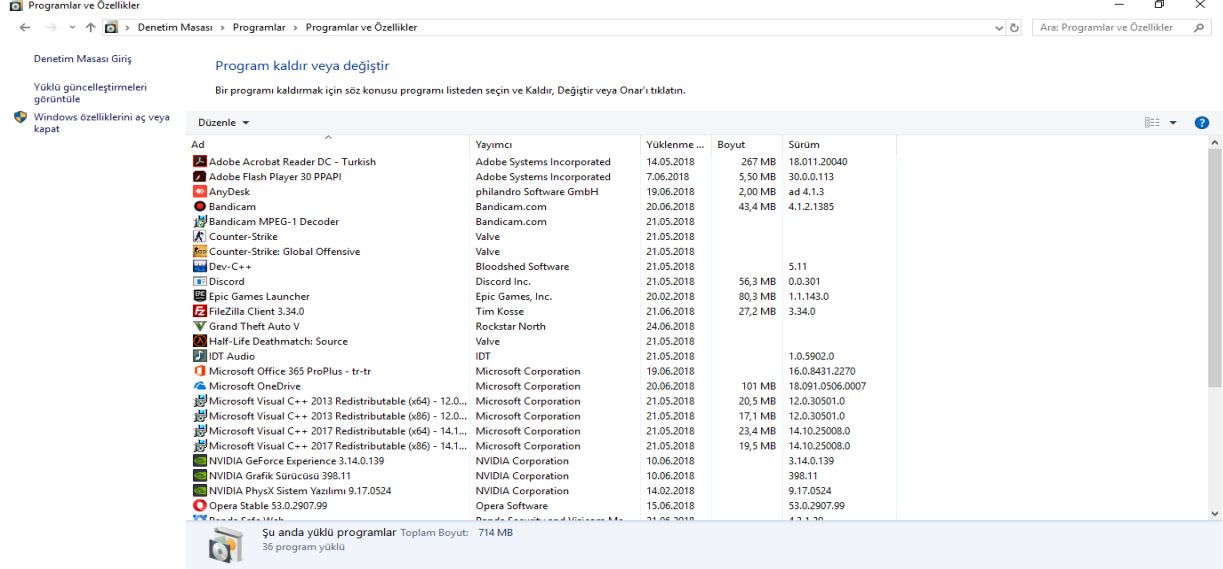


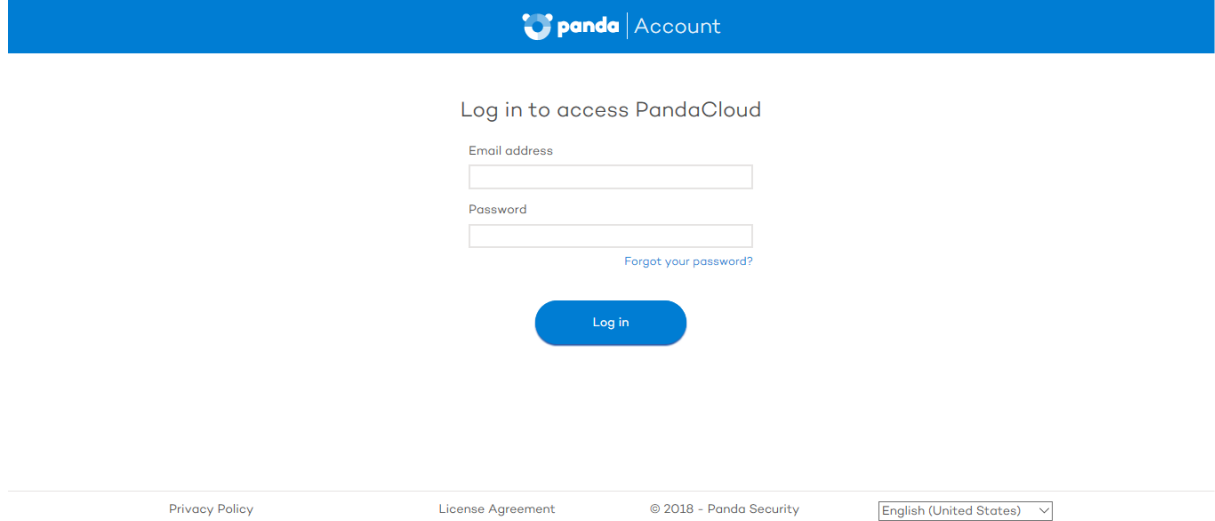
ADAPTIVE DEFENSE 360

1- Öncelikle kurmak istediğiniz bilgisayarın içinde herhangi bir antivirüs programı olmaması gerekmektedir.



2- Panda cloud hesabını oluştuktan sonra aktivasyon işlemi için mail adresinize bir PDF dosyası gelecektir.

3- www.pandacloudsecurity.com/PandaLogin/ sistemine giriş yapmanız gerekmektedir.



4- Giriş yaptıktan sonra ekrana kendi mevcut servisleriniz gözükmetedir.

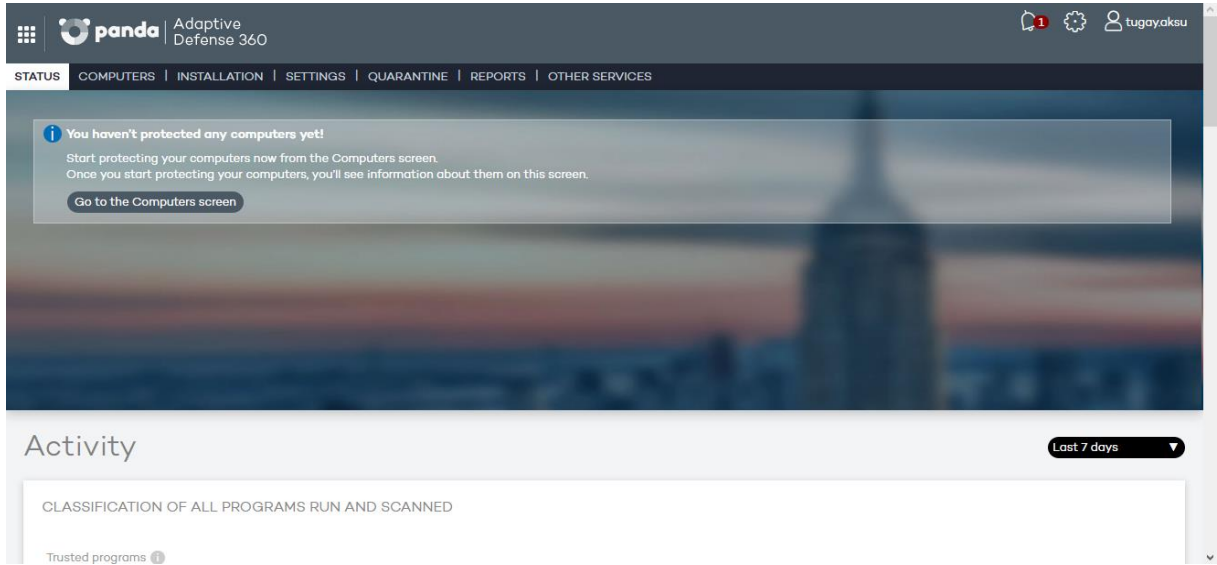
My services



Adaptive Defense
360
Trial version

5- Açılan pencerede Adaptive Defense 360 logosuna tıklıyoruz.

6- Karşımıza Adaptive Defense 360 ürünün arayüzü gelmektedir.



7- Buradan "Computers(Bilgisayarlar)" sekmesine tıklıyoruz. Açılan pencerede karşımıza "Install on this computer now" çıkmaktadır. Windows, Android ve Linux için indirme linkleride tam altında belirtilmiştir. Bu seçeneğe tıkladığımız takdirde WAAgent adında bir setup indirmektedir.

Start protecting your computers

You still haven't protected any computers. Once you start protecting them, they will appear on this screen.



 Install on this computer now

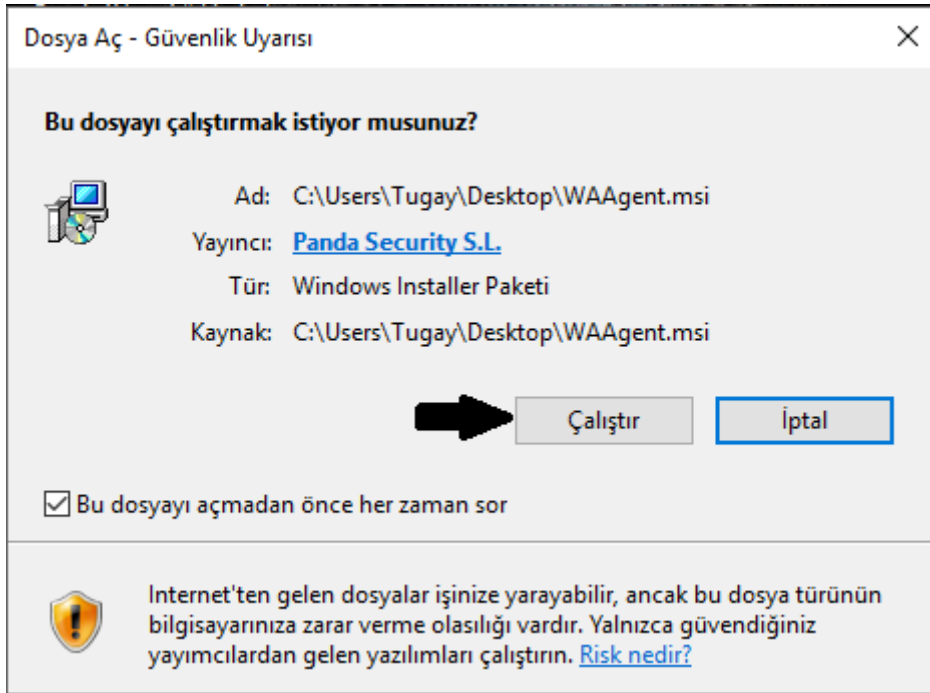
 Send installation URL by email

Download installer for: [Windows](#), [Linux](#) and [Android](#).

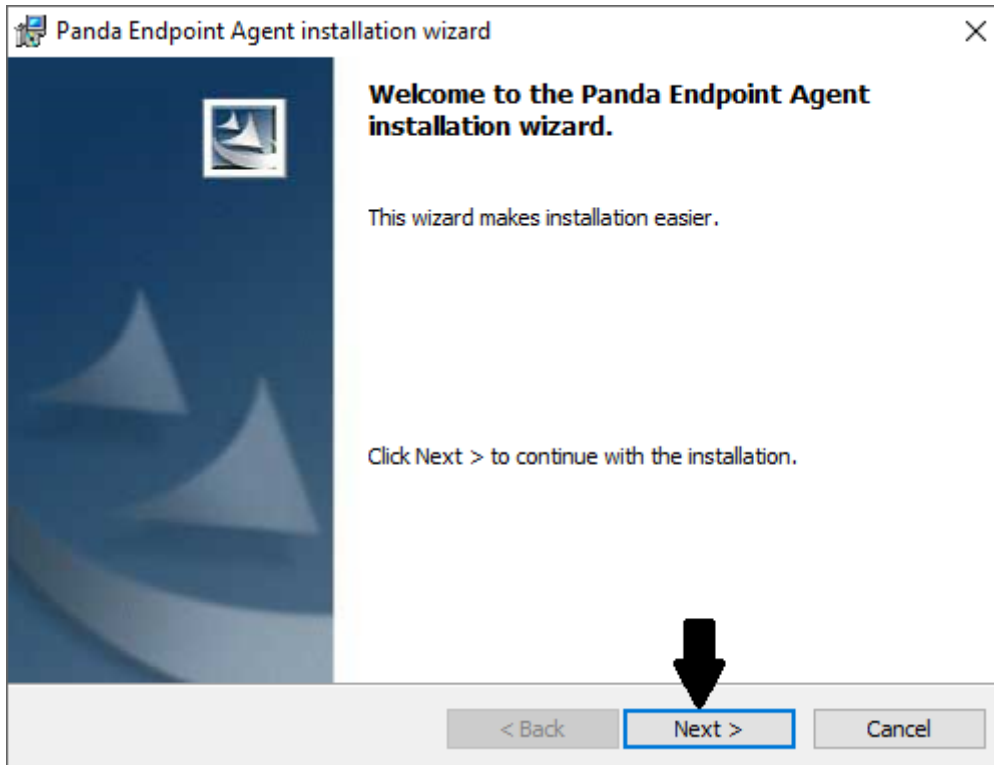
Download [distribution tool](#) for Windows.



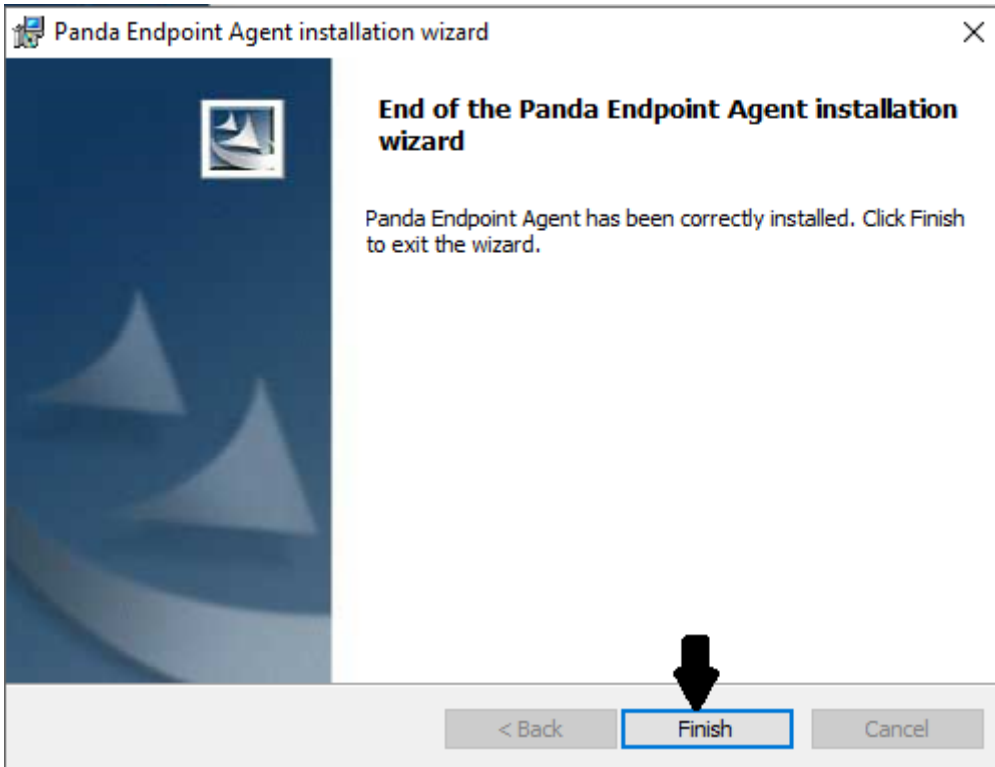
8- İndirilen WAAgent setup şeklinde çalıştırıyoruz.



9- “Çalıştır” dedikten sonra açılan pencerede “Next” butonuna basıyoruz.



10- Kurulum yapıldıktan sonra "Finish" butonuna basıyoruz.



11- Daha sonra bilgisayarın sağ altına icon gelecektir. Bunu sol tıklayıp açmamız gerekir.



12- Şekildeki simgeye tıkladığımızda bir ekran gelecektir. Bu ekranı beklememiz gerekmektedir.

Installing Panda Endpoint Agent

- Connecting to the server
- Getting configuration data
- Getting Knowledge
- Downloading protection
- Installing protection**

Close

13- Yüklemler bittikten sonra “close” seçeneğine basarak kapatabiliriz.

Installing Panda Endpoint Agent

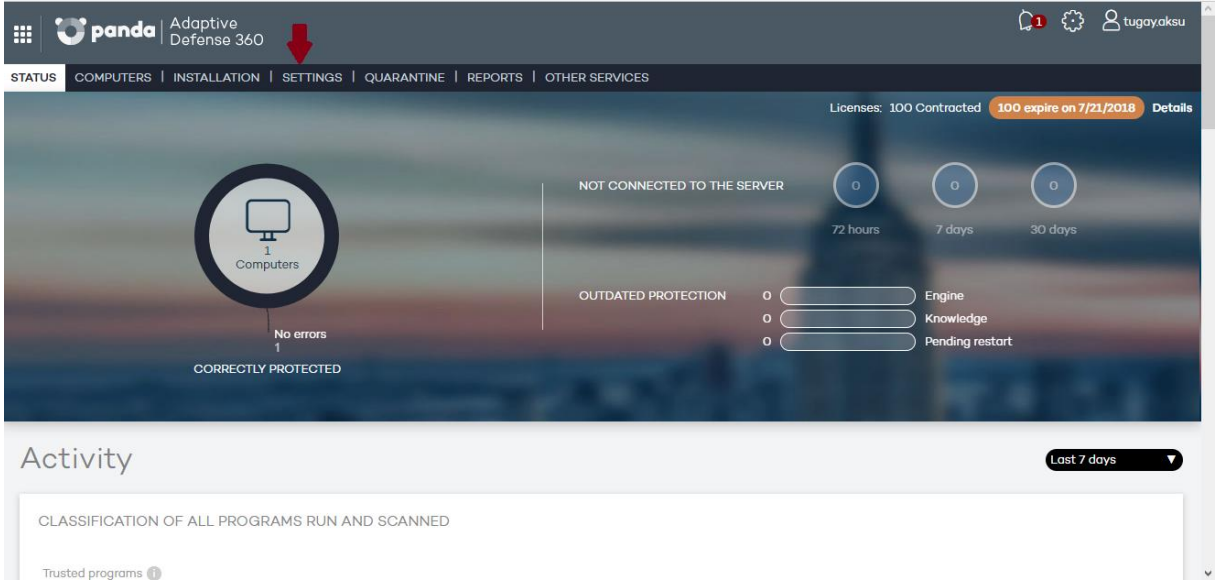
- Connecting to the server
- Getting configuration data
- Getting Knowledge
- Downloading protection
- Installing protection



14- Bilgisayarın istediği takdirde yeniden başlatın. Eğer istemezse yeniden başlatmanıza gerek yoktur.

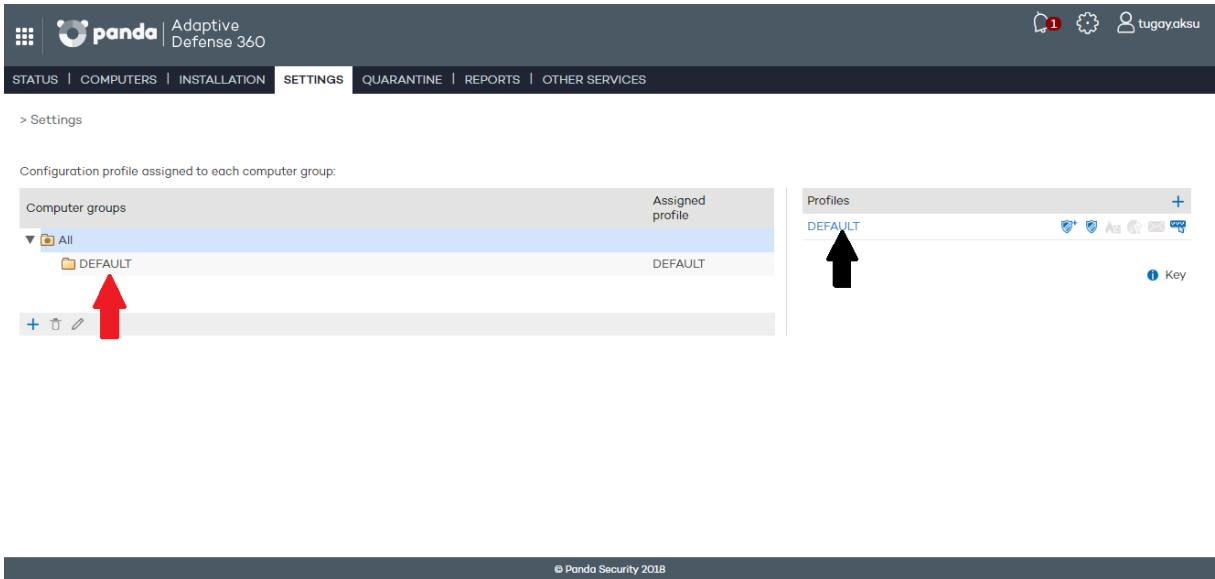
SETTINGS(AYARLAR)

1- Adaptive Defense arayüzünden settings(ayarlar) kısmına tıklıyoruz.



The screenshot shows the Panda Adaptive Defense 360 dashboard. The 'SETTINGS' tab is selected in the top navigation bar. The main dashboard area displays system status: 'Computers' (1), 'Licenses: 100 Contracted' (with a warning that 100 expire on 7/21/2018), and 'NOT CONNECTED TO THE SERVER' (72 hours, 7 days, 30 days). Below this, 'OUTDATED PROTECTION' is shown for Engine, Knowledge, and Pending restart. The 'Activity' section is also visible, showing 'CLASSIFICATION OF ALL PROGRAMS RUN AND SCANNED' and 'Trusted programs'.

2- Açılan pencerede siyah ok ile gösterilen yerde yeni profiller ekleyebilir veya eklediğimiz profilleri kaldırabiliriz. Kırmızı ok ile gösterilen yerde profilleri gruplandırabilme özelliği mevcuttur.

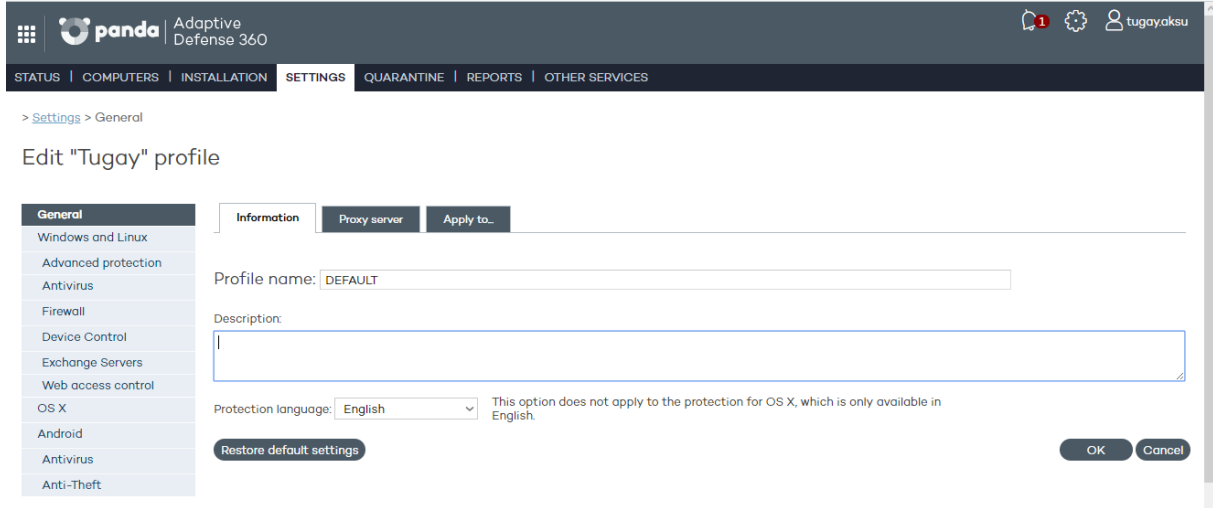


The screenshot shows the 'Settings' page in the Panda Adaptive Defense 360 interface. The 'Computer groups' table is visible, showing a table with columns 'Computer groups' and 'Assigned profile'. The table contains two rows: 'All' and 'DEFAULT'. A red arrow points to the '+' icon in the bottom left corner of the table. The 'Profiles' section is also visible, showing a 'DEFAULT' profile. A black arrow points to the 'DEFAULT' profile in the 'Profiles' section.

Computer groups	Assigned profile
All	
DEFAULT	DEFAULT

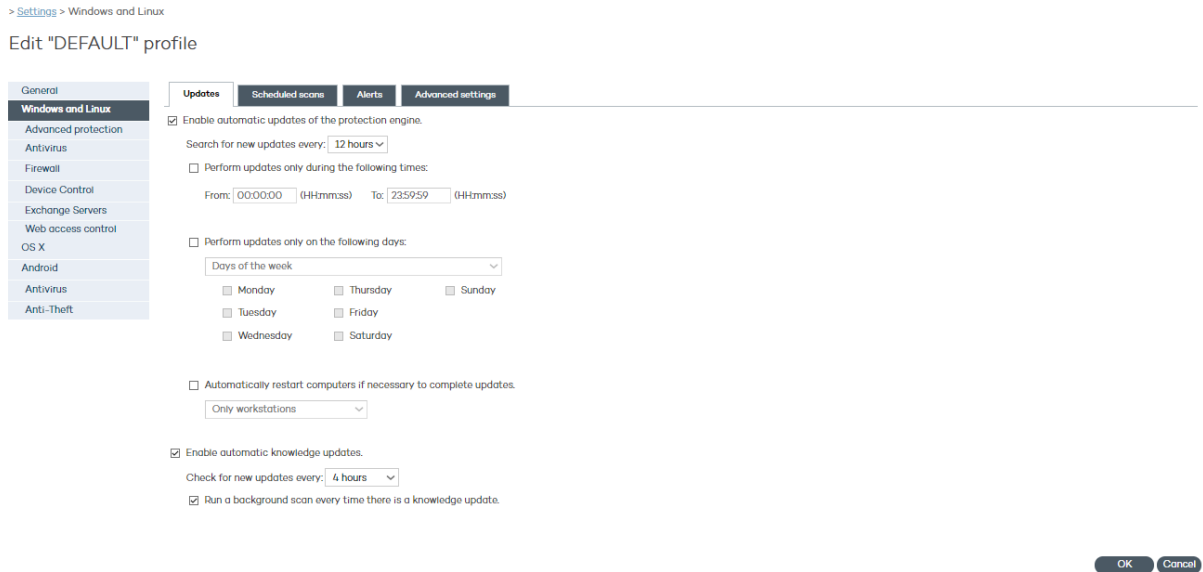
Profiles: DEFAULT

3- Siyah ok ile gösterilen yere tıkladığımızda karşımıza aşağıdaki gibi bir pencere gelmektedir. Ayrıca ayarları kaydetmek için ekran değiştirmeden önce "OK" butonuna basılmalıdır. Genel ayarlamalar bu sekme içinden yapılmaktadır. "General(Genel)" sekmesinden isim ve açıklama bölümlerini ayarlayabilirsiniz.



The screenshot shows the Panda Adaptive Defense 360 settings interface. The top navigation bar includes 'STATUS', 'COMPUTERS', 'INSTALLATION', 'SETTINGS', 'QUARANTINE', 'REPORTS', and 'OTHER SERVICES'. The user is logged in as 'tugay.aksu'. The current view is 'Settings > General' for the 'Tugay' profile. The 'General' tab is active, showing the following options: 'Information', 'Proxy server', and 'Apply to...'. The 'Profile name' is set to 'DEFAULT'. The 'Description' field is empty. The 'Protection language' is set to 'English'. A note states: 'This option does not apply to the protection for OS X, which is only available in English.' There are 'Restore default settings', 'OK', and 'Cancel' buttons.

4- "Windows and Linux" sekmesinde gerekli güncelleme ayarlarını ve ayarların saatlerini ayarlayabilirsiniz.



The screenshot shows the Panda Adaptive Defense 360 settings interface for the 'DEFAULT' profile. The 'Windows and Linux' tab is active, showing the following options: 'Updates', 'Scheduled scans', 'Alerts', and 'Advanced settings'. The 'Updates' section is expanded, showing the following options: 'Enable automatic updates of the protection engine' (checked), 'Search for new updates every: 12 hours', 'Perform updates only during the following times' (unchecked), 'Perform updates only on the following days' (unchecked), 'Automatically restart computers if necessary to complete updates' (unchecked), and 'Enable automatic knowledge updates' (checked). The 'Check for new updates every' is set to '4 hours'. There are 'OK' and 'Cancel' buttons.

5- "Advanced Protection" sekmesinde pandanın size sunmuş olduğu üst düzey korumadan yararlanabilirsiniz. Size sunulan özellikler sayesinde bilgisayarınıza herhangi bir virüs bulaştığında otomatik kaldıracaktır. Ayrıca bakılmaması gereken uzantı,klasör veya dosyaları el ile ayarlayabilirsiniz.

Edit "DEFAULT" profile

General	The advanced protection tracks the activity of every program run on your computers, immediately detecting and blocking malicious programs. Additionally, it acts against any suspicious or potentially dangerous item in record time thanks to direct monitoring by Panda lab technicians.
Windows and Linux	
Advanced protection	<input checked="" type="checkbox"/> Enable advanced protection. (Only Windows devices)
Antivirus	
Firewall	Behavior Anti-exploit Exclusions Network usage Privacy
Device Control	
Exchange Servers	<input type="radio"/> Audit The solution tracks the activity of every program run on your computers but will not act if a detection takes place.
Web access control	<input checked="" type="radio"/> Hardening Malicious and potentially malicious programs will be removed. Unknown programs coming from the Internet or an external storage drive will be blocked until our lab determines whether they are malware or not. <input type="radio"/> Do not report blocking to the computer user <input checked="" type="radio"/> Report blocking to the computer user Any other unknown program will be initially allowed to run while it is being analyzed by our lab.
OS X	
Android	
Antivirus	<input type="radio"/> Lock Malicious and potentially malicious programs will be removed. Unknown programs will be blocked until our lab determines whether they are malware or not. <input type="radio"/> Do not report blocking to the computer user <input checked="" type="radio"/> Report blocking to the computer user <input type="radio"/> Report blocking and give the computer user the option to run the item (recommended for advanced users or administrators only)
Anti-Theft	

OK Cancel

> Settings > Windows and Linux > Advanced protection

Edit "DEFAULT" profile

General	The advanced protection tracks the activity of every program run on your computers, immediately detecting and blocking malicious programs. Additionally, it acts against any suspicious or potentially dangerous item in record time thanks to direct monitoring by Panda lab technicians.
Windows and Linux	
Advanced protection	<input checked="" type="checkbox"/> Enable advanced protection. (Only Windows devices)
Antivirus	
Firewall	Behavior Anti-exploit Exclusions Network usage Privacy
Device Control	
Exchange Servers	The anti-exploit protection prevents malicious programs from exploiting known and unknown (zero-day) vulnerabilities in applications to access computers on the corporate network.
Web access control	<input checked="" type="checkbox"/> Detect exploits <input type="radio"/> Audit Tracks exploits' activities but doesn't take any action or display any information to the computer user upon detection.
OS X	<input checked="" type="radio"/> Block Blocks exploits. In some cases it may be necessary to end the compromised process or restart the computer. <input type="checkbox"/> Report blocking to the computer user <input checked="" type="checkbox"/> Ask the user for permission to end a compromised process (may result in data loss in some cases)
Android	
Antivirus	
Anti-Theft	

OK Cancel

General	The advanced protection tracks the activity of every program run on your computers, immediately detecting and blocking malicious programs. Additionally, it acts against any suspicious or potentially dangerous item in record time thanks to direct monitoring by Panda lab technicians.
Windows and Linux	
Advanced protection	<input checked="" type="checkbox"/> Enable advanced protection. (Only Windows devices)
Antivirus	
Firewall	Behavior Anti-exploit Exclusions Network usage Privacy
Device Control	
Exchange Servers	
Web access control	
OS X	
Android	
Antivirus	
Anti-Theft	

Changing these settings will reduce the security level
Every time you exclude a file or a folder from scanning, there is a chance that malware gets run on your computer without Adaptive Defense 360 being able to detect it.

These settings affect both the antivirus protection and the advanced protection.

Extensions to exclude:

Add

Delete

Clear

Folders to exclude:

Add

Delete

Clear

Files to exclude:

Add

Delete

Clear

OK Cancel

6- "Antivirüs" sekmesinde bilgisayardaki dosyaları ve kendisini korumamıza olanak sağlar. "Files", "Mail" ve "Web" seçeneklerindeki bütün kutulardaki tick işaretlerinin aktif olması gerekmektedir.

> Settings > Windows and Linux > Antivirus

Edit "DEFAULT" profile

General	Files	Mail	Web
Windows and Linux			
Advanced protection			
Antivirus			
Firewall			
Device Control			
Exchange Servers			
Web access control			
OS X			
Android			
Antivirus			
Anti-Theft			

Enable permanent file protection. [Advanced settings](#)

Scan compressed files.

Software to detect

Viruses

Hacking tools and PUPs

Behavioral detection technologies

Block malicious actions

OK Cancel

7- "Firewall" sekmesinden iş yerleri ya da serverlar için güvenlik ayarlarını yapılandırabilirsiniz.

> Settings > Windows and Linux > Firewall

Edit "DEFAULT" profile

General	<input type="radio"/> Let computer users configure the firewall.
Windows and Linux	<input checked="" type="radio"/> Apply the following settings to the firewall.
Advanced protection	<input type="checkbox"/> Enable firewall for Windows workstations
Antivirus	<input type="checkbox"/> Enable firewall for Windows servers
Firewall	General Programs Intrusion prevention System
Device Control	Computers are connected to the following network type:
Exchange Servers	<input type="radio"/> Public network Public places such as airports, Internet cafés, universities, etc. Computers are not visible to other users on the network and some programs will have limited access to the network.
Web access control	<input checked="" type="radio"/> Trusted network Home or office networks where you know and trust the other users and devices on the network. Computers are visible to the other computers and devices on the network.
OS X	
Android	
Antivirus	
Anti-Theft	

OK Cancel

8- "Device Control" sekmesinden bilgisayarınıza herhangi bir USB,telefon,CD/DVD/Blu-ray vs. gibi araçların kullanılabilmesi için ayarların yapıldığı yerdir. Ayrıca aşağıdaki kısımda istediğiniz cihazı tanıtırıp kısıtlama yapmadan çalışmaya olanak sağlar.

> Settings > Windows and Linux > Device Control

Edit "DEFAULT" profile

General

Windows and Linux

Advanced protection

Antivirus

Firewall

Device Control

Exchange Servers

Web access control

OS X

Android

Antivirus

Anti-Theft

Enable device control

Settings

Removable storage drives: Allow read & write access

Mobile devices: Allow

CD/DVD/Blu-ray drives: Allow read & write access

Image capture devices: Allow

Bluetooth devices: Allow

Modems: Allow

Allowed devices

The following devices can be used without restrictions:

Name	Type	Instance ID
------	------	-------------

Add_

Delete

Clear

Import_

Export

OK Cancel

9- "Exchange Servers" sekmesinde maillerden ve aktarım şeklinde koruma sağlamaktadır. Anti-spam sekmesinde ise "Detect Spam" kutusuna tıkladığınız takdirde spam algılamanıza ve neler yapılması gerektiğine karar vermenize olanak sağlar. Ayrıca "Content filtering" sekmesinde dosyaları uzantılarına göre işlem uygulayabilirsiniz.

> Settings > Windows and Linux > Exchange Servers

Edit "DEFAULT" profile

General | **Antivirus** | Anti-spam | Content filtering | Quarantine

Windows and Linux

Advanced protection
Antivirus
Firewall
Device Control

Exchange Servers

Web access control
OS X
Android
Antivirus
Anti-Theft

Enable mailbox protection
 Enable transport protection

Software to detect

Viruses
 Hacking tools and PUPs

Intelligent mailbox scan

The intelligent mailbox scan runs during periods of low server activity, scanning the email messages stored in the organization's Exchange server. Scanning is performed only on files that have not been previously scanned.

Enable intelligent mailbox scan

OK Cancel

> Settings > Windows and Linux > Exchange Servers

Edit "DEFAULT" profile

General | **Antivirus** | **Anti-spam** | Content filtering | Quarantine

Windows and Linux

Advanced protection
Antivirus
Firewall
Device Control

Exchange Servers

Web access control
OS X
Android
Antivirus
Anti-Theft

Detect spam

Action for spam messages

Specify what to do with spam messages:

Let the message through

The tag "[SPAM]" will be added to the subject line of messages let through.

Allowed addresses and domains

Emails coming from the following addresses and domains will be let through without being scanned:

Add
 Delete
 Clear

Spam addresses and domains

Emails coming from the following email addresses or domains will be considered spam:

Add
 Delete
 Clear

OK Cancel

> Settings > Windows and Linux > Exchange Servers

Edit "DEFAULT" profile

General | **Antivirus** | **Anti-spam** | **Content filtering** | Quarantine

Windows and Linux

Advanced protection
Antivirus
Firewall
Device Control

Exchange Servers

Web access control
OS X
Android
Antivirus
Anti-Theft

Take the following action on messages with dangerous attachments:

Delete the message

Consider files with the following extensions dangerous:

.ADE
.ADP
.BAS
.BAT
.CHM

Add
 Delete
 Clear
 Restore

Consider attachments with double extensions dangerous, except for the following:

.TAR.BZ2
.TAR.GZ
.TAR.LZ
.TAR.Z

Add
 Delete
 Clear
 Restore

OK Cancel

10- "Web Access Control" sekmesinde ise şirketlerdeki bilgisayarların girmesini istemediği siteler ayarlanabilir. Saat dilimlerinde siteleri açmak ve sadece belli başlı sitelere girmek için domain ve adreslerden erişimi sağlayan ek özellikler mevcuttur.

> Settings > Windows and Linux > Web access control

Edit "DEFAULT" profile

General

Windows and Linux

Advanced protection

Antivirus

Firewall

Device Control

Exchange Servers

Web access control

OS X

Android

Antivirus

Anti-Theft

Enable Web access control for Windows workstations

Enable Web access control for Windows servers

Always enabled

Enable only during the following times:

	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Monday																								
Tuesday																								
Wednesday																								
Thursday																								
Friday																								
Saturday																								
Sunday																								

Enabled Disabled Clear Select all

Web access restrictions

Deny access to pages belonging to the following categories:

<input type="checkbox"/> Advertisements & Pop-Ups	<input type="checkbox"/> Alcohol & Tobacco	<input type="checkbox"/> Anonymizers
<input type="checkbox"/> Arts	<input type="checkbox"/> Business	<input type="checkbox"/> Chat
<input type="checkbox"/> Child Abuse Images	<input type="checkbox"/> Computers & Technology	<input type="checkbox"/> Criminal Activity
<input type="checkbox"/> Cults	<input type="checkbox"/> Dating & Personals	<input type="checkbox"/> Download Sites
<input type="checkbox"/> Education	<input type="checkbox"/> Entertainment	<input type="checkbox"/> Fashion & Beauty
<input type="checkbox"/> Finance	<input type="checkbox"/> Forums & Newsgroups	<input type="checkbox"/> Gambling

Web access restrictions

Deny access to pages belonging to the following categories:

<input type="checkbox"/> Advertisements & Pop-Ups	<input type="checkbox"/> Alcohol & Tobacco	<input type="checkbox"/> Anonymizers
<input type="checkbox"/> Arts	<input type="checkbox"/> Business	<input type="checkbox"/> Chat
<input type="checkbox"/> Child Abuse Images	<input type="checkbox"/> Computers & Technology	<input type="checkbox"/> Criminal Activity
<input type="checkbox"/> Cults	<input type="checkbox"/> Dating & Personals	<input type="checkbox"/> Download Sites
<input type="checkbox"/> Education	<input type="checkbox"/> Entertainment	<input type="checkbox"/> Fashion & Beauty
<input type="checkbox"/> Finance	<input type="checkbox"/> Forums & Newsgroups	<input type="checkbox"/> Gambling

Deny access to pages categorized as unknown.

Always allow access to the following addresses and domains:

<input type="text"/>	Add
update.microsoft.com	Delete
http://www.update.microsoft.com	Clear
http://download.windowsupdate.com	
http://ds.download.windowsupdate.com	

Allows access to all addresses that start like the allowed addresses and domains (despite their full URL may be longer).

Deny access to the following addresses and domains:

<input type="text"/>	Add
<input type="text"/>	Delete
<input type="text"/>	Clear

Denies access to all addresses that start like the denied addresses and domains (despite their full URL may be longer).

OK Cancel