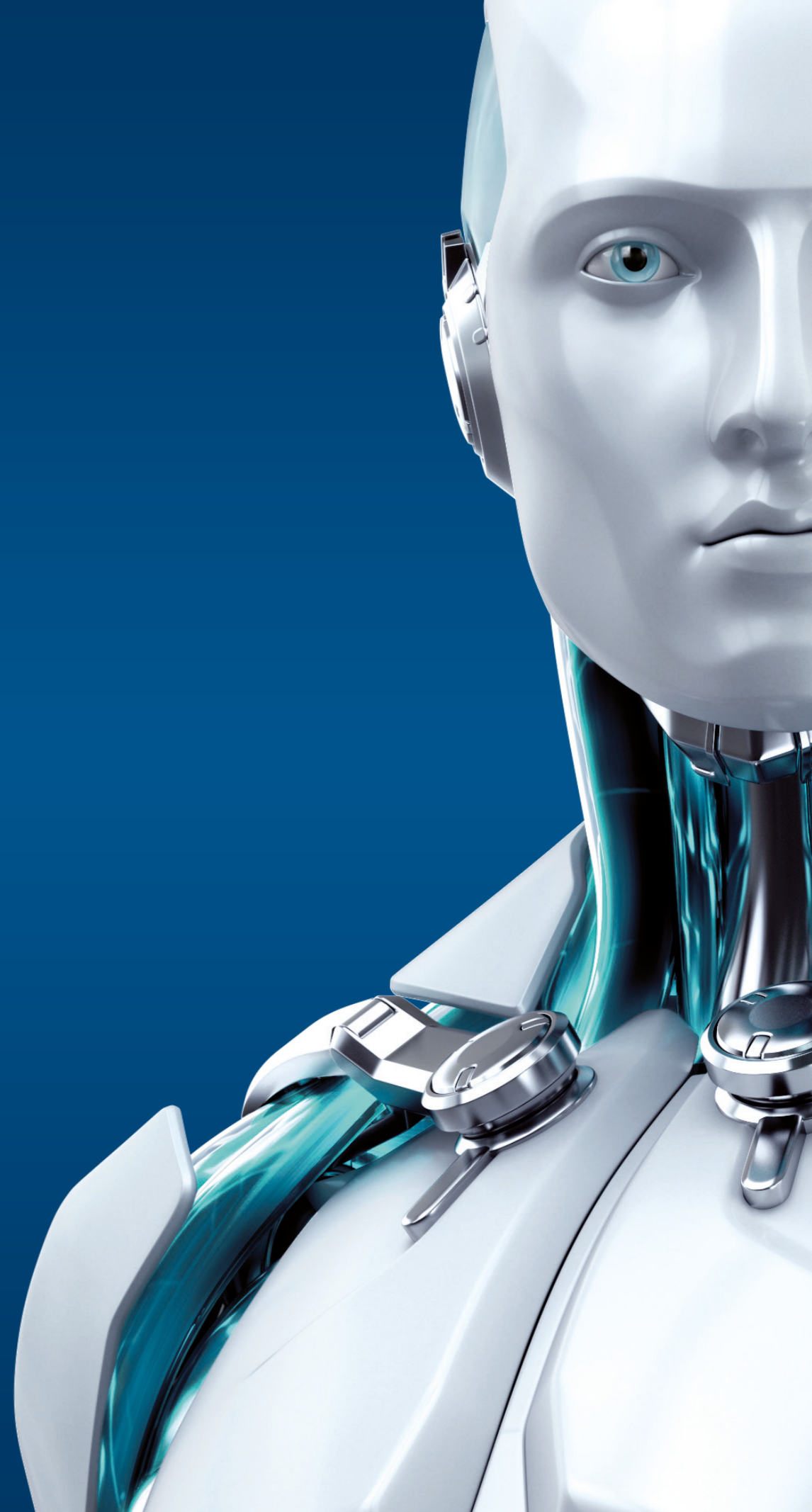


# ESET Remote Administrator kézikönyv

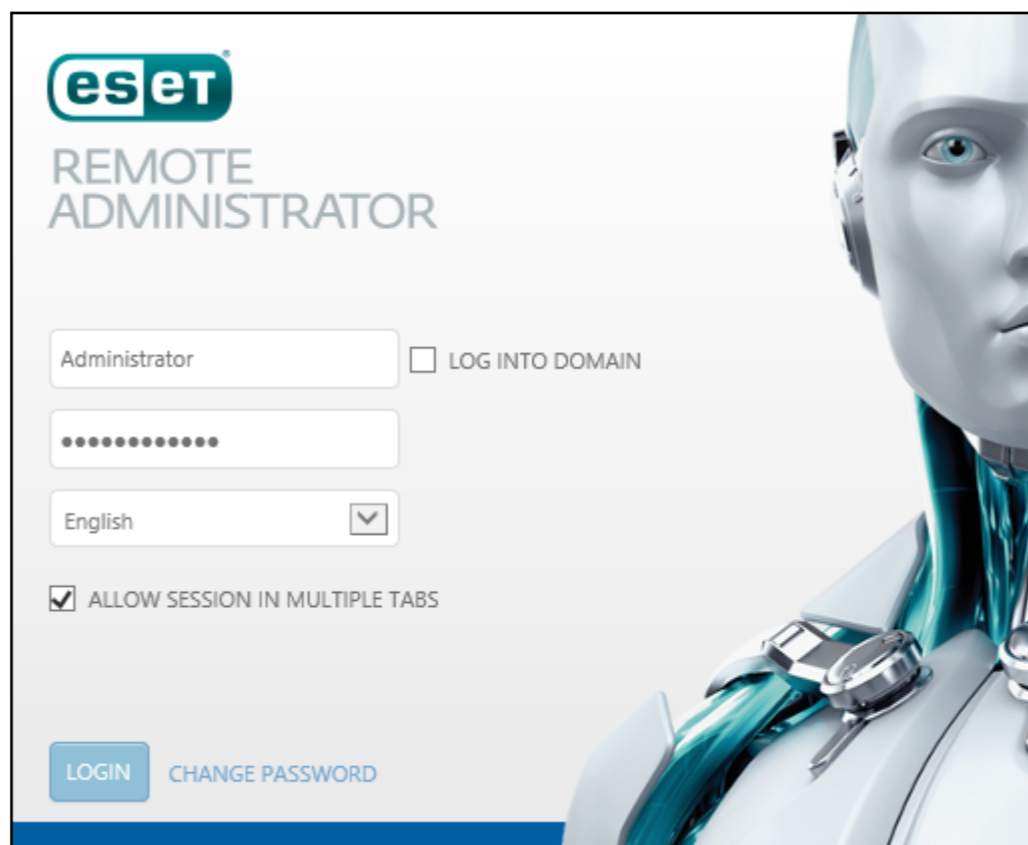


## Tartalomjegyzék

A távadminisztrációs rendszer.....	2
A távadminisztrációs rendszer részei.....	2
Elektronikus licenc .....	4
A távadminisztrációs rendszer telepítése, előkövetelményei.....	4
Licencek kezelése .....	6
Számítógépek felderítése .....	7
Remote Administrator Agent telepítése.....	9
Agent policy módosítása .....	10
Agent telepítése távtelepítéssel.....	11
Agent telepítése Live Installer segítségével .....	12
Távtelepítés kliensre.....	13
Csoportkezelés.....	17
Statikus csoportok .....	18
Dinamikus csoportok .....	19
Policy-k kezelése .....	21
Tükrözés beállítása.....	24
Események, feladatok, automatizálás.....	26
Feladatok.....	26
Triggerek.....	27
Automatizálás.....	29
Értesítések.....	30
Riportok.....	31
További információk.....	33

## A távadminisztrációs rendszer

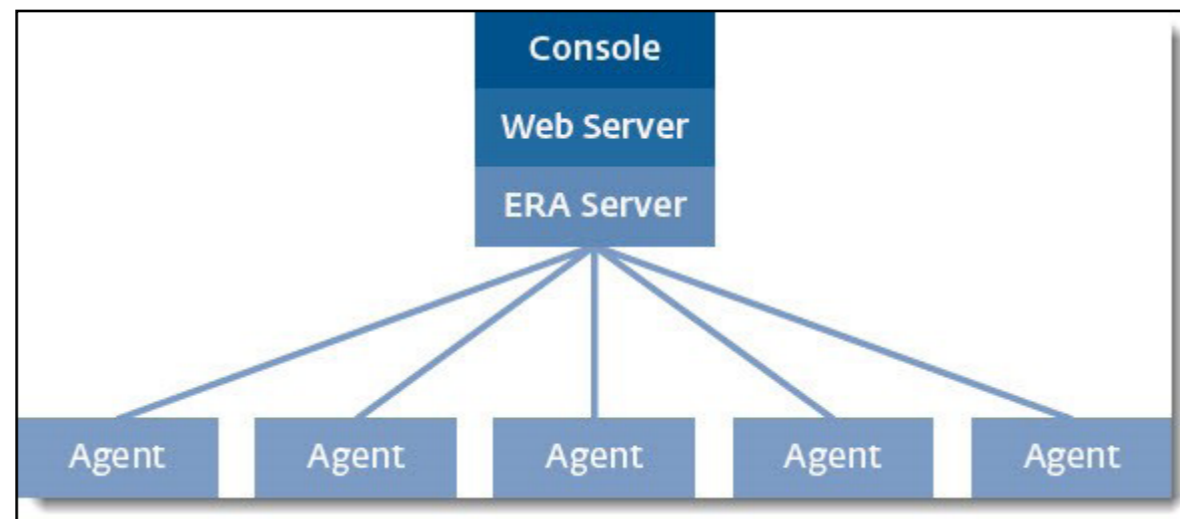
Az ESET Remote Administrator program az ESET vállalati végpontvédelmek és szervervédelmek központi menedzsment programja. Segítségével egyetlen webes felületen áttekinthető a teljes hálózatának biztonsága, telepíthetők, eltávolíthatók és konfigurálhatók a végpontok biztonsági szoftverei, és részletesen automatizálható módon kezelhetők az esetlegesen felmerülő problémák.



## A távadminisztrációs rendszer részei

A távadminisztrációs program struktúrájának központi része az **ESET Remote Administrator Server** (röviden ERAS), amely egy szolgáltatásként fut a szerveren. Ezzel áll összeköttetésben az **ESET Remote Administrator Web Console**, amely egy bárhonnán indítható webes konzol, ezen a felületen végezhető el a védelemmel kapcsolatos bármely feladat. Minden olyan számítógépre, amelyet központilag szeretnénk kezelni, szükséges feltelepíteni az **ESET Remote Administrator Agent** programot.

Ez a szolgáltatás végzi a kommunikációt az adott kliensen telepített végpontvédelemmel, ez továbbítja a klienssel kapcsolatos információkat és eseményeket a távadminisztrációs szerver felé és ez hajtja végre a szerveren létrehozott feladatokat és módosításokat a klienseken. Tulajdonképpen tekinthető egyfajta lokálisan telepített, leegyszerűsített távadminisztrációs szervernek. Azáltal, hogy lokálisan tárolja a kliensekre vonatkozó policy-ket (házi rendeket), csoportbeállításokat és az adott eseményekre beállított automatikusan futtatandó feladatokat, a kliens gépek távadminisztrációja offline állapotban is aktív marad.



A távadminisztrációs struktúra további komponensei a webes konzol felületét biztosító **Apache Tomcat Server**, a kliensek adatbázisát kezelő **Microsoft SQL Server Express**, a hálózaton található védelem nélküli kliensek felderítését végző **Rogue Detection Sensor** és az opcionálisan telepíthető, a távadminisztrációs szerver felé irányuló kommunikációt összefogó és ezáltal minimalizáló **Remote Administrator Proxy**. Ez a proxy nem összekeverendő az **Apache HTTP Proxy-val**, amely a vírusdefiníció adatbázis tükrözését valósítja meg http protokollon keresztül. A **Mobil Device Connector** szintén opcionálisan telepíthető, az Android-os okoseszközök védelmét ellátó ESET Endpoint Security for Android programok központi kezeléséhez szükséges.

## Elektronikus licenc

A vásárlás vagy a próbalicenc igénylése után kapott elektronikus licenclevél tartalmazza a távadminisztrációs rendszer használatához szükséges **licenckulcsát**. Ez a kulcs hordozza magában a központilag menedzselhető kliensek maximális számát és típusát, illetve a licenc érvényességi idejét. A licenc kezelése és az azzal kapcsolatos teendők (vagy akár a kezelésének delegálása) az ESET új webes felületén, az **ESET Licence Administrator** oldalon tehetők meg.

### 3 Aktiválás licenckulccsal

A vállalati megoldások 6-os verziójától kezdődően a termékek aktiválásához az alábbi licencadatok szükségesek:

<b>Licenckulcs:</b>	CE8E-X3PU-56V2-G8FR-CE8E
<b>Licenc adminisztrátori jelszó:</b>	abcdefghijkl123
<b>Nyilvános licencazonosító:</b>	33B-RW6-XT8

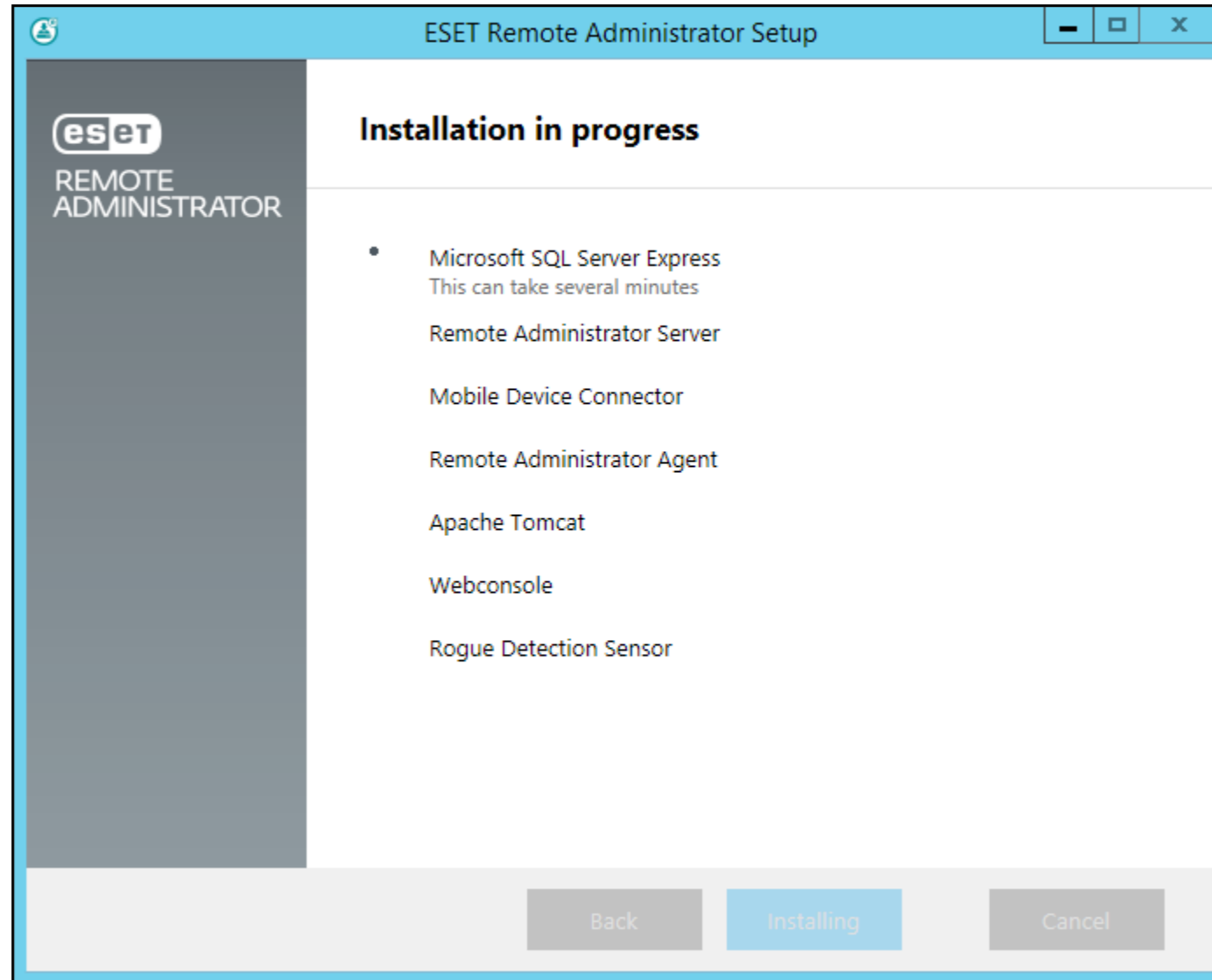
Lehetősége van az [ESET License Administrator portál](#) használatára a **Licenckulcs** és a **Licenc adminisztrátori jelszó** segítségével. Amennyiben licencének kezelését harmadik félre bízna, a **Nyilvános licencazonosító** megosztásával ezt is megteheti a weboldalon. A portál használatáról bővebben [itt olvashat](#).

## A távadminisztrációs rendszer telepítése, előkövetelményei

A központi menedzsment rendszer az összes komponensével telepíthető egyszerre, egyetlen telepítő futtatásával, vagy telepíthető akár komponensenként is, amennyiben a rendszer bizonyos részeit már korábban telepítette, vagy rendelkezik saját MySQL vagy MS SQL adatbázis szerverrel és azt kívánja használni az automatikusan települő helyett.

A sikeres telepítéshez szükséges három további program megléte a szerveren, a **.Net 3.5**-ös keretrendszer, a **Java Runtime Environment** legfrissebb verziója a webes felület működéséhez, illetve a **WinPcap** program a hálózaton található védtelen eszközök felderítéséhez. Utóbbi kettőt a gyártó honlapjáról töltheti le (a telepítőből néhány kattintással elérhető), míg a .Net

keretrendszert a Szerepkörök és szolgáltatások hozzáadása varázsló segítségével telepítheti a serveren.



A Mobile Device Connector-t abban az esetben szükséges telepítenie, ha az ESET Endpoint Security programokat Android rendszeren működő eszközök esetén is szeretné központilag kezelni.

A legelső lépésben kiválasztható Remote Administrator Proxy-t csak nagy hálózatok vagy több telephely esetén érdemes telepíteni a távadminisztrációs program hálózati forgalmának csökkentéséhez.

A telepítés során megadható a licenclévélben megkapott Licenckulcs, de azt később is hozzá lehet adni a távadminisztrációs programhoz.

## Licencek kezelése

A telepítés befejeztével már csatlakozhatunk is a távadminisztrációs szerverhez a webes felületen. Amennyiben nem adott meg licenckulcsot a telepítés során, ezt megteheti az **Admin** (szerszámoszláda ikon) → **License Management** részen az **ADD LICENSES** gombra kattintva. Ezt követően ugyanitt követhető nyomon, hogy hány licenc került felhasználásra a hálózaton.

The screenshot displays the ESET Remote Administrator web interface. The top navigation bar includes the ESET logo, the text 'REMOTE ADMINISTRATOR', a search bar, a help icon, the user name 'ADMINISTRATOR', and a session duration indicator '>9 MIN'. The left sidebar contains a navigation menu with the following items: Admin, Dynamic Group Templates, Groups, Policies, Client Tasks, Server Tasks, Notifications, Certificates, Access Rights, Server Settings, and License Management. The main content area is titled 'License Management' and contains a table with the following columns: PUBLIC ID, PRODUCT NAME, STATUS, ONLINE ACTIVATED SEATS, OFFLINE SEATS, TOTAL SEATS, EXPIRES, and OWNER NAME. A single license entry is visible in the table:

PUBLIC ID	PRODUCT NAME	STATUS	ONLINE ACTIVATED SEATS	OFFLINE SEATS	TOTAL SEATS	EXPIRES	OWNER NAME
<input type="checkbox"/> 33B-MHW-H97	ESET Endpoint Security for Windows	✓	6	0	100	2015 May 16 14:00:00	Sicontact Kft. nu

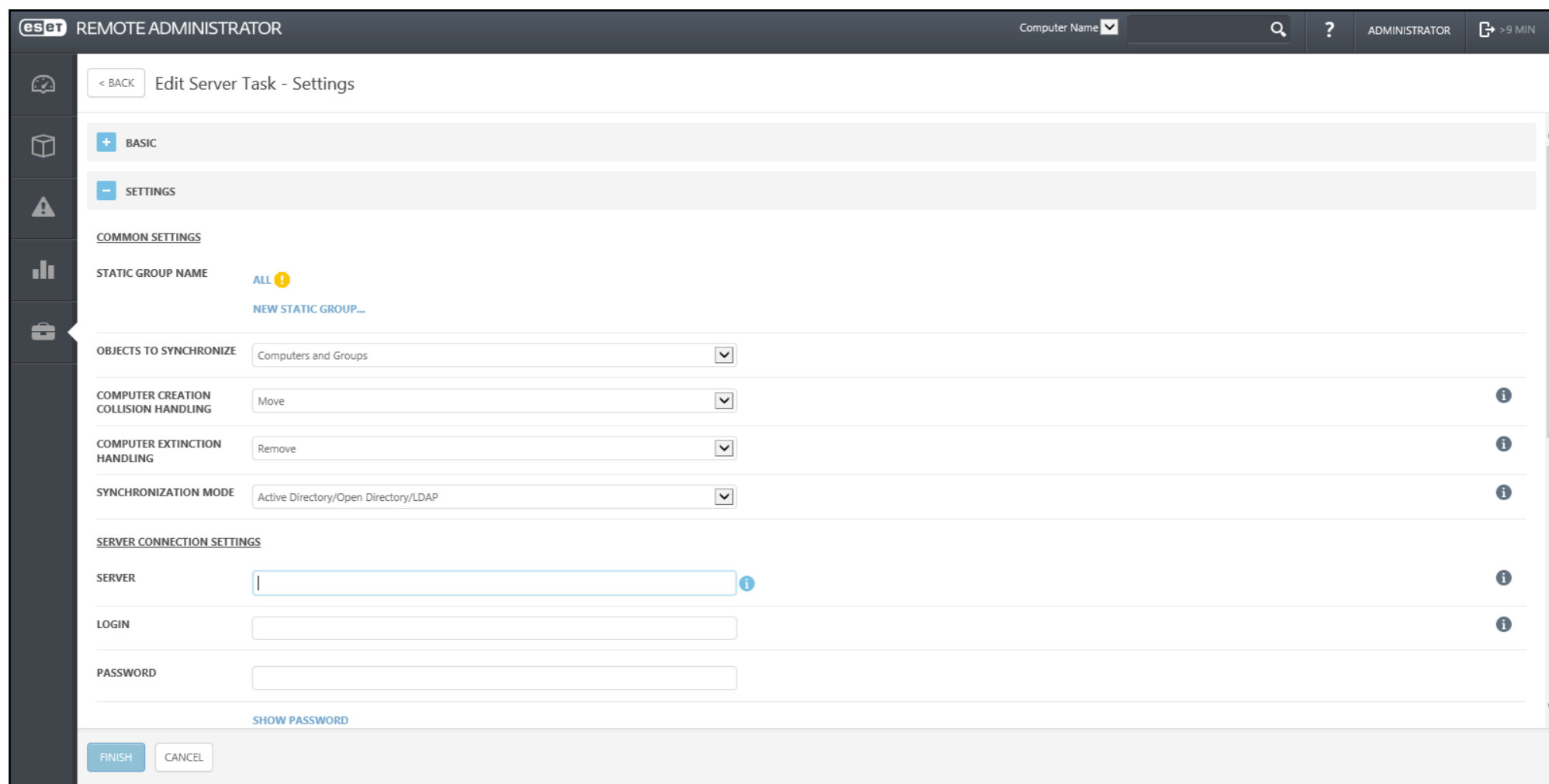
At the bottom of the interface, there are several buttons: 'SYNCHRONIZE LICENSES', 'OPEN ELA', 'OPEN MLS', 'ADD LICENSES', and 'REMOVE LICENSES'.

## Számítógépek felderítése

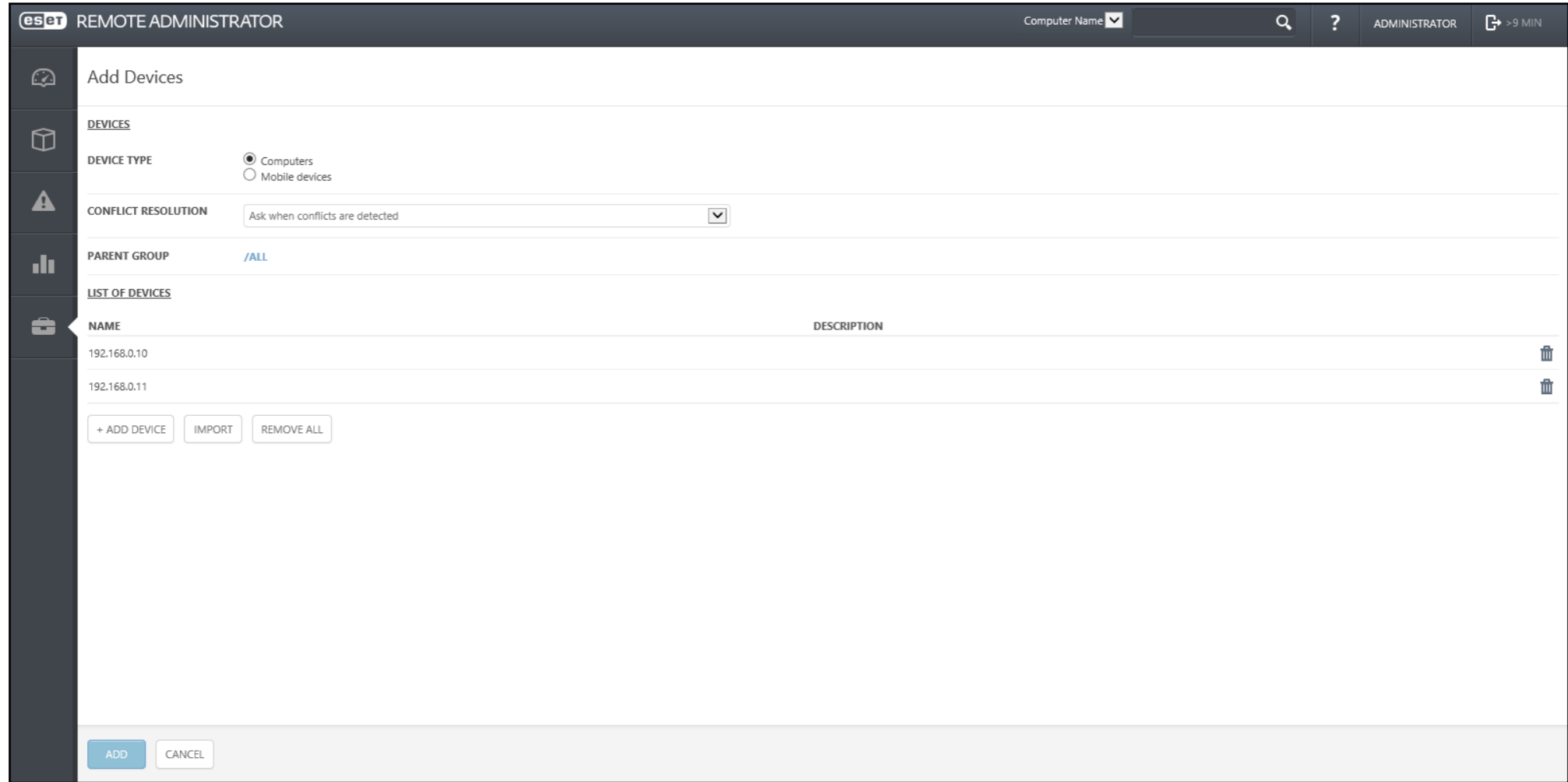
A hálózaton található számítógépek felderítésére legegyszerűbben az Active Directory szinkronizálásával van lehetőség, de amennyiben nem domain-es környezetben telepítette a távadminisztrációs programot, lehetősége van akár kézzel is hozzáadni a klienseket azok nevei vagy IP címei alapján, vagy importálhatja is azokat ugyanezen tulajdonságaik alapján egy CSV fájlból.

Az Active Directory-val való szinkronizálás feladat az **Admin -> Server Tasks** menüben a **Static Group Synchronization** elemet kiválasztva a **NEW...** gombra kattintva hozható létre. A feladat részletei között a **Settings** részt lenyitva adható meg, hogy mely csoportba szinkronizálja le a felderített számítógépeket, illetve az Active Directory helyét és az eléréséhez szükséges hitelesítő adatokat. A **Finish** gombbal hagyhatók jóvá a módosítások, ezt követően a feladat nevére kattintva a **Run now...** opció kiválasztásával futtatható le az. A feladat futásának állapota a feladat nevére kattintva, a Details lehetőséget kiválasztva az Executions fülön tekinthető meg.





A számítógépek kézzel történő hozzáadása az **Admin -> Groups** menüpontban végezhető el egy adott (célszerűen az All) csoport kiválasztásával és az **ADD NEW...** gombra történő kattintással. A megnyíló ablakban adhatók meg vagy importálhatók a számítógépek nevei vagy IP címei.

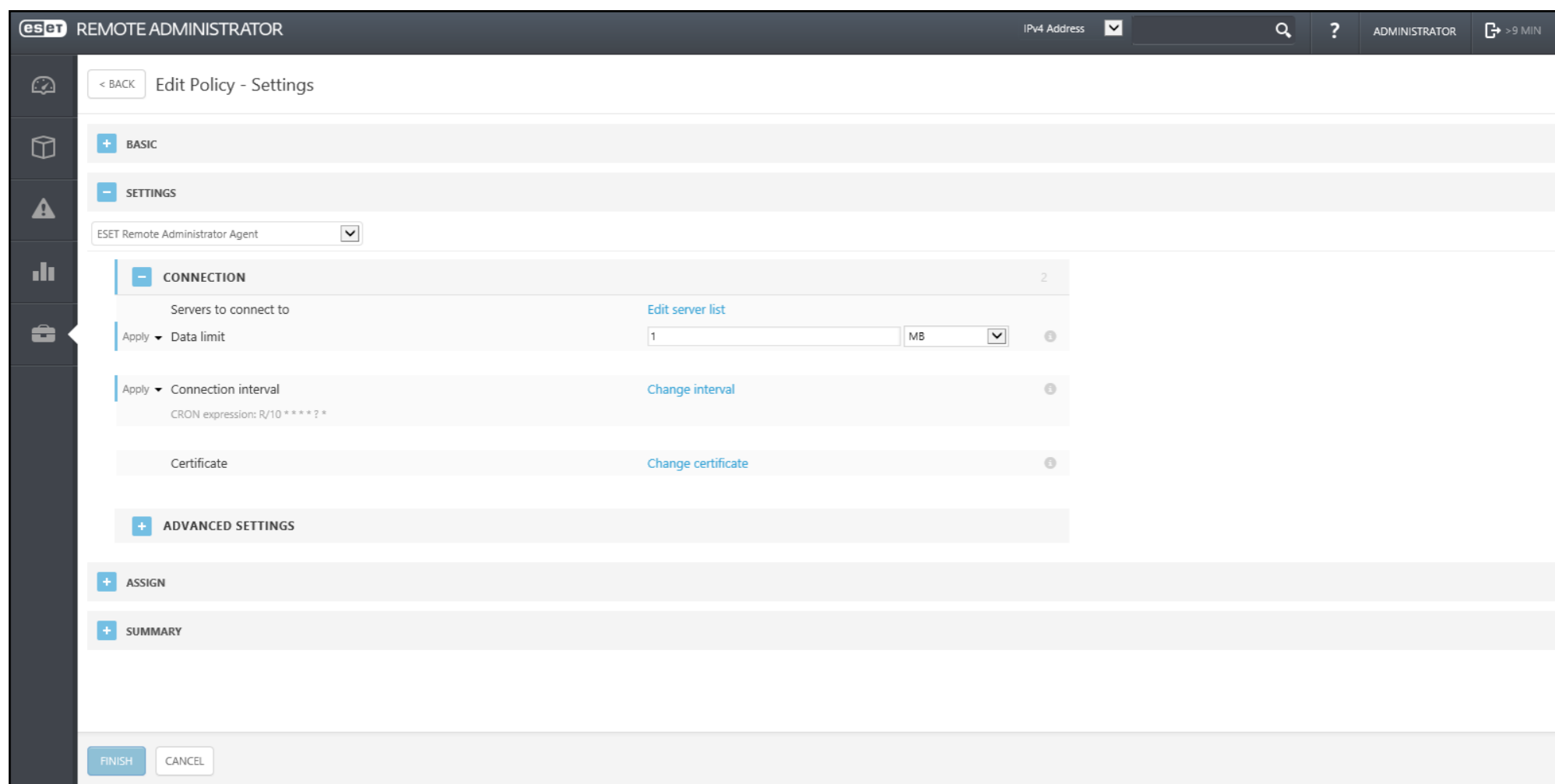


## Remote Administrator Agent telepítése

Ha megtörtént a hálózaton található számítógépek felvétele, a következő lépés azok menedzselhetővé tétele. Ehhez arra van szükség, hogy települjön a számítógépekre az ESET Remote Administrator Agent program, amely a háttérben fog futni egy szolgáltatásként és a távadminisztrációs szerver és a végpontvédelem közötti kommunikációért lesz felelős. Az Agent telepítésére többféle lehetőség is van, vagy távtelepítéssel leküldhető a munkaállomásokra, vagy egy önálló telepítő készíthető belőle, amely tetszőleges módon juttatható el a végpontokra.

## Agent policy módosítása

Az Agent telepítése előtt célszerű lecsökkenteni az Agent bejelentkezésének időközét a védelmi programok üzembe helyezésének idejére. Ez legegyszerűbben az Agent-ekre vonatkozó központi policy módosításával oldható meg, amelyet az **Admin -> Policies** menüpontban valamelyik **Remote Administrator Agent – Connection...** policy-t kiválasztva, majd alul a **POLICIES** gombra és a megjelenő **Edit...** lehetőségre kattintva tehető meg. A policy beállításai között a **BASIC** részen érdemes módosítani a policy nevében az időtartamot 10 másodpercre, majd a **SETTINGS** részt lenyitva a **Change interval** feliratra kattintva adható meg a kívánt gyakoriság. Az **ASSIGN** részen az **ASSIGN...** gombra kattintva, majd a megnyíló ablakban az **All** csoportot bepipálva adható meg, hogy a hálózat összes munkaállomására feltelepülő Agent-re vonatkozzon a gyakoribb bejelentkezési beállítás. Az Assign ablakban az **OK**, majd a **Finish** gombbal fejezhető be a policy módosítása.



## ***Agent telepítése távtelepítéssel***

Az Agent telepítése a szerverről történik, így az egy Server Task-nak minősül. Az új feladatot **Admin -> Server Tasks** menüben az **Agent deployment task**-ot kiválasztva a **NEW...** gombra kattintva vehető fel. A feladat beállításai között A Basic részen van lehetőség elnevezni a feladatot, majd a **Target(s)** feliratra kattintva választható ki, hogy mely számítógépekre vagy mely csoport összes számítógépére vonatkozzon a feladat. A célszámítógépeken rendszergazdai jogosultsággal rendelkező fiók hitelesítési adatait a **Username** és **Password** mezőkben szükséges definiálni. Ezt követően már csak az Agent kommunikációjához használandó **Agent certificate** tanúsítvány megadása van hátra a **<NO CERTIFICATE SELECTED>** feliratra kattintva megnyíló ablakban. A beállítások megadását követően a Finish gombra a feladat automatikusan elindul az imént definiált paraméterekkel. A távadminisztrációs szerver automatikusan észleli, hogy milyen típusú operációs rendszerre próbál telepíteni, és az annak megfelelő Agent telepítőjét használja. A feladat futásának állapota a feladat nevére kattintva, a Details lehetőséget kiválasztva az Executions fülön tekinthető meg.

Az Agent sikeres telepítésének érdekében a kliens gépeken a 139-es vagy a 445-ös TCP portok, illetve a 137-es és a 138-as UDP portok megnyitása szükséges.

### **Agent telepítése Live Installer segítségével**

A másik lehetőség az Agent telepítésére egy olyan végrehajtható fájl elkészítése, amely tartalmazza a távadminisztrációs szerver címét és a kommunikációhoz használatos tanúsítványt. A Live Installer készítése a webes konzol főablakán, a balról beúszó menüben az **Agent Live Installers...** szövegre kattintva készíthető el. A megnyíló ablakban meg kell adni a távadminisztrációs szerver szolgáltatást futtató számítógép nevét vagy IP címét, kiválasztani az Agent kommunikációjához használandó **Agent certificate** tanúsítványt, majd alul rákattintani a **GET INSTALLERS** gombra. Ekkor megjelennek a különböző operációs rendszereknek megfelelő Agent telepítők, amelyek a **DOWNLOAD** feliratokra kattintva tölthetők le majd juttathatók el a

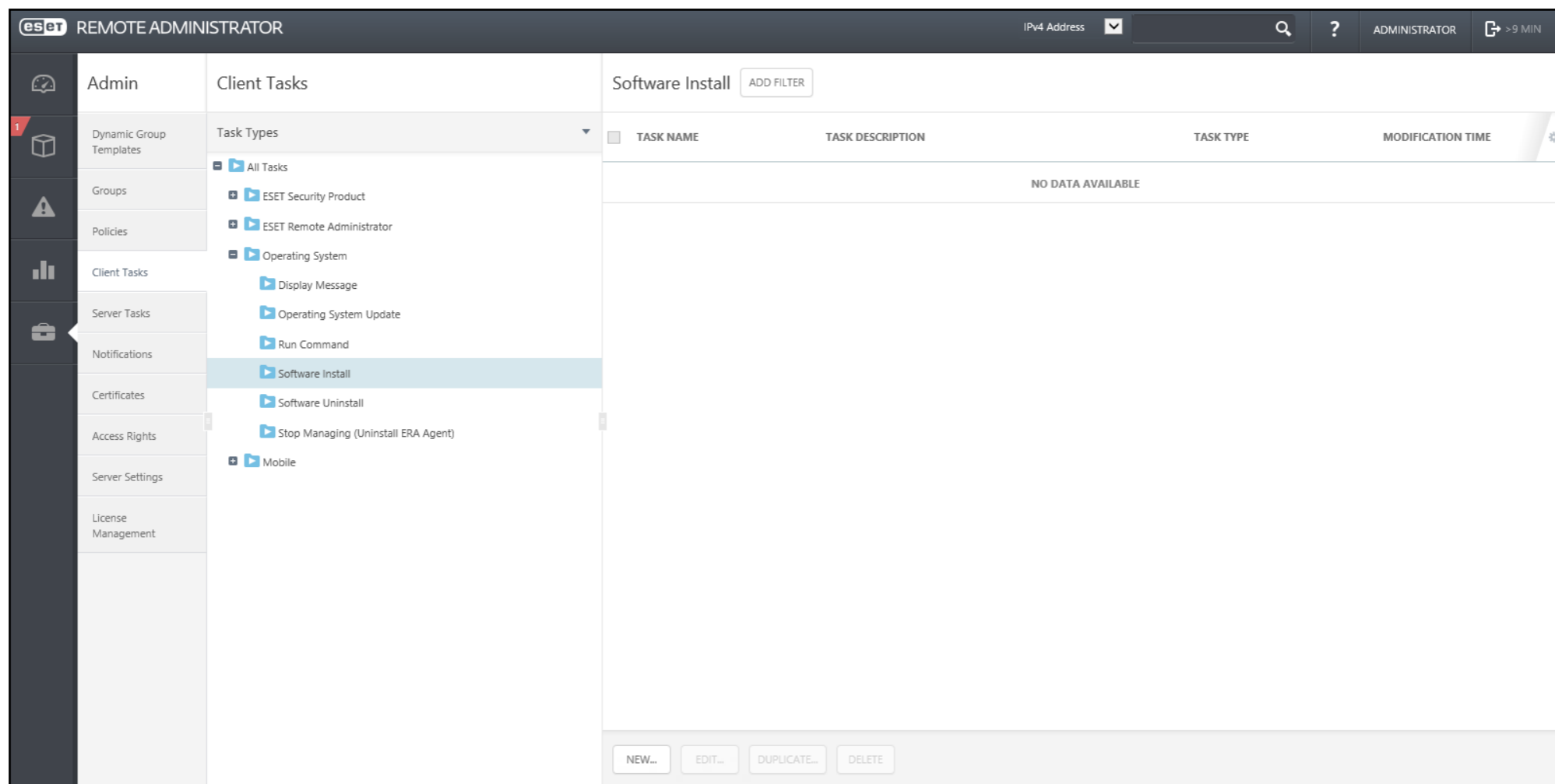
kliensekre igényeinek és lehetőségeinek megfelelően.

The screenshot shows the 'Agent Live Installers' configuration window in the ESET Remote Administrator. The interface includes a top navigation bar with the ESET logo, 'Computer Name' dropdown, search icon, help icon, 'ADMINISTRATOR' role, and '>9 MIN' timer. The main content area is divided into sections: 'INSTALLER CERTIFICATE' with fields for 'SERVER HOSTNAME (OPTIONAL)' (era-server), 'PEER CERTIFICATE' (radio buttons for 'ERA certificate' and 'Custom certificate'), 'ERA CERTIFICATE' (CN=AGENT AT \*), and 'CERTIFICATE PASSPHRASE' (with a 'SHOW CERTIFICATE PASSPHRASE' link). Below this is the 'PACKAGES TO DOWNLOAD' section with 'DOWNLOAD' buttons for 'AGENT INSTALLER FOR WINDOWS', 'AGENT INSTALLER FOR LINUX', and 'AGENT INSTALLER FOR MAC'. At the bottom, there are 'GET INSTALLERS' and 'CANCEL' buttons.

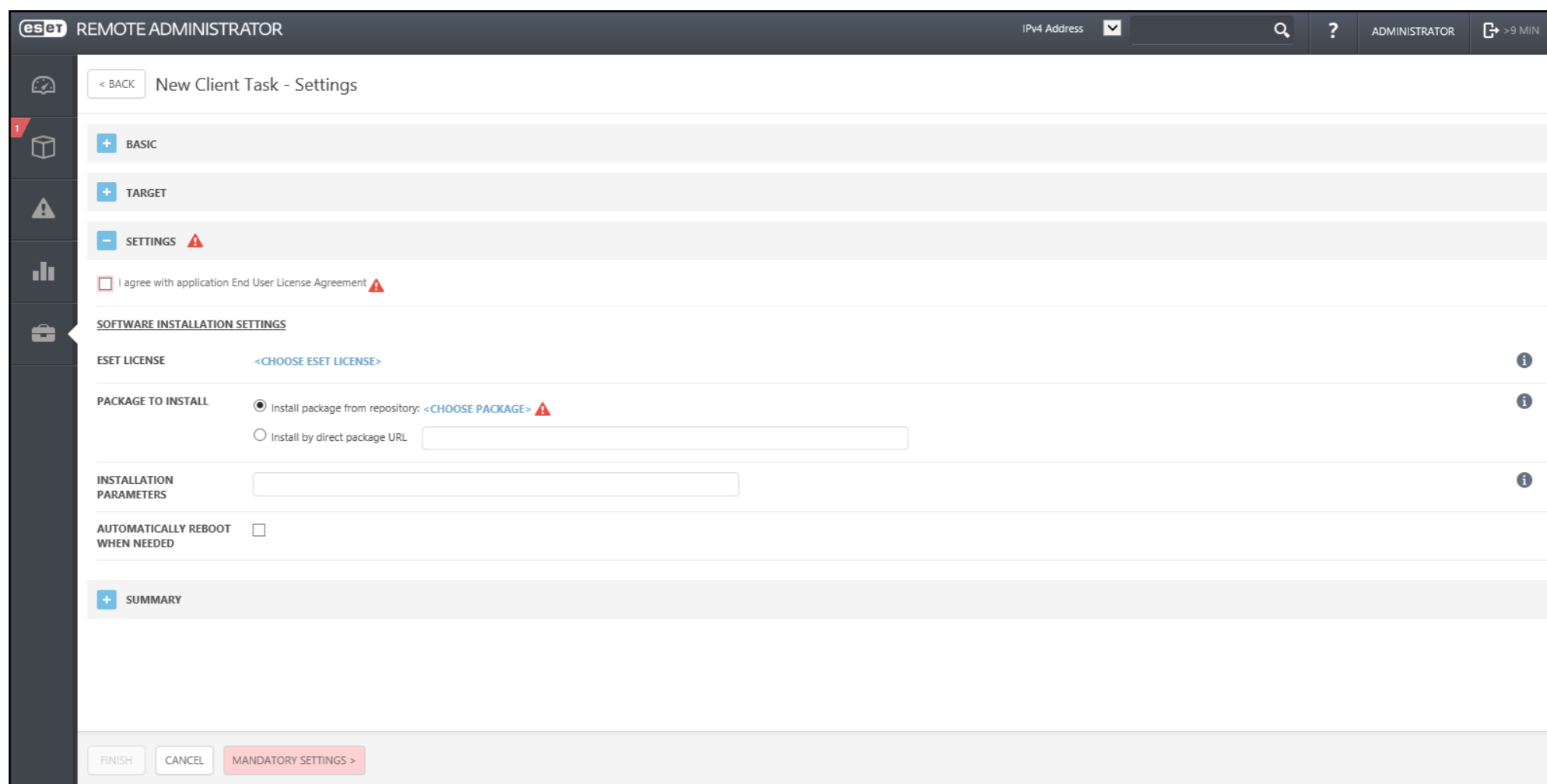
## Távtelepítés kliensre

Azt követően, hogy egy Agent telepítésre került egy munkaállomáson, minden további feladatot ez fog végrehajtani lokálisan. Éppen ezért a kliensekre történő távtelepítés már nem Server Task-nak számít, hanem Client Task-nak. Innentől kezdve a kliens számítógép a Computers csoportokban „Managable” jelzést kap, amely arra utal, hogy az Agent segítségével különböző feladatok végrehatásával kezelhetjük az adott számítógépeket központilag. Ilyen feladat lehet az adott gépről történő, más gyártótól származó védelmi programok eltávolítása, az operációs rendszer frissítése, üzenet megjelenítése vagy az ESET végpontvédelmi programjának telepítése.

Az ESET Endpoint programok távtelepítés megkezdéséhez szintén egy új feladat létrehozására van szükség, amely az **Admin -> Client Tasks** menüben az **Operating System** csoportban a **Software Install** elemet kiválasztva, majd a **NEW...** gombra kattintva történik.



A feladat részletei között megadható a telepítés neve, a szokásos módon kiválasztható, hogy az mely számítógépekre vagy csoportokra vonatkozzon (Agent megléte szükséges!), majd a végfelhasználói szerződés elfogadásának bepipálása után kiválasztható a végpontvédelmekre vonatkozó licence a **<CHOOSE ESET LICENSE>** feliratra, illetve a kívánt telepítő csomagot a **<CHOOSE PACKAGE>** szövegre kattintva. A beállítások megadását követően a **Finish** gombra a távtelepítési feladat automatikusan elindul az imént definiált paraméterekkel.





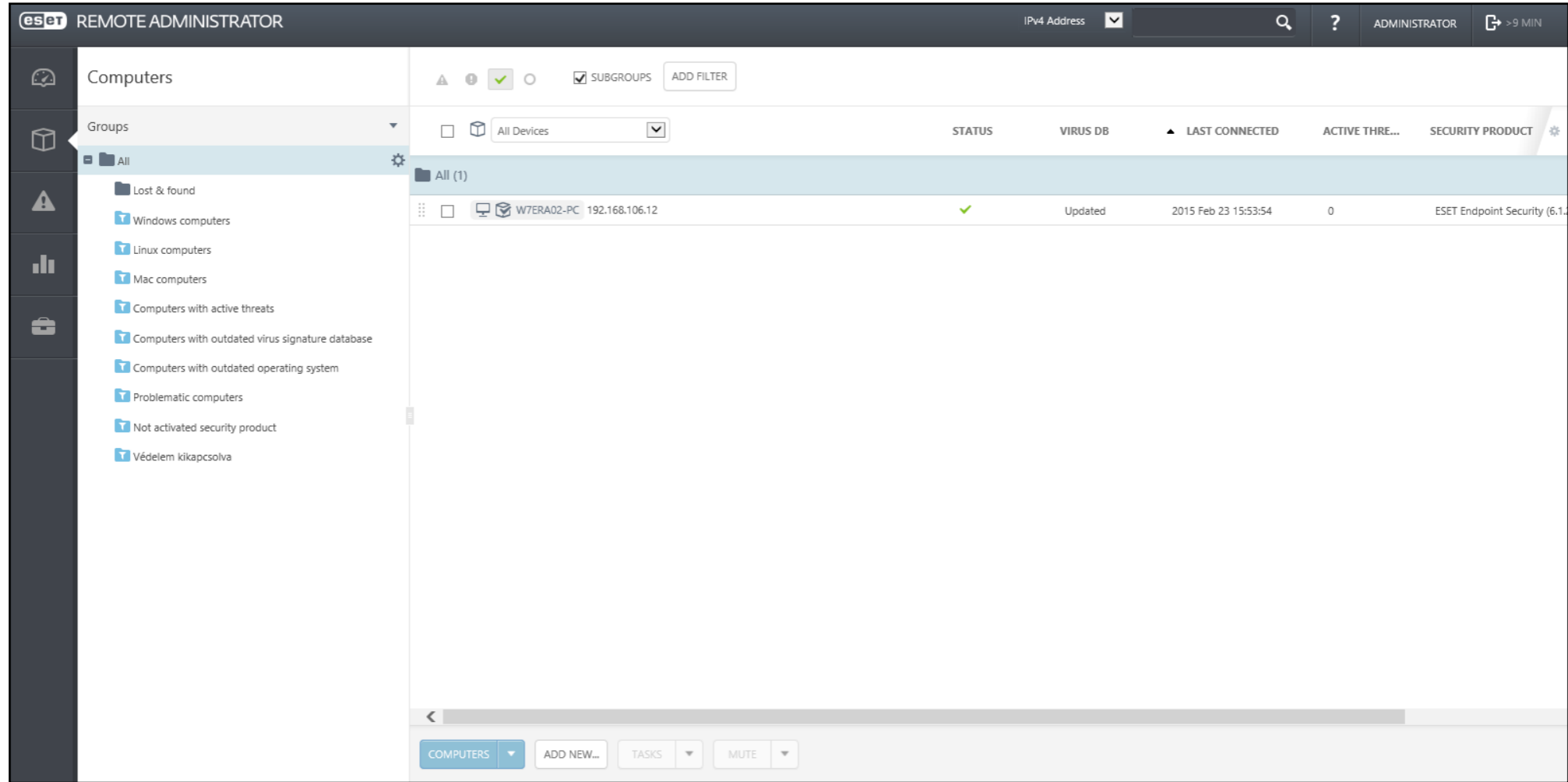
A feladat futásának állapota a feladat nevére kattintva, a **Details** lehetőséget kiválasztva az **Executions** fülön tekinthető meg.

The screenshot shows the ESET Remote Administrator web interface. The main window displays 'Client Task Detail: ESET Push-Install - Executions'. The interface includes a left-hand navigation menu with options like Admin, Dynamic Group Templates, Groups, Policies, Client Tasks, Server Tasks, Notifications, Certificates, Access Rights, Server Settings, and License Management. The main content area shows a table of task executions with the following data:

OCCURRED	COMPUTER NAME	COMPUTER DESCRIPTION	PRODUCT	STATUS	PROGRESS
2015 Feb 23 15:41:57	W7ERA02-PC		Operating system	Running	Task started
2015 Feb 23 15:41:57	W7ERA02-PC		ESET Remote Administrator Agent	Starting	Starting task

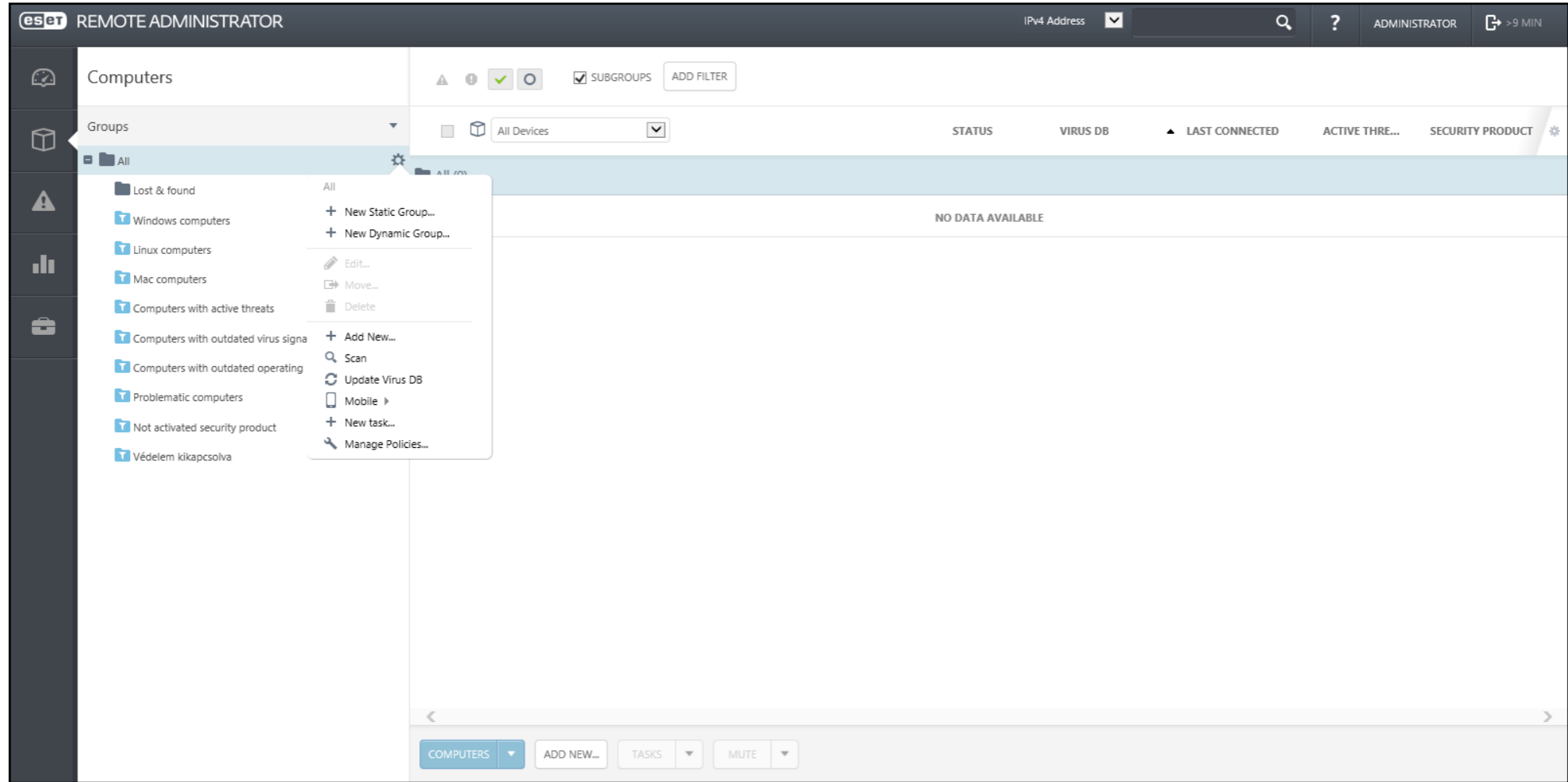
At the bottom of the window, there is a 'CLOSE' button.

Amikor a feladat sikeresen lefutott, a **Computers** részen már problémamentesen és biztonságos állapotban jelenik meg az adott számítógép.



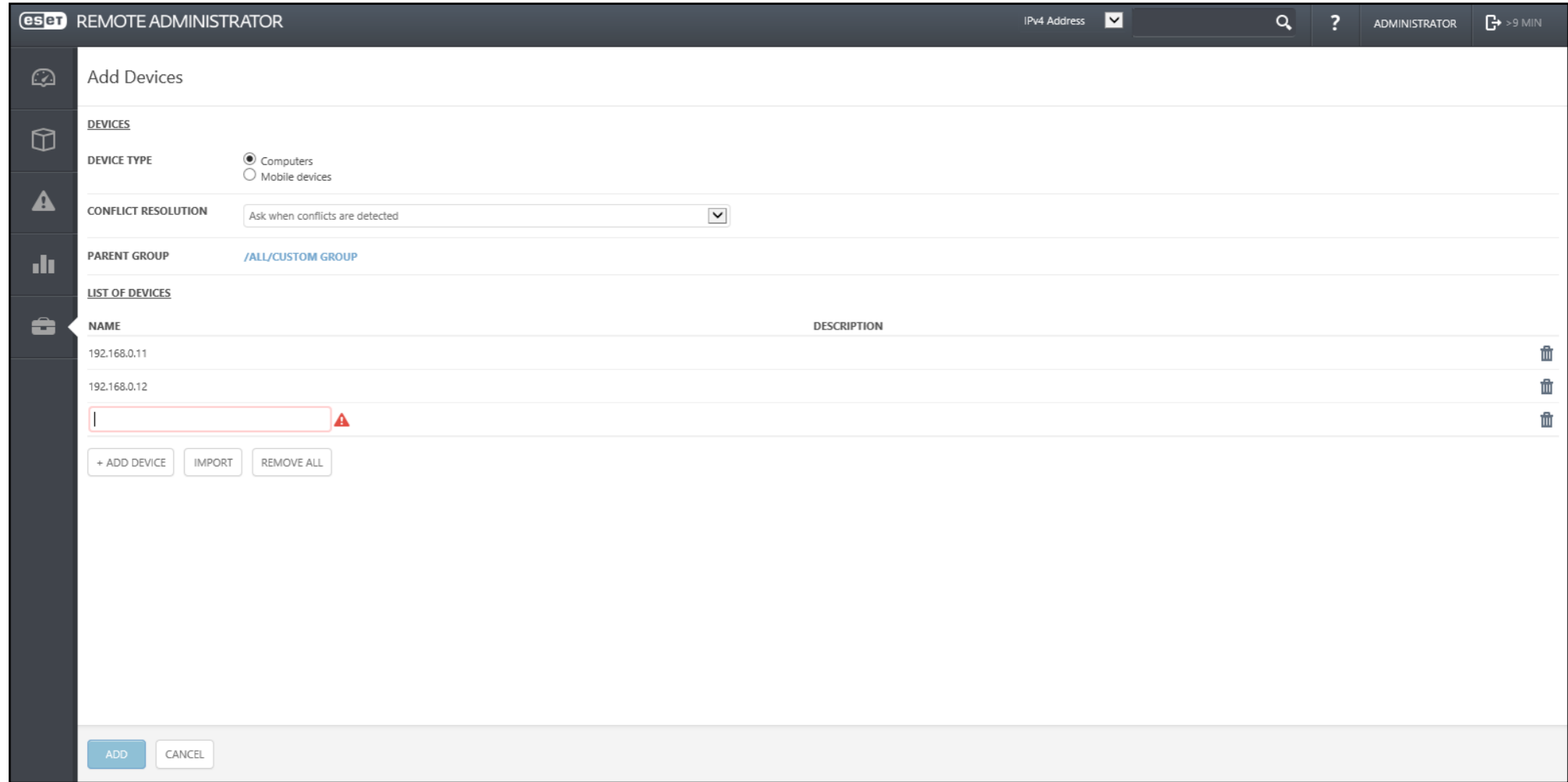
## Csoportkezelés

Egy távadminisztrációs program elengedhetetlen része a számítógépek logikai csoportokban történő egyszerű kezelése. Az ESET Remote Administrator erre kétféle lehetőséget biztosít, statikus és dinamikus csoportok létrehozását.



## Statikus csoportok

A statikus csoportok kezelése egyszerűbb, de nevükből fakadóan kevésbé rugalmasak és kevesebb funkcionalitás is köthető hozzájuk. A csoportot egyszerűen létre kell hozni, elnevezni, majd megmondani, hogy mely számítógépek legyenek a tagjai. Egy számítógép egy statikus csoportból csak kézi eltávolítás útján kerülhet ki, vagy magának a csoportnak a törlése esetén. Statikus csoport létrehozása a **Computers** menüpontban az All nevű csoport sorának végén lévő fogaskerékre kattintva a **New Static Group...** elem kiválasztásával történik. Létrehozása után a csoportot kiválasztva az **ADD NEW...** gombbal adhatók hozzá számítógépek, eszközök.

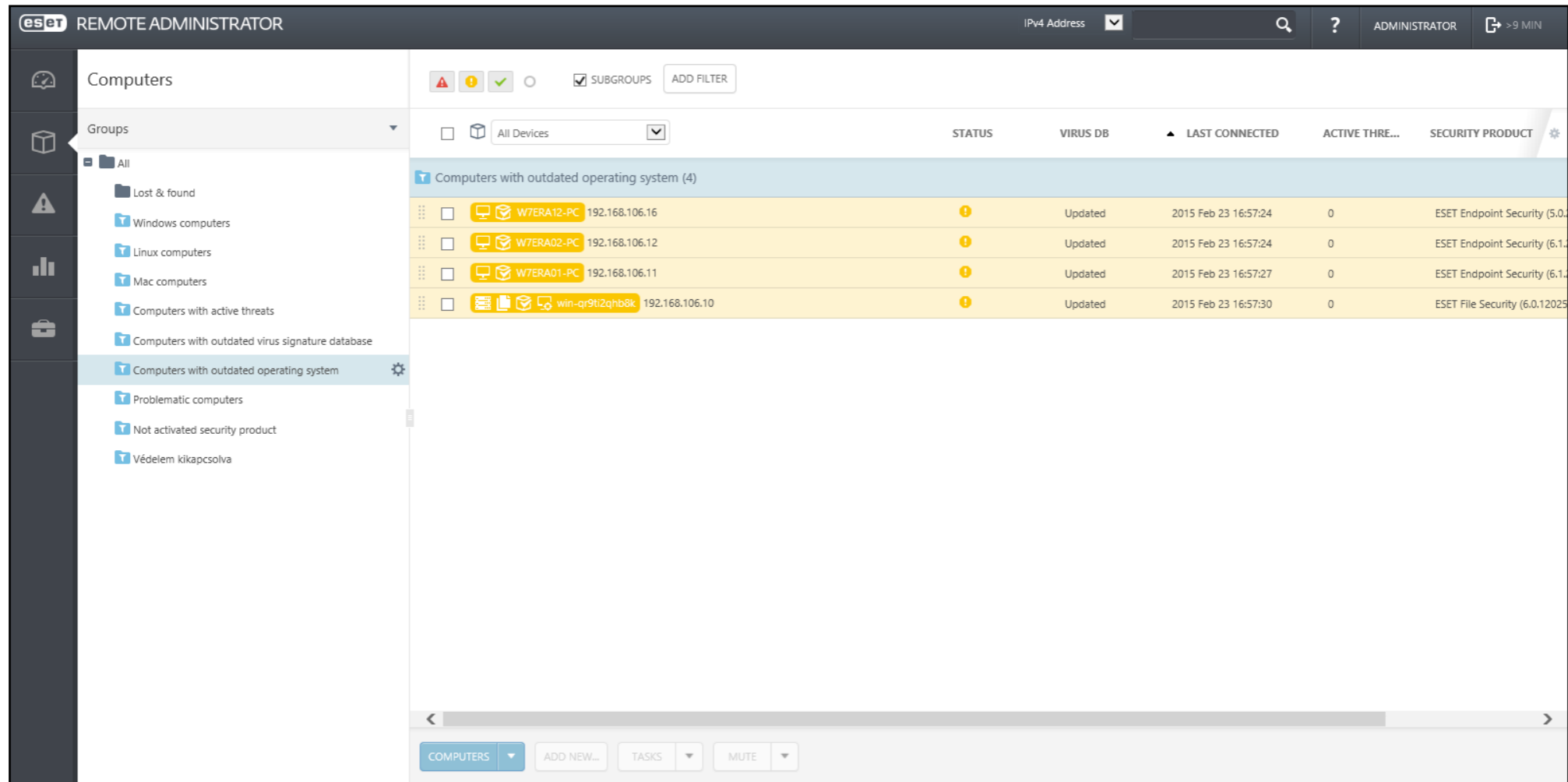


Statikus csoportokat az Active Directory lekérdezésével is fel lehet tölteni, ennek menete a Számítógépek felderítése bekezdésben már ismertetésre került.

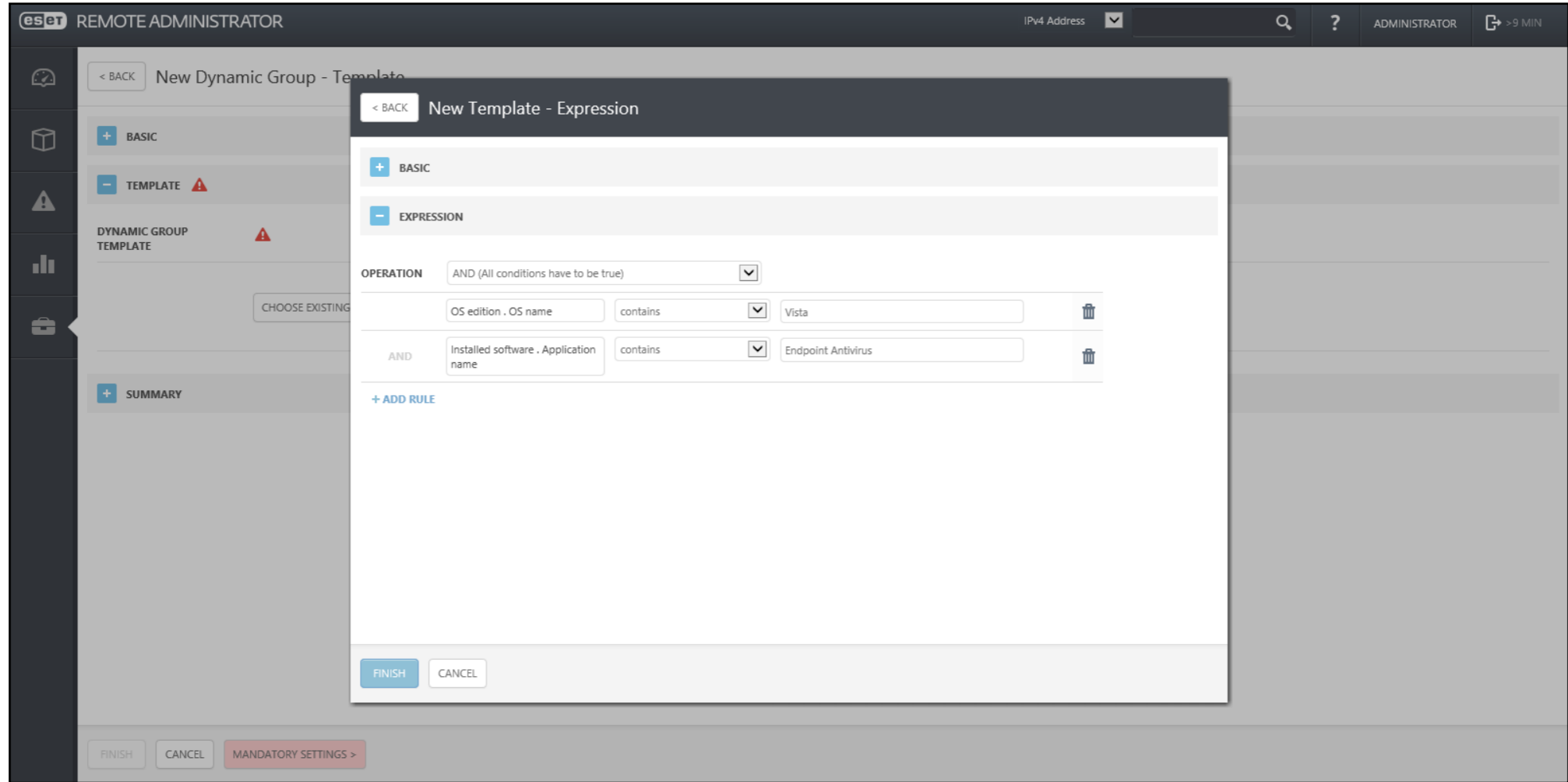
### **Dinamikus csoportok**

A dinamikus csoportok tagsága egy feltételhez kötött, azok létrehozásakor kell definiálni, hogy milyen feltétel teljesülése esetén kerül egy számítógép a csoport tagjai közé. Dinamikus csoport létrehozása a **Computers** menüpontban az **All** nevű csoport sorának végén lévő **fogaskerék** ikonra kattintva a **New Dynamic Group...** elem kiválasztásával történik. A csoport létrehozásakor annak elnevezése után a **Template** részen kiválasztható az előre definiált vagy már korábban létrehozott feltételek egyike a **CHOOSE EXISTING...** gombra kattintva, vagy a **NEW...** gombra kattintva létrehozható egy általunk

összeállított új feltétel-együttes, amelyek különböző logikai kapcsolókkal köthetők össze (AND, OR, NAND, stb.). A dinamikus csoportok és azok feltételei a számítógépeken futó Agentek-ben tárolásra kerülnek azok következő bejelentkezését követően, így egy számítógép ezentúl akkor is bekerülhet egy a dinamikus csoport valamelyikébe (és kaphatja meg annak policy-jét), ha épp nem csatlakozik a távadminisztrációs programhoz.



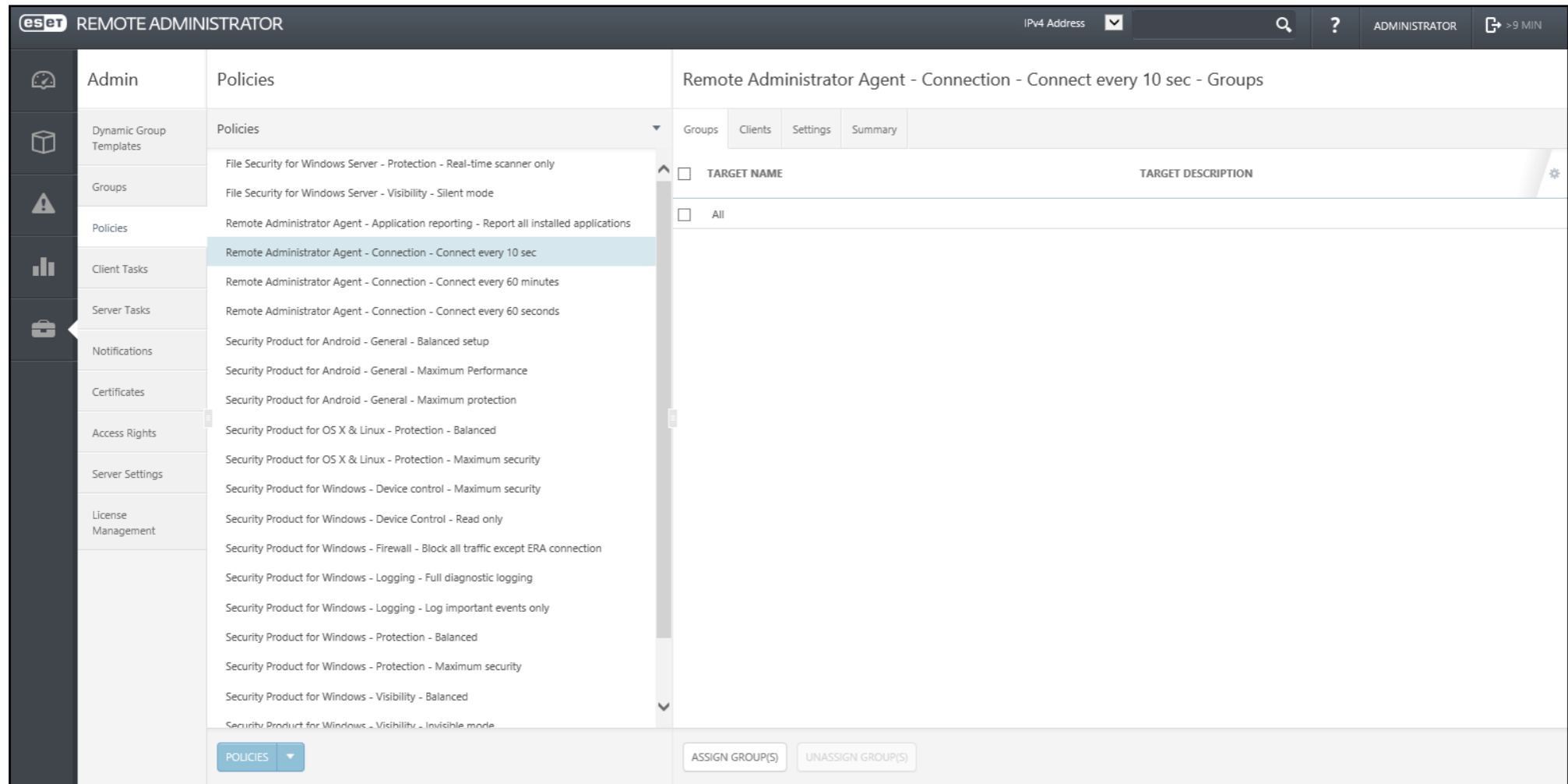
A dinamikus csoportok feltételei egyrészt lehetővé teszik, hogy adott állandó tulajdonságaik alapján kerüljenek a munkaállomások egy könnyen kezelhető logikai egységbe (pl. számítógépnév-maszk, IP cím, IP tartomány, operációs rendszer típusa, hardver elemek, stb.), másrészt dinamikusan kezelik a klienseket azok változó tulajdonságai alapján (adatbázis naprakésztsége, védelem állapota, operációs rendszer naprakésztsége, stb.).



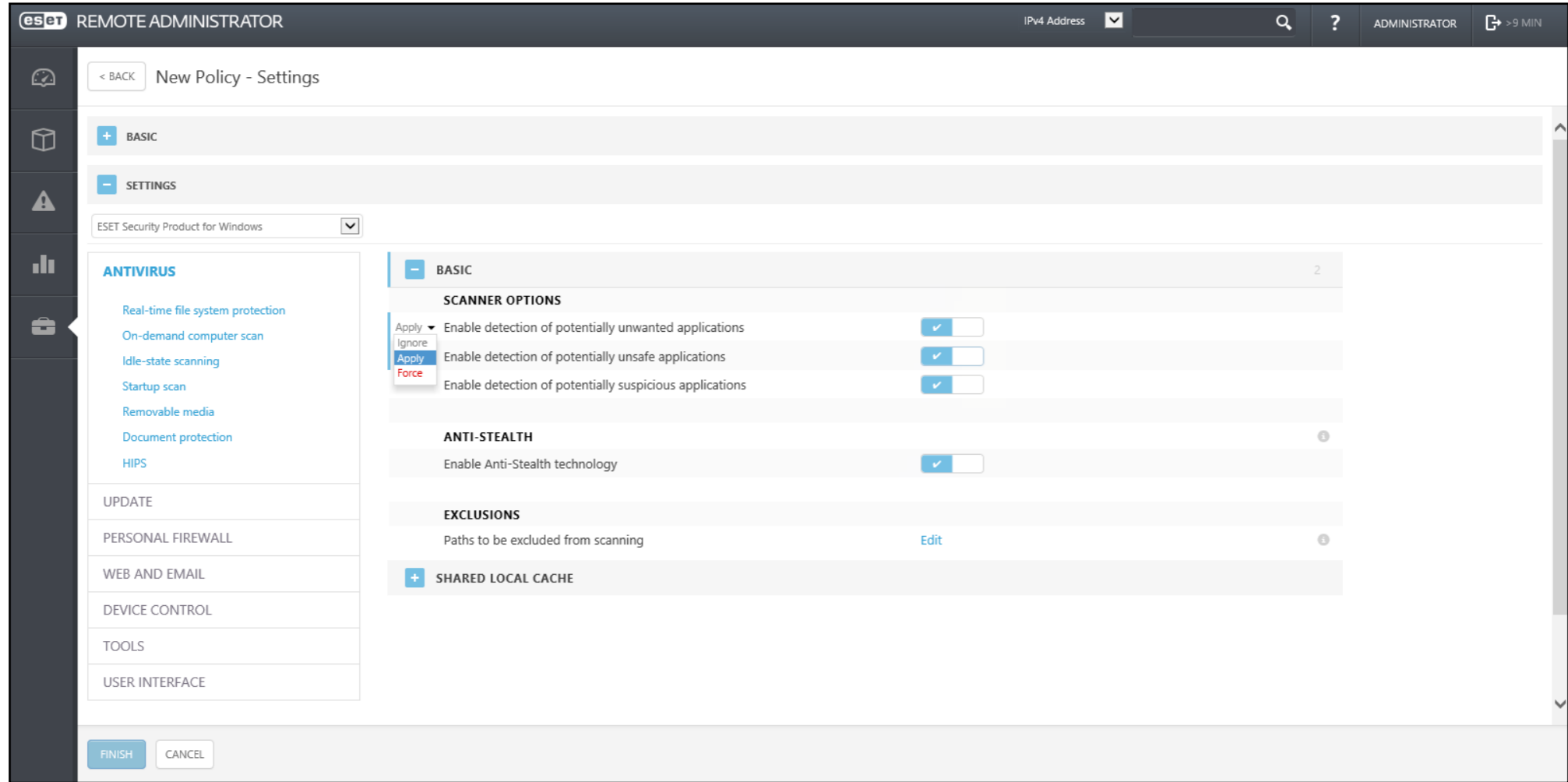
Egy dinamikus csoportba történő belépés kiváltó eseményéül szolgálhat bármilyen folyamatnak, ezáltal egy jól végiggondolt csoportosítással lehetőség nyílik az esetlegesen felmerülő problémák automatikus kezelésére. (lásd. később)

## Policy-k kezelése

A policy (másnéven házirend) egy beállításjegyzék, amely tartalmazza egy kliens (végpontvédelem, szervervédelem, Agent, stb.) azon beállításait, amelyek megváltoztatása nem engedélyezett a felhasználók számára. A policy-k kezelése az **Admin -> Policies** menüpontban történik, itt meg lehet tekinteni az előre definiált policy-ket és a korábban hozzáadott saját policy-ket, továbbá a jobb oldali részen a **Groups** illetve **Clients** fülön, hogy mely csoportokra és munkaadásokra érvényesek, a **Settings** fülön pedig hogy milyen beállításokat tartalmaznak.



Új policy létrehozása a **POLICIES** gombra kattintva megjelenő lehetőségek közül a **New...** kiválasztásával történik. A policy elnevezését követően a **Settings** részen meg kell adni, hogy milyen típusú termékekre vonatkozzon, majd módosítani vagy megjelölni a fenntartandó beállításokat a megjelenő beállítások között. Az itt látható beállítás teljes egészében megegyezik egy kliens lokálisan módosítható részletes beállításaival, így a beállítások kezelése könnyebben elsajátítható.



Egy adott beállítás három szinten képezheti részét egy policy-nek. **Ignore** állapotban egy beállítás nem része a policy-nek, alapértelmezetten az összes beállítás ebben az állapotban van. **Apply** állapotban a beállítás része egy policy-nek, de egy másik policy felülírhatja azt, amennyiben az később kerül kiértékelésre, vagy később kerül alkalmazásra az adott kliensen. A **Force** állapot mindenképpen alkalmazásra kerül egy kliensen és úgy is marad, még akkor is, ha egy később alkalmazásra kerülő policy más értéket adna szintén Force jelölővel.

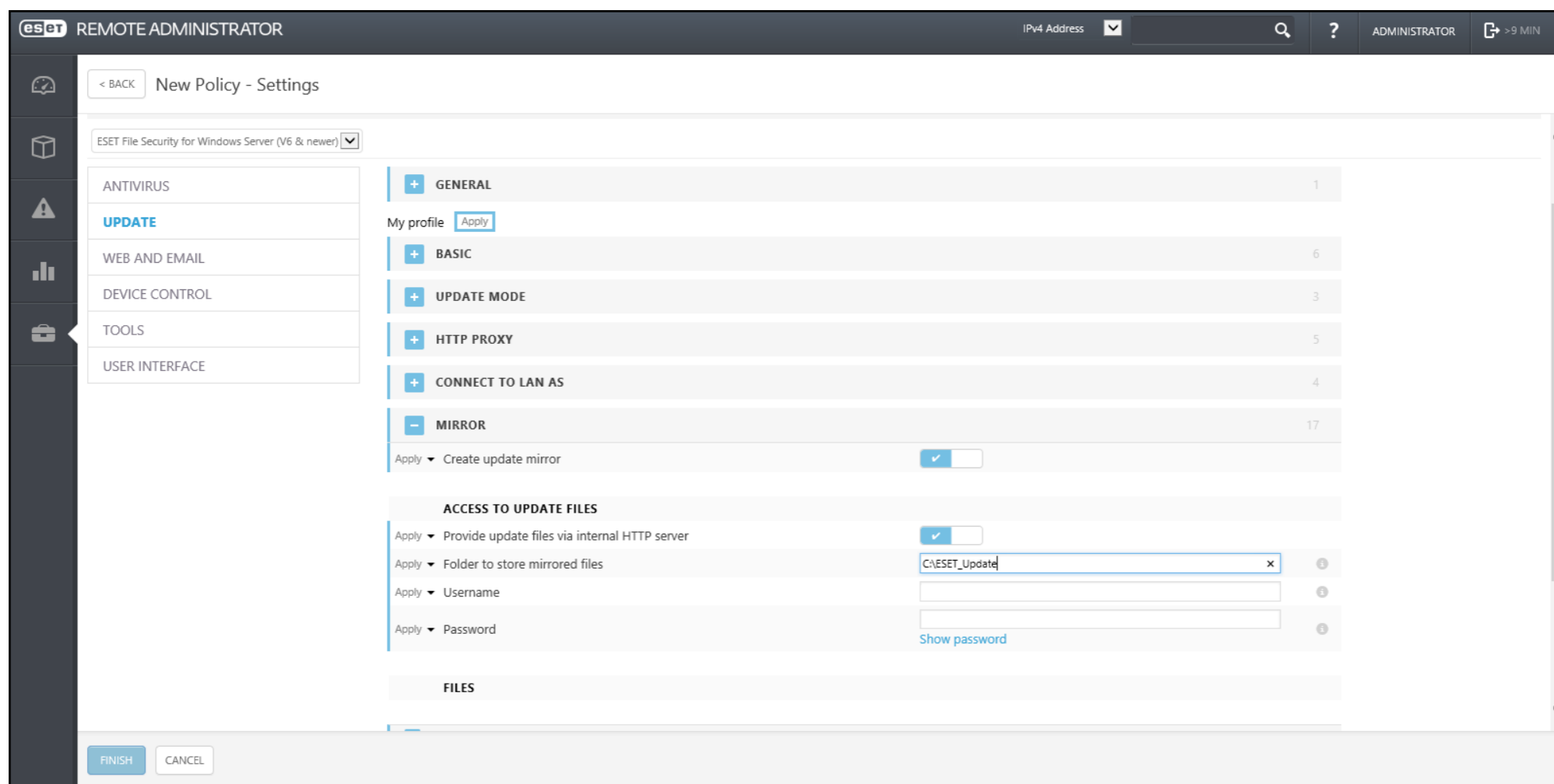
Az **Assign** részen az **ASSIGN...** gombra kattintva jelölhetjük ki, hogy az imént definiált beállításjegyzék mely kliensekre vagy mely csoport összes tagjára vonatkozzon.



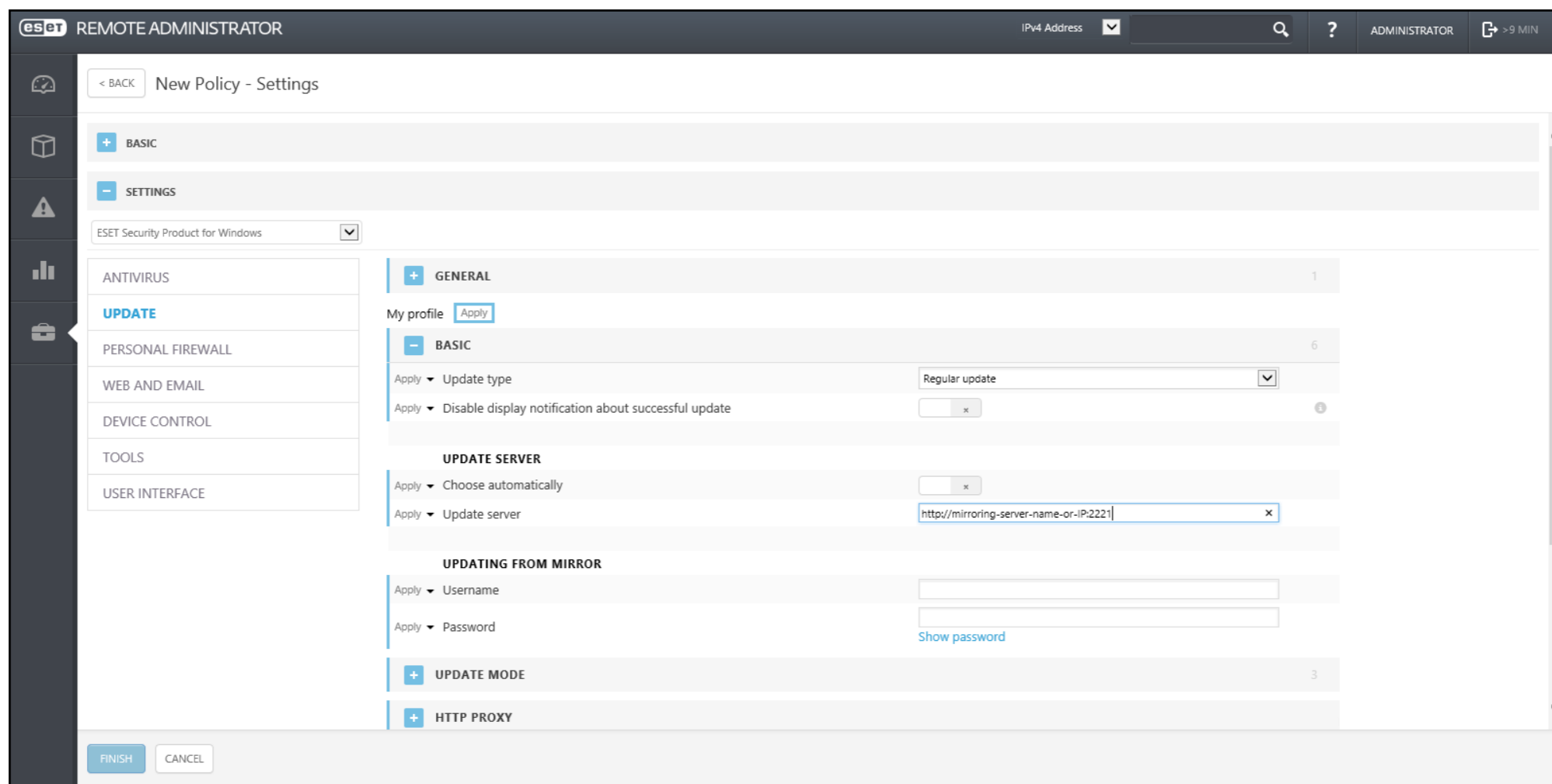
## Tükrözés beállítása

A vírusadatbázis tükrözésének beállítására, tehát hogy a frissítéseket ne minden kliens önállóan, az interneten keresztül töltsse le, kétféle megközelítés létezik az ESET Remote Administrator programban. Az egyszerűbb megoldás az adatbázis letöltését és megosztását a szerveren futó védelmi program (vagy egy dedikált kliens) policy-jének módosításával, majd a többi kliens frissítési szerverének erre a szerverre való beállításával történik.

A policy-k létrehozásának ismeretében a tükrözés beállítása a szerveren vagy egy dedikált kliensben a beállítások között az **Update** -> **Mirror** részen a **Create update mirror** opció engedélyezésével illetve a tárolási mappa megadásával történik (célszerűen C:\ESET\_Update mappa).



A többi kliens frissítési beállításait szintén a rájuk érvényes policy módosításával érdemes megoldani. Az imént létrehozott frissítési tükör használata a beállítások között az **UPDATE -> BASIC** részen az **Update szerver** tulajdonságai alatt a **Choose automatically** opció kikapcsolásával, majd a szerver kézi megadásával történik az **Update server** mezőben, **http://name-or-ip:2221** formában.



A tükrözés másik formája Apach HTTP Server Proxy konfigurálásával történik, ennek kialakítása kevésbé egyszerű, részletes leírását [itt találja.](#)

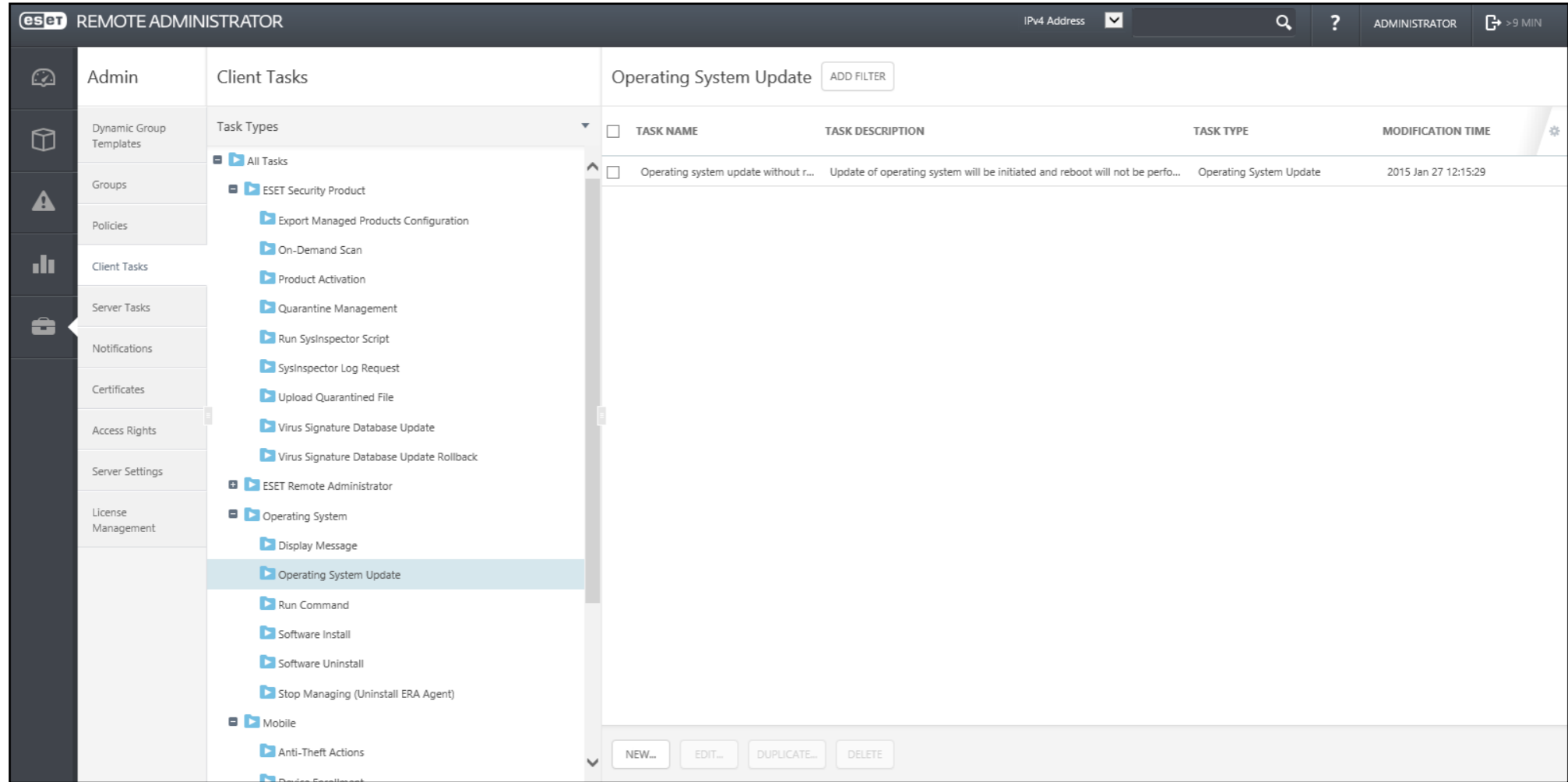
## Események, feladatok, automatizálás

Az ESET távadminisztrációs rendszerének egyik legnagyobb előnye annak automatizálhatósága. Előre beállított események hatására automatikus feladatok ütemezhetőek be, amelyek segítségével a rendszergazda távollétében is kezelésre kerülnek az esetlegesen felmerülő problémák.

### **Feladatok**

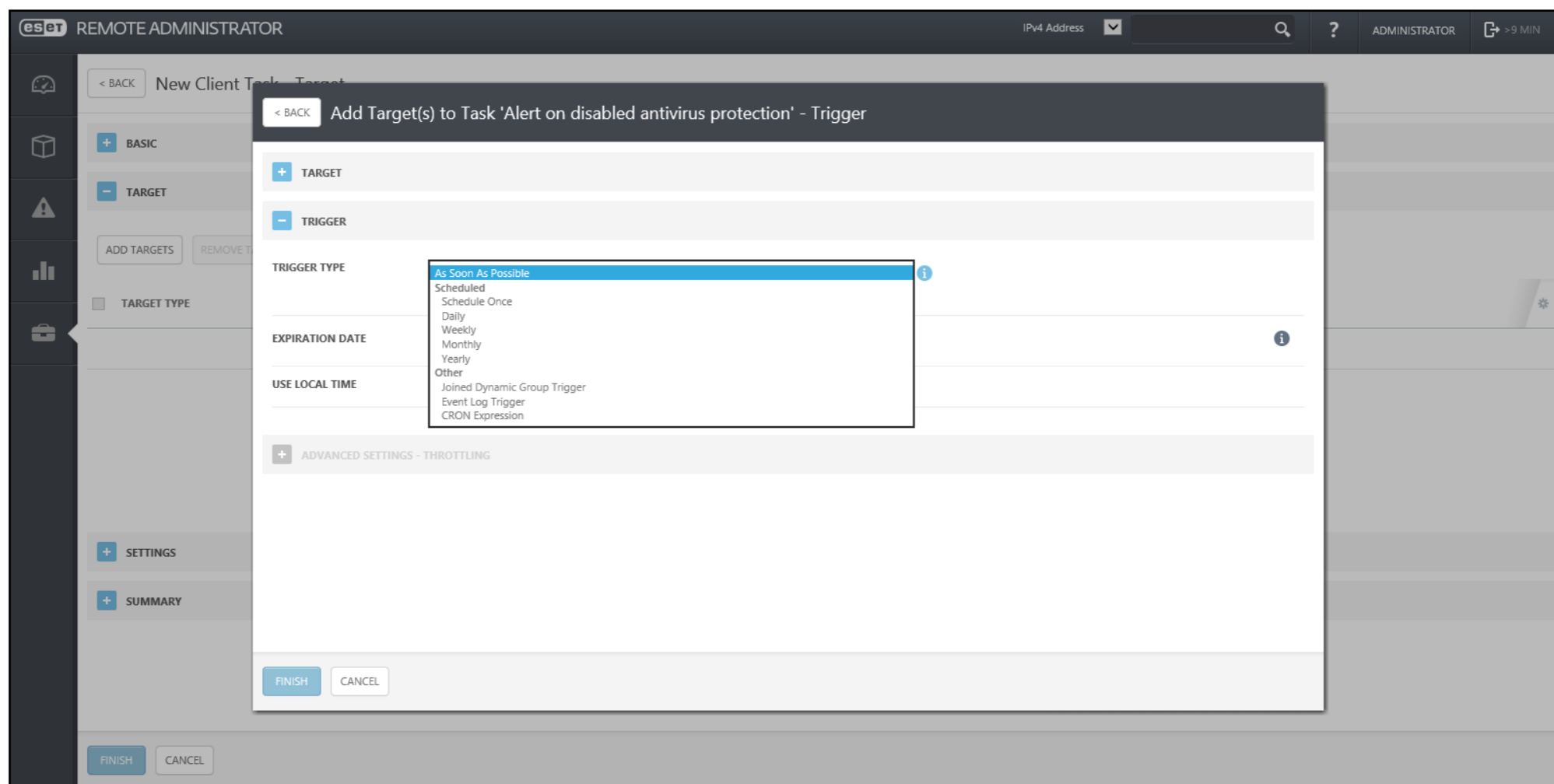
Az ESET Remote Administrator szerteágazó feladatok formájában végzi a klienseken vagy a szervereken eszközölt változtatásokat vagy folyamatokat. Szerverfeladatnak számít az Agent távtelepítése, az Active Directory szinkronizálása és a különböző riportok készítése. Az összes többi feladat a klienssel vagy az azon futó ESET programmal kapcsolatos, ezek futását az Agent vezérli lokálisan, így ezek kliensfeladatnak számítanak. A kliensfeladatok vonatkozhatnak az operációs rendszerre (rendszerfrissítés, program telepítése/eltávolítása, parancs futtatása, üzenet megjelenítése), lehetnek ESET specifikusak is (frissítés, aktiválás, ütemezett feladat futtatása, stb.), vonatkozhatnak mobil eszközökre (lopásvédelmi funkciók aktiválása, eszköz ellenőrzése, szoftver telepítése), illetve vonatkozhat magára a távadminisztrációs programra (komponensek telepítése, RD sensor adatbázisának törlése, stb.).

Szerverfeladatokat az **Admin -> Server Tasks** részen, kliensfeladatokat pedig az **Admin -> Client Tasks** részen lehet felvenni az adott feladat típus kiválasztását követően a **NEW...** gombra kattintva. Előredefiniált vagy már korábban létrehozott feladatot a feladat nevére kattintva a **Run now** opció kiválasztásával lehet ismételten lefuttatni (amennyiben az nem eseményhez kötött). A feladat futásának állapota a feladat nevére kattintva, a Details lehetőséget kiválasztva az Executions fülön tekinthető meg.

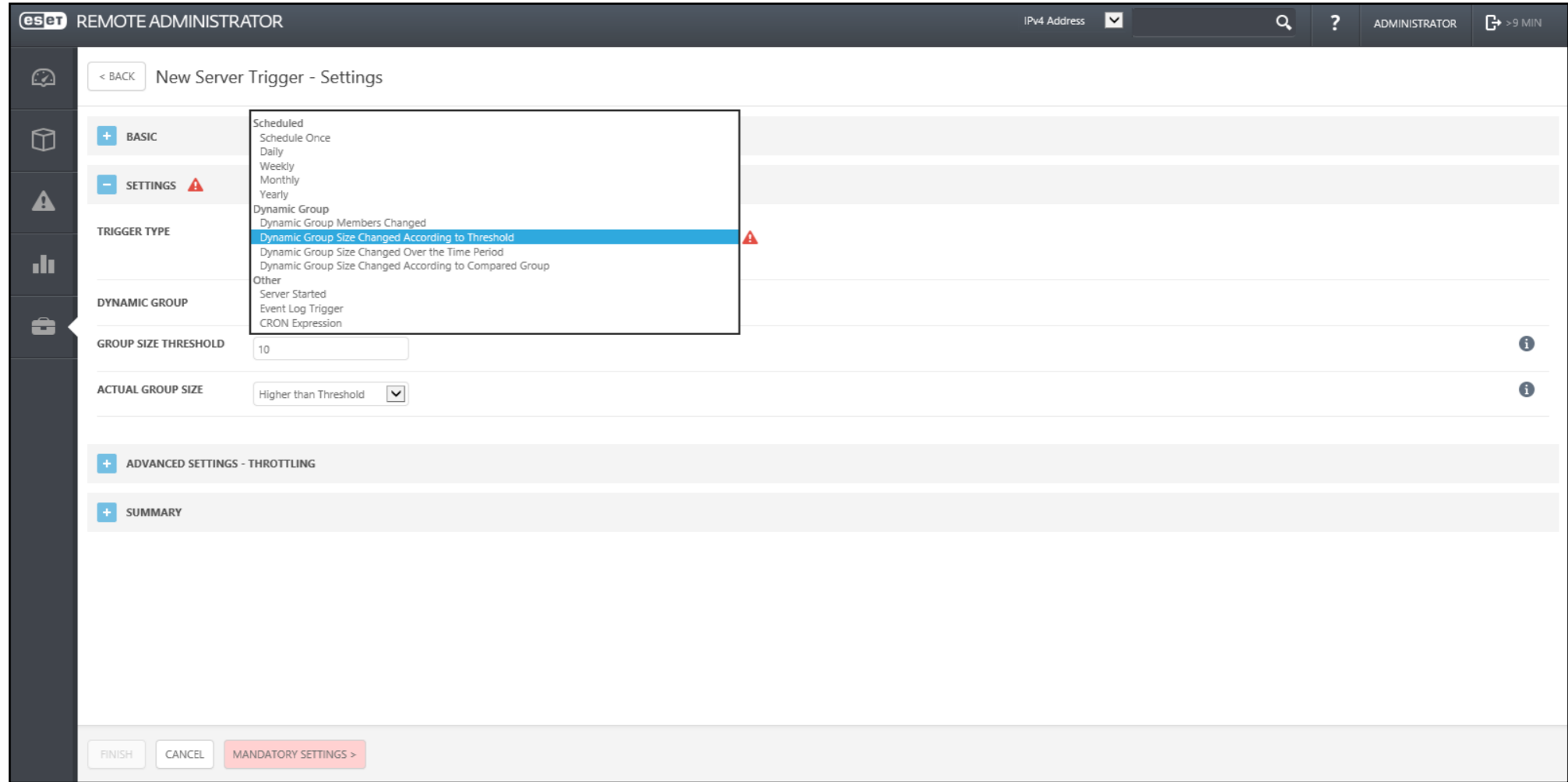


## Triggerek

A triggerek, másnéven kiváltó események, azokat az eseményeket jelölik, amelyek valamely feladat végrehajtásának alapjául szolgálhatnak. Minden felvett feladatnál be lehet állítani a **TARGET** részen az **ADD TARGETS** gombra kattintva, hogy mely kliensekre vonatkozzon, illetve a **TRIGGER** részen, hogy az mikor vagy minek hatására fusson le.



A triggerek definiálhatók külön az egyes folyamatokhoz, vagy előre is felvehetők későbbi használatra. A triggerek kezelése az **Admin -> Server Tasks -> Triggers** menüben történik, új triggert a **NEW...** gombra kattintva vehet fel. Itt megadható a szokásos időbeli gyakoriság mellett egy dinamikus csoportba való bekerülés, ha egy dinamikus csoport tagjainak a száma egy adott érték fölé nő, vagy egy megadott idő alatt meghatározott mértékben változik, de két különböző csoport tagjainak különbsége is lehet kiváltó esemény. Az esemény lehet még naplófájl beérkezése vagy a távadminisztrációs rendszer elindulása is.



## Automatizálás

A különböző csoportok, policy-k, feladatok és triggerek együttes használatával beállítható, hogy egy elavult védelmű program esetén a felhasználó figyelmeztetést kapjon arról, hogy a frissítésig a hálózati kapcsolatai blokkolásra kerültek, automatikusan futtatható operációs rendszer-frissítés, ha az elavult (tehát a kliens ezért bekerült a megfelelő csoportba), vagy automatikusan telepíthető az Agent és a védelmi program a védelem nélküli gépekre.

## Értesítések

A távadminisztrációs szerver értesítési funkciója bizonyos események hatására email-ben tájékoztatja a rendszergazdát. Az értesítések kezelése az **Admin -> Notifications** menüpontban történik. Itt megtekintheti és szerkesztheti az előre definiált értesítéseket, vagy létrehozhat újakat is a **NEW NOTIFICATION...** gombra kattintva, igényeinek megfelelően.

NOTIFICATION NAME	NOTIFICATION DESCRIPTION
<input type="checkbox"/> Malware outbreak alert (percentage criteria)	Notification is sent when at least 5% of managed computers have active threats (is located in Active threats dynamic group)
<input checked="" type="checkbox"/> Malware outbreak alert (count per time criteria)	Notification is sent when count of threat detection events in defined period of time exceeds the defined threshold
<input type="checkbox"/> Network attack alert	Notification is sent when count of firewall events in defined period of time exceeds the defined threshold
<input type="checkbox"/> Computers report problems alert	Notification is sent when at least 5% of managed computers have reported problem (is located in Computer has reported problem dyna...
<input type="checkbox"/> Outdated virus signature database alert	Notification is sent when at least 5% of managed computers have outdated virus signature database (is located in Outdated Virus Signat...
<input type="checkbox"/> Expiring CA certificate alert	Notification is sent when at least one of the CA certificates is due to expire in less than 30 days
<input type="checkbox"/> Expiring peer certificate alert	Notification is sent when at least one of the peer certificates is due to expire in less than 30 days
<input type="checkbox"/> Expiring license alert	Notification is sent when at least one of the managed licenses is due to expire in less than 30 days
<input type="checkbox"/> Overused license alert	Notification is sent when at least one of the managed licenses is overused
<input type="checkbox"/> License limit alert	Notification is sent when at least one of the managed licenses is utilized more than 90%
<input type="checkbox"/> Network peer overloaded alert	Notification is sent when at least one of the network peers is in state Limited or Overloaded
<input type="checkbox"/> Managed clients not connecting alert	Notification is sent when at least 5% of all managed clients have not connected for more than 2 days
<input type="checkbox"/> Outdated ESET software alert	Notification is sent when outdated ESET software is detected on at least one of managed computers
<input type="checkbox"/> Failing server task alert	Notification is sent if during the last 2 days any of the server tasks failed more than once

ONE ITEM SELECTED.

NEW NOTIFICATION... EDIT NOTIFICATION... DELETE

Az értesítések tekinthetők tulajdonképpen olyan e-mail küldési feladatoknak, amelyek a kiváltó eseményeik statisztikai gyakoriságát is figyelembe vehetik. Tehát definiálható, hogy a távadminisztrációs program csak bizonyos számú eseményt követően küldjön értesítést, vagy csak abban az esetben, ha az egy adott számban jelentkezik egy bizonyos időtartamon belül. Az értesítés típusa a **NOTIFICATION TEMPLATE** részen választható ki, az üzenet szövege és formátuma a **CONFIGURATION**

részen adható meg, a különböző számbeli vagy időbeli statisztikák pedig az **ADVANCED SETTINGS – THROTTLING** részt lenyitva definiálhatók. Ezt követően a **DISTRIBUTION** részen adható meg, hogy milyen e-mail címre szeretné eljuttatni az imént felvett feltételek teljesülése esetén elküldött értesítést.

The screenshot displays the 'New Notification - Notification Template' configuration window in the ESET Remote Administrator interface. The window is divided into several sections:

- BASIC**: A section header with a plus icon.
- NOTIFICATION TEMPLATE**: A section header with a minus icon. Below it, the 'NOTIFICATION TEMPLATE' dropdown is set to 'Other Event Log Template'. A note below reads: 'Notifications not associated with a dynamic group but rather a system events filtered out from the event log'.
- LOG TYPE**: A dropdown menu set to 'Antivirus threat'.
- LOGICAL OPERATOR FOR FILTERS**: A dropdown menu set to 'AND (All conditions have to be true)'. An information icon (i) is visible to the right.
- FILTER BY**: A section with a '+ ADD FILTER' button and an information icon (i) to the right.
- CONFIGURATION**: A section header with a plus icon.
- ADVANCED SETTINGS - THROTTLING**: A section header with a plus icon.
- DISTRIBUTION**: A section header with a plus icon.

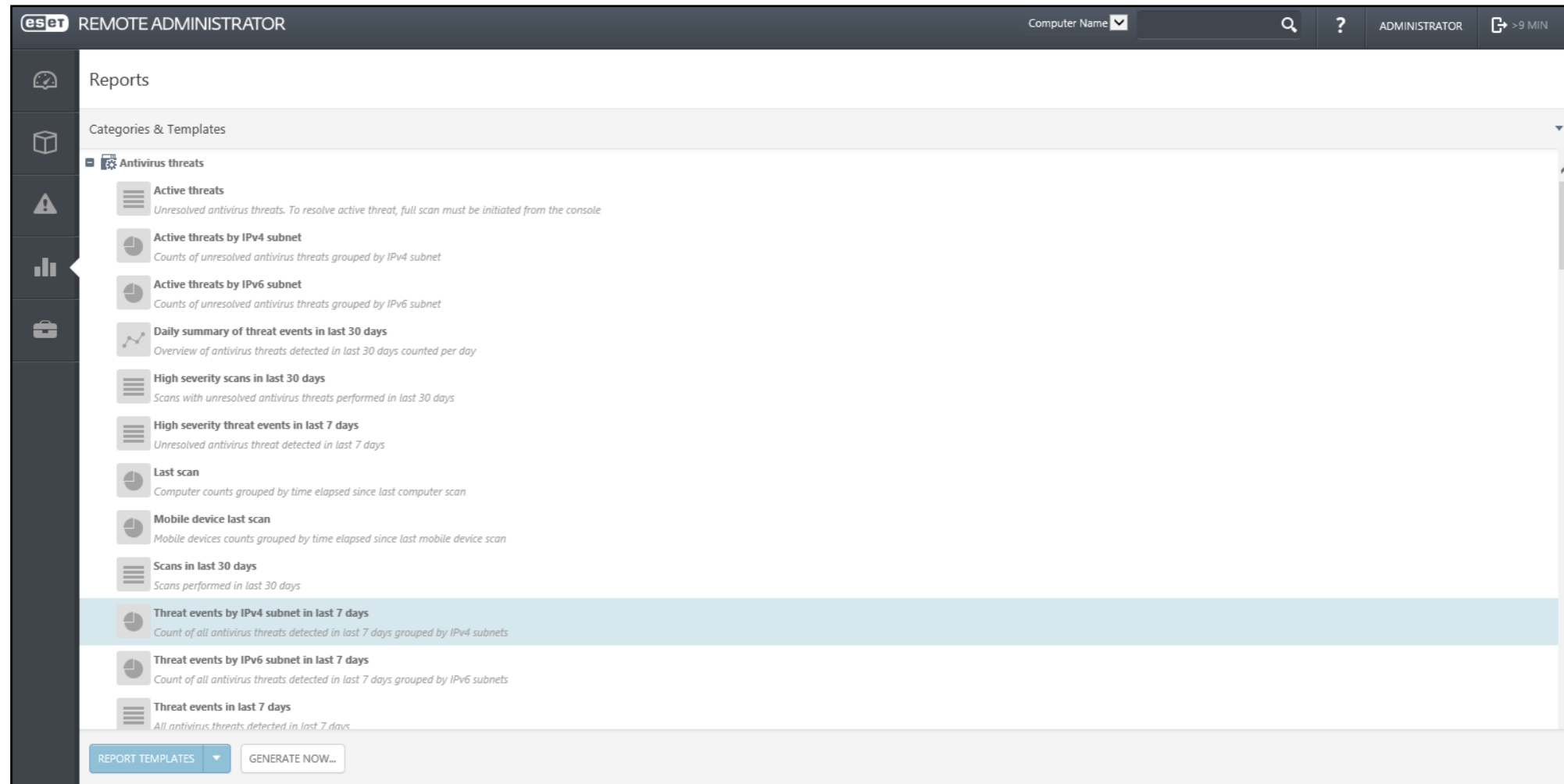
At the bottom of the window, there are 'FINISH' and 'CANCEL' buttons.

## Riportok

Az ESET Remote Adminsitrator számtalan előredefiniált riport készítésére és elküldésére alkalmas, de ugyanúgy készíthetők vele átfogó, testre szabott kimutatások is.



A riportokat a webes felület főablakán, a balról beúszó menüben a **Reports** menüpontra kattintva kezelheti.



Részletesen testre szabható riportokat ugyanezen az oldalon a **REPORT TEMPLATES** gombra kattintva a **New Report Template...** opciót kiválasztva készíthet.

The screenshot shows the 'New Report Template - Basic' configuration page in the ESET Remote Administrator interface. The page is divided into several sections:

- Navigation:** A sidebar on the left contains icons for home, reports, alerts, and a briefcase.
- Header:** The top header includes the ESET logo, 'REMOTE ADMINISTRATOR', an IPv4 address, a search icon, a help icon, the user role 'ADMINISTRATOR', and a session duration indicator '>9 MIN'.
- Form Fields:**
  - NAME:** A text input field containing 'Custom report'.
  - DESCRIPTION:** An empty text input field.
  - CATEGORY:** A dropdown menu showing 'Computers' and a 'CHANGE...' button below it.
- Expandable Sections:** Below the form are several sections, each with a plus icon and a title:
  - CHART:** Includes a red warning triangle icon.
  - DATA**
  - SORTING**
  - FILTER**
  - SUMMARY**
- Footer:** At the bottom of the form are three buttons: 'FINISH', 'CANCEL', and 'MANDATORY SETTINGS >'.

## További információk

Köszönjük, hogy végigolvasta a dokumentumot!

További kérdéseivel forduljon bizalommal [kollégáinkhoz](#), tekintse meg további segédleteinket és útmutatóinkat [honlapunkon](#) vagy a folyamatosan bővülő [ESET Tudásbázis](#) oldalon.