:
  - İş istasyonlarının donanım envanteri
  - Disk kullanımı
  - Yama durumu ve kritik yamalar eksik
- Listeler:
  - Yönetilen ağ cihazları
  - Yönetilen mobil cihazlar
- Özetler:
  - İzleme uyarıları (kategori başına toplam)
  - Cihazlarda etkinlik (kategori başına toplam, toplam süre ve en iyi 5 cihazın etkinlik sayısı)

## **30/7 Gnlk Site Yneticisi zeti (Site)**

**Zaman periyodu:** Son 7 veya 30 gn.

**Kapsam:** Site.

**Bilgi:**

- Kategoriye gre toplam etkinlik ve zaman
- İlk 5 cihazı aktivite sayısına gre listeler
- Her etkinlik iin ayrıntılar, cihaza gre

## **30 Gn - Ynetici zeti Raporu - Sadece Sunucular ve i İstasyonları (Site Dzeyi)**

**Zaman periyodu:** Son 30 gn.

**Kapsam:** Site.

**Bilgi:**

- Sunucuların durumu:
  - Envanter
  - Disk kullanımı
  - Yama durumu
  - Eksik kritik yamalar
  - alıma zamanı
- İ istasyonlarının durumu:
  - Deęitirme nerileri
  - Kullanılan iletim sistemleri
  - Stok kontrolleri
- Ayrıntılar i istasyonu:
  - Donanım envanteri
  - Disk kullanımı
  - Yama durumu
  - Eksik kritik yamalar

## **Faaliyet Raporları**

### **30/7 Gün Site Etkinliđi Özeti**

**Zaman periyodu:** Son 7 veya 30 gün.

**Kapsam:** Site.

**Bilgi:**

- Kategoriye göre toplam etkinlik ve zaman
- İlk 5 cihazı etkinlik sayısına göre listeler.
- Her etkinlik için ayrıntılar, cihaza göre

### **30 Gün / 7 Hesap Etkinliđi Özeti**

**Zaman periyodu:** Son 7 veya 30 gün.

**Kapsam:** Hesap.

**Bilgi:**

- Faaliyetlerin sayısına göre en iyi 5 site
- Her site için:
  - Toplam ve ayrıntı miktarları ile kategorilere göre aktiviteleri listeler

### **Site Etkinliđi**

**Zaman periyodu:** Son 30 gün.

**Kapsam:** Site.

**Bilgi:**

- İşler, Notlar ve Uzaktan Devralma oturumlarını listeler

### **30/7 Günlük Hesap Kullanıcı Özeti**

**Zaman periyodu:** Son 7 veya 30 gün.

**Kapsam:** Hesap.

**Bilgi:**

- Toplam miktar ve detaylarla kategoriye göre aktiviteleri listeler
- Her kullanıcı adı için:
  - Site aktivitesi, başlangıç ve bitiş zamanı ve toplam süre.



## **Uzak Etkinlik**

**Zaman aralığı:** Son ayın tamamı.

**Kapsam:** Hesap.

### **Bilgi:**

- Tüm uzaktan kumanda oturumlarını listeler:

- Kullanıcı adı, site ve ana makine adı, başlangıç ve bitiş tarihi ve saati, uzunluğu ve kullanılan uzaktan alım aracı.

## **30/7 Gün Cihaz Etkinliği Özeti**

**Zaman periyodu:** Son 7 veya 30 gün.

**Kapsam:** Cihaz.

### **Bilgi:**

- Kategoriye göre toplam etkinlik ve zaman

- Her etkinlik etkinliği için ayrıntıları listeler:

- Kullanıcı adı
- Tarih / saat başladı ve bitti
- Toplam zaman

## **Uyarı Raporları**

### **19.7.1 30/7 Gün Site Uyarısı Özeti**

**Zaman periyodu:** Son 7 veya 30 gün.

**Kapsam:** Site.

### **Bilgi:**

- Kategoriye göre toplam uyarı sayısı ve ortalama yanıt süresi.

- Her uyarı için:

- Öncelik, uyarı tarihi ve saati, bitiş zamanı ve yanıt süresi

### **30/7 Günlük Hesap Uyarısı Özeti**

**Zaman periyodu:** Son 7 veya 30 gün.

**Kapsam:** Hesap.

**Bilgi:**

- En iyi 5 siteyi uyarı sayısına göre listeler.
- Her site için:
  - Toplam sayı ve toplam süre ile türüne göre uyarılar.

### **30/7 Günlük Hesap Uyarısı Özeti**

**Zaman periyodu:** Son 7 veya 30 gün.

**Kapsam:** Hesap.

**Bilgi:**

- En iyi 5 siteyi uyarı sayısına göre listeler.
- Her site için:
  - Toplam sayı ve toplam süre ile türüne göre uyarılar.

### **30/7 Günlük Cihaz Uyarısı Özeti**

**Zaman periyodu:** Son 7 veya 30 gün.

**Kapsam:** Cihaz.

**Bilgi:**

- Kategoriye göre toplam uyarı sayısı ve ortalama yanıt süresi
- Her uyarı için:
  - Öncelik, uyarı tarihi ve saati, bitiş zamanı ve yanıt süresi

### **Monitör Uyarıları Raporu (Cihaz Seviyesi)**

**Zaman periyodu:** Akım.

**Kapsam:** Cihaz.

**Bilgi:**

- Yazılan her uyarı için:
  - Uyarı mesajı, öncelik ve uyarı zamanı içerir

## Monitör Uyarıları Raporu (Site Düzeyi)

**Zaman periyodu:** Akım.

**Kapsam:** Site.

**Bilgi:**

- Cihaz adını, uyarı türünü, mesajı ve önceliği ve uyarı saatini / tarihini listeler.

## Monitör Uyarıları Raporu (Hesap Seviyesi)

**Zaman periyodu:** Akım.

**Kapsam:** Hesap.

**Bilgi:**

- Cihaz adı, site, toplam aktif uyarı sayısı ve öncelik sırasına göre ayrılmış aktif uyarıların sayısını listeler.

## Envanter Raporları

### Bilgisayar Özeti

**Zaman periyodu:** Akım.

**Kapsam:** Site.

**Bilgi:**

- Her bilgisayar için:

- İsim, işletim sistemi ve servis paketi
- Bellek, işlemci, mektup etiketi
- Toplam sürücü alanı, miktarı ve boş alanın yüzdesi.

## Kritik 3. Tarafı Yazılım Özet Raporu

**Zaman periyodu:** Akım.

**Kapsam:** Site.

**Bilgi:**

- Sitede PCSM aracısı yüklü tüm Windows ve Mac cihazlarını listeler:

- Her aygıt için, raporlar çok kritik üçüncü taraf yazılım uygulamalarının sürümünü gösterir:
  - Skype
  - Quicktime
  - Java
  - Adobe Acrobat okuyucu

- Mozilla Firefox
- Adobe Flash
- Adobe Air
- Adobe Shockwave
- Google Chrome
- Silverlight

## **Site Seri Numaraları**

**Zaman periyodu:** Akım.

**Kapsam:** Site.

**Bilgi:**

- Her bir cihazı seri numarası ile listeler

## **Hesap Sunucusu IP Bilgisi**

**Zaman periyodu:** Akım.

**Kapsam:** Hesap.

**Bilgi:**

- Tüm sunucular için IP adresi

## **Hesap Sunucusu Depolama Alanı**

**Zaman periyodu:** Akım.

**Kapsam:** Hesap.

**Bilgi:**

- Sunucular için depolama bilgisi (grafiksel olarak görüntülenir):

- Sürücü etiketi, boyut
- Miktar ve alan yüzdesi
- Boş alanın miktarı ve yüzdesi.

## **Site Yazılımı**

**Zaman periyodu:** Akım.

**Kapsam:** Site.

**Bilgi:**

- Her yüklü yazılım için:

- Kurulum sayısı

## Site Yazılımı ve Düzeltmeler

**Zaman periyodu:** Akım.

**Kapsam:** Site.

**Bilgi:**

- Her yüklü yazılım için:

- Kurulum sayısı.

## Yazılım Denetim Raporu

**Zaman periyodu:** Akım.

**Kapsam:** Site.

**Bilgi:**

- Rapor, Site'deki her cihaz için aşağıdaki bilgileri gösterir:

- Yüklü yazılım
- Yazılım versiyonu

## Kullanıcı Yazılımı Kurulumu

**Zaman periyodu:** Son 30 gün.

**Kapsam:** Site.

**Bilgi:**

- Her yüklü yazılım için:

- Yazılım adı
- Sürüm
- Değişiklikler (eklenen veya silinmiş)
- Eylemin alındığı tarih

## Site Deposu

**Zaman periyodu:** Akım.

**Kapsam:** Site.

**Bilgi:**

- Her cihaz için:

- İsim
- Mektup
- Boyut
- Boş alanın miktarı ve yüzdesi

## Site IP Bilgisi

**Zaman periyodu:** Akım.

**Kapsam:** Site.

**Bilgi:**

- Her cihaz için:

- Adaptör adı
- IP adresi

## Detaylı Bilgisayar Denetimi

**Zaman periyodu:** Son 7 veya 30 gün.

**Kapsam:** Hesap.

**Bilgi:**

- Her bilgisayar için:

- Donanım bilgisi: varlık etiketi ve tarihi, Seri numarası, bellek, ana kart, BIOS, işlemci, video
- Alan adı ve kullanıcı adı
- Virüs tarayıcı detayları
- Son temas tarihi
- İşletim sistemi, Windows güncellemesi
- IP ve MAC adresleri
- Fiziksel disk sürücüsü boyutu ve boş alan

## Cihaz Özeti

**Zaman periyodu:** Akım.

**Kapsam:** Cihaz.

**Bilgi:**

- Her cihaz için:

- Ajan sürümü ve durumu
- Domain, son kullanıcı
- Son denetim tarihi, son görülme tarihi
- Donanım: üretici, model, kimlik, anakart, işlemci, bellek, depolama, ekran ve ağ bağdaştırıcıları ve bilgileri izleme
- Yazılım: işletim sistemi, servis paketi, seri numarası, sürüm numarası ile kurulmuş yazılım
- Güvenlik: anti-virüs, güvenlik duvarı ve güncellemeler

## **Cihaz Deęişiklięi Günlüęü**

**Zaman periyodu:** Son ajan kurulduęundan beri.

**Kapsam:** Cihaz.

**Bilgi:**

- Sistemdeki deęişiklikler:

- Yazılım deęiştirildięinde, eklenir veya silinir.
- Tarih ve IP adresi.

## **Site Cihazı**

**Zaman periyodu:** Akım.

**Kapsam:** Site.

**Bilgi:**

- Her cihaz için:

- IP adresi
- Son güncelleme tarihi
- Model, Seri Numarası
- Son giriş yapan kullanıcı

## **Envanter Yaşı**

**Zaman periyodu:** Akım.

**Kapsam:** Site.

**Bilgi:**

- Önümüzdeki 12 ay ile iki yıl arasındaki deęiştirme önerilerini gösterir
- Kullanımdaki işletim sistemlerini listeler
- Bireysel cihazları isme, son kullanıcıya, seri numarasına ve yapım tarihine göre listeler.
- Düşük bellek, boş disk alanı veya çevrimiçi olmayan bu ay için uyarılar

## **Microsoft Lisansı**

**Zaman periyodu:** Akım.

**Kapsam:** Site.

**Bilgi:**

- Yüklenen ürünle birlikte yazılım türünü, Microsoft ürün adını ve cihazların miktarını listeler.

## Sağlık Raporları

### Müşteri Sağlık Özeti

**Zaman periyodu:** Akım.

**Kapsam:** Site.

**Bilgi:**

- Donanım Özeti
- Güvenlik Özeti
- Bakım yazılımı Özeti
- Oyuncular ve okuyucular yüklü
- Kaç cihaz başarısız oldu veya testi geçti
- Uyarı veren cihazlar

### İstisna raporu

**Zaman periyodu:** Akım.

**Kapsam:** Site.

**Bilgi:**

- Tüm MS Windows cihazlarının özeti:
  - Güncellenmeyen virüsten korunmayan cihazlara yönelik uyarılar
  - MS güncellemeleri
  - Güvenlik Duvarı
  - Düşük boş disk alanı olan cihazlar
  - Bu ay çevrimiçi olmayan cihazlar

### Site Sağlığı

**Zaman periyodu:** Akım.

**Kapsam:** Site.

**Bilgi:**

- İşletim sistemine göre cihazların sayısını listeler:
  - Yapı numarası
- Olmayan cihaz sayısını listeler:
  - Güncellenmiş anti-virüs,
  - MS güncellemeleri veya güvenlik duvarı
  - Düşük boş disk alanı veya hafıza



- Bu ay çevrimiçi değil

- Her cihaz için:

- İsim
- Son giriş yapan kullanıcı
- Durum

## **Sağlık raporu**

**Zaman periyodu:** Son 30 gün.

**Kapsam:** Site.

### **Bilgi:**

- Uyarılar olsun veya olmasın sunucular ve iş istasyonları tarafından özet
- Uyarıları, işleri çalıştırır ve uzaktaki geçiş dakikalarını listeler
- Uyarı dönüş süresi özeti
- Tek tek cihazları ana makine adına, IP adresine ve son giriş yapan kullanıcıya göre listeler.
- Güncelleştirilmiş virüsten koruma, casus yazılım önleme, MS güncellemeleri veya güvenlik duvarları olmayan cihazlara yönelik uyarıları gösterir
- Bu ay çevrimiçi değil, düşük disk alanı olan cihazlar için uyarılar gösterir.

## **Yama Yönetimi Raporları**

### **Yama Yönetimi Etkinliği Raporu**

**Zaman periyodu:** Son 30 gün.

**Kapsam:** Site.

### **Bilgi:**

- Rapor, her cihaz için aşağıdaki bilgileri gösterir:
  - Serbest bırakılan yama sayısı, yüklü ve onaylanmış yamalar onaylanmış yamalar
  - Onaylanmış bekleyen yamaların yüzdesi ve uyarı sayısı
- Dikkat gerektiren cihazlar
- Tamamen yamulmuş / tamamen yamalanmamış cihazların özeti ve analizi
- Cihazlara göre yamaların ayrıntılı listesi:
  - İsim
  - Kritik derecelendirme
  - Kurulum durumu

## **Yama Yönetimi Detaylı Raporu**

**Zaman periyodu:** Akım.

**Kapsam:** Site.

### **Bilgi:**

- Her cihaz için:

- Yayılmış, yüklü ve eksik yama sayısı
- Yüzde kayıp ve uyarı sayısı

- Eksik yamaları içeren cihazları listeler

- Gereken yamalar sayısına göre yamaları gerektiren cihazların özeti ve analizi

- Cihazlara göre yamaların ayrıntılı listesi:

- İsim
- Kritik derecelendirme
- Kurulum durumu

## **Yama Yönetimi Özet Raporu**

**Zaman periyodu:** Akım.

**Kapsam:** Site.

### **Bilgi:**

- Cihazların yüzdesi tamamen yamalı veya belirli sayıda yamaları eksik

- Eksik yamaları ve eksik numaralarını listeler

- Her cihaz için:

- Yayılmış, yüklü ve eksik yama sayısı

## **Diğer Raporlar**

### **Site Kullanıcı Tanımlı Alanlar**

**Zaman periyodu:** Akım.

**Kapsam:** Site.

### **Bilgi:**

- Kullanıcı Tanımlı Alanlar Raporu

## **Sunucu Performans Raporu (Site Düzeyi)**

**Zaman periyodu:** Son 30 gün.

**Kapsam:** Site.

**Bilgi:**

- Her sunucu için performans gösterir:

- CPU
- Bellek
- Disk
- CPU ve Hafızanın Ortalama
- Kullanılabilir disk alanı deltası

## **Sunucu Performans Raporu (Hesap Seviyesi)**

**Zaman periyodu:** Akım.

**Kapsam:** Hesap.

**Bilgi:**

- Her sunucu için performans gösterir:

- CPU
- Bellek
- Disk
- CPU ve Hafızanın Ortalama
- Kullanılabilir disk alanı deltası

# Servis erişim güvenliği ve kontrolü

## Giriş

Yöneticiler, aşağıdakiler dahil olmak üzere, Panda Systems Management servisine erişim güvenliğini artırmak için çeşitli araçlara sahiptir:

- İki faktörlü kimlik doğrulama.
- Şifre politikaları.
- Konsola erişim izni vermek veya erişimi reddetmek için IP adresi kısıtlamaları.
- Aracıdan Sunucuya erişim izni vermek veya engellemek için IP adresi kısıtlamaları.

## İki faktörlü kimlik doğrulama

İki faktörlü kimlik doğrulama, Konsol giriş ekranında girilen yönetici kimlik bilgilerini doğrulamak için ikinci bir cihazın kullanılmasını gerekli kılar. Dolayısıyla, kimlik bilgilerini girmenin yanı sıra, yönetici, telefonlarında her dakika otomatik olarak oluşturulmuş bir kişisel kod da girmelidir.

## Temel gereksinimleri

- Jeton üreten uygulamayı destekleyen bir mobil cihaz.
- Ücretsiz uygulama Google Authenticator veya mobil cihazda yüklü diğer uyumlu uygulama.

## Ayarlar


Aşağıda, Konsolda oturum açan yönetici hesabında İki Faktörlü Kimlik Doğrulamanın etkinleştirilmesi için gerekli adımları açıklıyoruz:

- Genel menü Kurulum, Bilgilerim sekmesine gidin. Güvenlik ayarları bölümüne ilerleyin ve İki Faktörlü Kimlik Doğrulamayı Etkinleştir'e tıklayın.
- Ekranda bir QR Kodu ve belirteci girmek için bir boşluk göreceksiniz. Bu jeton Google Authenticator tarafından oluşturulmuştur. Bir QR Kodu okuyabilen bir kimlik doğrulama uygulamanız yoksa, sistemin aynı sayfada belirtilen yöneticinin e-posta adresine bir QR Kodu göndermesine izin veren onay kutusunu seçebilirsiniz.
- Konsoldan erişen yöneticinin mobil cihazında Google Play'den Google Authenticator'ı yükleyin (bkz. Bu bölümde daha sonra Google Authenticator'ı Yükleme konusuna bakın).
- Konsolda görüntülenen kodu taramak için Ayarlamaya başla ve barkodu tara'ya dokununuz. Yüklü barkod tarayıcısı yoksa, uygulama ücretsiz program ZXing Barkod Tarayıcısını yüklemenizi önerir.

### Enable Two-Factor Authentication


**Please Note:**

Before activating "Two-Factor Authentication" (2FA), ensure you have set a valid Telephone number that can receive SMS messages. This number will be used for account recovery purposes and needs to be set on the previous Account Details page.



Scan the QR Code to left using an application like Google Authenticator, then enter a generated code in the box below.

Save

Not got access to an authenticator? Have the codes emailed to you instead 

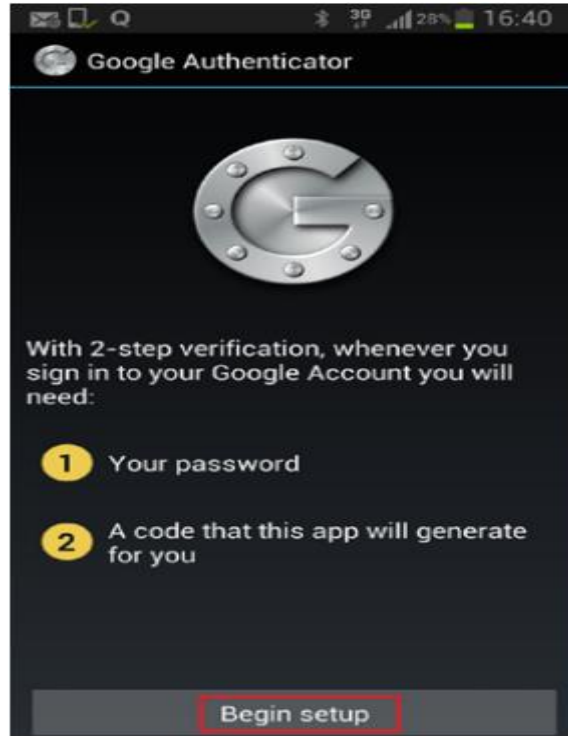
- QR kodunu taradıktan sonra, uygulama her 30 saniyede bir belirteç oluşturmaya başlar. Bir jeton oluşturmanız ve İki Faktörlü Kimlik Doğrulamayı tam olarak etkinleştirmek için Konsol giriş ekranındaki ilgili alana girmeniz gerekir.

- O andan itibaren, yönetici yalnızca geçerli bir belirteçle birlikte kimlik bilgilerini doğru bir şekilde girdiğinde hesaplarına erişebilir.

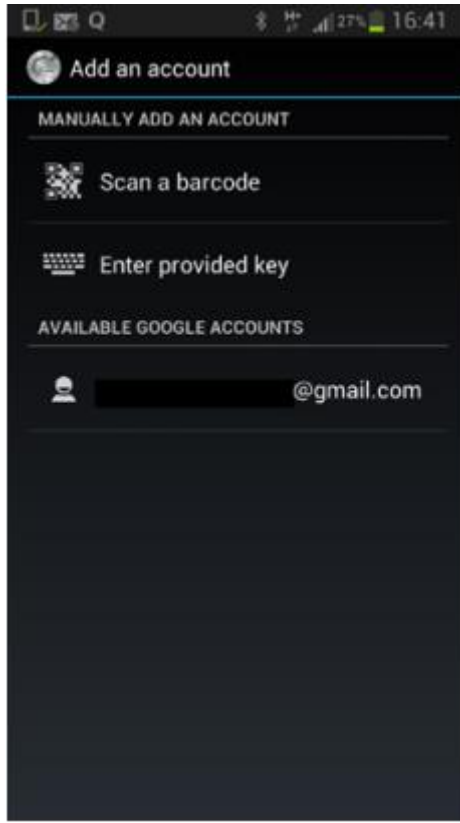
### Google Authenticator'ı yükleme

Android uyumlu bir mobil cihazda Google Authenticator'ı yüklemek için aşağıdaki adımları izleyin:

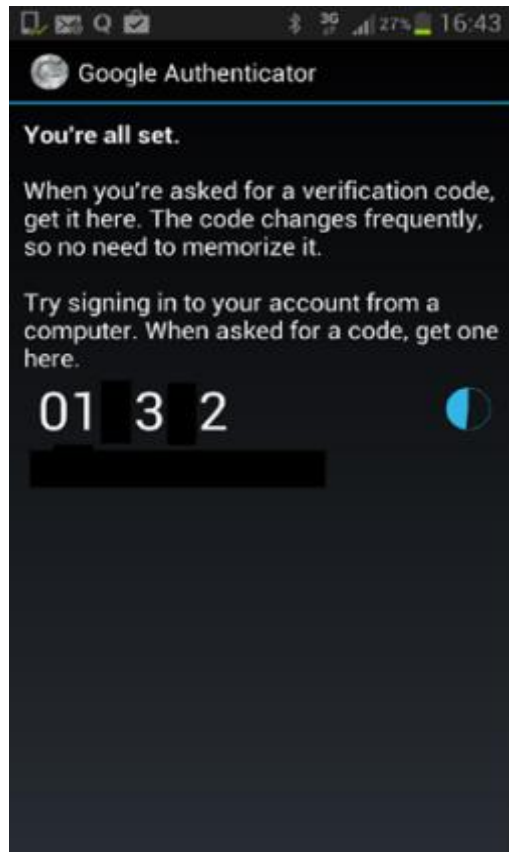
- Google Play'den uygulamayı indirin.
- Uygulama başladıktan sonra Kurulumu Başlat'a dokununuz



- Konsolda görüntülenen QR kodunu taramak için Bir barkod tarama'ya dokununuz.



- Uygulama otomatik olarak belirteçleri üretmeye başlayacaktır. Her simge 30 saniye boyunca geçerlidir.

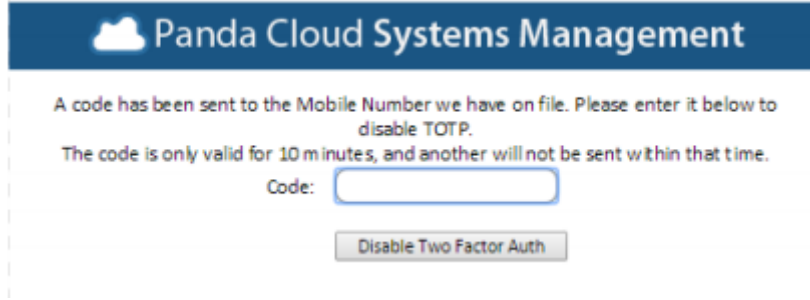


## Tüm hesaplar için iki faktör kimlik doğrulamasını etkinleştirme

Yönetici hesabı için iki Faktörlü Kimlik Doğrulama etkinleştirildikten sonra, Konsolda oluşturulan diğer yönetici hesapları için kullanılmasını zorlamak mümkündür. Bunu yapmak için genel menü Hesap, Kurulum, İki Faktör Kimlik Doğrulaması Gerektirir seçeneğini tıklatın. Fwo-Factor Authentication yapılandırılmamış bir kullanıcı Console'a eriştiğinde, bir uyarı mesajı görür ve konsolu kullanamazlar.

## Giriş ekranından İki Faktörlü Kimlik Doğrulamayı Devre Dışı Bırakma

Giriş ekranından İki Faktörlü Doğrulamayı devre dışı bırakmak mümkündür. Bunu yapmak için, kullanıcı adı ve şifreyi doğru bir şekilde girmeniz gerekir ve ekranın belirtilmesini istediğinizi göreceksiniz. Altta TOTP'yi Devre Dışı Bırakmak için bir bağlantı var. Bağlantıya tıklayın ve Sunucu, sistemde yapılandırılan telefon numarasına 10 dakika boyunca geçerli bir kod içeren bir SMS gönderecektir. İki Faktörlü Kimlik Doğrulama hizmetini devre dışı bırakmak için kodu girin.



The screenshot shows a web interface for Panda Cloud Systems Management. At the top, there is a blue header with the Panda logo and the text "Panda Cloud Systems Management". Below the header, there is a message: "A code has been sent to the Mobile Number we have on file. Please enter it below to disable TOTP. The code is only valid for 10 minutes, and another will not be sent within that time." Below the message, there is a text input field labeled "Code:" and a button labeled "Disable Two Factor Auth".

## Şifre Politikası(Password Policy)

Konsol'a erişim ile ilgili güvenliği güçlendirmek için, yöneticiler bir parola ilkesi kurabilir ve bu da tüm parolaların belirli gereksinimleri karşılaması gerektiği anlamına gelir.

Şifre politikasını yapılandırmak için Genel menüye, Hesaplar, Ayarlar'a gidin ve aşağıdaki alanlarda ilgili değerleri girin:

- **Şifre son kullanma tarihi:** Şifrenin maksimum süresini ayarlar (30, 60, 90 gün veya asla bitmez).
- **Benzersiz şifreler:** Sistem, her bir hesap için bir şifre listesi saklar, böylece yöneticiler bir şifre değiştirildiğinde bunları yeniden kullanamazlar. Şifre geçmişi, 0 (asla) ile 6 giriş arasında bir değere sahip olacaktır.

## Konsol'a erişim izni vermek veya erişimi reddetmek için IP adresi kısıtlamaları

Konsol'a erişimi bilinen bir IP adresi kümesine kısıtlamak için, Genel Ayarlar, Ayarlar menüsüne gidin ve PSM Konsolu IP Adresi Kısıtlama seçeneğini etkinleştirin. Daha sonra, Yasak IP Listesi'nde, Konsola erişiminin mümkün olabileceği IP'lerin listesini ayarlayın.

## **Ajandan Sunucuya eriřim izni vermek veya engellemek için IP adresi kısıtlamaları**

Araçlardan servise erişimi kısıtlamak için, Genel Ayarlar, Ayarlar menüsüne gidin ve Aracı IP Adresi Kısıtlama seçeneğini etkinleştirin. Sonra, Yasak IP Listesi'nde, Araçların Sunucuya erişebileceği IP'lerin listesini ayarlayın.