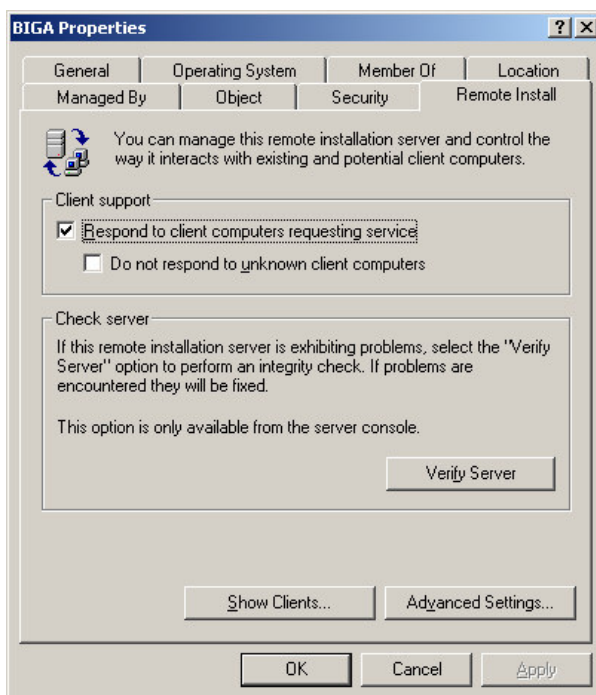


Remote Installation Services

A mai alkalommal a RIS kiszolgáló beállításait nézzük végig. A RIS összes felügyeleti szerve be van építve az Active Directory Users and Computers MMC snap-inbe, így ezzel a megszokott eszközzel (szinte) minden RIS-karbantartási feladatot elvégezhetünk.

A RIS kiszolgáló beállításai

Amikor a RIS kiszolgálóobjektumának tulajdonságait előhúzzuk (AD Users and Computers konzolon a kiszolgáló objektumán jobb klikk - properties), ott a következő kép fogad minket.

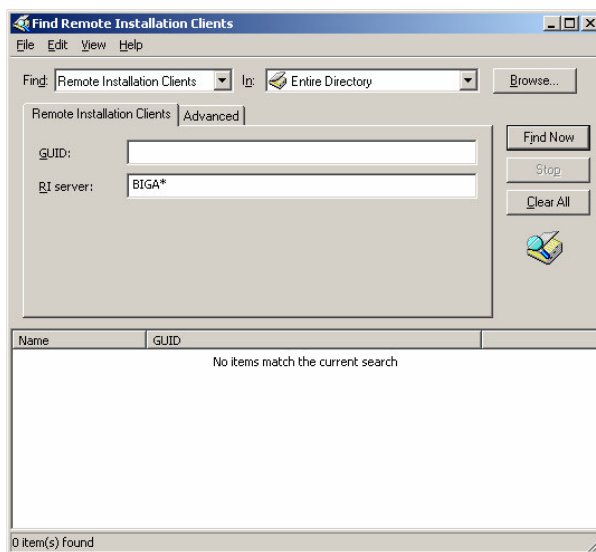


Remote Install tulajdonságok

Client support – itt lehet be és kikapcsolni a RIS kiszolgálást. A fenti képen látható beállítás minden ügyfélnek válaszolni fog aki hozzá eljut, míg ha bekapcsoljuk a második jelölőnégyzet is akkor csak azoknak fog válaszolni akiknek van már megfelelően előkészített számítógépazonosítója a tartományban. Értelmszerűen, ha egyik pipa sincs a helyén, akkor a RIS kiszolgálót kikapcsoltuk.

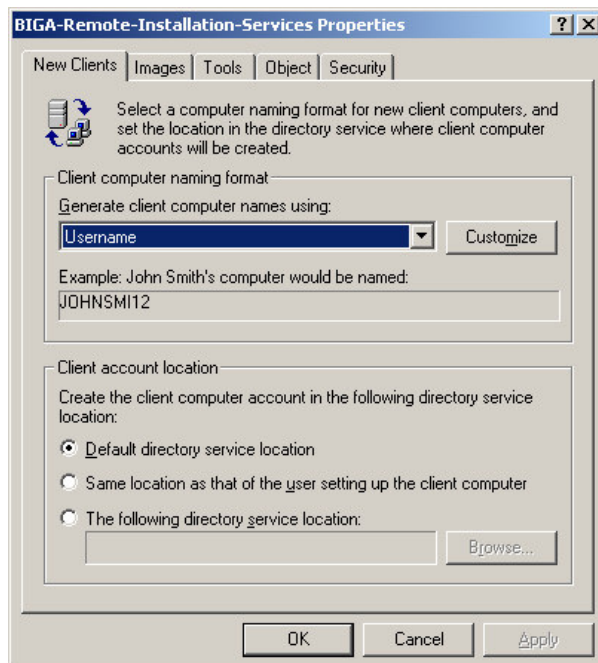
Verify Server – ellenőrizhetjük vele, hogy minden rendben van-e a kiszolgálóval – nem tesz mást, mint a risetup.exe-t indítja –check kapcsolóval, és csak akkor elérhető ez, ha az AD Users and Computers snap-int futtatjuk magán a kiszolgálón.

Show Clients – megmutatja azokat az ügyfeleket, akiket az adott RIS kiszolgálóról telepítettünk. Egyszerű keresés az Active Directory-ban.



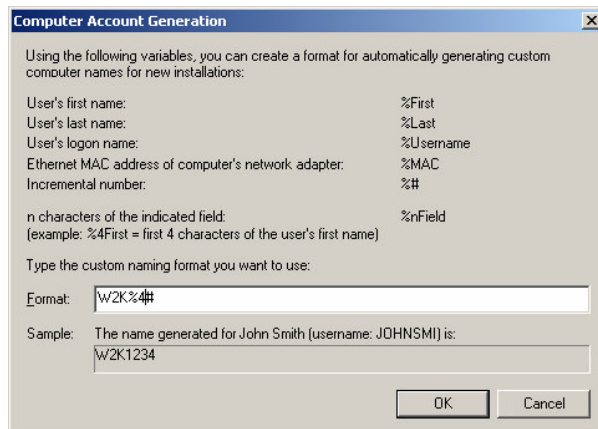
RIS ügyfelek felkutatása a tartományban

Advanced Settings – itt tulajdonképp az ügyfelek elnevezését szabályozhatjuk, valamint a telepítőkészletek hozzáadása/eltávolítása is innen lehetséges.



□ **Ügyfelek elnevezése**

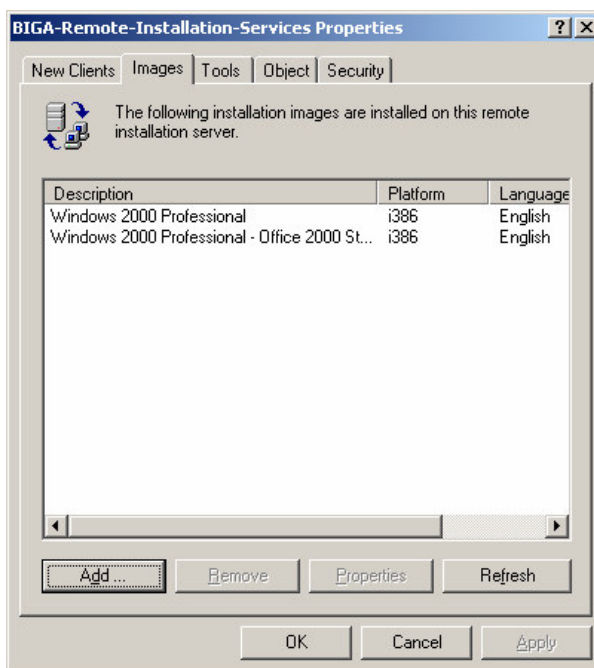
Nézzük meg közelebbről először az ügyfelek elnevezéseit. Itt tudjuk megmondani, hogy mi is legyen az Automatikus telepítéskor létrehozott gép név az Active Directory-ban. Választhatjuk a telepítést végző felhasználó nevét, vagy a vezetéknev és a keresztnév kombinációt, vagy NP plusz a gép MAC címe, de választhatunk egyedi elnevezést is.



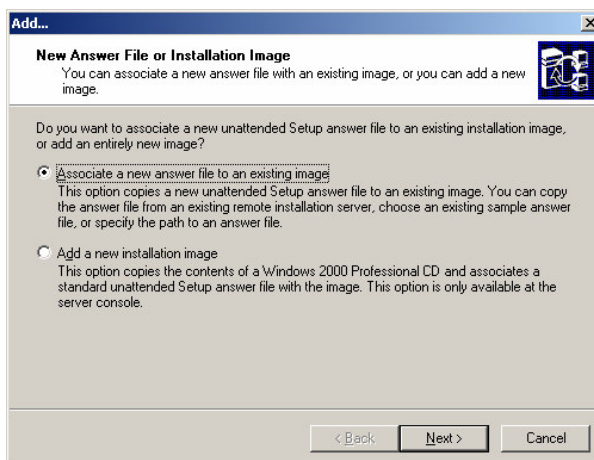
□ **Ügyfélnevek testreszabása**

Ilyenkor mi magunk rakhatjuk össze az elnevezési konvenciót, majdnem ahogy tetszik. Nézzük a képen is látható példát: Minden gép neve W2K-val fog kezdődni, majd jön egy növekvő szám, a mi esetünkben max. 4 számjegyű lehet, mindig a következő legkisebb még használaton kívüli számot fogja feljárnani az Ügyféltelepítő Varázsló. Ezen a néven fogja létrehozni a gépezonosítót a tartományban. Ha nem adunk meg számot, akkor az alapértelmezés szerint 2 számjegy kerülhet a végére.

Izgalmasabb az *Images* fül itt a beállítások közt.



Itt láthatjuk az összes telepítőkészletet, amelyek az adott RIS kiszolgálón megtalálhatóak. Egy telepítőkészlet két részből áll: vannak a telepítéshez szükséges állományok a RemoteInstall\Setup\%Language%\Images\<image dir> könyvtárban, és van a felügyelet nélküli telepítéshez használt válaszfájl – SIF fájl. Több SIF fájlt is rendelhetünk ugyanazokhoz a telepítendő állományokhoz, de egy SIF fájl mindenképp szükséges egy garnitúra telepítőkészlethez. Ebben a menüben adhatunk hozzá válaszfájlokat (Add gomb) a meglévő állományokhoz.



❑ Telepítőkészlet varázsló

Ha egy teljesen új telepítőkészletet akarunk létrehozni, (mondjuk több nyelvi verzióra is szükségünk van), akkor válasszuk az *Add a new installation Image* varázslót. Ilyenkor bekéri a Windows 2000 telepítő CD-t, fel fogja másolni annak tartalmát a megadott könyvtárba, és egy alapértelmezett válaszfájlt is hozzá fog rendelni.

Ha azonos a nyelvi verzió, de szükségünk van eltérő beállításokra a telepítésénél, akkor nincs más dolgunk, mint egy előre létrehozott SIF fájlt összekötünk a már fentlevő telepítő állományokkal. Legegyszerűbb az alapértelmezés szerint bepakolt SIF fájlt szerkeszteni. A következő részben lesz róla szó hogy mit lehet és kell tenni a válaszfájllal annak érdekében, hogy az valóban jól működjön.

Ezek a válaszfájlok a RemoteInstall\Setup\%Language%\Images\<imagedir>\i386\templates könyvtárban tárolódnak. Amikor letölünk egy telepítő készletet (Remove gomb) tulajdonképp csak a SIF fájlt töröljük, a mögötte levő X Mb-ot nekünk kell letörölni külön, az Explorer segítségével.

Azonos nyelvi és service pack verzióból nem tehetünk fel több készletet, de lássuk be, erre nincs is semmi szükség.

Viszont egyszerűen elérhetjük, hogy rögtön a Service Packal ellátott telepítő állományokat használjuk az ügyfelek telepítésénél. Lássuk hogyan:

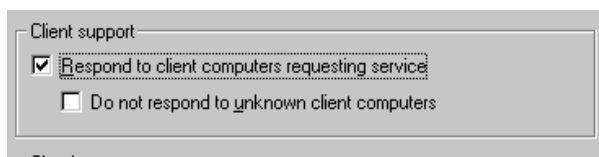
- Fel kell másoljuk a Windows 2000 Professional telepítő CD teljes tartalmát egy könyvtárba a merevlemezre. Legyen ez mondjuk d:\win2ksp2.pro könyvtár.
- Ezek után fogjuk a Service Packot, azt is bontsuk ki /x kapcsolóval.
- Majd az i386\Update könyvtárból futtassuk a következőt: update -s:<dir> – annak könyvtárnak a nevét és teljes elérési útját kell megadni, ahová a CD-t felmásoltuk, **nem** benne az i386 könyvtárat! Tehát az előbbi példánál maradva a parancs így fog kinézni: update -s:d:\win2ksp2.pro.
- Mindezek után hozzáadhatjuk az így előkészített telepítőállományokat az *Add new installation image varázslóval*, vagy a *risetup.exe* elindításával.
- Utolsó lépésként az eddig is használt válaszfájlt hozzárendeljük a telepítőállományokhoz, és máris kész van a friss, ropogós telepítő készlet.

Az ügyfélgépek előkészítése

Biztonsági szempontból mindenképp megfontolandó, hogy a RIS-es ügyfélgépeknek **jó előre** létrehozunk azonosítót a tartományban. Ezt hívjuk pre-stagingnek. Miért is jó ez? Nos, a felhasználó még véletlenül sem fogja tudni elindítani a telepítést, illetve nem kell a felhasználóknak extra jogokat osztani az Active Directoryban ahhoz, hogy telepíteni tudja a saját gépét, ha a rendszergazda előkészíti a gép accountot is.

A cikk legelején már láttuk, hogy a RIS kiszolgáló gép accountjának Remote Install tulajdonságai közt találhatjuk minjárt azt a beállítást, hogy a RIS kiszolgáló mely ügyfeleknek válaszoljon.

A lenti kép beállítása azt mutatja hogy a RIS kiszolgáló be van kapcsolva, tehát válaszolni fog az ügyfelek kéréseire válogatás nélkül. Ha a második négyzetben is ott figyelne a pipa akkor csak azoknak az ügyfeleknek válaszolna a melyeket már előkészítettünk. Ezt két okból lehet hasznos bekapcsolni. Ha a hálózaton van más olyan ügyfél, amely PXE-t használ, de nem RIS-sel akarunk rá telepíteni dolgokat, akkor ezeknek az ügyfeleknek a RIS kiszolgáló nem fog válaszolni. Másik ok pedig hogy senki nem fog tudni kalóz módon felhúzni egy gépet RIS-sel, ha az nincs előkészítve az Active Directoryban, ugyanakkor mi sem fogunk tudni felvenni újakat csak akkor, ha valamilyen módon tudjuk a gép GUID-ját, és nem kell hozzá elindítani az ügyfél telepítő varázslót.



RIS kiszolgáló ki/be kapcsolása

Ahhoz hogy accountot tudjunk létrehozni az ügyfélgépnek a RIS telepítéshez, tudnunk kell annak egyedi azonosítóját, a GUID-ot. Ezt BIOS-ból meg lehet tudni, vagy ha elindítjuk az ügyféltelepítő varázslót az F12-vel, akkor miután beléptünk, ki fogja írni a gép nevét (amit generált neki a kiszolgáló), a GUID-ot, és a RIS kiszolgáló nevét. Ezen a ponton le kell kapcsolni az ügyfélgépet, elég megjegyezni a gép nevét, majd ezt az ügyfél account-ot lehet manipulálni annak érdekében, hogy a megfelelő névhez a megfelelő GUID tartozzon.

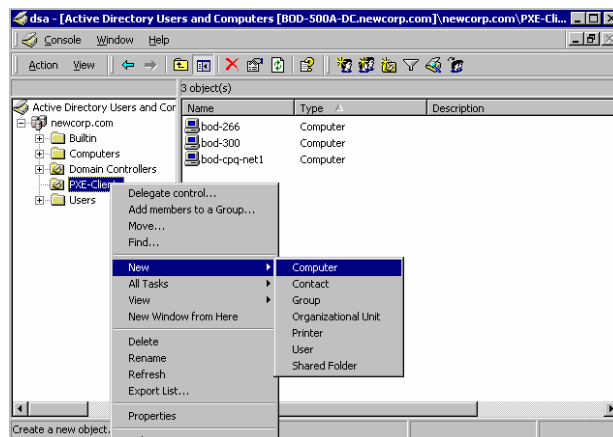
A GUID az egy csúnya 32-bites azonosító, amely a hálózati kártyához kötött. A PXE-t ismerő ügyfeleknél a GUID valahogy így néz ki:

```
{1f988641-3046-780a-1236-105146887113}
```

Amikor RIS indítólemezt használunk, ott a GUID nem más, mint az adott ügyfél hálózati kártyájának címe (MAC címe, rengeteg 0-val az elején, hogy kijöjjön a 32 bit:

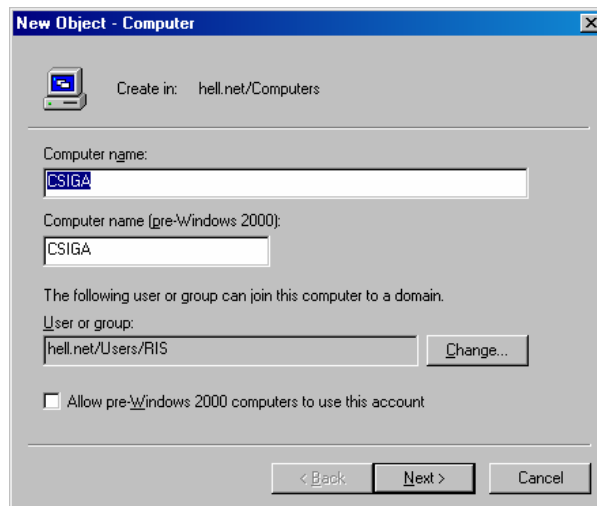
```
{00000000-0000-0000-0000-0050568F0102}
```

Miután megtudtuk a GUID-ot, az ügyfél előkészítéséhez az Active Directory Users and Computers-t használjuk.



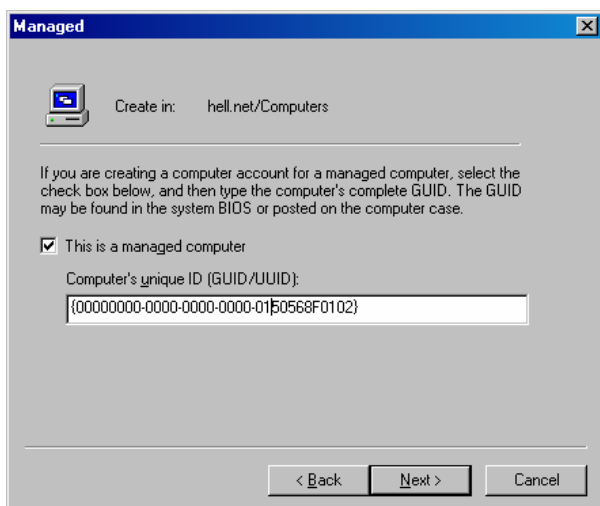
Új azonosító létrehozása

Ha a create a new computer (új számítógép létrehozása) opciót választjuk, megjelenik a következő párbeszédablak és beírhatjuk a számítógép nevét, valamint megadhatjuk azt, hogy az ügyfelet ténylegesen ki léptetheti be a tartományba. Alapbeállításként ez Domain Admins, ha ezt így hagyjuk, akkor hiába készítjük elő az ügyfélgép accountot, a RIS telepítés nem fog tudni elkezdődni csak olyan account segítségével, aki ennek a csoportnak a tagja. Tehát ide azt a csoportot kell megadni, amelynek tagja az, aki telepíteni fogja a gépet, vagy megadhatunk persze egy felhasználót is.



Új számítógép létrehozása

A következő párbeszédablakban a számítógép GUID-jét kell megadnunk (ha a RIS nincs telepítve, ez a párbeszédablak nem is jelenik meg).



GUID

Ezt a párbeszédablakot csak RIS kiszolgálókon vagy olyan kiszolgálókon és ügyfeleken tudjuk használni, ahol előzőleg telepítve lett az adminpak.msi.

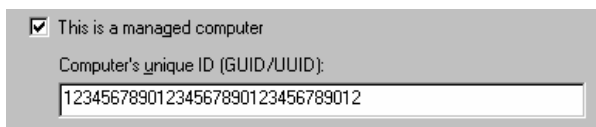
A RIS kiszolgáló a GUID segítségével ellenőrzi, hogy az ügyfél létezik-e már az Active Directory-ban.

Egy GUID egy ügyfélhez tartozhat, ezért, ha az ügyfélgépből úgy nyerjük ki a GUID-et hogy elindítottunk már egyszer a telepítőt, akkor először onnan kimásolhatjuk (CTRL+C) a GUID-et, azt az accountot töröljük az AD-ból, majd létrehozunk egy nekünk megfelelő néven, és itt beszúrjuk (CTRL+V) a kimásolt GUID-et, így biztos, hogy nem rontjuk el a gépelést.

Ha megadtuk a GUID-et akkor a következő párbeszédablakban megadhatjuk, hogy melyik RIS kiszolgálót használja az ügyfél. Ha manuálisan akarjuk elosztani a terhelést a hálózat RIS kiszolgálói között, hogy az egyes kiszolgálók csak a saját ügyfeleik kérését fogadják el, akkor itt pontosan megadhatjuk a RIS kiszolgáló nevét, amelyhez az adott ügyfélnek fordulni kell. Azonban ha ez a kiszolgáló nem működik, akkor más sem fogja az ügyfeleket kiszolgálni hiába elérhető még más RIS kiszolgáló is a környéken.

Ezután jön egy összegző képernyő, és már csak egy Next és elő is van készítve az ügyfélgép azonosítója.

De nézzük csak meg ezeket a GUID-okat! Ha a BOIS-ból kiolvasott GUID-et gépeljük be, akkor az így néz ki:



Az összegző ablakban pedig ez jelenik meg:

```
This is a managed PC.
GUID: {78563412-1290-5634-7890-123456789012}
Host Server: any available server
```

Nem egyezik azzal, ami itt az összegzésben megjelenik!

Közelebből megvizsgálva észrevehetjük, hogy az összegző képernyőn megjelenített szám első 16 bájta van megfordítva, a maradék 16 pedig a helyes sorrendben jelenik meg. Az információ, amit begépeztünk (12345678901234567890123456789012), „wire” formátumú (a hálózaton keresztül ebben a formában továbbítódik). Amikor a GUID megjelenik, „pretty print” formátumúvá alakul, ami a következőképpen néz ki: {78563412-1290-5634-7890-123456789012}

A GUID-et mindkét formában beírhatjuk, a program wire formátumúra alakítja és így menti az ügyfélgép account információi közt.. A felhasználói felületen a GUID-t mindig „pretty print” formátumban jelenik meg.

A szükséges jogosultságok

Ha a RIS-es telepítést maga a felhasználó fogja a saját felhasználói nevével és jelszavával indítani, akkor ahhoz extra jogokat kell biztosítanunk, hogy létre tudják hozni a gépük accountját a tartományban és hogy be is tudják léptetni azt. Amennyiben mi egyáltalán nem készítjük elő az előbbiekben leírt módon a gépeket, akkor ahhoz, hogy ezt megtehessék, a következő jogokra van szükségük az OU-n, amely az újonnan létrehozott gép azonosítóját tárolja:

- Olvasási jog
- Számítógép-objektumok létrehozása

Amennyiben előkészítettük az ügyfélgépek azonosítóit, akkor az egyes gépazonosítókhoz kell a következő jogokat rendelni annak érdekében, hogy a felhasználó azt a saját azonosítójával később telepíteni is tudja:

- Az ügyfélaazonosító jelszavának változtatása/beállítása
- A számítógépobjektum minden tulajdonságának olvasása/írása (Read/write all properties on the computer object)
- A számítógépobjektum jelszavának változtatása/beállítása.

Tehát nem az objektumot tartalmazó OU-hoz hanem magához a gép azonosítójához kell ezeket a jogokat rendelni!

Ez lehetővé teszi a felhasználó számára, hogy telepítse rendszerét, de csak akkor, ha egy rendszergazda előkészíti a gépazonosítót.

Tudom, az is elég ritkán fordul elő, hogy a felhasználóra bízunk a saját gépének telepítését, de itt lehet bátran, hisz erre találták ki. Ne kelljen előtte ülni, CD-ket adagolni időről-időre, egyszerűen lehet indítani. S ha átszabjuk a varázsló oldalait (erről lesz szó a következő részben), akkor magyarul beszél a felhasználóhoz. Szóval minden adott ahhoz, hogy valóban a legkevesebb beavatkozással telepítsük az ügyfélgépeket. Ám nem szeretünk kiadni felhasználóknak extra jogokat, ezért aztán jó megoldás az is, ha létrehozunk az AD-ban egy olyan felhasználót, akinek semmi más joga nincs, mint a RIS-sel telepített gépeket beléptetni a tartományba, ha azt a rendszergazda előkészítette. Majd amikor telefonon keresztül navigáljuk a felhasználót, hogyan is indítsa el a telepítőt, akkor egy ártatlan felhasználó azonosítóját kell megadnia, nem a sajátját ahhoz hogy elinduljon a telepítő. Így a rendszergazdának is a lehető legkevesebb a dolga, ugyanakkor nem hoztunk létre újabb biztonsági rést a pajzson, amely így is eléggé lyuggatott szegény.

Dorner Csilla
MCSE