7/2011. SZ. GF UTASÍTÁS 1. SZ. MELLÉKLETE A PTE VÍRUSVÉDELMÉRŐL

1. Vírusvédelmi utasítás (üzemeltetői munkatársak részére, IT belső használatra)

1.1. Telepítőcsomagok beszerzése:

Az Egyetem által jelenleg megvásárolt szoftvereket az alábbi helyekről lehet letölteni:

Admin Kit:
http://www.2f.hu/files/kav/prg/kasp8.0.2134_adminkiten.exe
FileServer:
http://www.2f.hu/files/kav/prg/kav8.0.0.559_fseeen.exe
Workstation: http://www.2f.hu/files/kav/prg/kav6.0.4.1424_winwksen.exe

Workstation - Magyar nyelvű verzió:
http://www.2f.hu/files/kav/prg/kav6.0.4.1424_winwkshu.exe

1.2. Licensz File kezelése

A licensz file érvényessége 1 év. A licensz lejáratát az ezzel megbízott Informatikai Igazgatóság munkatársa figyeli és szükség esetén (pl.: a lejárat előtt minimum 2 hónap) indítja a Licensz megújítását az illetékesnél (Service Desk Osztály).
A licenszért felelős személy az új licensz file-okat e-mail-ben kapja meg, feladata a licenszek terjesztése a Kaspersky alkalmazásgazdák felé, illetve megőrzése (Pl.: CD-re írás, majd szoftverkönyvtár.)
Kaspersky Licensz file-ok (2010):

1. **0DA91A91 Szerver, Workstation 7000 Computers**

   Érvényesség: 2012.07.06 –ig.

Kontakt személy: **Balázs Attila - Daemia Kft.** attila.balazs@daemia.hu

1.3. Licensz telepítése az IIG szolgáltatási területén

- **2009.07 hó előtt telepített notebookok** esetében külön telepítve, ezeknél kézzel kell minden egyes gépen telepíteni.
- **Admin kit -es gépeken** teszt csoportra létrehozni Group taskot, majd ha a telepítés sikeres ráengedhető az összes gépre. Ehhez Global taskot kell létrehozni és azt futtatni, így az összes gépen megtörténik a frissítés.

1.4. Ütemezett feladatok:

1.4.1. Frissítések az IIG szolgáltatási területén:

- **Az Admin kit** minden 3. órában lekérdezi van-e frissítés a Kaspersky update server-en.
- Az **Updater task** minden 4. órában frissíti Group-okban lévő elérhető számítógépeket

- **2009-07. hó előtt telepített Notebook**-ok közvetlenül a Kaspersky update server-től töltik le a frissítéseket.
- **Publikus csoportok** tagjai közvetlenül a Kaspersky update server-től töltik le a frissítéseket.
- **Admin Kit –es Notebookok** először az Admin Kit-től próbálják letölteni a frissítéseket, amennyiben az nem elérhető (pl.: Notebook nincs az egyetemi hálózatban) akkor a Kaspersky update servertől töltik.

1.4.2. Teljes keresés:

Keddenként 12 órakor indul. Azokon a gépeken fut le, melyek elérhetők, ezután amint megjelenik egy gép, melyen nem futott le elindítja ott is a teljes keresést. Ha mind kész, legközelebb következő kedd 12 órakor indul keresés.

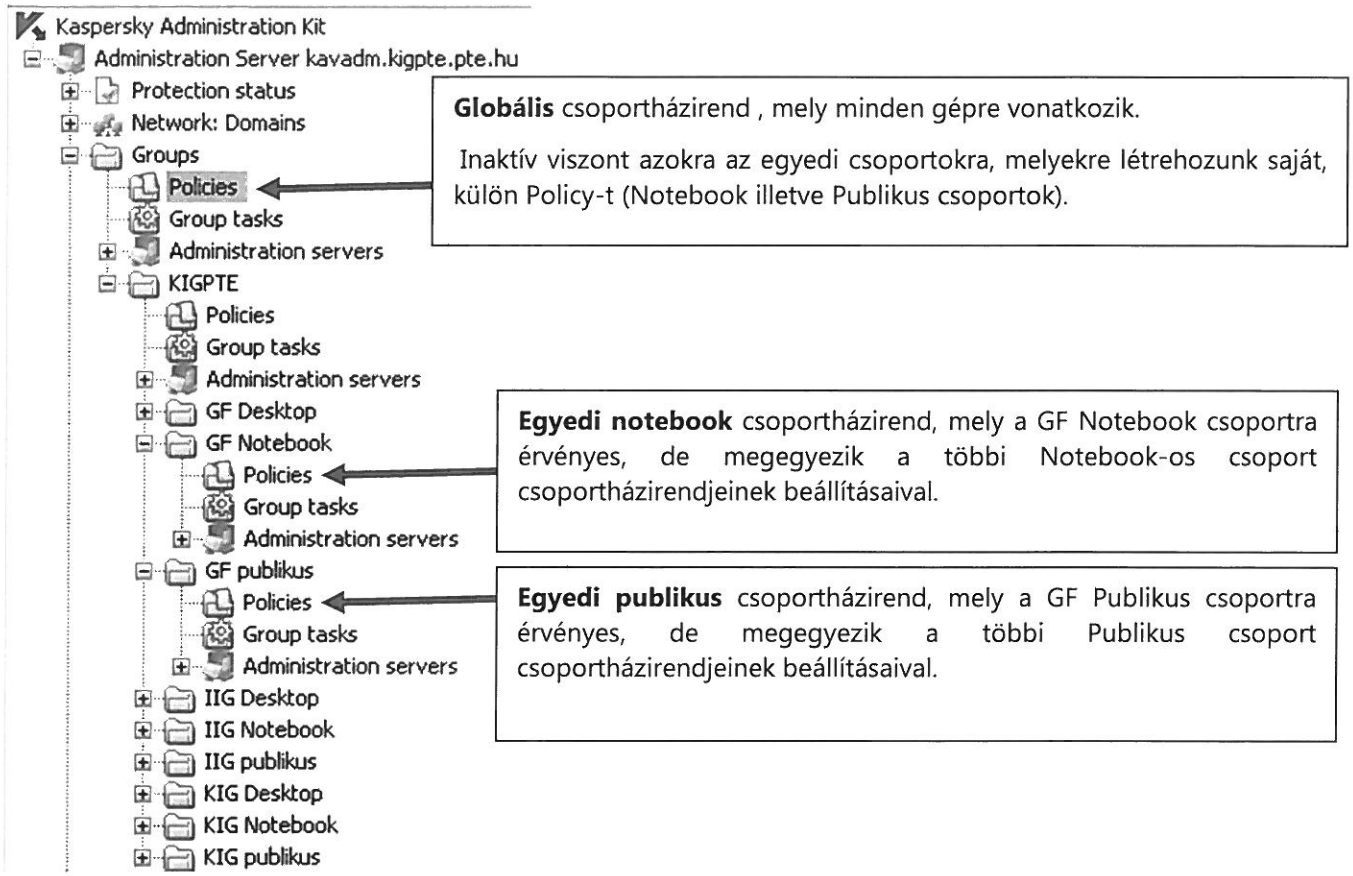
1.5. Csoportok létrehozása

Könnyebb keresés miatt csoportok lettek létrehozva az Admin Kit-ben, melyek vagy **subnetwork** szerintiek vagy **KIGPTE** tartományi gépeknél az alábbi szervezeti egységenkénti csoportok:

- IIG desktop
- IIG notebook
- IIG publikus
- KIG desktop
- KIG notebook
- KIG publikus
- GF desktop
- GF notebook
- GF publikus

1.6. Csoportházirendek (Group Policy)

A csoportházirendek a következőképpen vannak kialakítva:



1.6.1. Globális csoportházirend konfigurációja:

Groups→Policies→Kaspesrky Anti-virus for Windows Workstations Policy

Protection

- File Antivirus Optimal
- Mail Antivirus Optimal
- Web Antivirus Optimal
- Proactive Defense Optimal (Disable ott ahol ETR-ben dolgoznak)
- Anti-Spy Enable: Anti Phising , Popup Blocker, Anti-Dealer
- Anti Hacker Disable:
- Anti-Spam Disable
- Scan Optimal
- Update Source Kaspersky Admin Kit
- Network Setting Port Setting-Port 80-Disable /Kontroller2 iktató miatt/

1.6.2. Egyedi Notebook csoportházirend (Mobile user policy) konfigurációja:

- Groups→Kigpte→GF-Notebook→Policies→GF Notebook
- Groups→Kigpte→IIG-Notebook→Policies→IIG Notebook
- Groups→Kigpte→KIG-Notebook→Policies→KIG Notebook

Protection

- File Antivirus Optimal
- Mail Antivirus Optimal
- Web Antivirus Optimal
- Proactive Defense Enable: Application Activity Analizer
- Anti-Spy Optimal
- Anti Hacker Enable,Firewall:Enable-low securityAnti-Spam Disable
- Scan Optimal
- Update Source Kaspersky Admin Kit + Kaspersky Lab's update Servers

1.6.3. Egyedi Publikus csoportházirend konfigurációja:

- Groups→Kigpte→GF-Publikus→Policies→GF Publikus
- Groups→Kigpte→IIG-Publikus →Policies→IIG Publikus
- Groups→Kigpte→KIG-Publikus →Policies→KIG Publikus

Protection

- File Antivirus Custom
- Mail Antivirus Optimal
- Web Antivirus Optimal
- Proactive Defense Disable
- Anti-Spy Disable
- Anti Hacker Disable
- Anti-Spam Disable
- Scan Custom
- Update Source Kaspersky Admin Kit

1.7. Admin Kit Mentés

1.7.1. KIGPTE tartományban:

Admin Kit-be való belépés után ki kell választani a következőt: **Administration Server 193.6.50.110**

- **Main screen→Advanced→Backup Copying**
- Mentés a **E:\KAV-Backup**.Innen kerül archiválásra.

9.7.2 Klinikai Központ környezetben:

Admin Kit-be való belépés után ki kell választani a következőt: **Administration Server 10.18.3.194**

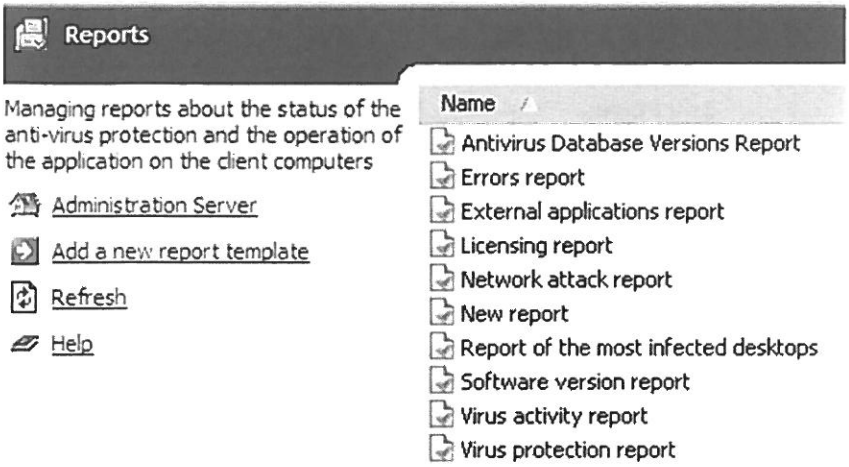
- **Main screen→Advanced→Backup Copying**
- Mentés a en **E:\Kaspersky backup mappába kerül,hétfőnként történik a szalagra írás.**

Mentést **minden hónap első munkanapján** illetve a **Kaspersky nagyobb mértékű konfigurálása esetén** ajánlott készíteni! **Utolsó 2 mentés megőrzése ajánlott!**

1.8. Automatikus értesítések

Admin Kit lehetőséget ad arra, hogy megadott e-mail címekre különböző értesítéseket küldjön.

Az alábbi értesítések definiálhatók:



Jelenleg **Network Attack report** van használatban, minden reggel 7 órakor jelenleg a kasreport@listserv.pte.hu e-mail címre küld egy összesítést az elmúlt 3 nap támadásairól, melyek forrását minden esetben lenyomozzuk, amennyiben lehetséges értesítjük , illetve kitiltjuk a felhasználót.

Küldések időpontja napi, havi,stb. módon konfigurálható és természetesen több személy e-mail címe is megadható!

1.9. Szoftverfrissítések kezelése

Ajánlott negyedévente felkeresni a http://www.kaspersky.com/productupdates - helyet, ahonnan letölthetők az aktuális szoftverfrissítések.

1.9.1. Szerver oldalon:

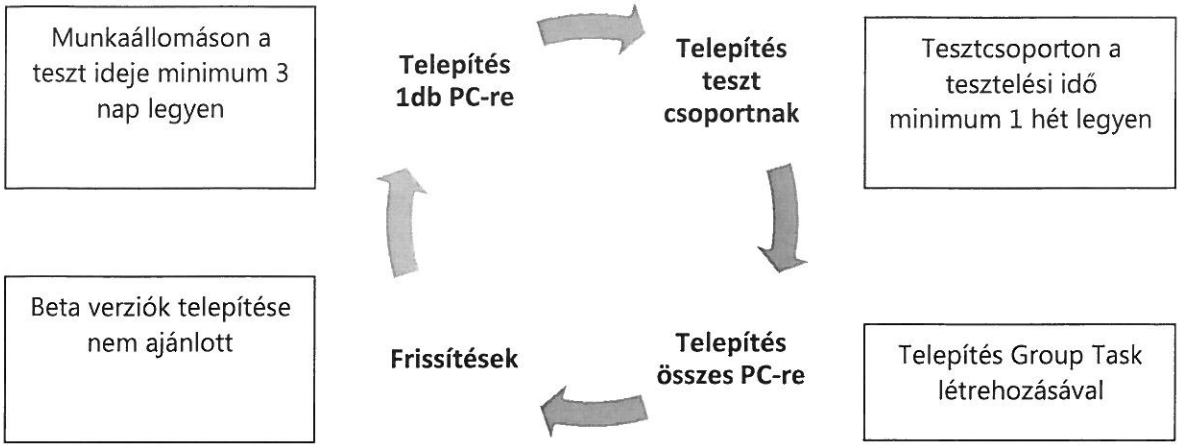
Frissítések telepítése előtt a 7-es pontban leírtak alapján készítsünk mentést, hogy esetleges probléma esetén azonnal vissza lehessen állítani a működőképes állapotot.

1.9.2. Munkaállomás oldalon:

Egy kijelölt teszt jelleggel használt munkaállomáson hajtsuk végre a szoftverfrissítést **először localhost-on történő telepítést** hajtsunk végre **majd mehet a Kaspersky Admin Kit- ben** létrehozott **telepítő csomaggal** is.

Amennyiben a frissítést követően problémamentes a működés ,egy **kijelölt teszt csoporton** (Pl.: Desktop és Periféria Üzemeltetési Csoport) is elvégezzük a szoftverfrissítést.

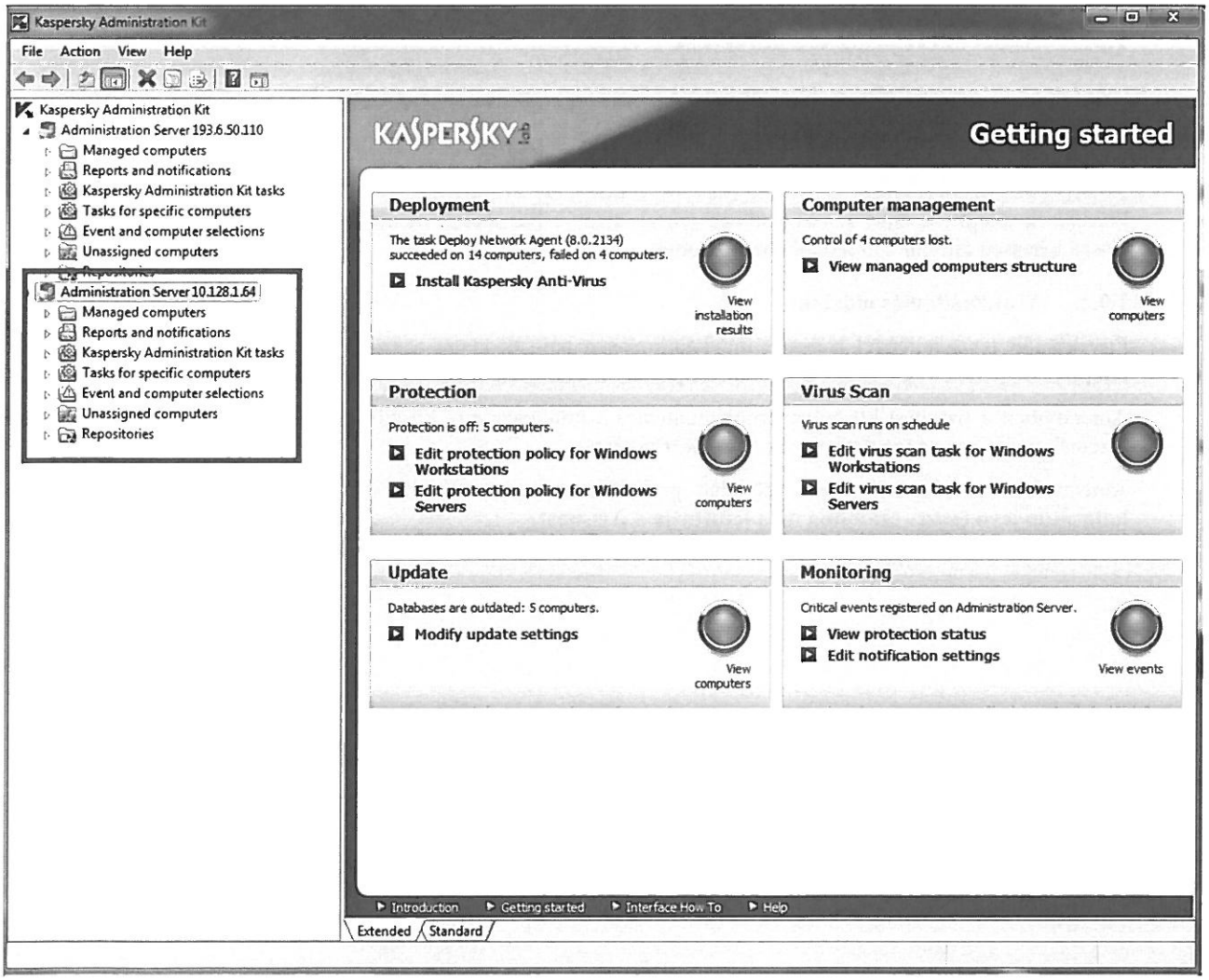
Amennyiben az előírt tesztelési idő alatt problémamentes a működés, létrehozhatunk egy **group taskot, mely a hálózaton lévő összes számítógépen lefuttatja a frissítést.**



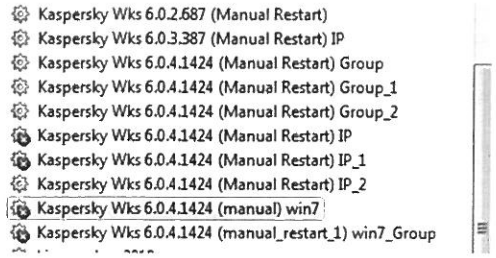
1.10. Kaspersky Admin Kit használata - Klinikai Központ

Admin Kit-ben csatlakoztatva van 10.128.1.64 (KK-SCCM) szerver és a 193.6.50.110 (KIGPTE) szerver is, így egy helyről elérhető, menedzselhető mindkettő.

Klinikai Központ menedzseléséhez válasszuk ki a következőt: **Administration Server 10.128.1.64**

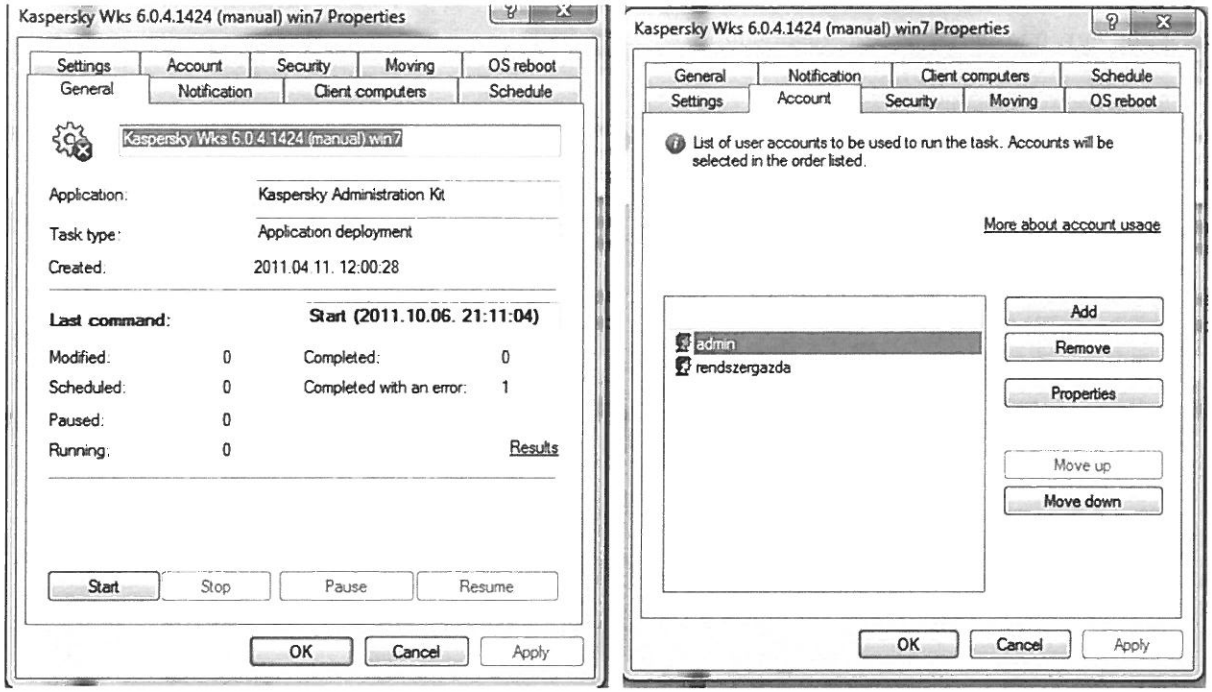


A Task for specific computers-nél a megfelelő task-ot kell kiválasztani az agent és maga a kaspersky is **együttesen fog települni úgy, mint KIGPTE tartományban.**

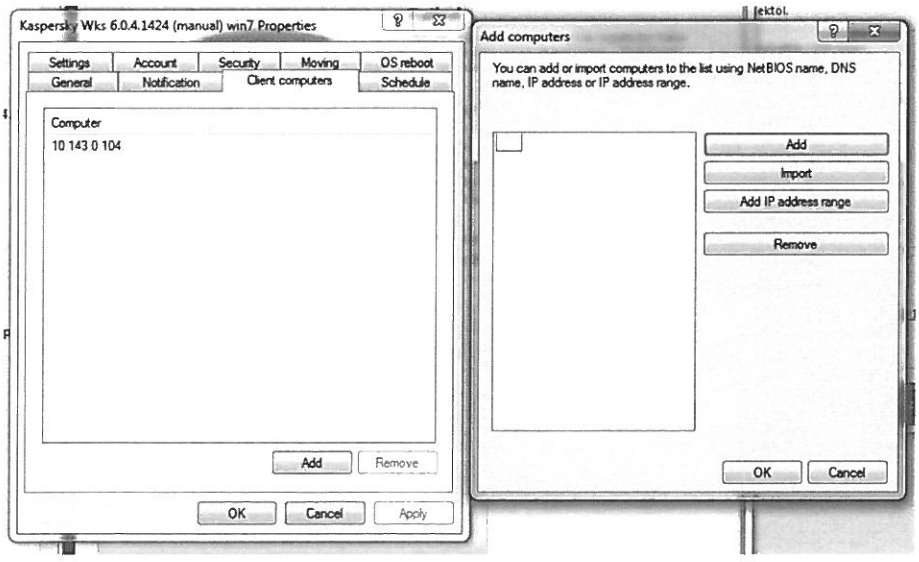


1. sz. melléklet Vírusvédelmi utasítás

A kaspersky WKS 6.0.4.1424 manual win7 task-nál az Edit settings- nél az alábbi beállításokkal települ a program



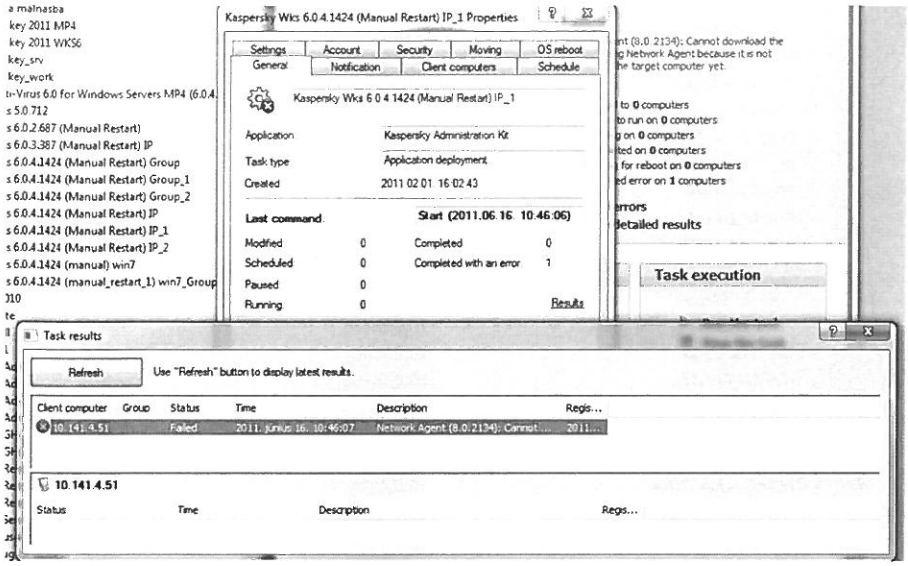
General fülnél lehet indítani, leállítani a telepítés, az Account fülnél a telepítéshez használtatos falhasználokat lehet berakni, akiknek rendszergazdai jogkörrel kell rendelkezniuk.



A Client Computers-nél lehet a telepítendő gép IP-ét megadni.

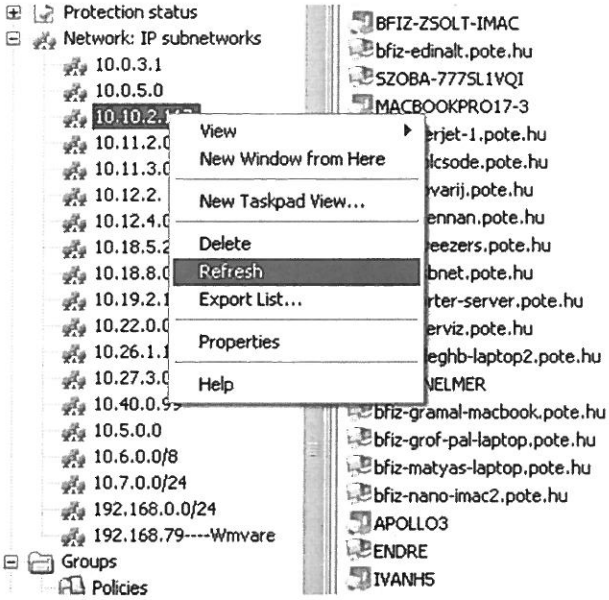
Ha valamilyen hiba történik telepítés során azt a General fül Results-t linken tudjuk megnézni.

1. sz. melléklet Vírusvédelmi utasítás



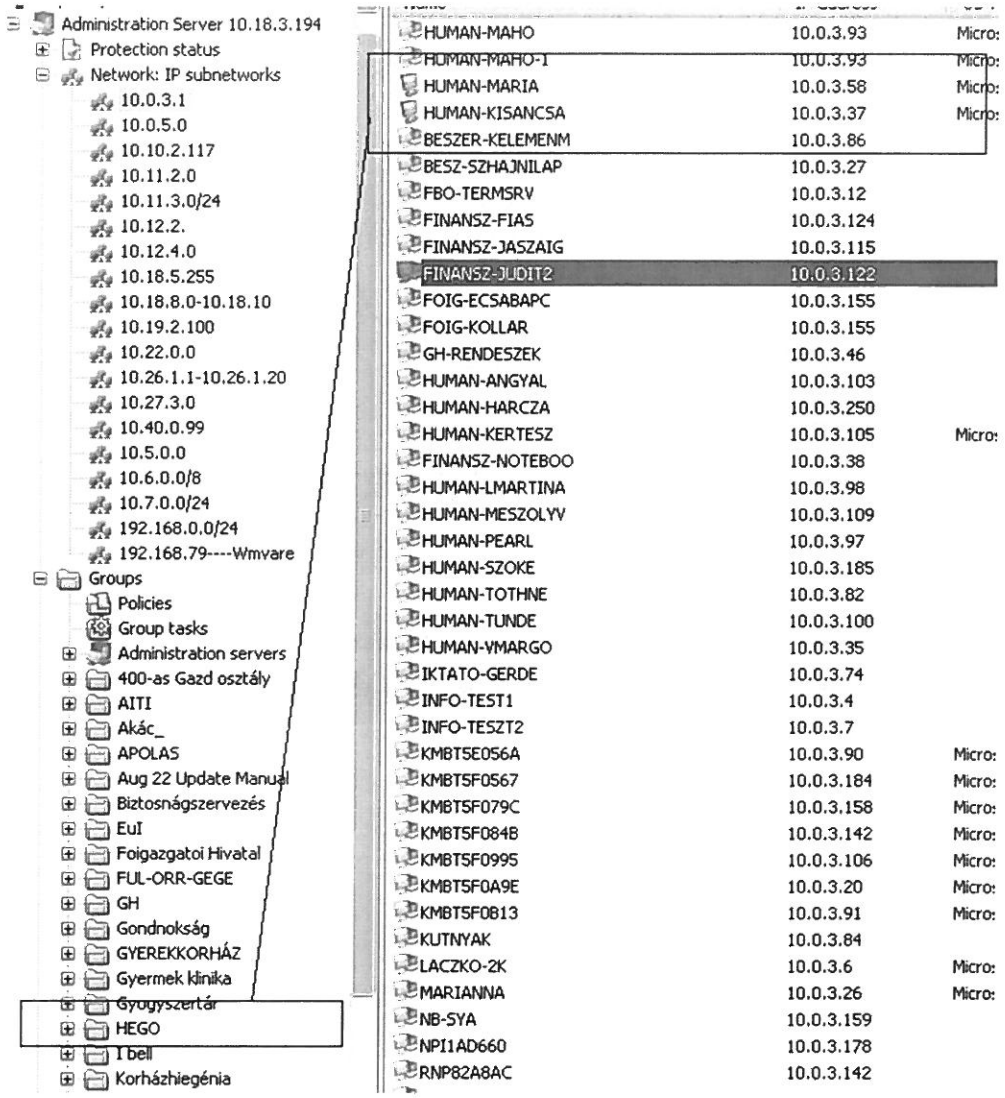
Ha semmilyen hibát nem tapasztaltunk, akkor a telepítési státusz Completed lesz.

Ezek után a gépet a megfelelő subnetworks-ben kell keresni, ha nem található, akkor frissíteni kell (Refresh).



Majd a megfelelő helyre kell húzni

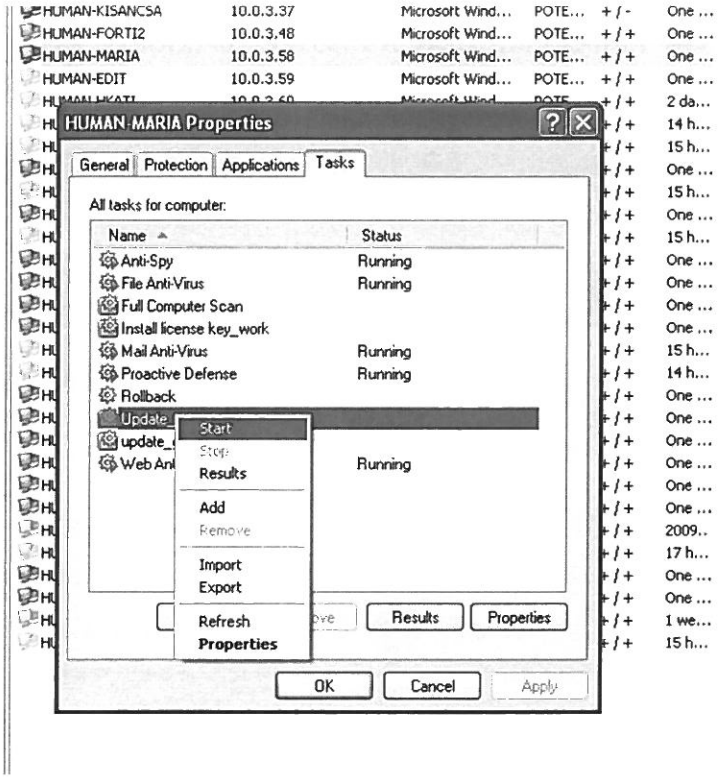
1. sz. melléklet Vírusvédelmi utasítás



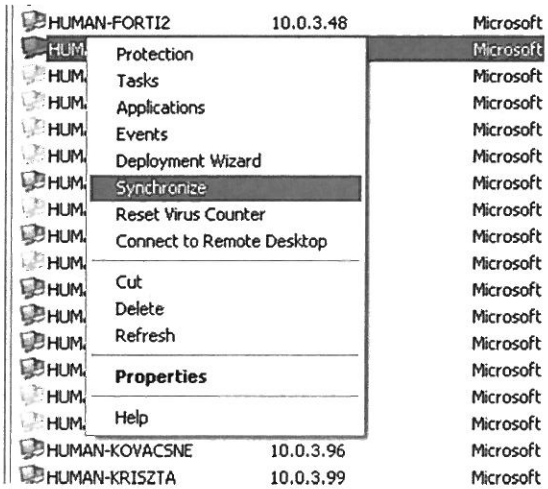
A gép piros színnel lesz jelölve mivel még nem lett update-elve.

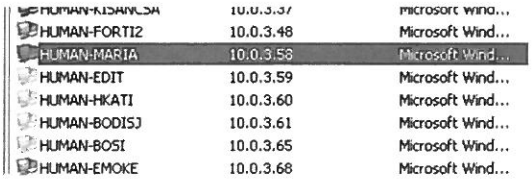
1. sz. melléklet Vírusvédelmi utasítás

Update: Jobb gomb – Properties – Tasks – Start –



Ezután szinkronizálni kell, zöld szín jelöli, hogy kész

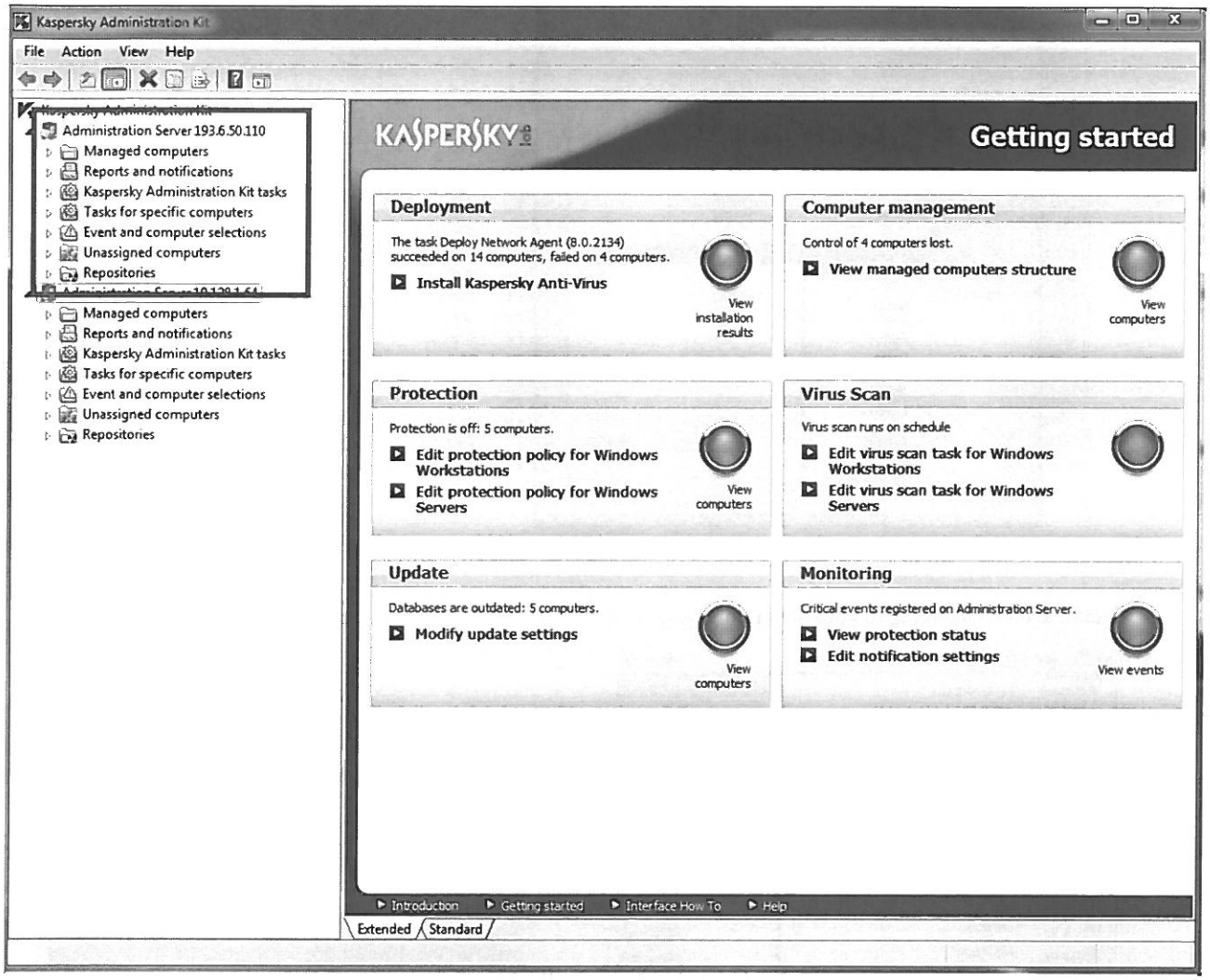




1.11. Kaspersky Admin Kit használata - KIGPTE tartományban

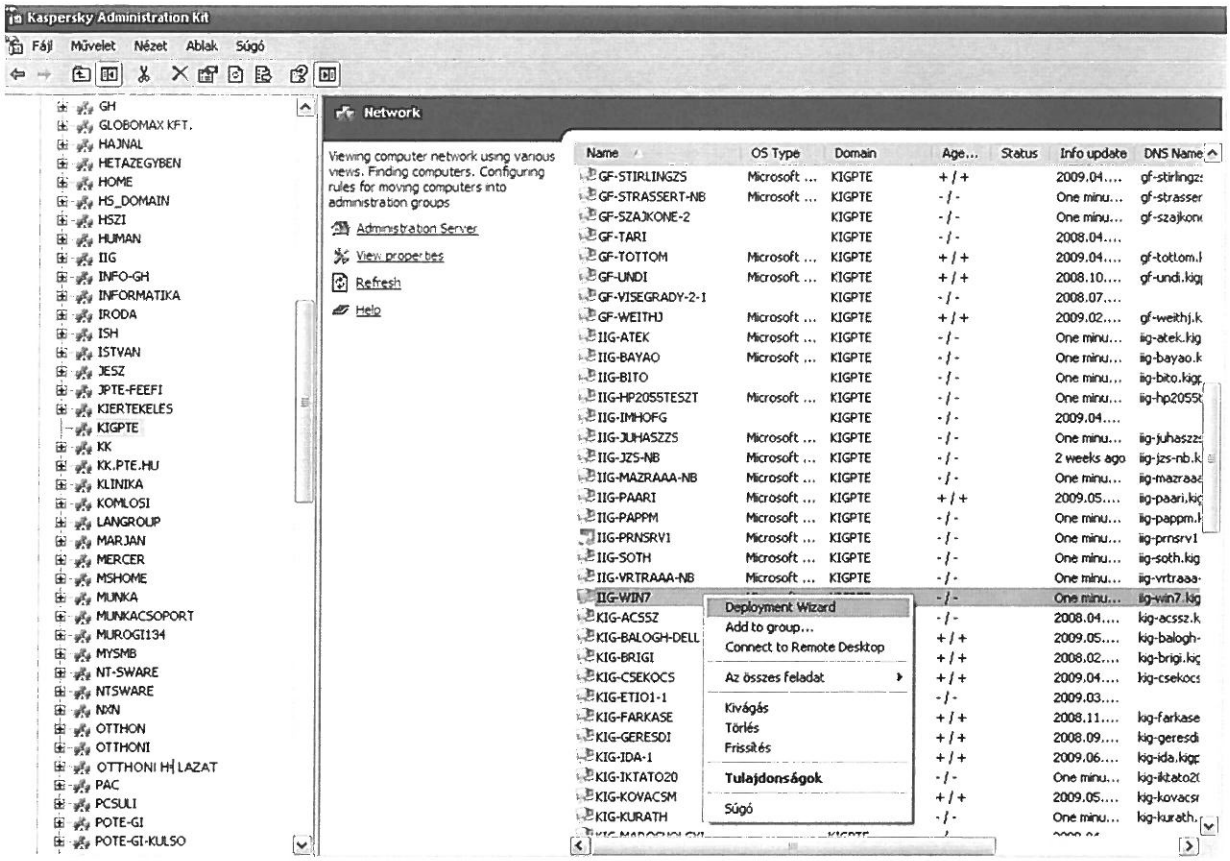
Admin Kit-ben csatlakoztatva van 10.128.1.64 (KK-SCCM) szerver és a 193.6.50.110 (KIGPTE) szerver is, így egy helyről elérhető, menedzselhető mindkettő.

KIGPTE tartomány menedzseléséhez válasszuk ki a következőt: **Administration Server 193.6.50.110**

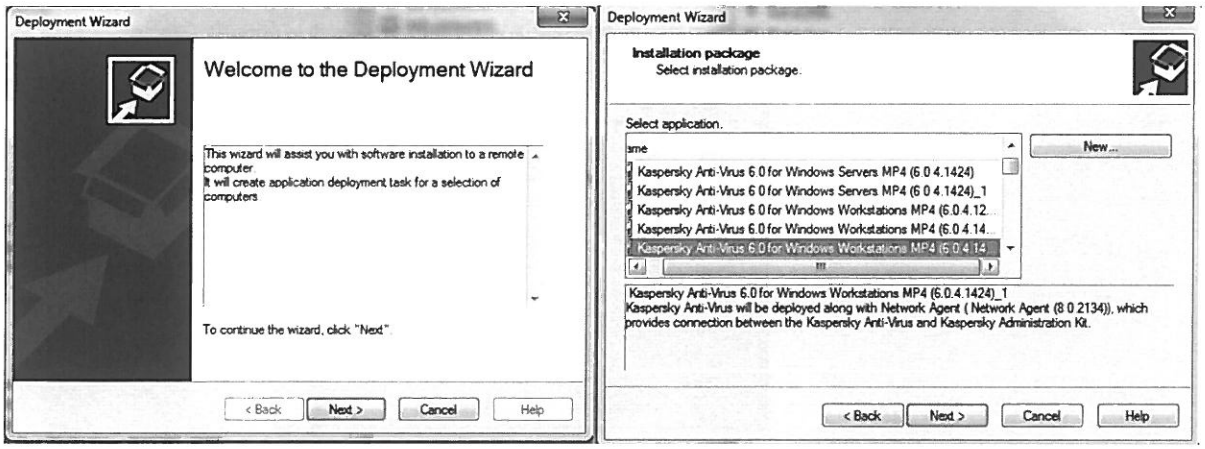


- Amint a PC-t a **kigpte.pte.hu** tartományba léptettük, megtaláljuk a **KIGPTE** csoportban
- Jobb click és Deployment Wizard, ezután indul a telepítés.

1. sz. melléklet Vírusvédelmi utasítás

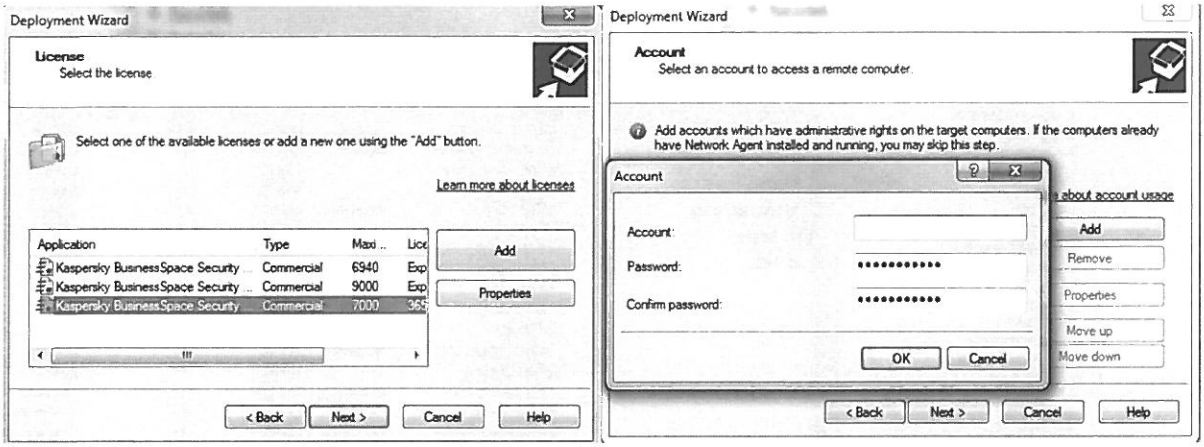


Jelenleg a 6.0.4.1424 verzió van használatban **KAV-WKS**-ből, ezért ezt jelöljük be, amennyiben a kiválasztott PC belső hálózatra csatlakozik, válasszuk a „**Belülről**”, ha külső IP címmel rendelkezik a „**Kívülről**” csomagot.

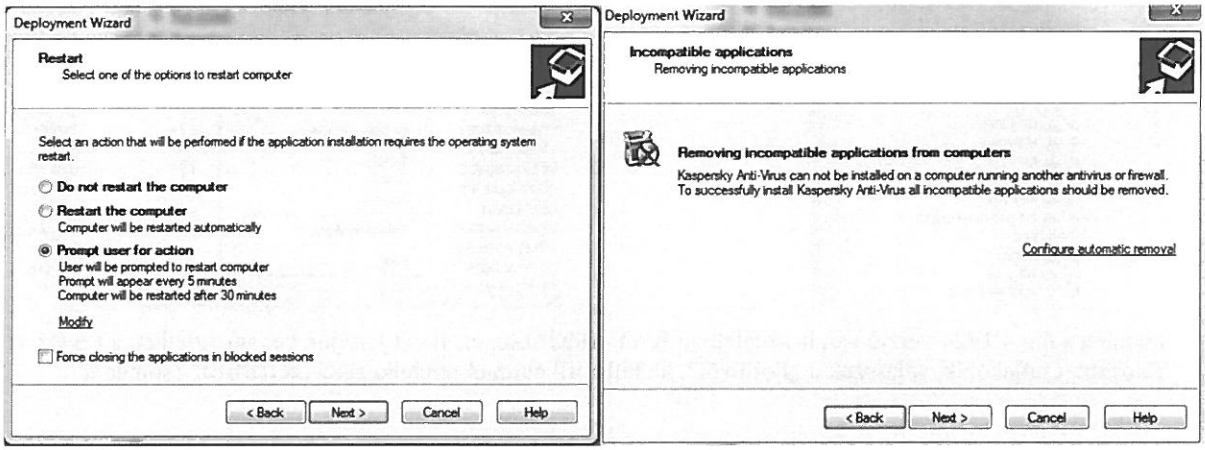


1. sz. melléklet Vírusvédelmi utasítás

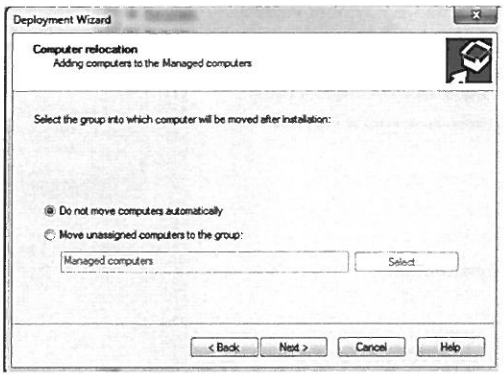
A megfelelő beállításokat az alábbi ablakokba meg tudjuk tenni. (melyik licenccel legyen telepítve, milyen user-el)



Legyen-e újraindítás a telepítés végén, ill. az inkompatibilis programokkal mit csináljon.



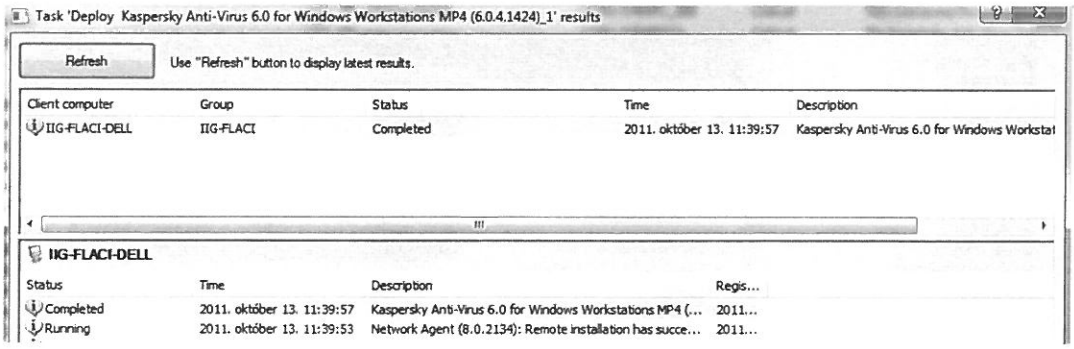
A feltelepített gépek elhelyezését lehet itt módosítani.



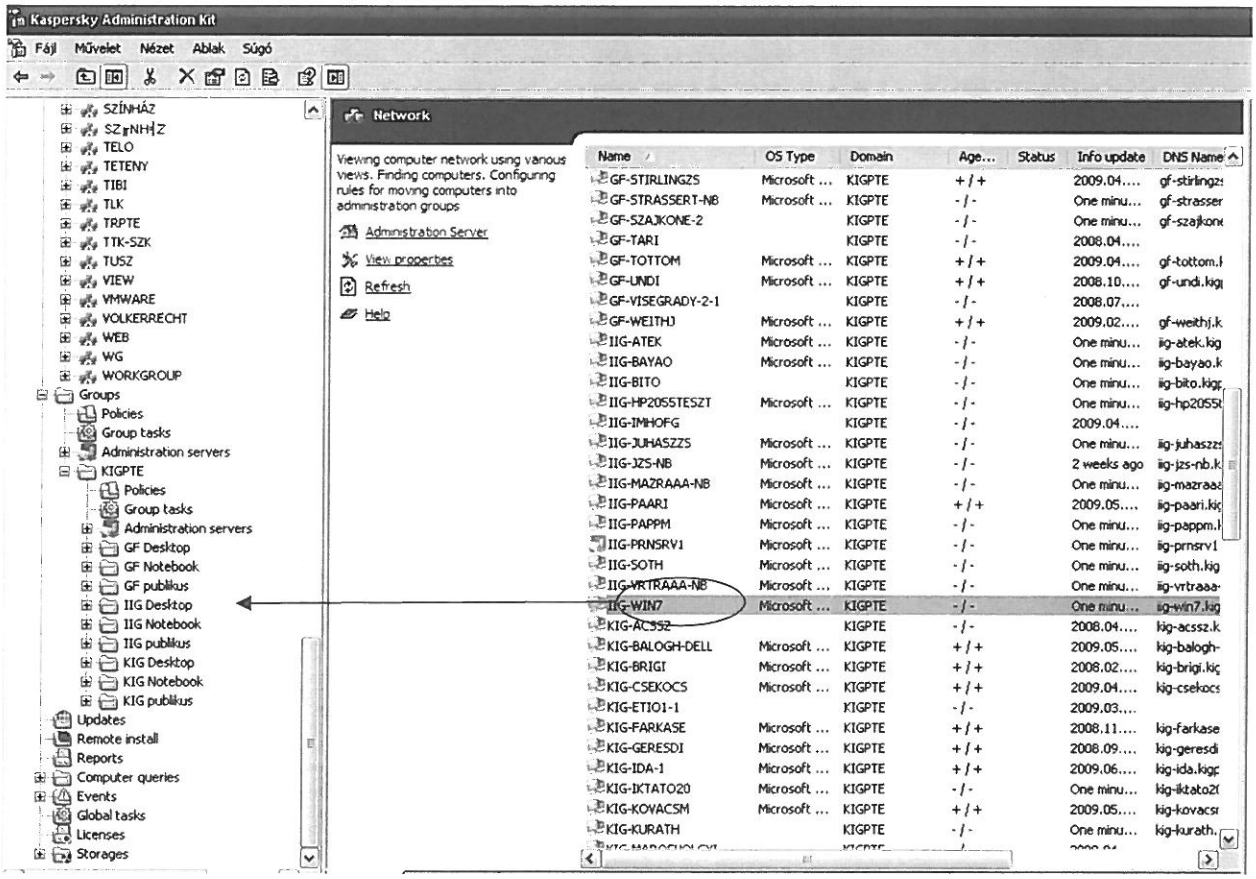
1. sz. melléklet Vírusvédelmi utasítás

A Telepítés akkor lesz 100%, ha újraindítjuk a PC-t.

Újraindítás után lesz a Status „ **Completed**”

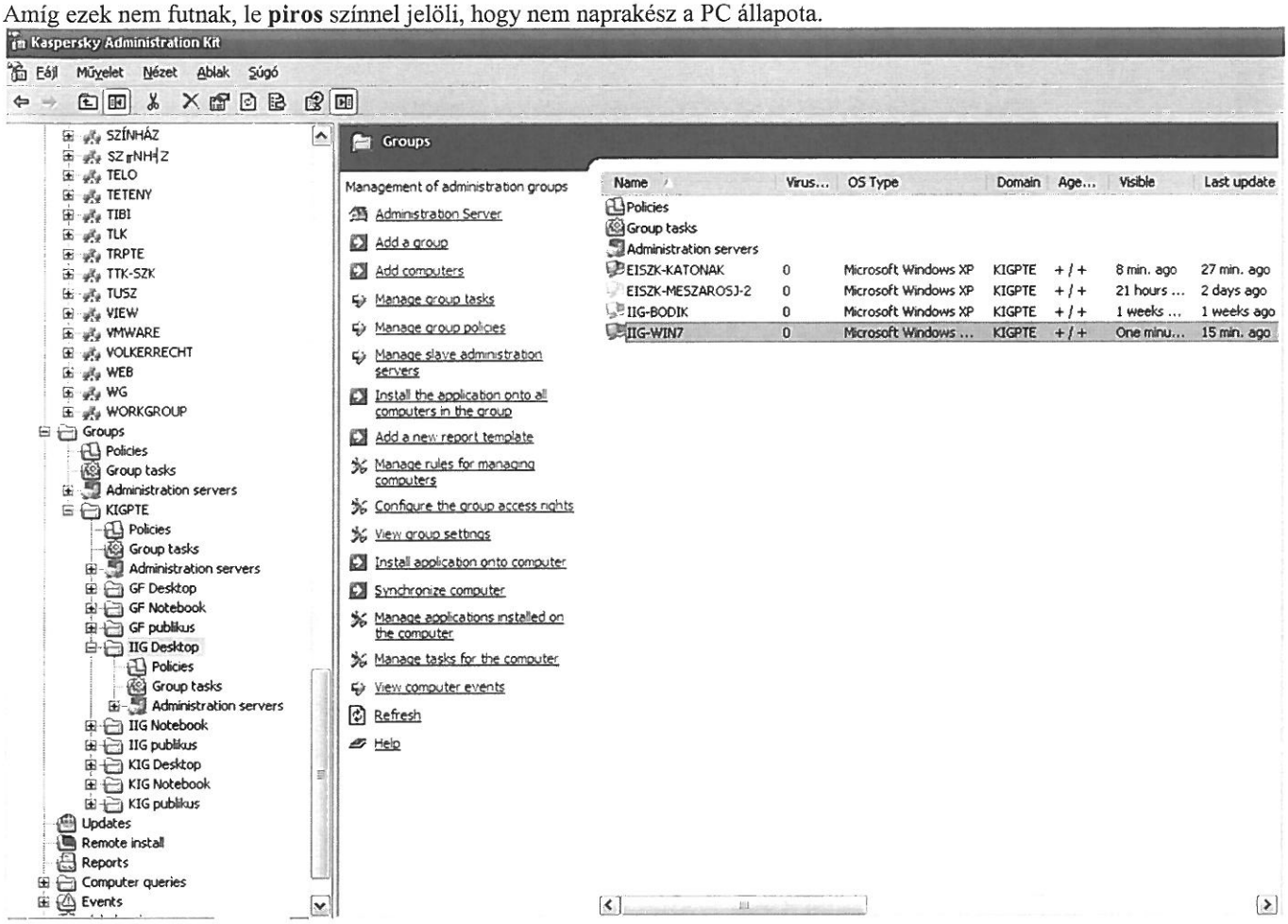


Majd a megfelelő csoportba húzzuk, ezután már az aktuális **Group Policy** érvényes a gépre.



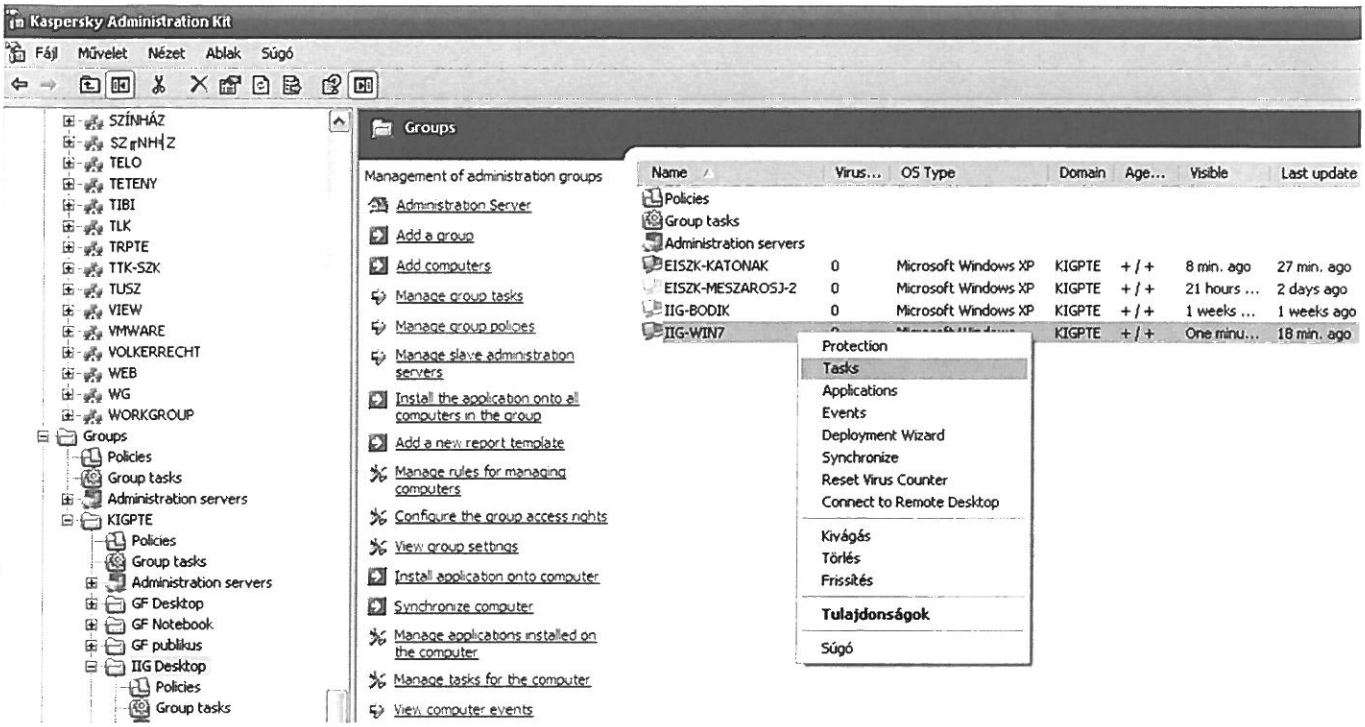
1. sz. melléklet Vírusvédelmi utasítás

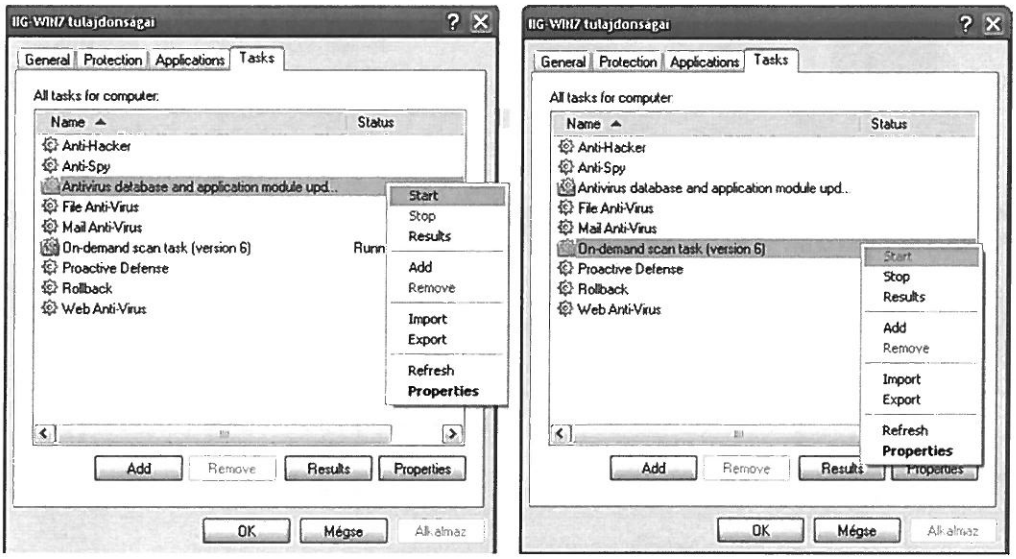
Frissítés és **full scan** az Admin Kit felületről indítható el.
Amíg ezek nem futnak, le **piros** színnel jelöli, hogy nem naprakész a PC állapota.



1. sz. melléklet Vírusvédelmi utasítás

Frissítés és **full scan** elindítása manuálisan:





Amint ezek lefutnak a PC állapota **zöld**-re vált, mely azt jeleni, hogy a PC állapota naprakész.

1.12. Kaspersky Admin Guide – English - (hivatkozás)

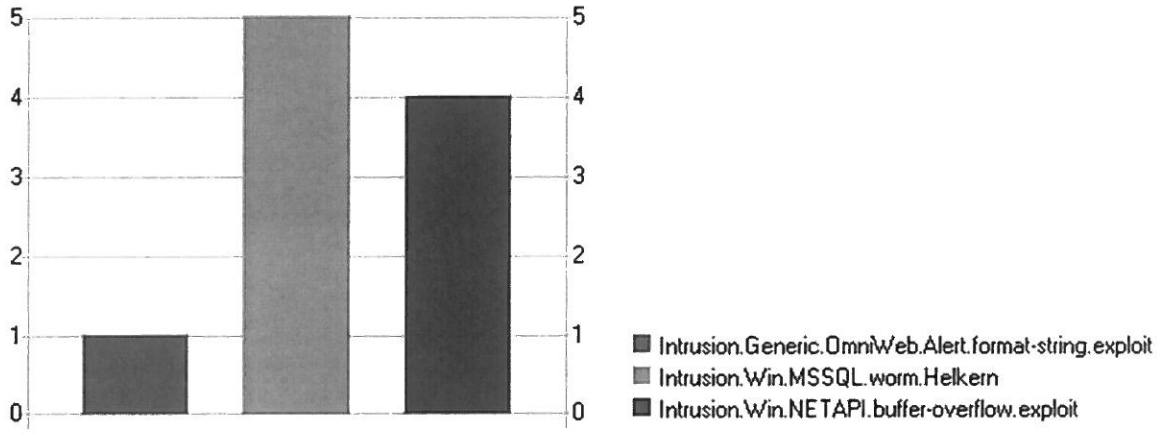
2. Network Attack Report

Kaspersky Administration Kit

Network attack report **2009. augusztus 19. 7:00:01**

Report contains information on network attacks recorded on logical network hosts for the entire system

Period: from 2009. augusztus 17. to 2009. augusztus 19.



Summary:

Attack occurrences:	**10**	**Various attacks:**	**3**	**Attackers' IPs:**	**5**	**Hosts attacked:**	**6**	**Groups attacked:**	**3**	**First detection time:**	**2009. augusztus 17. 12:55:47**	**Last detection time:**	**2009. augusztus 18. 13:43:20**

Attackers' IPs	Hosts attacked	Attack	Attack occurrences	Groups attacked	First detection time	Last detection time
1	1	Intrusion.Generic.OmniWeb.Alert.format-string.exploit	1	1	2009. augusztus 17. 14:56:53	2009. augusztus 17. 14:56:53
3	1	Intrusion.Win.MSSQL.worm.Helkern	5	1	2009. augusztus 17. 12:55:47	2009. augusztus 18. 13:43:20
1	4	Intrusion.Win.NETAPI.buffer-overflow.exploit	4	2	2009. augusztus 17. 18:29:02	2009. augusztus 17. 18:43:23

1. sz. melléklet Vírusvédelmi utasítás

Details 10 of 10

Attacker's IP	Attack time	Group	Client computer	Attack	Protocol	Port	Visible	Last connection date	IP-address	NetBIOS name	Domain	DNS Name	DNS domain
61.145.123.141	2009. augusztus 17. 12:55:47	IIG publikus	EISZK-GABE	Intrusion.Win.MSSQL.worm.Helkern	17	1434	2009. augusztus 18. 16:06:43	2009. augusztus 18. 16:06:43	193.6.50.86	EISZK-GABE	KIGPTE	eiszk-gabe	kigpte.pte.hu
218.16.82.18	2009. augusztus 17. 14:56:53	GF Desktop	GF-ARONFFY	Intrusion.Generic.OmniWeb.Alert.format-string.exploit	6	1892	2009. augusztus 18. 14:59:13	2009. augusztus 18. 14:59:13	10.0.5.42	GF-ARONFFY	KIGPTE	gf-aronffy	kigpte.pte.hu
219.76.200.50	2009. augusztus 17. 15:01:57	IIG publikus	EISZK-GABE	Intrusion.Win.MSSQL.worm.Helkern	17	1434	2009. augusztus 18. 16:06:43	2009. augusztus 18. 16:06:43	193.6.50.86	EISZK-GABE	KIGPTE	eiszk-gabe	kigpte.pte.hu
203.102.181.165	2009. augusztus 17. 15:54:12	IIG publikus	EISZK-GABE	Intrusion.Win.MSSQL.worm.Helkern	17	1434	2009. augusztus 18. 16:06:43	2009. augusztus 18. 16:06:43	193.6.50.86	EISZK-GABE	KIGPTE	eiszk-gabe	kigpte.pte.hu
10.0.2.176	2009. augusztus 17. 18:29:02	GF Desktop	GF-FROMVALD	Intrusion.Win.NETAPI.buffer-overflow.exploit	6	445	2009. augusztus 19. 6:47:52	2009. augusztus 19. 6:47:52	10.0.5.99	GF-FROMVALD	KIGPTE	gf-fromvald	kigpte.pte.hu
10.0.2.176	2009. augusztus 17. 18:31:09	KIG Desktop	KIG-DERIJ-1	Intrusion.Win.NETAPI.buffer-overflow.exploit	6	445	2009. augusztus 18. 14:05:15	2009. augusztus 18. 14:05:15	10.0.5.129	KIG-DERIJ	KIGPTE	kig-derij	kigpte.pte.hu
10.0.2.176	2009. augusztus 17. 18:33:06	KIG Desktop	KIG-RADICS	Intrusion.Win.NETAPI.buffer-overflow.exploit	6	445	2009. augusztus 18. 17:26:47	2009. augusztus 18. 17:26:47	10.0.5.157	KIG-RADICS	KIGPTE	kig-radics	kigpte.pte.hu
10.0.2.176	2009. augusztus 17. 18:43:23	KIG Desktop	KIG-CSONDORA	Intrusion.Win.NETAPI.buffer-overflow.exploit	6	445	2009. augusztus 19. 6:46:53	2009. augusztus 19. 6:46:53	10.0.6.48	KIG-CSONDORA	KIGPTE	kig-csondora	kigpte.pte.hu
61.145.123.141	2009. augusztus 18. 8:45:50	IIG publikus	EISZK-GABE	Intrusion.Win.MSSQL.worm.Helkern	17	1434	2009. augusztus 18. 16:06:43	2009. augusztus 18. 16:06:43	193.6.50.86	EISZK-GABE	KIGPTE	eiszk-gabe	kigpte.pte.hu
61.145.123.141	2009. augusztus 18. 13:43:20	IIG publikus	EISZK-GABE	Intrusion.Win.MSSQL.worm.Helkern	17	1434	2009. augusztus 18. 16:06:43	2009. augusztus 18. 16:06:43	193.6.50.86	EISZK-GABE	KIGPTE	eiszk-gabe	kigpte.pte.hu

3. Vírusvédelemért felelős személy – szervezeti egységenként

A vírusvédelemért felelős személy a szervezeti egység vezetője vagy a szervezeti egység vezető által kijelölt, a feladat elvégzésével megbízott személy.

A vírusvédelemért felelős személyek névsora az Informatikai Igazgatóságon lévő negyedévente frissített listán vagy adatbázisban található meg.